PASS4SURES.COM

A Composite Solution With Just One Click

Microsoft

70-643 PRACTICE EXAM

TS: Windows Server 2008 Applications Infrastructure

Question: 1

A server runs Windows Server 2008. The Terminal Services role is installed on the server. You deploy a new application on the server. The application creates files that have an extension of .xyz. You need to ensure that users can launch the remote application from their computers by double-clicking a file that has the .xyz extension. What should you do?

A. Configure the Remote Desktop Connection Client on the users' computers to point to the server.
B. Configure the application as a published application by using a Remote Desktop Program file.
C. Configure the application as a published application by using a Windows Installer package file.
D. Configure the application as a published application by using a Terminal Server Web Access Web site.

Answer: C

Explanation:
Launching Apps from the Desktop For users who want to double-click documents to launch the application, terminal services now provides the ability to "install" the remote application's link to the desktop. This process effectively wraps the RemoteApp's RDP file into a Windows Installer package—an MSI file—that is later installed to desktops in the environment. At the same time, the installed MSI can modify the file extension associations on the desktop to reroute a double-clicked file to its associated RemoteApp on the terminal server. Figure 3 shows how the file extension associations have been modified on a client system after a Word RemoteApp is installed. Now, double-clicking any of the common Word file extensions will launch Word via the Remote Desktop Connection.

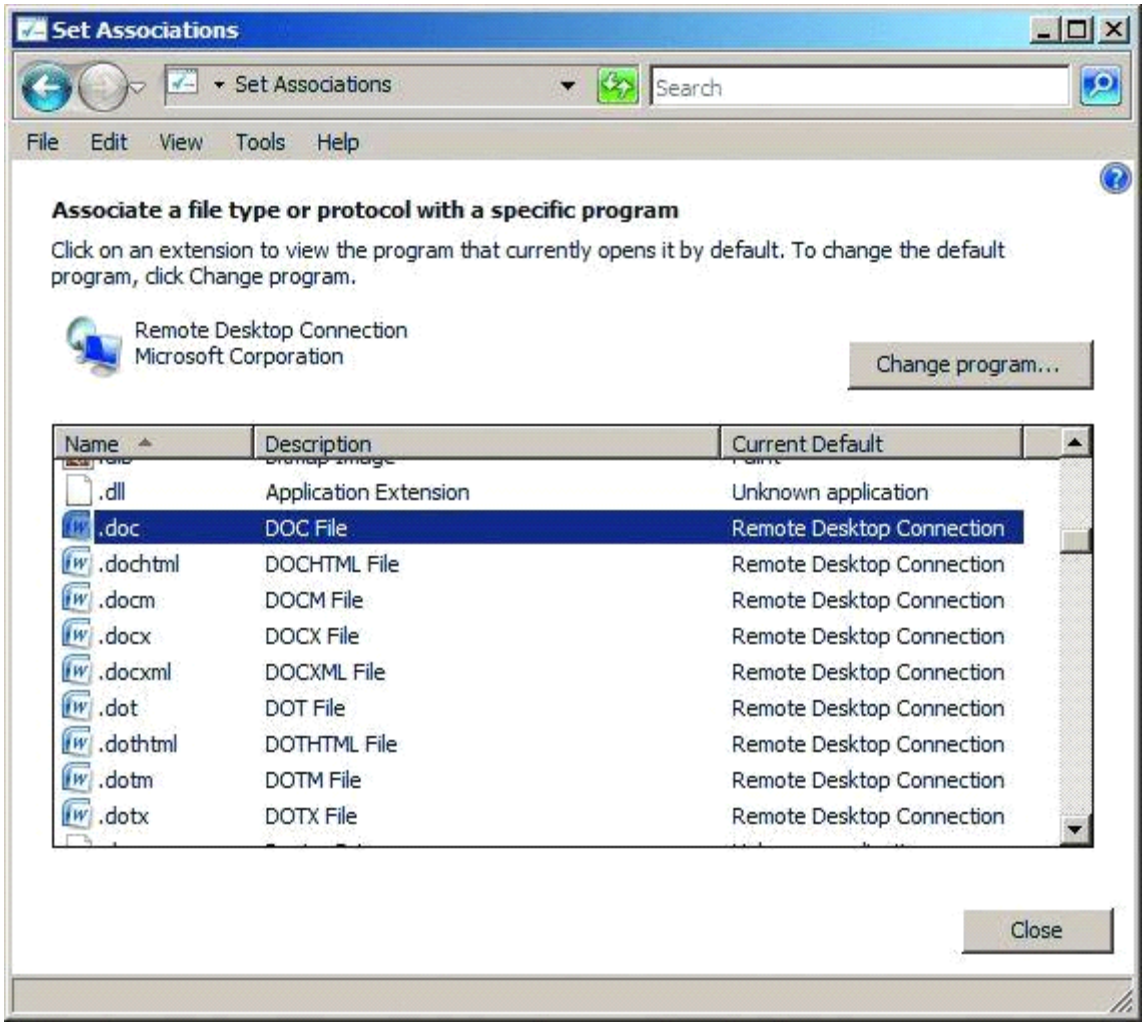


Figure 3 File extension associations that have been altered to launch the Remote Desktop Connection
To create a Windows Installer package out of an existing RemoteApp, first navigate to the TS RemoteApp Manager. Right-click the RemoteApp of interest and select Create Windows Installer Package. By default, all created Windows Installer packages are stored in the location C:\Program Files\Packaged Programs, but this location can be changed from within the RemoteApp Wizard. Also configurable within the wizard are the name and port for the server that will host the RemoteApp, as well as server authentication, certificate settings, and TS Gateway settings. Settings that relate to the application's location after installation to a candidate desktop are shown in Figure 4. As you can see, it is possible to create a shortcut on the desktop as well as to a location within the Start menu folder. The most important checkbox on this screen is at the very bottom. It's the checkbox for Take over client settings, and it re-associates any file extension associations for the RemoteApp from the local desktop to the terminal server. This checkbox must be selected if you want users to be able to double-click documents to launch their TS-hosted application. Click Next and Finish to complete the wizard. Please Note: -Since Windows2008R2 Terminal Services (TS) is now rebranded to Remote Desktop Services (RDS)-
Source: http://technet.microsoft.com/en-us/query/dd314392

Question: 2

You have a server that runs Windows Server 2008 R2. The server has the RD Gateway role service installed. You need to provide a security group access to the RD Gateway server. What should you do?

A. Add the security group to the Remote Desktop Users group.
B. Add the security group to the TS Web Access Computers group.

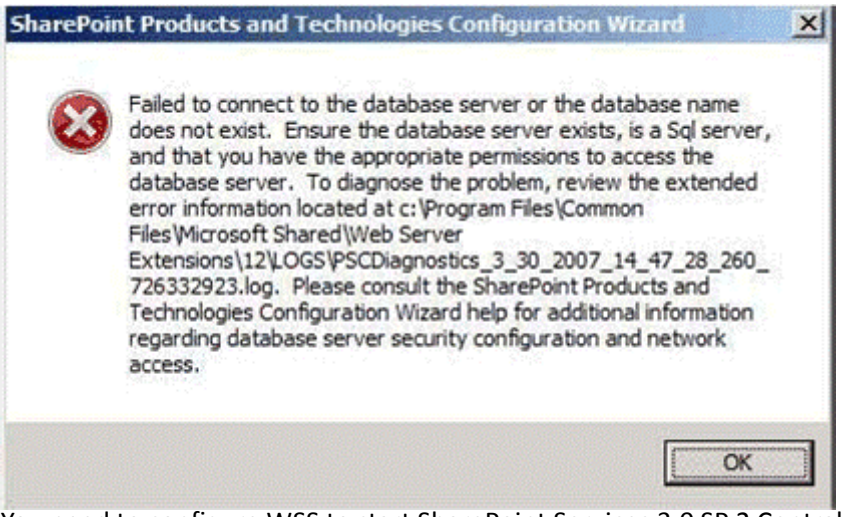
C. Create and configure a Remote Desktop Resource Authorization Policy.
D. Create and configure a Remote Desktop Connection Authorization Policy.

Answer: D

Explanation:
Remote Desktop connection authorization policies (RD CAPs) allow you to specify who can connect to an RD Gateway server.
Source: http://technet.microsoft.com/en-us/library/cc753324.aspx

Question: 3

Your company uses Public folders and Web Distributed Authoring and Versioning. The company asks you to install Microsoft Windows SharePoint Services (WSS) as a server in a new server farm. You plan to install WSS on a server that runs Windows Server 2008 R2. You start the Configuration Wizard to begin the installation. You receive an error message as shown in the exhibit.



You need to configure WSS to start SharePoint Services 3.0 SP 2 Central Administration. What should you do?

A. Install the Windows Internal Database.
B. Install a Microsoft SQL Server 2005 server.
C. Install the Active Directory Rights Management Services role.
D. Install the Active Directory Lightweight Directory Services role.

Answer: B

Explanation:
To resolve this problem, you need to install Microsoft SQL Server 2005 server on the farm. This error message occurs when either the SQL Server does not exist or the SQL Server services id stopped. The server farm account is used to access your configuration database. It also acts as the application pool identity for the SharePoint Central Administration application pool, and it is the account under which the Windows SharePoint Services Timer service runs. The SharePoint Products and Technologies Configuration Wizard adds this account to the SQL Server Logins, the SQL Server Database Creator server role, and the SQL Server Security Administrators server role. If SQL Server is not available then the above mentioned error message will appear.
Reference: Configuration Wizard - Failed to Connect
http://blogs.msdn.com/neilth/archive/2008/04/25/failed-to-connect-or-database-name-does-not-exist.aspx

Question: 4

You manage a member server that runs Windows Server 2008 R2. The server runs the Remote Desktop Gateway (RD Gateway) role service. You need to find out whether a user named User1 has ever connected to his office workstation through the RD Gateway server. What should you do?

A. View the events in the Monitoring folder from the RD Gateway Manager console.
B. View the Event Viewer Security log.
C. View the Event Viewer Application log.
D. View the Event Viewer Terminal Services-Gateway log.

Answer: D

Explanation:
By using TS Gateway Manager, you can specify the types of events that you want to monitor, such as unsuccessful or successful connection attempts to internal network computers through a TS Gateway server. When these events occur, you can monitor the corresponding events by using Windows Event Viewer. TS Gateway server events are stored in Event Viewer under Application and Services Logs\Microsoft\Windows \Terminal Services-Gateway\.
Source: http://technet.microsoft.com/en-us/library/cc730618(WS.10).aspx

Question: 5

Your company has an Active Directory domain. All the servers in the company run either Windows Server 2008 R2 or Windows Server 2003. A Windows Server 2003 server named Server1 runs Microsoft SQL Server 2005 SP2 and Microsoft Windows SharePoint Services (WSS) 2.0. The company plans to migrate to WSS 3.0 SP2 on a Windows Server 2008 R2 server named Server2. You need to migrate the configuration and content from Server1 to Server2. What should you do?

A. Back up the SharePoint configuration and content from Server1. Install WSS 3.0 SP2 on Server2. Restore the backup from Server1 to Server2.
B. Upgrade Server1 to Windows Server 2008 R2. Back up the SharePoint configuration and content from Server1. Install WSS 3.0 SP2 on Server2. Restore the backup from Server1 to Server2.
C. Back up the SQL Server 2005 configuration and the WSS 2.0 databases from Server1. Install SQL Server 2005 on Server2. Restore the SQL Server 2005 backup from Server1 to Server2.
D. Back up the WSS 2.0 configuration and content from Server1. Install WSS 2.0 on Server2. Restore the backup from Server1 to Server2. Perform an in-place upgrade of WSS 2.0 to WSS 3.0 SP2 on Server2.

Answer: D

Explanation:
To migrate to SharePoint Services (WSS) 3.0. from Server1 to Server2 with all the configuration and content, you need to install WSS 2.0 on Server2. Back up the WSS 2.0 configuration and content from Server1 and restore the backup from Server1 to Server2. Perform an in-place upgrade of WSS 2.0 to WSS 3.0 on Server2. When you run an in-place upgrade, all content and configuration data is upgraded in-place, at one time. When you start the in-place upgrade process, the Web server and Web sites remain offline until the upgrade has been installed. In-place upgrades are best for a stand-alone server and small installations as in this case Reference: Install and configure Office SharePoint Server for an in-place upgrade
http://technet.microsoft.com/en-us/library/cc263212(TechNet.10).aspx
Reference: Determine upgrade approach (Office SharePoint Server)
http://technet.microsoft.com/en-us/library/cc263447(TechNet.10).aspx

Question: 6

Your company has an Active Directory domain. You have a server named KMS1 that runs Windows Server 2008 R2. You install and configure Key Management Service (KMS) on KMS1. You plan to deploy Windows Server 2008 R2 on 10 new servers. You install the first two servers. The servers fail to activate by using KMS1. You need to activate the new servers by using the KMS server. What should you do first?

A. Complete the installation of the remaining eight servers.
B. Configure Windows Management Instrumentation (WMI) exceptions in Windows Firewall on the new servers.
C. Install Volume Activation Management Tool (VAMT) on the KMS server and configure Multiple Activation Key (MAK) Proxy Activation.
D. Install Volume Activation Management Tool (VAMT) on the KMS server and configure Multiple Activation Key (MAK) Independent Activation.

Answer: A

Explanation:
Key Management Service
With KMS, IT pros can complete activations on their local network, eliminating the need for individual computers to connect to Microsoft for product activation. KMS is a lightweight service that does not require a dedicated system and can easily be co-hosted on a system that provides other services. By default, volume editions of Windows 7 and Windows Server 2008 R2 connect to a system that hosts the KMS service to request activation. No action is required from the user.
KMS requires a minimum number of computers (physical or virtual machines) in a network environment.
The organization must have at least five computers to activate Windows Server 2008 R2 and at least 25 computers to activate clients that are running Windows 7. These minimums are referred to as activation thresholds.
To use KMS activation with Windows 7, the computer must have the qualifying OS license (often obtained through OEMs as part of the new PC purchase) and contain a Windows Marker in BIOS.
Source: http://technet.microsoft.com/en-us/library/ff793423.aspx

Question: 7

You have four Remote Desktop Session Host Servers that run Windows Server 2008 R2. The Remote Desktop Session Host Servers are named Server1, Server2, Server3, and Server4. You install the Remote Desktop Connection Broker role service on Server1. You need to configure load balancing for the four Remote Desktop Session Host Servers. You must ensure that Server2 is the preferred server for Remote Desktop Services sessions. Which tool should you use?

A. Group Policy Management
B. Remote Desktop Session Host Configuration
C. Remote Desktop Connection Manager
D. RD Gateway Manager

Answer: B

Explanation:
You can configure a Remote Desktop Session Host (RD Session Host) server to join a farm in RD Connection Broker, and to participate in RD Connection Broker Load Balancing, by using the Remote Desktop Session Host Configuration tool.
To configure RD Connection Broker settings

1. On the RD Session Host server, open Remote Desktop Session Host Configuration. To open Remote Desktop Session Host Configuration, click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Session Host Configuration .
2. In the Edit settings area, under RD Connection Broker, double-click Member of farm in RD Connection Broker.
3. On the RD Connection Broker tab of the Properties dialog box, click Change Settings.
4. In the RD Connection Broker Settings dialog box, click Farm member.
5. In the RD Connection Broker server name box, type the name of the RD Connection Broker server.
6. In the Farm name box, type the name of the farm that you want to join in RD Connection Broker.
7. Click OK to close the RD Connection Broker Settings dialog box.
8. To participate in RD Connection Broker Load Balancing, select the Participate in Connection Broker Load-Balancing check box.
9. Optionally, in the Relative weight of this server in the farm box, modify the server weight. By default, the value is 100. The server weight is relative. Therefore, if you assign one server a value of 50, and one a value of 100, the server with a weight of 50 will receive half the number of sessions.
10. Verify that you want to use IP address redirection. By default, the Use IP address redirection setting is enabled. If you want to use token redirection mode, select Use token redirection. For more information, see About IP Address and Token Redirection.
11. In the Select IP addresses to be used for reconnection box, select the check box next to each IP address that you want to use.
12. When you are finished, click OK.
Source: http://technet.microsoft.com/en-us/library/cc771383.aspx

Question: 8

You have a server that runs Windows Server 2008 R2. The server has Microsoft SharePoint Foundation 2010 installed. The server is configured to accept incoming email. You create a new document library. You need to ensure that any user can send email to the document library. What should you do?

A. Modify the RSS setting for the document library.
B. Modify the permissions for the document library.
C. Modify the incoming email settings for the document library.
D. Enable anonymous authentication for the Web application.

Answer: C

Explanation:
Enable and configure email settings for a library
Use this procedure to enable and configure email settings for a library to receive email messages in the SharePoint document library in a site.
Enable and configure email settings for a library
1. Open the site in which you want to receive email messages by using either of the following methods:
- In Internet Explorer, type the URL o the site.
- On the View Site Collection page, click the site collection that you want to view.
2. In the left navigation pane of the home page, click View All Site Content.
3. In the Documents section, click a document library name to open the library for which you want to enable and configure email settings.
4. On the Settings menu, click Document Library Settings, Picture Library Settings, or Form Library Settings, depending on the kind of library that you are enabling and configuring.
5. In the Communications section, click Incoming email settings.
6. In the Email section, select Yes to enable this library to receive email messages.
7. In the Email address box, type a unique name to use as part of the email address for this library.

8. In the Email Attachments section, decide where to save and how to group the email attachments in this library, and then choose whether to overwrite files that have the same name.
Note: If you decide not to overwrite files that have the same name and then later try to save a file that has the same name as one that already exists in the library, four random digits are appended to the file name for the new attachment. If this action fails, a globally unique identifier (GUID) is appended to the file name. If neither of these actions can produce a unique file name, the attachment is discarded.
9. In the Email Message section, choose whether to save the original email message in this library. If you select Yes, the original message is saved as a separate item in the library.
10. In the Email Meeting Invitations section, choose whether to save the attachments to your meeting invitations in this library.
11. In the Email Security section, choose whether to archive email messages only from members of the site who can write to the library or to archive regardless of who sends the email message.
12. Click OK to save the changes that you have made in the settings.
Source: http://technet.microsoft.com/en-us/library/cc262800.aspx

Question: 9

A server named Server2 runs Windows Server 2008 R2. The Remote Desktop Services server role is installed on Server2. You plan to deploy an application on Server2. The application vendor confirms that the application can be deployed in a Remote Desktop Services environment. The application does not use Microsoft Windows Installer packages for installation. The application makes changes to the current user registry during installation. You need to install the application to support multiple user sessions. What should you do?

A. Run the mstsc /v:Server2 /admin command from the client computer to log on to Server2. Install the application.
B. Run the change user /execute command on Server2. Install the application and run the change user /install command on Server2.
C. Run the change user /install command on Server2. Install the application and run the change user /execute command on Server2.
D. Run the change logon /disable command on Server2. Install the application and run the change logon /enable command on Server2.

Answer: C

Explanation:
Change user
Changes the install mode for the terminal server

```
Parameter   Description
/execute    Enables .ini file mapping to the home directory. This is the default
setting.
/install    Disables .ini file mapping to the home directory. All .ini files are
read and written to the system directory.            You must disable .ini file
mapping when installing applications on a terminal server.
/query      Displays the current setting for .ini file mapping.
/?          Displays help at the command prompt.
```

Source: http://technet.microsoft.com/en-us/library/cc730696(WS.10).aspx

Question: 10

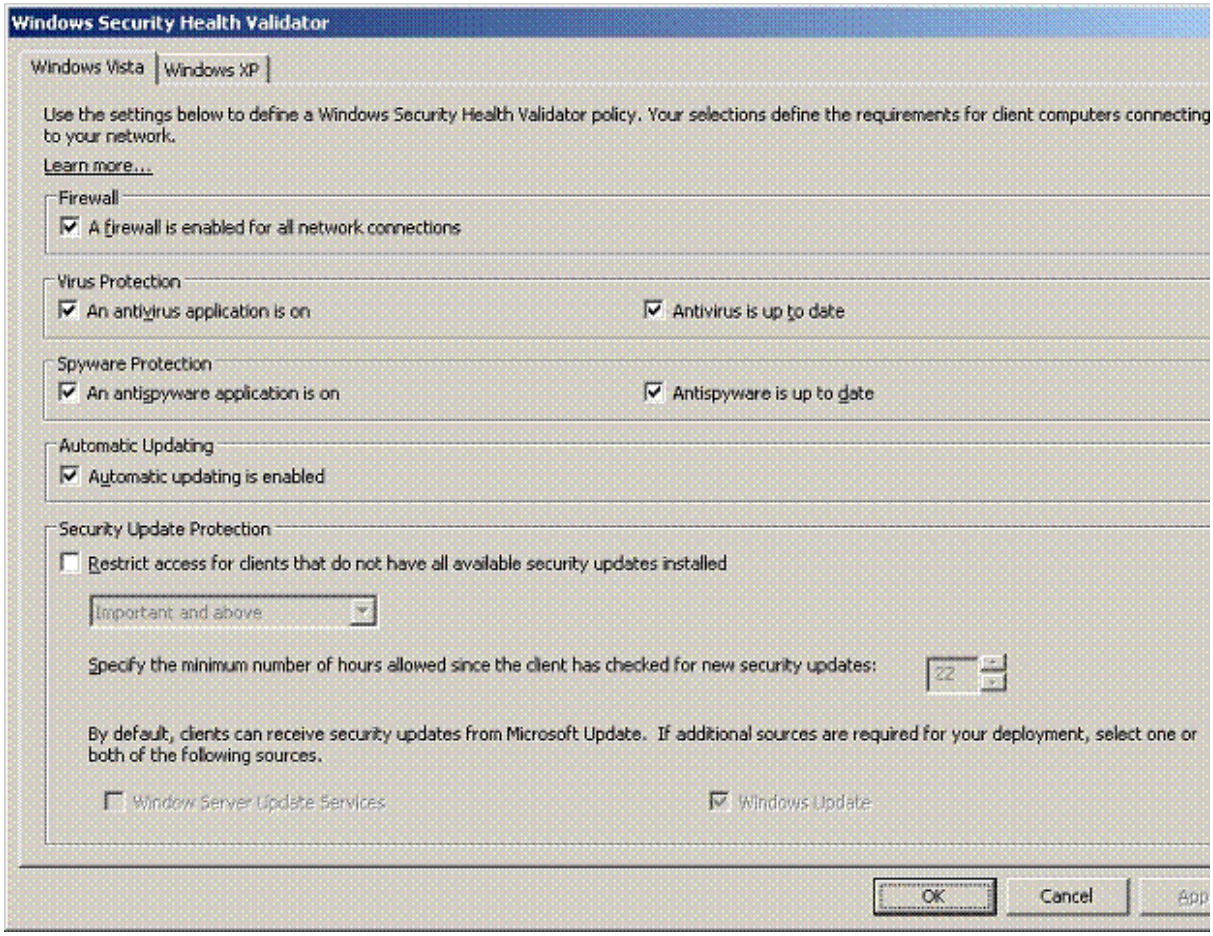
Your company has an Active Directory domain. A server named Server2 runs Windows Server 2008 R2. All client computers run Windows 7. You install the Remote Desktop Services server role, RD Web Access role service, and RD

Gateway role service on Server2. You need to ensure that all client computers have compliant firewall, antivirus software, and antispyware. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Configure Network Access Protection (NAP) on a server in the domain.
B. Add the Remote Desktop Services servers to the Windows Authorization Access domain local security group.
C. Add the Remote Desktop Services client computers to the Windows Authorization Access domain local security group.
D. Enable the Request clients to send a statement of health option in the Remote Desktop client access policy.

Answer: A, D

Explanation
To ensure that all client machines have firewall, antivirus software and anti-spyware software installed, you should set the Request clients to sent a health option statement in the Remote Desktop Services client access policy and install and configure Network Access Protection (NAP) on the server in the domain.



Question: 11

Your network consists of a single Active Directory domain. The domain contains a server that runs Windows Server 2008 R2. The server has Microsoft SharePoint Foundation 2010 installed. You need to allow users to create distribution lists from a SharePoint site. What should you do on the SharePoint Foundation 2010 server?

A. Set the outgoing mail character set to 1200(Unicode).
B. Enable the SharePoint Directory Management Service.

C. Configure the site to accept messages from authenticated users only.
D. Configure the site to use the default Rights Management server in Active Directory Domain Services.

Answer: B

Explanation:
To configure WSS server in such a way that it allow users to create distribution lists from a SharePoint site, you need to enable the SharePoint Directory Management Service on the server. A distribution list contains the email addresses of existing address lists as well as the email addresses of other site members. Distribution lists are available only if the SharePoint Directory Management Service is enabled in Central Administration. All new subsites that are created in an email-enabled site collection are automatically email-enabled also. If you choose to use an existing group during site creation, the distribution list for the parent site (if available) will be associated with the new site
Reference: Introduction to incoming email/ New site creation walkthrough
http://office.microsoft.com/en-us/help/HA100823061033.aspx

Question: 12

You manage a server that runs Windows Server 2008. The server has the Web Server (IIS) role installed. The server hosts an Internet-accessible Web site that has a virtual directory named /orders/. A Web server certificate is installed and an SSL listener has been configured for the Web site.
The /orders/ virtual directory must meet the following company policy requirements:
- Be accessible to authenticated users only.
- Allow authentication types to support all browsers.
- Encrypt all authentication traffic by using HTTPS.
- All other directories of the Web site must be accessible to anonymous users and be available without SSL

You need to configure the /orders/ virtual directory to meet the company policy requirements.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Configure the Web site to the Require SSL setting.
B. Configure the /orders/ virtual directory to the Require SSL setting.
C. Configure the Digest Authentication setting to Enabled for the /orders/ virtual directory.
D. Configure the Basic Authentication setting to Enabled and the Anonymous Authentication setting to Disabled for the Web site.
E. Configure the Basic Authentication setting to Enabled and the Anonymous Authentication setting to Disabled for the / orders/ virtual directory.

Answer: BE

Explanation:
To configure the /salesorders/ virtual directory so that it is accessible to authenticated users only and it should allow authentication types to support all browsers, you need to configure the Basic Authentication setting to Enabled for the / salesorders / virtual directory, because the Basic authentication is supported by mostly all the browsers. Next you need to Disable the Anonymous Authentication setting to for the / salesorders / virtual directory, so that only authenticated users can access the virtual directory. Finally, you need to configure only the /salesorders / virtual directory to the Require SSL setting so that only the authentication traffic to this directory is encrypted and all other directories of the Website must be accessible to anonymous users and be available without SSL. To configure authentication for a virtual directory or a physical directory in a Web site, you need to configure the virtual directory for the Web site and not the website.
Reference: How to configure IIS Web site authentication
http://support.microsoft.com/kb/308160

Question: 13

You have a Windows Server 2008 R2 server that has the Web Server (IIS) server role installed. The server hosts multiple Web sites. You need to configure the server to automatically release memory for a single Web site. You must achieve this goal without affecting the other Web sites. What should you do?

A. Create a new Web site and edit the bindings for the Web site.
B. Create a new application pool and associate the Web site to the application pool.
C. Create a new virtual directory and modify the Physical Path Credentials on the virtual directory.
D. From the Application Pool Defaults, modify the Recycling options.

Answer: B

Explanation:
To configure the server to automatically release memory for a single website without affecting the other Web sites, you need to create a new application pool and associate the Web site to the application pool An application pool is a group of one or more URLs that are served by a worker process or a set of worker processes. Application pools set boundaries for the applications they contain, which means that any applications that are running outside a given application pool cannot affect the applications in the application pool. You can configure the server to automatically release memory or to release memory after reaching maximum used memory.
Reference: IIS 7.0: Managing Application Pools in IIS 7.0
http://technet2.microsoft.com/windowsserver2008/en/library/1dbaa793-0a05-4914-a065-4d109db3b9101033.mspx?mfr=true
Reference: IIS 7.0: Configuring Recycling Settings for an Application Pool
http://technet2.microsoft.com/windowsserver2008/en/library/0d5770e3-2f6f-4e11-a47c-9bab6a69ebc71033.mspx?mfr=true

Question: 14

You install the Windows Deployment Services (WDS) role on a server that runs Windows Server 2008 R2. You plan to install Windows 7 on a computer that does not support Preboot Execution Environment (PXE). You have a Windows 7 image that is stored on the WDS server. You need to start the computer and install the image that is stored on the WDS server. What should you create?

A. a capture image
B. a CD-ROM that contains PXE drivers
C. a discover image
D. an install image

Answer: C

Explanation:
To start the computer and install Windows Vista image stored on the WDS server, you should create the Discover image. If you have a computer that is not PXE enabled, you can create a discover image and use it to install an operating system on that computer. When you create a discover image and save it to media (CD, DVD, USB drive, and so on), you can then boot a computer to the media. The discover image on the media locates a Windows Deployment Services server, and the server deploys the install image to the computer. You can configure discover images to target a specific Windows Deployment Services server. This means that if you have multiple servers in your environment, you can create a discover image for each, and then name them based on the name of the server.

Reference:
http://technet2.microsoft.com/WindowsVista/en/library/9e197135-6711-4c20-bfad-fc80fc2151301033.mspx?mfr=true

Question: 15

Your company has an Active Directory domain. The Terminal Services role is installed on a member server named TS01. The Terminal Services Licensing role service is installed on a new test server named TS10 in a workgroup. You cannot enable the Terminal Services Per User Client Access License (TS Per User CAL) mode in the Terminal Services Licensing role service on TS10. You need to ensure that you can use TS Per User CAL mode on TS10. What should you do?

A. Join TS10 to the domain.
B. Disjoin TS01 from the domain.
C. Extend the schema to add attributes for Terminal Services Licensing.
D. Create a Group Policy object (GPO) that configures TS01 to use TS10 for licensing.

Answer: A

Explanation:
To ensure that you could employ Terminal Services per User CAL mode on TK2, you need to connect TK2 to the Active Directory domain because TS Per User CAL tracking and reporting is supported only in domain-joined scenarios.
Reference: TS Licensing/Are there any special considerations?
http://technet2.microsoft.com/windowsserver2008/en/library/5a4afe2f-5911-4b3f-a98a-338b442b76041033.mspx?mfr=true

Question: 16

You have a Windows Server 2008 R2 server that has the Web Server (IIS) server role installed. The server contains a Web site. You need to ensure that the cookies sent from the Web site are encrypted on users' computers. Which Web site feature should you configure?

A. Authorization Rules
B. Machine Key
C. Pages And Controls
D. SSL Settings

Answer: B

Explanation:
To encrypt the cookies sent from the website on the users' computer, you need to use machine key. Encrypting cookies is important to prevent tampering. A hacker can easily view a cookie and alter it. So to protect the cookie, machine key is used in ASP .NET 2.0. Encryption is based on a hash plus the actual data encrypted, so that if you try to change the data, it's pretty difficult. ASP.NET's ViewState uses the Machinekey config file section to configure the keys and such... this is important when the application is going to be run on a web farm, where load balancing webservers may be in no affinity mode.
Reference: http://www.codeproject.com/KB/web-security/HttpCookieEncryption.aspx

Question: 17

Your company has a server that runs Windows Server 2008 R2. The server has the Web Server (IIS) role installed. You need to activate SSL for the default Web site. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Obtain and import a server certificate by using the IIS Manager console.
B. Select the Generate Key option in the Machine Key dialog box for the default Web site.
C. Add bindings for the HTTPS protocol to the default Web site by using the IIS Manager console.
D. Install the Digest Authentication component for the Web server role by using the Server Manager console.

Answer: A, C

Explanation:
To activate SSL for the default Web site on the server, you need to get an appropriate certificate and create an HTTPS binding on a site. On Windows Vista and Windows Server 2008, HTTP.sys handles SSL encryption/decryption in kernel mode, resulting in up to 20% better performance for secure connections. Moving SSL to kernel mode requiresstoring SSL binding information in two places. First, the binding is stored in %windir%\system32\inetsrv\applicationHost.config for your site. When the site starts, IIS 7.0sends the binding to HTTP.sys and HTTP.sys starts listening for requests on the specified IP:Port (this works for all bindings). Second, SSL configuration associated with the binding is stored in HTTP.sys configuration.When a client connects and initiates an SSL negotiation, HTTP.sys looks in its SSL configuration for the IP:Port pair that the client connected to. The HTTP.sys SSL configuration must include a certificate hash and the name of the certificate's store for the SSL negotiation to succeed.
Reference: How to Setup SSL on IIS 7.0
http://learn.iis.net/page.aspx/144/how-to-setup-ssl-on-iis-7/

Question: 18

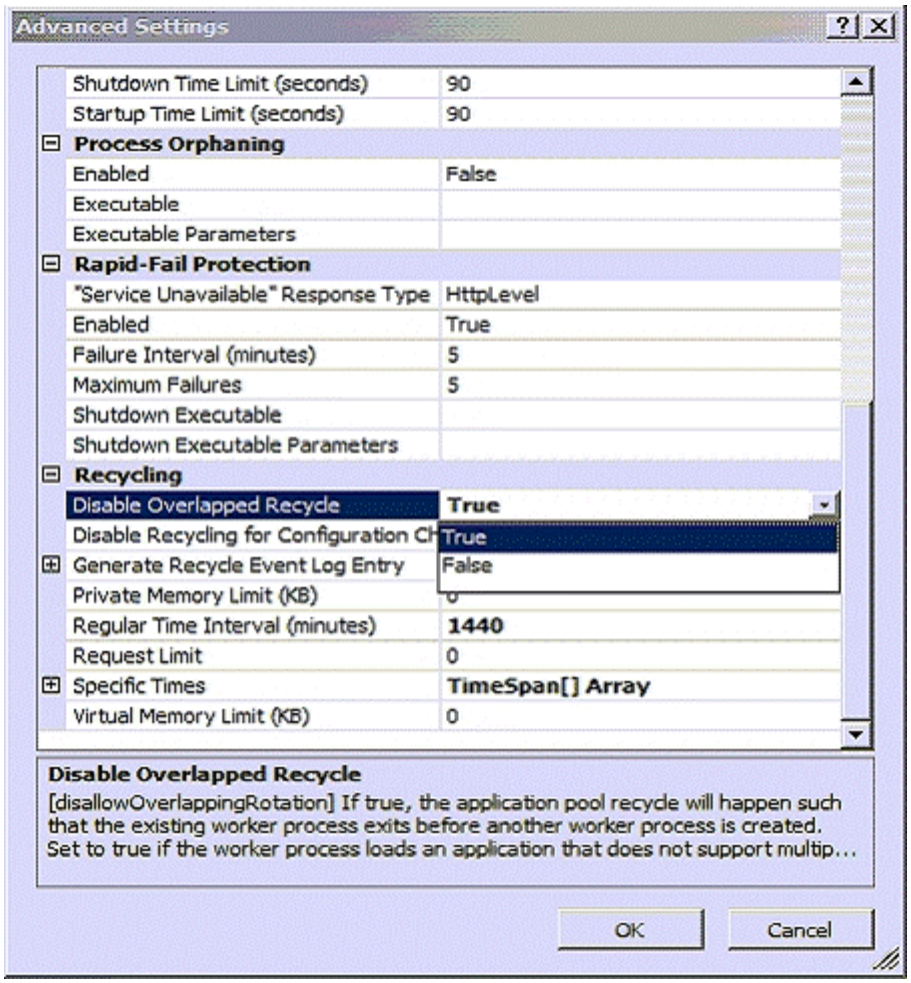
Your network contains a Windows Server 2008 R2 server that has the Web Server (IIS) server role installed. You have a Web application that uses a custom application pool. The application pool is set to recycle every 1,440 minutes. The Web application does not support multiple worker processes. You need to configure the application pool to ensure that users can access the Web application after the application pool is recycled. What should you do?

A. Set the Shutdown Executable option to True.
B. Set the Process Orphaning Enabled option to True.
C. Set the Disable Overlapped Recycle option to True.
D. Set the Disable Recycling for Configuration Changes option to True.

Answer: C

Explanation:
Overlapped Recycling
In an overlapped recycling scenario, the process targeted for a recycle continues to process all remaining requests while a replacement worker process is created simultaneously. The new process is started before the old worker process stops, and requests are then directed to the new process. This design prevents delays in service, since the old process continues to accept requests until the new process has initialized successfully, and is instructed to shut down only after the new process is ready to handle requests.
Considerations When Recycling Applications
When applications are recycled, it is possible for session state to be lost. During an overlapped recycle, the occurrence of multi-instancing is also a possibility.
Loss of session state: Many IIS applications depend on the ability to store state. IIS 6.0 can cause state to be lost if it

automatically shuts down a worker process that has timed out due to idle processing, or if it restarts a worker process during recycling. Occurrence of multi-instancing: In multi-instancing, two or more instances of a process run simultaneously. Depending on how the application pool is configured, it is possible for multiple instances of a worker process to run, each possibly loading and running the same application code. The occurrence of an overlapped recycle is an example of multi-instancing, as is a Web garden in which two or more processes serve the application pool regardless of the recycling settings. If your application cannot run in a multi-instance environment, you must configure only one worker process for an application pool (which is the default value), and disable the overlapped recycling feature if application pool recycling is being used.



Question: 19

You manage a server that runs Windows Server 2008 R2. The Remote Desktop Services server role is installed on the server. A Remote Desktop Services application runs on the server. Users report that the application stops responding. You monitor the memory usage on the server for a week. You discover that the application has a memory leak. A patch is not currently available. You create a new resource-allocation policy in Windows System Resource Manager (WSRM). You configure a Process Matching Criteria named TrackShip and select the application. You need to terminate the application when the application consumes more than half of the available memory on the server. What should you do?

A. Configure the resource-allocation policy and set the maximum working set limit option to half the available memory on the server. Set the new policy as a Profiling Policy.
B. Configure the resource-allocation policy and set the maximum working set limit option to half the available memory on the server. Set the new policy as a Managing Policy.
C. Configure the resource-allocation policy and set the maximum committed memory option to half the available

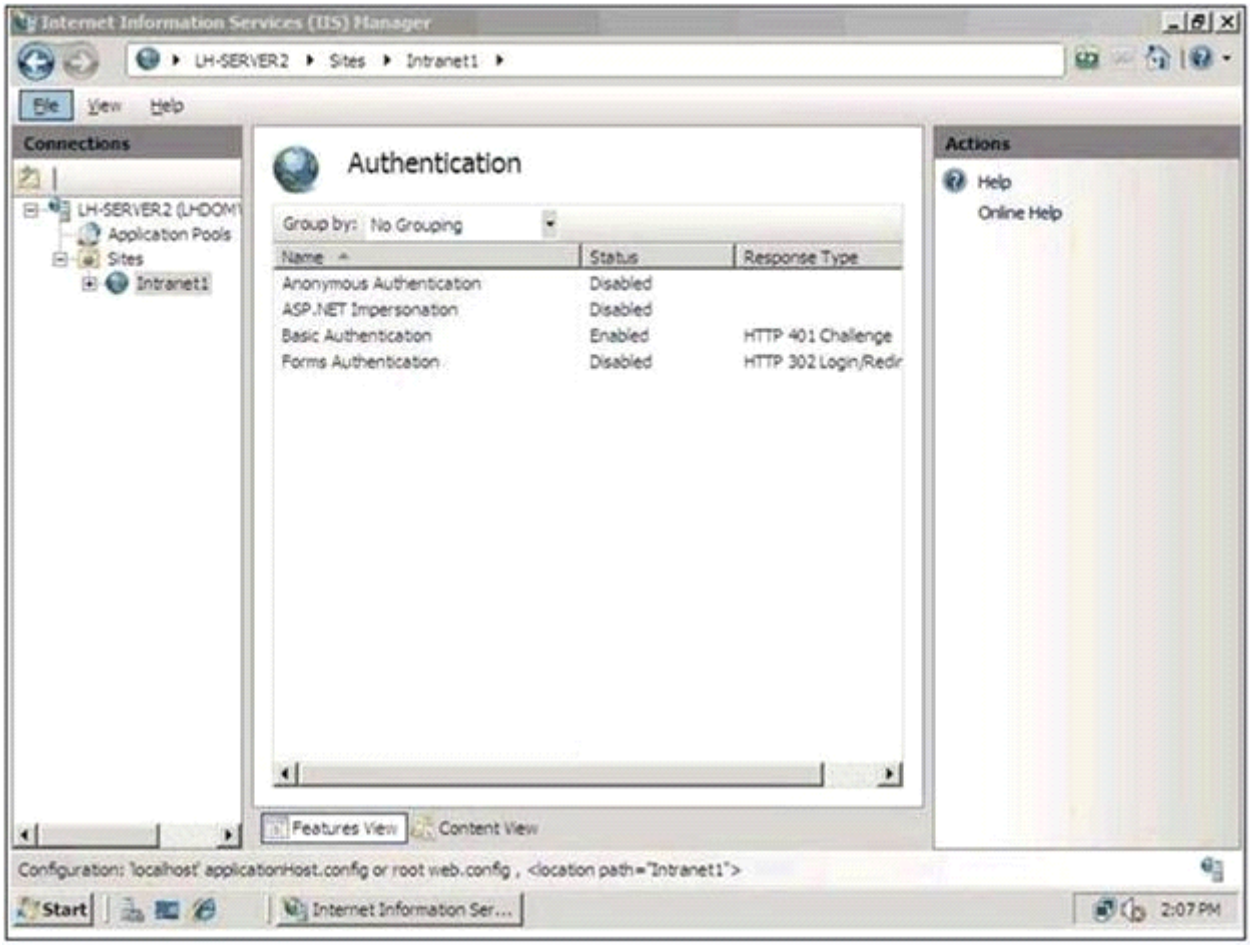
memory on the server. Set the new policy as a Profiling Policy.
D. Configure the resource-allocation policy and set the maximum committed memory option to half the available memory on the server. Set the new policy as a Managing Policy.

Answer: D

Explanation:
To create a memory resource allocation
1. In the Add or Edit Resource Allocation dialog box, on the General tab, in the Process matching criteria list, select a process matching criterion for the matched processes that will be managed by the resource allocation.
2. On the Memory tab, select one or both:
Use maximum committed memory for each process
Use maximum working set limit for each process
3. If you selected Use maximum committed memory for each process:
In the Maximum committed memory limit per process box, type a value in megabytes (MB).
In the If memory is surpassed box, select an action to take when the limit is reached.
4. If you selected Use maximum working set limit for each process, in the Maximum working set limit per process box, type a value in MB.
5. Click OK.
To add additional memory resource allocations, click Add, and then repeat steps 1–5.
Source: http://technet.microsoft.com/en-us/library/cc771472.aspx

Question: 20

You manage a member server that runs Windows Server 2008 R2. The server has the Web Server (IIS) role installed. The Web server hosts a Web site named Intranet1. Only internal Active Directory user accounts have access to the Web site. The authentication settings for Intranet1 are configured as shown in the exhibit. (Click the Exhibit button.)



You need to ensure that users authenticate to the Web site by using only the Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) encrypted Active Directory credentials. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Add the Digest Authentication role service and the URL Authorization role service to the server.
B. Add the Windows Authentication role service to IIS. Configure the Windows Authentication setting to Enabled in the Intranet1 properties.
C. Configure the Basic Authentication setting to Disabled in the Intranet1 properties.
D. Configure the Default domain field for the Basic Authentication settings on Intranet1 by adding the name of the Active Directory domain.
E. Configure the Basic Authentication setting to Disabled and the Anonymous Authentication setting to Enabled in the Intranet1 properties.

Answer: B, C

Explanation:
To ensure that the users accessing the website are authenticated through MS-CHAPv2 encrypted Active Directory credentials, you should Add Windows Authentication role service to the IIS server. Enable the Windows Authentication settings in the intranet-e properties and disable the basic authentication setting in the intranet-e properties. Basic authentication is a set of basic rules that authenticate users. To implement MS-CHAPv2, you have to disable the basic authentication and then, add windows authentication role services to the IIS server. After adding it, you should enable it. The Windows Authentication role service will allow the website to be authenticated through MS-CHAPv2.

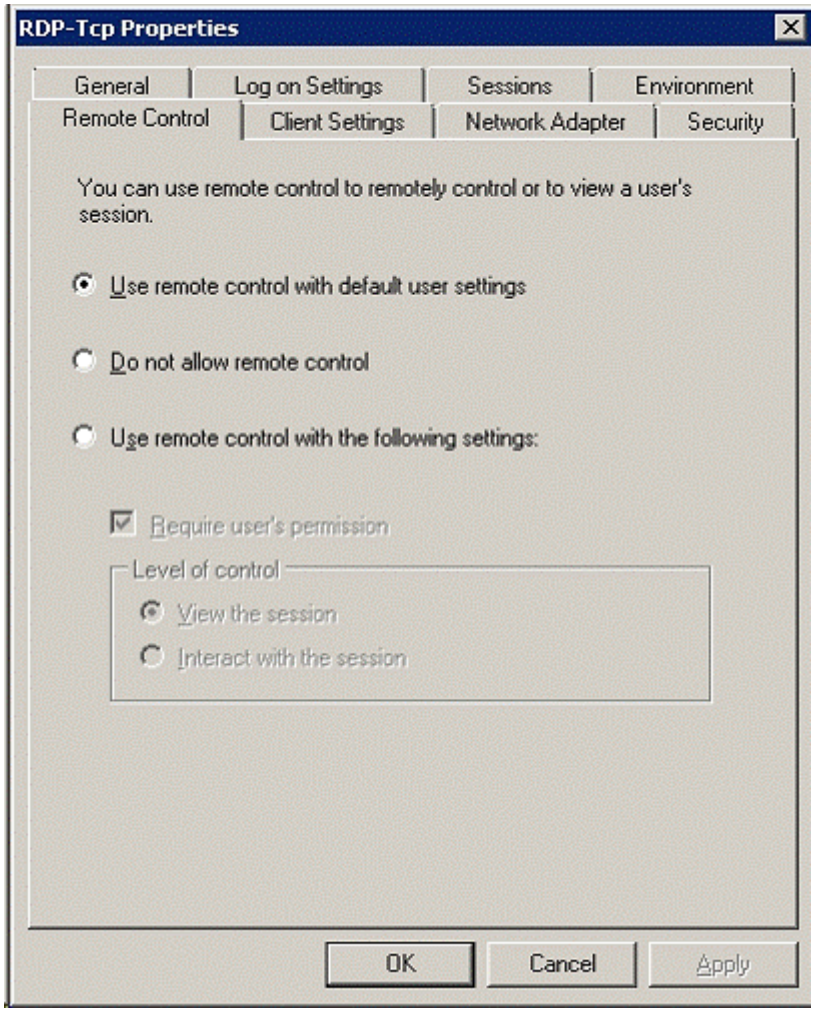
Question: 21

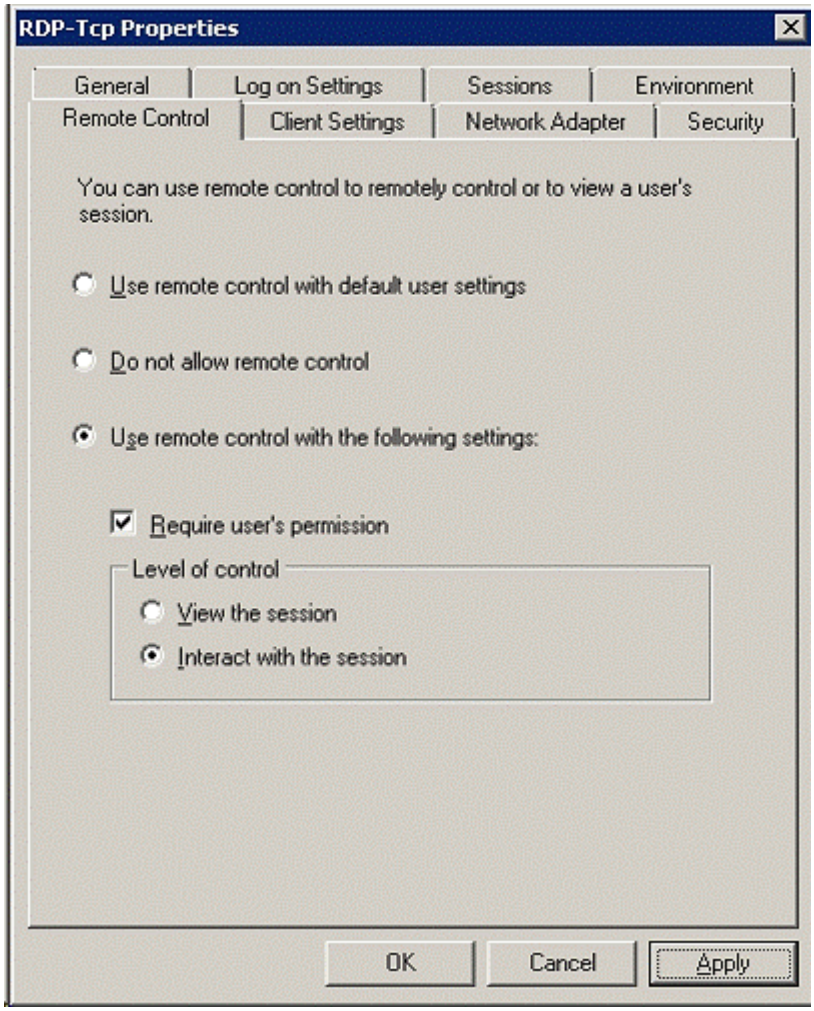
Your company has an Active Directory domain. The company runs Remote Desktop Services. A user has remotely logged on to the Remote Desktop Session Host Server. The user requires help to use an application. When you connect to the Remote Desktop session, you cannot operate any applications. You need to ensure that you can assist any user on the Remote Desktop Session Host Server. What should you do?

A. From the Remote Desktop Session Host Server run the Tscon /v command. Then reconnect to the session.
B. Run the Chgusr /execute command on the Remote Desktop Session Host Server. Then reconnect to the session.
C. Enable Use remote control with default user settings in the RDP-Tcp Properties.
D. Enable Use remote control with the following settings in the RDP-Tcp Properties. Configure the Level of control policy setting to Interact with the session. Instruct the user to log off and log back on.

Answer: D

Explanation:
In Remote Desktop Session Host Configuration rightclick RDP-Tcp and choose properties.





Question: 22

Your company runs Windows Server 2008. The company network is configured as an Active Directory domain named contoso.com. The network has a Web server named WEB1. The domain users access WEB1 by using http://web1. You generate a self-signed certificate for WEB1 and configure WEB1 to use SSL. Users report that they get a warning message when they connect to WEB1 by using https://web1. You need to ensure that users can connect to WEB1 without receiving a warning message. What should you do?

A. Add the https: //web1 name to the list of Trusted Sites zone on all the computers in the domain.
B. Open the Certificates console on WEB1. Export the self-signed certificate to a web1.cer file. Install the web1.cer file on all the computers in the domain.
C. Join WEB1 to the contoso.com domain. Reissue the self-signed certificate. Request all the users to use https://web1.contoso.com to connect to WEB1.
D. Create a DNS Host (A) Record for WEB1 in the contoso.com zone. Reissue the self-signed certificate. Request all the users to use https: //webl.contoso.com to connect to WEB1.

Answer: B

Explanation:
To ensure that the users can connect to TK2.com without getting warning messages, you should export the self-signed certificate to a TK2.cer file. Then, you install the tk2.cer file on all computers accessing the website. The users account will be authenticated through the certificate and they will not get any warning messages. The .cer file is an internet

security certificate extension which confirms the authenticity of a website installed on a server.

Question: 23

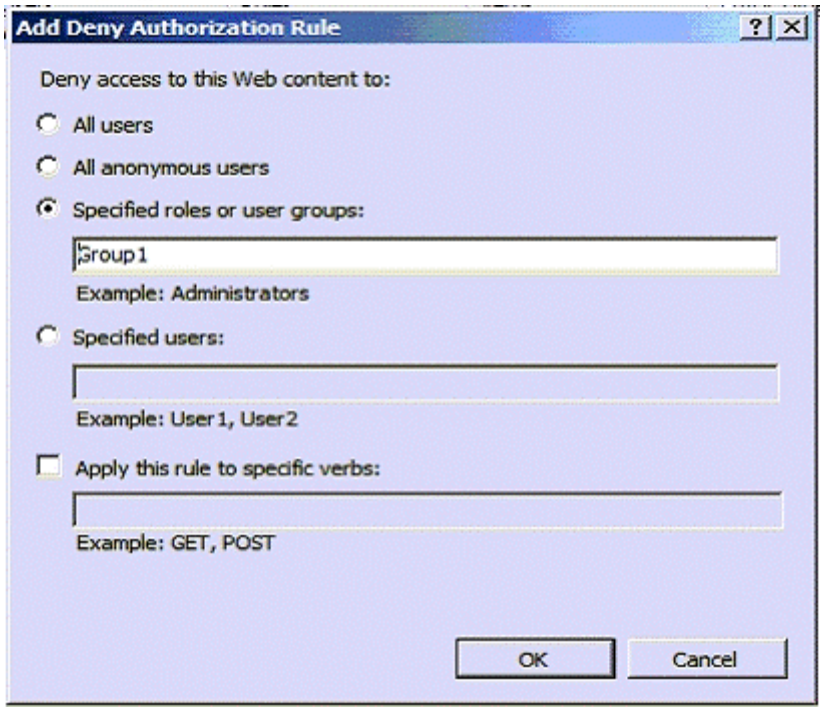
You have a server that runs Windows Server 2008 R2. The server has the Web Server (IIS) server role installed. The server contains a Web site that is configured to use only Windows Authentication. You have a security group named Group1 that contains several user accounts. You need to prevent the members of Group1 from accessing a Web site. You must not prevent other users from accessing the Web site. Which Web site feature should you configure?

A. Authentication
B. Authorization Rules
C. IIS Manager Permissions
D. SSL Settings

Answer: B

Explanation:
Add or Edit Allow Authorization Rule and Add or Edit Deny Authorization Rule Dialog Boxes Use the Add Allow Authorization Rule,the Edit Allow Authorization Rule, the Add Deny Authorization Rule, or the Edit Deny Authorization Rule dialog box to define rules for access to content.

Element Name	Description
All users	Select this option to manage access to content for both anonymous and authenticated users. By default, there is an allow rule configured for **All users**.
All anonymous users	Select this option to manage access to content for users that are not authenticated.
Specified roles or user groups	Select this option to manage access to content for specific Microsoft Windows roles or user groups.
Specified users	Select this option to manage access to content for a specific user account.
Apply this rule to specific verbs	Specifies that the rule applies to specific HTTP verbs such as GET or POST.



Question: 24

You install the Web Server (IIS) server role on a new server that runs Windows Server 2008 R2. You install a Microsoft

.NET Framework 1.0 application on a Web site on the Web server. The company security policy states that all applications must run by using the minimum level of permission. You need to configure the Web site application so that it has the permissions to execute without creating any other content and without accessing any operating system components. What should you do?

A. Set the .NET Framework trust level to Full for the Web site.
B. Set the .NET Framework trust level to Low for the Web site.
C. Set the .NET Framework trust level to High for the Web site.
D. Set the .NET Framework trust level to Medium for the Web site.

Answer: A

Explanation:
To configure the website application to have permission to execute without creating other content or accessing Windows Server 2008 system components, you should configure the .NET Framework website trust level to full.
In the .NET Framework, code access security controls access to resources by controlling how code runs. When a user runs an application, the common language runtime assigns the application to any one of the following five zones:
My Computer - The application code is hosted directly on the user's computer.
Local Intranet - The application code runs from a file share on the user's intranet.
Internet - The application code runs from the Internet.
Trusted Sites - The application code runs from a Web site that is defined as "Trusted" in Internet Explorer.
Untrusted Sites - The application code runs from a Web site that is defined as "Restricted" in Internet Explorer.
You can set the security level for each zone to High, Medium, Medium-low, or Low.
Reference: http://support.microsoft.com/kb/832742

Question: 25

Your company named Contoso, Ltd. runs Windows Server 2008 R2. You manage a Web server named Server1. Internet users access Server1 by using http://www.contoso.com and https://www.contoso.com. The Server1 server uses an SSL certificate from a public certification authority (CA). You install an additional Web server named Server2. You configure a Network Load Balancing cluster to distribute the incoming HTTP and HTTPS traffic between both Web servers. You need to configure an SSL certificate on Server2 to support HTTPS connections. You must ensure that all users can connect to https://www.contoso.com without receiving security warnings. What should you do?

A. Open the IIS Manager console on Server2. Create a self-signed certificate.
B. Open the IIS Manager console on Server1. Export the SSL certificate to a .pfx file. Import the .pfx file to Server2.
C. Open the Certificates console on Server1. Export the SSL certificate to a .cer file. Import the .cer file to Server2.
D. Request a new SSL certificate from the public CA. Use Server2 as the Common Name in the request. Install the new certificate on Server2.

Answer: B

Explanation:
To configure an SSL certificate on Server2 also to support HTTPS connections so that all users can connect to https://www.contoso.com without receiving security warnings, you need to configure the same certificate on that exists on Server1 to Server2 also. To do this you need to export the SSL certificate to a .pfx file and import the .pfx file to Server2. The certificate can be exported to pfx file therefore you need to export it to .pfx file and not .cer file.
Reference: Exporting Existing SSL OWA Certificates from Exchange 2003 FES to Exchange 2007 SP1 CAS on Windows2008
http://telnetport25.wordpress.com/2008/03/28/exporting-existing-ssl-owa-certificates-from-exchange-2003-fes-to-

exchange-2007-sp1-cas-on-windows-2008/

Question: 26

You have two servers that run Windows Server 2008 R2 named Server1 and Server2. Both servers have the Windows Media Services server role installed. Server2 is a License Clearing House. You publish an audio file on Server1. The audio file is licensed by Server2. You need to ensure that users are allowed to use the audio file for only two days. What should you do?

A. On Server1, modify the key ID.
B. On Server1, modify the license key seed.
C. On Server2, modify the license.
D. On Server2, create a new package.

Answer: C

Explanation:
Windows Media Rights Manager is a digital rights management (DRM) platform that can be used by content providers and retailers to distribute digital media files securely over a network, such as the Internet. The Windows Media Rights Manager SDK helps protect digital media content (such as songs and videos) by packaging Windows Media files in an encrypted file format. A packaged file contains a version of a "protected" file that was encrypted and locked with a "key" after business usage and distribution rules were added to the content header. This packaged file is also bundled with additional information from the content provider and, optionally, from the distributor. The result is a protected Windows Media file that can only be played by a user who has obtained a license. The basic Windows Media Rights Manager process is as follows:
Playing the file. To play the file, the user needs a player that supports Windows Media Rights Manager. Support for Windows Media Rights Manager was first added to Windows Media Player for Windows XP. Players that were created using the Windows Media Player ActiveX control version 8 or later also support this DRM platform. With the appropriate version of the Player installed, the customer can then play the file according to the rules or rights that are included in the license. Licenses can have different rights, such as start times and dates, duration, and counted operations. For instance, default rights may allow the user to play the file on a specific computer and copy the file to a portable device. Licenses, however, are not transferable. If a customer sends a protected file to a friend, this friend must acquire a different license to play the file. This per-computer licensing scheme ensures that the protected file can only be played by the computer that has been granted the license key for that file.
Source: http://technet.microsoft.com/en-us/library/cc732309.aspx

Question: 27

You have two servers that run Windows Server 2008 named Server1 and Server2. Both servers have the Windows Server visualization role service installed. You need to remotely manage the visualization settings of Server2 from Server1. What should you do?

A. From the command prompt, run vmconnect.exe server2.
B. From the command prompt, run vmconnect.exe server1 server2.
C. Open the Visualization Management Console. From the left-hand pane, right-click Server1, point to New and then click Virtual machine.
D. Open the Virtualization Management Console. From the left-hand pane, right-click Virtualization Services and then click Connect to Server.

Answer: D

Explanation:
To remotely manage the virtualization settings of Server2 from Server1, you need to right-click Virtualization Services from the Virtualization Management Console and then click Connect to Server. You can manage multiple Hyper-V server instances in the management console's left pane. Selecting a server instance displays that server's VMs in the center Virtual Machines pane. You can manage the VMs by right-clicking them and selecting the desired commands on the context menu. The Connect command allows you to connect to a running VM, which starts the Virtual Machine Connection window. Reference: A First Look at Windows Server 2008 Hyper-V
http://windowsitpro.com/Windows/Articles/ArticleID/97857/pg/2/2.html

Question: 28

You have a server that runs Windows Server 2008. The server has the Web Server (IIS) server role installed and all the Web Server role services installed. You need to provide a user the ability to administer a Web site. Which feature should you configure?

A. .Net Roles
B. .Net Users
C. Authentication
D. IIS Manager Permissions

Answer: D

Explanation:
To provide a user the ability to administer a website, you need to configure IIS Manager Permissions feature on the server. The IIS Manager Permissions feature is used to allow users to connect to sites and applications in IIS Manager. Permitted users can configure delegated features in any sites or applications for which they have permission. Users can be either IIS Manager users, which are credentials created in IIS Manager by using the IIS Manager Users feature, or Windows users and groups on the local computer or on the domain to which the computer belongs.
Reference: IIS 7.0: Configuring Permissions for IIS Manager Users and Windows Users
http://technet2.microsoft.com/windowsserver2008/en/library/33aaec94-c0cb-4402-b91e-a5e3b9c3e0e01033.mspx?mfr=true

Question: 29

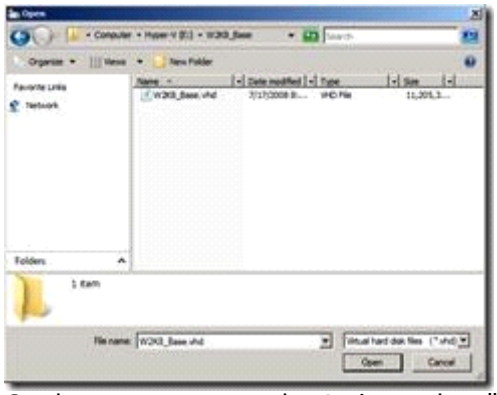
You have a server that runs Windows Server 2008 R2. The server has the Hyper-V server role installed. You need to merge a differencing disk and a parent disk. What should you do?

A. Edit the parent disk.
B. Inspect the parent disk.
C. Edit the differencing disk.
D. Inspect the differencing disk.

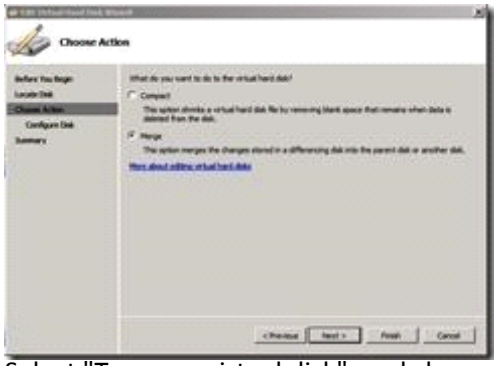
Answer: C

Explanation:Merging Differencing Disks with Hyper-V
A differencing disk is a disk that is a child of a parent disk. Differencing disks are very helpful in keeping disk images small, manageable and consistent, because you can create a base parent disk- such as a Windows 2008 Standard base image- and use it as the foundation for all other guest virtual machines and disks that will be based on Windows Server 2008. For example, I have a Windows Server 2008 guest that I use exclusively as sandbox for development. I

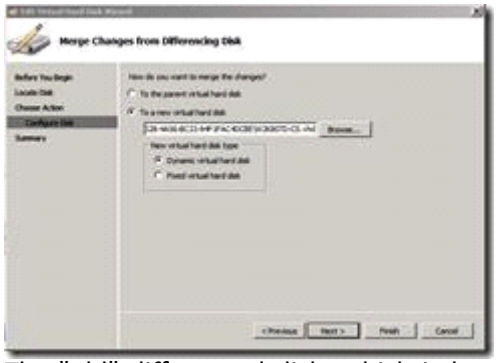
am in the process of building out another guest based on Windows Server 2008 that will be for some TFS 2008 demos that I am working on for an upcoming series of talks. Rather than copy the Windows Server 2008 guest VPC over and over again, I can simply create one differencing disk for my development environment role and one for my TFS role. The result is a VHD that represents the intersection of the base/parent disk (in this case, a barebones install of Windows Server 2008 Standard) and any additional software I've installed or configuration changes I have made. This not only conserves disk space, but also saves me a lot of time in copying hefty giga-some-odd vhds around. Sometimes it is necessary to merge a differencing disk back to it's parent or into a new disk. For example, you may be moving VHDs around as I did recently to a new, high speed E-SATA drive. My old drive hosted a vhd that I used as my development sandbox that used a parent on the old disk. I certainly don't want to depend on my clunky old USB 2.0 drive for the parent (the IO cost alone would be just silly), and at a minimum, there is state on the differenced guest OS that I do not want to lose. The first thing to do is copy over the parent VHD, create a new differencing disk based on the same parent, but in the new location. Next, since the differenced guest VHD has state that you want to move over (lest you lose it), it is necessary to merge the state of the "old" differenced guest VHD with the new copy. To do so, under Server Manager, in the Hyper-V Manager, click "Edit Disk", and locate the disk that you want to merge into a new differenced disk:



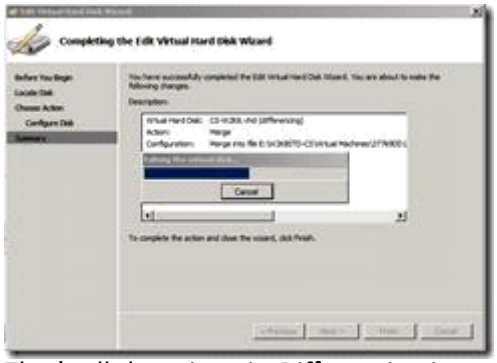
On the next screen, under Action, select "Merge":



Select "To a new virtual disk", and choose a name and path for the new disk that you created in the initial copy:



The "old" differenced disk, which is based on the original parent disk plus state from the "old" differenced disk is merged into the new disk on the drive you specified:



That's all there is to it. Differencing is a powerful feature in virtualization, and there is very nice support for migration of differenced disks right within the Server Manager.
Source: http://rickgaribay.net/archive/2008/08/15/merging-differencing-disks-with-hyper-v.aspx

Question: 30

You have a server that runs Windows Server 2008. The server has the Windows Server virtualization role service installed. You create a new virtual machine and perform an installation of Windows Server 2008 on the virtual machine. You configure the virtual machine to use the physical network card of the host server. You notice that you are unable to access network resources from the virtual machine. You need to ensure that the virtual host can connect to the physical network. What should you do?

A. On the host server, install the MS Loopback adapter.
B. On the host server, enable the Multipath I/O feature.
C. On the virtual machine, install the MS Loopback adapter.
D. On the virtual machine, install Windows Server virtualization Guest Integration Components.

Answer: D

Explanation:
To ensure that the virtual host can connect to the physical network, you need to install Windows Server virtualization Guest Integration Components on the virtual machine. The network adapter in the VM ported from Virtual Server to Windows Server is no longer recognized. Workaround is to add a legacy network adapter to the VM. In WSv, the network adapter seen by the guest OS is not an emulated device (DEC/Intel 21140 Ethernet adapter. It is an entirely new, high performance, purely synthetic device available as part of the Windows Server virtualization Integration Components call Microsoft VMBus Network Adapter
Reference: Archive for the 'Virtual Server/PC/WSv/Hyper-V' Category / Windows Server 2008 Common FAQ (condensed)
http://www.leedesmond.com/weblog/index.php?cat=6HYPERLINK
"http://www.leedesmond.com/weblog/index.php?cat=6&paged=3#_blank"&HYPERLINK
"http://www.leedesmond.com/weblog/index.php?cat=6&paged=3#_blank"paged=3

Question: 31

You manage a server named SSP1 that runs Windows Server 2008. SSP1 has the Windows SharePoint Services (WSS) role in standalone mode. You manage another Windows Server 2008 server named SSP2. You install the WSS role on SSP2. During the installation, you indicate that SSP2 must be a member of a WSS server farm. You are unable to connect to SSP1 in the server farm. You need to configure SSP1 and SSP2 in a WSS server farm. What should you do?

A. Restart the Web Management service on SSP1.
B. Set the Microsoft .NET Framework Trust Level to Low on both SSP1 and SSP2.

C. Set the Microsoft .NET Framework Trust Level to Medium on both SSP1 and SSP2.
D. Uninstall and reinstall WSS on SSP1 and select the server farm mode during the installation.

Answer: D

Explanation:
To configure both ERA1 and ERA2 in the WSS server farm, you should uninstall the WSS on ERA1 and select the server farm mode while reinstalling it. The server farm mode will enable you to configure both the servers in the WSS server farm. Microsoft Windows SharePoint Services was designed to be useful in large server farms, supporting hundreds or thousands of SharePoint sites and millions of users. When you manage a server farm environment for Windows SharePoint Services, you need to make certain choices about configuring your environment, and you need to be aware of how Windows SharePoint Services works in that environment. This topic explains those choices, and describes how to work with Windows SharePoint Services in a large-scale, server farm environment.
Reference:
http://www.microsoft.com/resources/documentation/wss/2/all/adminguide/en-us/stsf15.mspx?mfr=true

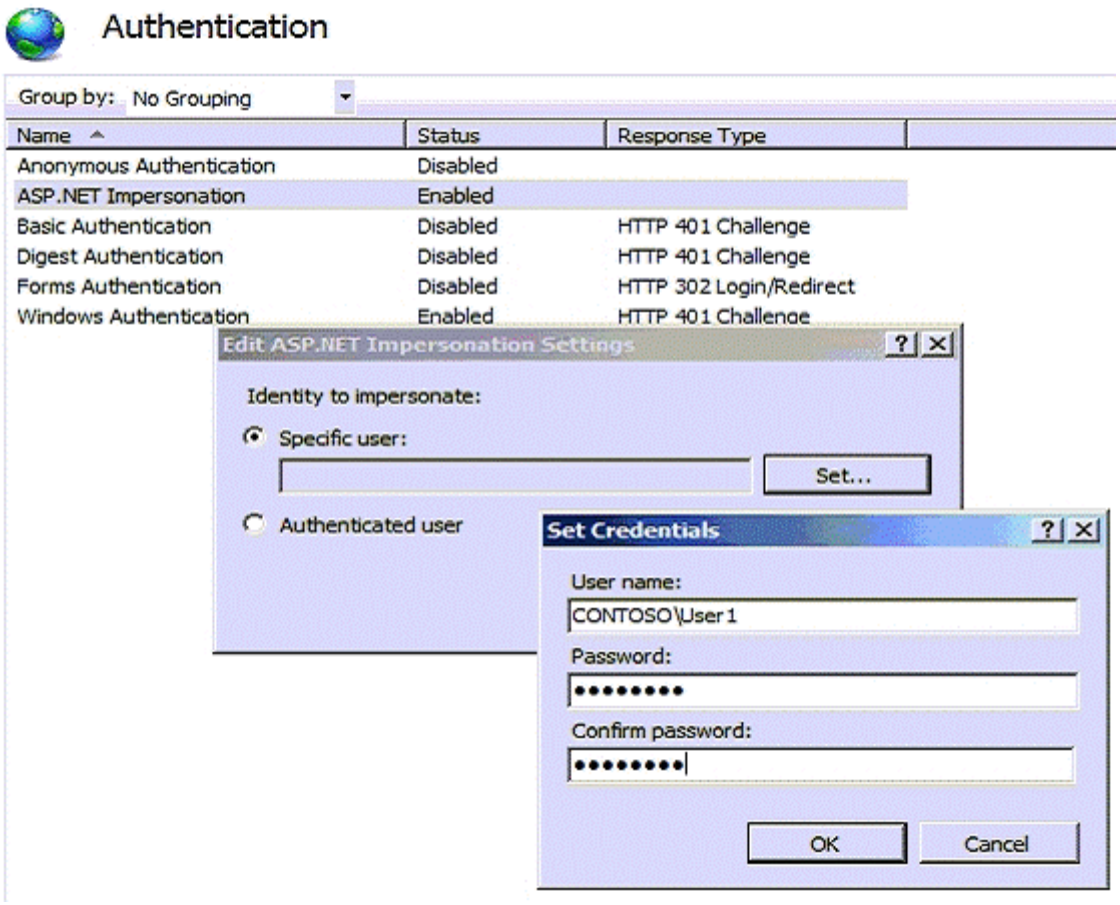
Question: 32

You manage a server that runs Windows Server 2008 R2. The server has the Web Server (IIS) role installed. The Web developer at your company creates a new Web site that runs an ASP.NET 3.0 Web application. The ASP.NET Web application must run under a security context that is separate from any other ASP.NET application on the Web server. You create a local user account and grant account rights and permissions to run the ASP.NET Web application. You need to configure authentication for the new Web site to support the Web application. What should you do?

A. Configure the Windows Authentication setting to Enabled.
B. Configure the Forms Authentication setting to Enabled by using all the default settings.
C. Configure the ASP.NET State service to log on to the new local user account by using the Services console.
D. Configure the ASP.NET Impersonation setting to Enabled. Edit the ASP.NET Impersonation setting by specifying the new local user account.

Answer: D

Explanation:



Question: 33

You have a server that runs Windows Server 2008. The Web Server (IIS) role is installed. You plan to host multiple Web sites on the server. You configure a single IP address for the server. All Web sites are registered in DNS to point to the single IP address. You need to ensure that each Web site only responds to requests by name from all client computers. What should you do?

A. Configue a unique port for each Web site.
B. Configue a unique IP address for each Web site.
C. Configue a unique Host Header for each Web site.
D. Edit the Hosts file on the server to add all the Web site names associated to the network address.

Answer: C

Explanation:
To ensure that each and every website responds only to the name requests from all client machines, you should configure and assign a unique Host Header to each website. A host header is a third piece of information that you can use in addition to the IP address and port number to uniquely identify a Web domain or, as Microsoft calls it, an application server. For example, the host header name for the URL http://www.fabrikam.com is www.fabrikam.com.
Reference: http://www.visualwin.com/host-header/

Question: 34

Your company has an Active Directory domain. The company runs Terminal Services. All client computers run

Windows Vista Service Pack 1. You need to ensure that users are able to run Windows Media Player 11 during a Terminal Services session. What should you do?

A. Install the Desktop Experience feature on the Terminal Server.
B. Install the Quality Windows Audio Video Experience feature on the Terminal Server.
C. Create a new Group Policy object (GPO) by using the Desktop Window Manager template. Configure the Do not allow desktop composition option to True. Apply the GPO to all client computers in the domain.
D. Create a new Group Policy object (GPO) that configures the Policy-based QoS option and set the Differential Services Code Point value to 10 for the Windows Media Player 11 executable. Apply the GPO to the Terminal Server.

Answer: A

Explanation:
When Desktop Experience is installed on Windows Server 2008, the user can use Windows Vista features, such as Windows Media Player, desktop themes, and photo management within their remote connection. Therefore to ensure that the users could run Windows Media Player 11 during the Terminal services session, you need to Install and configure the Desktop Experience feature on the terminal server Reference: Windows Server 2008 Technical Overview / Terminal Services
http://www.microsoft.com/technet/windowsserver/longhorn/evaluate/whitepaper.mspx?wt.svl=globalheadline

Question: 35

Your company has an Active Directory domain. All servers in the domain run Windows Server 2008 R2. The RD Gateway role service is installed on a server named Server1. The Remote Desktop Services server role is installed on two servers named Server2 and Server3. Server2 and Server3 are configured in a load balancing Remote Desktop Services farm named Farm1. You deploy the RD Connection Broker service on a new server named Server4. You confirm that the RD Connection Broker works correctly. You deploy a hardware load balancing device to handle the load distribution to the Remote Desktop Services farm. The device has specialized support for remote desktop services and routing tokens. You discover that the RD Connection Broker no longer works correctly. You need to ensure that the RD Connection Broker works correctly. Which Group Policy object (GPO) should you create and apply to the Remote Desktop Server farm?

A. A GPO that enables the Use IP Address Redirection policy setting in the RD Connection Broker section of the Remote Desktop Services Group Policy template.
B. A GPO that disables the Use IP Address Redirection policy setting in the RD Connection Broker section of the Remote Desktop Services Group Policy template.
C. A GPO that enables the Use RD Connection Broker load balancing policy setting in the RD Connection Broker section of the Remote Desktop Services Group Policy template.
D. A GPO that disables the Use RD Connection Broker Load Balancing policy setting in the RD Connection Broker section of the Remote Desktop Services Group Policy template.

Answer: A

Explanation:
To ensure that the RD Connection Broker works correctly in the above given scenario, you need to create a GPO that disables the Use IP Address Redirection policy setting in the RD Connection Broker section of the Remote Desktop Server Group Policy template. The RD Connection Broker service is failing because you have recently deployed a hardware load balancing device that has specialized support for RD servers and routing tokens to the RD Server farm. When routing tokens are used the IP address of the RD server is not sent to the client. Instead, the IP address is embedded in a token. This can happen when you disable Use IP Address Redirection policy setting. When a client

reconnects to the load balancer, the routing token is used to redirect the client to their existing session on the correct terminal server in the farm.
Reference: RD Connection Broker.
http://technet2.microsoft.com/windowsserver2008/en/library/8a46c71e-cc7d-4bf0-82cc-8261f7c3069c1033.mspx?mfr=true

Question: 36

You install the Web Server (IIS) server role on a server that runs Windows Server 2008 R2. You configure a Web site named contoso.com and a Web application named Acctg on the Web server. The Web server runs out of disk space. You move Acctg to another drive on the Web server. The following table shows the current application configuration:

Application	Web location	Original location	New location
Acctg	contoso/Acctg	D:\Acctg	F:\Acctg

Users report that they cannot access Acctg.
You need to enable users to access Acctg.
Which command should you run on the server?

A. appcmd add app /site.name: contoso /path:/Acctg /physicalPath:d:\Acctg
B. appcmd add app /site.name: contoso /path:/Acctg /physicalPath:f:\Acctg
C. appcmd set app /site.name: contoso /path:/Acctg /physicalPath:d:V\cctg
D. appcmd set app /site.name: contoso /path:/Acctg /physicalPath:f:\Acctg

Answer: D

Explanation: Explanation:
* The mentioned answer does not work in reallife, atleast not on Windows2008R2 RTM.* But it is the awnser that looks syntax wise the most as the following:
appcmd set app /app.name: contoso/Acctg /[path='/Acctg'].physicalPath:F:\Acctg
Command Line To change the path of an application's content, use the following syntax: appcmd set app /app.name: string /[path='/'].physicalPath: string The variable app.name string is the virtual path of the application, and physicalPath string is the physical path of the application's content. For example, to change the physical path of the location D:\Acctg for an application named Acctg in a site named contoso, type the following at the command prompt, and then press ENTER:
appcmd set app /app.name: contoso/Acctg /[path='/Acctg'].physicalPath:F:\Acctg
Source: http://technet.microsoft.com/nl-nl/library/cc725781(WS.10).aspx

Question: 37

You have a Terminal Server that runs Windows Server 2008. You need to configure the server to end any sessions that are inactive for more than one hour. What should you do?

A. From Terminal Services Manager, create a new group.
B. From Terminal Services Manager, delete the inactive sessions.
C. From Terminal Services Configuration, modify the RDP-Tcp settings.
D. From Terminal Services Configuration, modify the User logon mode setting.

Answer: C

Explanation:

To configure the Terminal Server to end any sessions that are inactive for more than one hour, you need to modify the RDP-Tcp settings from Terminal Services Configuration. You can configure the properties of the terminal server's RDP-TCP connection to provide better protection. You can set session time limits that help to ensure that sessions are not left unattended and active for long periods Reference: How Secure are Windows Terminal Services? / Securing the RDP-TCP Connection
http://www.windowsecurity.com/articles/Windows_Terminal_Services.html

Question: 38

You have a server that runs Windows Server 2008. The server has the Windows Media Services server role installed. You plan to distribute a video file on DVD media. Users will view the video while working on computers that are not connected to the Internet. You need to distribute the video to users. You also need to protect the video from unauthorized use and illegal distribution. What should you do?

A. From Windows Media Services, publish the video as streaming content, and then burn the video to a DVD.
B. From Windows Media Services, advertise the video. Create a DVD that contains the HTML and ASPX files for the advertised video.
C. From Windows Media Digital Rights Manager, package the video and then advertise the video on the corporate Web site.
D. From Windows Media Digital Rights Manager, create a package and a license for the video file. Burn the packaged video to a DVD.

Answer: D

Explanation:
To distribute a video file on DVD media while making sure that the video file is protected from unauthorized use and illegal distribution, you need to create a package and a license for the video file and then burn the packaged video to a DVD using Windows Media Digital Rights Manager
Windows Media Rights Manager is the technology that allows you to package Windows Media DRM files and issues licenses. You can use Windows Media Rights Manager to encrypt a given digital media file, lock it with a key, and bundle additional information from the content provider. This results in a packaged file that can only be played by the person who has obtained a license. Windows Media Rights Manager can also act as the license clearing house, authenticating the consumer's request for a license and issuing the license to the user.
Reference: Windows Media DRM FAQ
http://www.microsoft.com/windows/windowsmedia/forpros/drm/faq.aspx#drmfaq_1_1

Question: 39

Your company has an Active Directory domain. A server named Server1 runs Windows Server 2008 R2. The Remote Desktop Services server role and the RD Web Access role service are installed on Server1. You install the RD Gateway role service on Server1. You create the Remote Desktop connection authorization policy. Users report that they cannot connect to Server1. You need to ensure that users can connect to Server1. What should you do?

A. Configure Network Access Protection (NAP) on Server1.
B. Configure the Remote Desktop Resource Authorization Policy (RD RAP) on Server1.
C. Create a Remote Desktop Group Policy object (GPO). Enable the Allow log on through Remote Desktop Services setting on the GPO. Link the GPO to the domain.
D. Create a Remote Desktop Group Policy object (GPO). Enable the Set path for Remote Desktop Services Roaming User Profile setting on the GPO. Create an organization unit (OU) named RDSUsers. Link the GPO to the RDSUsers OU.

Answer: B

Explanation:
Remote Desktop resource authorization policies (RD RAPs) allow you to specify the internal network resources (computers) that remote users can connect to through an RD Gateway server. Remote users connecting to the network through an RD Gateway server are granted access to computers on the internal network if they meet the conditions specified in at least one RD CAP and one RD RAP.
Source: http://technet.microsoft.com/en-us/library/cc772397.aspx

Question: 40

Your company runs Terminal Services on a server named Server2. You need to prevent new sessions on the Terminal Server without affecting current user sessions. Which command should you run?

A. Change logon /disable
B. Change user /execute disable
C. Tskill /server:Server2 /A
D. Taskkill /S Server2 /fi "MODULES eq TermSrv"

Answer: A

Explanation:
To prevent new sessions on the Terminal Server without affecting current user sessions, you need to run Change logon /disable command. This command disables subsequent logons from client sessions, but not from the console. This also ensures that the currently logged on users do not get affected. Reference: Change logon
http://technet2.microsoft.com/windowsserver/en/library/85af3fd0-b518-4b91-9f93-24c75173494e1033.mspx?mfr=true

Question: 41

You have two servers that run Windows Server 2008 named Server1 and Server2. You install Windows SharePoint Services (WSS) 3.0 on Server1. You install the SMTP feature on Server2. You configure the outgoing email settings on Server1 to use the SMTP service on Server2. You need to ensure that email messages from Server1 are forwarded to users. What should you do?

A. On Server2, create a new application pool, and then associate the application pool with a new Web site.
B. On Server2, configure the SMTP service to accept anonymous connections and to relay email messages.
C. On Server1, create a new application pool. On an internal DNS server, create a new MX record for Server1.
D. On Server1, create a new application pool. On an internal DNS server, create a new MX record for Server2.

Answer: B

Explanation:
You can configure the SMTP service to accept relayed email from servers in your farm. You can decide to accept relayed email from all servers except those you specifically exclude. Alternatively, you can block email from all servers except those you specifically include. You can include servers individually, or in groups by subnet or domain. You can enable both anonymous access and email relaying but by doing this, you increase the possibility that the SMTP server will be used to relay unsolicited commercial email (spam). Reference: Configure outgoing email settings (Windows SharePoint Services)
http://technet.microsoft.com/en-us/library/cc288949(TechNet.10).aspx

Question: 42

Your company has an Active Directory domain. You have a server that runs Windows Server 2008. The Terminal Services role is installed on the server. The company security policy does not allow users to copy and paste information to a local computer during a Terminal Services session. You deploy the remote application named APP1. You need to configure Terminal Services to meet the security requirement. What should you do?

A. Enable the Use temporary folders per session option.
B. Change the Security Encryption Level to FIPS Compliant.
C. Deselect the Clipboard option in the RDP Settings for the published application.
D. Disable the Drive option in the RDP-Tcp Client Setting properties for the server.

Answer: C

Explanation:
To ensure that the users are not allowed to copy and paste information to a local computer during a Terminal Services session, you need to deselect the Clipboard option in the RDP Settings for the published application When connecting to a terminal server using an RDP client, many of the local resources are available within the remote session, including the client file system, smart cards, audio (output), serial ports, printers (including network), and the clipboard. These redirection facilities allow users to easily take advantage of the capabilities of their client device from within the remote session. Similarly clipboard can be used to copy and paste information to local computer. To stop the copy paste, you need to go to Terminal Services Configuration and on the Client Settings tab, under Disable the following Clipboard mapping to disable client clipboard mapping. Reference: Configure settings for mapping client devices/ Using Terminal Services Configuration
http://technet2.microsoft.com/windowsserver/en/library/17d44d9a-cf4b-4a6a-94ec-093cb5f8b2b71033.mspx?mfr=true
Reference: Frequently Asked Windows Terminal Services Questions! / New Features and Improvements
http://www.msterminalservices.org/faq/WindowsTerminalServices/?page=5

Question: 43

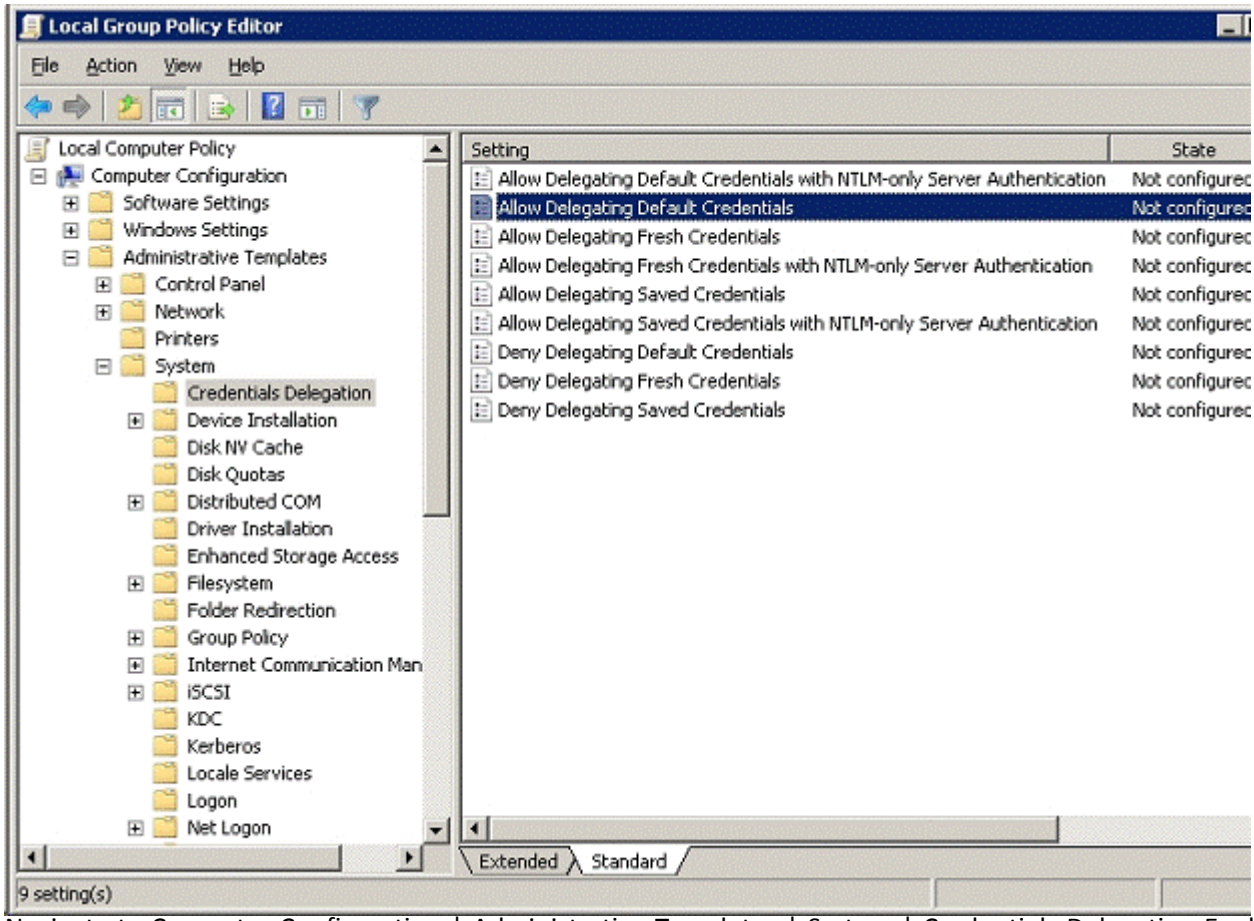
Your network consists of a single Active Directory domain. The network contains a Remote Desktop Session Host Server that runs Windows Server 2008 R2, and client computers that run Windows 7. All computers are members of the domain. You deploy an application by using the RemoteApp Manager. The Remote Desktop Session Host Server's security layer is set to Negotiate. You need to ensure that domain users are not prompted for credentials when they access the application. What should you do?

A. On the server, modify the Password Policy settings in the local Group Policy.
B. On the server, modify the Credential Delegation settings in the local Group Policy.
C. On all client computers, modify the Password Policy settings in the local Group Policy.
D. On all client computers, modify the Credential Delegation settings in the local Group Policy.

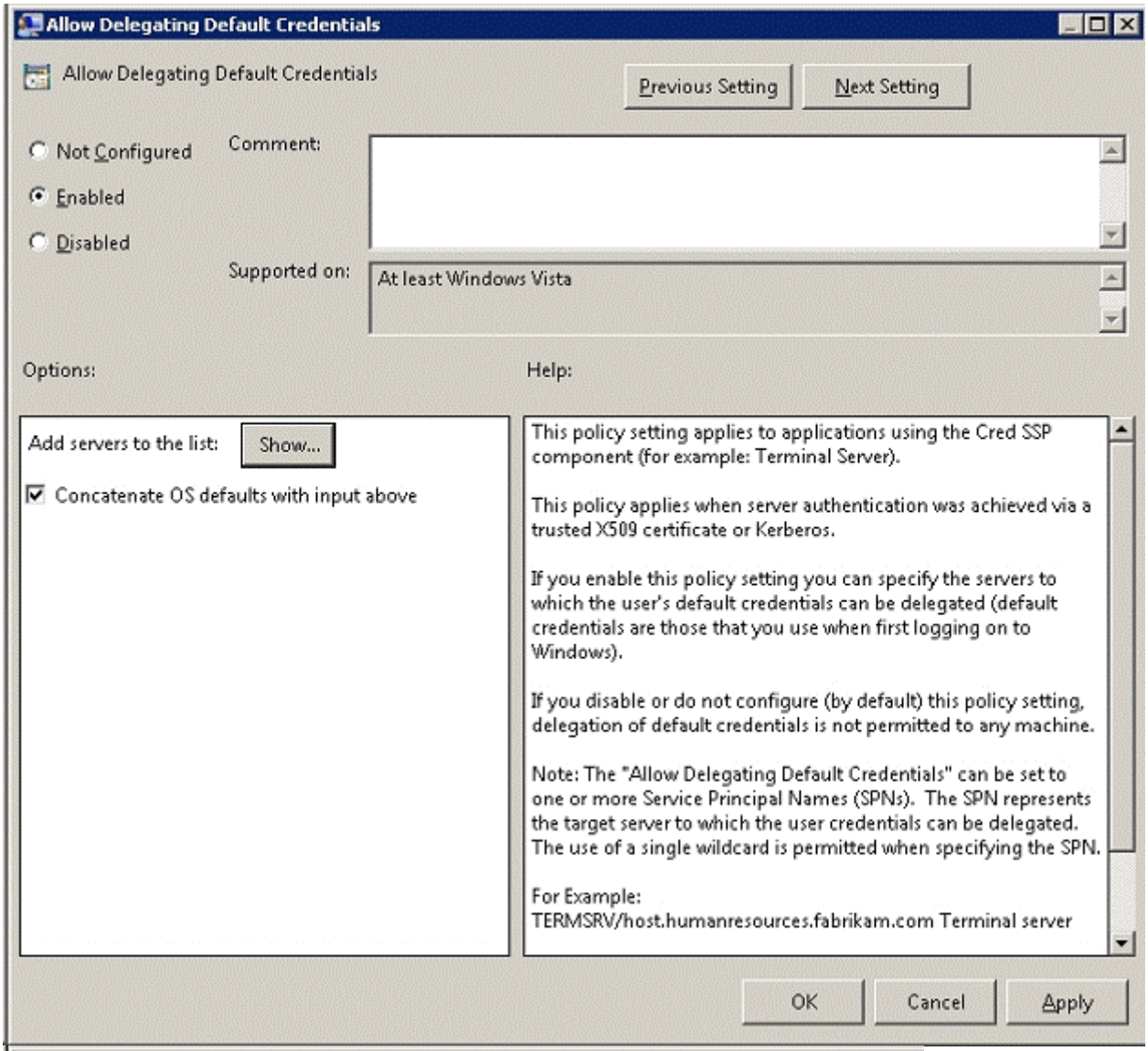
Answer: D

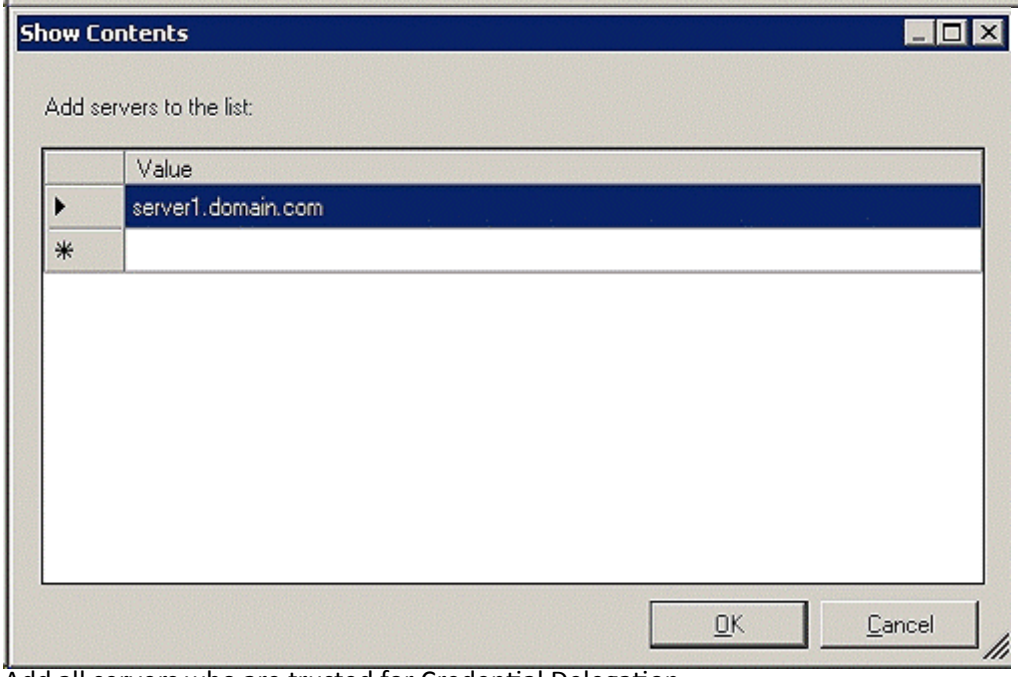
Explanation:
Configuration
CredSSP policies, and by extension the SSO functionality they provide to Terminal Services, are configured via Group Policy. Use the Local Group Policy Editor to navigate to Local Computer Policy\Computer Configuration\Administrative Templates\System\Credentials Delegation , and enable one or more of the policy options. Source:

http://technet.microsoft.com/en-us/library/cc749211(WS.10).aspx
One needs to enable the policy on the client computers, because one want to allow the client computer to reuse the credentials.



Navigate to Computer Configuration | Administrative Templates | System | Credentials Delegation Enable the Allow Delegating Default Credentials Setting





Add all servers who are trusted for Credential Delegation.

Source: http://technet.microsoft.com/en-us/library/cc749211(WS.10).aspx

Question: 44

You have a server named Server1 that runs Windows Server 2008 R2. The server has the Web Server (IIS) server role installed. You have an SMTP gateway that connects to the Internet. The internal firewall prevents all computers, except the SMTP gateway, from establishing connections over TCP port 25. You configure the SMTP gateway to relay email for Server1. You need to configure a Web site on Server1 to send email to Internet users. What should you do?

A. On Server1, install the SMTP Server feature.
B. On Server1, configure the SMTP Email feature for the Web site.
C. On an internal DNS server, create an MX record for Server1.
D. On an internal DNS server, create an MX record for the SMTP gateway.

Answer: B

Explanation:
Configure SMTP Email (IIS 7)
Configure SMTP email in IIS when you want to deliver email messages from your site. Mail can be delivered immediately or it can be delivered to a file location on disk where it can be retrieved for delivery later. For example, a company can provide an email link for sending feedback messages or for requesting information.
To configure SMTP email for a Web application
1. Open IIS Manager and navigate to the level you want to manage. For information about opening IIS Manager, see Open IIS Manager (IIS 7). For information about navigating to locations in the UI, see Navigation in IIS Manager (IIS 7).
2. In Features View, double-click SMTP Email.
3. On the SMTP Email page, type the email address of the sender in the Email address text box.
4. On the SMTP Email page, select one of the following delivery methods:
a. Deliver email to SMTP server: to deliver email messages immediately. This requires an operational SMTP server for which the user has credentials.
b. Store email in pickup directory: to store emails in a file location on disk for later delivery by an application such as an ASP.NET application, or by a user, such as an administrator.
5. If Deliver email to SMTP server is selected, do the following:
a. Type the unique name of your SMTP server in the SMTP Server text box or select the Use localhost box to set the name to LocalHost. Setting the name to LocalHost means that ASP.NET will use an SMTP server on the local computer. Typically, this is the default SMTP virtual server.
b. Enter a TCP port in the Port text box. Port 25 is the SMTP standard TCP port and is the default setting.
More than one virtual server can use the same TCP port if all servers are configured by using different IP addresses.
c. Under Authentication Settings, specify the authentication mode and credentials if your SMTP server requires these.
6. If Store email in pickup directory is selected, type the batch email location in the Store email in pickup directory text box.
7. Click Apply in the Actions pane.
Source: http://technet.microsoft.com/en-us/library/cc772058(WS.10).aspx

Question: 45

You install a new server named MediaSrv2 that runs Windows Server 2008. The server has the Streaming Media Services role installed. All client computers run Windows Vista and use the Windows Media Player 11 application. You configure a Publishing Point and assign a content source that has video media. Users are unable to pause and rewind the media player. You need to ensure that the users are able to control the playback of the streaming media.
What should you do?

A. Reconfigure the Publishing Point as an on-demand publishing point.
B. Configure MediaSrv2 to only use the Real Time Streaming Protocol (RTSP).
C. Configure MediaSrv2 to only use the Hypertext Transfer Protocol (HTTP).
D. Enable Publishing Points ACL Authorization on the Publishing Point.

Answer: A

Explanation:
To ensure that the users have full playback control of the streaming media, you should reconfigure the Publishing Point as an on-demand publishing point. On-demand publishing point distributes the content only when it is requested by a client. Users that receive this content might be able to modify its playback by pausing, rewinding, or fast-forwarding the stream. This type of publishing point is commonly used when the content originates from a file, such as a playlist or other Windows Media file, and can be used for personalized radio stations, online video stores, and self-paced training applications. On-demand publishing points always deliver their content as a unicast stream.
Reference: http://technet2.microsoft.com/windowsserver2008/en/library/0e1137b9-d97a-4eae-a6f1-8c0f7227a3b11033.mspx?mfr=true

Question: 46

Your company has an Active Directory domain. All servers in the domain run Windows Server 2008 R2. The RD Gateway role service is installed on a server named Server1. The Remote Desktop Services server role is installed on servers named Server2 and Server3. Server2 and Server3 are configured in a load balancing Remote Desktop Server farm named Farm1. You install and configure the RD Connection Broker service on a new server named Server4. You need to configure Server2 and Server3 to join the RD Connection Broker. What should you do next?

A. Configure Server2 and Server3 to use the RD Gateway role service to access RD Connection Broker.
B. Create a new Group Policy object (GPO) that assigns Server4 to Server2 and Server3 as their connection broker server. Apply the GPO to Server2 and Server3.
C. Configure a Group Policy object (GPO) to set the Set RD Gateway server address option in the Remote Desktop Services section to Server1. Apply the GPO to all client computers.
D. Configure a Group Policy object (GPO) to set the Require secure RPC communications option in the Remote Desktop Services section to False. Apply the GPO to Server2 and Server3.

Answer: B

Explanation: Explanation:
Policy settings in this node control configuration of a Remote Desktop Session Host server that is a member of a load-balanced Remote Desktop Session Host server farm. Join RD Connection Broker This policy setting allows you to specify whether the RD Session Host server should join a farm in RD Connection Broker. RD Connection Broker tracks user sessions and allows a user to reconnect to their existing session in a load-balanced RD Session Host server farm. To participate in RD Connection Broker, the Remote Desktop Session Host role service must be installed on the server. If the policy setting is enabled, the RD Session Host server joins the farm that is specified in the Configure RD Connection Broker Farm Name setting. The farm exists on the RD Connection Broker server that is specified in the Configure RD Connection Broker Server name policy setting. !If you enable this setting, you must also enable the "Configure RD Connection Broker Farm Name" and Configure RD Connection Broker Server name policy settings, or configure these settings by using either the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider. Configure RD Connection Broker farm name This policy setting allows you to specify the name of a farm to join in RD Connection Broker. RD Connection Broker uses the farm name to determine which RD Session Host servers are in the same RD Session Host server farm. Therefore, you must use the same farm name for all RD Session

Host servers in the same loadbalanced farm. The farm name does not have to correspond to a name in Active Directory Domain Services. If you specify a new farm name, a new farm is created in RD Connection Broker. If you specify an existing farm name, the server joins that farm in RD Connection Broker. !If you enable this policy setting, you must specify the name of a farm in RD Connection Broker. Configure RD Connection Broker server name This policy setting allows you to specify the RD Connection Broker server that the RD Session Host server uses to track and redirect user sessions for a load-balanced RD Session Host server farm. The specified server must be running the Remote Desktop Connection Broker service. All RD Session Host servers in a load-balanced farm should use the same RD Connection Broker server.
Source: http://technet.microsoft.com/en-us/library/ee791821(WS.10).aspx

Question: 47

Your company has an Active Directory domain. The company runs Remote Desktop Services. You configure the main office printer as the default printer on the Remote Desktop Session Host Server. The company policy states that all remote client computers must meet the following requirements:
The main office printer must be the default printer of the client computers.
Users must be able to access their local printers during a terminal session.
You need to create a Group Policy Object by using the Remote Desktop Session Host Services Printer Redirection template to meet the company policy. What should you do?

A. Set the Easy Print driver first option to Disabled. Apply the GPO to the Terminal Server.
B. Set the Use Terminal Services Easy Print driver first option to Disabled. Apply the GPO to all the client computers.
C. Set the Do not set default client printer to be default printer in a session option to Enabled. Apply the GPO to the Terminal Server.
D. Set the Do not set default client printer to be default printer in a session option to Enabled. Apply the GPO to all the client computers.

Answer: C

Explanation:
To set a Group Policy Object by using the Remote Desktop Services Printer Redirection template, you should access the session options and set the 'Do not set default client printer' to default printer Enabled. Apply GPO to the Remote Desktop Session Host Server. When you set the default client printer to default printer enabled, the main printer will become the default printer. The GPO will set the policy of accessing the main office printer by default and the user printers will also be accessible during Remote Desktop Connection so if the default printer is busy or has any problem, the next available printer (user printer) will automatically print the required document.

Question: 48

You manage a member server that runs Windows Server 2008 R2. The server has the Remote Desktop Services server role installed. Windows System Resource Manager (WSRM) is installed on the server. Users report performance degradation on the Remote Desktop Session Host Server. You monitor the server and notice that one user is consuming 100 percent of the processor time. You create a resource-allocation policy named Policy1 that limits each user to 30 percent of the total processor time. You observe no performance improvement. You need to configure WSRM to enforce Policy1. What should you do?

A. Set Policy1 as the Profiling Policy.
B. Set Policy1 as the Managing Policy.
C. Restart the Remote Desktop Configuration service.
D. Launch the WSRM application by using the user context of the Remote Desktop Session Host Server System

account.

Answer: B

Resource-Allocation Policies
WSRM uses resource-allocation policies to determine how computer resources, such as CPU and memory, are allocated to processes running on the computer. There are two resource-allocation policies that are specifically designed for computers running Terminal Services. The two Terminal Services-specific resource-allocation policies are:
Equal_Per_User
Equal_Per_Session
To implement the Equal_Per_Session resource-allocation policy
Open the Windows System Resource Manager snap-in.
In the console tree, expand the Resource Allocation Policies node.
Right-click Equal_Per_Session, and then click Set as Managing Policy.
If a dialog box appears informing you that the calendar will be disabled, click OK.
Source: http://technet.microsoft.com/en-us/library/cc771218(WS.10).aspx

Question: 49

Your company has a single Active Directory domain named contoso.com. All servers in the domain run Windows Server 2008. The DNS service is installed on two domain controllers named DC1 and DC2. Both DNS servers host Active Directory integrated zones that are configured to allow the most secure updates only. DC1 has Key Management Service (KMS) installed and activated. You discover that the service locator records from the contoso.com zone hosted on DC1 and DC2 are missing. You need to force registration of the KMS service locator records in the contoso.com zone. What should you do?

A. Configure the contoso.com zone to accept non-secure updates.
B. On DC1 at the command prompt, run the slmgr.vbs Crearm script.
C. On DC1 at the command prompt, run the net stop sppsvc command, and then run the net start sppsvc command.
D. On DC2 at the command prompt, run the net stop netlogon command, and then run the net start netlogon command.

Answer: C

Explanation:
To force registration of the KMS service locator records in the contoso.com zone, you should run the net stop sppsvc command at the command prompt and then execute the net start sppsvc command. This whole procedure is to start the KMS service locator records to force registration in the contoso.com zone.

Question: 50

You have a server that runs the Terminal Services Gateway (TS Gateway) role service. Users need to connect remotely through the gateway to desktop computers located in their offices. You create a security group named Remote1 for the users who need to connect to computers in their offices. You need to enable the users to connect to the TS Gateway. What should you do?

A. Add the Remote1 security group to the local remote desktop users group on the TS Gateway server.
B. Create a client authorization policy. Add the Remote1 security group and enable Device redirection.
C. Create a resource authorization policy. Add the Remote1 security group and enable Users to connect to any resource.

D. Create a Group Policy object and enable the Set TS Gateway authentication method properties to Ask for credentials, use Basic protocol. Apply the policy to the TS Gateway server.

Answer: B

Explanation:
To enable the remote users belonging to RemoteUsersGrp1 to connect to the TS Gateway, you need to create a client authorization policy. Add the RemoteUsersGrp1 security group and enable Device redirection. A connection authorization policy (CAP) allows you to control who can connect to the Terminal Server through the Terminal Services Gateway. The Device Redirection gives you the option of disabling redirection for trusted a remote client devices. The tab contains a series of checkboxes that you can use to disable things like disk drives, the Windows clipboard, printers, serial ports, and even plug and play devices. Reference: Configuring the Windows Server 2008 Terminal Services Gateway (Part 2)/ Create a Terminal Services Gateway CAP
http://www.windowsecurity.com/articles/Configuring-Windows-Server-2008-Terminal-Services-Gateway-Part2.html
Reference: An Overview of Longhorn Server's Terminal Service Gateway (Part 4)
http://www.msterminalservices.org/articles/Overview-Longhorn-Servers-Terminal-Service-Gateway-Part4.html

Question: 51

You manage a computer named FTPSrv1 that runs Windows Server 2008. Your company policy requires that the FTP service be available only when required by authorized projects. You need to ensure that the FTP service is unavailable after restarting the server. What should you do?

A. Run the iisreset command on the FTPSrv1 server.
B. Run the net stop msftpsvc command on the FTP server.
C. Run the suspend-service msftpsvc cmdlet in Microsoft Windows PowerShell tool.
D. Run the WMIC /NODE:FTPSrv1 SERVICE WHERE caption="FTP Publishing Service" CALL ChangeStartMode "Disabled" command on the FTP server.

Answer: D

Explanation:
To make sure that FTP service unavailable after restarting the server, you need to Run the WMIC /NODE: TKFSVE SERVICE WHERE the caption="FTP Publishing Service" CALL ChangeStartMode "Disabled" command on this particular FTP server. The WMI command-line (WMIC) utility provides a command-line interface for WMI. The /Node command allows you to specify computer names and synchronously execute all commands against all computers listed in this value. To disable FTP service on the computer, you need to use ChangeStartMode "Disabled" command.
Reference: http://msdn2.microsoft.com/en-us/library/aa394531(VS.85).aspx
Reference: Gathering WMI Data without Writing a Single Line of Code / System Configuration Changes
http://technet.microsoft.com/en-us/magazine/cc160919.aspx

Question: 52

Your company has an Active Directory domain. The company has a server named Server1 that has the Terminal Services role and the Terminal Services Web Access role installed. All client computers run Windows XP Service Pack 2 (SP2). You deploy and publish an application named TimeReport on Server1. The Terminal Services Web Access role uses Active Directory Domain Services (AD DS) and Network Level Authentication is enabled. You need to ensure that the users can launch TimeReport on Server1 from the Terminal Services Web Access Web page. What should you do?

A. Disable publishing to AD DS for the TimeReport remote application.

B. Install the Remote Desktop Client 6.1 application on the client computers that run Windows XP SP2.
C. Publish TimeReport on Server1 as a Microsoft Windows Installer package. Distribute the Windows Installer package to the users.
D. Install the Terminal Services Gateway (TS Gateway) role on Server1. Reconfigure the TimeReport remote application publishing to reflect the change in the infrastructure.

Answer: B

Explanation:
To ensure that the users can launch App1 on Server1 from the Terminal Services Web Access Web page, you need to install the Remote Desktop Client 6.1 application on the client computers, which eases the deployment of Windows Server 2008 Terminal services on the client computers that run Windows XP Service Pack 2. Because the Remote Desktop Client 6.1 application supports Terminal Services Web Access, the Windows XP users can launch App1 on Server1 from their Terminal Services Web Access Web page. Reference: Download Microsoft Remote Desktop Connection (Terminal Services Client 6.1) for Windows XP SP2
http://www.dabcc.com/article.aspx?id=8044

Question: 53

You manage 20 servers that run Windows Server 2008 R2. The Remote Desktop Services server role and the Windows System Resource Manager (WSRM) feature are installed on all the servers. You create and configure a resource-allocation policy that has the required custom settings on a server named TS01. You need to configure the WSRM settings on all the servers to match the WSRM settings on TS01. What should you do?

A. Use the Windows Backup tool to back up only the System State data on TS01. Use the Windows Backup tool to restore the System State data on each server.
B. Use the WSRM console on each server to enable the Accounting function. Configure the Remote WSRM accounting option to TS01 on each server.
C. Use the WSRM console on TS01 to export the WSRM information to a shared folder. Use the WSRM console to import the WSRM information from the shared folder.
D. Use the regedit tool to export the HKLM\SYSTEM\CurrentControlSet\Services\WSRM registry key on TS01 to a shared folder. On each server, delete this registry key and use the regedit tool to import the registry key from the shared folder.

Answer: C

Explanation:
Import or Export Criteria, Policies, and Schedules
You can import or export Windows System Resource Manager configuration information between computers. Configuration information stored includes process matching criteria, resource allocation policies, calendar events and schedules, and conditional policies. In this way, you can create management scenarios and then deploy them on other computers without performing the configuration multiple times. Files Created and Imported The files created by or imported by Windows System Resource Manager are:
Exporting and Importing Configuration Information To export configuration information
1. Open Windows System Resource Manager.
2. In the navigation tree, right-click Windows System Resource Manager, and then click Export WSRM Information.
3. In Location, type a directory path where you want to save the configuration information, or click Browse to find the directory you want to use. When you have entered the directory information, click OK.
4. Windows System Resource Manager creates four XML documents in the specified directory that contain information about criteria, policies, and schedules.

To import configuration information
1. Open Windows System Resource Manager.
2. In the navigation tree, right-click Windows System Resource Manager, and then click Import WSRM Information.
3. In Location, type a directory path where the configuration information you want to import is located, or click Browse to find the directory you want to use. When you have entered the directory information, click OK.
4. Windows System Resource Manager loads the XML files into its current configuration, overwriting any previous configuration data.
Source: http://technet.microsoft.com/en-us/library/cc771960(WS.10).aspx

Question: 54

You have the Web Server (IIS) role installed on a server that runs Windows Server 2008. You make changes to the configuration of an application named APP1. Users report that the application fails. You examine the event log and discover the following error message:
You need to ensure that users are able to connect to APP1. Which command should you run at the command prompt on the server?

A. appcmd set config
B. appcmd stop apppool
C. appcmd start apppool
D. appcmd set apppool

Answer: C

Explanation:
To ensure that users are able to connect to App1, you need to run appcmd start apppool on the server.
The "503 Service Unavailable" error mostly occurs whenever HTTP.SYS, the kernel HTTP driver that manages http connections for IIS, fails to create an IIS worker process to process the request. This failure is typically caused by a critical error during worker process initialization, or more likely an unhandled exception / access violation occurring during worker process startup. After a certain number of failures, the application pool will trigger Rapid Fail Protection, a WAS feature designed to stop application pools with a persistent failure condition to avoid an endless loop of failing to start worker processes. At this point, all requests to applications within the stopped application pool will result in the 503 error, and the application pool will need to be re-started manually Reference: Troubleshooting IIS7 503 "Service unavailable" errors with startup debugging
http://mvolo.com/blogs/serverside/archive/2007/05/19/Troubleshooting-IIS7-503-_2200_Service-unavailable_2200_-errors-with-startup-debugging.aspx

Question: 55

Your company has a server that runs Windows Server 2008. The Windows SharePoint Services (WSS) role is installed on the Windows Server 2008 server. You need to configure WSS to support SMTP. What should you do?

A. Bind the SharePoint Web site to port 25.
B. Uninstall and reinstall the WSS role.
C. Install the SMTP Server feature by using the Server Manager console.
D. Install the Application Server role by using the Server Manager console.

Answer: C

Explanation:

To configure WSS to support SMTP, you should install the SMTP server feature through Server Manager Console. Based on SMTP, WSS works with any mail server or SMTP gateway. It acts as an SMTP relay (it does not store mail, only forwards it) and handles all incoming and outgoing SMTP traffic. For most installations, you'll simply have to modify your domain MX record and make a few configuration changes on your email server. When installing WSS on the same host as your mail server, you must make additional configuration changes, such as SMTP port numbers.
Reference: http://www.networkcomputing.com/913/913sp3.html

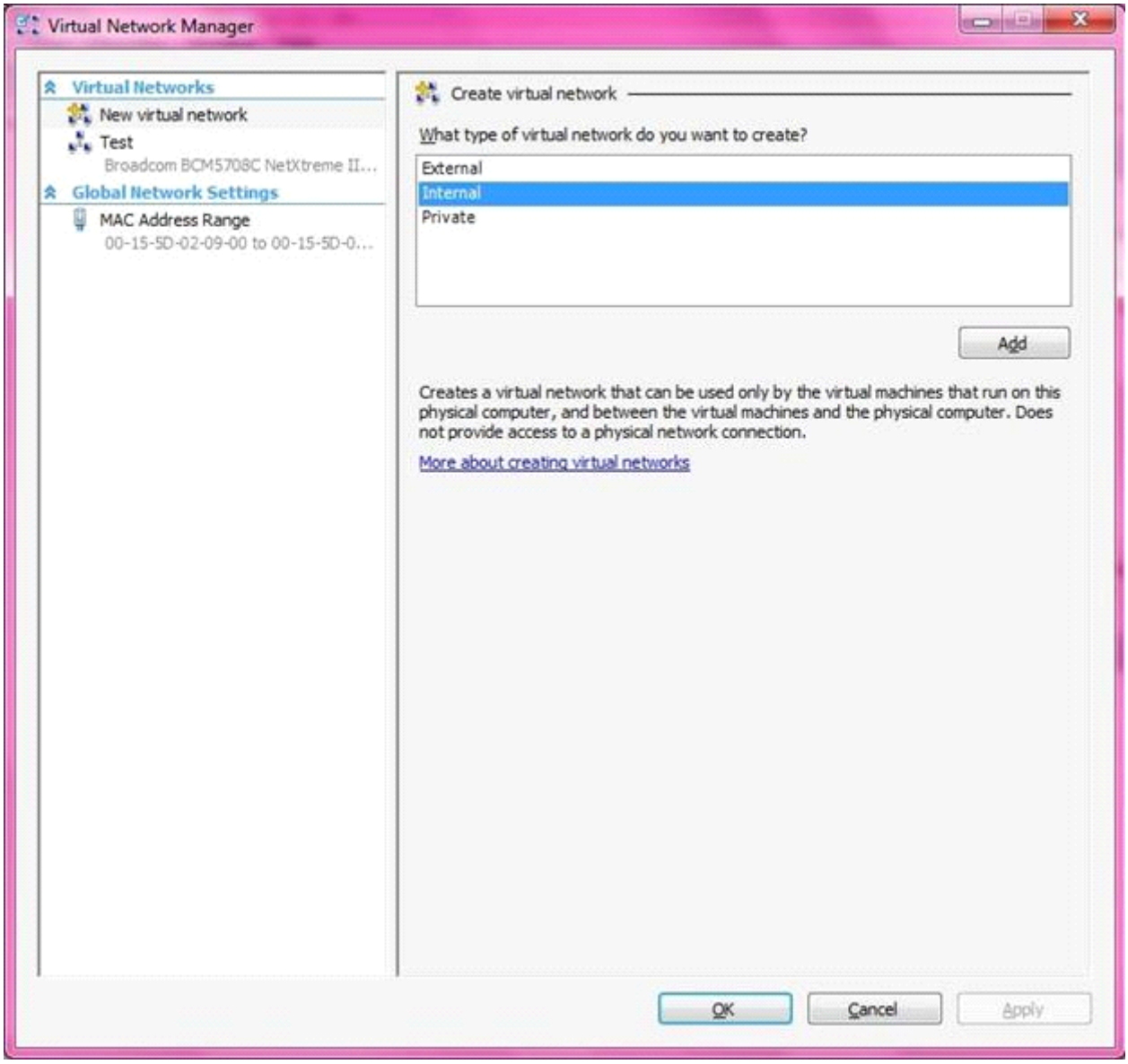
Question: 56

Your company has a server named Server1 that runs Windows Server 2008 and Microsoft Hyper-V. Server1 hosts three virtual machines. Company policy states that the virtual machines must not connect to the company network. You need to configure all of the virtual machines to connect to each other. You must meet the company policy. Which two actions should you perform? (Each answer presents part of the solution. Choose two.)

A. Select the Not connected option for each virtual machine.
B. Enable the Enable virtual LAN identification option for each virtual machine.
C. Set the Connection to Host for the network interface card.
D. Set the Connection to None for the network interface card.

Answer: B, C

Explanation:
To ensure that all the virtual machines connect to each other and you meet the company policy also, you need to first enable the Enable virtual LAN identification option for each virtual machine and then set the Connection to Host for the network interface card. You can use virtual LAN identification as a way to isolate network traffic. However, this type of configuration must be supported by the physical network adapter.
Reference: Step-by-Step Guide to Getting Started with Hyper-V To create a virtual network
http://technet2.microsoft.com/windowsserver2008/en/library/c513e254-adf1-400e-8fcb-c1aec8a029311033.mspx?mfr=true



Question: 57

Your company has a new server that runs Windows Server 2008. The Web Server (IIS) role is installed. Your company hosts a public Web site. You notice unusually high traffic volume on the Web site. You need to identify the source of the traffic.
What should you do?

A. Enable the Web scripting option.
B. Run the netstat Can command on the server.
C. Create a custom view in Event Viewer to filter information from the security log.
D. Enable Web site logging in the IIS Server Manager and filter the logs for the source IP address.

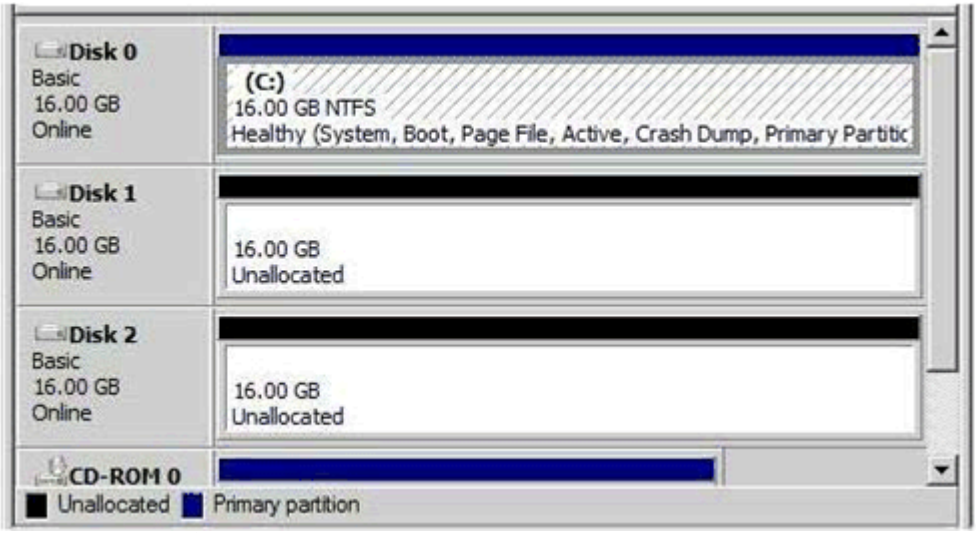
Answer: D

Explanation:
To find the source of unexpected source of traffic, you should open the IIS server manager and enable website logging which will filter the logs for the source IP address. It will list the IP addresses of the people visiting the website and a

lot more information.

Question: 58

Your company has a single Active Directory domain. All the servers run Windows Server 2008. You have a server named FS1 that has the File Services role installed. The company requires that the data disk drives provide redundancy. The disks are configured as shown in the following exhibit.



You need to configure the hard disk drives to support RAID 1.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

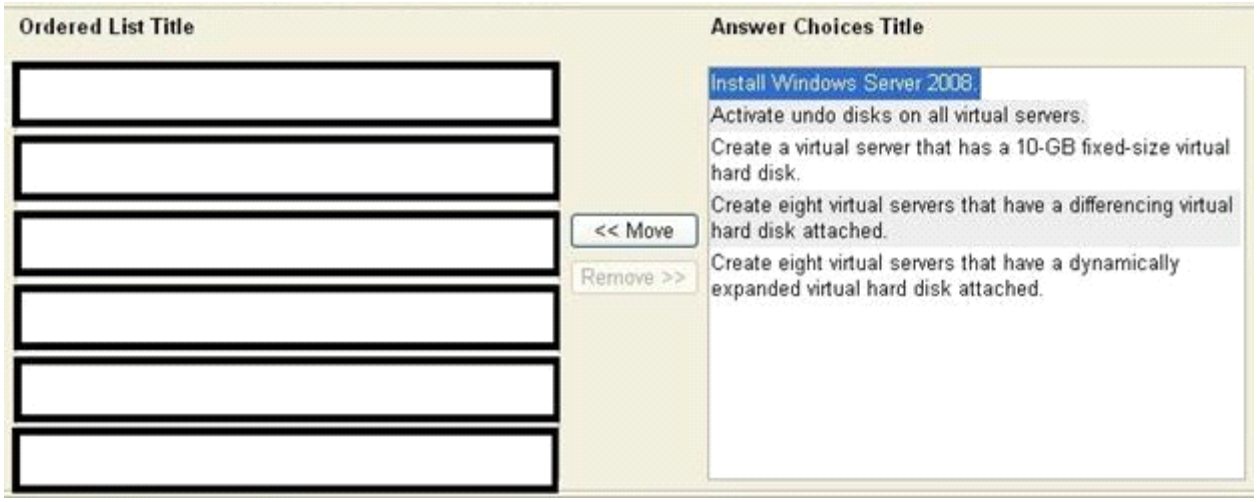
A. Convert Disk 1 and Disk 2 to Dynamic.
B. Create a Striped Volume across Disk 1 and Disk 2.
C. Create a New Mirrored Volume by using Disk 1 and Disk 2.
D. Create a New Spanned Volume by using Disk 1 and Disk 2.

Answer: A, C

Explanation:
To configure the hard drives to support Raid1, you should create Disk1 and Disk 2 as dynamic drives and create a new mirrored volume using Disk1 and Disk 2. In data storage, disk mirroring or RAID1 is the replication of logical disk volumes onto separate physical hard disks in real time to ensure continuous availability. A mirrored volume is a complete logical representation of separate volume copies. Reference: technet2.microsoft.com/windowsserver/en/library/28af1c0d-8490-4ab0-8be0-49e5923c4bae1033.mspx

Question: 59

DRAG DROP
Your company has a server named VS1 that runs Windows Server 2008 and Microsoft Hyper-V. You want to create eight virtual servers that run Windows Server 2008 and configure the virtual servers as an Active Directory forest for testing purposes.
You discover that VS1 has only 30 GB of free hard disk space.
You need to install the eight new virtual servers on VS1.
What should you do? (To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.)



Answer:

Ordered List Title:

Create a virtual server that has a 10-GB fixed-size virtual hard disk.
Install Windows Server 2008.
Create eight virtual servers that have a differencing virtual hard disk attached.

Explanation:
To install the eight new servers on VS1, you need to create a virtual server with a 10 GB fixed-size virtual hard disk and then install Windows Server 2008. After that, you should create eight differencing virtual hard disks and then create eight virtual servers with a differencing virtual hard disk attached. The virtual hard disk should be created first because you need space for eight virtual servers. The fixed-size virtual hard disk can be created through a virtual server. Then you install Windows Server 2008 on it. After that you have to allocate the space for eight virtual servers. To do that, you create differencing virtual hard disk to solve the space problem. Then you create the eight virtual servers with differencing virtual hard disk attached.

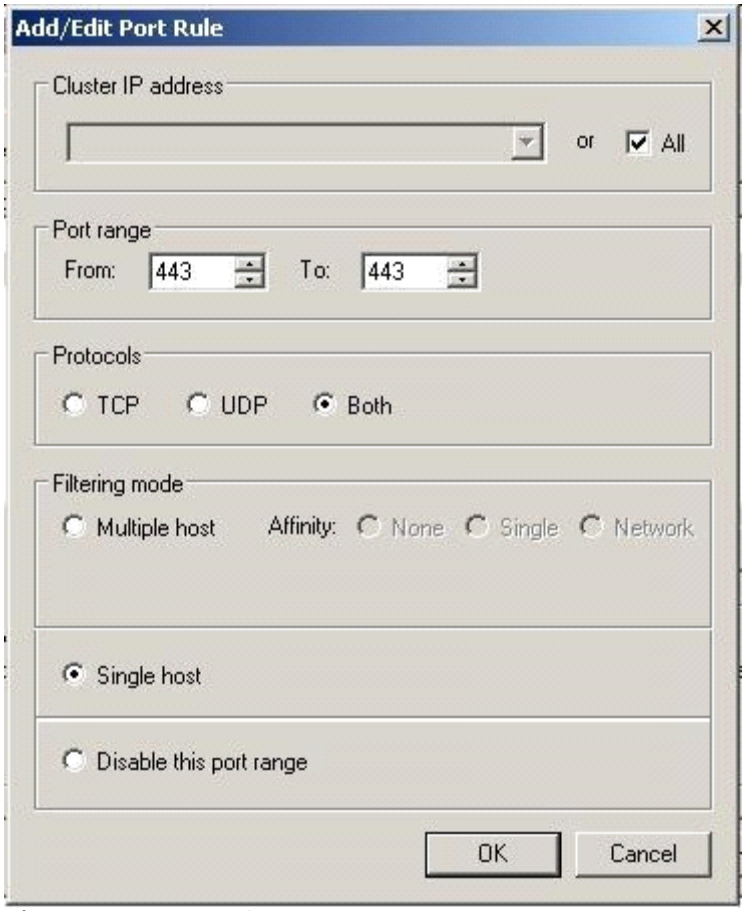
Question: 60

Your company named Contoso, Ltd. has a Network Load Balancing cluster named nlb.contoso.com. The cluster hosts are named WEB1 and WEB2. The cluster is configured with a single port rule that evenly distributes HTTP traffic between both hosts.
You need to configure WEB2 to handle all HTTPS traffic for nlb.contoso.com. You must retain the even distribution of HTTP traffic between WEB1 and WEB2.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

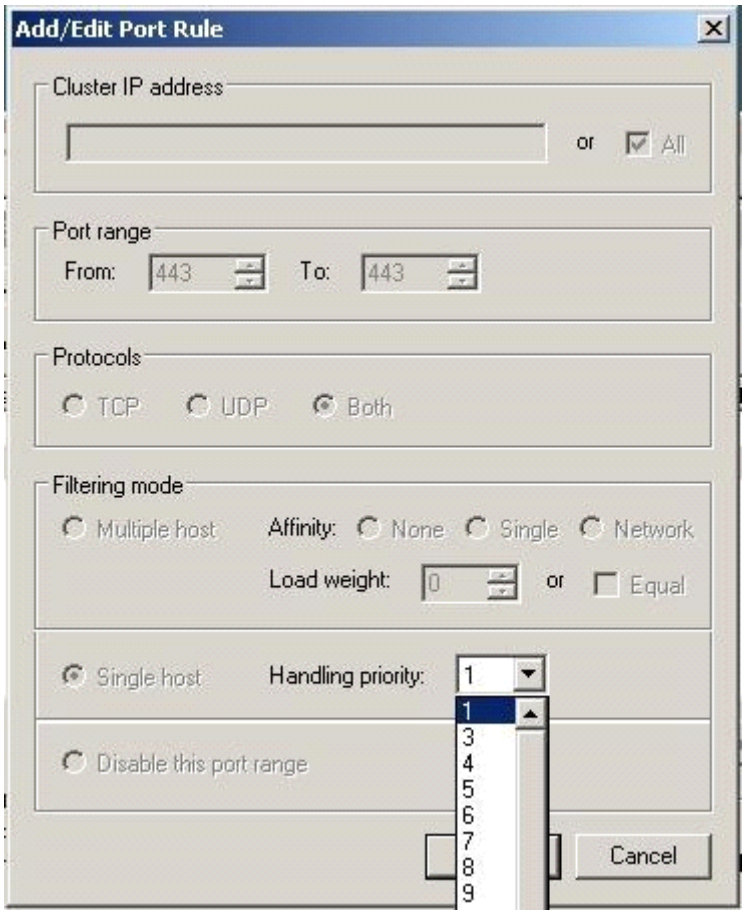
A. In the properties for WEB2, change the Handling priority option for the TCP 443 port rule to the value of 1.
B. In the properties for WEB1, change the Handling priority option for the TCP 443 port rule to the value of 0.
C. In the properties for the cluster, create a new port rule for port TCP 443 that has the Filtering mode option set to Single host.
D. In the properties for the cluster, create a new port rule for port TCP 443 that has the Filtering mode option set to Multiple host and the Affinity option set to the value of Single.

Answer: A, C

Explanation:
Cluster Properties



Cluster Host Properties



Question: 61

You install the Windows SharePoint Services (WSS) role on a server that runs Windows Server 2008. You create a group named SPReviewers that will access content on the WSS server. You need to restrict the permissions for the SPReviewers group to viewing items, opening items, and viewing versions. Which permissions should you configure for the SPReviewers group?

A. Read
B. Design
C. Contribute
D. Limited Access

Answer: A

Explanation:
To restrict the permissions of the group to viewing items, opening items, and viewing versions, you need to assign Read permission. The Read permission level includes the View Items, Open Items, View Pages, and View Versions permissions (among others), all of which are needed to read documents, items, and pages on a SharePoint site.
Reference: About security features of Windows SharePoint Services 3.0
http://office.microsoft.com/en-us/sharepointtechnology/HA100215781033.aspx

Question: 62

Your company has a single Active Directory domain. All servers run Windows Server 2008 R2. You install an iSCSI storage area network (SAN) for a group of file servers. Corporate security policy requires that all data communication to and from the iSCSI SAN must be as secure as possible. You need to implement the highest security available for communications to and from the iSCSI SAN. What should you do?

A. Create a Group Policy object (GPO) to enable the System objects: Strengthen default permission of internal systems objects setting.
B. Create a Group Policy object (GPO) to enable the System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing setting.
C. Implement IPsec security in the iSCSI Initiator Properties. Set up inbound and outbound rules by using Windows Firewall.
D. Implement mutual Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv2) authentication in the iSCSI Initiator Properties. Set up inbound and outbound rules by using Windows Firewall.

Answer: C

Explanation:Explanation:
Security
Microsoft iSCSI Initiator supports using and configuring Challenge Handshake Authentication Protocol (CHAP) and Internet Protocol security (IPsec). All supported iSCSI HBAs also support CHAP; however, some may not support IPsec.
Ipsec
IPsec is a protocol that provides authentication and data encryption at the IP packet layer. The Internet Key Exchange (IKE) protocol is used between peers to allow the peers to authenticate each other and negotiate the packet encryption and authentication mechanisms to be used for the connection. Because Microsoft iSCSI Initiator uses the Windows TCP/IP stack, it can use all of the functionality that is available in the Windows TCP/IP stack. For authentication, this includes preshared keys, Kerberos protocol, and certificates. Active Directory is used to distribute

the IPsec filters to computers running Microsoft iSCSI Initiator. 3DES and HMAC-SHA1 are supported, in addition to tunnel and transport modes. Because iSCSI HBA has a TCP/IP stack embedded in the adapter, the iSCSI HBA can implement IPsec and IKE, so the functionality that is available on the iSCSI HBA may vary. At a minimum, it supports preshared keys and 3DES and HMAC-SHA1. Microsoft iSCSI Initiator has a common API that is used to configure IPsec for Microsoft iSCSI Initiator and iSCSI HBA.
Easier Firewall configuration for Windows Server 2008 R2 and Windows 7
Allowing the use of an Internet Storage Name Service (iSNS) server through the firewall is possible directly from the iSCSICLI command-line utility. However, you can still controll it through the Windows Firewall with Advanced Security, if desired.
To enable iSNS traffic for use with Microsoft iSCSI Initiator Use the following command to enable iSNS traffic through the firewall. This allows you to use an iSNS server with the local Microsoft iSCSI Initiator:
iscsicli FirewallExemptiSNSServer
Source: http://technet.microsoft.com/en-us/library/ee338480.aspx

Question: 63

Your company has an Active Directory domain. The company has a server named Server1 that has the Remote Desktop Services server role and the RD Web Access role service installed. The company has a server named Server2 that runs ISA Server 2006. The company deploys the Remote Desktop Gateway (RD Gateway) role on a new server named Server3. The company wants to use ISA as the SSL endpoint for Remote Desktop connections. You need to configure the RD Gateway role on Server3 to use ISA 2006 on Server2. What should you do?

A. Configure the RD Gateway to use SSL HTTPS-HTTP bridging.
B. Configure the Remote Desktop Connection Authorization Policy Store on Server3 to use Server2 as the Central Network Policy Server.
C. Export the SSL certificate from Server2 and install the SSL certificate on Server3. Configure the RD Gateway to use the SSL certificate from Server2.
D. Export a self-signed SSL certificate from Server3 and install the SSL certificate on Server2.
Configure the ISA service on Server2 to use the SSL certificate from Server3.

Answer: A

Explanation:Explanation:
To enhance security for an RD Gateway server, you can configure Microsoft Internet Security and Acceleration (ISA) Server or a non-Microsoft product to function as a Secure Sockets Layer (SSL) bridging device. The SSL bridging device can enhance security by terminating SSL sessions, inspecting packets, and re-establishing SSL sessions. You can configure ISA Server communication with the RD Gateway server in either of the two following ways: HTTPS-HTTPS bridging. In this configuration, the RD Gateway client initiates an SSL (HTTPS) request to the SSL bridging device. The SSL bridging device initiates a new HTTPS request to the RD Gateway server, for maximum security. HTTPS-HTTP bridging. In this configuration, the RD Gateway client initiates an SSL (HTTPS) request to the SSL bridging device. The SSL bridging device initiates a new HTTP request to the RD Gateway server. To use HTTPS-HTTPS or HTTPS-HTTP bridging, you must enable the Use SSL Bridging setting on the RD Gateway server.
Source: http://technet.microsoft.com/en-us/library/cc772387.aspx

Question: 64

You install the Web Server (IIS) role on a server that runs Windows Server 2008. Your companys human resources department has a Web site named www.contoso.com/hr. You need to create a virtual directory on the company Web site for the HR department. Which command should you run on the Web server?

A. appcmd add app /app.name:contoso /path:/hr/physicalPath:c:\websites\hr
B. appcmd add site/name:hr/physicalPath:c:\websites\hr
C. appcmd add vdir/app.name:contoso /path:/hr/physicalPath:c:\websites\hr
D. appcmd set vdir/vdir.name:hr/path:/hr /physicalPath:c:\websites\hr

Answer: C

Explanation:
The syntax to add a virtual directory to the root application in a site is:
appcmd add vdir /app.name:string/ /path:string /physicalPath:string The variable app.namestring is the site name and the / following the name specifies that the virtual directory should be added to the root application of the site. The variable pathstring is the virtual path of the virtual directory, such as /sl, and physicalPathstring is the physical path of the virtual directory's content in the file system. For example, to add a virtual directory named sl with a physical location of c:\websites to the root application in a site named contoso, you need to type the following command prompt appcmd add vdir /app.name: contoso / path:/sl /physicalPath:c:\websites\sl
Reference: IIS 7.0: Create a Virtual Directory
http://technet2.microsoft.com/windowsserver2008/en/library/87d8a3d7-8d90-4626-8f85-3c782ec9a5331033.mspx?mfr=true

Question: 65

You have two servers named FC1 and FC2 that run Windows Server 2008 R2 Enterprise. Both servers have the Failover Clustering feature installed. You configure the servers as a two-node cluster. The cluster runs an application named APP1. Business hours for your company are 09:00 to 17:00. APP1 must be available during these hours. You configure FC1 as the preferred owner for APP1. You need to prevent failback of the cluster during business hours. What should you do?

A. Set the Period option to 8 hours in the Failover properties.
B. Set the Allow failback option to allow failback between 17 and 9 hours in the Failover properties.
C. Enable the Prevent failback option in the Failover properties.
D. Enable the If resource fails, attempt restart on current node policy for all APP1 resources. Set the Maximum restarts for specified period to 0.

Answer: B

Explanation:
Failback timing
You can set a group to fail back to its preferred node as soon as the Cluster service detects that the failed node has been restored, or you can instruct the Cluster service to wait until a specified hour of the day, such as after peak business hours.
Important
Failback only occurs when you have defined a preferred nodes list for a resource group and failback is allowed for that resource group. If you specify that a group failback to a preferred node and then restart the node to test the failback policy you set, the resource group will not failback. A resource group will not failback when a node is restarted after a planned shutdown and restart. To test the failback policy, you must press the reset button on the node.
Source: http://technet.microsoft.com/en-us/library/cc737785.aspx

Question: 66

You have a Terminal Server that runs Windows Server 2008. You create a Windows Installer package for Microsoft

Office Word 2007 by using Terminal Services RemoteApp (TS RemoteApp). You install the package on a client computer. You double-click on a Word document and receive the following error. Windows cannot open this file. You need to ensure that you can open the Word document by double-clicking on the file. What should you do?

A. Recreate the Windows Installer package.
B. Modify the file association on the client computer.
C. Modify the file association on the TS RemoteApp server.
D. Install the Windows Installer package by using msiexec.exe.

Answer: C

Question: 67

Your company has an Active Directory domain. The company runs Remote Desktop Services. All Remote Desktop Services accounts are configured to allow session takeover without permission. A user has logged on to a server named Server2 by using an account named User1. The session ID for User1 is 1337. You need to perform a session takeover for session ID 1337. Which commands should you run?

A. Chgusr 1337 /disable, and then Tscon 1337
B. Takeown /U User1 1337, and then Tscon 1337
C. Tsdiscon 1337, and then Chgport /U User1 1337
D. Tsdiscon 1337, and then Tscon 1337

Answer: D

Explanation:

tsdiscon

Disconnects a session from a terminal server.

```
tsdiscon [<SessionID> | <SessionName>] [/server:<ServerName>] [/v]
```

Parameter	Description
<SessionId>	Specifies the ID of the session to disconnect.
<SessionName>	Specifies the name of the session to disconnect.
/server:<ServerName>	Specifies the terminal server that contains the session that you want to disconnect. Otherwise, the current terminal server is used.
/v	Displays information about the actions being performed.
/?	Displays help at the command prompt.

Source: http://technet.microsoft.com/en-us/library/cc770592(WS.10).aspx

tscon

Connects to another session on a terminal server.

```
tscon {<SessionID> | <SessionName>} [/dest:<SessionName>] [/password:<pw> | /
password:*] [/v]
```

Parameter	Description
<SessionID>	Specifies the ID of the session to which you want to connect. If you use the optional **/dest:**<*SessionName*> parameter, this is the ID of the session to which you want to connect.
<SessionName>	Specifies the name of the session to which you want to connect.
/dest:<SessionName>	Specifies the name of the current session. This session will disconnect when you connect to the new session.
/password:<pw>	Specifies the password of the user who owns the session to which you want to connect. This password is required when the connecting user does not own the session.
/password:*	Prompts for the password of the user who owns the session to which you want to connect.
/v	Displays information about the actions being performed.
/?	Displays help at the command prompt.

Source: http://technet.microsoft.com/en-us/library/cc770988(WS.10).aspx

Wrong answers:

chgport
Lists or changes the COM port mappings to be compatible with MS-DOS applications.
Source: http://technet.microsoft.com/en-us/library/cc771976(WS.10).aspx
chgusr
Changes the install mode for the terminal server.
Source: http://technet.microsoft.com/en-us/library/cc755189(WS.10).aspx takeown
Enables an administrator to recover access to a file that previously was denied, by making the administrator the owner of the file.
Source: http://technet.microsoft.com/en-us/library/cc753024(WS.10).aspx

Question: 68

You have a server that runs Windows Server 2008. You install the Windows Media Services server role on the server. You plan to publish an audio file to the Internet by using Media Server. You need to create a license for the audio file. What should you do first?

A. Publish the audio file to a new Web site.
B. Publish the audio file to the Windows Media Services server.
C. Package the audio file as a Windows Installer application.
D. Package the audio file by using Windows Media Rights Manager.

Answer: D

Question: 69

You manage a new server that runs Windows Server 2008 R2. You plan to install the Streaming Media Services server role on the server. Users will access content on the new server by using Windows Media Player for Windows 7 and Windows Media Player for Mac. You need to install the Streaming Media Services server role on the server to support both media players. What should you do?

A. Install Session Initiation Protocol (SIP).
B. Install Simple Object Access Protocol (SOAP).
C. Install Stream Control Transmission Protocol (SCTP).
D. Install RPC over HTTPS.

Answer: B

Explanation:
SCTP: No support in Mac
SIP: Identification over VoIP
SOAP: Access object web

Question: 70

You implement a member server that runs Windows Server 2008 R2. The member server has the Web Server (IIS) role installed. The member server also hosts intranet Web sites.
Your company policy has the following requirements:
Use encryption for all authentication traffic to the intranet Web site.
Authenticate users by using their Active Directory credentials.
Avoid the use of SSL on the Web server for performance reasons.

You need to configure all the Web sites on the server to meet the company policy.
Which three actions should you perform? (Each correct answer presents part of the solution. Choose three.)

A. Configure the Basic Authentication setting on the server to Enabled.
B. Configure the Digest Authentication setting on the server to Enabled.
C. Configure the Windows Authentication setting on the server to Enabled.
D. Configure the Anonymous Authentication setting on the server to Disabled.
E. Configure the Active Directory Client Certificate Authentication setting on the server to Enabled.

Answer: B, C, D

Question: 71

You have a server that runs Windows Server 2008 Enterprise Edition. The server has the Failover Clustering feature installed. The server has three nodes named NODE1, NODE2, and NODE3. The Microsoft Distributed Transaction Coordinator (MSDTC) resource is installed on the cluster. The cluster has a dedicated cluster group named Group1 that includes the MSDTC resource. You discover that Group1 is unable to failover to NODE3 from NODE1 or NODE2. The failover from NODE1 to NODE2 functions without errors. You need to configure Group1 to support the failover between all cluster nodes. What should you do?

A. Remove the MSDTC resource from Group1.
B. Select NODE3 as a preferred owner for Group1.
C. Remove NODE3 as a possible owner from all cluster resources in Group1.
D. Configure NODE3 as a possible owner for all cluster resources in Group1.

Answer: D

Question: 72

You have 10 servers that run Windows Server 2008 R2. The servers have the Web Server (IIS) server role installed. The servers are members of a Web server farm. The servers host the same Web site. You need to configure the servers to meet the following requirements:

- Allow changes to the Web server configurations that are made on one server to be made on all servers in the farm.
- Minimize administrative effort to perform the configuration changes.

What should you do?

A. On all servers, configure the Shared Configuration settings.
B. On one server, configure the Shared Configuration setting.
C. On one server, create a scheduled task that copies the Intepub folder to the other servers.
D. Create a DFS Namespace. On each server configure the Inetpub folder as the target of the DFS Namespace.

Answer: A

Explanation:
To configure settings to use shared configuration files and encryption keys
1. Open IIS Manager and click the server node. For information about opening IIS Manager, see Open IIS Manager (IIS 7).
2. In Features View, double-click Management Service.
3. On the Management Service page, in the Actions pane, click Stop.
4. In the toolbar, click the back button.

5. In Features View, double-click Shared Configuration.
6. Select Enable shared configuration to enable the Shared Configuration feature.
7. Under Configuration Location, in the Physical path box, type the physical path or click the browse button (...) to locate the physical path of the configuration directory.
8. In the User name box, type a user name of an account that has access to the configuration directory. Then in the Password and Confirm Password boxes, type the password associated with this user account.
9. In the Actions pane, click Apply.
10. In the Encryption Keys Password dialog box, in the Enter encryption key password box, type the password that is used to access the encryption keys in the configuration directory. Then click OK.
Note This is the password that was specified when the configuration files and encryption keys were exported.
11. Close IIS Manager and then reopen it. In the Connections pane, click the server node.
12. In Features View, double-click Management Service.
13.On the Management Service page, in the Actions pane, click Start
Source: http://technet.microsoft.com/en-us/library/cc771871(WS.10).aspx

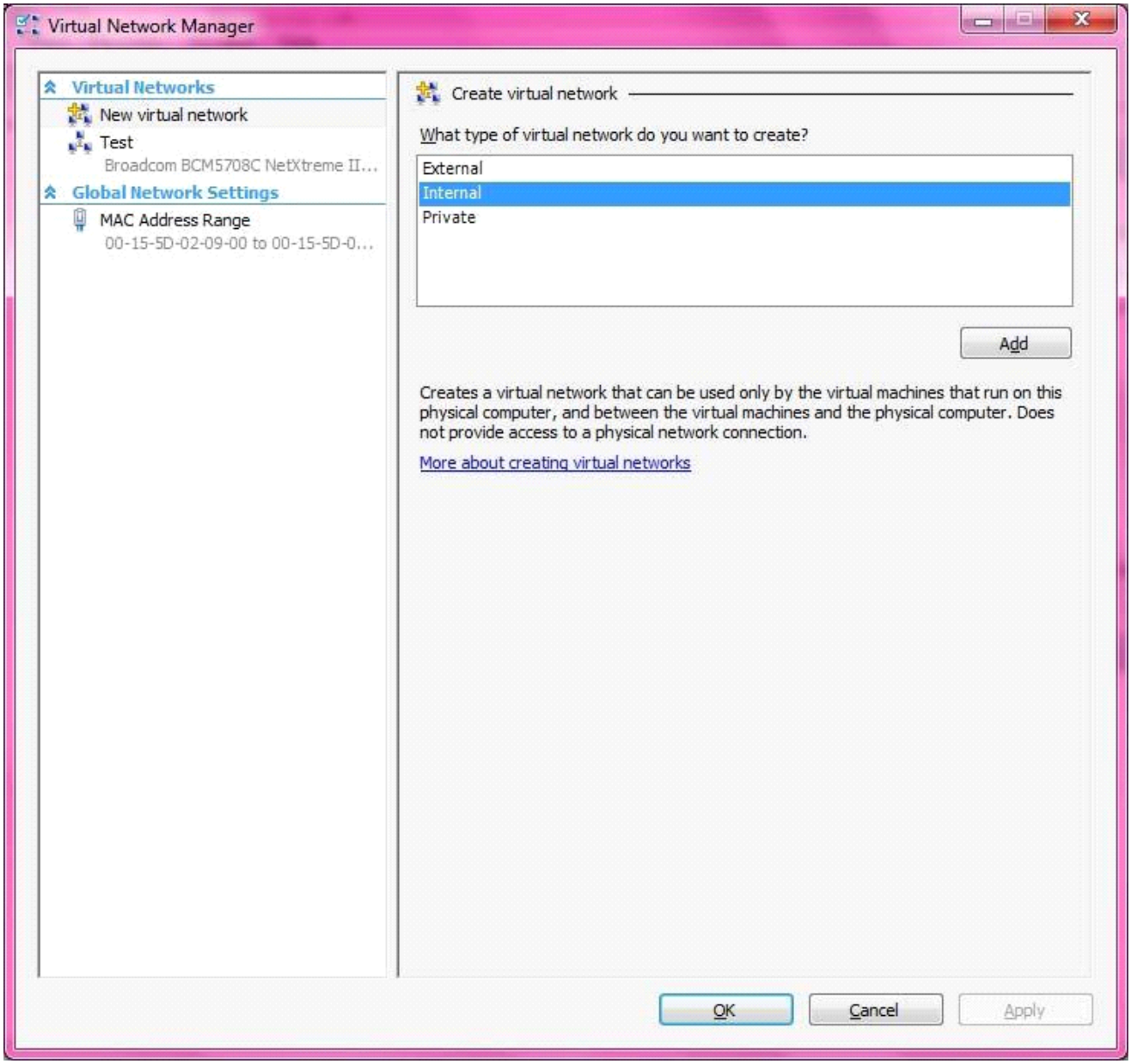
Question: 73

You have a server that runs Windows Server 2008 R2 and has the Hyper-V server role installed? You create a new virtual machine.
You need to configure the virtual machine to meet the following requirements:
Allow network communications between the virtual machine and the host system.
Prevent communications to other network servers.
What should you do first?

A. Install the Microsoft Loopback Adapter.
B. Create a new Virtual Network.
C. Enable Internet Connection Sharing (ICS).
D. Set the Connection to None for the network interface card.

Answer: B

Explanation:



Question: 74

Your company has a server named VS1 that runs Windows Server 2008 and Microsoft Hyper-V. VS1 hosts 10 virtual machines. You need to configure VS1 to shut down each virtual machine before the server shuts down. What should you do?

A. Create a shutdown script on each virtual machine.
B. Install Integration Services on each virtual machine.
C. Enable the Turn off the virtual machine option in the Automatic stop action properties on each virtual machine.
D. Enable the Shut down the guest operating system option in the Automatic stop action properties on each virtual machine.

Answer: D

Question: 75

You install the FTP role service on a server that runs Windows Server 2008 R2. Users receive an error message when they attempt to upload files to the FTP site. You need to allow authenticated users to upload files to the FTP site. What should you do?

A. Run the ftp Ca 192.168.1.200 command on the server that runs Windows Server 2008.
B. Run the appcmd unlock config command on the server that runs Windows Server 2008.
C. Configure Write permissions on the FTP site. Configure the NTFS permissions on the FTP destination folder for the Authenticated Users group to Allow- Modify.
D. Configure Write permissions on the FTP site. Configure the NTFS permissions on the FTP destination folder for the Authenticated Users group to Allow C Write attributes.

Answer: C

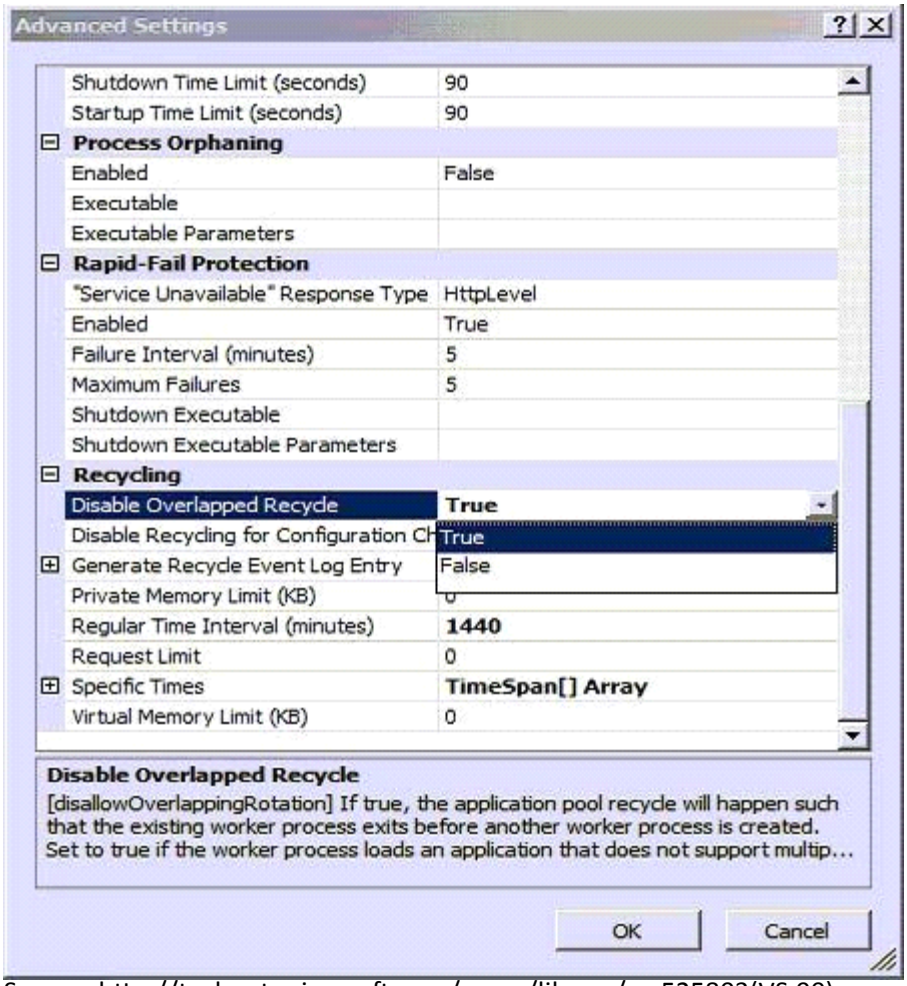
Question: 76

You have the Web Server (IIS) server role installed on a server that runs Windows Server 2008 R2. You create a Web site named contoso.com. You copy an application named WebContent to the server. You need to enable the WebContent application on the Web site. What should you do?

A. At the command prompt on the server, run the appcmd add site command.
B. At the command prompt on the server, run the appcmd add vdir command.
C. Select the Web site from the Internet Information Services (IIS) Manager console. Select Add Application.
D. Select the Web site from the Internet Information Services (IIS) Manager console. Select Add Virtual Directory.

Answer: C

Explanation:
Overlapped Recycling
In an overlapped recycling scenario, the process targeted for a recycle continues to process all remaining requests while a replacement worker process is created simultaneously. The new process is started before the old worker process stops, and requests are then directed to the new process. This design prevents delays in service, since the old process continues to accept requests until the new process has initialized successfully, and is instructed to shut down only after the new process is ready to handle requests. Considerations When Recycling Applications When applications are recycled, it is possible for session state to be lost. During an overlapped recycle, the occurrence of multi-instancing is also a possibility. Loss of session state: Many IIS applications depend on the ability to store state. IIS 6.0 can cause state to be lost if it automatically shuts down a worker process that has timed out due to idle processing, or if it restarts a worker process during recycling. Occurrence of multi-instancing: In multi-instancing, two or more instances of a process run simultaneously. Depending on how the application pool is configured, it is possible for multiple instances of a worker process to run, each possibly loading and running the same application code. The occurrence of an overlapped recycle is an example of multi-instancing, as is a Web garden in which two or more processes serve the application pool regardless of the recycling settings. If your application cannot run in a multi-instance environment, you must configure only one worker process for an application pool (which is the default value), and disable the overlapped recycling feature if application pool recycling is being used.



Source: http://technet.microsoft.com/en-us/library/ms525803(VS.90).aspx

Question: 77

Your company has a single Active Directory domain. You have a server named WDS1 that runs Windows Server 2008. You install the Windows Deployment Services (WDS) role on WDS1. You capture an image of a reference computer. You deploy the image to 30 client computers. The client computers have the same name. You need to ensure that each client computer receives a unique security identifier. What should you do?

A. Create an image group by using the WDS snap-in. Redeploy the image to the client computers.
B. Run the imagex /append "computername" command at the command prompt on the WDS1 server. Redeploy the image to the client computers.
C. Run the wdsutil /answerclients:all command at the command prompt on the WDS1 server. Redeploy the image to the client computers.
D. Run the wdsutil /set-server/prestageusingMAC: yes command at the command prompt on the WDS1 server. Redeploy the image to the client computers.

Answer: D

Question: 78

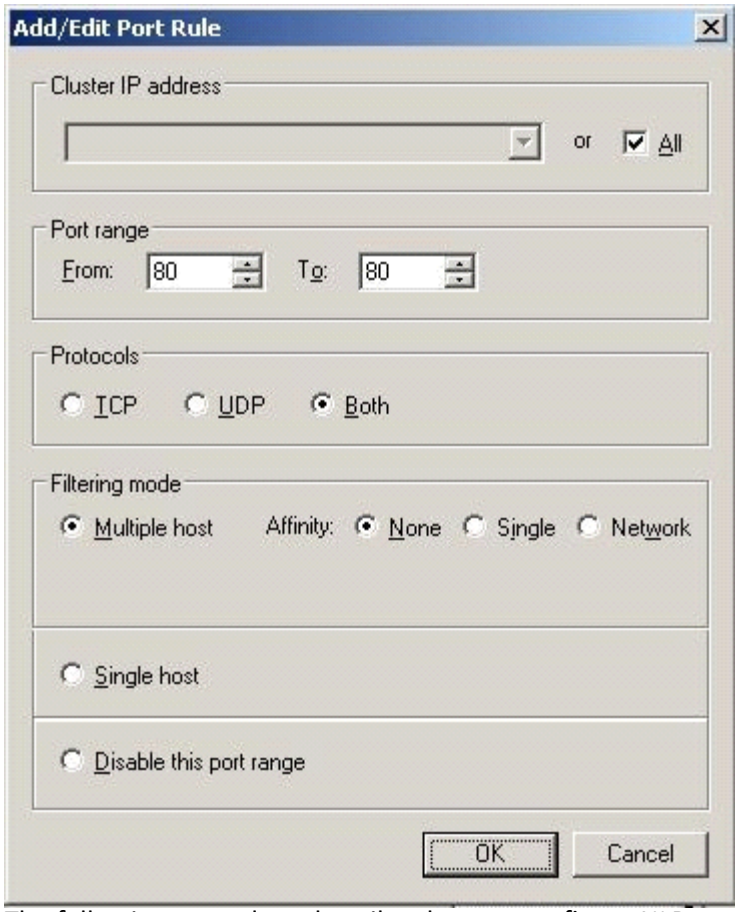
Your company named Contoso, Ltd. has a two-node Network Load Balancing cluster. The cluster is intended to provide high availability and load balancing for only the intranet Web site. The name of the cluster is web.contoso.com. You

discover that Contoso users can see the Network Load Balancing cluster in the network neighborhood and can connect to various services by using the web.contoso.com name. The web.contoso.com Network Load Balancing cluster is configured with only one port rule. You need to configure the web.contoso.com Network Load Balancing cluster to accept only HTTP traffic. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Log on to one of the cluster nodes and run the wlbs disable all command.
B. Open the Network Load Balancing Clusters console and delete the default port rules.
C. Open the Network Load Balancing Clusters console and create a new Allow rule for TCP port 80.
D. Open the Network Load Balancing Clusters console and change the default port rule to a disabled port range rule.

Answer: B, C

Explanation:



The following procedure describes how to configure NLB on the Web tier for a typical deployment. To configure NLB on the Web tier Open properties for the front-end adapter (for communicating with clients on the Internet). In Network Load Balancing Properties dialog box, on the Cluster Parameters tab, type the Primary IP address (the virtual IP address shared across all cluster members), Subnet Mask, and Full Internet name. In Network Load Balancing Properties dialog box, on the Host Parameters tab, type the Priority (Unique host ID), Dedicated IP address, and Subnet Mask In Network Load Balancing Properties dialog box, on the Port Rules tab, remove the default port rule covering ports 0 to 65535 by selecting the port rule, then clicking Remove. Create a port rule for HTTP using the information in the following table, and then click Add.
Source: http://technet.microsoft.com/en-us/library/ee784931(CS.20).aspx

Question: 79

You install the Web Server (IIS) role on and the SMTP Server feature on a server that runs Windows Server 2008. You need to configure the new SMTP server to forward mail to the mail server of the Internet Service Provider (ISP). What should you do?

A. Configure the smart host setting to use the local host.
B. Configure the smart host setting to use the mail server of the ISP.
C. Run the appcmd /delivery method:PickupDirectoryFromlis command.
D. Configure the SMTP delivery setting to Attempt direct delivery before sending to smart host.

Answer: B

Question: 80

You have a server that runs Windows Server 2008. The server has the Windows Server virtualization role service installed and has one virtual machine. The virtual machine runs Windows Server 2008. You plan to install a new application on the virtual machine. You need to ensure that you can restore the virtual machine to its original state in the event the application installation fails. What should you do?

A. Log on to the virtual host and enable the Remote Differential Compression Features.
B. Log on to the virtual host and enable the Windows Recovery Disk feature.
C. From Virtualization Management Console, create a snapshot.
D. From Virtualization Management Console, save the state of the virtual machine.

Answer: C

Question: 81

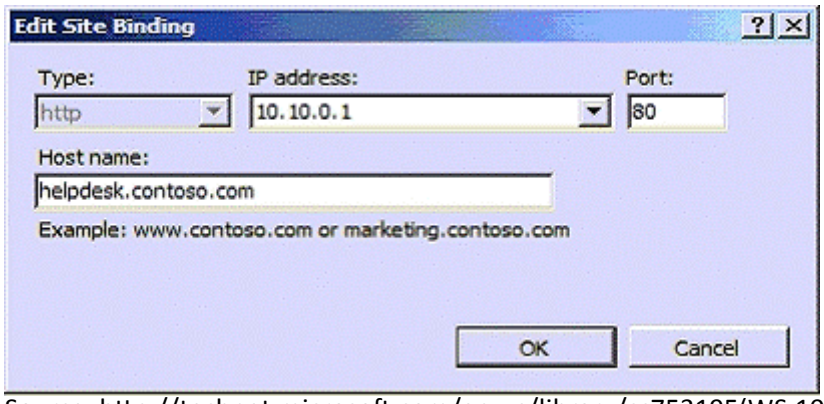
You install the Web Server (IIS) role on a server that runs Windows Server 2008 R2. Your company's default Web site has an IP address of 10.10.0.1. You add a Web site named HelpDesk. The HelpDesk Web site cannot be started. You need to configure the Helpdesk Web site so that it can be started. What should you do?

A. Run the iisreset /enable command on the server.
B. Configure the Helpdesk Web site to use a host header.
C. Run the appcmd add site /name: HelpDesk /id:2 /physicalPath: c:\HelpDesk /binding:http/*:80: helpdesk command on the server.
D. Run the set-location Cliteralpath "d:\HelpDesk_content" HelpDesk ID:2 location port:80 domain:helpdesk command in the Microsoft Windows PowerShell tool on the server.

Answer: B

Explanation:
Configure a Host Header for a Web Site (IIS 7)
Host headers (also known as domain names or host names) let you assign more than one site to a single IP address on a Web server. To configure a host header for a site
1. Open IIS Manager. For information about opening IIS Manager, see Open IIS Manager (IIS 7).
2. In the Connections pane, expand the Sites node in the tree, and then select the site for which you want to configure a host header.
3. In the Actions pane, click Bindings.
4. In the Site Bindings dialog box, select the binding for which you want to add a host header and then click Edit or click Add to add a new binding with a host header.

5. In the Host name box, type a host header for the site, such as www.contoso.com.
6. Click OK.
7. To add an additional host header, create a new binding with the same IP address and port, and the new host header. Repeat for each host header that you want to use this IP address and port.



Source: http://technet.microsoft.com/en-us/library/cc753195(WS.10).aspx

Question: 82

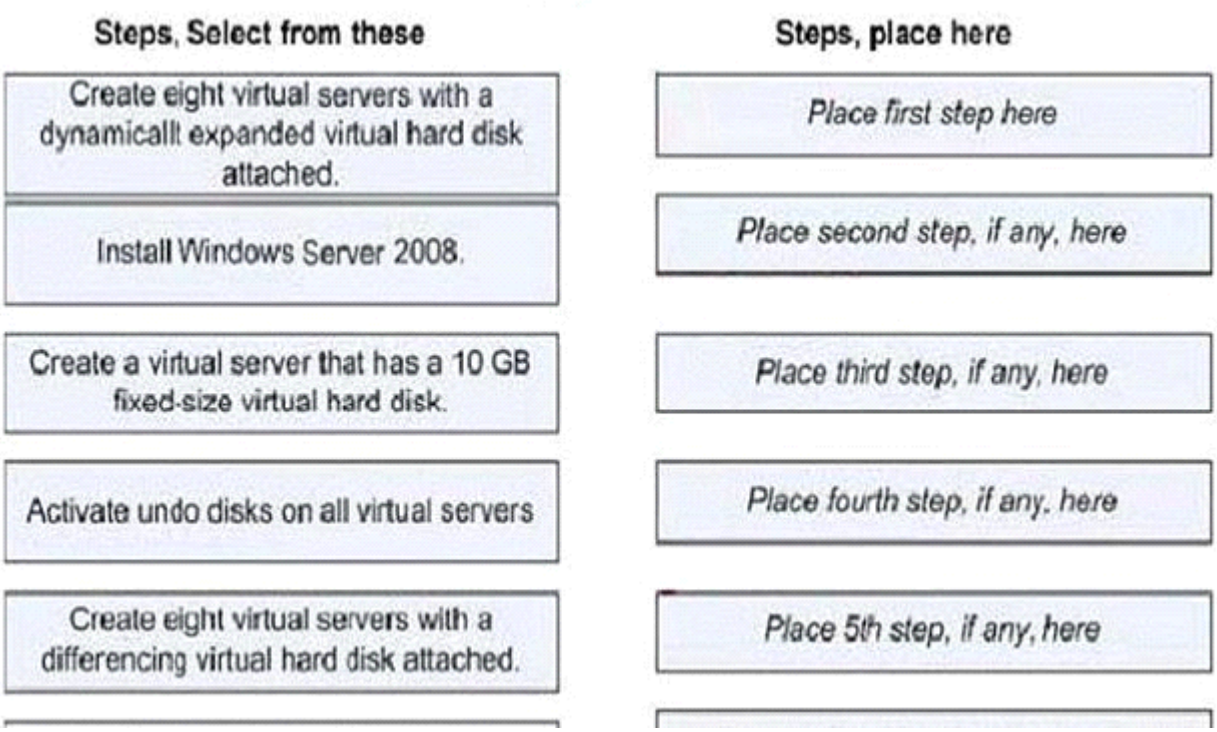
Your company named Contoso, Ltd. has a Web server named WEB1.
The Web server runs Windows Server 2008. The fully qualified domain name of WEB1 is web1.contoso.com. The public DNS server has an alias record named owa.contoso.com that maps to web1.contoso.com. Users access WEB1 from the Internet by using http://owa.contoso.com. The new company security policy states that the owa.contoso.com site must be available for Internet users only through secure HTTP (HTTPS) protocol. The security policy also states that users must not get security warnings when they connect to the site. You need to request a certificate from a public certification authority (CA). Which Common Name should you use?

A. Contoso, Ltd.
B. owa.contoso.com
C. WEB1
D. web1.contoso.com

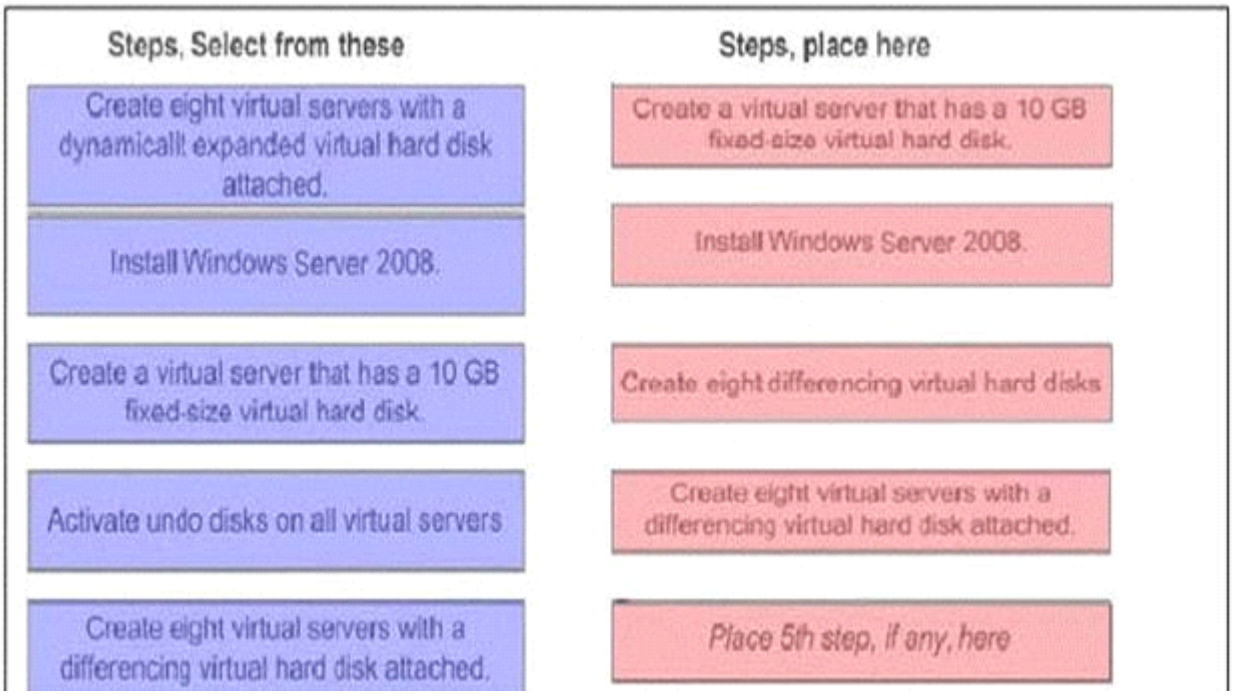
Answer: B

Question: 83

DRAG DROP
Your company has a server named VS1 that runs Windows Server 2008 R2 and Hyper-V. You want to create eight virtual servers that run Windows Server 2008 R2 and configure the virtual servers as an Active Directory forest for testing purposes. You discover that VS1 has only 30 GB of free hard disk space. You need to install the eight new virtual servers on VS1. What should you do? (To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.)



Answer:



Question: 84

You manage a server named Server2 that runs Windows Server 2008 R2. You install and test the Remote Desktop Services server role on Server2. You publish an application by using Remote Desktop Services. All users must connect to the Remote Desktop Services application by using the Remote Desktop Protocol. You install and configure the RD Gateway role service on Server2. You configure a default domain policy to enable the Enable Connection through RD Gateway setting. Users report that they cannot connect to the Remote Desktop Services application. You need to

ensure that users can access the Remote Desktop Services application on the intranet and from the Internet. What should you do?

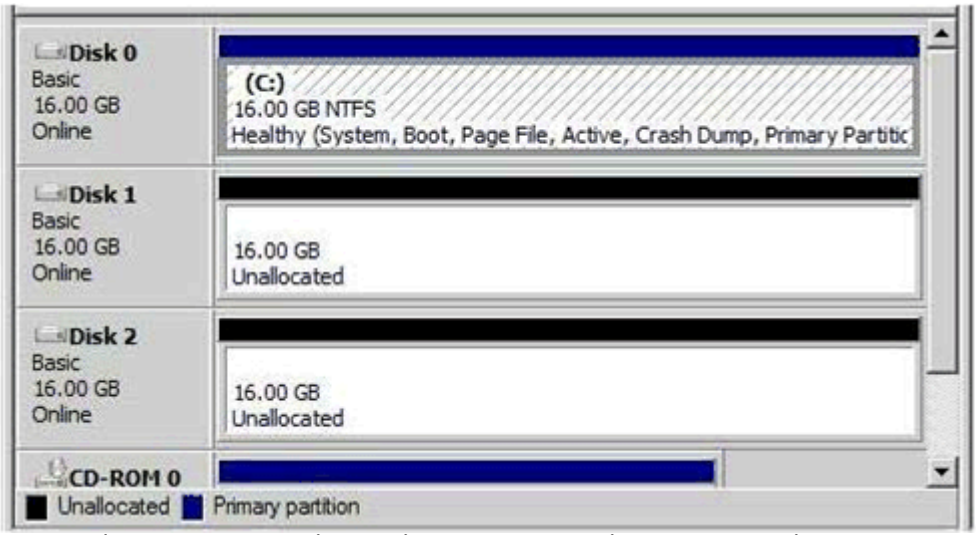
A. Configure the Enable Connection through RD Gateway Group Policy setting to Disabled.
B. Configure the Set RD Gateway server address Group Policy and configure the IP address of the RD Gateway server. Link the Group Policy object (GPO) to the domain.
C. Configure Server Authentication on the Remote Desktop Connection client to Always connect, even if server authentication fails for all users.
D. Enable the Set RD Gateway server authentication method Group Policy to the Ask for credential, use NTLM protocol setting. Link the Group Policy object (GPO) to the domain.

Answer: B

Explanation:
How to use the Group Policy Management Console (GPMC) to enable connections through RD Gateway. When this policy setting is enabled, when Remote Desktop Services clients cannot connect directly to an internal network resource (computer), the clients will attempt to connect to the computer through the RD Gateway server that is specified in the Set RD Gateway server address policy setting.
Source: http://technet.microsoft.com/en-us/library/cc726011.aspx

Question: 85

Your company has a single Active Directory domain. All the servers run Windows Server 2008 R2. You have a server named FS1 that has the File Services server role installed.
The disks are configured as shown in the following exhibit.



You need to create a new drive volume to support data striping with parity.
What should you do?

A. Add another disk. Create a New RAID-5 Volume.
B. Create a new Striped Volume by using Disk 1 and Disk 2.
C. Create a New Mirrored Volume by using Disk 1 and Disk 2.
D. Create a New Spanned Volume by using Disk 1 and Disk 2.

Answer: A

Question: 86

Your company has four regional offices. You install the Windows Deployment Services (WDS) role on the network. Your company creates three images for each office. There are a total of 12 images for the company. The images will be used as standard images for workstations. You deploy the images by using WDS. You need to ensure that each administrator can view only the images for his or her regional office. What should you do?

A. Create a global group for each regional office and place the computers in the appropriate global group.
B. Create an organizational unit (OU) for each regional office and place the computers in the appropriate OU.
C. Place all images into a single image group on the WDS server. Grant each administrator permissions to the image group.
D. Place each regional office into a separate image group on the WDS server. Grant each administrator permissions to his or her regional offices image group.

Answer: D

Explanation:
Image group: Each image group has a unique name and an ACL to specify users who are allowed to deploy OS images from the image group. An image group may contain multiple OS image containers. Source: http://msdn.microsoft.com/en-us/library/dd891274%28v=prot.10%29.aspx

Question: 87

Your company has an Active Directory domain. The company runs Remote Desktop Services. Standard users who connect to the Remote Desktop Session Host Server are in the TSUsers organizational unit (OU). Administrative users are in the TSAdmins OU. No other users connect to the Remote Desktop Session Host Server. You need to ensure that only members of OU1 can run the Remote Desktop Protocol files. What should you do?

A. Create a Group Policy object (GPO) that configures the Allow .rdp files from unknown publishers policy setting in the Remote Desktop Client Connection template to Disabled. Apply the GPO to the TSUsers OU.
B. Create a Group Policy object (GPO) that configures the Allow .rdp files from valid publishers and users default .rdp settings policy setting in the Remote Desktop Client Connection template to Disabled. Apply the GPO to the TSUsers OU.
C. Create a Group Policy object (GPO) that configures the Allow .rdp files from valid publishers and users default .rdp settings policy setting in the Remote Desktop Client Connection template to Enabled. Apply the GPO to the TSAdmins OU.
D. Create a Group Policy object (GPO) that configures the Specify SHA1 thumbprints of certificates representing trusted .rdp publishers policy setting in the Remote Desktop Client Connection template to Enabled. Apply the GPO to the TSAdmins OU.

Answer: C

Explanation:
To ensure that only members of the TermSerAdmin OU can run the Remote Desktop Protocol files, you need to enable the Allow .rdp files from valid publishers and users default .rdp settings policy setting in the Remote Desktop Client Connection template. This policy setting allows you to specify whether users can run Remote Desktop Protocol (.rdp) files from a publisher that signed the file with a valid certificate. A valid certificate is one issued by an authority recognized by the client, such as the issuers in the client's Third-Party Root Certification Authorities certificate store. This policy setting also controls whether the user can start an RDP session by using default .rdp settings (for example, when a user directly opens the Remote Desktop Connection [RDC] client without specifying an .rdp file). If you enable

this policy setting, users can run .rdp files that are signed with a valid certificate. Users can also start an RDP session with default .rdp settings by directly opening the RDC client. When a user starts an RDP session, the user is asked to confirm whether they want to connect. If you disable this policy setting, users cannot run .rdp files that are signed with a valid certificate. Additionally, users cannot start an RDP session by directly opening the RDC client and specifying the remote computer name. When a user tries to start an RDP session, the user receives a message that the publisher has been blocked Reference: Remote Desktop Connection Client
http://technet2.microsoft.com/windowsserver2008/en/library/76fb7e12-b823-429b-9887-05dc70d28d0c1033.mspx?mfr=true

Question: 88

You have installed the Web Server (IIS) role on a server with Windows Server 2008. Company uses SMTP for email. You need prevent unauthorized transmissions without disrupting valid email traffic.

A. Creata firewall role to block all outbound SMTP traffic.
B. Configure High alert items to be removed in Windows Defender.
C. Enable the TLS encryption option in the outbound security settings.
D. Add an SMTP relay restriction that limits access to authorized server on the network.

Answer: D

Question: 89

You have a w2k8 IIS server. Your company uses SMTP email. Now you want to prevent the sending of unauthorized email and restrict SMTP only to internal servers without affecting the current mail flow. What should you do?

A. Block all outbound email with a windows firewall rule
B. Disable the high alerts in windows defender
C. Enable tls-encryption on the outbound security
D. You add a SMTP relay restriction that allows SMTP-relaying only from the servers in your domain

Answer: D

Question: 90

Your network contains a server named Server1 that has Microsoft SharePoint Foundation 2010 installed. You configure the incoming email settings to use the SharePoint Directory Management service to create distribution groups and contacts in an organizational unit (OU) named OU1. You need to ensure that email distribution groups created from SharePoint are automatically created in OU1. What should you do?

A. From Central Administration, create a new trust relationship.
B. From Central Administration, modify the Directory Management Service Approval List.
C. From Active Directory Users and Computers, delegate permissions to the SharePoint 2010 Timer service account in OU1.
D. From Active Directory Users and Computers, delegate permissions to the SharePoint Central Administration v4 application pool identity in OU1.

Answer: D

Explanation:
Configure Active Directory
Incoming email uses the Microsoft SharePoint Directory Management Service to connect SharePoint sites to the directory services used by your organization. If you enable the Microsoft SharePoint Directory Management Service, users can create and manage distribution groups from SharePoint sites. SharePoint lists that use email can then be found in directory services, such as the Address Book. You must also select which distribution group requests from SharePoint lists require approval. The Microsoft SharePoint Directory Management Service can be installed on a server in the farm, or you can use a remote Microsoft SharePoint Directory Management Service. To use the Microsoft SharePoint Directory Management Service on a farm or server, you must configure the Central Administration application pool identity account to have the Create, delete, and manage user accounts right to the container that you specify in Active Directory. The preferred way to do this is by delegating the right to the Central Administration application pool identity account. An Active Directory administrator must set up the organizational unit (OU) and delegate the Create, delete, and manage user accounts right to the container. The advantage of using the Microsoft SharePoint Directory Management Service on a remote farm is that you do not have to delegate rights to the organizational unit for multiple farm service accounts. If the application pool account for Central Administration is different from the application pool account for the Web application of the list or site that is enabled for email, you must use the application pool account for the Web application when completing the following procedures. You must then delegate additional rights to the Central Administration application pool account. The following procedures are performed on a domain controller that runs Microsoft Windows Server 2003 SP1 (with DNS Manager) and Microsoft Exchange Server 2003 SP1. In some deployments, these applications might run on multiple servers in the same domain. Important: Membership in the Domain Administrators group or delegated authority for domain administration is required to complete this procedure.
Create an organizational unit in Active Directory
1. Click Start, point to Control Panel, point to Administrative Tools, and then click Active Directory Users and Computers.
2. In Active Directory Users and Computers, right-click the folder for the second-level domain that contains your server farm, point to New, and then click Organizational Unit.
3. Type the name of the organizational unit, and then click OK.
After creating the organization unit, we recommend that you delegate the Create, delete, and manage user accounts right to the container.
Important: Membership in the Domain Administrators group or the Enterprise Administrators group in Active Directory, or delegated authority for administration, is required to complete this procedure.
Delegate right to the application pool account
1. In Active Directory Users and Computers, find the organizational unit that you just created.
2. Right-click the organizational unit, and then click Delegate control.
3. On the Welcome page of the Delegation of Control Wizard, click Next.
4. On the Users and Groups page, click Add, and then type the name of the application pool identity account that the Web application uses.
5. In the Select Users, Computers, and Groups dialog box, click OK.
6. On the Users or Groups page of the Delegation of Control Wizard, click Next.
7. On the Tasks to Delegate page of the Delegation of Control Wizard, select the Create, delete, and manage user accounts check box, and then click Next.
8. On the last page of the Delegation of Control Wizard, click Finish to exit the wizard.
If you must add permissions for the application pool identity account directly, complete the following procedure.
Important: Membership in the Account Operators group, Domain Administrators group, or the Enterprise Administrators group in Active Directory, or delegated authority for administration, is required to complete this procedure.
Add permissions for the application pool account
1. In Active Directory Users and Computers, click the View menu, and then click Advanced Features.
2. Right-click the organizational unit that you just created, and then click Properties.

3. In the Properties dialog box, click the Security tab, and then click Advanced.
4. Click Add, and then type the name of the application pool identity account for the Web application.
5. Click OK.
6. In the Permission Entries section, double-click the application pool identity account.
7. In the Permissions section, under Allow, select the Modify permissions check box.
8. Click OK to close the Permissions dialog box.
9. Click OK to close the Properties dialog box.
10. Click OK to close the Active Directory Users and Computers plug-in.

If you decide instead to use the remote Microsoft SharePoint Directory Management Service, you must know the URL for the Web service. This URL is typically in the following format: http:// server:adminport/_vti_bin/SharePointEmailWS.asmx.

Source: http://technet.microsoft.com/en-us/library/cc262947.aspx

Question: 91

Your network contains a server named Server1 that has Microsoft SharePoint Foundation 2010 installed. You install the Office Web Apps Feature on Server1. You need to ensure that users can use their Web browsers to open the Microsoft Office Word documents stored in the SharePoint site collections. What should you do first?

A. Activate the Office Web Apps Feature.
B. Install the Office File Converter Pack on Server1.
C. Install Microsoft Office Professional 2010 on Server1.
D. Create a new Web application named Office Web Apps.

Answer: A

Explanation:

Understanding Office Web Apps (Installed on SharePoint 2010 Products)

Microsoft Office Web Apps is the online companion to Office Word, Excel, PowerPoint and OneNote applications that enables users regardless of their location to access documents and edit documents. Users can view, share, and work on documents with others online across personal computers, mobile phones, and the Web. Office Web Apps is available to users through Windows Live and to business customers with Microsoft Office 2010 volume licensing and document management solutions based on Microsoft SharePoint 2010 Products.

Integration with SharePoint 2010 Products

Office Web Apps is tightly integrated with SharePoint 2010 Products. When you install Office Web Apps, the Office Web Apps Services are added to the list of SharePoint Services and the Office Web Apps Feature is added to the available SharePoint Features. Office Web Apps services include the Word Viewing Service, PowerPoint Service, and Excel Calculation Services that are created and run within the context of SharePoint Services. The Office Web Apps Feature and services integrate with SharePoint's robust enterprise content management capabilities to provide users the ability to access and work on your organization's documents from anywhere using a Web browser.

Understanding the Office Web Apps user experience

Viewing and editing Office documents

Office Web Apps gives users a browser-based viewing and editing experience by providing a representation of an Office document in the browser. When a user clicks on a document stored in a SharePoint document library, the document opens directly in the browser. The document appears in the browser similar to how it appears in the Office client application. The Web app also provides many of the same editing features as an Office client application. Office Web Apps provides this representation of an Office Word document, PowerPoint presentation, Excel workbook, or OneNote notebook using native browser objects such as HTML, JavaScript, and images. Each document type is handled differently depending on the Office Web Apps services started and whether the Office Web Apps Feature is activated. A document in the Word Web App, PowerPoint Web App, or Excel Web App can be edited in the browser or can be opened for editing in the associated Office client application. If while viewing or working in a Web app a user

clicks the Edit in Browser button on the Home tab of the toolbar, the user can perform light editing tasks in the browser. A notebook in the OneNote Web App can be edited in the browser natively without having to click the Edit in Browser button or it can be opened for editing in the OneNote client application by clicking Open in OneNote.
If while in a Web app a user clicks the Open in Word, Open in PowerPoint, Open in Excel, or Open in OneNote button on the toolbar, the document will open in the associated Office client application if it is installed on the client computer. Improving the user experience with Silverlight Silverlight is a free plugin that can provide richer Web experiences for many browsers. The Silverlight plugin is not required to be installed on the client browser to use Office Web Apps. However, having the Silverlight plugin installed on the browser can provide the following benefits: When using the Word Web App on browsers with the Silverlight plugin installed, users can experience faster page loading, improved text fidelity at full zoom, ClearType tuner settings support, and improved accuracy in location of search string instances when using the find on this page feature. When using the PowerPoint Web App on browsers with the Silverlight plugin installed, users can experience faster page loading, animations will appear smoother than without, and presentation slides will scale with the\ browser window size. Having Silverlight installed on the client browser does not provide any additional benefits in Excel Web App and
OneNote Web App.
Source: http://technet.microsoft.com/en-us/library/ff431685.aspx

Question: 92

Your network contains a server farm that has Microsoft SharePoint Foundation 2010 installed. You need to ensure that users can receive SMS alerts. What should you do?

A. Configure the User Alerts settings.
B. Configure the Send To Connections.
C. Modify the Outgoing Email Settings.
D. Modify the Mobile Accounts Settings.

Answer: D

Explanation:
Configure a mobile account (SharePoint Foundation 2010) This article discusses how to configure and manage a mobile account for Microsoft SharePoint Foundation 2010 to enable users to subscribe to alerts that are sent by using Short Message Service (SMS). The alerts are sent to users' mobile phones when changes are made to a SharePoint list or item. The mobile alert feature resembles a feature that already exists in SharePoint Foundation 2010 that enables outgoing email alerts. However, instead of receiving alerts via email when changes are made in a SharePoint list or item, users receive the alerts on their mobile phones. For more information about email alerts, see Configure outgoing email (SharePoint Foundation 2010). A SharePoint site is usually located on an intranet. As a result, access to the SharePoint site can be difficult when users are away from the office — for example, when they are traveling or attending a business dinner. The mobile alert feature enables users to react quickly when they receive an SMS alert that an item in a SharePoint list has changed.
Configure a mobile account
You can configure a mobile account for a server farm or for a specific Web application, either by using Central Administration or Windows PowerShell.
Note: If you cannot configure a mobile account, you may have the wrong certificate file. In that case, contact your service provider. If you cannot configure a mobile account, you may have the wrong certificate file. In that case, contact your service provider.
To configure or edit a mobile account for a server farm by using Central Administration
1. Verify that you have the following administrative credentials:
To configure a mobile account for a server farm, you must be a member of the Farm Administrators group on the computer that is running the SharePoint Central Administration Web site.
2. On the Central Administration Home page, click System Settings.

3. On the System Settings page, in the Email and Text Messages (SMS) section, click Configure mobile account.
4. On the Mobile Account Settings page, in the Text Message (SMS) Service Settings section, click the Microsoft Office Online link to access a list of service providers.
5. On the Find an Office 2010 Mobile Service Provider page, in the Choose your wireless service provider's country/region list, select the country or region in which your wireless service provider is located.
6. On the Find an Office 2010 Mobile Service Provider page, in the Choose your current wireless service provider list, select the wireless service provider that you want to use. After you make this selection, you are directed to the Web site of the service provider that you selected. On the Web site, you apply for the SMS service. When you receive the required information from the service provider, return to the Mobile Accounts Settings page.
7. In the The URL of Text Message (SMS) Service box, type the URL of the SMS service.
Note: Ensure that the service URL you enter is an HTTPS URL.
8. In the User Name box and Password box, type the user name and password that you received from the SMS service provider.
9. To confirm that the URL and user credentials are correct, click Test Service.
10. Click OK.
Source: http://technet.microsoft.com/en-us/library/ee428292.aspx

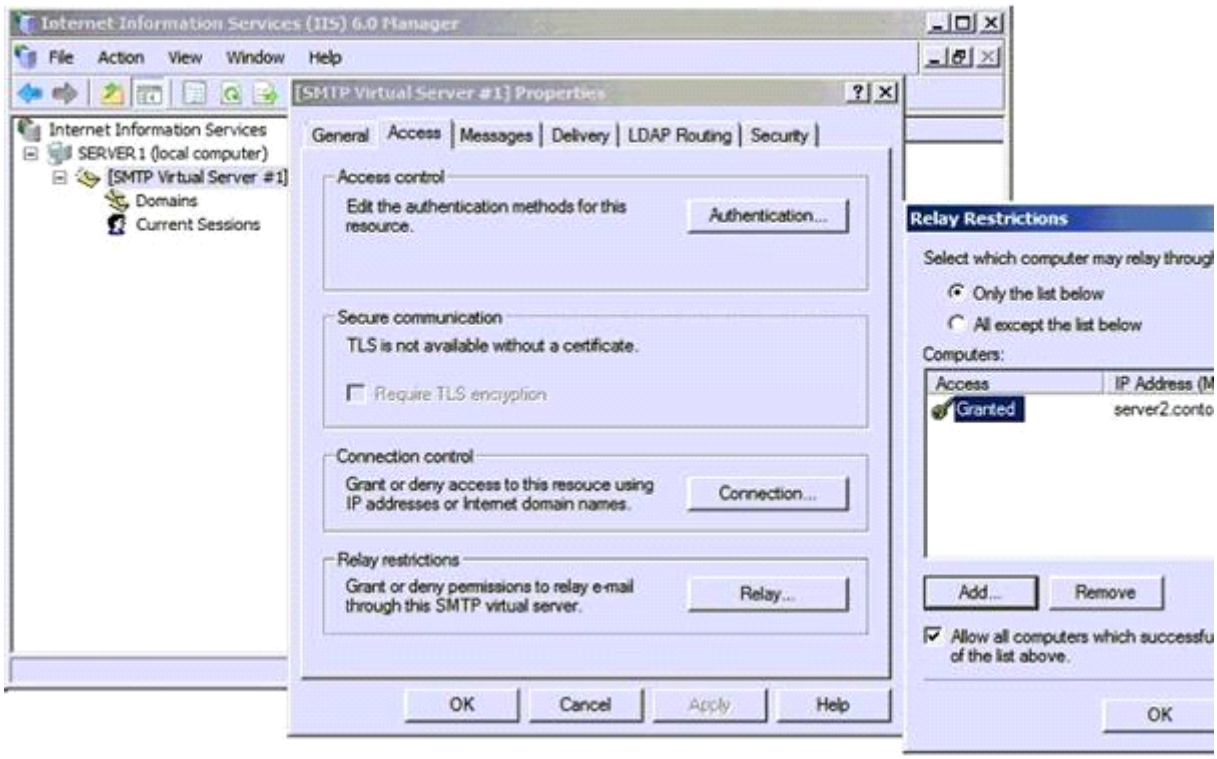
Question: 93

Your network contains two servers named Server1 and Server2 that run Windows Server 2008 R2. Server1 is an SMTP server. Server2 has Microsoft SharePoint Foundation 2010 installed. On Server2, you configure Server1 as an outbound email server. You discover that users never receive email alerts and invitations. You need to ensure that users receive email alerts and invitations. What should you do?

A. On Server1, modify the relay restrictions.
B. On Server1, modify the connection control settings.
C. On Server2, create a Send To Connection.
D. On Server2, modify the Mobile Account Settings.

Answer: A

Explanation:
To change the SMTP Virtual Server Relay Restrictions, one needs to use the Internet Information Servers (IIS) 6.0 Manager. This is an IIS Role Service that needs to be installed (IIS 6 Management Console)



Question: 94

Your network contains a server farm that has Microsoft SharePoint Foundation 2010 installed. The farm contains two Web applications named WebApp1 and WebApp2. You need to ensure that WebApp1 is enabled for outgoing email. What should you configure on WebApp1?

A. the General settings
B. the Manage Features
C. the Service Connections settings
D. the User Policy

Answer: A

Section: SharePoint
Explanation:
To configure outgoing email for a specific Web application by using Central Administration Verify that you have the following administrative credentials: You must be a member of the Farm Administrators group on the computer that is running the SharePoint Central Administration Web site. In Central Administration, in the Application Management section, click Manage web applications. On the Web Applications Management page, select a Web application, and then in the General Settings group on the Ribbon, click Outgoing Email. On the Web Application Outgoing Email Settings page, in the Mail Settings section, type the SMTP server name for outgoing email (for example, mail.fabrikam.com) in the Outbound SMTP server box. In the From address box, type the email address (for example, the site administrator alias) as you want it to be displayed to email recipients. In the Reply-to address box, type the email address (for example, a help desk alias) to which you want email recipients to reply. In the Character set list, click the character set that is appropriate for your language. Click OK.

Question: 95

Your network contains a server that has Microsoft SharePoint Foundation 2010 installed. You need to configure the incoming e-mail settings to use the Automatic settings mode. What should you do first?

A. Configure the outgoing email settings.
B. Configure the Message Queuing feature.
C. Install the SMTP Server feature.
D. Install the Message Queuing Triggers feature.

Answer: C

Section: SharePoint
Explanation:
When incoming email is enabled, SharePoint sites can receive and store email messages and attachments in lists and libraries. This article describes two scenarios, one basic and one advanced. The basic scenario applies to a single-server farm environment and is recommended if you want to use default settings, whereas the advanced scenario applies to a single-server farm or a multiple-server farm and contains several advanced options from which to choose.
Install and configure the SMTP service
Incoming email for SharePoint Foundation 2010 uses the SMTP service. You can use the SMTP service in one of two ways. You can install the SMTP service on one or more servers in the farm, or administrators can provide an email drop folder for email that is forwarded from the service on another server.
Install the SMTP service
If you are not using a drop folder for email, the SMTP service must be installed on every front-end Web server in the farm that you want to configure for incoming email. To install the SMTP service, use the Add Features Wizard in Server Manager. After the procedure is complete, a default SMTP configuration has been created. You can customize this default SMTP configuration to meet the requirements of your environment.
To install the SMTP service
1. Verify that you have the following administrative credentials:
- You must be a member of the Administrators group on the local computer.
2. Click Start, point to Administrative Tools, and then click Server Manager.
3. In Server Manager, click Features.
4. In Features Summary, click Add Features to open the Add Features Wizard.
5. On the Select Features page, select SMTP Server.
6. In the Add Features Wizard dialog box, click Add Required Features, and then click Next.
7. On the Confirm Installation Selections page, click Install.
8. On the Installation Results page, ensure that the installation finished successfully, and then click Close.
Source: http://technet.microsoft.com/en-us/library/cc287879.aspx

Question: 96

Your network contains a server named Server1 that has Microsoft SharePoint Foundation 2010 installed.
Server1 contains a Web application named WebApp1.
You activate the Office Web Apps Feature on WebApp1.
When users open Microsoft Office Word documents from WebApp1, the documents open in Word. You need to ensure that when users open Word documents from WebApp1, the documents open in a Web browser. What should you do?

A. Deactivate the OpenInClient feature.
B. Run the Set-SPWebApplication cmdlet.
C. Restart the SharePoint 2010 User Code Host service.
D. Recycle the SharePoint Web Services Root application pool.

Answer: A

Explanation:
Configure the default open behavior for documents
In SharePoint, you can configure whether browser-enabled documents are opened in a client application or in the browser. By default, when Office Web Apps is installed, Office documents will open in the browser. You can override this setting using the SharePoint OpenInClient feature. The OpenInClient feature can be configured in Central Administration or by using the SPFeature cmdlet in Windows PowerShell. How documents open in SharePoint varies depending on whether the OpenInClient feature is present, and either enabled or disabled: If the OpenInClient feature is not present and Office Web Apps is not installed, documents will open in the client application (SharePoint default). If the OpenInClient feature is not present, Office Web Apps is installed and Office Web Apps service applications are activated, documents will open in the browser (Office Web Apps default). If the OpenInClient Feature is present and enabled, and Office Web Apps service applications are activated, documents will open in the client application.
If the OpenInClient Feature is present and disabled, and Office Web Apps service applications are activated, documents in will open in the browser.
Source: http://technet.microsoft.com/en-us/library/ee837425.aspx

Question: 97

You install the Windows Deployment Services (WDS) role on a server that runs Windows Server 2008 R2. When you attempt to upload spanned image files to the WDS server, you receive an error message. You need to ensure that the image files can be uploaded. What should you do?

A. Grant the Authenticated Users group Full Control on the \REMINST directory.
B. Run the wdsutil /Convert command at the command prompt on the WDS server.
C. Run the imagex /Export command at the command prompt to export *.swm files to one destination *.wim on the WDS server.
D. Run the wdsutil /add-image /imagefile:\\server\share\sources\install.wim /image type:install command for each component file individually at the command prompt on the WDS server.

Answer: C

Explanation:
Known issues with creating images
You cannot add split .wim (.swm) files to your Windows Deployment Services server. Instead, you must combine the split images into a single .wim file. Source: http://download.microsoft.com/download/b/b%2F5/bb50037f-e4ae-40d1-a898-7cdfcf0ee9d8/ WS08_STEP_BY_STEP_GUIDE/Step-by StepGuideForWindowsDeploymentServicesInWindowsServer2008_En.doc One can combine multiple .swm files to an .wim file with imagex.exe: imagex /export src_file src_numbersrc_name dest_file dest_name {/boot | /check | /compress [type] | /ref [splitwim.swm] /temp| /logfile filename.log} Exports a copy of the specified .wim file to another .wim file. The source and destination files must use the same compression type. You can also optimize an image by exporting to a new image file. When you modify an image, ImageX stores additional resource files that increase the overall size of the image. Exporting the image will remove unnecessary resource files.
src_file Specifies the file path of the .wim file that contains the image to be copied.
src_number Specifies the number of the specific volume within the .wim file.
src_name Specifies the name that identifies the image in the source .wim file.
dest_file Specifies the file path of the .wim file that will receive the image copy.
dest_name Specifies the unique name for the image in the destination .wim file.
/ref splitwim.swm

Enables the reference of split .wim files (SWMs). splitwim.swm is the name and location of additional split files. Wildcards are accepted.
Source: http://technet.microsoft.com/en-us/library/dd799302%28WS.10%29.aspx
Image Merge
Merge the previously splitted image file back into a single image file.
imagex /ref c:\data\splitmerge\output2\splitmerge*.swm /check /export c:\data \splitmerge\output2\splitmerge.swm 1 c:\data\splitmerge\output3\splitmerge.wim "splitmerge" /COMPRESS maximum
Source: http://www.verboon.info/index.php/2009/10/splitting-and-merging-image-files-with-imagex/
* I've changes the answer from wdsutil /Export to imagex /Export because I couldn't verify the awnser in the dump.*

Because wdsutil does not have an /Export parameter:

Command	Description
/add	Adds objects or prestages computers.
/approve-AutoAddDevices	Approves computers that are pending administrator approval.
/convert-RiprepImage	Converts an existing Remote Installation Preparation (RIPrep) image to a Windows Image (.wim) file.
/copy-DriverGroup	Copies an image or a driver group.
/delete-AutoAddDevices	Deletes computers that are in the Auto-Add database (which stores information about the computers on the server).
/disable	Disables all services for Windows Deployment Services.
/disconnect-Client	Disconnects a client from a multicast transmission or namespace.
/enable	Enables all services for Windows Deployment Services.
/export-Image	Exports an image from the image WDS store to a .wim file.
/get	Retrieves properties and attributes about the specified object.
/initialize-Server	Configures a Windows Deployment Services server for initial use.
/new	Creates new capture and discover images as well as multicast transmissions and namespaces.
/progress	Displays the progress status while a command is being executed.
/reject-AutoAddDevices	Rejects computers that are pending administrator approval.
/remove	Removes objects.
/replace-Image	Replaces a boot or installation image with a new version of that image.
/set	Sets properties and attributes on the specified object.
/start	Starts all services on the Windows Deployment Services server, including multicast transmissions, namespaces, and the Transport Server.
/stop	Stops all services on the Windows Deployment Services server.
/uninitialize-Server	Reverts changes made during server initialization.
/update-ServerFiles	Updates server files on the RemoteInstall share.
/verbose	Displays verbose output for the specified command.

Source: http://technet.microsoft.com/en-us/library/cc771206%28WS.10%29.aspx

Question: 98

Your company has a single Active Directory domain named contoso.com. All servers in the domain run Windows Server 2008 R2. The DNS Server server role is installed on two domain controllers named DC1 and DC2. Both DNS servers host Active Directory-integrated zones that are configured to allow the most secure updates only. DC1 has Key Management Service (KMS) installed and activated. You discover that the service locator records from the contoso.com zone hosted on DC1 and DC2 are missing. You need to force registration of the KMS service locator records in the contoso.com zone. What should you do?

A. Configure the contoso.com zone to accept non-secure updates.
B. On DC1 at the command prompt, run the slmgr.vbs rearm script.
C. On DC1 at the command prompt, run the net stop slsvc command, and then run the net start slsvc command.
D. On DC2 at the command prompt, run the net stop netlogon command, and then run the net start netlogon command.

Answer: C

Question: 99

Your company has a single Active Directory domain named contoso.com. The domain has two domain controllers and 60 member servers. All servers run Windows Server 2008 R2. One of the domain controllers has Key Management Service (KMS) installed and activated. All servers use KMS auto-discovery to find the KMS server. You need to change the port used by KMS from its default port to port 12200. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Restart the slsvc service on the KMS server.
B. Restart the DNS Server service on the KMS server.
C. On the KMS server at the command prompt, run the slmgr.vbs skms KMSServer: 12200 command.
D. On the client computers at the command prompt, run the slmgr.vbs skms KMSServer: 12200 command.

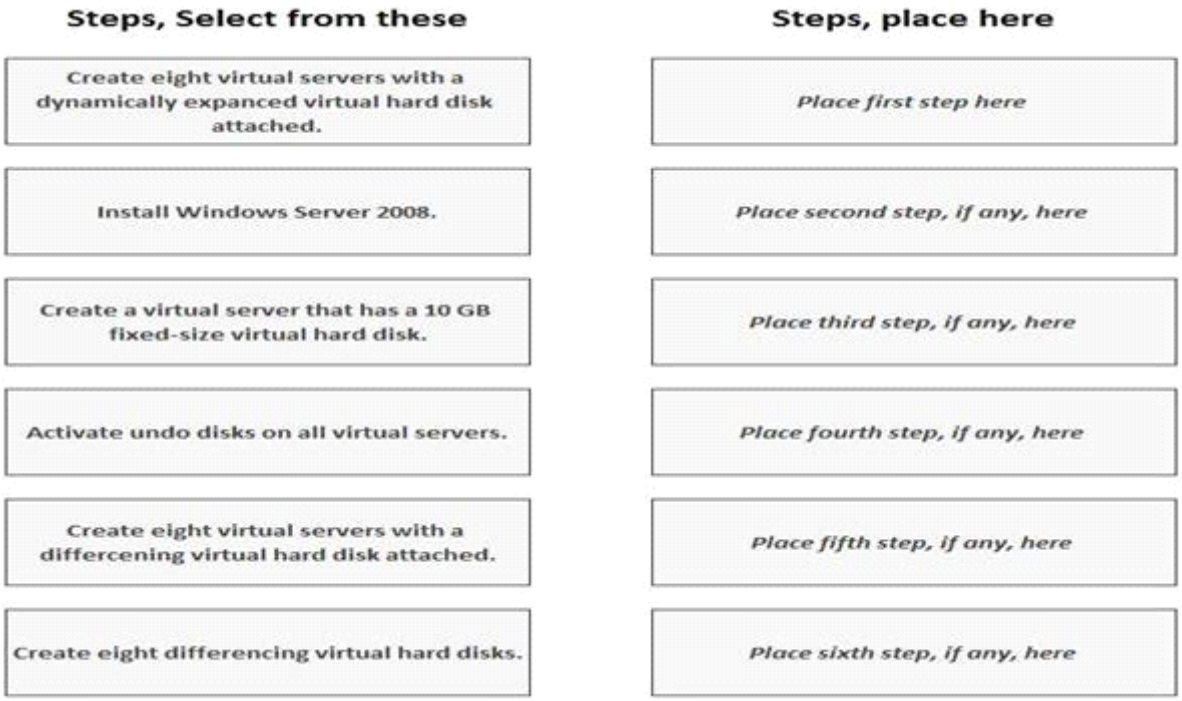
Answer: A, C

Explanation:
To change the port of the KMS server:
To set the TCP communications port on a KMS host. Replace PortNumber with the TCP port number to use. The default setting is 1688.
slmgr.vbs /sprt PortNumber
Source: http://technet.microsoft.com/en-us/library/ff793407.aspx
Restart slsvc service: A KMS host will automatically update its SRV entries if the software licensing service (slsvc.exe) detects that the computer name or TCP port has changed during service startup. It will also update them once each day, in order to ensure that they are not automatically removed (scavenged) by the DNS system.
Source: http://download.microsoft.com/download/c/3/8/c3815ed7-aee7-4435-802b-8e855d549154/VolumeActivation2.0Step-By-StepGuide.doc Force the KMS client to update the portnumber:
If configuring KMS clients to use auto-discovery, they automatically choose another KMS host if the original KMS host does not respond to renewal requests. If not using auto-discovery, update the KMS client computers that were assigned to the failed KMS host by running Slmgr.vbs /skms. To avoid this scenario, configure KMS clients to use auto-discovery. For more information, see the Volume Activation Deployment Guide.
Source: http://technet.microsoft.com/en-us/library/ff793439.aspx
OR
Configuring KMS Hosts (Server)
Sets the TCP communications port on a KMS host. Replace PortNumber with the TCP port number to use. The default setting is 1688.
Slmgr.vbs /sprt PortNumber
The Software Licensing Service must be restarted for any changes to take effect. To restart the Software Licensing Service, use the Microsoft Management Console (MMC) Services snap-in, or run the following command at an elevated command prompt:
net stop sppsvc && net start sppsvc
Configuring KMS Clients
This section describes concepts for installing and configuring computers as KMS clients. By default, Volume Licensing editions of Windows Vista, Windows 7 , Windows Server 2008, and Windows Server 2008 R2 are KMS clients. If the computers the organization wants to activate using KMS are using any of these operating systems and the network allows DNS auto-discovery, no further configuration is needed. If a KMS client is configured to search for a KMS host using DNS but does not receive SRV records from DNS, Windows 7 and Windows Server 2008 R2 log the error in the event log.
Manually Specifying a KMS Host
You can manually assign a KMS host to KMS clients by using KMS host caching. Manually assigning a KMS host disables

auto-discovery of KMS on the KMS client. Manually assign a KMS host to a KMS client by running:
slmgr.vbs /skms <value>:<port>
where value is either the KMS_FQDN, IPv4Address, or NetbiosName of the KMS host and port is the TCP port on the KMS host.
Source: http://technet.microsoft.com/en-us/library/ff793409.aspx
"You must restart the SLSVC service (Vista/2008) or SPPSVC(Win7/R2)"
Source: http://blogs.technet.com/b/askcore/archive/2009/03/09/kms-error-0xc004c008-activating-client.aspx

Question: 100

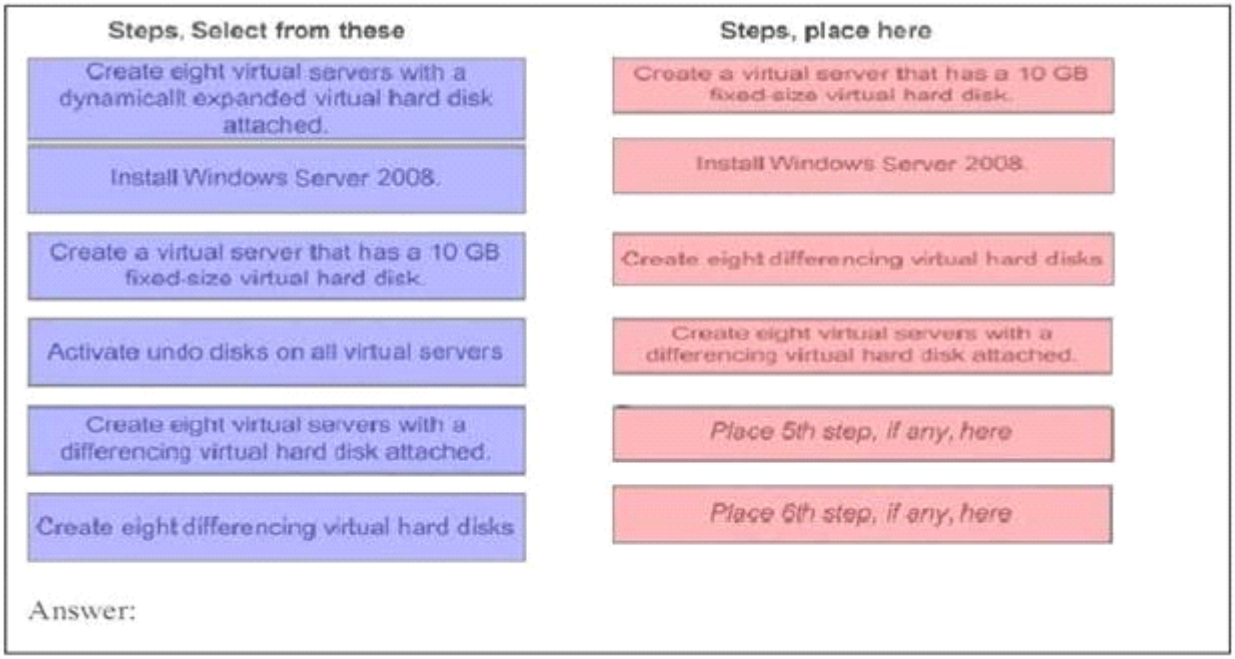
DRAG DROP
Your company has a server named VS1 that runs Windows Server 2008 R2 and Hyper-V. You want to create eight virtual servers that run Windows Server 2008 R2 and configure the virtual servers as an Active Directory forest for testing purposes. You discover that VS1 has only 30 GB of free hard disk space. You need to install the eight new virtual servers on VS1. What should you do? (To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.)
Answer Area



Answer:

Steps, Select from these	Steps, place here
Create eight virtual servers with a dynamically expanced virtual hard disk attached.	Create a virtual server that has a 10 GB fixed-size virtual hard disk.
	Install Windows Server 2008.
	Create eight differencing virtual hard disks.
Activate undo disks on all virtual servers.	Create eight virtual servers with a differcening virtual hard disk attached.
	Place fifth step, if any, here
	Place sixth step, if any, here

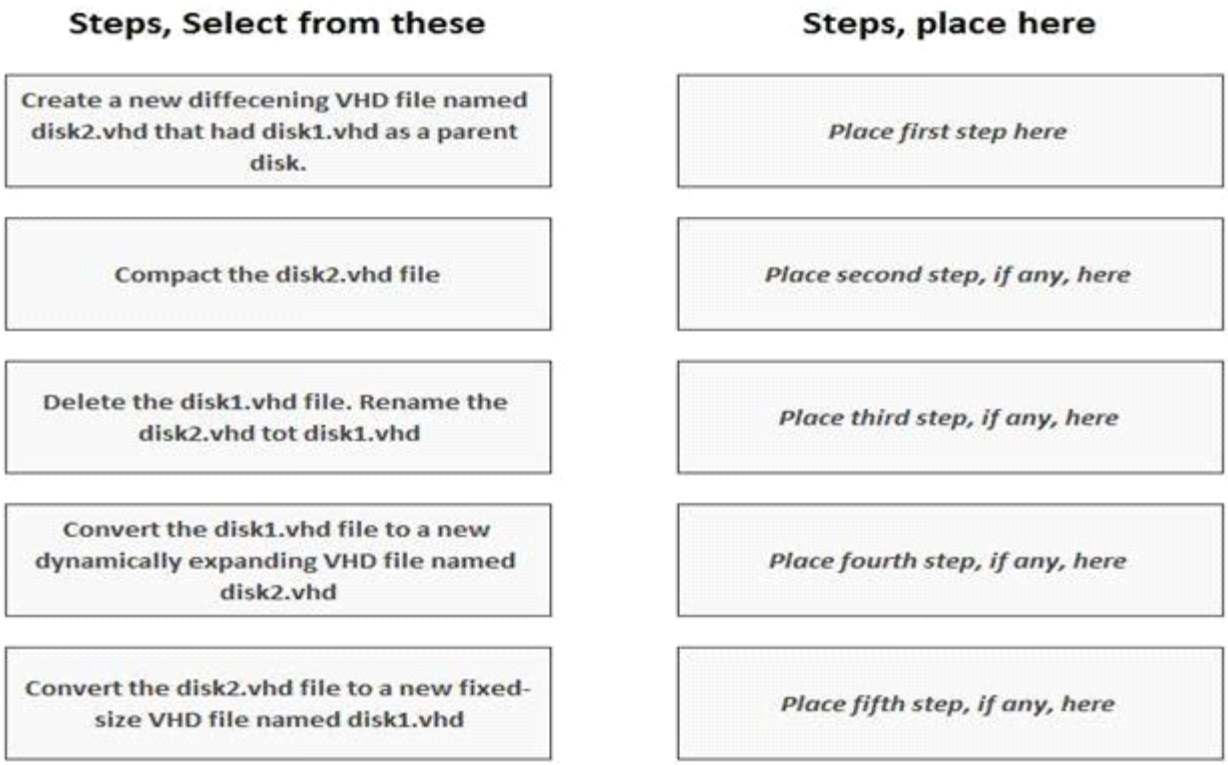
Explanation:



Question: 101

DRAG DROP

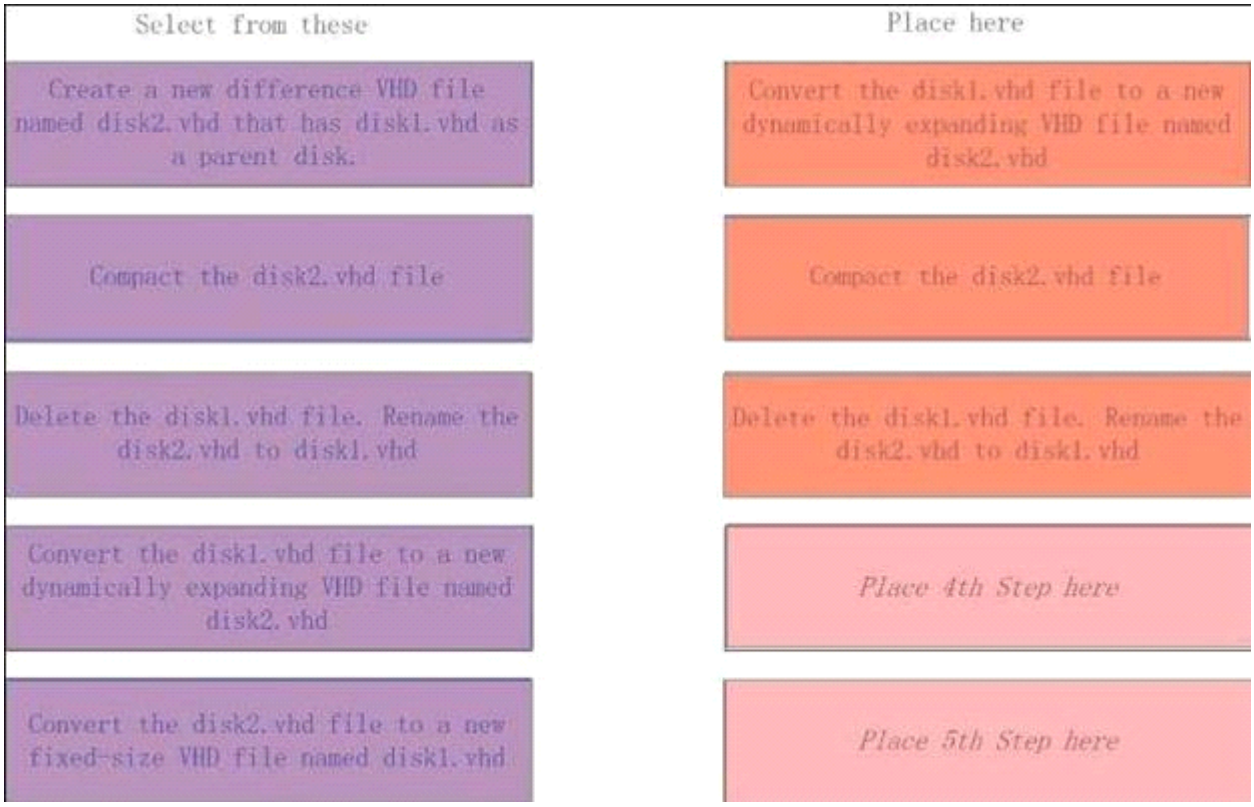
Your company has a server named VS1 that runs Windows Server 2008 R2 and Hyper-V. The VS1 server hosts 10 virtual servers. A virtual server named VS-DB has one 64-GB fixed-size virtual hard disk (VHD). The VHD file name is disk1.vhd. You discover that VS-DB utilizes only 5 GB of the VHD. You turn off the VS-DB virtual server and want to regain the unused disk space on the VS1 physical server. You need to configure VS-DB to make the disk1.vhd file as small as possible. What should you do? (To answer, move the appropriate tasks from the list of tasks to the answer area and arrange them in the correct order.)



Answer:

Steps, Select from these	Steps, place here
Create a new diffecening VHD file named disk2.vhd that had disk1.vhd as a parent disk.	Convert the disk1.vhd file to a new dynamically expanding VHD file named disk2.vhd
	Compact the disk2.vhd file
	Delete the disk1.vhd file. Rename the disk2.vhd tot disk1.vhd
	Place fourth step, if any, here
Convert the disk2.vhd file to a new fixed-size VHD file named disk1.vhd	*Place fifth step, if any, here*

Explanation:



Question: 102

You have a server that runs Windows Server 2008 R2. The server has the Hyper-V server role installed. You create a new virtual machine and perform an installation of Windows Server 2003 on the virtual machine. You configure the virtual machine to use the physical network card of the host server. You notice that you are unable to access network resources from the virtual machine. You need to ensure that the virtual host can connect to the physical network. What should you do?

A. On the host server, install the Microsoft Loopback adapter.
B. On the host server, enable the Multipath I/O feature.
C. On the virtual machine, install the Microsoft Loopback adapter.
D. On the virtual machine, install Microsoft Hyper-V Integration Components.

Answer: D

Explanation:
Networking and virtual machines
To connect a virtual machine to a virtual network, you add a virtual network adapter to the virtual machine and then connect the virtual network adapter to an existing virtual network. There are two types of network adapters available for Hyper-V: a network adapter and a legacy network adapter. The network adapter is designed specifically for Hyper-V and requires a virtual machine driver that is included with the Hyper-V integration services. This type of networking adapter provides better performance than a legacy network adapter and is the recommended choice when it can be used. Because this type of virtual network adapter requires integration services in the guest operating system, it can be used only with guest operating systems for which integration services are available. Note If a network adapter is configured for a virtual machine but integration services are not installed in the guest operating system, Device Manager lists the network adapter as an unknown device.
Source: http://technet.microsoft.com/en-us/library/cc816585.aspx
Integration services Integration services are available for supported guest operating systems as described in the

following table. Windows 2003 SP2 Guest operating system - Device and service support Windows Server 2003 (x64 editions) with Service Pack 2 Drivers: IDE, SCSI, networking, video, and mouse Services: operating system shutdown, time synchronization, data exchange, heartbeat, and online backup
Note This operating system does not support a legacy network adapter. Windows Server 2003 (x86 editions) with Service Pack 2 Drivers: IDE, SCSI, networking, video, and mouse Services: operating system shutdown, time synchronization, data exchange, heartbeat, and online backup
Source: http://technet.microsoft.com/en-us/library/cc794868(WS.10).aspx

Question: 103

You have two servers that run Windows Server 2008 R2 Enterprise. Both servers have the Failover Clustering feature installed. You configure the servers as a two-node cluster. The cluster nodes are named NODE1 and NODE2. You have an application named PrintService that includes a print spooler resource. You need to configure the cluster to automatically return the PrintService application to NODE1 after a failover. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Set the Period (hours) option to 0 in the properties of the print spooler resource.
B. Move NODE1 to the top of the list of preferred owners for the PrintService application.
C. Enable the Allow Failback and Immediate options for the PrintService application.
D. Disable the If restart is unsuccessful, failover all resources in this server or application option in the properties of the print spooler resource.

Answer: B, C

Explanation:
Preferred nodes list defined
If you define a complete preferred nodes list for a group (that is, one listing all the nodes in the cluster), then the Cluster service uses this defined list as its internal list. However, if you define a partial preferred nodes list for a group, then the Cluster service uses this defined list as its internal list and appends any other installed nodes not on the preferred list, ordered by their node IDs. For example, if you created a 5-node cluster (installing the nodes in the order Node1, Node2, Node3, Node4, and Node5) and defined Node3, Node4, and Node5 as preferred owners for the resource group, PRINTGR1, the Cluster service would maintain this ordered list for PRINTGR1: Node3, Node4, Node5, Node1, Node2. How the Cluster service uses this list depends on whether the resource group move is due to a resource/node failure or a manual move group request.
Preferred lists and resource or node failures
For resource group or node failures, the group fails over to the node next to the current owner on the preferred nodes list. In the example above, if the resource group PRINTGR1 on Node3 fails, then the Cluster service would fail that group over to the next node on the list, Node4. If you allow failback for that group, then when Node3 comes up again, the Cluster service will fail back PRINTGR1 to that node.
Source: http://technet.microsoft.com/en-us/library/cc737785.aspx

Question: 104

A server runs Windows Server 2008 R2. The Remote Desktop Services server role is installed on the server. You deploy a new application on the server. The application creates files that have an extension of .xyz. You need to ensure that users can launch the remote application from their computers by double- clicking a file that has the .xyz extension. What should you do?

A. Configure the Remote Desktop Connection Client on the users' computers to point to the server.
B. Configure the application as a published application by using a Remote Desktop Program file.

C. Configure the application as a published application by using a Microsoft Windows Installer package file.
D. Configure the application as a published application by using a Remote Desktop Web Access Web site.

Answer: C

Explanation/Reference:
Launching Apps from the Desktop
For users who want to double-click documents to launch the application, terminal services now provides the ability to "install" the remote application's link to the desktop. This process effectively wraps the Remote-App's RDP file into a Windows Installer package—an MSI file—that is later installed to desktops in the environment.
At the same time, the installed MSI can modify the file extension associations on the desktop to reroute a double-clicked file to its associated RemoteApp on the terminal server. Figure 3 shows how the file extension associations have been modified on a client system after a Word RemoteApp is installed. Now, double-clicking any of the common Word file extensions will launch Word via the Remote Desktop Connection.

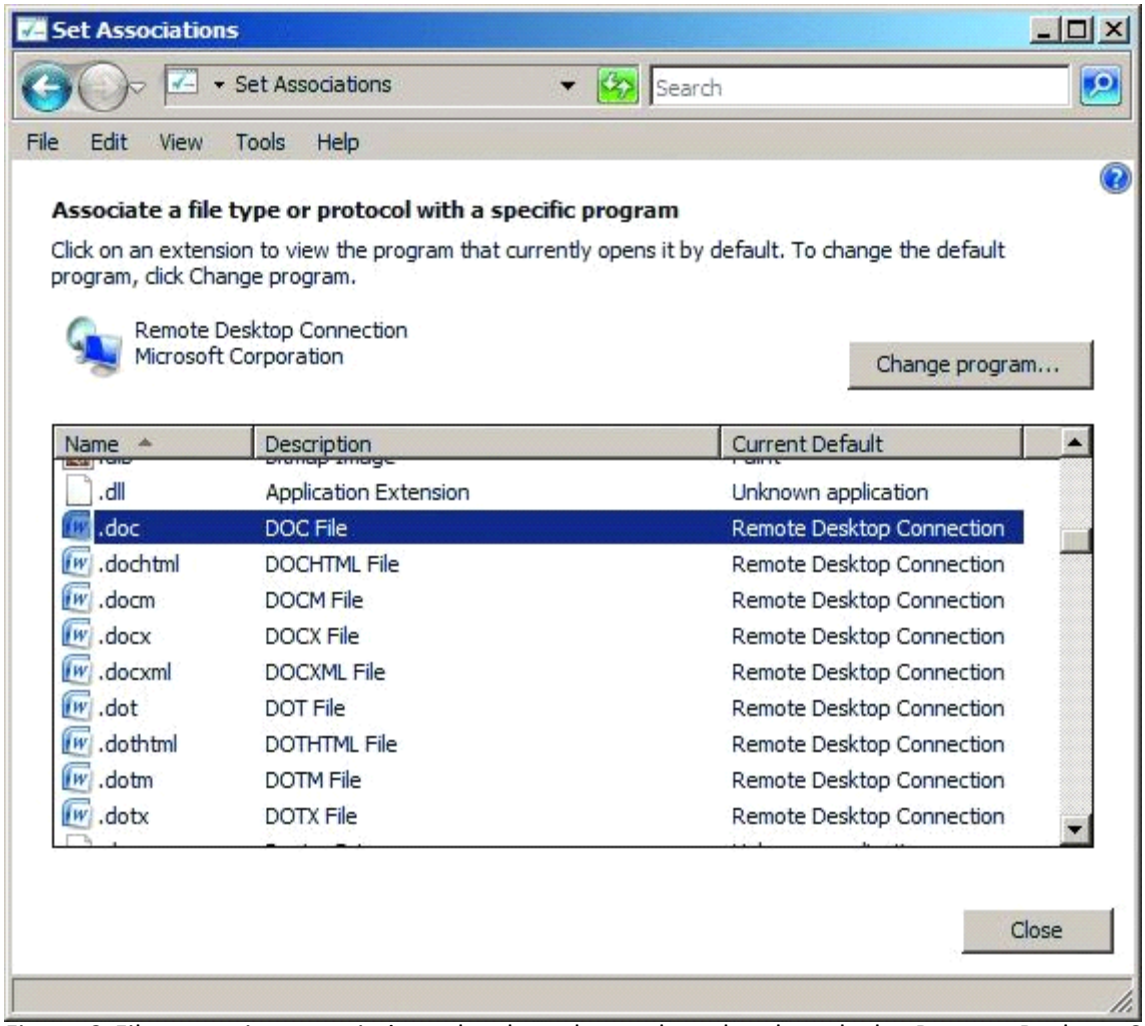


Figure 3 File extension associations that have been altered to launch the Remote Desktop Connection To create a Windows Installer package out of an existing RemoteApp, first navigate to the TS RemoteApp Manager. Right-click the RemoteApp of interest and select Create Windows Installer Package. By default, all created Windows Installer packages are stored in the location C:\Program Files\Packaged Programs, but this location can be changed from within the RemoteApp Wizard. Also configurable within the wizard are the name and port for the server that will host the RemoteApp, as well as server authentication, certificate settings, and TS Gateway settings. Settings that relate to the application's location after installation to a candidate desktop are shown in Figure 4. As you can see, it is possible to create a shortcut on the desktop as well as to a location within the Start menu folder. The most important checkbox on this screen is at the very bottom. It's the checkbox for Take over client settings, and it re-associates any file

extension associations for the RemoteApp from the local desktop to the terminal server. This checkbox must be selected if you want users to be able to double-click documents to launch their TS-hosted application. Click Next and Finish to complete the wizard. Please Note: -Since Windows2008R2 Terminal Services (TS) is now rebranded to Remote Desktop Services (RDS)-
Source: http://technet.microsoft.com/en-us/query/dd314392

Question: 105

You have a server that runs Windows Server 2008 R2. The server has Remote Desktop Web Access (RD Web Access) installed. Several line-of-business applications are available on the server by using RD Web Access. You install a new application on the server. You need to make the application available through RD Web Access. What should you do?

A. From the command prompt, run the mstsc.exe command and specify the /v parameter.
B. From the RD Web Access Web site, specify the data source for RD Web Access.
C. From RemoteApp Manager, add the application to the RemoteApp Programs list.
D. From the Local Users and Groups snap-in, add the users to the TS Web Access Computers group.

Answer: C

Explanation:
Once you've installed a RemoteApp, enabling it for TS Web Access is done by right-clicking the configured RemoteApp in the TS RemoteApp Manager and selecting Show in TS Web Access. Please Note: -Since Windows2008R2 Terminal Services (TS) is now rebranded to Remote Desktop Services (RDS)-
Source: http://technet.microsoft.com/en-us/query/dd314392

Question: 106

You have a server that runs the Remote Desktop Gateway (RD Gateway) role service. Users need to connect remotely through the gateway to desktop computers located in their offices. You create a security group named Remote1 for the users who need to connect to computers in their offices. You need to enable the users to connect to the RD Gateway. What should you do?

A. Add the Remote1 security group to the local remote desktop users group on the RD Gateway server.
B. Create a connection authorization policy. Add the Remote1 security group and enable Device redirection.
C. Create a resource authorization policy. Add the Remote1 security group and enable Users to connect to any resource.
D. Create a Group Policy object and enable the Set RD Gateway authentication method properties to Ask for credentials, use Basic protocol. Apply the policy to the RD Gateway server.

Answer: B

Explanation:
Once you've installed a RemoteApp, enabling it for TS Web Access is done by right-clicking the configured RemoteApp in the TS RemoteApp Manager and selecting Show in TS Web Access. Please Note: -Since Windows2008R2 Terminal Services (TS) is now rebranded to Remote Desktop Services (RDS)-
Source: http://technet.microsoft.com/en-us/query/dd314392

Question: 107

Your network contains a server that has Microsoft SharePoint Foundation 2010 installed. You need to ensure that a

user named User1 can use Windows PowerShell to back up SharePoint site collections. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Run the Add-SPShellAdmin cmdlet.
B. Run the Start-SPAssignment cmdlet.
C. Add User1 to the Farm Administrators group.
D. Add User1 to the local Backup Operators group.

Answer: A, C

Explanation:
Group memberships required to run backup and restore operations in Central Administration
You must ensure that all user accounts that will be backing up or restoring your farm and farm components by using Central Administration have the group memberships that are described in the following table. Required group memberships Setting permissions for running backup and restore operations by using Windows PowerShell You must ensure that all user accounts that will be backing up or restoring your farm and farm components by using Windows PowerShell are added to the SharePoint_Shell_Access role for a specified database and have the permissions described in the table later in this section. You can run the Add-SPShellAdmin cmdlet to add a user account to this role. You must run the command for each user account. Moreover, you must run the command for all databases to which you want to grant access.
Add-SPShellAdmin -Username <User account> -Database <Database ID>
Source: http://technet.microsoft.com/en-us/library/ee748626.aspx

Question: 108

Your network contains a server that runs Windows Server 2008 R2. The server has Microsoft SharePoint Foundation 2010 installed. You create a new Web application named WebApp1. Webapp1 is configured to use a service account named Service1. You need to ensure that the password for Service1 is automatically changed every 30 days. What should you modify from Central Administration?

A. the Authentication Providers
B. the Managed Accounts settings
C. the Password Management Settings
D. the Service Account settings

Answer: B

Explanation:
Configure managed accounts
You need to register managed accounts with the farm to make the accounts available to multiple services. You can register a managed account by using the Register Managed Account page in Central Administration. There are no options on the Register Managed Account page to create an account in Active Directory Domain Services, or on the local computer. The options can be used to register an existing account on the SharePoint Foundation 2010 farm. Perform the steps in the following procedure to use Central Administration to configure managed account settings.
To configure managed account settings by using Central Administration
1. Verify that the user account that is performing this procedure is a farm administrator.
2. On the Central Administration Web site, select Security.
3. Under General Security, click Configure managed accounts.
4. On the Managed Accounts page, click Register Managed Account.
5. In the Account Registration section of the Register Managed Account page, enter the service account credentials.

6. In the Automatic Password Change section, select the Enable automatic password change check box to allow SharePoint Foundation 2010 to manage the password for the selected account. Next, enter a numeric value that indicates the number of days prior to password expiration that the automatic password change process will be initiated.
7. In the Automatic Password Change section, select the Start notifying by email check box, and then enter a numeric value that indicates the number of days prior to the initiation of the automatic password change process that an email notification will be sent. You can then configure a weekly or monthly email notification schedule.
8. Click OK.
Source: http://technet.microsoft.com/en-us/library/ff607826.aspx

Question: 109

Your network contains a server that runs Windows Server 2008 R2. The server has Microsoft SharePoint Foundation 2010 installed.
You create a new Web application named WebApp1.
You need to configure WebApp1 to meet the following requirements:
Internal users must be authenticated by using Kerberos authentication.
External users must be authenticated by using NTLM authentication.
What should you do first?

A. Extend WebApp1.
B. Modify the User Policy.
C. Modify the Permissions Policy.
D. Configure the Alternate Access Mappings.

Answer: A

Explanation:
Extend a Web application
If you want to expose the same content in a Web application to different types of users by using additional URLs or authentication methods, you can extend an existing Web application into a new zone. When you extend the Web application into a new zone, you create a separate Internet Information Services (IIS) Web site to serve the same content, but with a unique URL and authentication type. An extended Web application can use up to five network zones (Default, Intranet, Internet, Custom, and Extranet). For example, if you want to extend a Web application so that customers can access content from the Internet, you select the Internet zone and choose to allow anonymous access and grant anonymous users readonly permissions. Customers can then access the same Web application as internal users, but through different URLs and authentication settings. For more information, see Configure anonymous access for a claims-based Web application (SharePoint Foundation 2010), and Plan authentication methods (SharePoint Foundation 2010).
Source: http://technet.microsoft.com/en-us/library/cc288162.aspx

Question: 110

Your network contains a server that has Microsoft SharePoint Foundation 2010 installed.
You create a new SharePoint site named Site1. You have a group named Group1.
You need to grant Group1 access to Site1. Group1 must have the following permissions:
Add Items
Edit Items
Approve Items
The solution must minimize the number of permissions assigned to Group1.

Which permission level should you assign to Group1?

A. Contribute
B. Design
C. Full Control
D. Read

Answer: B

Section: SharePoint
Explanation:
Default permission levels
Permission levels are collections of permissions that allow users to perform a set of related tasks. SharePoint Foundation 2010 includes five permission levels by default. You can customize the permissions available in these permission levels (except for the Limited Access and Full Control permission levels), or you can create customized permission levels that contain only the permissions you need. The following table lists the default permission levels for team sites in SharePoint

Permission level	Description	Permissions included by default
Limited Access	Allows access to shared resources in the Web site so that the users can access an item within the site. Designed to be combined with fine-grained permissions to give users access to a specific list, document library, folder, list item, or document, without giving them access to the entire site. Cannot be customized or deleted.	View Application Pages Browse User Information Use Remote Interfaces Use Client Integration Features Open
Read	View pages, list items and download documents.	Limited Access permissions, plus: View Items Open Items View Versions Create Alerts Use Self-Service Site Creation View Pages
Contribute	View, add, update, and delete items in the existing lists and document libraries.	Read permissions, plus: Add Items Edit Items Delete Items Delete Versions Browse Directories Edit Personal User Information Manage Personal Views Add/Remove Personal Web Parts Update Personal Web Parts
Design	View, add, update, delete, approve, and customize items or pages in the Web site.	Approve permissions, plus: Manage Lists Add and Customize Pages Apply Themes and Borders Apply Style Sheets
Full Control	Allows full control of the scope.	All permissions

Question: 111

Your network contains a server named Server1 that has Microsoft SharePoint Foundation 2010 installed. You configure Server1 to receive email by using the Automatic settings mode. You discover that the email enabled libraries on Server1 receive email from unauthorized SMTP servers. You need to ensure that Server1 only accepts email from authorized SMTP servers. What should you configure?

A. From the settings of the libraries, modify the permissions.
B. From the settings of the libraries, modify the incoming email settings.
C. From Central Administration, modify the incoming email settings.

D. From Central Administration, modify the list of approved distribution groups.

Answer: C

Explanation:
To configure incoming email in an advanced scenario
1. Verify that you have the following administrative credentials:
- You must be a member of the Administrators group on the computer that is running the SharePoint Central Administration Web site.
2. In Central Administration, click System Settings.
3. On the System Settings page, in the Email and Text Messages (SMS) section, click Configure incoming email settings.
4. If you want to enable sites on this server to receive email, on the Configure Incoming Email Settings page, in the Enable Incoming Email section, click Yes.
5. Select the Advanced settings mode.
If you select Advanced, you can specify a drop folder instead of using an SMTP server.
6. If you want to connect to Directory Management Service, in the Directory Management Service section, click Yes.If you select this option, you must first configure Active Directory Domain Services (AD DS). If you use Exchange Server, you must also configure the DNS Manager and add an SMTP connector. For more information, see the "Configure AD DS to be used with Directory Management Service", "Configure DNS Manager", and "Add an SMTP connector in Exchange Server 2010" sections later in this article.
a. In the Active Directory container where new distribution groups and contacts will be created box, type the name of the container in the format OU=ContainerName, DC=domain, DC=com, where ContainerName is the name of the OU in AD DS, domain is the second-level domain, and com is the toplevel domain.
b. In the SMTP mail server for incoming mail box, type the name of the SMTP mail server. The server name must match the FQDN in the A resource record entry for the mail server in DNS Manager.
c. To accept only messages from authenticated users, click Yes for Accept messages from authenticated users only. Otherwise, click No.
d. To enable users to create distribution groups from SharePoint sites, click Yes for Allow creation of distribution groups from SharePoint sites . Otherwise, click No.
e. Under Distribution group request approval settings , select the actions that will require approval.
Actions include the following:
- Create new distribution group
- Change distribution group email address
- Change distribution group title and description
- Delete distribution group
7. If you want to use a remote Directory Management Service, select Use remote. If you select this option and you are using Exchange Server, you must configure the DNS Manager and add an SMTP connector. For more information, see the "Configure DNS Manager" and "Add an SMTP connector in Exchange Server 2010" sections later in this article. The AD DS has most likely already been configured, so you do not need to do this. a. In the Directory Management Service URL box, type the URL of the Directory Management Service that you want to use. The URL is typically in the following format: http://server:adminport/_vti_bin/ SharePointEmailWS.asmx.
b. In the SMTP mail server for incoming mail box, type the name of the SMTP mail server. The server name must match the FQDN in the A resource record entry for the mail server in DNS Manager on the domain server. c. To accept messages from authenticated users only, click Yes for Accept messages from authenticated users only. Otherwise, click No.
d. To allow creation of distribution groups from SharePoint sites, click Yes for Allow creation of distribution groups from SharePoint sites. Otherwise, click No.
8. If you do not want to use Directory Management Service, click No.
9. In the Incoming Email Server Display Address section, in the Email server display address box, type a display name for the email server (for example, mail.fabrikam.com). You typically use this option together with the Directory Management Service.

10. In the Email Drop Folder section, in the Email drop folder box, type the name of the folder from which SharePoint 2010 Timer service retrieves incoming email from the SMTP service. If you select this option, ensure that you configure the necessary permissions to the email drop folder. For more information, see the "Configure permissions to the email drop folder" section later in this article. It is useful to have a dedicated email drop folder if the default email drop folder is full or almost full. Ensure that the logon account for the SharePoint 2010 Timer service has Modify permissions on the email drop folder. For more information, see "To configure email drop folder permissions for the logon account for the SharePoint 2010 Timer service" procedure later in this article.
11. In the Safe Email Servers section, select whether you want to accept email from all email servers or from several specified email servers
12. Click OK.

Question: 112

You deploy a server that has Microsoft SharePoint Foundation 2010 installed. Users report that they cannot configure the Alert Me option for SharePoint documents. You need to ensure that users can create alerts. What should you modify from Central Administration?

A. Configure Send To Connections
B. Information Rights Management
C. the Outgoing Email Settings
D. the Workflow Settings

Answer: C

Explanation:
Configure alert settings for a Web application To help users keep track of changes that are made to a Web site, Microsoft SharePoint Foundation 2010 includes the alerts feature, which is an email notification service. Users can configure which alerts they want to receive or send to communicate and track changes to items on a Web site. Users can create alerts on the following items in a site:
Lists Users are notified of changes to the list, such as when an item is added, deleted, or changed in a list.
List items Users are notified of changes to a particular item in a list.
Document libraries Users are notified of changes to the document library, such as when a document is added, deleted, or changed in a document library or when Web discussions are added, changed, deleted, closed, or started for a document.
Documents
Users are notified of changes in a particular document such as when a document is changed, added, deleted, or closed. You can use Central Administration to configure alerts. You can turn on or turn off alerts, and you can specify how many alerts users can create. Before alerts can work for any Web site, outgoing email must be enabled for the server.
To configure alert settings for a Web application by using Central Administration
1. Verify that the user account that is performing this task is a member of the Farm Administrators SharePoint group.
2. On the SharePoint Central Administration Web site, click Application Management.
3. On the Application Management page, click Manage Web Applications.
4. Click the Web application for which you want to configure alerts. The ribbon becomes active.
5. On the ribbon, click the General Settings drop-down menu, and then click General Settings.
6. On the Web Application General Settings page, in the Alerts section, configure the following settings:
Specify whether alerts are On or Off. By default, alerts are On.
Specify the Maximum number of alerts that a user can create in a SharePoint Web site. This value can be any integer from 1 through 2,000,000,000, or you can specify that the number of alerts is unlimited. The default value is 500 alerts.
7. After you have finished configuring alerts, click OK.

Source: http://technet.microsoft.com/en-us/library/cc287751.aspx

Question: 113

You have a Remote Desktop Services farm that contains several Remote Desktop Session Host Servers. You need to configure one of the Remote Desktop Session Host Servers as a dedicated redirector. You configure the appropriate DNS records.
What should you do next?

A. From Remote Desktop Session Host Configuration, set the licensing mode to per user.
B. From Remote Desktop Session Host Configuration, set the licensing mode to per device.
C. From Remote Desktop Session Host Configuration, change the relative weight of the server to 50.
D. From Remote Desktop Session Host Configuration, configure the server to deny new user logons.

Answer: D

Explanation:
To configure dedicated redirectors, you must do the following:
1. Create DNS round robin entries for the terminal servers that you want to use as dedicated redirectors. When you do so, you must map the IP address of each terminal server that you want to use as a dedicated redirector to the terminal server farm name in DNS. (The farm name is the virtual name that clients use to connect to the terminal server farm.) The farm name must not match an existing server name in Active Directory Domain Services (AD DS).
2. Configure the terminal servers that you want to use as dedicated redirectors to deny new user logon requests.
Source: http://technet.microsoft.com/en-us/library/ff519163(WS.10).aspx

Question: 114

Your company has a Windows Server 2003 Active Directory domain. A server named Server1 runs Windows Server 2008 R2. The Remote Desktop Services server role is installed on Server1. A server named Server2 runs Windows Server 2003. The TS Licensing role service is installed on Server2. You need to configure the Remote Desktop Services Per User Client Access License (RD Per User CAL) tracking and reporting to work on both Server1 and Server2. What should you do?

A. Rename Server1 to have the same computer name as the domain and join it to a workgroup.
B. Add Server1 to the servers managed by the Windows Server 2003 TS Licensing service.
C. Uninstall the TS Licensing role service on Server2 and install Remote Desktop Licensing role service on Server1. Configure RD Per User CAL tracking and reporting on Server1.
D. Activate the TS Licensing Server on Server 2.

Answer: C

Explanation:
Q: We have a Windows 2003 domain network and are planning to add a Windows 2008 R2 member server to the domain and use it as a remote desktop server. My question is this a supported configuration? If yes, should I install the TS licensing server on our 2003 DC and add the Windows 2008 R2 CALs in there or we should install the RD license service role in the same server as the Remote Desktop service role computer.
A: That scenario is supported. However, 2008 R2 RDS CALs can ONLY be issued by a Windows 2008 R2 Licensing Server. So yes, you will have to install the licensing role onto your r2 server and use that as the license manager.
Q: So all I need is to install all the necessary RDS components including the license services onto the member server and add the TS CALs in there. There is nothing I have to do on the existing Windows CALs license server or DC, right?

A: That's correct. You will, however, most likely have to manually point your 2008 R2 RDSHS to the R2 license server (itself in your case).
Source: http://social.technet.microsoft.com/Forums/en-US/windowsserver2008r2rds/thread/561828c7-e7b5-4f9c-bae1-2331214a0ed7

Question: 115

Your company has an Active Directory domain. A server named Server1 runs Windows Server 2008 R2. The Remote Desktop Services server role is installed on Server1. A server named Server2 runs Windows Server 2008 R2. The Remote Desktop Licensing role service is installed on Server2. Only 10 Remote Desktop Services Client Access Licenses are available. You need to limit the number of concurrent users connected to the Remote Desktop Session Host Server to 10. What should you do?

A. Create a Group Policy object (GPO). Enable the Set the Remote Desktop licensing mode policy setting and select the Per User option. Apply the GPO to Server1.
B. Create a Group Policy object (GPO). Enable the Set the Remote Desktop licensing mode policy setting and select the Per User option. Apply the GPO to Server2.
C. Create a Group Policy object (GPO). Enable the Set the Remote Desktop licensing mode policy setting and select the Per Device option. Apply the GPO to Server1.
D. Create a Group Policy object (GPO). Enable the Set the Remote Desktop licensing mode policy setting and select the Per Device option. Apply the GPO to Server2.

Answer: A

Explanation:
Set the Remote Desktop licensing mode
This policy setting allows you to specify the type of Remote Desktop Services client access license (RDS CAL) that is required to connect to this RD Session Host server. You can use this policy setting to select one of two licensing modes: Per User or Per Device. Per User licensing mode requires that each user account connecting to this RD Session Host server have an RDS Per User CAL. Per Device licensing mode requires that each device connecting to this RD Session Host server have an RDS Per Device CAL. If you enable this policy setting, the licensing mode that you specify takes precedence over the licensing mode that is specified during the installation of Remote Desktop Session Host or specified in the Remote Desktop Session Host Configuration tool. If you disable or do not configure this policy setting, the licensing mode that is specified during the installation of Remote Desktop Session Host role service or specified in the Remote Desktop Session Host Configuration tool is used.
Source: http://technet.microsoft.com/en-us/library/ee791926(WS.10).aspx

Question: 116

Your company runs Remote Desktop Services. You plan to install an application update for the lobapp.exe application on the Remote Desktop Session Host Server. You find instances of the lobapp.exe processes left behind by users who have disconnected. You need to terminate all instances of the lobapp.exe processes so that you can perform an application update. What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two.)

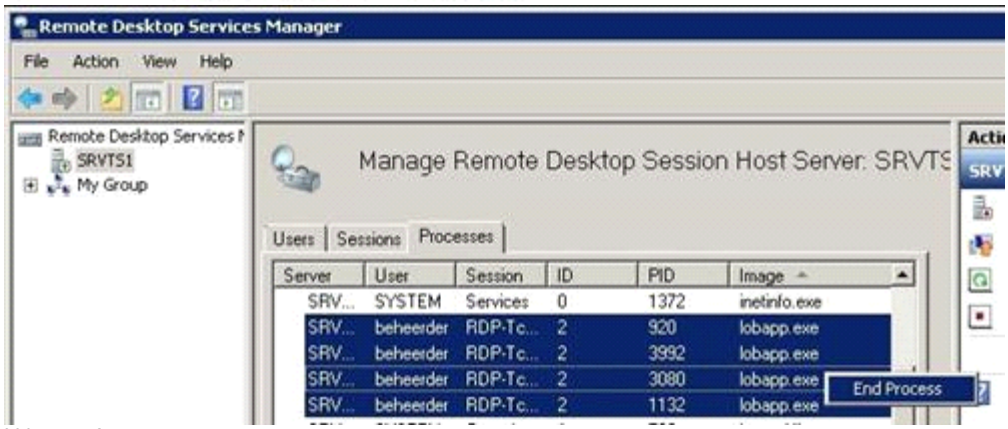
A. Run the Get-Process cmdlet on the Remote Desktop Session Host Server.
B. Run the Tskill lobapp /a command on the Remote Desktop Session Host Server.
C. End all instances of lobapp.exe in the Remote Desktop Services Manager console.
D. Run the Tasklist /fi "IMAGENAME eq lobapp.exe" command on the Remote Desktop Session Host Server.

Answer: B, C

Explanation:

```
tskill {<ProcessID> | <ProcessName>} [/server:<ServerName>] [/id:<SessionID> | /a]
[/v]
```

Parameter	Description
<ProcessID>	Specifies the ID of the process that you want to end.
<ProcessName>	Specifies the name of the process that you want to end. This parameter can include wildcard characters.
/server: <ServerName>	Specifies the terminal server that contains the process that you want to end. If /server is not specified, the current terminal server is used.
/id:<SessionID>	Ends the process that is running in the specified session.
/a	Ends the process that is running in all sessions.
/v	Displays information about the actions being performed.
/?	Displays help at the command prompt.



Wrong Awnsers:

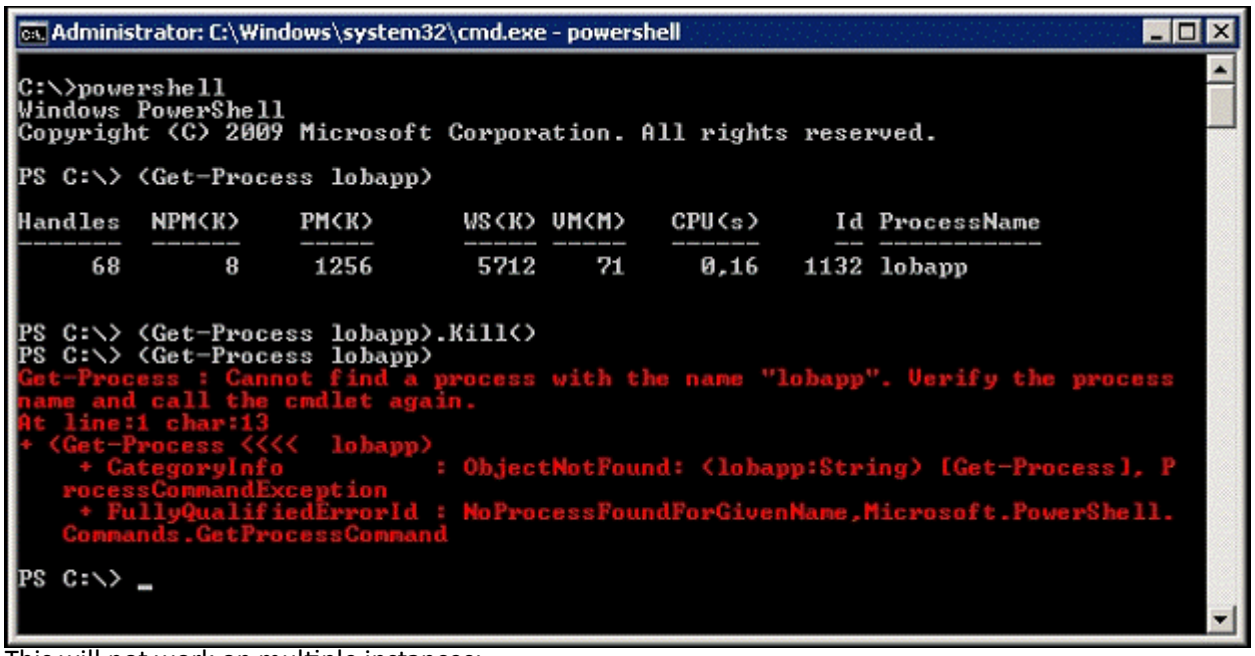
Tasklist

Displays a list of currently running processes on the local computer or on a remote computer. Tasklist replaces the tlist tool.

Source: http://technet.microsoft.com/en-us/library/cc730909(WS.10).aspx

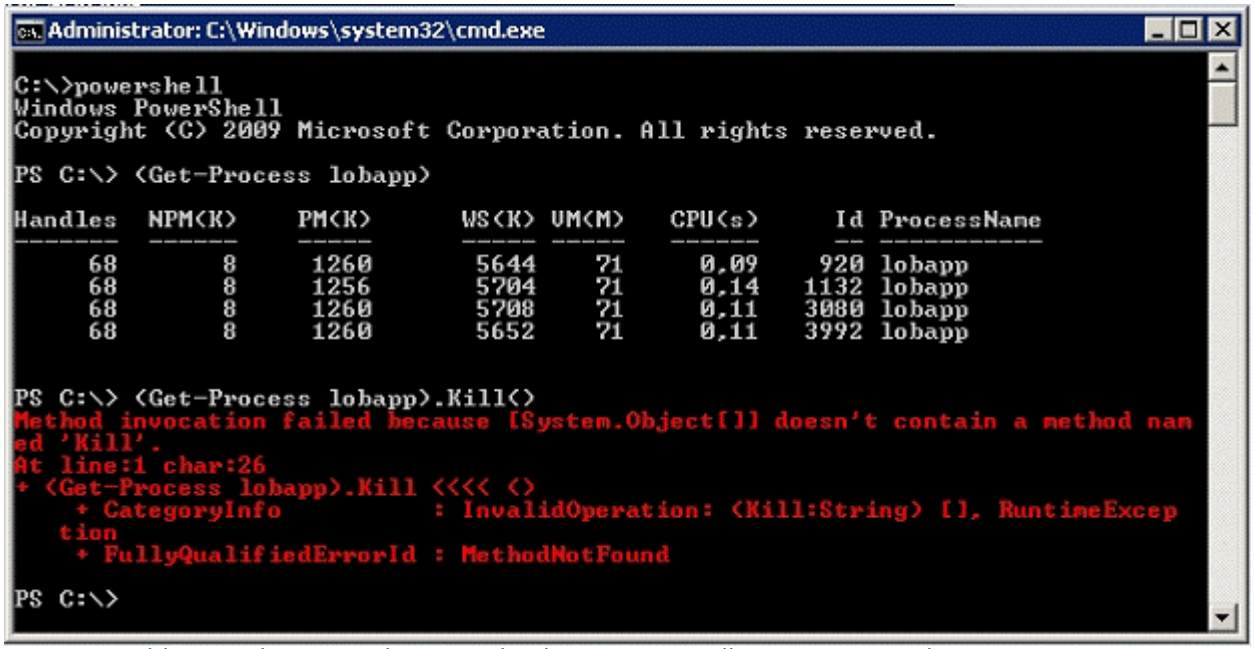
Get-Process Although the following will work for a single instance:

(Get-Process lobapp).Kill()

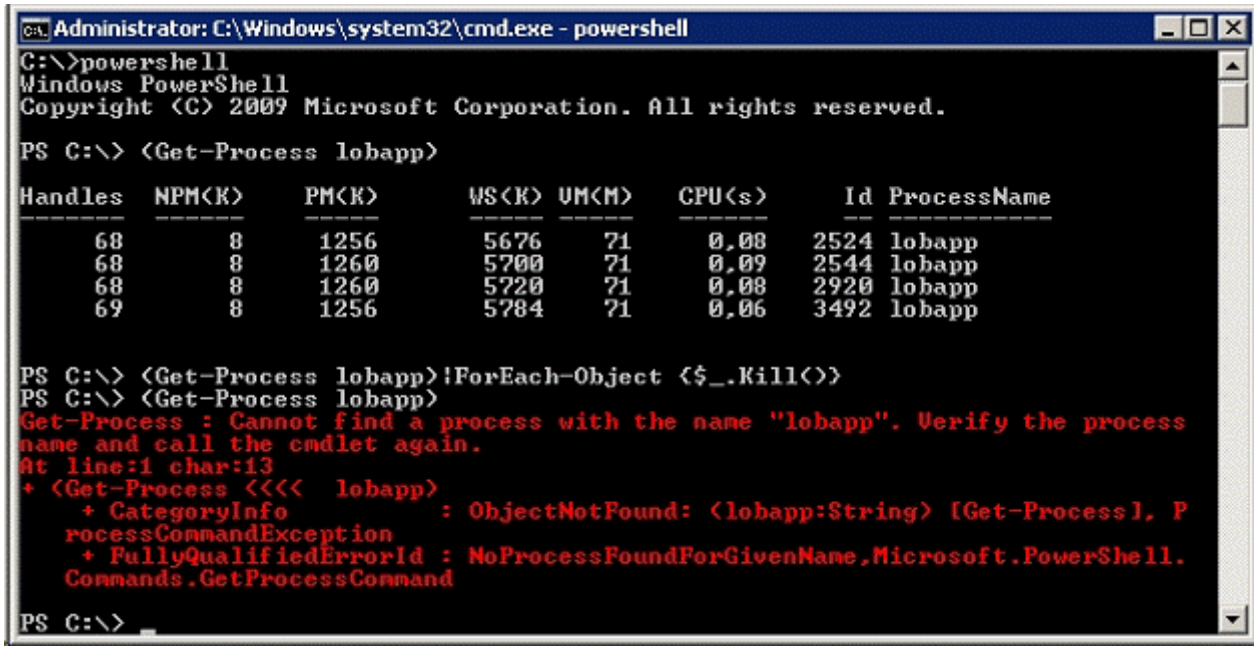


This will not work on multiple instances:

(Get-Process lobapp).Kill()



But one could argue that using the ForEach-Object commandlet circumvents the issue:
(Get-Process lobapp)|ForEach-Object {$_.Kill()}
However because this requires more than just the Get-Process cmdlet, I choose to render this answer invalid.



Question: 117

You install the Web Server (IIS) server role on two servers named Server1 and Server2. The servers run Windows Server 2008 R2. Your company has a Web site named www.contoso.com hosted on Server1. The Web site is due for maintenance. The Web content must be available during maintenance. You create a mirror Web site located on Server2. You need to configure the www.contoso.com site to redirect requests to Server2. What should you do first?

A. Run the appcmd set config /section:httpRedirect /enabled:true command.
B. Run the appcmd set config /section:httpRedirect /enabled:false command.
C. Run the appcmd set site /site.name:contoso /-bindings.[protocol='http',www.contoso.com] command.

D. Run the appcmd set site /site.name:contoso /+bindings.[protocol='http',www1.contoso.com] command.

Answer: A

Explanation:
To enable redirection
You can perform this procedure by running Appcmd.exe commands in a command-line window.
Command Line
To enable or disable redirection, use the following syntax:
appcmd set config /section:httpRedirect /enabled:true |false /destination:location
By default, the redirection feature is disabled, but you can enable it by specifying true for the enabled attribute and configuring the location to which to redirect users in the destination attribute. For example, if you want to enable redirection and redirect users to http://www.contoso.com, type the following at the command prompt, and then press ENTER:
appcmd set config /section:httpRedirect /enabled:true /destination:http://www.
contoso.com
Source: http://technet.microsoft.com/en-us/library/cc732930(WS.10).aspx

Question: 118

You install the Web Server (IIS) server role on a new server that runs Windows Server 2008 R2. You install a Microsoft .NET Framework application on a Web site on the Web server. The application launches a process that presents a real-time graphical report to the Web browser and creates a text report file on the hard disk drive. The company security policy states that the application must not perform any of the following tasks:
Write to the event log.
Access Open Database Connectivity (ODBC) data sources.
Make network or Web service calls.
You need to configure the Web site so that the application can be executed. You must ensure that the application meets the outlined security requirements. What should you do?

A. Set the .NET Framework trust level to Full for the Web site.
B. Set the .NET Framework trust level to Low for the Web site.
C. Set the .NET Framework trust level to High for the Web site.
D. Set the .NET Framework trust level to Medium for the Web site.

Answer: D

Explanation:
Use the .NET Trust Levels feature page to set the trust element in the web.config file. The trust element enables you to configure the level of code access security (CAS) that is applied to an application. Full (internal) - Specifies unrestricted permissions. Grants the ASP.NET application permissions to access any resource that is subject to operating system security. All privileged operations are supported. High (web_hightrust.config) - Specifies a high level of code access security, which means that the application cannot do any one of the following things by default:
Call unmanaged code.
Call serviced components.
Write to the event log. Access Message Queuing service queues.
Access ODBC, OleDb, or Oracle data sources. Medium (web_mediumtrust.config) - Specifies a medium level of code access security, which means that, in addition to High Trust Level restrictions, the ASP.NET application cannot do any of the following things by default:
Access files outside the application directory.

Access the registry.
Make network or Web service calls. Low (web_lowtrust.config) - Specifies a low level of code access security, which means that, in addition to Medium Trust Level restrictions, the application cannot do any of the following things by default:
Write to the file system.
Call the Assert method.
Minimal (web_minimaltrust.config) - Specifies a minimal level of code access security, which means that the application has only execute permissions.
Source: http://technet.microsoft.com/en-us/library/cc754779.aspx

Question: 119

You install the Web Server (IIS) on a server that runs Windows Server 2008 R2. You install a Microsoft .NET Framework application on a Web site that is hosted on the server in a folder named \wwwroot. The .NET Framework application must write to a log file that resides in the \Program Files\WebApp folder. You need to configure the .NET Framework trust level setting for the Web site so that the application can write to the log file. What should you do?

A. Set the .NET Framework trust level to Full for the Web site.
B. Set the .NET Framework trust level to High for the Web site.
C. Set the .NET Framework trust level to Minimal for the Web site.
D. Set the .NET Framework trust level to Medium for the Web site.

Answer: D

Explanation:
Use the .NET Trust Levels feature page to set the trust element in the web.config file. The trust element enables you to configure the level of code access security (CAS) that is applied to an application. Full (internal) - Specifies unrestricted permissions. Grants the ASP.NET application permissions to access any resource that is subject to operating system security. All privileged operations are supported. High (web_hightrust.config) - Specifies a high level of code access security, which means that the application cannot do any one of the following things by default:
Call unmanaged code.
Call serviced components.
Write to the event log.
Access Message Queuing service queues.
Access ODBC, OleDb, or Oracle data sources.
Medium (web_mediumtrust.config) - Specifies a medium level of code access security, which means that, in addition to High Trust Level restrictions, the ASP.NET application cannot do any of the following things by default:
Access files outside the application directory.
Access the registry.
Make network or Web service calls.
Low (web_lowtrust.config) - Specifies a low level of code access security, which means that, in addition to Medium Trust Level restrictions, the application cannot do any of the following things by default:
Write to the file system.
Call the Assert method.
Minimal (web_minimaltrust.config) - Specifies a minimal level of code access security, which means that the application has only execute permissions.
Source: http://technet.microsoft.com/en-us/library/cc754779.aspx

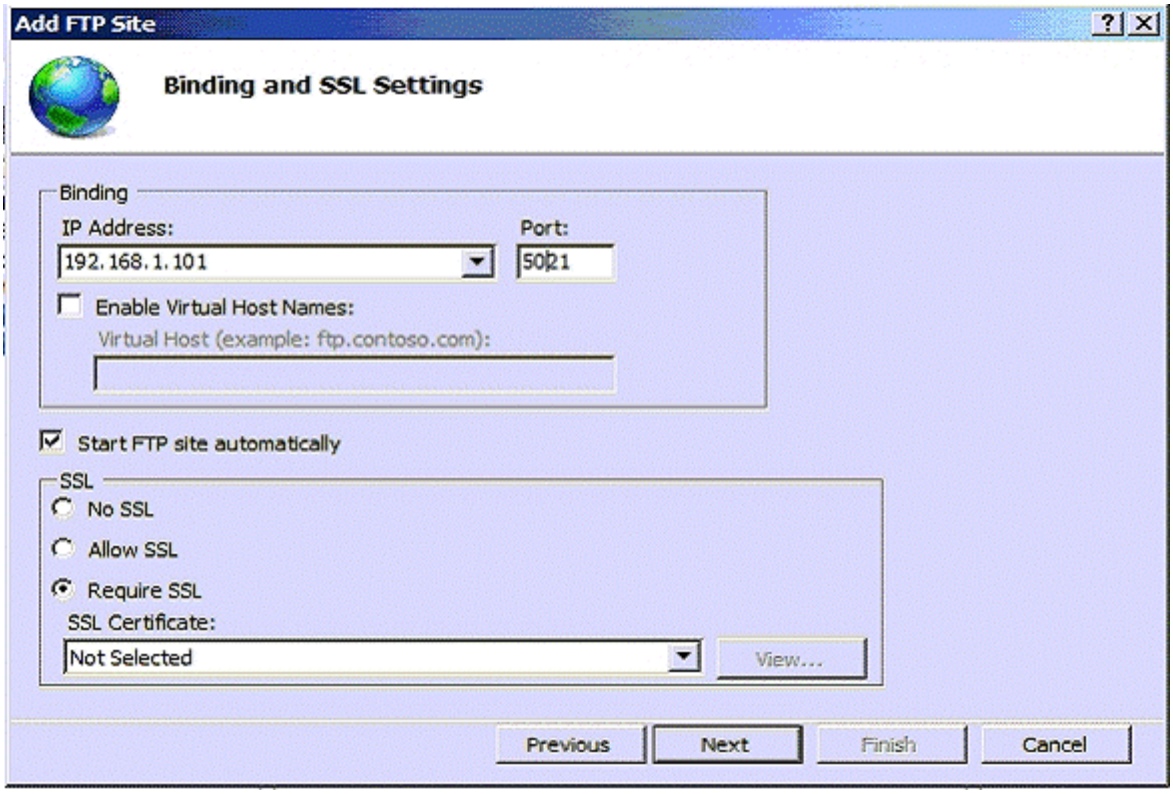
Question: 120

You have a server that runs Windows Server 2008 R2. The server has the Web Server (IIS) server role and the FTP Service role service installed. You add a new FTP site to the server. You need to ensure that the new FTP site is available. What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two.)

A. Run the iisreset command on the server.
B. Configure an alternate TCP port in the FTP site properties.
C. Configure an alternate IP address in the FTP site properties.
D. Configure a host header file in the default Web site properties.
E. Configure an alternate IP address in the default Web site properties.

Answer: B, C

Explanation:
Creating Multiple FTP Sites
You can create multiple FTP sites using multiple IP addresses and multiple ports. While creating multiple sites with multiple IP addresses is a common and recommended practice, it can be more complicated because, by default, clients call port 21 when using the FTP protocol. Therefore, if you create multiple FTP sites using multiple ports, you need to inform users of the new port number so their FTP clients can locate and connect to the port. If you create a new site using the same port as an existing site with the same IP address, the new site will not start. The general rule is that you can have multiple sites using the same IP and port, but only one site from this group can run at a time. If you try to start another site from this group, you receive an error message.
Procedures
To create multiple FTP sites using multiple IP addresses
1. In IIS Manager, expand the local computer, right-click the FTP Sites folder, point to New, and click FTP Site
2. Click Next.
3. In the Description box, type a description of your FTP site, and then click Next.
4. Under Enter the IP address to use this FTP site, type a new IP address, and leave the TCP port setting at 21.
5. Complete the rest of the FTP Site Creation Wizard.
To create multiple FTP sites using multiple ports
1. In IIS Manager, expand the local computer, right-click the FTP Sites folder, point to New, and click FTP Site
2. Click Next.
3. In the Description box, type a description of your FTP site, and then click Next.
4. Under Enter the IP address to use for this FTP site , type your Web server's IP address.
5. Under Type the TCP port for this FTP site , change the TCP port from the default setting of 21 to an unallocated port number. If you are uncertain which port numbers are already allocated, choose a high number, for example a number between 5000 and 5999.
6. Complete the rest of the FTP Site Creation Wizard.



Question: 121

You have a test lab that contains 20 client computers and a server named Server1. The client computers run Windows 7. Server1 runs Windows Server 2008 Service Pack 2 (SP2). You install the Key Management Service (KMS) on Server1. You need to ensure that the client computers can successfully activate by using Server1. What should you do?

A. Upgrade Server 1 to Windows Server 2008 R2.
B. Deploy five additional client computers that run Windows 7.
C. On each client computer, run slmgr.vbs /rearm.
D. On Server1, restart the Windows Activation Technologies service.

Answer: B

Explanation:
Minimum Computer Requirements
When planning for KMS activation, the network must meet or exceed the activation threshold, or the minimum number of qualifying computers that KMS requires. You must also understand how the KMS host tracks the number of computers on the network.
KMS Activation Thresholds
KMS can activate both physical computers and virtual machines. To qualify for KMS activation, a network must meet the activation threshold: KMS hosts activate client computers only after meeting this threshold. To ensure that the activation threshold is met, a KMS host counts the number of computers that are requesting activation on the network. For computers running Windows Server 2008 or Windows Server 2008 R2, the activation threshold is five. For computers running Windows Vista or Windows 7, the activation threshold is 25. The thresholds include client computers and servers that are running on physical computers or virtual machines.
Source: http://technet.microsoft.com/en-us/library/ff793434.aspx

Question: 122

You need to manually create a service location (SRV) record for a server that has the Key Management Service (KMS) installed. Which SRV record should you create?

A. _kms._tcp.contoso.com
B. _kms._tcp._msdcs.contoso.com
C. _mskms._tcp.contoso.com
D. _vlmcs._tcp.contoso.com

Answer: D

Explanation:
Manually Create SRV Records in DNS
If the environment does not support DDNS, the SRV RRs must be manually created to publish the KMS host. Environments that do not support DDNS should disable publishing on all KMS hosts to prevent event logs from collecting failed DNS publishing events. To disable auto-publishing, use the Slmgr.vbs script with the /cdns command-line option. See the "Configuring KMS" section for more information about the Slmgr.vbs script. Note Manually created SRV RRs can coexist with SRV RRs that KMS hosts automatically publish in other domains as long as all records are maintained to prevent conflicts. Using DNS Manager, in the appropriate forwarding lookup zone, create a new SRV RR using the appropriate information for the location. By default, KMS listens on TCP port 1688, and the service is _VLMCS. Table 2 contains example settings for a SRV RR.
Table 2 SRV Resource Record

Name	Setting
Service	_VLMCS
Protocol	_TCP
Port number	1688
Host offering the service	FQDN of KMS Host

Question: 123

Your network contains a server named Server1 that runs Windows Server 2008 R2. You need to configure Server1 as a Key Management Service (KMS) host. What should you do first?

A. At the command prompt, run slmgr.vbs and specify the /dli option.
B. At the command prompt, run slmgr.vbs and specify the /ipk option.
C. From the Server Manager console, run the Add Features Wizard and install the Online Responder Tools.
D. From the Server Manager console, run the Add Features Wizard and install the Windows Process Activation Service.

Answer: B

Explanation:
To install a KMS host on a Windows Vista or Windows Server 2008 computer
1. Log on to the computer that will serve as the KMS host.
2. Open an elevated command prompt. To do this, click Start, click All Programs, click Accessories, right-click Command Prompt, and then click Run as administrator.
3. To install your KMS key, type the following at the command prompt, and then press Enter: cscript C:\windows\system32\slmgr.vbs /ipk <KmsKey>
4. Activate the KMS host with Microsoft® using one of the following:

4a. For online activation, type the following at the command prompt and then press Enter:
cscript C:\windows\system32\slmgr.vbs /ato
4b. For telephone activation, type the following at the command prompt and then press Enter:
slui.exe 4
5. After activation is complete, restart the Software Licensing Service using the Service application.
Source: http://technet.microsoft.com/en-us/library/cc303280.aspx#_Install_KMS_Hosts

Question: 124

Your network contains a server named Server1. Server1 has the Volume Activation Management Tool (VAMT) installed. You need to activate Windows on a server named Server2 by using VAMT. Which firewall rule should you enable on Server2?

A. COM+ Network Access (DCOM-In)
B. COM+ Remote Administration (DCOM-In)
C. Remote Service Management (RPC)
D. Windows Management Instrumentation (WMI-In)

Answer: D

Section: Key Management Services (KMS)
Explanation:
Product key management with VAMT enables:
Single local console to manage keys for Windows client, Windows Server and Office 2010
Installation of the keys on remote managed systems through WMI
Tracking remaining activations on MAKs3
Source: http://technet.microsoft.com/en-us/library/ff686876.aspx

Question: 125

Your network contains a server named Server1 that has the Hyper-V server role installed. Server1 has two network adapters.
You need to configure Server1 to meet the following requirements:
All virtual machines (VMs) on Server1 must be able to communicate with other computers on the network.
The number of virtual network connections must be minimized.
What should you do?

A. Create one internal virtual network. Clear the Enable virtual LAN identification for management operating system check box for the virtual network.
B. Create one internal virtual network. Select the Enable virtual LAN identification for management operating system check box for the virtual network.
C. Create one external virtual network. Clear the Allow management operating system to share this network adapter check box for the virtual network.
D. Create one external virtual network. Select the Allow management operating system to share this network adapter check box for the virtual network.

Answer: C

Explanation:
External virtual networks. Use this type when you want to provide virtual machines with access to a physical network

to communicate with externally located servers and clients. This type of virtual network also allows virtual machines on the same virtualization server to communicate with each other. This type of network may also be available for use by the management operating system, depending on how you configure the networking. (The management operating system runs the Hyper-V role.) For more information, see “A closer look at external virtual networks” later in this topic.
Source: http://technet.microsoft.com/en-us/library/cc816585%28WS.10%29.aspx

Question: 126

Your network contains a server named Server1 that has the Hyper-V server role installed. Server1 hosts a virtual machine (VM) named VM1. You add an additional hard disk to Server1. The hard disk is configured as a basic disk. You need to configure VM1 to use the new hard disk as a pass-through disk. What should you do before you configure the pass through disk?

A. Create a simple volume.
B. Take the new hard disk offline.
C. Convert the new hard disk to a GPT disk.
D. Convert the new hard disk to a dynamic disk.

Answer: B

Explanation:
Pass -through Disk Configuration
Hyper-V allows virtual machines to access storage mapped directly to the Hyper-V server without requiring the volume be configured. The storage can either be a physical disk internal to the Hyper-V server or it can be a Storage Area Network (SAN) Logical Unit (LUN) mapped to the Hyper-V server. T o ensure the Guest has exclusive access to the storage, it must be placed in an Offline state from the Hyper-V server perspective. Additionally, this raw piece of storage is not limited in size so, hypothetically, it can be a multiterabyte LUN. After storage is mapped to the Hyper-V server, it will appear as a raw volume and will be in an Offline state (depending on the SAN Policy (Figure 1-1)) as seen in Figure 1.

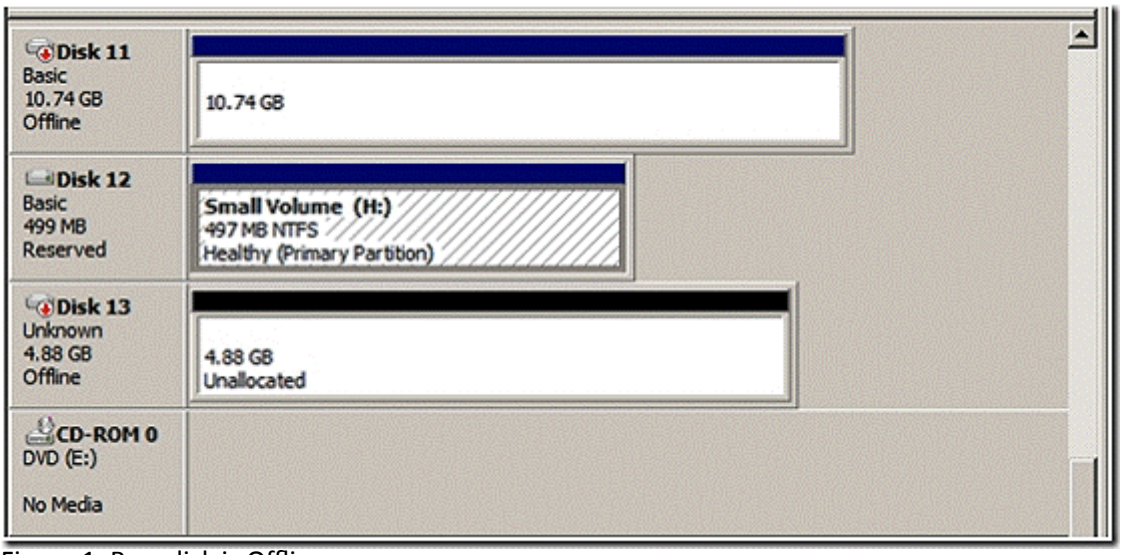


Figure 1: Raw disk is Offline

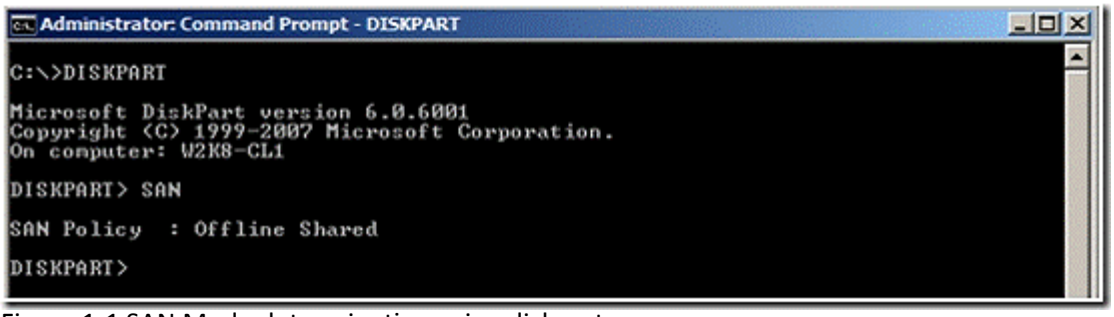


Figure 1-1 SAN Mode determination using diskpart.exe

I stated earlier that a disk must be Offline from the Hyper-V servers' perspective in order for the Guest to have exclusive access. However, a raw volume must first be initialized before it can be used. To accomplish this in the Disk Management interface, the disk must first be brought Online. Once Online, the disk will show as being Not Initialized (Figure 2).

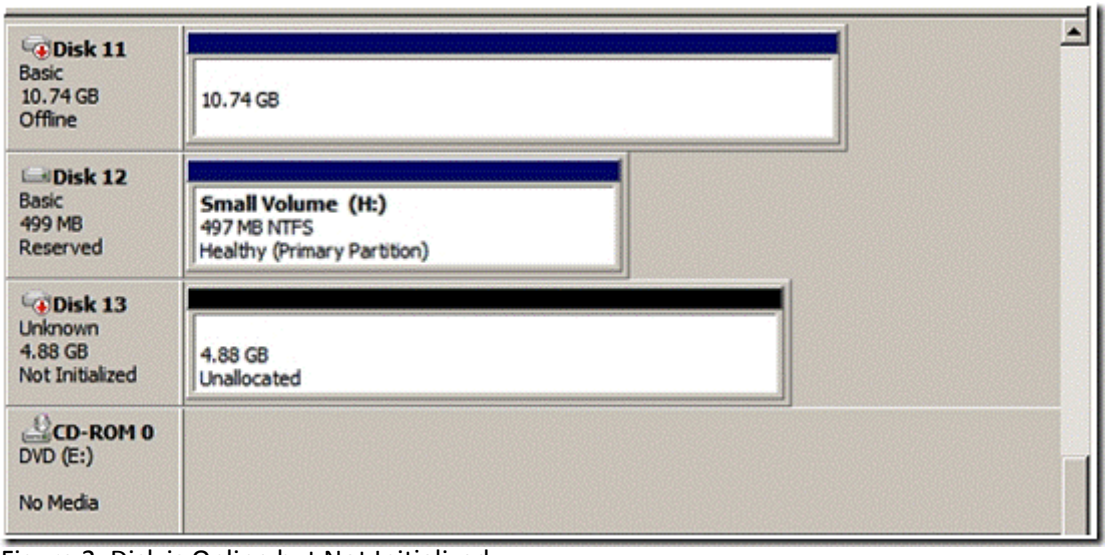


Figure 2: Disk is Online but Not Initialized

Right-click on the disk and select Initialize Disk (Figure 3)

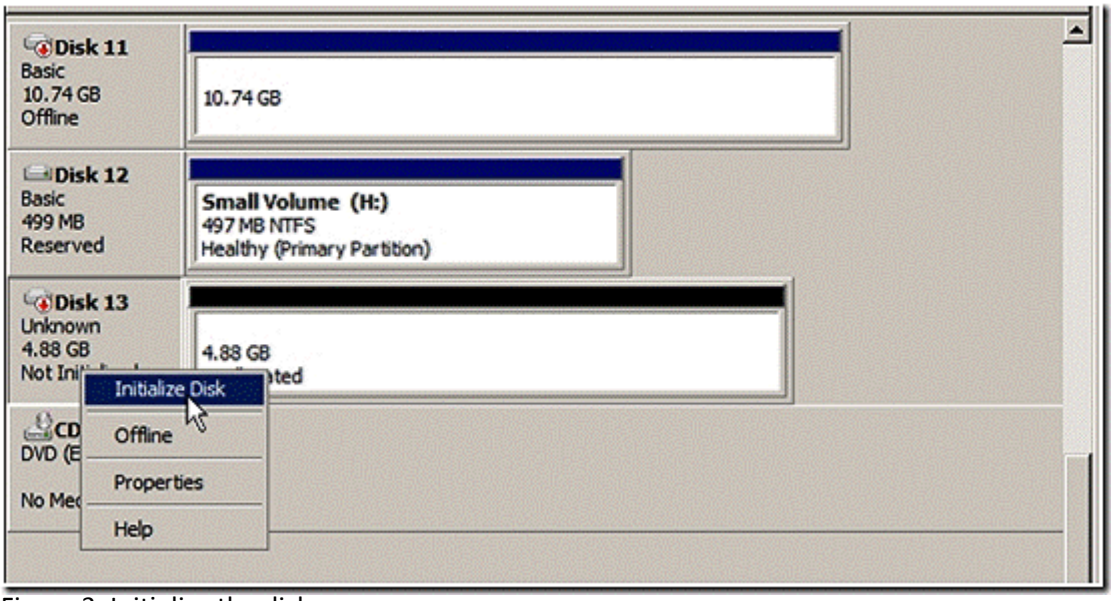


Figure 3: Initialize the disk

Select either an MBR or GPT partition type (Figure 4).

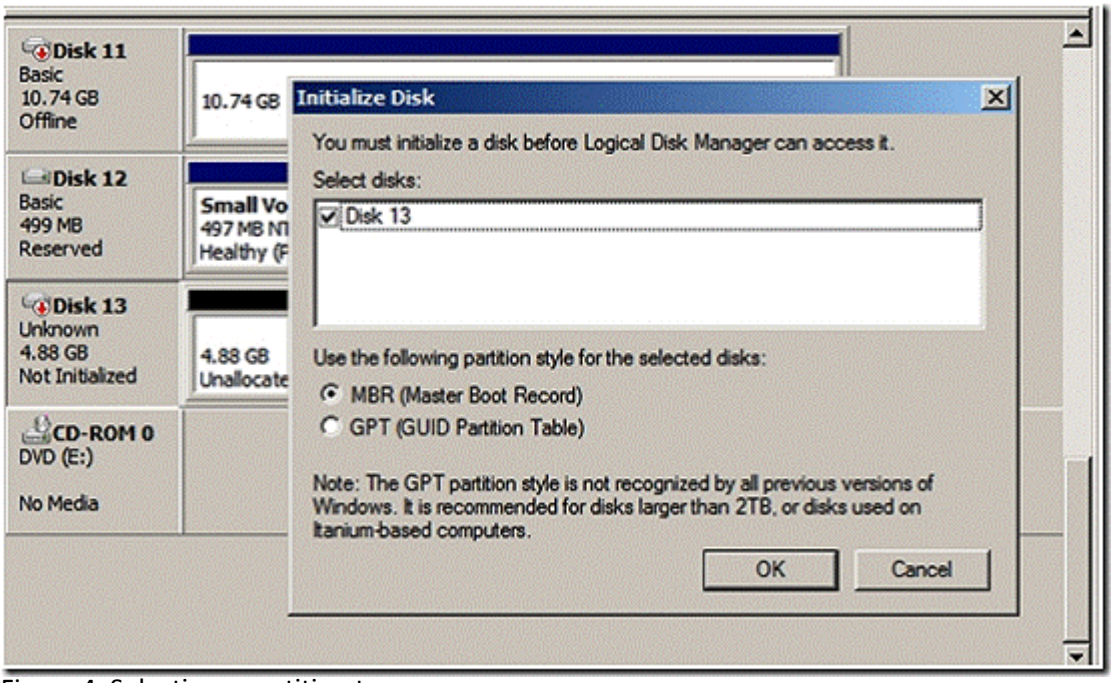


Figure 4: Selecting a partition type

Once a disk is initialized, it can once again be placed in an Offline state. If the disk is not in an Offline state, it will not be available for selection when configuring the Guest's storage. In order to configure a Pass-through disk in a Guest, you must select Attach a virtual disk later in the New Virtual Machine Wizard (Figure 5).

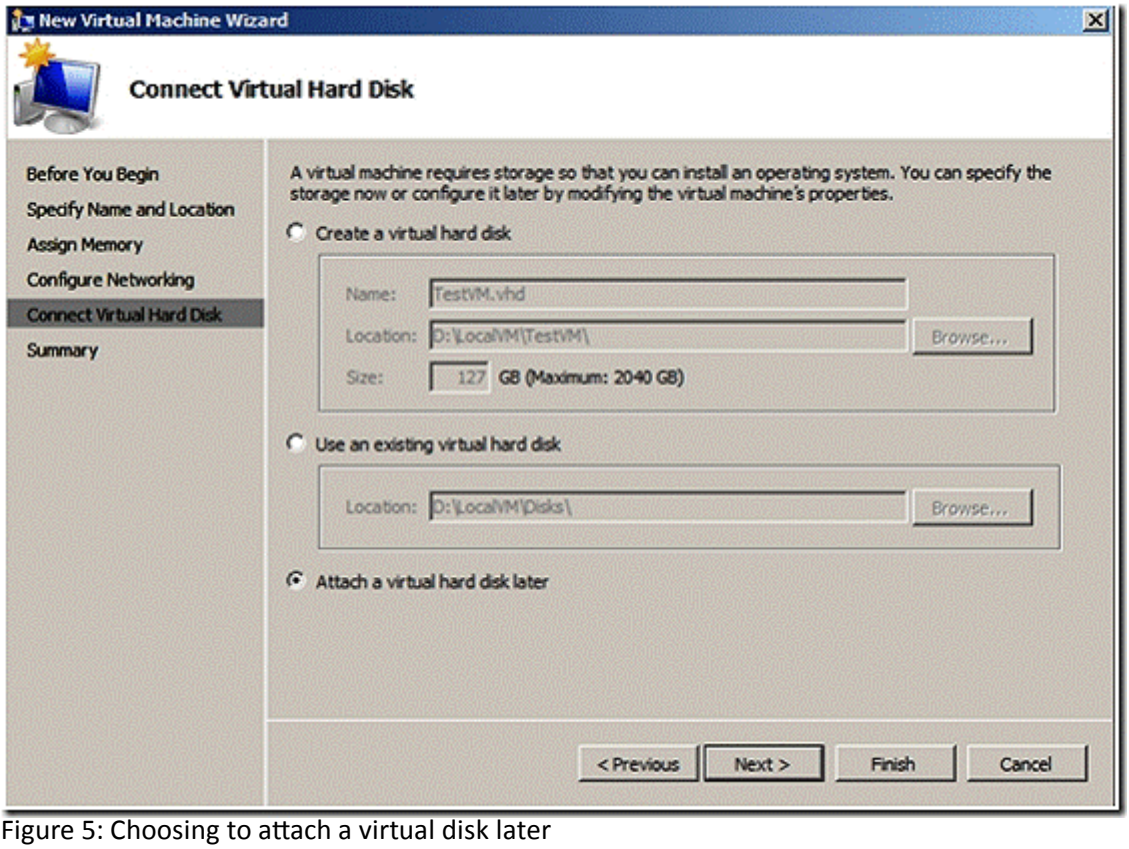


Figure 5: Choosing to attach a virtual disk later

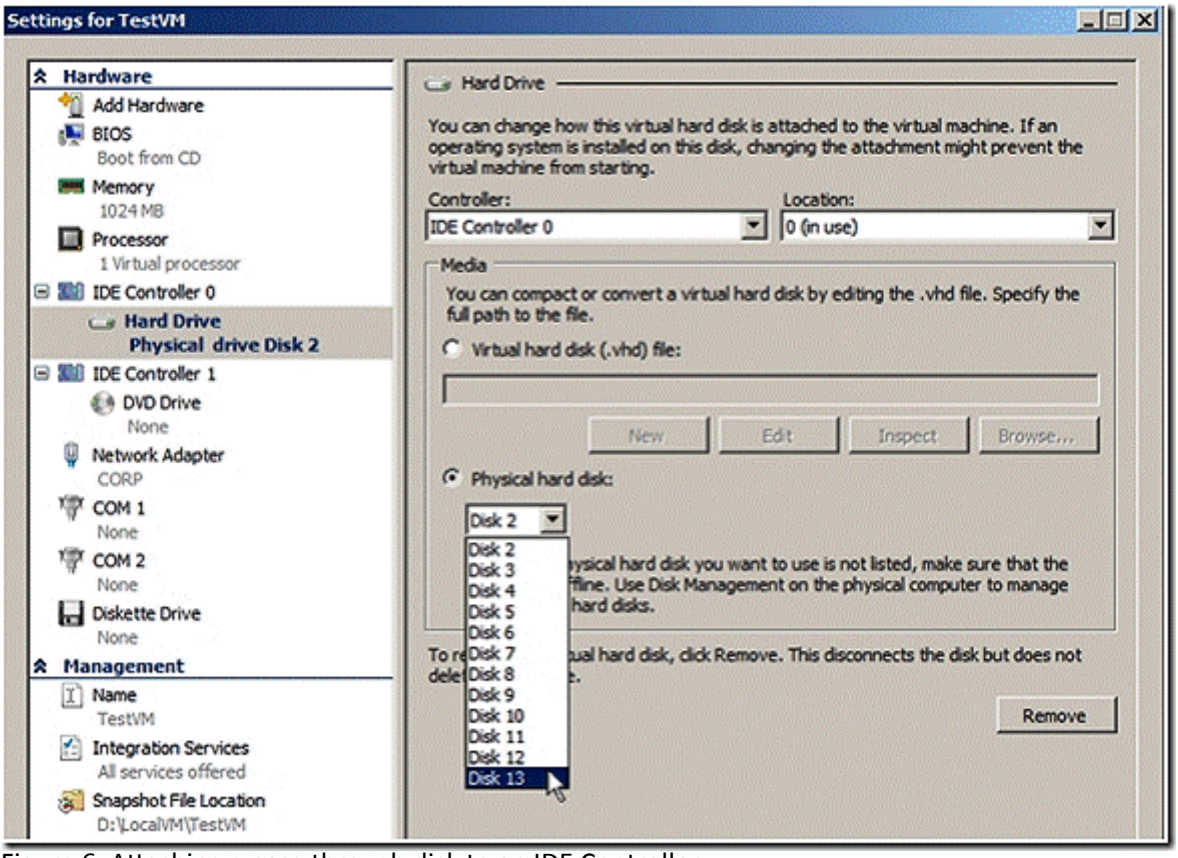


Figure 6: Attaching a pass-through disk to an IDE Controller

Note: If the disk does not appear in the drop down list, ensure the disk is Offline in the Disk Management interface (In Server CORE, use the diskpart.exe CLI).

Once the Pass-through disk is configured, the Guest can be started and data can placed on the drive. If an operating system will be installed, the installation process will properly prepare the disk. If the disk will be used for data storage, it must be prepared in the Guest operating system before data can be placed on it. If a Pass-through disk, being used to support an operating system installation, is brought Online before the Guest is started, the Guest will fail to start. When using Pass-through disks to support an operating system installation, provisions must be made for storing the Guest configuration file in an alternate location. This is because the entire Pass-through disk is consumed by the operating system installation. An example would be to locate the configuration file on another internal drive in the Hyper-V server itself. Or, if it is a cluster, the configuration file can be hosted on a separate cluster providing highly available file services. Be aware that Pass-through disks cannot be dynamically expanded. Additionally, when using Pass-through disks, you lose the capability to take snapshots, and finally, you cannot use differencing disks with Pass-through disks. Note: When using Pass-through disks in a Windows Server 2008 Failover Cluster, you must have the update documented in KB951308: Increased functionality and virtual machine control in the Windows Server 2008 Failover Cluster Management console for the Hyper-V role installed on all nodes in the cluster.

Source: http://blogs.technet.com/b/askcore/archive/2008/10/24/configuring-pass-through-disks-in-hyper-v.aspx

Question: 127

Your network contains a server named Server1 that has the Hyper-V server role installed. Server1 hosts a virtual machine (VM) named VM1 that runs Windows Server 2003 Service Pack 2 (SP2). VM1 is configured to use a 127-GB dynamically-expanding virtual hard disk (VHD). You need to add 500 GB of disk space to VM1. The solution must minimize the amount of downtime for VM1. What should you do?

A. Increase the size of the VHD drive.
B. Convert the VHD to a fixed-size disk.

C. Add a new VHD drive to a SCSI controller.
D. Add a new VHD drive to an IDE controller.

Answer: C

Dynamic virtual machine storage. Improvements to virtual machine storage include support for hot plug-in and hot removal of the storage on a SCSI controller of the virtual machine. By supporting the addition or removal of virtual hard disks and physical disks while a virtual machine is running, it is possible to quickly reconfigure virtual machines to meet changing requirements. Hot plug-in and removal of storage requires the installation of Hyper-V integration services (included in Windows Server 2008 R2) on the guest operating system.
Source: http://technet.microsoft.com/en-us/library/dd446676.aspx

Question: 128

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Hyper-V server role installed. Server1 hosts a virtual machine (VM) named VM1. You take a snapshot of VM1 at 05:00 and at 19:00. You use Hyper-V Manager to delete the snapshot taken at 05:00. You need to ensure that the files created by the 05:00 snapshot are deleted from the hard disk on Server1. What should you do?

A. At the command prompt, run the rmdir.exe command.
B. From Windows PowerShell, run the Remove-Item cmdlet.
C. From the Hyper-V Manager console, shut down VM1.
D. From the Hyper-V Manager console, right-click VM1 and click Revert.

Answer: C

Explanation:
When you delete a snapshot, the .avhd files that store the snapshot data remain in the storage location until the virtual machine is shut down, turned off, or put into a saved state. As a result, when you delete a snapshot, you will need to put the production virtual machine into one of those states at some point to be able to complete the safe removal of the snapshot.
Source: http://technet.microsoft.com/en-us/library/dd560637.aspx

Question: 129

Your network contains an Active Directory domain. The domain contains 20 member servers. The domain contains have two servers named Server1 and Server2 that run Windows Server 2008 R2. You connect Server1 and Server2 to a logical unit number (LUN) on a Storage Area Network (SAN). You create a failover cluster named Cluster1. You add Server1 and Server2 as nodes to Cluster1. You discover that there are no cluster disks available for a new clustered file server service on Cluster1. You need to ensure that you can add a clustered file server service to Cluster1. What should you do?

A. Enable cluster shared volumes.
B. Run the Provision Storage Wizard.
C. Configure Cluster1 to use a No Majority: Disk Only quorum configuration.
D. Configure Cluster1 to use a Node and File Share Majority quorum configuration.

Answer: D

Explanation:

Quorum configuration choices
You can choose from among four possible quorum configurations:
Node Majority (recommended for clusters with an odd number of nodes) Can sustain failures of half the nodes (rounding up) minus one. For example, a seven node cluster can sustain three node failures.
Node and Disk Majority (recommended for clusters with an even number of nodes) Can sustain failures of half the nodes (rounding up) if the disk witness remains online. For example, a six node cluster in which the disk witness is online could sustain three node failures. Can sustain failures of half the nodes (rounding up) minus one if the disk witness goes offline or fails. For example, a six node cluster with a failed disk witness could sustain two (3-1=2) node failures.
Node and File Share Majority (for clusters with special configurations)
Works in a similar way to Node and Disk Majority, but instead of a disk witness, this cluster uses a file share witness. Note that if you use Node and File Share Majority, at least one of the available cluster nodes must contain a current copy of the cluster configuration before you can start the cluster. Otherwise, you must force the starting of the cluster through a particular node.
No Majority: Disk Only (not recommended) Can sustain failures of all nodes except one (if the disk is online). However, this configuration is not recommended because the disk might be a single point of failure.
Source: http://technet.microsoft.com/en-us/library/cc731739.aspx

Question: 130

Your network contains two servers named Server1 and Server2 that run Windows Server 2008 R2. Server1 and Server2 have the Hyper-V server role and the Failover Clustering feature installed. You deploy a new virtual machine (VM) named VM1 on Server1. You need to ensure that VM1 is available if one of the Hyper-V servers fails. What should you do?

A. Install the Network Load Balancing (NLB) feature on VM1.
B. Install the Network Load Balancing (NLB) feature on Server1.
C. Install the Failover Clustering feature on VM1. From Failover Cluster Manager on VM1, click Configure a Service or Application.
D. From Failover Cluster Manager on Server1, click Configure a Service or Application.

Answer: D

Explanation:
To configure a virtual machine for high availability
1. Be sure that you have installed the Hyper-V role and have reviewed the steps in Checklist: Create a Clustered Virtual Machine. This procedure is a step in that checklist. 2. In the Failover Cluster Manager snap-in, if the cluster that you want to configure is not displayed, in the console tree, right-click Failover Cluster Manager, click Manage a Cluster, and then select or specify the cluster that you want. 3. If the console tree is collapsed, expand the tree under the cluster that you want to configure.
4. Click Services and Applications.
5. If you have already created the virtual machine, skip to step 6. Otherwise, use the New Virtual Machine
Wizard to create a virtual machine and configure it for high availability:
a. In the Action pane, click Virtual machines, point to Virtual machine, and then click a node. The virtual machine will initially be created on that node, and then be clustered so that it can move to another node or nodes as needed.
b. If the Before You Begin page of the New Virtual Machine Wizard appears, click Next.
c. Specify a name for the virtual machine, and then select Store the virtual machine in a different
location and specify a disk in shared storage or, if Cluster Shared Volumes is enabled, a Cluster Shared Volume (a volume that appears to be on the system drive of the node, under the \ClusterStorage folder).
d. Follow the instructions in the wizard. You can specify details (such as the amount of memory, the network, and the virtual hard disk file) now, and you can also add or change configuration details later.

e. When you click Finish, the wizard creates the virtual machine and also configures it for high availability.
Skip the remaining step in this procedure.
6. If you have already created the virtual machine and only want to configure it for high availability, first make sure that the virtual machine is not running. Then, use the High Availability Wizard to configure the virtual machine for high availability:
a. In the Action pane, click Configure a Service or Application.
b. If the Before You Begin page of the High Availability Wizard appears, click Next.
c. On the Select Service or Application page, click Virtual Machine and then click Next.
d. Select the virtual machine that you want to configure for high availability, and complete the wizard.
e. After the High Availability wizard runs and the Summary page appears, if you want to view a report of the tasks that the wizard performed, click View Report.
Source: http://technet.microsoft.com/en-us/library/dd759216.aspx

Question: 131

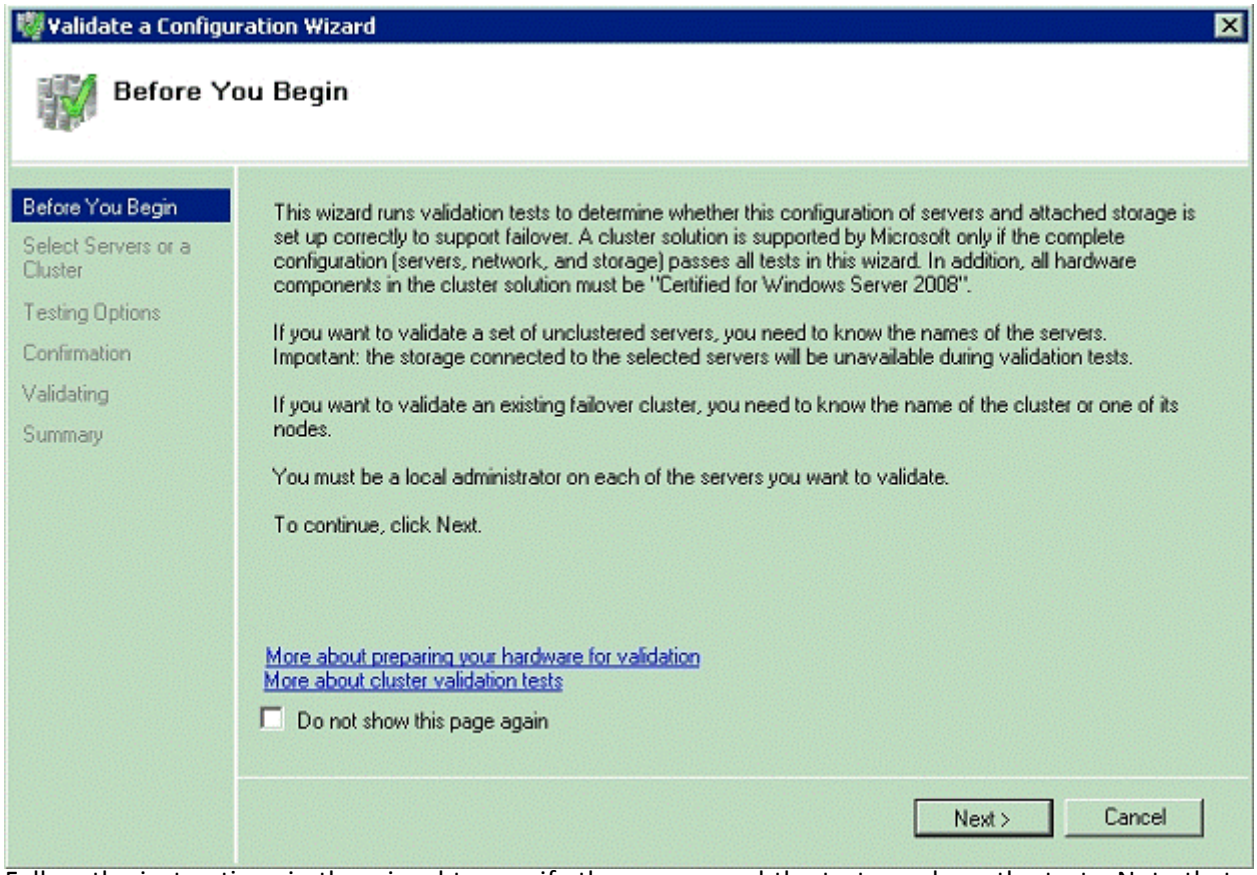
Your network contains an Active Directory domain. The domain contains two servers named Server1 and Server2. You connect Server1 and Server2 to a logical unit number (LUN) on a Storage Area Network (SAN). You need to ensure that you can use the LUN in a failover cluster. What should you do?

A. From Server Manager, run the Best Practices Analyzer.
B. From File Server Resource Manager, generate a storage report.
C. From Failover Cluster Manager, run the Validate a Configuration Wizard.
D. From Share and Storage Management, verify the advanced settings of the LUN.

Answer: C

Explanation:
Ensure that the disks (LUNs) that you want to use in the cluster are exposed to the servers you will cluster (and only those servers). You can use any of the following interfaces to expose disks or LUNs:
1. Microsoft Storage Manager for SANs (part of the operating system in Windows Server 2008). To use this interface, you need to contact the manufacturer of your storage for a Virtual Disk Service (VDS) provider package that is designed for your storage.
2. If you are using iSCSI, an appropriate iSCSI interface.
3. The interface provided by the manufacturer of the storage.
Source: http://technet.microsoft.com/es-es/library/dd197507(WS.10).aspx
Considerations when including storage tests : When cluster validation is performed on an already configured cluster, if the default tests (which include storage tests) are selected, only disk resources that are in an Offline state or are not assigned to a clustered service or application will be used for testing the storage. This builds in a safety mechanism, and the cluster validation wizard warns you when storage tests have been selected but will not run on storage in an Online state, that is, storage used by clustered services or applications. This is by design to avoid disruption to highly available services or applications that depend upon these disk resources being online. One scenario where Microsoft CSS may request you to run validation tests on production clusters is when there is a cluster storage failure that could be caused by some underlying storage configuration change or failure. By default, the wizard warns you if storage tests have been selected but will not be run on storage that is online, that is, storage used by clustered services or applications. In this situation, you can run validation tests (including storage tests) by creating or choosing a new logical unit number (LUN) from the same shared storage device and presenting it to all nodes. By testing this LUN, you can avoid disruption to clustered services and applications already online within the cluster and still test the underlying storage subsystem
.
How to run the cluster validation wizard for a failover cluster
To validate a new or existing failover cluster

Identify the server or servers that you want to test and confirm that the failover cluster feature is installed:
If the cluster does not yet exist, choose the servers that you want to include in the cluster, and make sure you have installed the failover cluster feature on those servers. To install the feature, on a server running Windows Server 2008 or Windows Server 2008 R2, click Start, click Administrative Tools, click Server Manager, and under Features Summary, click Add Features. Use the Add Features wizard to add the Failover Clustering feature. If the cluster already exists, make sure that you know the name of the cluster or a node in the cluster. Review network or storage hardware that you want to validate, to confirm that it is connected to the servers. For more information, see http://go.microsoft.com/fwlink/?LinkId=111555.
Decide whether you want to run all or only some of the available validation tests. For detailed information about the tests, see the topics listed in http://go.microsoft.com/fwlink/?LinkId=111554.
The following guidelines can help you decide whether to run all tests:
For a planned cluster with all hardware connected: Run all tests.
For a planned cluster with parts of the hardware connected: Run System Configuration tests, Inventory tests, and tests that apply to the hardware that is connected (that is, Network tests if the network is connected or Storage tests if the storage is connected).
For a cluster to which you plan to add a server: Run all tests. Before you run them, be sure to connect the networks and storage for all servers that you plan to have in the cluster.
For troubleshooting an existing cluster: If you are troubleshooting an existing cluster, you might run all tests, although you could run only the tests that relate to the apparent issue.
Important If a clustered service or application is using a disk when you start the wizard, the wizard will prompt you about whether to take that clustered service or application offline for the purposes of testing. If you choose to take a clustered service or application offline, it will remain offline until the tests finish. In the failover cluster snap-in, in the console tree, make sure Failover Cluster Management is selected and then, under Management, click Validate a Configuration.



Follow the instructions in the wizard to specify the servers and the tests, and run the tests. Note that when you run the cluster validation wizard on unclustered servers, you must enter the names of all the servers you want to test, not just one. The Summary page appears after the tests run.

While still on the Summary page, click View Report to view the test results.
To view the results of the tests after you close the wizard, see SystemRoot\Cluster\Reports\Validation Report date and time.html where SystemRoot is the folder in which the operating system is installed (for example, C:\Windows).
To view Help topics that will help you interpret the results, click More about cluster validation tests .
To view Help topics about cluster validation after you close the wizard, in the failover cluster snap-in, click Help, click Help Topics, click the Contents tab, expand the contents for the failover cluster Help, and click\ Validating a Failover Cluster Configuration
Source: http://technet.microsoft.com/en-us/library/cc732035(WS.10).aspx

Question: 132

Your network contains two servers named Server1 and Server2. The network contains a Storage Area Network (SAN). Server1 and Server2 each connect to two logical unit numbers (LUNs) on the SAN. You create a failover cluster named Cluster1. Server1 and Server2 are nodes in Cluster1. One of the LUNs is used as a witness disk. You plan to create 10 virtual machine (VM) instances in Cluster1. You need to ensure that each VM instance can be moved between nodes independently of the other VMs. How should you configure Cluster1?

A. Enable cluster shared volumes.
B. Modify the quorum configuration.
C. Create a clustered Generic Service instance.
D. Create a clustered Microsoft Distributed Transaction Coordinator (MSDTC) resource.

Answer: A

Explanation:
Storage: You must use shared storage that is compatible with Windows Server 2008 R2. A feature of failover clusters called Cluster Shared Volumes is specifically designed to enhance the availability and manageability of virtual machines. Cluster Shared Volumes are volumes in a failover cluster that multiple nodes can read from and write to at the same time. This feature enables multiple nodes to concurrently access a single shared volume. The Cluster Shared Volumes feature is only supported for use with Hyper-V and other technologies specified by Microsoft. On a failover cluster that uses Cluster Shared Volumes, multiple clustered virtual machines that are distributed across multiple cluster nodes can all access their Virtual Hard Disk (VHD) files at the same time, even if the VHD files are on a single disk (LUN) in the storage. This means that the clustered virtual machines can fail over independently of one another, even if they use only a single LUN. When Cluster Shared Volumes is not enabled, a single disk (LUN) can only be accessed by a single node at a time. This means that clustered virtual machines can only fail over independently if each virtual machine has its own LUN, which makes the management of LUNs and clustered virtual machines more difficult. For a two-node failover cluster, the storage should contain at least two separate volumes (LUNs), configured at the hardware level. Do not expose the clustered volumes to servers that are not in the cluster. One volume will function as the witness disk (described later in this section). One volume will contain the files that are being shared between the cluster nodes. This volume serves as the shared storage on which you will create the virtual machine and the virtual hard disk. To complete the steps as described in this document, you only need to expose one volume. For Cluster Shared Volumes, there are no special requirements other than the requirement for NTFS. For the partition style of the disk, you can use either master boot record (MBR) or GUID partition table (GPT).
Source: http://technet.microsoft.com/en-us/library/cc732181.aspx

Question: 132

Your network contains a single Active Directory domain. The domain contains two Active Directory sites named Site1 and Site2. You have a cluster named Cluster1. Cluster1 has two nodes named Server1 and Server2. Server1 is located

in Site1. Server2 is located in Site2. Cluster1 uses a file share witness that is located in Site1. Cluster1 hosts a clustered application named App1. The network in Site1 fails. You need to ensure that users can access App1. What should you do?

A. Force quorum on Server2.
B. Enable persistent mode for App1.
C. Modify the dependencies for App1.
D. Modify the failover settings for App1.

Answer: A

Explanation:
Force Quorum in a Single-Site or Multi-Site Failover Cluster
You can force quorum in a single-site or multi-site cluster. Forcing quorum means that you start the cluster even though only a minority of the elements that are required for quorum are in communication. This command is important to know for multi-site clusters with an odd number of nodes. The recommended design for a multi-site cluster has an even number of nodes, but it is possible to create a multi-site design using an odd number of nodes, with the majority of nodes at the main site. As with all configurations with an odd number of nodes, such a design should use the Node Majority quorum configuration. If you use this design and the main site goes down, to start the secondary site (which has a minority of the nodes) you will need to force quorum, that is, force all nodes which can communicate with each other to begin working together as a cluster.
To force quorum in a single-site or multi-site cluster
1. On a node that contains a copy of the cluster configuration that you want to use, open a Command Prompt window. Important The choice of node can be important when you are forcing quorum, because one node could potentially have an older copy of the cluster configuration database than another node or nodes. The cluster will use the copy of the cluster configuration that is on the node on which you perform this procedure. The cluster will then replicate that copy to all other nodes.
2. On that node, type the following command: net start clussvc /fq
Additional considerations
To open a Command Prompt window, click Start, right-click Command Prompt, and then either click Run as administrator or click Open. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.
When a cluster is forced to start without quorum it continually looks to add nodes to the cluster and is in a special "forced" state. Once it has majority, the cluster moves out of the forced state and behaves normally, which means it is not necessary to rerun the command without the /fq option. If the cluster moves out of the forced state, loses a node, and drops below quorum, it will go offline again. At that point, to bring it online again while it does not have quorum would require running the command again with the /fq option.
Source: http://technet.microsoft.com/nl-nl/library/dd197500.aspx

Question: 134

Your network contains two servers named Server1 and Server2 that run Windows Server 2008 R2. Server1 and Server2 are configured as a failover cluster named Cluster1. Cluster1 hosts a clustered application named App1. App1 has a physical disk resource named Cluster Disk 1. You need to use the Chkdsk tool to fix all of the errors on Cluster Disk 1. What should you do first?

A. From Disk Management, take Cluster Disk 1 offline.
B. From Disk Management, disable write caching for Cluster Disk 1.
C. From Failover Cluster Manager, modify the dependencies for Cluster Disk 1.
D. From Failover Cluster Manager, enable maintenance mode for Cluster Disk 1.

Answer: D

Explanation:
Run a Disk Maintenance Tool Such as Chkdsk on a Clustered Disk
To run a disk maintenance tool such as Chkdsk on a disk or volume that is configured as part of a clustered service, application, or virtual machine, you must use maintenance mode. When maintenance mode is on, the disk maintenance tool can finish running without triggering a failover. If you have a disk witness, you cannot use maintenance mode for that disk. Maintenance mode works somewhat differently on a volume in Cluster Shared Volumes than it does on other disks in cluster storage, as described in Additional considerations, later in this topic.
Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure
To run a disk maintenance tool such as Chkdsk on a clustered disk
1. In the Failover Cluster Manager snap-in, if the cluster is not displayed, in the console tree, right-click Failover Cluster Manager, click Manage a Cluster, and select or specify the cluster you want.
2. If the console tree is collapsed, expand the tree under the cluster that uses the disk on which you want run a disk maintenance tool.
3. In the console tree, click Storage.
4. In the center pane, click the disk on which you want to run the disk maintenance tool.
5. Under Actions, click More Actions, and then click the appropriate command:
If the disk you clicked is under Cluster Shared Volumes and contains multiple volumes, click Maintenance, and then click the command for the appropriate volume. If prompted, confirm your action.
If the disk you clicked is under Cluster Shared Volumes and contains one volume, click Maintenance, and then click Turn on maintenance mode for this volume . If prompted, confirm your action.
If the disk you clicked is not under Cluster Shared Volumes, click Turn on maintenance mode for this disk.
6. Run the disk maintenance tool on the disk or volume. When maintenance mode is on, the disk maintenance tool can finish running without triggering a failover.
7. When the disk maintenance tool finishes running, with the disk still selected, under Actions, click More Actions, and then click the appropriate command:
If the disk you clicked is under Cluster Shared Volumes and contains multiple volumes, click Maintenance, and then click the command for the appropriate volume. If the disk you clicked is under Cluster Shared Volumes and contains one volume, click Maintenance, and then click Turn off maintenance mode for this volume .
If the disk you clicked is not under Cluster Shared Volumes, click Turn off maintenance mode for this disk.
Source: http://technet.microsoft.com/en-us/library/cc772587.aspx

Question: 135

Your network contains a Windows Server 2003 server cluster named Cluster1. Cluster1 hosts a print server instance named Print1. You deploy a Windows Server 2008 R2 failover cluster named Cluster2. You configure Cluster2 to use the physical disk resource used by Print1. From Cluster2, you run the Migrate a Cluster Wizard to migrate Print1 to Cluster2. You need to ensure that Print1 runs on Cluster2. What should you do first?

A. On Cluster1, take Print1 offline.
B. On Cluster1, modify the failover settings of Print1.
C. On Cluster2, modify the failover settings of Print1.
D. On Cluster2, modify the preferred owner settings of Print1.

Answer: A

Question: 136

Your network contains a server named Server1.

You add a new hard disk to Server1.
When you run the Provision Storage Wizard, you do not see the new disk. You need to ensure that you can provision the new disk by using the Provision Storage Wizard.
What should you do?

A. At the command prompt, run chkdsk.exe /f.
B. From Disk Management, initialize the disk.
C. From Services, restart the Virtual Disk service.
D. From Storage Explorer, click Refresh SAN View.

Answer: B

Question: 137

Your network contains a single Active Directory domain. The domain contains a server named Server1 that runs Windows Server 2008 R2. Server1 has an iSCSI host bus adapter that connects to an iSCSI target. You install an additional iSCSI host bus adapter on Server1. You need to ensure that Server1 can access the iSCSI target if a host bus adapter fails. What should you do first?

A. At the command prompt, run mpclaim.exe -l m 6.
B. Install the Multipath I/O feature.
C. Bridge the iSCSI host bus adapters.
D. Install the Internet Storage Name Server (iSNS) feature.

Answer: B

Explanation:
About MPIO
Microsoft Multipath I/O (MPIO) is a Microsoft-provided framework that allows storage providers to develop multipath solutions that contain the hardware-specific information needed to optimize connectivity with their storage arrays. These modules are called device-specific modules (DSMs). The concepts around DSMs are discussed later in this document. MPIO is protocol-independent and can be used with Fibre Channel, Internet SCSI (iSCSI), and Serial Attached SCSI (SAS) interfaces in Windows ServerR 2008 and Windows Server 2008 R2.
Multipath solutions in Windows Server 2008 R2
When running on Windows Server 2008 R2, an MPIO solution can be deployed in the following ways: By using a DSM provided by a storage array manufacturer for Windows Server 2008 R2 in a Fibre Channel, iSCSI, or SAS shared storage configuration. By using the Microsoft DSM, which is a generic DSM provided for Windows Server 2008 R2 in a Fibre Channel, iSCSI, or SAS shared storage configuration.
High availability through MPIO
MPIO allows WindowsR to manage and efficiently use up to 32 paths between storage devices and the Windows host operating system. MPIO provides fault tolerant connectivity to storage. By employing MPIO users are able to mitigate the risk of a system outage at the hardware level. MPIO provides the logical facility for routing I/O over redundant hardware paths connecting server to storage. These redundant hardware paths are made up of components such as cabling, host bus adapters (HBAs), switches, storage controllers, and possibly even power. MPIO solutions logically manage these redundant connections so that I/O requests can be rerouted if a component along one path fails. As more and more data is consolidated on storage area networks (SANs), the potential loss of access to storage resources is unacceptable. To mitigate this risk, high availability solutions, such as MPIO, have now become a requirement.
Source: http://technet.microsoft.com/en-us/library/ee619734(WS.10).aspx

Question: 138

Your network contains a single Active Directory domain. The domain contains a server named Server1 that runs Windows Server 2008 R2. Server1 has two unallocated disks. You need to create a mirrored volume. Which tool should you use?

A. Disk Management
B. File Server Resource Manager
C. Share and Storage Management
D. Storage Explorer

Answer: A

Section: Storage Management
Explanation:
To create a mirrored volume
1. Open Server Manager (Local).
2. In the console tree, click Server Manager (Local), click Storage, and then click Disk Management.
3. Right-click the unallocated space on one of the dynamic disks on which you want to create the mirrored volume, and then click New Volume.
4. In the New Volume Wizard, click Next, click Mirrored, and then follow the instructions on your screen.
Notes
To perform this procedure on a local computer, you must be a member of the Backup Operators group or Administrators group on the local computer, or you must have been delegated the appropriate authority. To perform this procedure remotely, you must be a member of the Backup Operators group or Administrators group on the remote computer. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure. As a security best practice, consider using Run as to perform this procedure.
To open Server Manager, click Start, click Administrative Tools, and then click Server Manager.
You need two dynamic disks to create a mirrored volume.
You can mirror an existing simple volume.
Mirrored volumes are fault tolerant and use RAID-1, which provides redundancy by creating two identical copies of a volume.
Mirrored volumes cannot be extended.
Both copies (mirrors) of the mirrored volume share the same drive letter.
Source: http://technet.microsoft.com/en-us/library/cc776202.aspx

Question: 139

Your network contains a single Active Directory domain. The domain contains a server named Server1 that runs Windows Server 2008 R2. An administrator connects Server1 to an iSCSI target. You restart Server1 and discover that the iSCSI target is not connected. You need to ensure that Server1 automatically connects to the iSCSI target when you restart the server. What should you do?

A. From the iSCSI Initiator console, add Server1 as a target portal.
B. From the iSCSI Initiator console, add the target to the favorite targets list.
C. From the Storage Explorer console, add a new iSCSI initiator.
D. From the Storage Explorer console, disable the default Discovery Domain Set.

Answer: B

By marking a target as a favorite target, Microsoft iSCSI Initiator configures software and hardware initiators to always

attempt to reconnect to a target whenever the computer is rebooted. The login information that is needed to connect to the favorite targets (for example, Challenge-Handshake Authentication Protocol (CHAP) secrets, portal information, etc.) is captured when you log in, and is saved by the software and hardware initiators in non-volatile storage. Hardware initiators can initiate a reconnection early in the boot process while the Microsoft Software Initiator kernel mode driver initiates a reconnection as soon as the Windows TCP/IP stack and the Microsoft iSCSI Initiator service loads.
Source: http://technet.microsoft.com/en-us/library/dd759126.aspx
Favorite targets
Microsoft iSCSI Initiator supports favorite (formerly called persistent) targets. By using common APIs and UI, Microsoft iSCSI Initiator can configure software and hardware initiators to always reconnect to a target when the computer is rebooted. Consequently, this requires that the devices on the target are connected to the computer at all times. The logon information that is needed to connect to the favorite targets (for example, CHAP secrets and portal) is captured when the persistent logon is performed by the administrator and saved by the software and hardware initiators in non-volatile storage. Hardware initiators can initiate reconnection early in the boot process, but the kernel-mode driver in Microsoft iSCSI Initiator initiates reconnection when the Windows TCP/IP stack and Microsoft iSCSI Initiator load.
Source: http://technet.microsoft.com/en-us/library/ee338477(WS.10).aspx

Question: 140

Your network contains a server named Server1. Server1 has three hard disk drives. Two hard disk drives named C and E are configured as simple volumes. The third hard disk drive contains 500 GB of unallocated space.
Drive E hosts a shared folder named Folder1.
Users report that they fail to save files to Folder1.
You discover that drive E has no free space.
You need to ensure that users can save files to Folder1.
What should you do?

A. From the Disk Management console, run the Add Mirror wizard.
B. From the Disk Management console, run the Extend Volume Wizard.
C. From the Share and Storage Management console, run the Provision Storage Wizard.
D. From the Share and Storage Management console, run the Provision a Shared Folder Wizard.

Answer: B

Explanation:
Extend a Simple or Spanned Volume
A spanned volume is a dynamic volume that consists of disk space on more than one physical disk. If a simple volume is not a system volume or boot volume, you can extend across additional disks. If you extend a simple volume across multiple disks, it becomes a spanned volume. You can extend a volume only if it does not have a file system or if it is formatted using the NTFS file system. You cannot extend volumes formatted using FAT or FAT32.
Backup Operator or Administrator is the minimum membership required to complete the actions below.
Extending a simple or spanned volume
1. In Disk Management, right-click the simple or spanned volume you want to extend.
2. Click Extend Volume.
3. Follow the instructions on your screen.
Source: http://technet.microsoft.com/en-us/library/cc753058.aspx

Question: 141

Your network contains a server named Server1 that has two volumes named C and D.
You add a new volume. You need to ensure that you can access data on the new volume by using the path D:\data.
What should you do?

A. From Disk Management, create a volume mount point.
B. From Disk Management, attach a virtual hard disk (VHD).
C. At the command prompt, run the diskraid.exe command and specify the /v parameter.
D. At the command prompt, run the dism.exe command and specify the /mount-wim parameter.

Answer: A

Explanation:
Assign a mount point folder path to a drive
You can use Disk Management to assign a mount-point folder path (rather than a drive letter) to the drive. Mount-point folder paths are available only on empty folders on basic or dynamic NTFS volumes.
Backup Operator or Administrator is the minimum membership required.
Assigning a mount-point folder path to a drive
1. In Disk Manager, right-click the partition or volume where you want to assign the mount-point folder path, and then click Change Drive Letter and Paths.
2. Do one of the following:
To assign a mount-point folder path, click Add. Click Mount in the following empty NTFS folder , type the path to an empty folder on an NTFS volume, or click Browse to locate it.
To remove the mount-point folder path, click it and then click Remove.
Additional considerations
If you are administering a local or remote computer, you can browse NTFS folders on that computer.
When assigning a mount-point folder path to a drive, use Event Viewer to check the system log for any Cluster service errors or warnings indicating mount point failures. These errors would be listed as ClusSvc in the Source column and Physical Disk Resource in the Category column.
Source: http://technet.microsoft.com/en-us/library/cc753321.aspx

Question: 142

Your network contains a server named Server1.
You start Server1 by using a Microsoft Windows Preinstallation Environment (Windows PE) image. You copy a virtual hard disk (VHD) image named VHD1 to Server1. VHD1 contains a Windows Server 2008 R2 image.
You need to configure Server1 to start from VHD1.
Which tool should you use?

A. Bcdedit
B. Bootcfg
C. Diskpart
D. Dism

Answer: A

Explanation:
To add a native-boot VHD to an existing Windows 7 boot menu
If you are deploying the VHD to a computer with an existing Windows 7 or Windows ServerR 2008 R2 installation, you can use the BCDedit tool to make the new VHD bootable and add it to the boot menu. For more information about using the BCDedit tool, see this Microsoft Web site.

1. Copy an existing boot entry for a Windows 7 installation. You will then modify the copy for use as the VHD boot entry. At a command prompt, type:
bcdedit /copy {default} /d "vhd boot (locate)" When the BCDedit command completes successfully, it returns a {GUID} as output in the Command Prompt window.
2. Locate the {GUID} in the command-prompt output for the previous command. Copy the GUID, including the braces, to use in the following steps.
3. Set the device and osdevice options for the VHD boot entry. At a command prompt, type:
bcdedit /set {guid} device vhd=[locate]\windows7.vhd
bcdedit /set {guid} osdevice vhd=[locate]\windows7.vhd
4. Set the boot entry for the VHD as the default boot entry. When the computer restarts, the boot menu will display all of the Windows installations on the computer and boot into the VHD after the operating-system selection countdown completes. At a command prompt, type:
bcdedit /default {guid}
5. Some x86-based systems require a boot configuration option for the kernel in order to detect certain hardware information and successfully native-boot from a VHD. At a command prompt, type: bcdedit /set {guid} detecthal on
Source: http://technet.microsoft.com/en-us/library/dd799299.aspx

Question: 143

Your network contains a server named Server1 that runs Windows Server 2008 R2.
You add a new 3-terabyte hard disk to Server1.
You need to create a 3-terabyte volume.
What should you do first?

A. Disable write caching for the hard disk.
B. Initialize the disk as a Master Boot Record (MBR) disk.
C. Initialize the disk as a GUID Partition Table (GPT) disk.
D. Disable direct memory access (DMA) for the hard disk controller.

Answer: C

Explanation:
A GPT disk uses the GUID partition table (GPT) disk partitioning system. A GPT disk offers these benefits: Allows up to 128 primary partitions. Master Boot Record (MBR) disks can support up to four primary partitions and an additional 124 partitions inside extended partitions.
Allows a much larger partition size--greater than 2 terabytes (TB), which is the limit for MBR disks.
Provides greater reliability because of replication and cyclical redundancy check (CRC) protection of the partition table can be used as a storage volume on all x64-based platforms, including platforms running Windows XP Professional x64 Edition. Starting with Windows Server 2003 SP1, GPT disks can also be used as a storage volume on x86-based Windows platforms. Can be used as a boot volume on x64-based editions of Windows 7, Windows Vista, and Windows Server 2008. Starting with Windows Server 2003 SP1, GPT disks can also be used as a boot volume on Itaniumbased\ systems.
Note: Windows only supports booting from a GPT disk on systems that contain Unified Extensible Firmware Interface (UEFI) boot firmware.
Source: http://www.microsoft.com/whdc/device/storage/GPT-on-x64.mspx

Question: 144

Your network contains a server named Server1 that runs Windows Server 2008 R2.
You install three new hard disk drives on Server1. The drives are identical in size.

You need to create a volume by using the three new disk drives.
The volume must meet the following requirements:
Provide the maximum amount of usable storage.
Provide the fastest read/write performance available.
Which type of volume should you create?

A. mirrored
B. RAID-5
C. spanned
D. striped

Answer: D

Explanation:
RAID 0 - Striped
+ Fast, reads and writes to all disks at the same time
+ Flexible, can be used with any number of disks
+ Cheap, uses all disks in the array for data.
- Non redundant
- Dangerous: failure risk increases with every disk added to the array. If one disk failes all data is lost.
RAID 1 - Mirrored
- Slow, needs to write the same data to all disks,
- Inflexible, needs an even number of disks.
- Costly, only 50% of the available total disk space can be used (the other 50% is used for the mirror)
+ Redundant
+ Safe
RAID 5 - Striped with distributed parity
+ Fast, reads and writes to all - 1 disks at the same time
+ Flexible, can be used with any number of disks, but needs atleast 3.
+ Less expensive, uses all - 1 disks in the array for data. Penalty is max 33%, penalty shrinks with every disk added to the array.
+ Redundant
+ Safe
Spanned - Just a Bunch Of Disks
- Slow, writes to one disk, untill it is filled up.
+ Flexible, can be used with any number of disks
+ Cheap, used all disks in the array for data.
- Non redundant
- Dangerous: failure risk increases with every disk added to the array. If one disk failes all data may be lost.

Question: 145

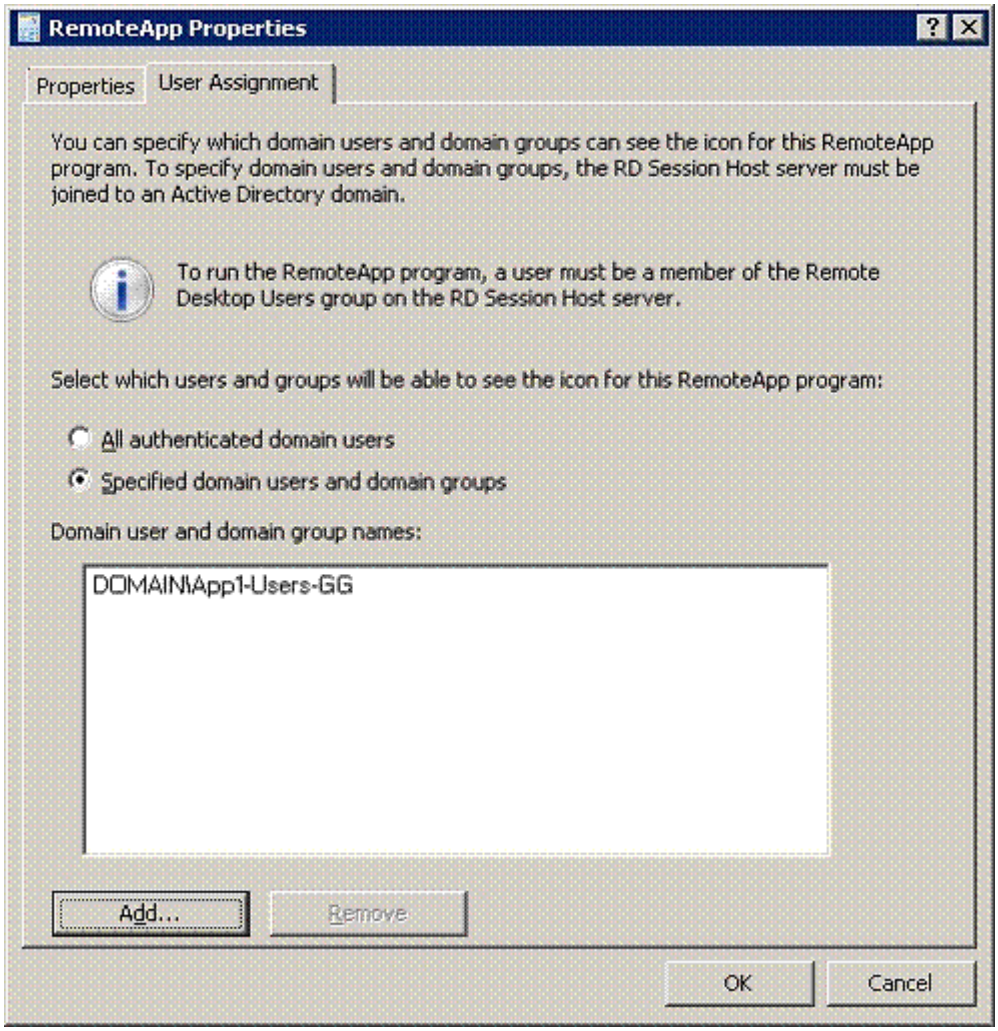
Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the following Remote Desktop Services (RDS) role services installed:
· Remote Desktop Session Host (RD Session Host)
· Remote Desktop Web Access (RD Web Access)
You publish 10 RemoteApp programs on Server1 by using RD Web Access. You need to ensure that when users log on to the RD Web Access page, they see only the RemoteApp programs assigned to them.
What should you modify from RemoteApp Manager?

A. the properties of each RemoteApp program

B. the RD Gateway Settings
C. the RDP Settings
D. the RD Session Host Server Settings

Answer: A

Explanation:



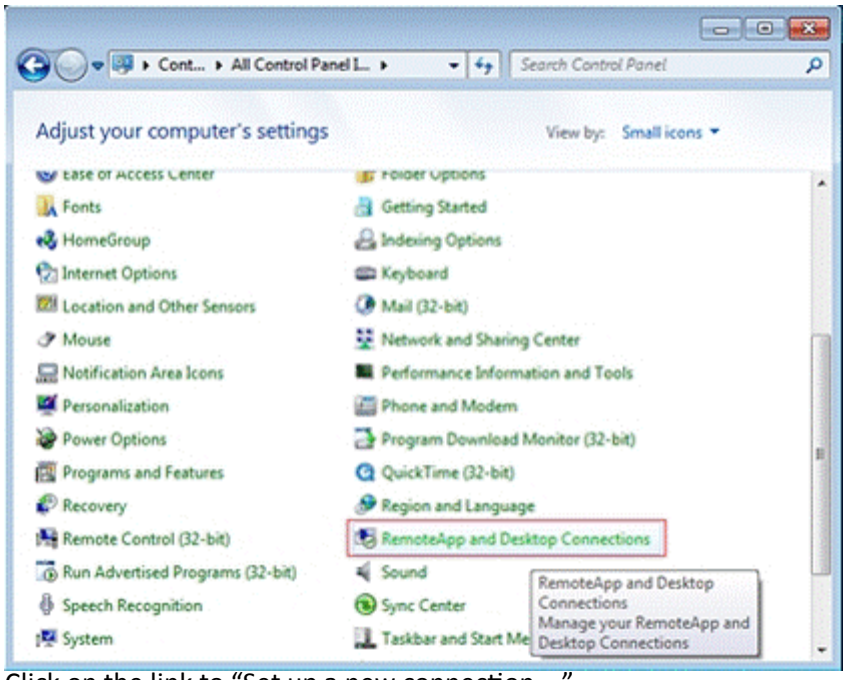
Question: 146

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 and a client computer named Computer1. Server1 runs Windows Server 2008 R2. Computer1 runs Windows 7. Server1 has the Remote Desktop Session Host (RD Session Host) role service and the Remote Desktop Web Access (RD Web Access) role service installed. You need to ensure that new RemoteApp programs published on Server1 are automatically added to the Start menu on Computer1.
What should you do?

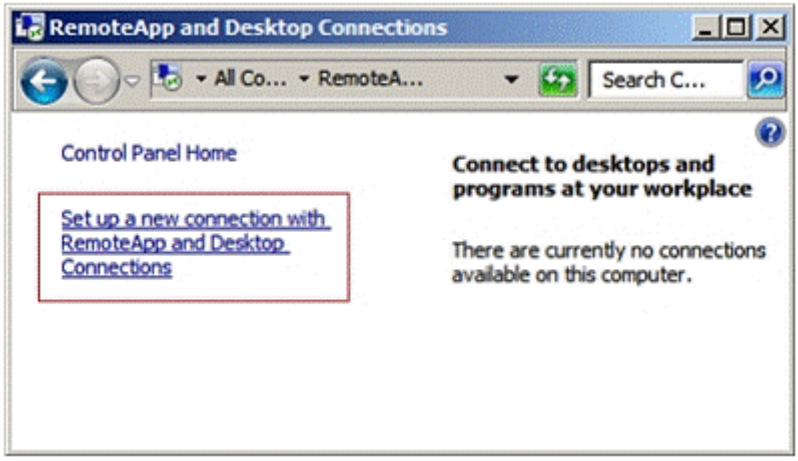
A. From RemoteApp and Desktop Connections on Server1, set up a new connection.
B. From RemoteApp and Desktop Connections on Computer1, set up a new connection.
C. From RemoteApp Manager on Server1, create an .rdp file. Deploy the .rdp file to Computer1.
D. From RemoteApp Manager on Server1, create a Windows Installer package. Deploy the package to Computer1.

Answer: B

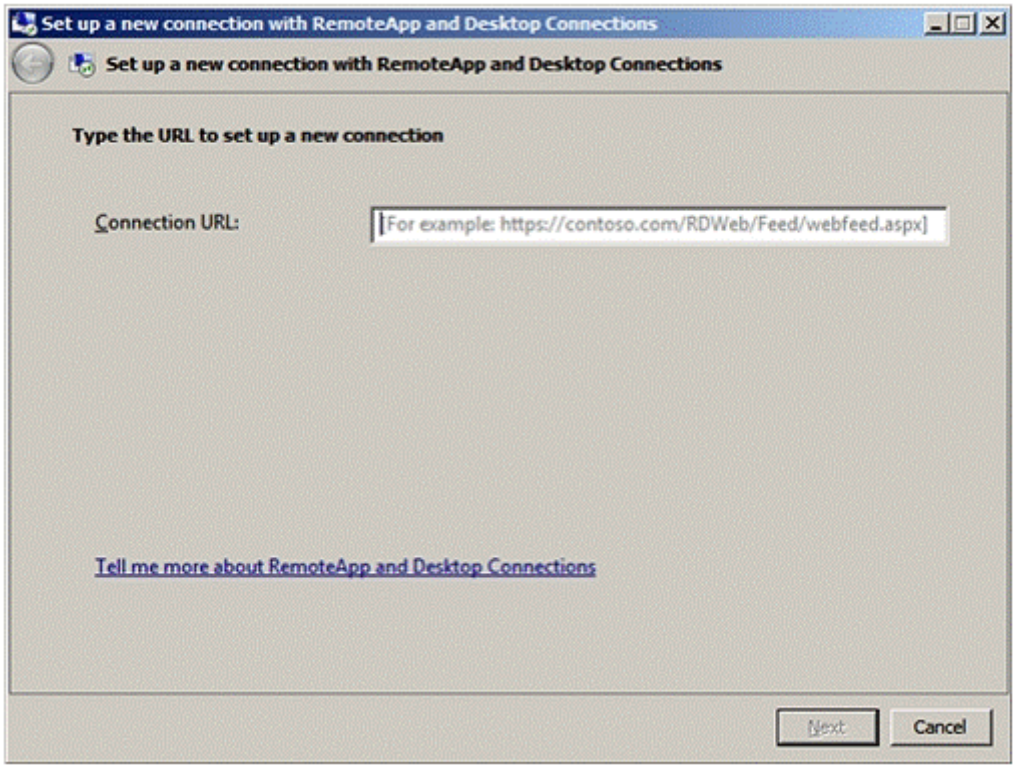
Explanation:
RemoteApp and Desktop Connection
In Windows Server 2008, Terminal Services introduced RemoteApp programs, which are programs that are accessed remotely through Remote Desktop Services and appear as if they are running on the end user's local computer. In Windows Server 2008 R2, Remote Desktop Services provides administrators the ability to group and personalize RemoteApp programs as well as virtual desktops and make them available to end users on the
Start menu of a computer that is running WindowsR 7. This new feature is called RemoteApp and Desktop Connection. RemoteApp and Desktop Connection provides a personalized view of RemoteApp programs, session-based desktops, and virtual desktops to users. When a user starts a RemoteApp program or a session-based desktop, a Remote Desktop Services session is started on the Remote Desktop Session Host (RD Session Host) server that hosts the remote desktop or RemoteApp program. If a user connects to a virtual desktop, a remote desktop connection is made to a virtual machine that is running on a Remote Desktop Virtualization Host (RD Virtualization Host) server. To configure which RemoteApp programs, session-based desktops, and virtual desktops are available through RemoteApp and Desktop Connection, you must add the Remote Desktop Connection Broker (RD Connection Broker) role service on a computer that is running Windows Server 2008 R2, and then use Remote Desktop Connection Manager. In Windows 7 and Windows Server 2008 R2, you configure RemoteApp and Desktop Connection by using Control Panel. After RemoteApp and Desktop Connection is configured, RemoteApp programs, session-based desktops, and virtual desktops that are part of this connection are available to users on the Start menu of their computer. Any changes that are made to RemoteApp and Desktop Connection, such as adding or removing RemoteApp programs or virtual desktops, are automatically updated on the client and on the Start menu.
Source: http://technet.microsoft.com/en-us/library/dd560650(WS.10).aspx
Step-by-Step Client configuration of a RemoteApp and Desktop Connection web feed via the control panel.
The first step is to open the RemoteApp and Desktop Connection Applet:



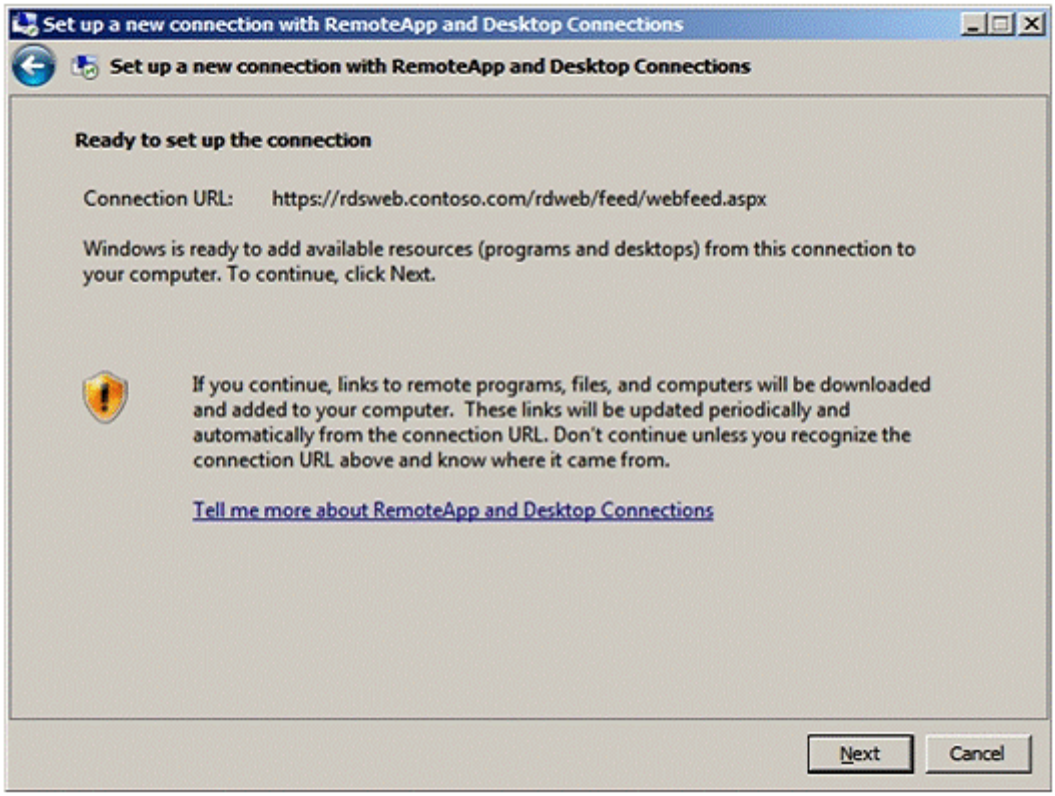
Click on the link to “Set up a new connection …”



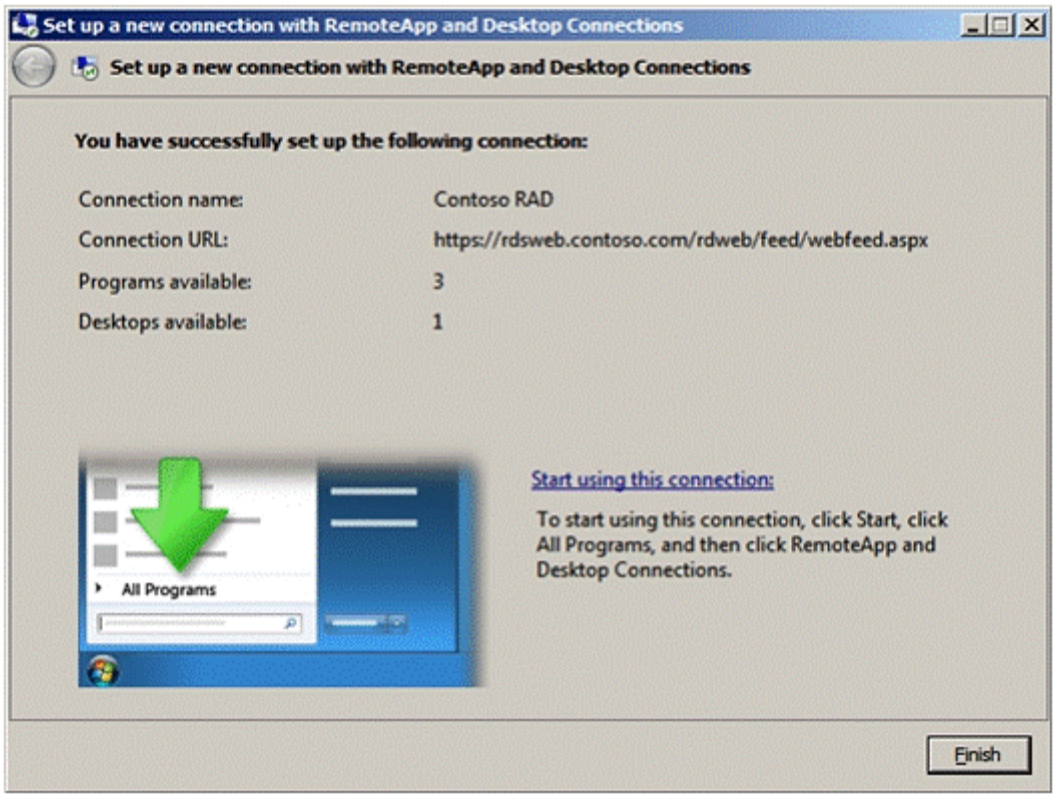
Specify the URL for the web feed:



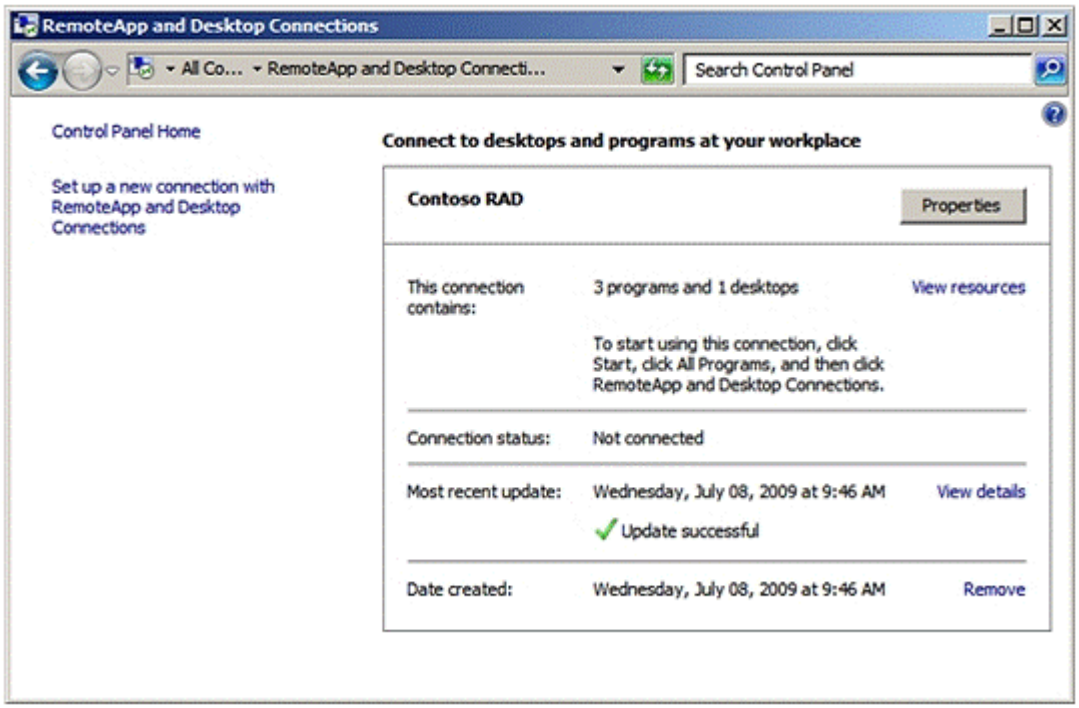
Click Next and confirm your selection:



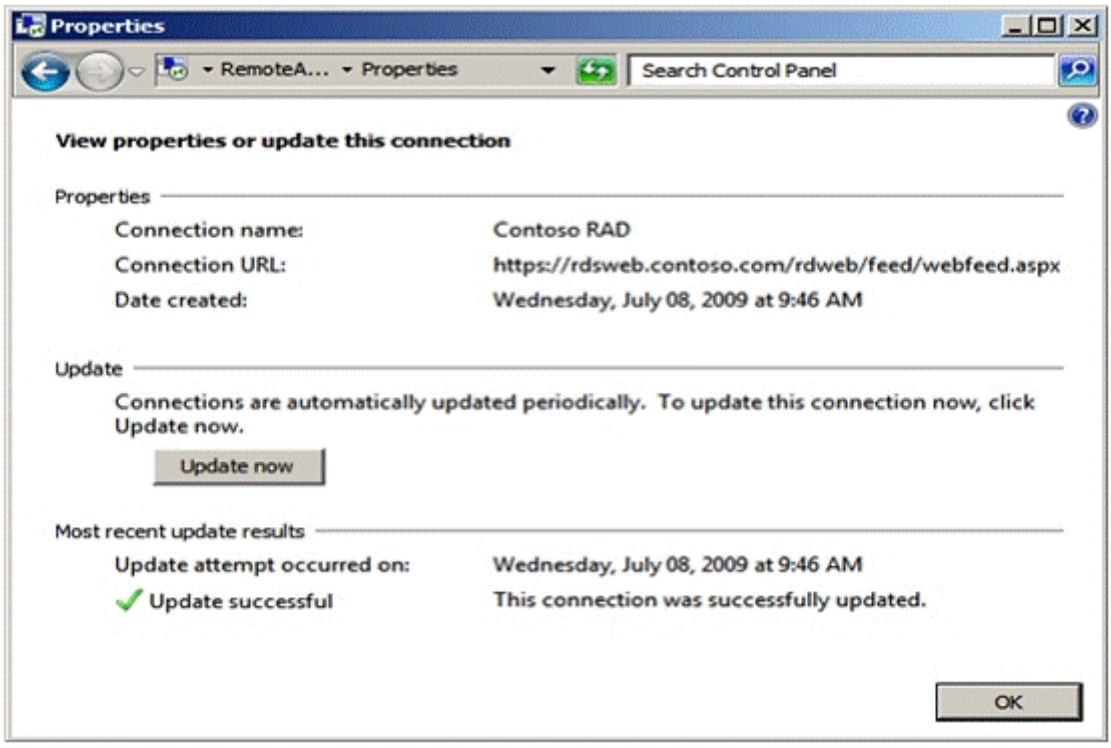
You receive confirmation that the connection was successfully added:



And you can then see the connection in the applet:



If you click on the Properties button, you can see the connection's details and you also have an "Update Now" button that you can use to manually update the list of RemoteApps and Desktops:



Source: http://blogs.technet.com/b/askperf/archive/2009/10/14/windows-7-windows-server-2008-r2-remoteapp-and-desktop-connection. aspx

Question: 147

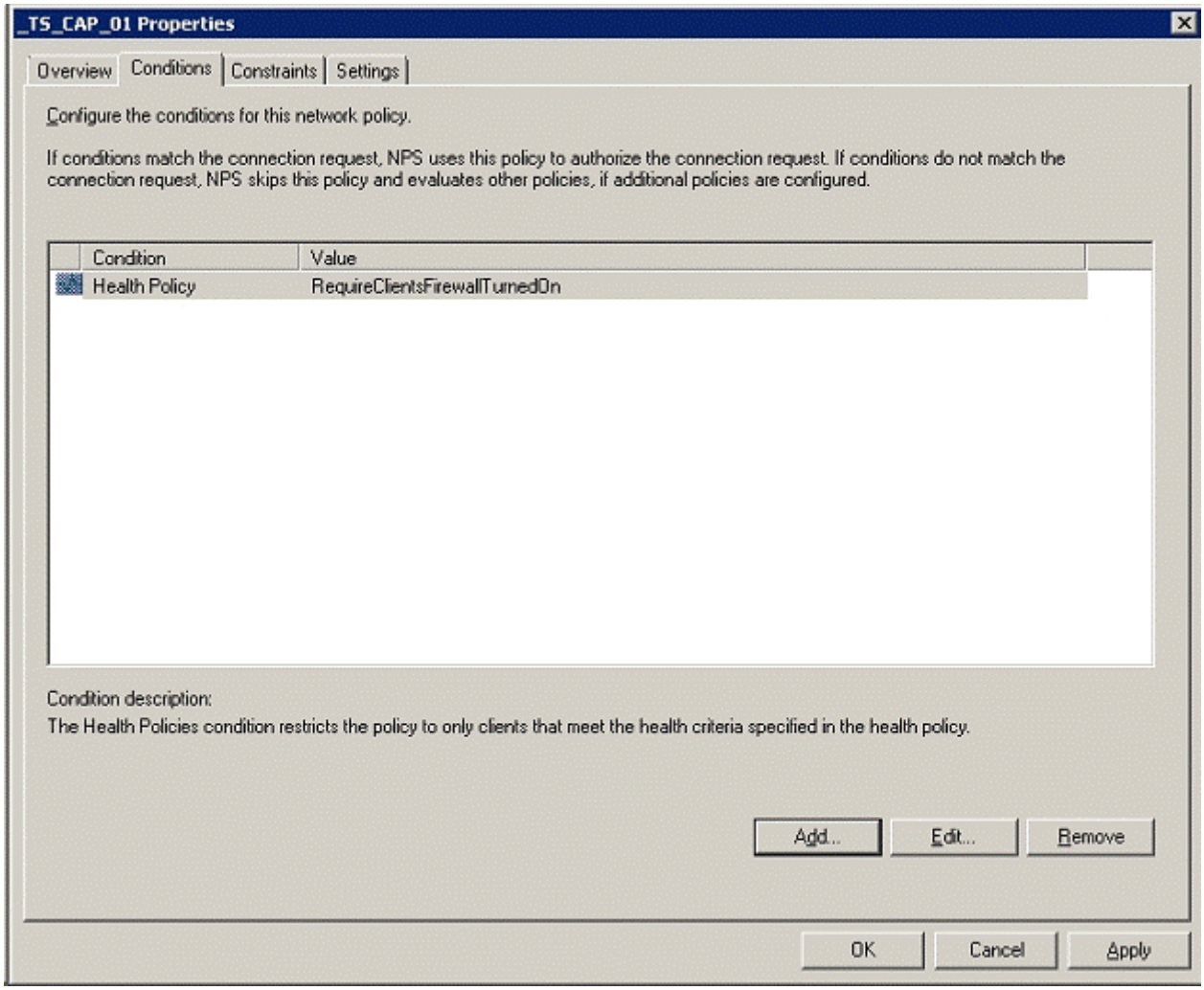
Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Remote Desktop Gateway (RD Gateway) role service installed. You add the Domain Users group to a connection authorization policy named TS_CAP_01. You need to ensure that only client computers that have Windows Firewall enabled can connect

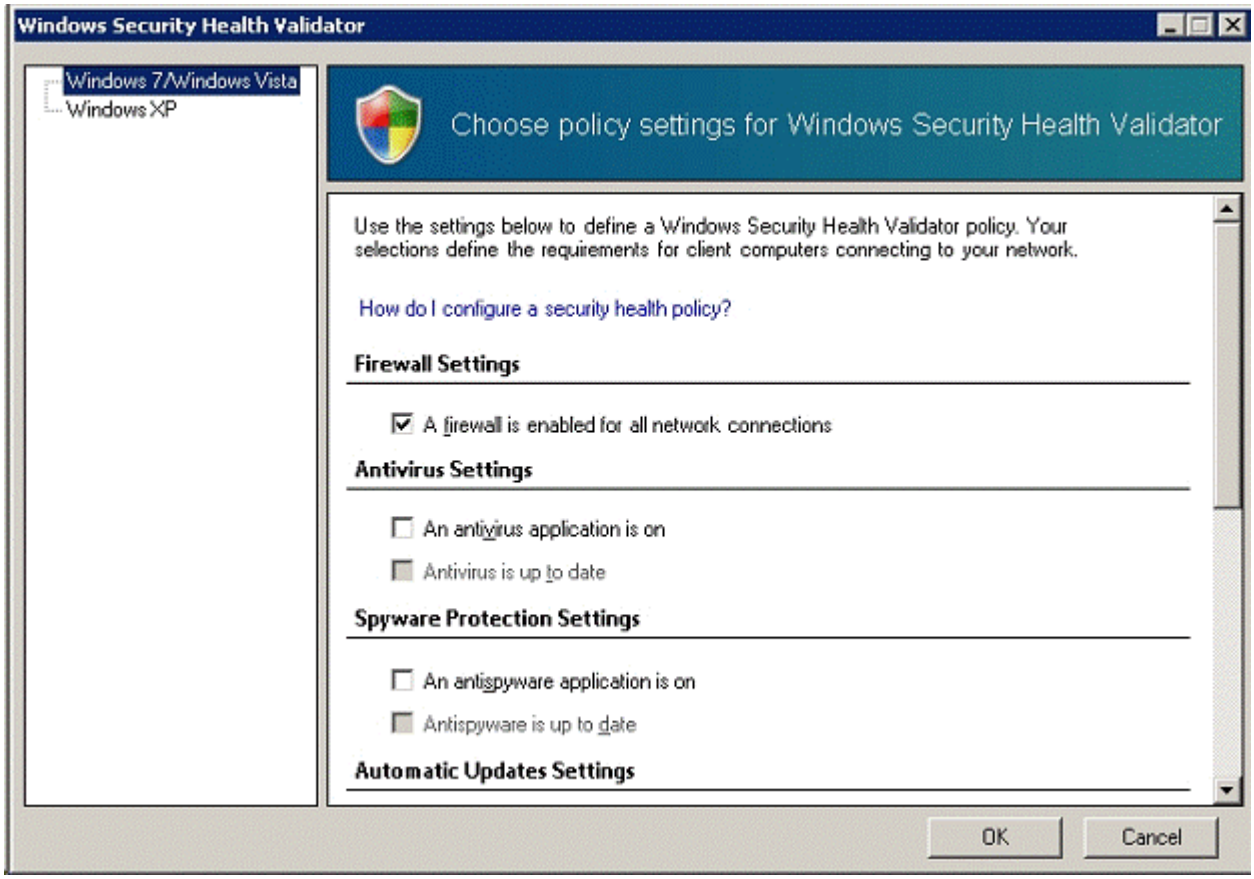
to Remote Desktop resources through the RD Gateway. What should you do?

A. From Remote Desktop Gateway Manager, modify the properties of the TS_RAP_01 resource authorization policy.
B. From Remote Desktop Gateway Manager, modify the properties of the TS_CAP_01 connection authorization policy.
C. From the Network Policy Server console, modify the properties of the TS_CAP_01 network policy.
D. From the Network Policy Server console, modify the properties of the TS GATEWAY AUTHORIZATION POLICY connection request policy.

Answer: C

Explanation:





Question: 148

Your network contains two servers that run Windows Server 2008 R2. The servers are configured as shown in the following table.

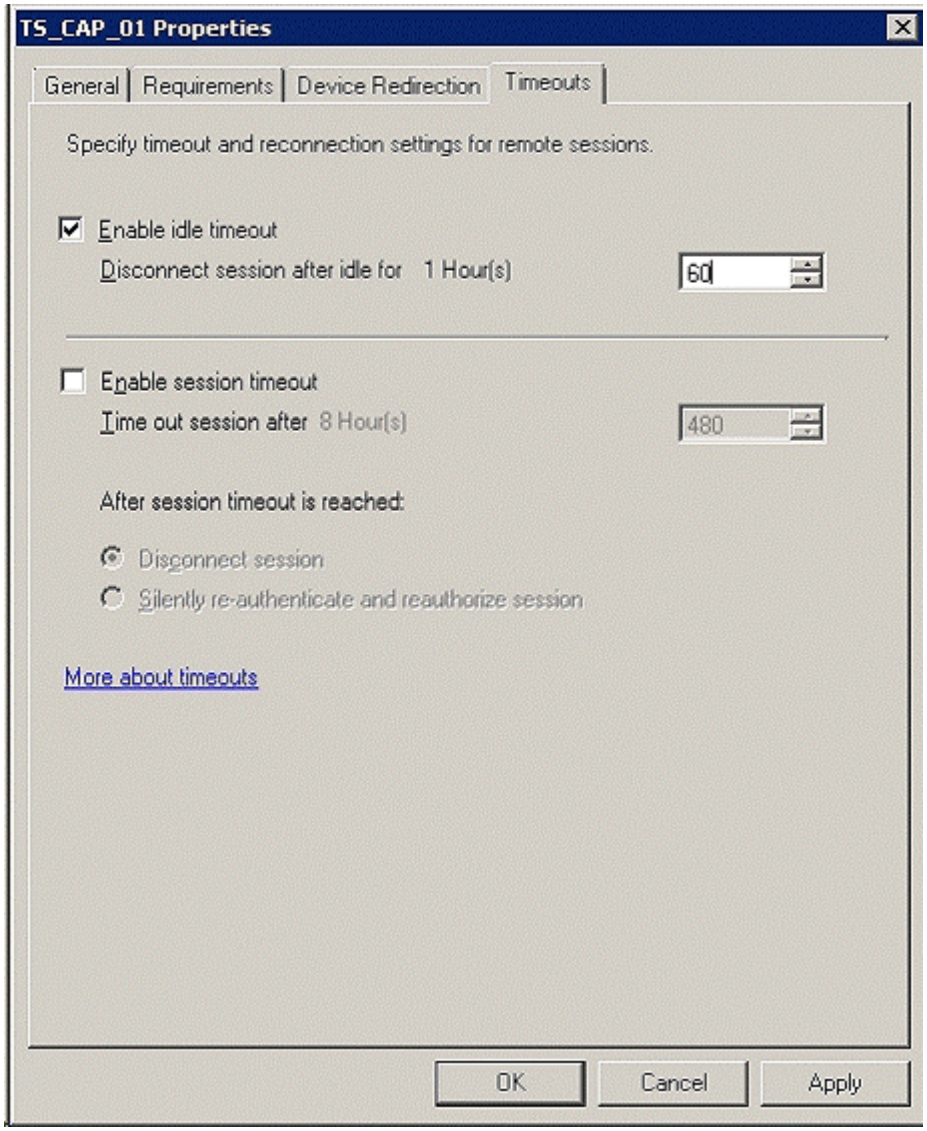
Server name	Role service
Server1	Remote Desktop Session Host (RD Session Host) Remote Desktop Web Access (RD Web Access)
Server2	Remote Desktop Gateway (RD Gateway)

Remote users connect to Remote Desktop resources on the internal network through Server2. Internal users access Remote Desktop resources on the internal network directly. You need to ensure that the remote users' Remote Desktop sessions are disconnected if their sessions are idle for more than 60 minutes. The internal users must not be disconnected if their Remote Desktop sessions are idle for more than 60 minutes. What should you do?

A. From RemoteApp Manager on Server1, modify the RD Gateway settings.
B. From Remote Desktop Gateway Manager on Server2, modify the properties of the resource authorization policy.
C. From Remote Desktop Gateway Manager on Server2, modify the properties of the connection authorization policy.
D. From Remote Desktop Session Host Configuration on Server1, modify the properties of the RDP- Tcp connection.

Answer: C

Explanation:



Question: 149

Your network contains three servers that run Windows Server 2008 R2. The servers are configured as shown in the following table.

Server name	Role services
Server1	Remote Desktop Connection Broker (RD Connection Broker)
Server2	Remote Desktop Virtualization Host (RD Virtualization Host)
Server3	Remote Desktop Session Host (RD Session Host) Remote Desktop Web Access (RD Web Access)

On Server1, you configure a virtual desktop pool named Pool1. Pool1 contains a Windows 7 virtual machine (VM) named Computer1. You need to ensure that when a user logs off of Computer1, all of the changes made to Computer1 are discarded. What should you do?

A. On Server2, enable shadow copies.
B. On Server2, take a snapshot of Computer1 and rename the snapshot RDV_Rollback.
C. From the properties of Pool1 on Server1, modify the Automatically save virtual machines setting.
D. From the Remote Desktop Session Host Configuration console on Server1, modify the Delete temporary folders on

exit setting.

Answer: B

Explanation:
To enable rollback on a virtual machine
1. Log on to RD Virtualization Host using an Administrator account.
2. Open Hyper-V Manager. To open Hyper-V Manager, click Start, point to Administrative Tools, and then click Hyper-V Manager.
3. Under Virtual Machines, right-click the virtual machine to enable rollback, and then click Snapshot.
4. Under Snapshots, right-click the snapshot of the virtual machine, and then click Rename.
5. Type RDV_Rollback and then press ENTER.
6. Close Hyper-V Manager.
7. Repeat these steps for each virtual machine.
Source: http://technet.microsoft.com/en-us/library/ff710411(WS.10).aspx

Question: 150

Your network contains three servers that run Windows Server 2008 R2. The servers are configured as shown in the following table.

Server name	Role service	IP address
server1.contoso.com	Remote Desktop Session Host (RD Session Host)	10.0.0.10
server2.contoso.com	Remote Desktop Session Host (RD Session Host)	10.0.0.11
server3.contoso.com	Remote Desktop Connection Broker (RD Connection Broker)	10.0.0.12

Server1 and Server2 are members of an RD Session Host server farm named farm1.contoso.com. You configure the RD Connection Broker role service on Server3 to support farm1.contoso.com. You need to create DNS records to support RD Connection Broker load balancing. Which record or records should you create for farm1.contoso.com?

A. One Alias (CNAME) record
B. One Host (AAAA) record
C. Two Host (A) records
D. Two service location (SRV) records

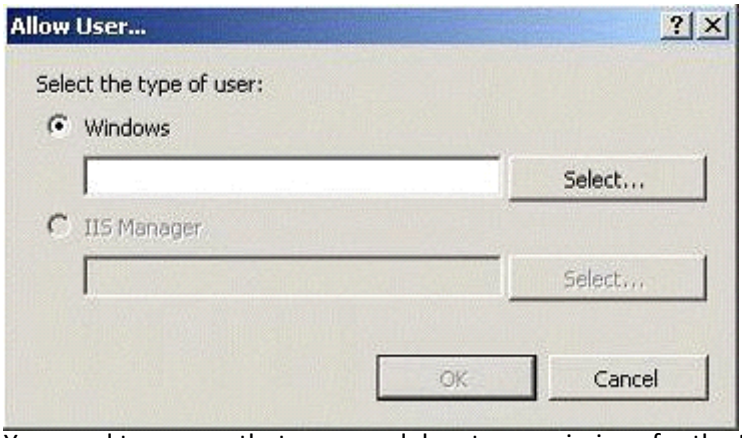
Answer: C

Explanation:
Configure DNS for RD Connection Broker Load Balancing
To load balance sessions in an RD Session Host server farm, you can use the RD Connection Broker Load Balancing feature together with Domain Name System (DNS) round robin. To configure DNS, you must create a DNS host resource record for each RD Session Host server in the farm that maps the RD Session Host server's IP address to the RD Session Host server farm name in DNS.
To add DNS entries for each RD Session Host server in the farm
1. Open the DNS snap-in. To open the DNS snap-in, log on to a computer where the DNS snap-in has been installed, click Start, point to Administrative Tools, and then click DNS.
2. Expand the server name, expand Forward Lookup Zones, and then expand the domain name.
3. Right-click the appropriate zone, and then click New Host (A or AAAA).
4. In the Name (uses parent domain name if blank) box, type the RD Session Host server farm name.
5. The farm name is the virtual name that clients will use to connect to the RD Session Host server farm. Do not use

the name of an existing server. For management purposes, we recommend that you use the same farm name that you specified when you configured the RD Session Host servers to join a farm in RD Connection Broker.
6. In the IP address box, type the IP address of an RD Session Host server in the farm.
7. Click Add Host.
Repeat steps three through six for each RD Session Host server in the farm.
Source: http://technet.microsoft.com/en-us/library/cc772506.aspx

Question: 151

Your network contains a Web server that runs Windows Server 2008 R2. You create an IIS Manager user account for a user named User1. When you attempt to delegate permissions for the Default Web Site to User1, you receive the following dialog box.

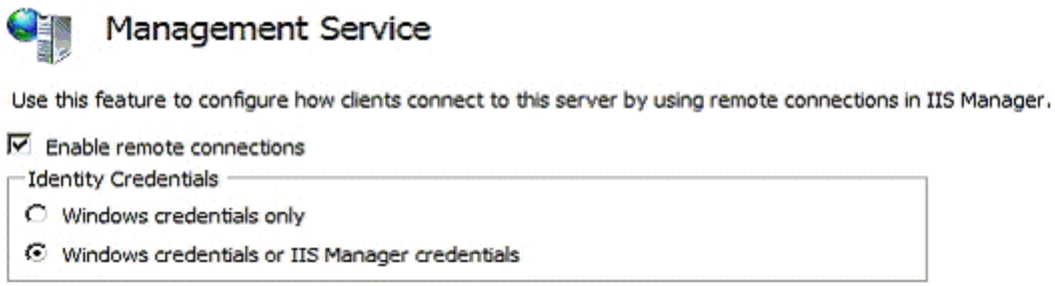


You need to ensure that you can delegate permissions for the Default Web Site to User1.
Which feature should you modify?

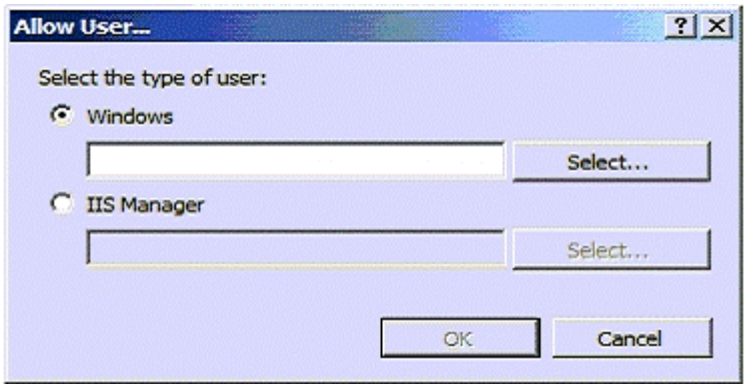
A. Feature Delegation
B. IIS Manager Permissions
C. IIS Manager Users
D. Management Service

Answer: D

Explanation:



Allow both Windows credentials AND IIS Manager credentials:



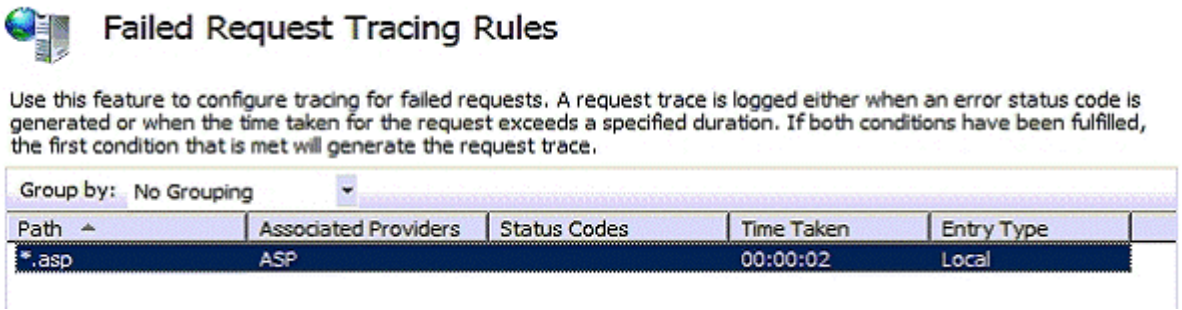
Question: 152

Your network contains a Web server that runs Windows Server 2008 R2. You need to generate a report for each Active Server Page (ASP) that takes more than two seconds to process. What should you use?

A. Reports in Performance Monitor
B. Data Collector Sets (DCSs) in Performance Monitor
C. Logging in Internet Information Services (IIS) Manager
D. Failed Request Tracing Rules in Internet Information Services (IIS) Manager

Answer: D

Explanation:



Question: 153

Your network contains a Web server that runs Windows Server 2008 R2. You need to back up all Web site content. Which tool should you use?

A. Appcmd
B. Internet Information Services (IIS) Manager
C. Internet Information Services (IIS) 6.0 Manager
D. Wbadmin

Answer: D

Explanation:
Wbadmin
Backups are usally done with Windows Server Backup;
Wbadmin is the command-line counterpart to Windows Server Backup. You use Wbadmin to manage all aspects of

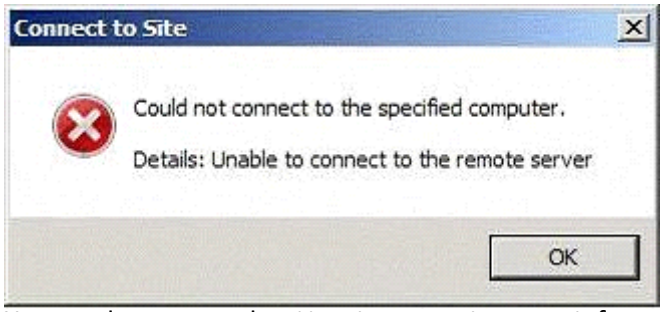
backup configuration that you would otherwise manage in Windows Server Backup. This means that you can typically use either tool to manage backup and recovery.
Source: http://technet.microsoft.com/en-us/magazine/dd767786.aspx To not only backup the website content but also the IIS configuration backup the systemstate:
The -systemState parameter:
For Windows7 and Windows Server 2008 R2, creates a backup that includes the system state in addition to any other items that you specified with the -include parameter. The system state contains boot files (Boot.ini,
NDTLDR, NTDetect.com), the Windows Registry including COM settings, the SYSVOL (Group Policies and Logon Scripts), the Active Directory and NTDS.DIT on Domain Controllers and, if the certificates service is installed, the Certificate Store. If your server has the Web server role installed, the IIS Metadirectory will be included. If the server is part of a cluster, Cluster Service information will also be included.
Source: http://technet.microsoft.com/en-us/library/cc742083(WS.10).aspx
Appcmd
The backup feature of Appcmd only backups the configuration of the IIS server, not the websites:
After you install IIS 7.0, you can backup your configuration by using the built-in command-line tool, AppCmd. exe. You can run AppCmd.exe to create a backup of your Web server before you have changed any configuration.
Files configuration IIS server:

- Administration.config
- ApplicationHost.config
- Redirection.config
- MBSchema.xml
- MetaBase.xml

To create a backup using AppCmd.exe
1. Open a command prompt as administrator and change to the %windir%\system32\inetsrv\ directory.
2. At the command prompt, type appcmd add backup "FirstBackup" and then press Enter.
3. This creates a backup with the name "FirstBackup". At a later date, if you need to restore the backup, use appcmd restore backup "FirstBackup"
Source: http://learn.iis.net/page.aspx/199/create-a-backup-with-appcmd/

Question: 154

You install all of the Web Server (IIS) role services on a server named Server1. You configure the Default Web Site to assign the IIS Manager Permissions for the site to a user named User1. From a different computer, User1 attempts to connect to the Default Web Site on Server1 by using Internet Information Services (IIS) Manager and receives the following error message.



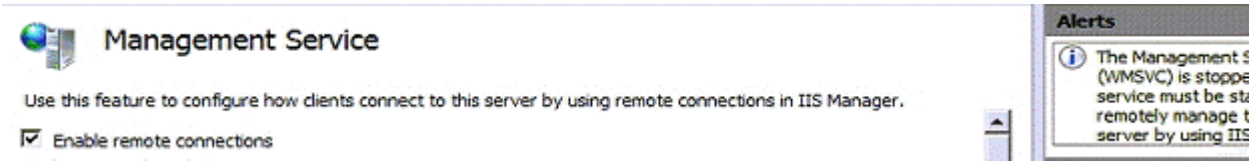
You need to ensure that User1 can use Internet Information Services (IIS) Manager to remotely administer the Default Web Site on Server1. What should you do first?

A. From the Internet Information Services (IIS) Manager console, configure the Feature Delegation feature.
B. From the Internet Information Services (IIS) Manager console, configure the Management Service feature.
C. From the Services console, modify the properties of the Web Management Service service.
D. From the Services console, modify the properties of the Windows Remote Management (WS- Management)

service.

Answer: B

Explanation:



Question: 155

Your network contains two Web servers named Server1 and Server2. Server1 has a Web site named Site1. Site 1 is configured to use SSL. You need to import the SSL certificate from Server1 to Server2. The solution must ensure that the private key is also imported. Which format should you use to export the certificate?

A. Base-64 encoded X.509 (.cer)
B. Cryptographic Message Syntax Standard PKCS #7 (.p7b)
C. DER encoded binary X.509 (.cer)
D. Personal Information Exchange PKCS #12 (.pfx)

Answer: D

Explanation:
To export a certificate with the private key
1. Open the Certificates snap-in for a user, computer, or service.
2. In the console tree under the logical store that contains the certificate to export, click Certificates.
3. In the details pane, click the certificate that you want to export.
4. On the Action menu, point to All Tasks, and then click Export.
5. In the Certificate Export Wizard, click Yes, export the private key. (This option will appear only if the private key is marked as exportable and you have access to the private key.)
6. Under Export File Format, do any of the following, and then click Next.
- To include all certificates in the certification path, select the Include all certificates in the certification path if possible check box.
- To delete the private key if the export is successful, select the Delete the private key if the export is successful check box. - To export the certificate's extended properties, select the Export all extended properties check box.
7. In Password, type a password to encrypt the private key you are exporting. In Confirm password, type the same password again, and then click Next.
8. In File name, type a file name and path for the PKCS #12 file that will store the exported certificate and private key. Click Next, and then click Finish.
Source: http://technet.microsoft.com/en-us/library/cc754329.aspx

Question: 156

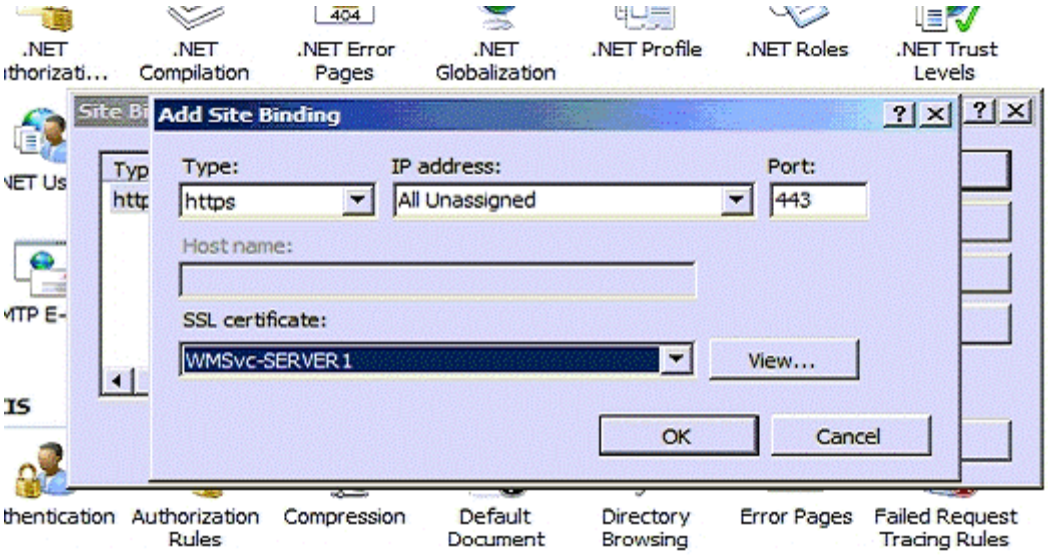
Your network contains a Web server named Web1 that runs Windows Server 2008 R2.
You import an SSL certificate to Web1.
You need to enable SSL encryption for the Web site.
What should you do?

A. Add a new binding to the Web site.

B. Modify the Server Certificates settings.
C. Configure the handler mappings for the Web site.
D. Configure the Machine Key feature for the Web site.

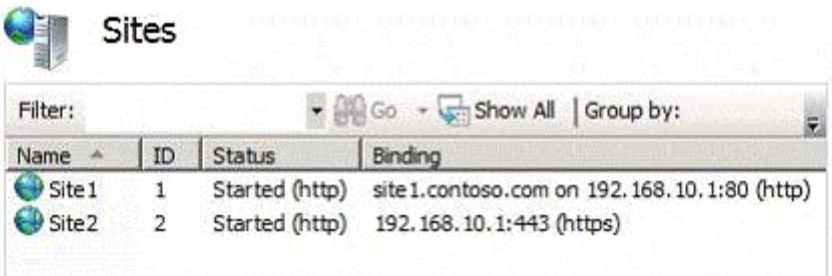
Answer: A

Explanation:



Question: 157

Your network contains a Web server named Web1 that runs Windows Server 2008 R2. Web1 has a wildcard certificate installed. Web1 has two Web sites as shown.



You discover that when you go to the URL https://site1.contoso.com in Internet Explorer, you connect to Site2. You need to ensure that when users go to https://site1.contso.com in Internet Explorer, they connect to Site1. The solution must ensure that all connections to Site1 are secure. Which two settings should you modify? (Each correct answer presents part of the solution. Choose two.)

A. the bindings for Site1
B. the bindings for Site2
C. the HTTP Redirect settings for Site1
D. the HTTP Redirect settings for Site2

Answer: A, B

Question: 158

Your network contains a Web server that runs Windows Server 2008 R2. The server has two Web sites named Site1

and Site2. Site1 is accessed by using the name site1.contoso.com. Site2 is accessed by using the name site2.contoso.com. You plan to configure both Web sites to use SSL encryption. You need to ensure that users can access Site1 by using the URL https://site1.contoso.com and Site2 by using the URL https://site2.contoso.com. What should you configure for each Web site?

A. a different application pool
B. a different host header site binding
C. a different IP address site binding
D. a different port site binding

Answer: C

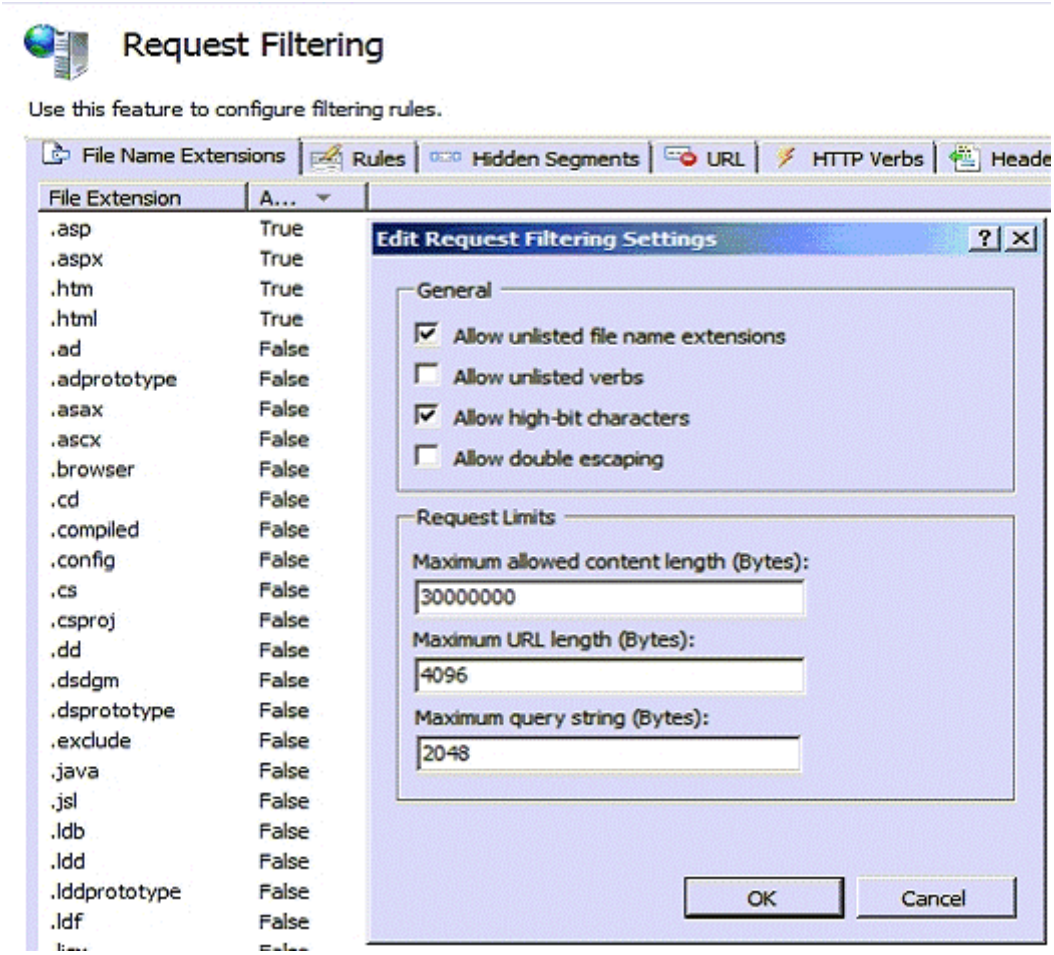
Question: 159

Your network contains a Web server. You need to ensure that users can only access files that have the .htm, .html, .asp, and .aspx file extensions. What should you do?

A. Add an authorization rule.
B. Modify the handler mappings.
C. Update the default documents list.
D. Configure the request filtering settings.

Answer: D

Explanation:



Question: 160

Your network contains a Web server that runs Windows Server 2008 R2. The Web server has the Client Certificate Mapping Authentication role service installed. You create a Web site that requires client certificates for authentication. You need to enable client certificate mapping for the Web site. Which tool should you use?

A. Appcmd
B. Certutil
C. the Authorization Manager snap-in
D. the Certificates snap-in

Answer: A

Explanation:
Client Certificate Mapping Authentication
Client Certificate Mapping Authentication enables clients to authenticate with the Web server by presenting client certificates over Secure Socket Layer (SSL) connections.
Note Certificate-based authentication enables clients to use client certificates to authenticate with the Web server. It is not required to enable secure communication between the client and the server. The Client Certificate Mapping Authentication uses the Directory Services Mapper (DS Mapper) service in Active Directory to map client certificates provided by the user to domain accounts. IIS also provides a custom certificate mapping feature, the IIS Client Certificate Mapping Authentication, which allows for more flexible mapping of client certificates to Windows accounts. See the section titled "IIS Client Certificate Mapping Authentication" later in this chapter for more

information.
Note Client Certificate Mapping Authentication is not part of the default IIS install and is not enabled by default. You can manually install it from the Security feature category through Turn Windows Features On And Off on Windows Vista. You can also install it via the Security role service category of the Web Server (IIS) role in Server Manager on Windows Server 2008. See Chapter 12 for more information about installing and enabling modules. After the module is installed, you have to explicitly enable Client Certificate Mapping Authentication for it to be available. To use Client Certificate Mapping Authentication, you need to meet the following requirements: The Web server must be a member of a Windows domain. You must issue client certificates to your users by using a Certificate Authority (CA) trusted by the Web server. You must map each client certificate to a valid domain account in Active Directory.
Note You do not need to use Client Certificate Mapping Authentication to require clients to present client certificates. You can configure the server to always require client certificates to access the server, but use another authentication scheme to authenticate the client. To do this, see the section titled "Client Certificates" later in this chapter. To enable Client Certificate Mapping Authentication on the Web server, you need to perform the following steps (after installing the Certificate Mapping Authentication module).
1. Enable Client Certificate Mapping Authentication. You can do this in IIS Manager by clicking the server node, double-clicking Authentication, selecting Active Directory Client Certificate Authentication, and clicking Enable in the Actions pane. Note that this can only be done at the server level when using IIS Manager, although you can enable Client Certificate Mapping Authentication for a specific URL through configuration.
2. Configure SSL on each Web site using this authentication method. Certificate authentication is possible only if the Web site is being accessed over an SSL connection and therefore requires an SSL binding to be configured for the Web site. See the section titled "Configuring SSL" later in this chapter for more details.
3. Enable DS Mapper for each Web site SSL binding. IIS Manager does this automatically for each Web site when the Client Certificate Mapping Authentication is enabled and you add an SSL binding for the Web site. To do this manually, use the Netsh.exe command with the following syntax: netsh http add sslcert IP
Address:Port dsmapperusage=enable, where IP Address and Port are the IP address and port of the corresponding binding.
4. Configure each Web site using this authentication method to accept client certificates (and possibly require them). This ensures that the server accepts client certificates when provided by the client and can also configure the server to require the client to present a certificate to proceed with the request. See the section titled "Client Certificates" later in this chapter for more details.
You can also enable Client Certificate Mapping Authentication by editing the system.webServer/security/authentication/clientCertificateMappingAuthentication configuration section directly or by using Appcmd or other configuration APIs. You can enable this authentication method by using the following Appcmd syntax.
%systemroot%\system32\inetsrv\Appcmd set config /section: system.webServer/ security/authentication/clientCertificateMappingAuthentication /enabled: true
The enabled attribute specifies whether or not the Client Certificate Mapping Authentication is enabled. You can enable this method for a specific URL. However, do note that the decision to use the Directory Services Mapper to map certificates to Windows domain accounts is dependent on each Web site binding having been configured to use the HTTP.sys DS Mapper setting.
Source: http://technet.microsoft.com/en-us/library/dd163543.aspx

Question: 161

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Streaming Media Services role and the Web Server (IIS) role installed. Server1 hosts the company's intranet Web site. You need to configure Windows Media Services to stream content by using HTTP. What should you do first?

A. Install the RPC over HTTP proxy server feature.
B. Configure a host header for the intranet Web site.
C. Configure the server to have an additional IP address.

D. Create a new virtual directory on the intranet Web site.

Answer: C

Microsoft Windows Media Services (WMS) and Microsoft Internet Information Services (IIS) can coexist on a computer when you use their default values. By default, WMS does not enable the WMS HTTP Server Control Protocol plug-in. In this manner, IIS can safely bind to port 80 for delivery of Web-based content. Sometimes it can be useful for WMS to use port 80 to deliver content. For example, if the majority of a content provider's clients are behind a firewall, it can be better to use port 80 for delivery of streaming content, because most firewalls have port 80 opened. With IIS 6.0, HTTP requests are handled by the Http.sys listener. By default, Http.sys will listen to all requests coming in on port 80 for all IP addresses bound to the computer (except for the loopback address: 127.0.0.1). For WMS to bind to use port 80 for streaming content, you must configure the Http.sys listener so that WMS can listen to the specified IP addresses. If you enable the HTTP Server Control Protocol plug-in without configuring the listener, you may receive the following error:
One usage of each socket address (protocol/network address/port) is permitted. Verify that other services (such as IIS) or applications are not attempting to use the same port and then try to enable the plug-in again.
Error Code: 0xC00D158B
MORE INFORMATION
For both IIS and WMS to use port 80, one of the following two conditions must be true:
One (1) network adapter has at least 2 IPs bound to the adapter.
Two (2) network adapters have at least 1 IP bound to each adapter.
Source: http://support.microsoft.com/kb/328728

Question: 162

Your network contains a server that runs Windows Server 2008 R2. You need to install the Streaming Media Services role on the server. What should you do first?

A. Download and install Windows Media Encoder 9 Series x64 Edition.
B. Download and install Windows Media Services 2008 for Windows Server 2008 R2.
C. From Server Manager, click Check for new roles.
D. From Server Manager, install the Quality Windows Audio Video Experience (qWave) feature.

Answer: B

Explanation:
How to install Windows Media Services for Windows Server 2008 R2
The Streaming Media Services role is not included in the Windows Server 2008 R2 operating system. This role includes the latest version of Microsoft Windows Media Services, Windows Media Services 2008 for Windows Server 2008 R2. To obtain Windows Media Services 2008 for Windows Server 2008 R2, you must obtain and then run the Microsoft Update Standalone Package (MSU) file for the Streaming Media Services role. You must run this file on the updated platform.
1. Download and then run the MSU file for the Streaming Media Services role. To do this, follow these steps:
a. Visit the following Microsoft Web site:
http://www.microsoft.com/downloads/details.aspx?FamilyID=b2cdb043-d611-41c9-91b7-cddf6e5fdf6b
b. Download and run the Windows6.1-KB963697-x64.msu file.
2. Start Server Manager. To do this, click Start, point to Administrative Tools, and then click Server Manager.
3. On the Action menu in Server Manager, click Refresh, and then wait for the update to finish.
Note You can check the update status on the lower-left side of the status bar in Server Manager.
4. Restart Server Manager.

5. In Server Manager, add the Streaming Media Services role. To do this, click Add Roles under Roles Summary, and then click Streaming Media Services in the Add Roles wizard.
Source: http://support.microsoft.com/kb/963697

Question: 163

Your network contains a server that runs Windows Server 2008 R2. The server has the Streaming Media Services role installed.
The network is configured to use IPv6 only.
You need to configure a multicast stream.
Which IPv6 prefix should you use?

A. FD00::/8
B. FE80::/10
C. FEC0::/10
D. FF00::/8

Answer: D

Explanation:
Multicast IPv6 addresses
A multicast address identifies multiple interfaces. With the appropriate multicast routing topology, packets addressed to a multicast address are delivered to all interfaces that are identified by the address. IPv6 multicast addresses have the Format Prefix (FP) of 1111 1111. An IPv6 address is simple to classify as multicast because it always begins with FF. Multicast addresses cannot be used as source addresses. Beyond the FP, multicast addresses include additional structure to identify their flags, scope, and multicast group, as shown in the following illustration.

The fields in the multicast address are as follows:
Flags
The Flags field indicates flags that are set on the multicast address. The size of this field is 4 bits. As of RFC 2373, the only flag defined is the Transient (T) flag. The T flag uses the low-order bit of the Flags field. When set to 0, the T flag indicates that the multicast address is a permanently-assigned (well-known) multicast address allocated by the Internet Assigned Numbers Authority (IANA). When set to 1, the T flag indicates that the multicast address is a transient (not permanently assigned) multicast address.
Scope
The Scope field indicates the scope of the IPv6 internetwork for which the multicast traffic is intended. The size of this field is 4 bits. In addition to information provided by multicast routing protocols, routers use the multicast scope to determine whether multicast traffic can be forwarded. The following scopes are defined in RFC 2373:
Scope field value Scope
1 Node-local
2 Link-local
5 Site-local
8 Organization-local
E Global
For example, traffic with the multicast address of FF02::2 has a link-local scope. An IPv6 router never forwards this traffic beyond the local link.

Group ID
The Group ID field identifies the multicast group and is unique within the scope. The size of this field is 112 bits.
Permanently assigned group IDs are independent of the scope. Transient group IDs are only relevant to a specific scope. Multicast addresses from FF01:: through FF0F:: are reserved, well-known addresses. To identify all nodes for the node-local and link-local scopes, the following multicast addresses are defined:
FF01::1 (node-local scope all-nodes address)
FF02::1 (link-local scope all-nodes address)
To identify all routers for the node-local, link-local, and site-local scopes, the following multicast addresses are defined:
FF01::2 (node-local scope all-routers address)
FF02::2 (link-local scope all-routers address)
FF05::2 (site-local scope all-routers address)
With 112 bits in the Group ID, it is possible to have 2112 group IDs. However, because of the way in which IPv6 multicast addresses are mapped to Ethernet multicast MAC addresses, RFC 2373 recommends assigning the Group ID from the low order 32 bits of the IPv6 multicast address and setting the remaining original group ID bits to 0. By using only the low-order 32 bits in the group ID, each group ID maps to a unique Ethernet multicast MAC address.
Source: http://technet.microsoft.com/en-us/library/cc781068.aspx

Question: 164

Your network contains two servers named Server1 and Server2 that have the Streaming Media Services role installed. Server1 is located in a subnet named Subnet1. Server2 is located in a subnet named Subnet2. Server1 has an on-demand publishing point named Content1. Content1 has a 1-Mbps bit rate. Server2 is configured as a cache/proxy server. You need to ensure that users on Subnet2 can stream Content1 from Server2. The solution must ensure that Content1 is available on Server2 before the users request the stream. What should you modify?

A. the Cache settings on Server1
B. the Prestuff settings on Server2
C. the Proxy settings on Server1
D. the Cache settings on Server2

Answer: B

Explanation:
WMS Cache Proxy - Prestuff properties
You can configure the following options on the Prestuff tab for this plug-in.
Item Description
Prestuff from
Stream
Select this option to enable this server to cache content by streaming it from the origin server, even when it is not requested by clients. Type the URL of the file on the origin server in the URL box (for example, http://server/publishing_point/file), and then select one of the following Prestuff Rate options that specify the speed at which this server caches content from the origin server: Maximum Available Bandwidth. Choose this option to cache content from the origin server as fast as the network will allow. Content Bit Rate. Choose this option to cache content from the origin server at the same bit rate as the requested content bit rate. Note that for MBR content, the caching speed is the same as the average bit rate of the content.
Kbps. Enter a value in this box to specify the bit rate at which this server caches content from the origin server.
Prestuff from
File
Select this option to enable this server to make a file on an available file storage system, such as a local file system, storage area network (SAN), or network-attached storage (NAS), available for streaming to clients. To copy the file

from file storage to the cache directory on this server and make it available to clients before it is requested, do the following:
Type the UNC path of the file in the Content Path box (for example, \\server\folder\file or network_share\file). Type the URL that clients must use to stream the file in the Stream URL box (for example, rtsp://server/publishing_point/file or http://server/publishing_point/file).
Select the Copy content to local cache directory check box.
To copy the file from file storage to the cache directory on this server only after a client requests it, do the following:
1. Type the UNC path of the file in the Content Path box.
2. Type the URL that clients must use to stream the file in the Stream URL box. for example,
rtsp://server/publishing_point/file or
http://server/publishing_point/file).
3. Select the Copy content to local cache directory check box.
Make sure that the Copy content to local cache directory check box is not selected.
Note that this server cannot use freshness checking to determine whether the file in the file storage system has been updated. It the file has been updated, you must click Prestuff to cache the updated file to the cache directory. Prestuff Click this button to start caching the specified content from the origin server, even when it is not requested by clients.

Question: 165

Your network contains a server that runs Windows Server 2008 R2. You install Windows Media Services on the server. You need to stream a live video broadcast. The solution must minimize any delays caused by network congestion. What should you do?

A. Create a broadcast publishing point that delivers content by using unicast. Stream the content by using HTTP.
B. Create an on-demand publishing point that delivers content by using unicast. Stream the content by using HTTP.
C. Create a broadcast publishing point that delivers content by using multicast. Stream the content by using real-time streaming protocol (RTSP).
D. Create an on-demand publishing point that delivers content by using unicast. Stream the content by using real-time streaming protocol (RTSP).

Answer: C

Question: 166

Your network contains a server that runs Windows Server 2008 R2. You install Windows Media Services on the server. You need to create an announcement file that allows Windows Media Player clients to decode multicast streams. Which file extension should you use for the announcement file?

A. .asx
B. .htm
C. .nsc
D. .wsx

Answer: C

Explanation:
Announcing content
Before you can stream content, you need to let your users know that it is available by using an announcement. An announcement is a Windows Media metafile with an .asx extension that provides the Player with the information needed to connect to a Windows Media server to receive content. You can place a link to an announcement on a Web

page, make the announcement available in a shared file, or send an announcement in an email message. Users can access your content either by clicking the link to the announcement on a Web page or by opening the announcement directly. The announcement wizards on the Announce tab of the Windows Media Services snap-in help you create announcement files (.asx files) and multicast information files (.nsc files) that players can use connect to your content. The wizards can also help you create a Web page with an embedded Windows Media Player control or provide you with the syntax to embed a Player in your own Web page.
Source: http://technet.microsoft.com/en-us/library/cc753414.aspx

Question: 167

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Streaming Media Services role installed. You discover that anonymous users can access video content stored on Server1. You need to ensure that user access to videos on the server requires authentication. What should you do?

A. From the Windows Media Services console, configure the Authorization properties.
B. From the Windows Media Services console, configure the Authentication properties.
C. From Internet Information Services (IIS) Manager, configure the Authentication settings.
D. From Internet Information Services (IIS) Manager, configure the .Net Authorization Rules settings.

Answer: B

Explanation:
About authentication
Authentication is a fundamental aspect of security for a server running Windows Media Services. It confirms the identity of any user trying to access resources on your Windows Media server. Windows Media Services includes the following authentication plug-ins that you can enable to validate user credentials:
WMS Anonymous User Authentication
WMS Negotiate Authentication
WMS Digest Authentication
Authentication plug-ins work in conjunction with authorization plug-ins: after users are authenticated, authorization plug-ins control access to content. Windows Media Services authentication plug-ins fall into the following categories: Anonymous authentication. These are plug-ins that do not exchange challenge and response information between the server and a player, such as the WMS Anonymous User Authentication plug-in. Network authentication. These are plug-ins that validate users based on logon credentials, such as the WMS Negotiate Authentication plug-in. When a user tries to access a server or publishing point, the server tries to authenticate users through an anonymous authentication plug-in. If more than one anonymous authentication plug-in is enabled, the server only uses the first one listed. If that attempt fails or an anonymous authentication plug-in is not enabled, the server tries to authenticate the user by using a network authentication plug-in. If more than one network authentication plug-in is enabled, the server tries to use the first one that is also supported by the client.
Source: http://technet.microsoft.com/en-us/library/cc754800.aspx

Question: 168

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Streaming Media Services role and the Web Server (IIS) role installed. You have a confidential media file. You need to ensure that the media file streams are encrypted. Which protocol should you configure?

A. HTTPS
B. IPSec
C. Microsoft Media Server (MMS)

D. real-time streaming protocol (RTSP)

Answer: B

Question: 169

Your network contains a server named Server1. Server1 has the Streaming Media Services role installed. You have media files stored on a hard disk drive. The hard disk drive is formatted by using the NTFS file system and protected by using Encrypted File System (EFS). You need to ensure that Windows Media Services can open the EFS-encrypted files. What should you do?

A. From the Windows Media Services console, configure the WMS NTFS ACL Authorization plug-in.
B. From the Windows Media Services console, configure the WMS Publishing Points ACL Authorization plug-in.
C. From the Services console, configure the properties of the Protected Storage service, and then start the service.
D. From the Services console, configure the properties of the Windows Media Services service, and then restart the service.

Answer: D

Explanation:
Sourcing from an encrypted directory
Security concerns may require that you maintain some or all of your content in an encrypted directory. The encryption process encodes the data in a file so that it is unreadable to a computer or account that does not have the appropriate file encryption key. In the Windows operating system, the file encryption key is assigned to an account. Anyone who logs on using that account is then able to decrypt and use the content. Windows Media Services can decrypt and stream encrypted content if it is logged on to the proper account. By default, Windows Media Services logs on to the Network Service account. To access the encrypted content, you must set Windows Media Services to log on to the same account that encrypted the content. You can change the account Windows Media Services uses to log on to the computer by using Microsoft Management Console. For more information about encryption, accounts, and user privileges, see Windows Help and Support.
Source: http://technet.microsoft.com/en-us/library/cc754882.aspx

Question: 170

Your network contains a server named Server1. Server1 has the Streaming Media Services role installed. The network contains two subnets named Subnet1 and Subnet2. You create an on-demand publishing point named Publishing1 on Server1. You need to ensure that only users from Subnet1 can access Publishing1. What should you configure from the Windows Media Services console?

A. From the properties of Server1, configure the Limits settings.
B. From the properties of Server1, configure the Authentication settings.
C. From the properties of Publishing1, configure the Credentials settings.
D. From the properties of Publishing1, configure the Authorization settings.

Answer: D

Explanation:
WMS IP Address Authorization
The WMS IP Address Authorization plug-in is used to control access to your content based on client Internet Protocol (IP) addresses. You can add specific IP addresses or ranges of IP addresses for which you want to allow or restrict

access. You can configure the following options on the General tab for this plug-in.

Item	Description
Set IP address access permissions	
Allow all except those in the Deny list	Select this option to restrict clients from accessing your server based on their IP addresses. If this permission level is set, all clients have access by default.
Deny all except those in the Allow list	Select this option to allow clients to access your server based on their IP addresses. If this permission level is set, all clients do not have access by default.
Restrict as specified in the following lists	Select this option to allow and deny access to the content on your server based on client IP addresses.
Allow	Displays the IP addresses and subnet masks that are allowed to access the content on your publishing points. ▪ Click **Add IP** to add an IP address or subnet to the list. ▪ Click **Edit IP** to modify an IP address or subnet in the list. ▪ Click **Remove IP** to delete an IP address or subnet from the list.
Deny	Displays a list of IP addresses and subnet masks that are not allowed to access the content on your publishing points. ▪ Click **Add IP** to add an IP address or subnet to the list. ▪ Click **Edit IP** to modify an IP address or subnet in the list. ▪ Click **Remove IP** to delete an IP address or subnet from the list.

Source: http://technet.microsoft.com/en-us/library/cc770273.aspx

Question: 171

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Streaming Media Services role installed. On Server1, you create an on-demand publishing point named PublishingPoint1. You need to ensure that only members of a group named Group1 can access content from PublishingPoint1. Which two plug-ins should you configure for PublishingPoint1? (Each correct answer presents part of the solution. Choose two.)

A. WMS Anonymous User Authentication
B. WMS IP Address Authorization
C. WMS Negotiate Authentication
D. WMS Publishing Points ACL Authorization

Answer: C, D

Explanation:
WMS Negotiate Authentication
The WMS Negotiate Authentication plug-in grants access to the server based upon the user's network logon approval. This plug-in uses an encrypted challenge/response scheme to authenticate users. It is a secure form of authentication because the user name and password are not sent across the network; the player acknowledges the password by using a cryptographic exchange with the Windows Media server. Because this plug-in relies upon established user logon credentials, the player and server must be on the same domain or on trusted domains. Negotiate authentication does not work across proxy servers or other firewall applications.
Source: http://technet.microsoft.com/en-us/library/cc730972.aspx
WMS Publishing Points ACL Authorization
The WMS Publishing ACL Authorization plug-in is used to control access to your content based on the permissions you have set on your publishing points. You can configure the following options on the General tab for this plug-in.

Item	Description
Name	Displays the users and groups that are allowed to access content on your server. Do any of the following: ▪ Click **Add** to add a user or group to the list. ▪ Click **Remove** to remove the selected user or group from the list.
Permissions	
Read	Select either the **Allow** or **Deny** check box to set whether the user or group can read data from your server.
Write	Select either the **Allow** or **Deny** check box to set whether the user or group can write data to your server. You must select both **Write** and **Create** to allow a user or group to create a publishing point. When setting permission levels for a server, select either the **Allow** or **Deny** check box to set whether the user or group can create publishing points on your server.
Create	When setting permission levels for a publishing point, select either the **Allow** or **Deny** check box to set whether the user or group can use this publishing point as a template for creating other publishing points on your server when pushing content from an encoder. You must select both **Write** and **Create** to allow a user or group to create a publishing point. Create permissions alone are not sufficient to create a new publishing point.

Source: http://technet.microsoft.com/en-us/library/cc770267.aspx

Question: 172

Your network contains a hardware firewall between the internal network and the Internet. On the internal network, you install a new server named Server1. Server1 has the Streaming Media Services role installed. You configure Server1 to use only real-time streaming protocol (RTSP) streaming. You create an on-demand unicast publishing point. You need to ensure that users from the Internet can access the publishing point on Server1. Which inbound ports should you allow on the hardware firewall?

A. TCP 21, UDP 5000, and UDP 5001
B. TCP 80, TCP 1024, and UDP 500
C. TCP 443, TCP 8080, and UDP 5000
D. TCP 554, UDP 5004, and UDP 5005

Answer: D

Explanation:
Delivering a unicast stream

Application Protocol	Protocol	Port	Description
RTSP	TCP	554 (In/Out)	Used for accepting incoming RTSP client connections and for delivering data packets to clients that are streaming by using RTSPT.
RTSP	UDP	5004 (Out)	Used for delivering data packets to clients that are streaming by using RTSPU.
RTSP	UDP	5005 (In/Out)	Used for receiving packet loss information from clients and providing synchronization information to clients that are streaming by using RTSPU.
MMS	TCP	1755 (In)	Used for accepting incoming MMS client connections.
HTTP	TCP	80 (In/Out)	Used for accepting incoming HTTP client connections and for delivering data packets to clients that are streaming by using HTTP.

To make sure that your content is available to all client versions that connect to your server, open all ports described in the table for all of the connection protocols that might be used during protocol rollover. When you install Windows Media Services 2008 on a computer that is running Windows Server 2008 or Windows Server 2008 R2, the Windows Media Services program (wmserver.exe) is added as an exception in Windows Firewall to open the default inbound ports for unicast streaming, and manually opening ports in the firewall is not required.
Source: http://technet.microsoft.com/en-us/library/ee126132.aspx

Question: 173

Your network contains an Active Directory domain. The domain contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Streaming Media Services role installed. You need to ensure that all streaming media is encrypted when the media is sent over the network. What should you do?

A. Configure a connection security rule.
B. Configure the WMS Digest Authentication plug-in.
C. Configure the WMS Publishing Points ACL Authorization plug-in.
D. Install an SSL certificate and bind the certificate to port 443.

Answer: A

Question: 174

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Streaming Media Services role and the Web Server (IIS) role installed. Server1 has a broadcast publishing point named Broadcast1. Broadcast1 publishes a file named Broadcast1.wmv. You run the Unicast Announcement Wizard for Broadcast1 and create a new announcement file. You need to ensure that only authorized users have permission to access the announcement file. What should you modify?

A. the Authentication settings for Broadcast1
B. the Authorization settings for Broadcast1
C. the NTFS permissions on c:\inetpub\wwwroot\Broadcast1.asx
D. the NTFS permissions on c:\wmpub\wmroot\Broadcast1.wmv

Answer: C

Question: 175

Your network contains a server that has Microsoft SharePoint Foundation 2010 installed. A user named User1 is a member of the Members group. You create a new page in an existing SharePoint site. You need to prevent User1 from modifying the page. The solution must ensure that User1 is allowed to modify other pages in the site. What should you do first?

A. Modify the site permissions.
B. Edit the properties of the page.
C. Stop the inheritance of permissions.
D. Change the default Permission Levels.

Answer: C

Explanation:
About permission inheritance
Permissions on securable objects within a site are inherited from the parent object by default. You can break inheritance and use fine-grained permissions — unique permissions on the list or library, folder, or item or document level — to gain more control of the actions users can take on your site. Stopping inheriting permissions copies the groups, users, and permission levels from the parent object to the child object, and then breaks the inheritance. When permission inheritance is broken, all permissions are explicit and any changes to parent object do not affect the child object. If you restore inherited permissions, the child object will inherit its users, groups, and permission levels from the parent again, and you will lose any users, groups, or permission levels that were unique to the child object.

For ease of management, use permission inheritance wherever possible.
Source: http://technet.microsoft.com/en-us/library/cc287752.aspx

Question: 176

You deploy a server that has Microsoft SharePoint Foundation 2010 installed. You create several SharePoint site collections in the default Web application. You need to ensure that a user named User1 can access all of the site collections in the Web application. What should you modify in the properties of the default Web application?

A. the General Settings
B. the Permissions Policy
C. the User Permissions
D. the User Policy

Answer: D

Explanation:
Manage permission policies for a Web application
A Web application is composed of an Internet Information Services (IIS) Web site that acts as a logical container for the site collections that you create. Before you can create a site collection, you must first create a Web application. A Web application can contain as many as 500,000 site collections. Managing permissions for so many site collections can be complicated and error-prone, especially if some users or groups need permissions other than those that apply for the entire Web application. Permission policies provide a centralized way to configure and manage a set of permissions that applies to only a subset of users or groups in a Web application The differences between specifying user permissions for a Web application and creating a permission policy for a Web application are the users and to which the permissions apply and the scope at which the permissions apply. There is also a difference in the permissions lists where individual permissions are selected. Permissions for a Web application are comprehensive settings that apply to all users and groups for all site collections within a Web application. The permissions list contains only one column, and all permissions are enabled by default. You must disable specific permissions individually A permission policy level for a Web application contains permissions that enable a subset of users or groups to work with site collections in a specific way. For example, you might want to create a permission policy level for users of a site collection who will be allowed to add, edit, or delete items from a list, open a list, and view items, lists, and pages. However, you might want to prevent the same users from creating or deleting lists, which would require the Manage Lists permission. The permissions list contains a Grant All column and a Deny All column. You can either grant or deny all permissions as part of a permission policy level. You can also grant or deny individual permissions. No permissions are enabled by default. If an individual permission is neither granted nor denied, it can be set at the discretion of the site collection administrator or site administrator.
Manage user permission policy
You can add users to a permission policy, edit the policy settings, and delete users from a permission policy.
The following settings can be specified or changed:
Zone: If a Web application has multiple zones, you can specify the zone that you want the permission policy to apply to. The default is all zones, which can be specified for Windows users only.
Permissions: You can specify Full Control, Full Read, Deny Write, and Deny All permissions, or you can specify a custom permission level.
System: This setting enables SharePoint to display SHAREPOINT\System for system-related activity regardless of the Windows user accounts that have been configured for the hosting application pool and the SharePoint farm service account. You may want to specify this setting to prevent unnecessary information disclosure to end users and potential hackers who would be interested in knowing more about how SharePoint is deployed in your enterprise.
Add users to a permission policy
You may want to add users to a permission policy to ensure that all users are accessing content with the same\ set of permissions.

To add users to a permission policy
1. Verify that you have the following administrative credentials: You must be a member of the Farm Administrators group on the computer that is running the SharePoint Central Administration Web site.
2. On the Central Administration Web site, in the Application Management section, click Manage web applications.
3. Click to highlight the line for the Web application whose permission policy you want to manage.
4. In the Policy group of the ribbon, click User Policy.
5. In the Policy for Web Application dialog box, select the check box next to the user or group that you want to manage, and then click Add Users.
6. In the Add Users dialog box, in the Zone list, click the zone to which you want the permissions policy to apply.
7. In the Choose Users section, type the user names, group names, or email addresses that you want to add to the permissions policy. You can also click the applicable icon to check a name or browse for names.
8. In the Choose Permissions section, select the permissions that you want the users to have.
9. In the Choose System Settings section, check Account operates as System to specify whether a user account should be displayed as SHAREPOINT\System instead of the actual accounts that perform specific tasks within the SharePoint environment.
10. Click Finish.
Source: http://technet.microsoft.com/en-us/library/ff607712.aspx

Question: 177

You deploy a server that has Microsoft SharePoint Foundation 2010 installed.
You create a Web application named WebApp1.
You need to enable anonymous access to WebApp1.
Which settings should you configure first?

A. Anonymous Policy
B. Authentication Providers
C. User Permissions
D. User Policy

Answer: B

Explanation:
Enable anonymous access for a zone of a Web application
1. From Administrative Tools, open the SharePoint Central Administration Web site application.
2. On the Central Administration home page, click Application Management.
3. On the Application Management page, in the Application Security section, click Authentication providers.
4. On the Authentication Providers page, make sure the Web application that is listed in the Web Application box (under Site Actions) is the one that you want to configure. If the listed Web application is not the one
that you want to configure, click the drop-down arrow to the right of the Web Application drop-down list box and select Change Web Application.
5. In the Select Web Application dialog box, click the Web application that you want to configure.
6. On the Authentication Providers page, click the zone of the Web application on which you want to enable anonymous access. The zones that are configured for the selected Web application are listed on the Authentication Providers page.
7. On the Edit Authentication page, in the Anonymous Access section, select Enable Anonymous Access, and then click Save.
At this point, the Web application zone has been enabled for anonymous access.
Source: http://technet.microsoft.com/en-us/library/cc561167.aspx

Question: 178

Your network contains a server that has Microsoft SharePoint Foundation 2010 installed. You discover that the SharePoint database has a large amount of unused space. You need to reduce the amount of unused space in the database. What should you do?

A. From Central Administration, run the farm configuration wizard.
B. From Microsoft SQL Server Management Studio, use the Object Explorer.
C. From the SharePoint 2010 Management Shell, run the Set-SPContentDatabase cmdlet.
D. At the command prompt, run the stsadm.exe command and specify the mergecontentdbs parameter.

Answer: B

Explanation:
How to: Shrink a Database
This topic describes how to shrink a database by using Object Explorer in SQL Server Management Studio. The database cannot be made smaller than the minimum size of the database. The minimum size is the size specified when the database was originally created, or the last explicit size set by using a file-size-changing operation, such as DBCC SHRINKFILE. For example, if a database was originally created with a size of 10 MB and grew to 100 MB, the smallest size the database could be reduced to is 10 MB, even if all the data in the database has been deleted.
To shrink a database
1. In Object Explorer, connect to an instance of the SQL Server Database Engine, and then expand that instance.
2. Expand Databases, and then right-click the database that you want to shrink.
3. Point to Tasks, point to Shrink, and then click Database.
4. Optionally, select the Reorganize files before releasing unused space check box. If selected, a value must be specified for Maximum free space in files after shrinking .
Selecting this option is the same as specifying a target_percent value when executing DBCC SHRINKDATABASE. Clearing this option is the same as executing DBCC SHRINKDATABASE using the TRUNCATEONLY option. TRUNCATEONLY shrinks the file to the last allocated extent. This reduces the file size without moving any data. By default, the option is cleared.
5. Enter the maximum percentage of free space to be left in the database files after the database has been shrunk. Permissible values are between 0 and 99. This option is only available when Reorganize files before releasing unused space is selected.
6. Click OK.
Source: http://technet.microsoft.com/en-us/library/ms189035.aspx

Question: 179

You deploy a server that has Microsoft SharePoint Foundation 2010 installed. You need to ensure that all SharePoint site content and server farm configurations are backed up automatically every night. What should you do?

A. From Central Administration, configure a Full Backup.
B. From Central Administration, configure a Granular Backup.
C. Create a scheduled task that uses the Backup-SPSite cmdlet.
D. Create a scheduled task that uses the Backup-SPFarm cmdlet.

Answer: D

Explanation:
Backup-SPFarm

Creates a backup of an individual database, Web application, or the entire farm.

```
Backup-SPFarm -BackupMethod <String> -Directory <String> [-AssignmentCollection
<SPAssignmentCollection>] [-BackupThreads <Int32>] [-ConfigurationOnly
<SwitchParameter>] [-Confirm [<SwitchParameter>]] [-Force <SwitchParameter>] [-
Item <String>] [-Percentage <Int32>] [-WhatIf [<SwitchParameter>]]
```

Source: http://technet.microsoft.com/en-us/library/ff607881.aspx
Backup-SPSite
Performs a backup of a site collection.

```
Backup-SPSite [-Identity] <SPSitePipeBind> -Path <String> [-AssignmentCollection
<SPAssignmentCollection>] [-Confirm [<SwitchParameter>]] [-Force
<SwitchParameter>] [-NoSiteLock <SwitchParameter>] [-UseSqlSnapshot
<SwitchParameter>] [-WhatIf [<SwitchParameter>]]
```

Source: http://technet.microsoft.com/en-us/library/ff607901.aspx

Question: 180

Your network contains a server that has Microsoft SharePoint Foundation 2010 installed. You need to ensure that a user named User1 can use Central Administration to back up SharePoint site collections. The solution must minimize the number of permissions assigned to User1. To which group should you add User1?

A. local Administrators
B. local Backup Operators
C. SharePoint Delegated Administrators
D. SharePoint Farm Administrators

Answer: D

Explanation:
Group memberships required to run backup and restore operations in Central Administration
You must ensure that all user accounts that will be backing up or restoring your farm and farm components by using Central Administration have the group memberships that are described in the following table.
Required group memberships

Farm component	Member of Administrators group on the local computer	Member of Farm Administrators SharePoint group
Farm	Yes	No
Content Database	Yes	No
Site Collection	No	Yes
Site, list, document library	No	Yes

Question: 181

Your company named Contoso, Ltd. runs Windows Server 2008 R2. You manage a Web server named web.contoso.com. The Web server hosts two Web sites named www.contoso.com and webmail.contoso.com. Users connect to both the sites from the Internet by using HTTP. The new company security policy has the following requirements: · The webmail.contoso.com site must be available for Internet users only through Secure HTTP (HTTPS).
· Two folders named Order and History on www.contoso.com must be available only through HTTPS.
· All users must be able to connect to both sites without receiving any security warnings.
You need to add SSL certificates on web.contoso.com. You must meet the company security policy requirements. What should you do first?

A. Generate a self-signed certificate for web.contoso.com.
B. Generate separate domain certificates for www.contoso.com and webmail.contoso.com.
C. Request one certificate from the public trusted certification authority for web.contoso.com.
D. Request separate certificates from the public trusted certification authority for www.contoso.com and webmail.contoso.com.

Answer: D

Explanation:
The steps for configuring Secure Sockets Layer (SSL) for a site are the same in IIS 7 and IIS 6.0.
There are three things that a browser usually verifies in a server certificate:
1. That the current date and time is within the "Valid from" and "Valid to" date range on the certificate.
2. That the certificate's "Common Name" (CN) matches the host header in the request. For example, if the client is making a request to http://www.contoso.com/, then the CN must also be http://www.contoso.com/.
3. That the issuer of the certificate is a known and trusted CA.
Source: http://learn.iis.net/page.aspx/144/how-to-set-up-ssl-on-iis-7/
Creating Certificate Requests
Each Web site hosted on your Web server needs a separate certificate if you want SSL to work properly. The first step in the certificate creation process is to generate a certificate request.
Source: http://technet.microsoft.com/en-us/library/bb727098.aspx

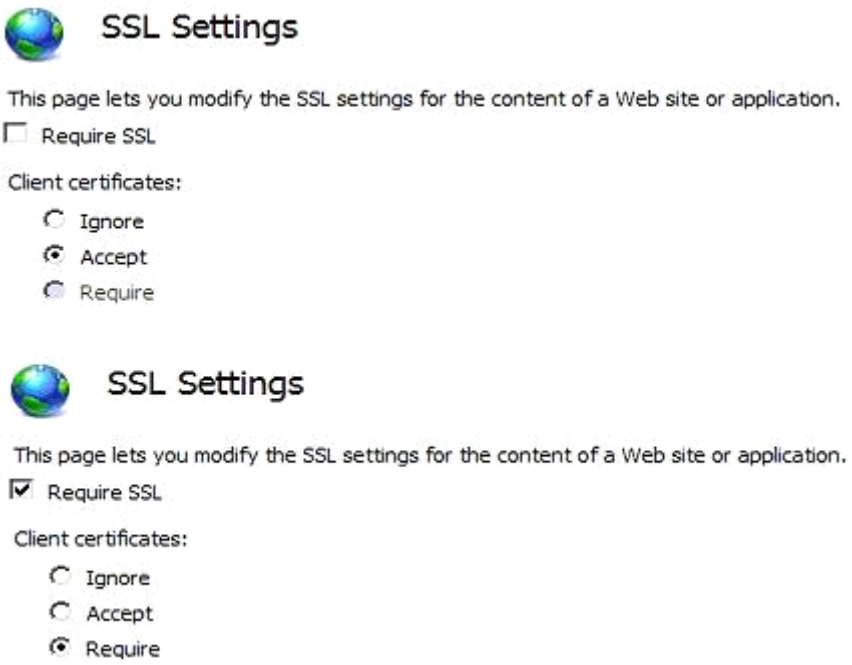
Question: 182

You manage a member server that runs Windows Server 2008 R2. The member server has the Web Server (IIS) server role installed. The server hosts a Web site that is only accessible to the executives of your company. The company policy states that the executives must access the confidential Web content by using user certificates. You need to ensure that the executives can only access the secure Web site by using their installed certificates. What should you do?

A. Configure the SSL settings to Require 128-bit SSL on the confidential Web site.
B. Configure the Client Certificates settings to Accept on the SSL settings for the confidential Web site.
C. Configure the Client Certificates settings to Require on the SSL settings for the confidential Web site.
D. Configure a Certificate Trust list to include the executives' certification authority (CA) certificate.

Answer: C

Explanation:



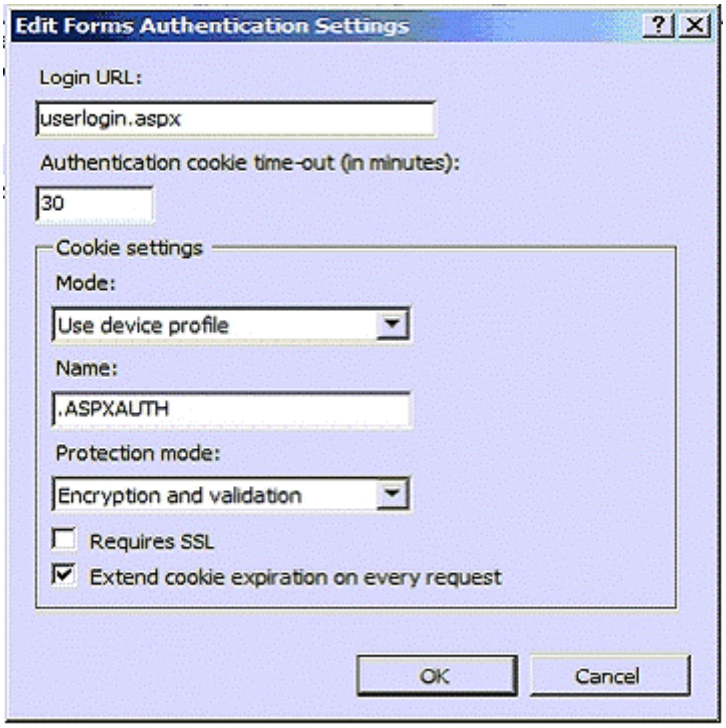
Question: 183

Your company hosts a Web site on a server that runs Windows Server 2008 R2. The server has the Web Server (IIS) server role installed. SSL is configured on the Web site for virtual directories that require encryption. You are implementing a new Web application on the Web site. The new application has its own logon page named userlogin.aspx. You enable Forms Authentication in the Web site properties. You need to configure the Web site to use userlogin.aspx to authenticate user accounts. What should you do?

A. Configure the Forms Authentication Settings to Require SSL.
B. Configure the Name property of the Cookie Settings to the userlogin.aspx filename.
C. Configure the Login URL property for the Forms Authentication Settings to the userlogin.aspx filename.
D. Configure the Default Document setting to add the userlogin.aspx filename in the Web site properties.

Answer: C

Explanation:



Question: 184

You install a new server named Server1 that runs Windows Server 2008 R2. The server has the Streaming Media Services server role installed. You install and activate all Windows Media Services control protocols. Users connect to Server1 locally and remotely through a firewall. You need to ensure that the protocol rollover will occur only if the users are accessing Server1 from the Internet. What should you do?

A. Install the Reliable Multicast Protocol on Server1.
B. Install the Quality of Service (QoS) service on the network adapter.
C. Configure the firewall to forward incoming port 1755 traffic to Server1.
D. Use announcements to enable users to access the streaming media.

Answer: D

Explanation:
You can force your Windows Media server to use a specific protocol by identifying the protocol to be used in the announcement file (for example, rtspu:// server/publishing_point/file). However, to provide an optimal streaming experience for all client versions, we recommend that the URL use the general MMS protocol. If clients connect to your stream using a URL with an MMS URL moniker, any necessary protocol rollover occurs automatically. Be aware that users can disable streaming protocols in the property settings of Windows Media Player. If a user disables a protocol, it is skipped during rollover. For example, if HTTP is disabled, then URLs will not roll over to HTTP.
Source: http://technet.microsoft.com/en-us/library/ee126137.aspx

Question: 185

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2008 R2. A server named Server1 has the Windows Deployment Services (WDS) server role installed. A custom Windows 7 image is available for download from Server1. A server named Server2 has the Hyper-V server role installed. You create a virtual machine (VM) named VM1 on Server2. You need to deploy the Windows 7 image from Server1 to VM1. What

should you do first?

A. On Server1, configure a multicast transmission.
B. On Server1, adjust the PXE Response Delay setting.
C. From the properties of VM1, install a legacy network adapter.
D. From the properties of VM1, install a synthetic network adapter.

Answer: C

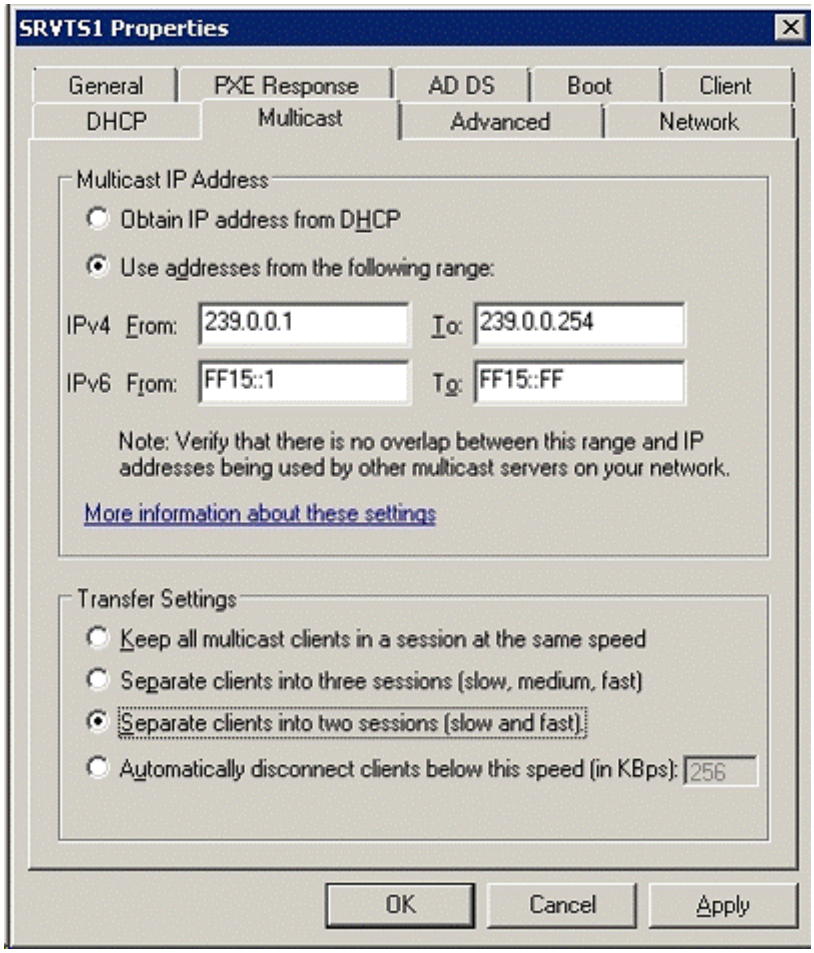
Question: 186

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2008 R2. Routers on the network support multicast transmissions. A server named Server1 has the Windows Deployment Services (WDS) server role installed. A custom Windows 7 image is available for download from Server1. You need to deploy the image to 100 new computers by using multicast. The solution must prevent computers that use low-bandwidth connections from slowing the deployment to computers that use high bandwidth connections. What should you do?

A. Enable Auto-Cast.
B. Enable Scheduled-Cast.
C. From the WDS server properties, adjust the Transfer Settings.
D. From the WDS server properties, modify the Multicast IP Address settings.

Answer: C

Explanation:
To enable multicasting of an install image
Before you create a transmission, you should set the transfer policy for the server. To do this, right-click the server, click Properties, click the Multicast tab, and select an option under Transfer Settings. These settings allow you to enable the following:
Multiple stream transfer. The first option under Transfer Settings uses a single stream for all multicast clients, regardless of client speed. The next two options allow you to separate slower clients into their own multicast stream, which enables faster clients to complete their deployment more quickly instead of being held back by slower clients. These settings are only available for clients that boot into a boot image from Windows 7 or Windows Server 2008 R2.



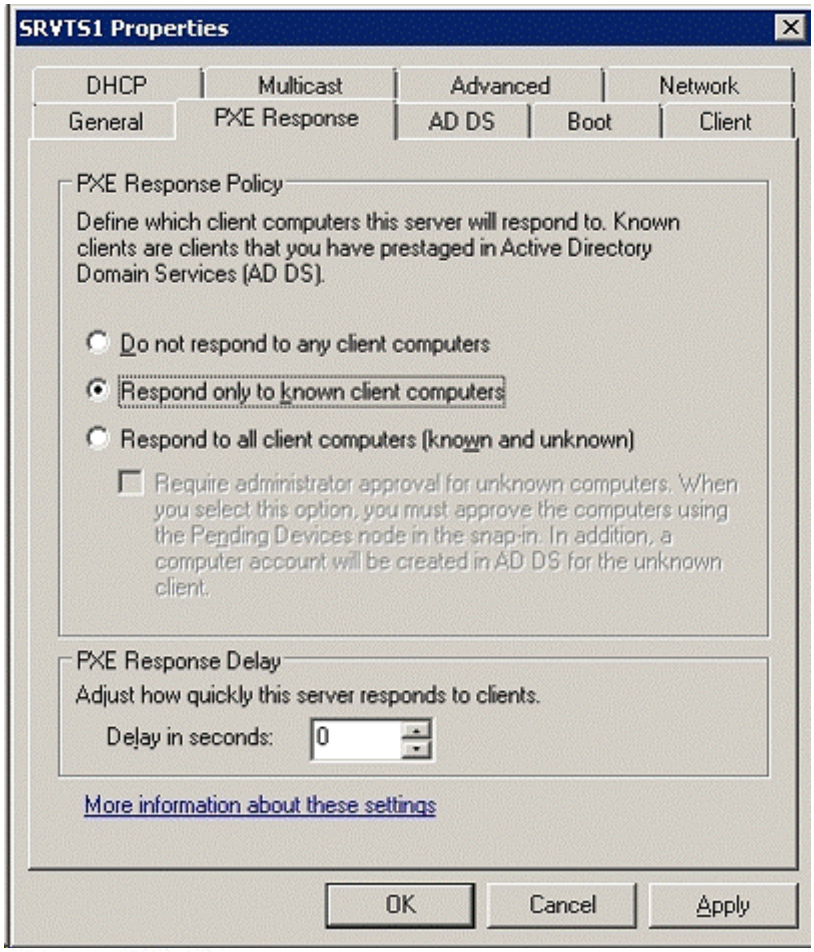
Question: 187

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Windows Deployment Services (WDS) server role installed. You need to ensure that WDS only responds to computers that are prestaged in Active Directory. Which WDS properties should you modify?

A. DHCP Authorization
B. PXE Boot Policy
C. PXE Response Policy
D. Transfer Settings

Answer: C

Explanation:



Option	Explanation
PXE Response Policy	This option specifies how the Windows Deployment Services PXE server responds to incoming client PXE requests. **Respond only to known client computers**. Choose this option if you have prestaged clients in Active Directory. When you select this option, clients that are not prestaged will not be able to PXE boot to the Windows Deployment Services server. **Respond to all (known and unknown) client computers**. Choose this option to allow *all* clients to PXE boot to the Windows Deployment Services server. **For unknown clients, notify administrator and respond after approval**. Choose this option if you want to approve new clients before allowing them to receive boot services from a Windows Deployment Services server.
PXE Response Delay	Use this setting to adjust how quickly the server responds to clients on the network. It sets the amount of time the PXE server waits for other PXE servers to respond. This setting should remain at zero (default) unless there are other PXE responders on the network that have precedence or if your network requires an increased PXE response delay.

Source: http://technet.microsoft.com/en-us/library/cc732360(WS.10).aspx

Question: 188

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Windows Deployment Services (WDS) server role installed. You need to copy a default Windows 7 image to Server1. Which type of image should you add?

A. boot
B. capture
C. discover
D. install

Answer: D

Explanation:
Install images. Install images are the operating system images that you deploy to the client computer. You can use the Install.wim file from the product DVD to deploy images for Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2. For operating systems released prior to Windows Vista, you must create a custom install image.
Source: http://technet.microsoft.com/en-us/library/cc771670%28WS.10%29.aspx

Question: 189

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Windows Deployment Services (WDS) server role installed. You need to create a multicast session to deploy a virtual hard disk (VHD). Which tool should you use?

A. Wdsmcast
B. Wdsutil
C. Windows System Image Manager (SIM)
D. the Windows Deployment Services console

Answer: B

Explanation:
Creating a multicast transmission for a virtual hard disk image
You can create multicast transmissions for your .vhd images in the same way that you can for .wim images (except you can only create the transmissions from the command line).
To create a multicast transmission
1. Click Start, right-click Command Prompt, and then click Run as administrator.
2. Do one of the following:
To create an Auto-Cast transmission, use the following syntax: WDSUTIL /New-MulticastTransmission /
Image:<image name> /FriendlyName:<friendly name> /ImageType:Install /ImageGroup:<Image group name> [/FileName:<file name>] /TransmissionType:AutoCast.
Example: WDSUTIL /New-MulticastTransmission /Image:WindowsServer2008R2 /
ImageType:Install /ImageGroup:"VHD Image Group" /FileName:install.vhd /
TransmissionType:AutoCast
To create a Scheduled-Cast transmission, use the following syntax: WDSUTIL /New-MulticastTransmission /
Image:<image name> /FriendlyName:<friendly name> /ImageType:Install /ImageGroup:<Image group name> /TransmissionType:ScheduledCast [/Time:<yyyy/mm/dd:hh:mm>][/Clients:<no of clients>].
Example: WDSUTIL /New-MulticastTransmission /Image:WindowsServer2008R2 /
ImageType:Install /ImageGroup:"VHD Image Group" /TransmissionType:ScheduledCast
/Time:"2008/01/20:17:00" /Clients:10
Source: http://technet.microsoft.com/en-us/library/dd363560(WS.10).aspx#BKMK5

Question: 190

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Windows Deployment Services (WDS) server role installed. You have a client computer named Client1 that does not support the Pre-boot Execution Environment (PXE). You need to ensure that Client1 can connect to Server1 to download an image. Which type of image should you use?

A. boot
B. capture
C. discover
D. install

Answer: C

Explanation:
Boot images. Boot images are images that you boot a client computer into to perform an operating system installation. In most scenarios, you can use the Boot.wim from the installation DVD (in the \Sources directory). The Boot.wim contains Windows PE and the Windows Deployment Services client (which is basically Windows Vista Setup.exe and supporting files).
Install images. Install images are the operating system images that you deploy to the client computer. You can also use the install.wim from the installation DVD, or you can create your own install image.
Capture images. Capture images are boot images that you boot a client computer into in order to capture the operating system into a .wim file. You can also create media (CD, DVD, USB drive, and so on) that contains a capture image, and then boot a computer from the media. These images provide an alternative to the command-line utility, ImageX.exe. Except in advanced scenarios, you can create a capture image using the Boot.wim file from the Windows Vista media (located in the \Sources folder). You can also use the WinPE.wim from the Windows AIK to create a capture image, which is slightly smaller than the Boot.wim.
Discover images. If you have a computer that is not PXE enabled, you can create a discover image and use it to install an operating system on that computer. When you create a discover image and save it to media (CD, DVD, USB drive, and so on), you can then boot a computer to the media. The discover image on the media locates a Windows Deployment Services server, and the server deploys the install image to the computer. You can configure discover images to target a specific Windows Deployment Services server. This means that if you have multiple servers in your environment, you can create a discover image for each, and then name them based on the name of the server.
Source: http://technet.microsoft.com/en-us/library/cc766320(WS.10).aspx

Question: 191

Your network contains two servers named Server1 and Server2 that run Windows Server 2008 R2. Server1 and Server2 have the Windows Deployment Services (WDS) server role installed. You need to prestage a computer. The solution must ensure that when the prestaged computer is deployed, it downloads a boot image from Server2. What should you do?

A. At the command prompt, run the dsadd.exe server command.
B. From Active Directory Users and Computers, create a new computer account.
C. From Windows PowerShell, run the New-Object cmdlet and specify the property parameter.
D. From the Windows Deployment Services console, modify the PXE Response Settings for the server.

Answer: B

Explanation:
Creating Computer Account Objects in AD DS
You can use Windows Deployment Services to link physical computers to computer account objects in Active Directory Domain Services (AD DS). Computer accounts are created when you:
Create an account before you have attempted a network boot. You can do this using the Active
Directory Users and Computers snap-in or WDSUTIL.
Once a computer is linked to a computer account object in AD DS, the computer is considered “prestaged” or

"known." Then, you can configure properties on the computer account to control the client's installation (using WDSUTIL alone). For example, you can configure the unattend file that the client should receive and the server that the computer should contact for a network boot. For instructions, see the "Prestage Computers" section in How to Manage Client Computers.
Benefits of Prestaging Client Computers Prestaging clients provides three main benefits:
An additional layer of security. You can configure Windows Deployment Services to answer only prestaged clients, therefore ensuring that clients that are not prestaged will not be able to boot from the network. Additional flexibility. Prestaging clients increases flexibility by enabling you to control the following. For instructions on performing these tasks, see the "Prestage Computers" section of How to Manage Client Computers.
- The computer account name and location within AD DS.
- Which server the client should network boot from.
- Which network boot program the client should receive.
- Other advanced options — for example, what boot image a client will receive or what Windows
Deployment Services client unattend file the client should use.
The ability for multiple Windows Deployment Services servers to service the same network segment. You can do this by restricting the server to answer only a particular set of clients. Note that the prestaged client must be in the same forest as the Windows Deployment Services server (trusted forests do not work).
Source: http://technet.microsoft.com/en-us/library/cc770832(WS.10).aspx

Question: 192

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Windows Deployment Services (WDS) server role and the Windows Automated Installation Kit (Windows AIK) installed. You create a new x86 Microsoft Windows Preinstallation Environment (Windows PE) image and add it as a boot image to Server1. You run the Create Capture Image wizard and receive the following error message: "The Windows Deployment Services Image Capture Wizard could not be located in the specified Windows PE image." You need to ensure that you can create a capture image by using the Create Capture Image wizard. What should you do first?

A. Create an x64 Windows PE image and add the image to Server1 as a boot image.
B. Add a new boot image to Server1 and specify the Sources\Boot.wim file from the Windows Server 2008 R2 installation media.
C. Mount the Windows PE boot image and add the contents of the %programFiles%\Windows AIK\Tools \amd64 folder to the image.
D. Mount the Windows PE boot image and add the contents of the %programFiles%\Windows AIK\Tools\PETools folder to the image.

Answer: B

Explanation:
Answer "Create an x64 Windows PE image and add the image to Server1 as a boot image." is most likely incorrect because custom WinPE images are considered an advanced scenario, while just adding the Boot.wim from the Windows Server 2008 R2 installation media is more straightforward.
Custom Capture Images
For advanced scenarios as part of a custom deployment solution, you can create discover or capture images manually by using the tools provided in the Windows AIK.
To create a discover or capture image manually
1. Locate the boot image that you want to modify, and save it to a known location. This boot image can be either the custom boot image that you created earlier, or the Boot.wim from the product DVD.
2. Mount the image using either DISM or ImageX.
3. Create a Winpeshl.ini file in the Windows\System32 folder of the custom boot image with the following section.
[LaunchApps]%SYSTEMROOT%\system32\wdscapture.exe

4. Unmount and commit the changes using either DISM or ImageX.
5. Update the image metadata to reflect any changes to the image name or description.
Source: http://technet.microsoft.com/nl-nl/library/cc730907(WS.10).aspx

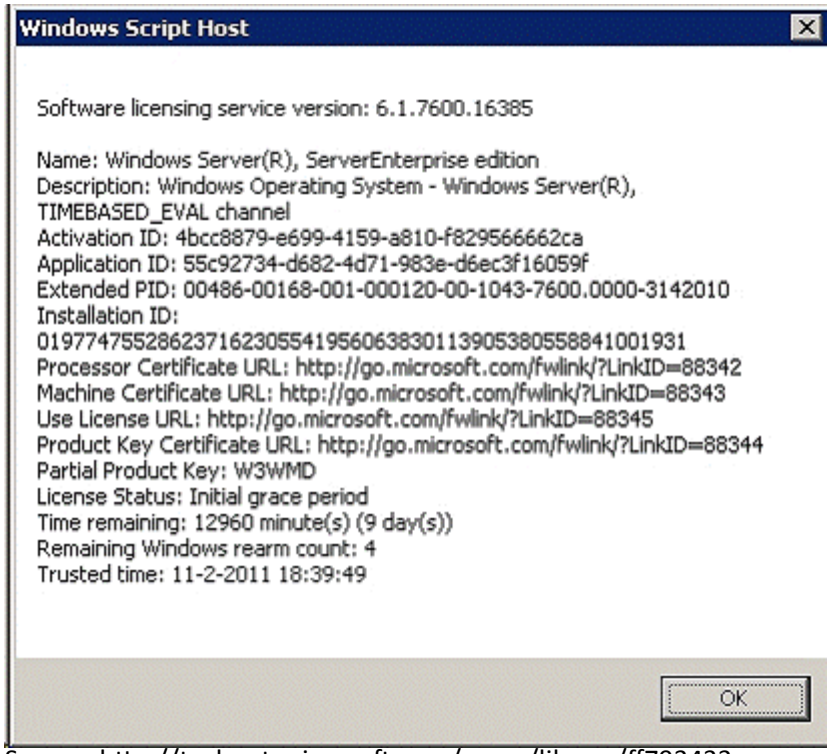
Question: 193

Your network contains a server named Server1 that runs Windows Server 2008 R2. You plan to create an image of Server1 to deploy to additional servers. You need to identify how many more times you can rearm the Windows activation clock. What should you run on Server1?

A. msinfo32.exe
B. slmgr.vbs /dlv
C. slui.exe
D. winrm.vbs enumerate

Answer: B

By default, /dlv displays the license information for the installed operating system. Specifying the [Activation ID] parameter displays the license information for the specified edition associated with that Activation ID. Specifying the [All] parameter displays all applicable installed products' license information.



Source: http://technet.microsoft.com/en-us/library/ff793433.aspx

Question: 194

Your network contains a server named Server1 that runs Windows Server 2008 R2. The network contains two sites named Site1 and Site2 that are separated by a firewall. Server1 is configured as a Key Management Service (KMS) host located in Site1. You need to configure the firewall so that computers in Site2 can activate Windows by using Server1. Which TCP port should you allow through the firewall?

A. 135

B. 443
C. 1433
D. 1688

Answer: D

Explanation:
KMS requires a firewall exception on the KMS host. If using the default TCP port, enable the KMS Traffic exception in Windows Firewall. If using a different firewall, open TCP port 1688. If using a non-default port, open the custom TCP port in the firewall. Source: http://technet.microsoft.com/en-us/library/ff793409.aspx

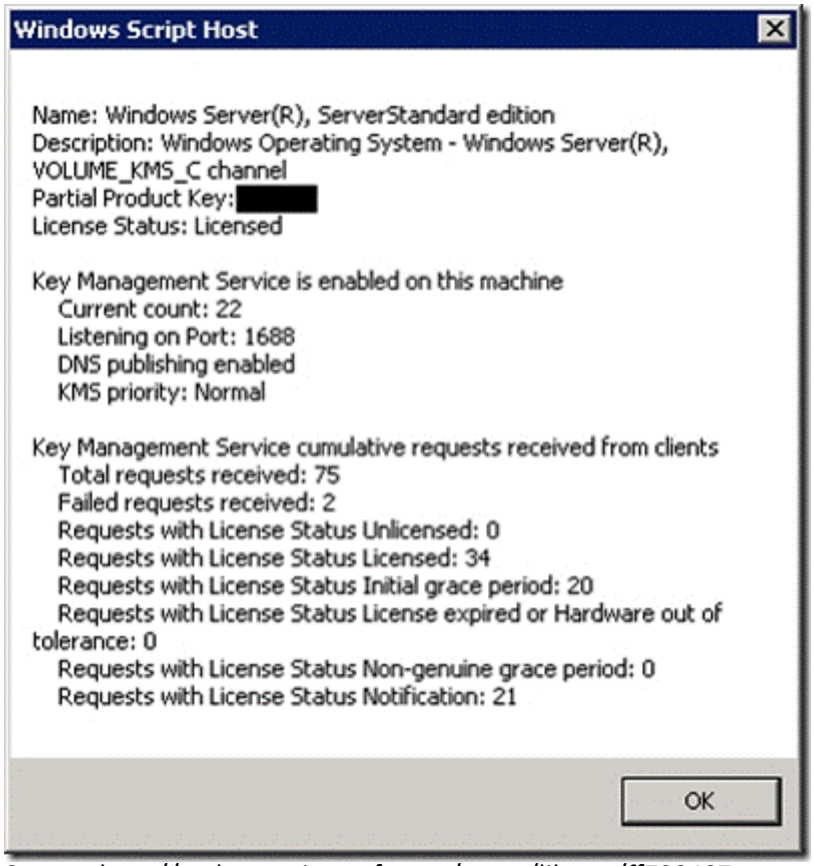
Question: 195

You have a server named Server1 that runs Windows Server 2008 R2. Server1 has the Key Management Service (KMS) installed. You need to identify how many computers were activated by Server1. What should you run?

A. cliconfg.exe
B. mrinfo.exe Server1
C. slmgr.vbs /dli
D. slui.exe

Answer: C

Explanation:
slmgr.vbs /dli - Retrieves the current KMS activation count from the KMS host.



Source: http://technet.microsoft.com/en-us/library/ff793407.aspx

Question: 196

Your network contains four servers that run Windows Server 2008 R2. The servers are configured as shown in the following table.

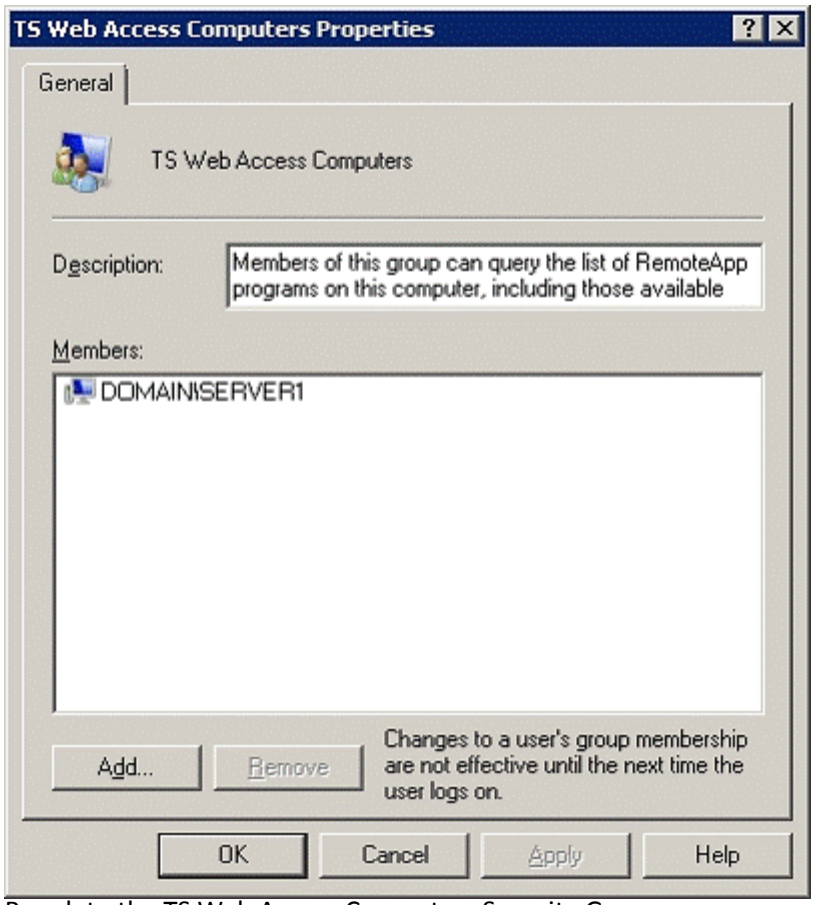
Server name	Role services
Server1	Remote Desktop Web Access (RD Web Access)
Server2	Remote Desktop Session Host (RD Session Host)
Server3	Remote Desktop Session Host (RD Session Host)
Server4	Remote Desktop Connection Broker (RD Connection Broker)

Server4 Remote Desktop Connection Broker (RD Connection Broker) Server2 and Server3 are configured as RemoteApp sources on Server4. You need to ensure that the RemoteApp programs are listed on the RD Web Access Web page on Server1. What should you do?

A. On Server4, add Server1 to the Session Broker Computers group.
B. On Server4, add Server1 to the TS Web Access Computers group.
C. On Server1, add Server4 to the TS Web Access Administrators group.
D. On Server1, add Server2 and Server3 to the TS Web Access Administrators group.

Answer: B

Explanation:



Populate the TS Web Access Computers Security Group

If the RD Web Access server and the Remote Desktop Session Host (RD Session Host) server that hosts the RemoteApp programs are separate servers, you must add the computer account of the RD Web Access server to the TS Web Access Computers security group on the RD Session Host server.
To add the computer account of the RD Web Access server to the security group
On the RD Session Host server, click Start, point to Administrative Tools, and then click Computer Management.
In the left pane, expand Local Users and Groups, and then click Groups.
In the right pane, double-click TS Web Access Computers.
In the TS Web Access Computers Properties dialog box, click Add.
In the Select Users, Computers, or Groups dialog box, click Object Types.
In the Object Types dialog box, select the Computers check box, and then click OK.
In the Enter the object names to select box, specify the computer account of the RD Web Access server, and then click OK.
Click OK to close the TS Web Access Computers Properties dialog box.
Source: http://technet.microsoft.com/en-us/library/cc771623.aspx

Question: 197

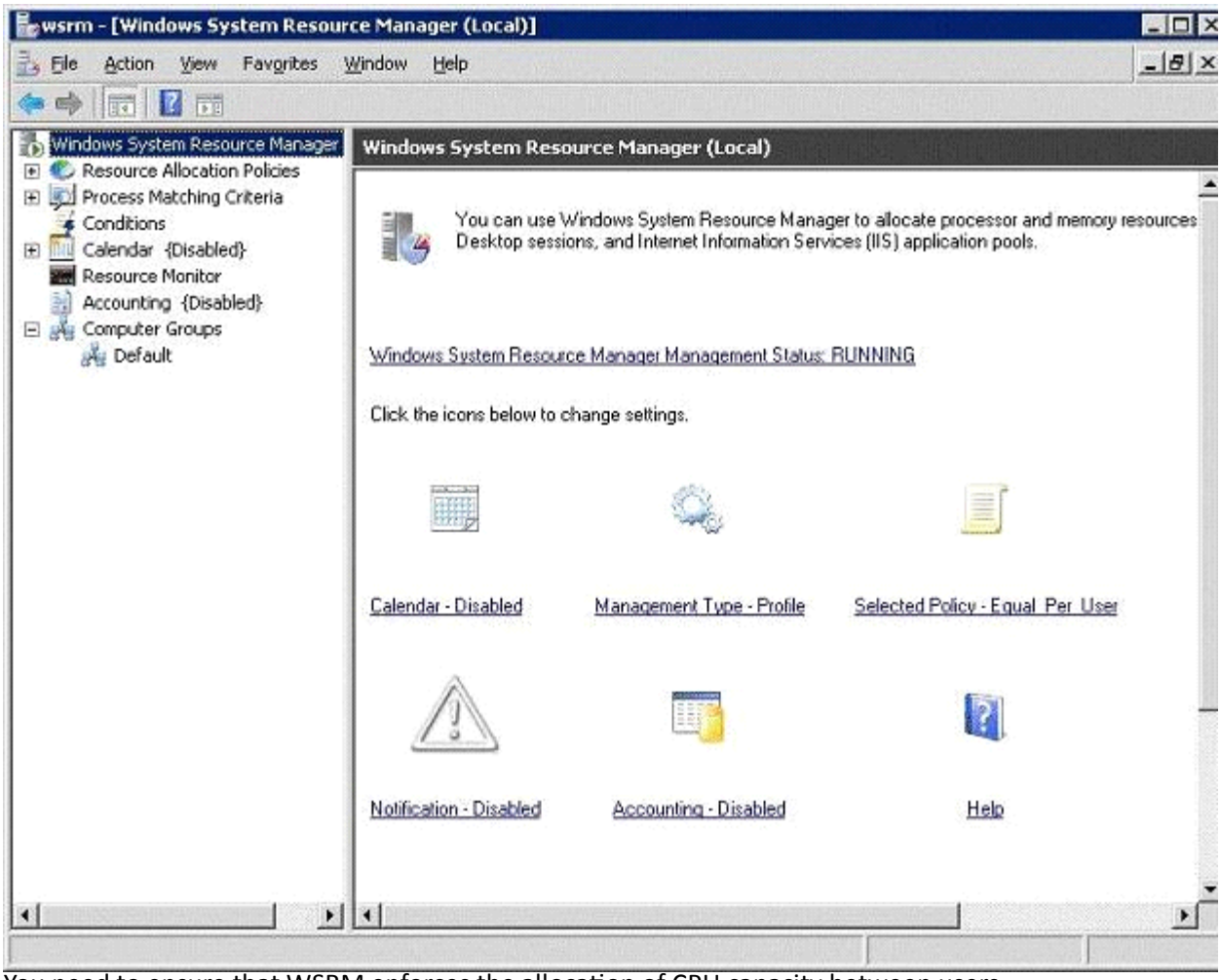
Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Remote Desktop Session Host (RD Session Host) role service installed. Server1 hosts Remote App programs. Two hundred users connect to Server1 to run the RemoteApp programs. You need to use Performance Monitor to view the CPU usage of each RemoteApp program. Which Performance Monitor object should you monitor?

A. Process
B. Processor
C. Terminal Services
D. Terminal Services Session

Answer: A

Question: 198

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server 1 has the Remote Desktop Session Host (RD Session Host) role service installed. On server1, you install and configure the Windows System Resource Manager (WSRM) feature as shown in the exhibit. (Click the Exhibit button.)



You need to ensure that WSRM enforces the allocation of CPU capacity between users.
What should you do?

A. Enable Accounting.
B. Change the Management type to Manage.
C. Add Server1 to the Default computer group.
D. Change the resource allocation policy to Equal_per_process.

Answer: B

Explanation:
Management type
When the management type is Manage, resources are actively managed according to the resource allocation policy that is currently in effect.
When the management type is Profile, accounting information is logged according to the resource allocation policy that is currently in effect, but the resources are not actually being managed.
Source: http://technet.microsoft.com/en-us/library/cc730662.aspx

Question: 199

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Remote Desktop Session Host (RD Session Host) role service and the Windows System Resource Manager (WSRM) feature installed. Users from two Active Directory groups named Group1 and Group2 connect to Server1 and run the same RemoteApp

program. You need to ensure that when Server1 experiences high CPU usage, Group1 users have priority over Group2 users regarding the use of CPU resources. You want to achieve this goal by using the minimum amount of administrative effort. What should you do from the WSRM console?

A. Add a new Conditional Policy.
B. Create a new Calendar Schedule.
C. Create a new Process Matching criteria.
D. Implement Weighted_Remote_Sessions.

Answer: D

Explanation:
When the Weighted_Remote_Sessions resource allocation policy is managing the system, the processes are grouped according to the priority assigned with the user account. For example, if three users are remotely connected, the user assigned Premium priority will receive highest priority access to the CPU, the user assigned Standard priority will receive second priority to the CPU, and the user assigned Basic priority will receive lowest priority to the CPU. This policy is for use with RD Session Host servers.
Source: http://technet.microsoft.com/en-us/library/cc732553.aspx

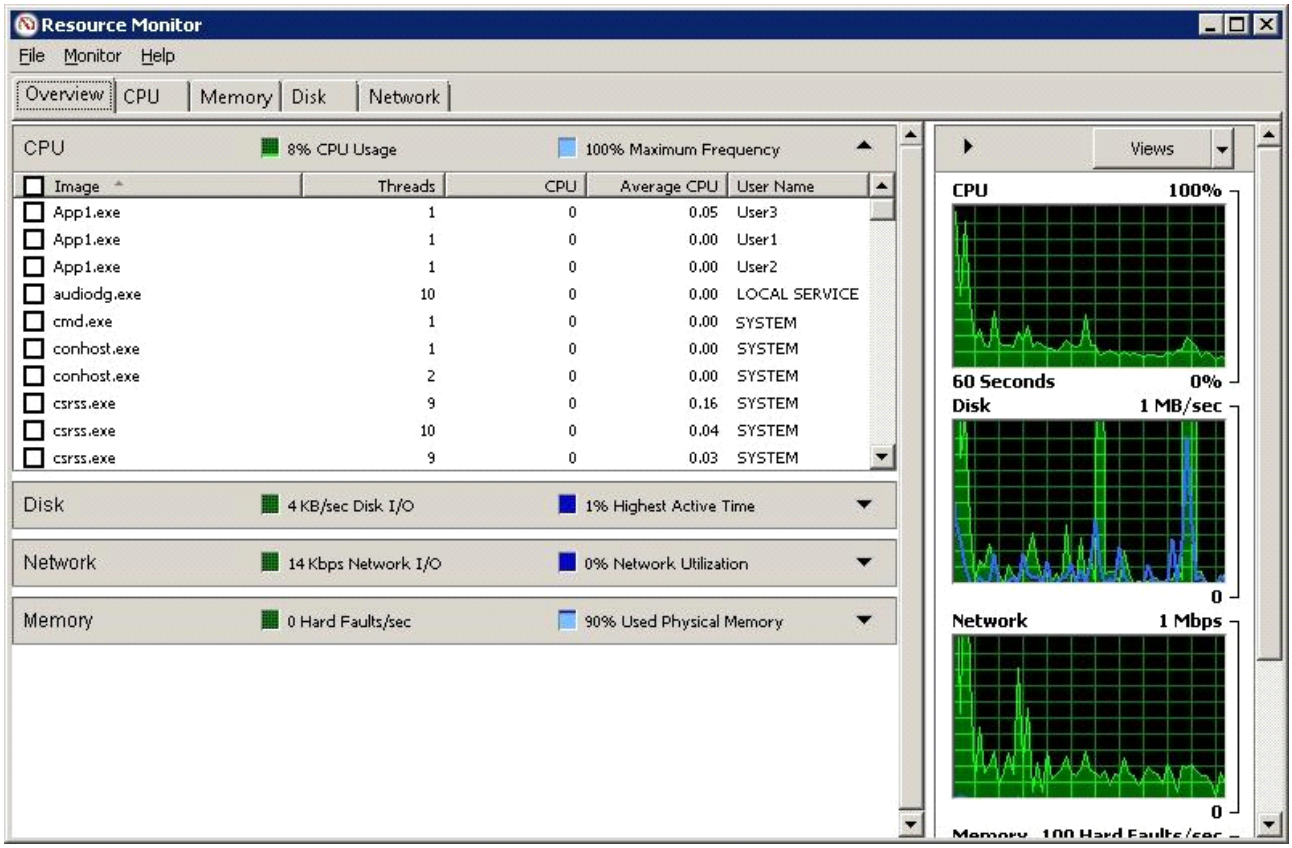
Question: 200

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Remote Desktop Session Host (RD Session Host) role service installed. Server1 hosts a RemoteApp program named App1. You need to view a list of users who are currently running App1. The list must display the CPU resources that App1 uses for each user. Which tool should you use?

A. Performance Monitor
B. RemoteApp Manager
C. Remote Desktop Services Manager
D. Resource Monitor

Answer: D

Explanation:



Question: 201

Your network contains two servers. The servers are configured as shown in the following table.

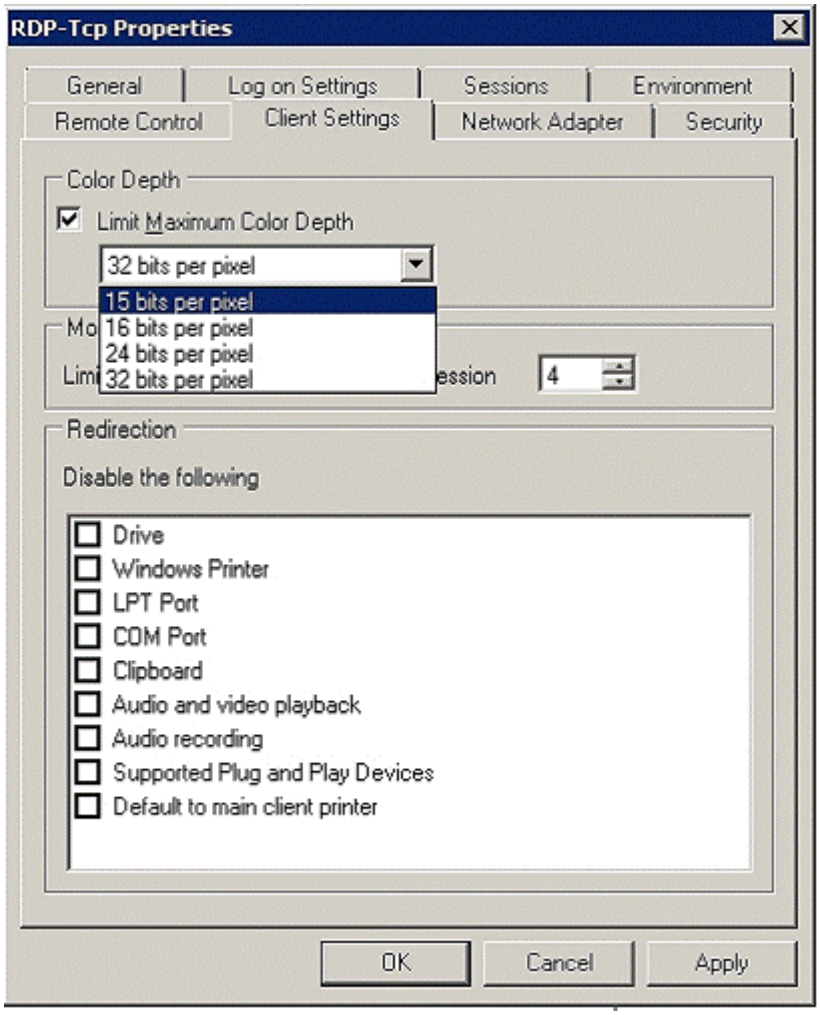
Server name	Role services
Server1	Remote Desktop Session Host (RD Session Host) Windows System Resource Manager (WSRM)
Server2	Remote Desktop Gateway (RD Gateway)

You need to limit the display quality of Remote Desktop connections.
What should you do?

A. Create a Remote Desktop resource allocation policy (RD RAP) on Server2. B. Create a Windows System Resource Manager (WSRM) resource allocation policy on Server1. C. Edit the properties of the RDP-Tcp connection on Server1. D. Edit the properties of the Remote Desktop connection authorization policy (RD CAP) on Server2.

Answer: C

Explanation:



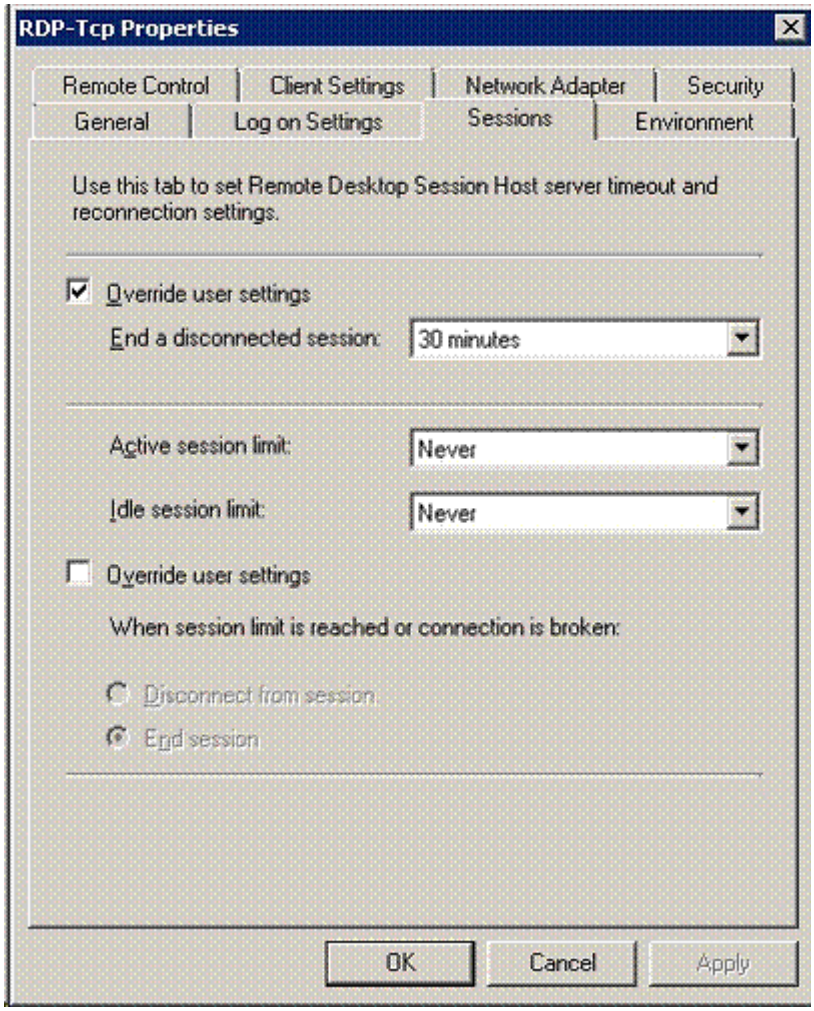
Question: 202

Your network contains a server named Server1. Server1 has the Remote Desktop Session Host (RD Session Host) role service installed. You need to ensure that when a user disconnects a Remote Desktop connection, the connection is forcibly terminated after 30 minutes. Which RDP-Tcp settings should you configure?

A. Client Settings
B. Environment
C. Log on Settings
D. Sessions

Answer: D

Explanation:



Question: 203

Your network contains a server named Server1 that has the Remote Desktop Licensing (RD Licensing) role service installed. You need to ensure that you can restore the RD Licensing environment if Server1 fails. What should you include in the backup? (Each correct answer presents part of the solution. Choose two.)

A. the folder that contains the configuration files of the license server
B. the folder that contains the database of the license server
C. the local certificate store
D. the system state

Answer: B, D

Explanation:
Back Up a Remote Desktop License Server
You should back up your Remote Desktop license server regularly by using the Windows Server Backup tool or the backup software deployed in your environment. This helps protect your licensing data from accidental loss if your system experiences hardware or storage failure. When backing up a license server, back up both the System State data and the folder in which the RD
Licensing database is installed. This ensures that data in both the registry and the RD Licensing database is backed up
Source: http://technet.microsoft.com/en-us/library/cc753582.aspx

Question: 204

Your network contains a single Active Directory domain. The domain contains two servers. The servers are configured as shown in the following table.

Server name	Role services
Server1	Remote Desktop Licensing (RD Licensing) Remote Desktop Session Host (RD Session Host)
Server2	Remote Desktop Session Host (RD Session Host)

Server2 is configured to use Server1 as a licensing server. You install 100 Remote Desktop Services Per User client access licenses (RDS Per User CALs) on Server1. You discover that when users connect to Remote Desktop Services (RDS) on Server2, they receive temporary licenses. You need to ensure that users receive permanent licenses when they connect to Server2. What should you do?

A. On Server2, install the RD Licensing role service.
B. On Server2, change the Remote Desktop licensing mode to Per User.
C. On Server1, remove the RD Session Host role service.
D. On Server1, change the discovery scope of the license server to Domain.

Answer: B

Explanation:
When a Remote Desktop Session Host (RD Session Host) server is configured to use Per Device licensing mode, and a client computer or device connects to an RD Session Host server for the first time, the client computer or device is issued a temporary license by default. When a client computer or device connects to an RD Session Host server for the second time, if the Remote Desktop license server is activated and enough RDS Per Device CALs are available, the license server issues the client computer or device a permanent RDS Per Device CAL. If the license server is not activated or does not have any RDS Per Device CALs available, the device continues to use the temporary license. The temporary license is valid for 90 days. Because no Per Device CALs are available, we've got "100 Remote Desktop Services Per User client access licenses (RDS Per User CALs)" on Server1, the device will never get its permanent Per Device CAL.
Source: http://technet.microsoft.com/en-us/library/cc732416.aspx

Question: 205

Your network contains two servers that run Windows Server 2008 R2. The servers are configured as shown in the following table.

Server name	Role services
Server1	Remote Desktop Licensing (RD Licensing)
Server2	Remote Desktop Session Host (RD Session Host)

The network contains 100 client computers that connect to Remote Desktop Services (RDS) on Server2. Server1 has 100 Remote Desktop Services Per Device client access licenses (RDS Per Device CALs) installed. You exchange 10 client computers for 10 new client computers. You need to ensure that the RDS Per Device CALs allocated to the old client computers can be immediately reallocated to the new client computers. What should you do?

A. From the Remote Desktop Session Host Configuration console on Server2, modify the Licensing settings.
B. From the Remote Desktop Licensing Manager tool on Server1, run the Manage RDS CALs wizard and click the Migrate action.

C. From the Remote Desktop Licensing Manager tool on Server1, navigate to the Windows Server 2008 R2 - Installed RDS Per Device CALs node and run the Install Licenses wizard.
D. From the Remote Desktop Licensing Manager tool on Server1, navigate to the Windows Server 2008 R2 - Installed RDS Per Device CALs node and click the Revoke RDS CAL action.

Answer: D

Explanation:
Revoke a Remote Desktop Services Per Device Client Access License
When a Remote Desktop Session Host (RD Session Host) server is configured to use Per Device licensing mode, and a client computer or device connects to an RD Session Host server for the first time, the client computer or device is issued a temporary license by default. When a client computer or device connects to an RD Session Host server for the second time, if the Remote Desktop license server is activated and enough RDS Per Device CALs are available, the license server issues the client computer or device a permanent RDS Per Device CAL. If the license server is not activated or does not have any RDS Per Device CALs available, the device continues to use the temporary license. The temporary license is valid for 90 days. In some circumstances, you might want or need to return an RDS Per Device CAL that has been issued back to the available pool on the license server before the automatic expiration period has been reached. For example, you might want to do this if the client computer or device is no longer a part of your environment. You can revoke an RDS Per Device CAL by using the Remote Desktop Licensing Manager tool. After you have revoked the RDS Per Device CAL, that RDS Per Device CAL is immediately available to be issued to another client computer or device. Revocation is not a substitute for ensuring that you have enough RDS Per Device CALs to support your environment. You can only revoke up to twenty percent of the number of RDS Per Device CALs of a particular version installed on your license server.
Source: http://technet.microsoft.com/en-us/library/cc732416.aspx

Question: 206

Your network contains a server named Server1 that has the Remote Desktop Licensing (RD Licensing) role service installed. You install the RD Licensing role service on a server named Server2. You need to move all Remote Desktop Services client access licenses (RDS CALs) from Server1 to Server2. What should you do?

A. From the Remote Desktop Session Hosts console on Server1, modify the licensing settings.
B. From the Remote Desktop Session Hosts console on Server2, modify the licensing settings.
C. From the Remote Desktop Licensing Manager console on Server2, run the Manage RDS CALs Wizard.
D. From the Remote Desktop Licensing Manager console on Server2, run the Repeat Last Installation action.

Answer: C

Explanation:
You can use the Manage RDS CALs Wizard in the Remote Desktop Licensing Manager tool to migrate Remote Desktop Services client access licenses (RDS CALs) from one Remote Desktop license server to a Remote Desktop license server that is running Windows Server 2008 R2.
Source: http://technet.microsoft.com/en-us/library/dd851844.aspx

Question: 207

Your network contains three servers that run Windows Server 2008 R2. The servers are configured as shown in the following table.

Server name	Role services
Server1	Remote Desktop Licensing (RD Licensing)
Server2	Remote Desktop Session Host (RD Session Host)
Server3	Remote Desktop Session Host (RD Session Host)

Server1 has Remote Desktop Services Per Device client access licenses (RDS Per Device CALs) installed. Server2 and Server3 are members of a Remote Desktop Connection Broker (RD Connection Broker) farm. Four months after Server2 and Server3 are deployed, you discover that users can no longer establish Remote Desktop sessions on Server3. You verify that Server3 is online and that all required services on Server3 run properly. You verify that the users can establish Remote Desktop sessions on Server2. You need to ensure that the users connecting to the RD Connection Broker farm can establish sessions on Server3. What should you do?

A. On Server3, enable dedicated farm redirection.
B. On Server3, configure the Remote Desktop licensing settings.
C. On Server1, install additional RDS Per Device CALs.
D. On Server1, run the Manage RDS CALs wizard and click the Migrate action.

Answer: B

Explanation:
You must configure RD Licensing correctly in order for your RD Session Host server to accept connections from clients. To allow ample time for you to deploy a license server, Remote Desktop Services provides a licensing grace period for the RD Session Host server during which no license server is required. During this grace period, an RD Session Host server can accept connections from unlicensed clients without contacting a license server. The grace period begins the first time the RD Session Host server accepts a client connection. A permanent RDS CAL is issued by a license server to a client connecting to the RD Session Host server. The number of days in the grace period is exceeded. The length of the grace period is based on the operating system running on the RD Session Host server.
The grace periods are as follows:
Source: http://technet.microsoft.com/en-us/library/cc725933.aspx

Question: 208

Your network contains a single Active Directory domain. The domain contains four servers that run Windows Server 2008 R2. The servers are configured as shown in the following table.

Server name	Role services
Server1	Remote Desktop Licensing (RD Licensing)
Server2	Remote Desktop Session Host (RD Session Host)
Server3	Remote Desktop Licensing (RD Licensing)
Server4	Remote Desktop Session Host (RD Session Host)

You need to ensure that Server1 only issues Remote Desktop Services client access licenses (RDS CALs) to Server2. Which two tasks should you perform? (Each correct answer presents part of the solution. Choose two.)

A. On Server1, add Server2 to the Terminal Server Computers group.
B. On Server1, enable the License Server Security Group Group Policy setting.
C. In the domain, add Server2 to the Terminal Server License Servers group.
D. In the domain, configure the Set the Remote Desktop licensing mode Group Policy setting.

Answer: A, B

Explanation:
When the Remote Desktop Licensing role service is installed on the server, the Terminal Server Computers local group is created. The license server will respond only to requests for RDS CALs from Remote Desktop Session Host servers whose computer accounts are members of this group if the Computer Configuration \Administrative Templates\Windows Components\Remote Desktop Services\RD Licensing\License server security group Group Policy setting has been enabled and applied to the license server. By default, the Terminal Server Computers local group is empty. When the Remote Desktop Licensing role service is removed from the server, the Terminal Server Computers local group is deleted.
Source: http://technet.microsoft.com/en-us/library/ee891291(WS.10).aspx

Question: 209

Your network contains a server that has the Remote Desktop Session Host (RD Session Host) role service installed. You need to increase the bandwidth that is allocated for printing and for file transfers between the RD Session Host server and the Remote Desktop clients. What should you do?

A. On the server, modify the RDP-Tcp settings.
B. On the server, modify the FlowControlChannelBandwidth registry setting.
C. On the clients, modify the FlowControlDisplayBandwidth registry setting.
D. On the clients, modify the Local Resources settings of the Remote Desktop connections.

Answer: B

Explanation:
Display data prioritization
Display data prioritization automatically controls virtual channel traffic so that display, keyboard, and mouse data is given a higher priority over other virtual channel traffic, such as printing or file transfers. This prioritization is designed to ensure that your screen performance is not adversely affected by bandwidth intensive actions, such as large print jobs. The default bandwidth ratio is 70:30. Display and input data will be allocated 70 percent of the bandwidth, and all other traffic, such as clipboard, file transfers, or print jobs, will be allocated 30 percent of the bandwidth. You can adjust the display data prioritization settings by making changes to the registry of the terminal server. You can change the value of the following entries under the
HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\TermDD subkey:
FlowControlDisable
FlowControlDisplayBandwidth
FlowControlChannelBandwidth
FlowControlChargePostCompression
If these entries do not appear, you can add them. To do this, right-click TermDD, point to New, and then click DWORD (32-bit) Value.
You can disable display data prioritization by setting the value of FlowControlDisable to 1. If display data prioritization is disabled, all requests are handled on a first-in-first-out basis. The default value for FlowControlDisable is 0. You can set the relative bandwidth priority for display (and input data) by setting the FlowControlDisplayBandwidth value. The default value is 70; the maximum value allowed is 255. You can set the relative bandwidth priority for other virtual channels (such as clipboard, file transfers, or print jobs) by setting the FlowControlChannelBandwidth value. The default value is 30; the maximum value allowed is 255. The bandwidth ratio for display data prioritization is based on the values of FlowControlDisplayBandwidth and FlowControlChannelBandwidth. For example, if FlowControlDisplayBandwidth is set to 150 and FlowControlChannelBandwidth is set to 50, the ratio is 150:50, so display and input data will be allocated 75 percent of the bandwidth.

Source: http://technet.microsoft.com/en-us/library/cc772472(WS.10).aspx

Question: 210

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Remote Desktop Session Host (RD Session Host) role service installed. You need to ensure that Remote Desktop users can use the user interface elements of Windows Aero. What should you do on Server1?

A. Change the display settings.
B. Add the Desktop Experience feature.
C. Install a DirectX 10 compliant video adapter.
D. Add the Quality Windows Audio Video Experience feature.

Answer: B

Explanation:
When a user uses Remote Desktop Connection to connect to a Remote Desktop Session Host (RD Session Host) server, the desktop that exists on the RD Session Host server is reproduced, by default, in the remote session. To make the remote session look and feel more like the user's local Windows 7 desktop experience, install the Desktop Experience feature on an RD Session Host server that is running Windows Server 2008 R2. Desktop Experience installs components and features of Windows 7, such as Windows Media Player, Windows Defender, and Windows Calendar
Source: http://technet.microsoft.com/en-us/library/cc772567.aspx

Question: 211

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the DHCP server role and the Remote Desktop Session Host (RD Session Host) role service installed. Server1 hosts one RemoteApp program named App1. You have 200 client computers that run Windows 7. The client computers obtain their IP configurations from the DHCP server. You enable Remote Desktop IP Virtualization on Server1. You discover that some Remote Desktop connections to App1 are assigned the same IP address. You need to ensure that all Remote Desktop connections receive a unique IP address. What should you do?

A. Reconcile the DHCP scope.
B. Change the properties of the DHCP scope.
C. Change the Remote Desktop licensing settings.
D. Change the mode for Remote Desktop IP Virtualization.

Answer: B

Question: 212

Your network contains a server that runs Windows Server 2008 R2. The server has the Web Server (IIS) role installed. The server has a Web application that uses HTTP. All authentication methods are enabled for the Web application. You need to prevent passwords from being sent over the network in clear text. Which two authentication methods should you disable? (Each correct answer presents part of the solution. Choose two.)

A. Anonymous
B. Basic
C. Digest
D. Forms

E. Windows Integrated

Answer: B, D

Explanation:
Configure Basic Authentication (IIS 7)
Basic authentication requires that users provide a valid user name and password to access content. This authentication method does not require a specific browser, and all major browsers support it. Basic authentication also works across firewalls and proxy servers. For these reasons, it is a good choice when you want to restrict access to some, but not all, content on a server.
However, the disadvantage of Basic authentication is that it transmits unencrypted base64-encoded passwords across the network. You should use Basic authentication only when you know that the connection between the client and the server is secure. The connection should be established either over a dedicated line or by using Secure Sockets Layer (SSL) encryption and Transport Layer Security (TLS). For example, to use Basic authentication with Web Distributed Authoring and Versioning (WebDAV), you should configure SSL encryption.
http://technet.microsoft.com/en-us/library/cc772009(WS.10).aspx
Configuring Forms Authentication (IIS 7)
Forms authentication uses client-side redirection to forward unauthenticated users to an HTML form where they can enter their credentials, which are usually a user name and password. After the credentials are validated, users are redirected to the page they originally requested.
Because Forms authentication sends the user name and password to the Web server as plain text , you should use Secure Sockets Layer (SSL) encryption for the logon page and for all other pages in your application except the home page.
http://technet.microsoft.com/en-us/library/cc771077(WS.10).aspx
Check this link on MSDN for a nice comparisation of all authentication methods:
http://msdn.microsoft.com/en-us/library/aa292114.aspx

Question: 213

Your network contains a Web server that runs a Server Core installation of Windows Server 2008 R2. You need to install the ASP.NET feature on the server. What should you run?

A. appcmd.exe
B. dism.exe
C. sconfig.cmd
D. slmgr.vbs

Answer: B

Explanation:
Enable ASP.NET on Windows Server 2008 R2
Windows Server 2008 R2 Server Core includes subsets of the 2.0/3.0/3.5 .NET Framework. The Framework makes it possible to run an almost full-featured version of ASP.NET. However, there are 3 limitations that you should take into consideration when working with ASP.NET on Server Core:
No MMC Snap-in. To configure, host, and manage Server Core hosted ASP.NET websites, you must do so via a remote connection from an IIS Management Console (i.e. MMC snap-in) running on a client computer. You can also manage practically every aspect of IIS sites and applications via a local administrative command console using the command line utility APPCMD.
No System.Web.Mail Namespace. The namespace System.Web.Mail is not supported because CDOSYS is not present on Server Core. The System.Web.Mail namespace was deprecated some time ago, so chances are that your code is no

longer using them anyway. Use System.Net.Mail instead as it offers the same functionality. The Web Application Tool (WAT) is not available on Windows Server 2008 R2 Core. Before installing the Web Server Role, IIS and dependencies, we must make sure that the .NET Framework is installed. To install the 2.0 and 3.0 .NET Framework, use the Deployment Image Servicing and Management
(DISM) utility using the following parameters:
dism /online /enable-feature /featurename:NetFx2-ServerCore
dism /online /enable-feature /featurename:NetFx3-ServerCore
The optional server role that must be configured to enable ASP.NET on IIS 7 is called IIS-ASPNET. This role has various pre-requisites that must first be installed. The first one is the Web Server Role, which can be enabled via following command:
dism /online /enable-feature /featurename:IIS-WebServerRole
Once you have enabled the IIS-WebServerRole, three additional roles must be installed prior to the installation of the IIS-ASPNET role:
IIS-ISAPIFilter
IIS-ISAPIExtensions
IIS-NetFxExtensibility
These roles are installed by issuing the following commands (in corresponding order):
dism /online /enable-feature /featurename:IIS-ISAPIFilter
dism /online /enable-feature /featurename:IIS-ISAPIExtensions
dism /online /enable-feature /featurename:IIS-NetFxExtensibility
Now, install the IIS-ASPNET optional feature using the following command:
dism /online /enable-feature /featurename:IIS-ASPNET
Source: http://code.msdn.microsoft.com/R2CoreASPNET

Question: 214

You create a managed service account. You need to configure a Web application pool to use the managed service account. What should you do first?

A. Add the account to the IIS_IUSRS group.
B. Run the New-WebServiceProxy cmdlet.
C. Run the Install-ADServiceAccount cmdlet.
D. Modify the permissions of the computer account.

Answer: C

Explanation:
Managed service accounts and virtual accounts are two new types of accounts introduced in Windows ServerR 2008 R2 and WindowsR 7 to enhance the service isolation and manageability of network applications such as
Microsoft Exchange and Internet Information Services (IIS).
To create a new managed service account
1. On the domain controller, click Start, and then click Run.
2. In the Open box, type dsa.msc, and then click OK to open the Active Directory Users and Computers snapin.
3. Confirm that the Managed Service Account container exists.
4. Click Start, click All Programs, click Windows PowerShell 2.0, and then click the Windows PowerShell icon.
5. Run the following command:
New-ADServiceAccount [-SAMAccountName <String>] [-Path <String>] .
To install a managed service account on a local computer
1. Click Start, click All Programs, click Windows PowerShell 2.0, and then click the Windows PowerShell icon.
2. Run the following command:
Install-ADServiceAccount [-Identity] <ADServiceAccount> [-Confirm] [-WhatIf] [-

Credential <PSCredential>].
To use the Internet Information Services (IIS) Manager snap-in to configure a service to use a managed service account
1. Click Start, point to Administrative Tools, and then click Internet Information Services (IIS) Manager .
2. Double-click <Computer name>, double-click Application Pools, right-click <Pool Name>, and click Advanced Settings.
3. In the Identity box, click …, click Custom Account, and then click Set.
4. Type the name of the managed service account in the format domainname\accountname.
Important: Leave the password blank, and ensure that the account name has a dollar sign ($) at the end.
5. Under Application Pool Tasks, click Stop, and then click Start.
Source: http://technet.microsoft.com/en-us/library/dd548356.aspx

Question: 215

Your network contains a Web server that runs Windows Server 2008 R2. Users can connect to the Default Web Site. You create a new Web site and assign the site a host header. Users cannot connect to the new Web site by using the host header. You need to ensure that users can connect to the new Web site by using the host header. What should you do?

A. Create an Alias (CNAME) record in DNS for the host header.
B. Create a service location (SRV) record in DNS for the host header.
C. Modify the Windows Firewall configuration on the Web server.
D. Modify the Windows Firewall configuration on the users' computers.

Answer: A

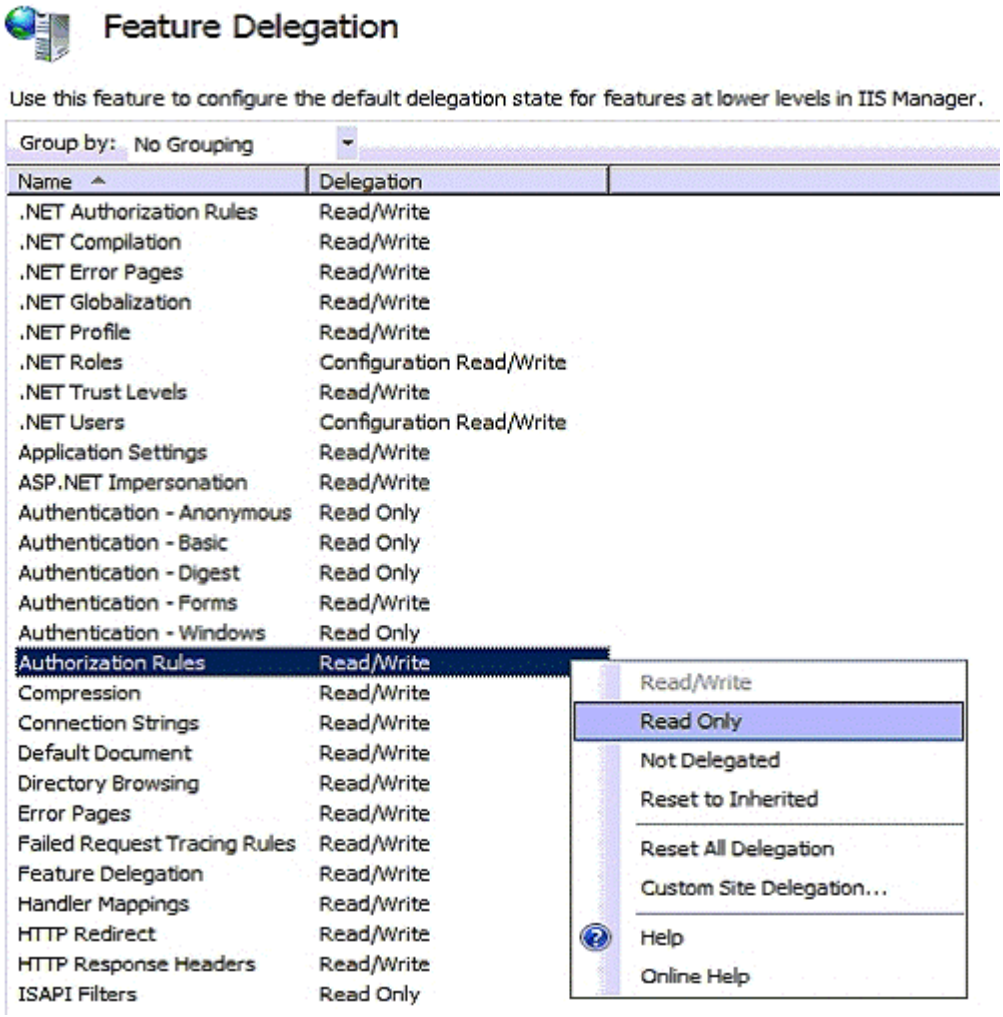
Question: 216

Your network contains a Web server that runs Windows Server 2008 R2. Remote management is configured for Internet Information Services (IIS). From IIS Manager Permissions, you add a user to a Web site. You need to prevent the user from using Internet Information Services (IIS) Manager to modify the authorization rules of the Web site. Which settings should you configure?

A. Authorization Rules
B. Feature Delegation
C. IIS Manager Permissions
D. IIS Manager Users

Answer: B

Explanation:



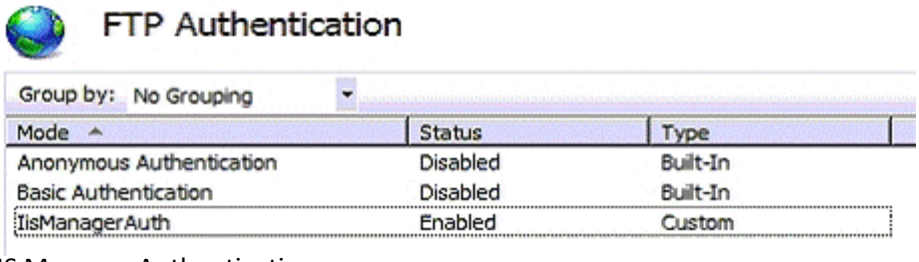
Question: 217

Your network contains an FTP server that runs Windows Server 2008 R2. You create an FTP site on the server and allow Read access for all users. You create an IIS Manager user account for a user named User1. You need to ensure that User1 can connect to the FTP site. What should you do?

A. Enable FTP user isolation
B. Enable Basic authentication
C. Add an FTP authorization rule
D. Add a custom provider for FTP authentication

Answer: D

Explanation:



IIS Manager Authentication
IIS Manager authentication is a custom authentication method that requires users to provide a valid IIS Manager user name and password to gain access to content. IIS Manager authentication requires that the IIS Management Service is installed and configured to use both Windows credentials and IIS Manager credentials. (The IIS Management Service does not have to be running when you use IIS Manager authentication.)
Source: http://technet.microsoft.com/en-us/library/dd722688.aspx

Question: 218

You network contains an Active Directory domain named contoso.com. The domain contains an FTP server named Server1.

You create a domain user account named User1. You create an FTP site on Server1 and configure the site to use a host name of public.contoso.com. You need to log on to the FTP site as User1. What should you specify as the username?

A. contoso.com\user1
B. public.contoso.com|user1
C. user1
D. user1@contoso.com

Answer: B

Explanation:
Logging in to the First FTP Site Using Your Administrator Account
1. On your FTP server, open a command prompt session.
2. Type the following command to connect to your FTP server:
FTP 127.0.0.1
3. When prompted for a user name, enter the "www.example.com" virtual host name followed by the vertical line (|) character.
For example: "www.example.com|administrator"
4. When prompted for a password, enter your administrator password.
5. You should now be logged in to the "www.example.com" FTP site as the local administrator.
Logging in to the Second FTP Site Using Your Administrator Account
1. On your FTP server, open a command prompt session.
2. Type the following command to connect to your FTP server:
FTP 127.0.0.1
3. When prompted for a user name, enter the "www.contoso.com" virtual host name followed by the vertical line (|) character.
For example: "www.contoso.com|administrator"
4. When prompted for a password, enter your administrator password.
5. You should now be logged in to the "www.contoso.com" FTP site as the local administrator.
Source: http://learn.iis.net/page.aspx/320/using-ftp-virtual-host-names/
FTP 7.0 introduced support for virtual host names as documented in the article http://learn.iis.net/page.

aspx/320/using-ftp-virtual-host-names/. Because of variety of compatibility challenges, the decision was made to use the pipe sign "|" as a separator between the virtual host name and the actual account name. To connect to an ftp site configured with virtual host name such as ftp.contoso.com, that was sharing port 21 with some other site, one would need to type ftp.contoso.com|ftpuser to log on successfully.
Source: http://blogs.iis.net/jaroslad/archive/2009/04/16/addressing-the-separator-problem-for-virtual-ftp-sites-ftp-7-5.aspx
Since you have a single IP, you can use FTP virtual hosts by adding a host name to each FTP binding, e.g. ftp.contoso.com, ftp.fabrikam.com, etc. When your FTP users log in, they just need to specify the FTP virtual host name as part of their login, e.g. ftp.contoso.com|user1, ftp.fabrikam.com|user2, etc. Jaroslav discussed the FTP useDomainNameAsHostName attribute in one of his blog posts, which allows you to use a backslash ("\") instead of a pipe ("|") character, so you can use login strings like ftp.contoso.com\user1, ftp.fabrikam.com\user2, etc.
Source: http://forums.iis.net/t/1162437.aspx

Question: 219

Your network contains an FTP server named Server1. Server1 has an FTP site named FTP1. You need to hide all of the files in FTP1 that have an .exe file extension. The solution must ensure that users can list other files in FTP1. What should you modify?

A. the FTP authorization rules
B. the FTP directory browsing
C. the FTP request filtering
D. the NTFS permissions

Answer: C

Explanation:
Use the FTP Request Filtering feature page to define the request filtering settings for your FTP site. FTP request filtering is a security feature that allows Internet service providers (ISPs) and Application service providers to restrict protocol and content behavior. For example, using the File Name Extensions tab you can specify a list of file name extensions that are allowed or denied.
Source: http://technet.microsoft.com/en-us/library/dd851560.aspx

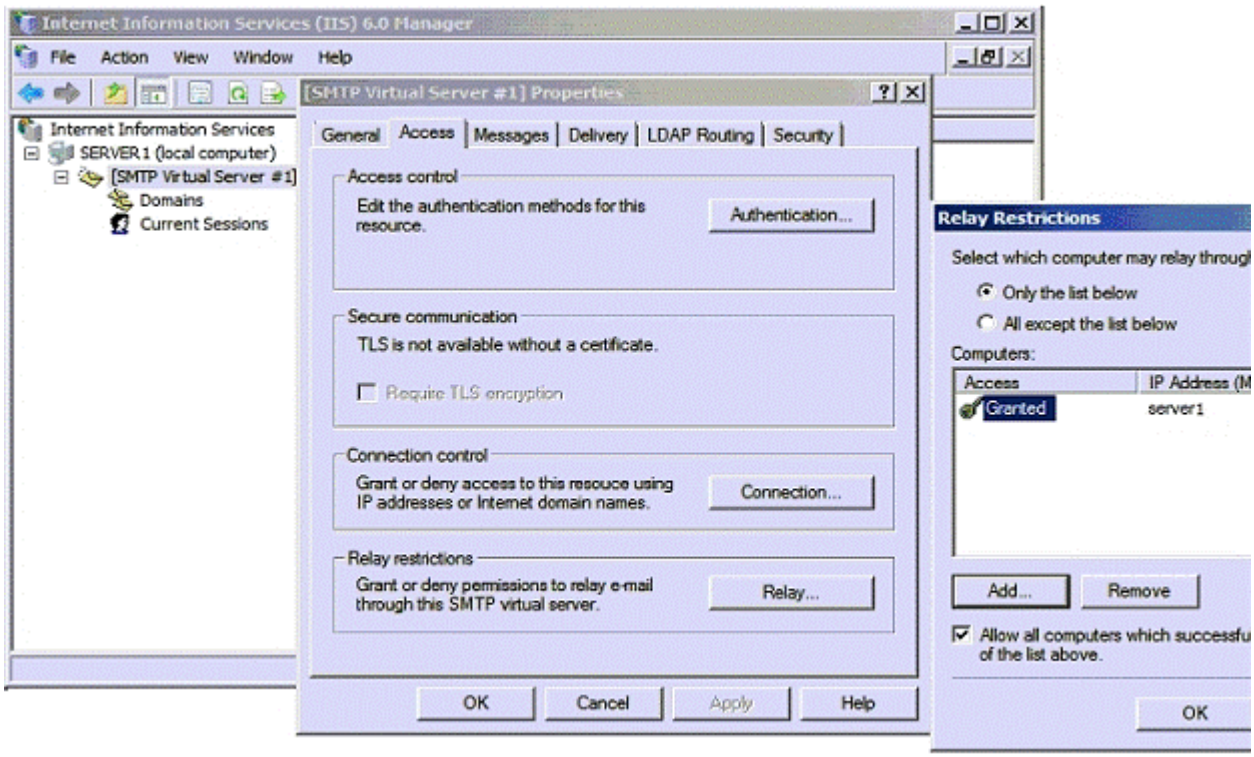
Question: 220

Your network contains two standalone servers named Server1 and Server2. Server1 has Microsoft SQL Server 2008 Reporting Services installed. Server2 has the SMTP Server feature installed. You configure the Reporting Services on Server1 to send reports by using Server2. You need to ensure that Server2 sends the reports.
What should you do on Server2?

A. Configure a smart host
B. Configure TLS encryption
C. Modify the Relay restrictions settings
D. Modify the Connection control settings

Answer: C

To change the SMTP Virtual Server Relay Restrictions, one needs to use the Internet Information Servers (IIS) 6.0 Manager. This is an IIS Role Service that needs to be installed (IIS 6 Management Console)



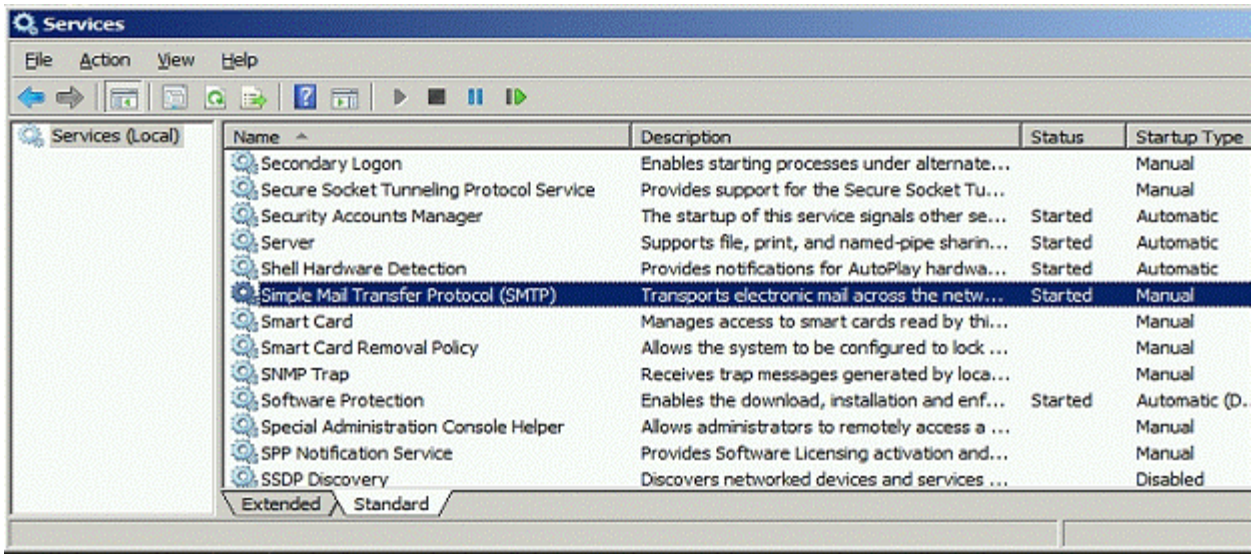
Question: 221

Your network contains an SMTP server named server1.contoso.com that runs Windows Server 2008 R2. You run telnet.exe server1.contoso.com 25 and successfully connect to Server1. You restart Server1. You run telnet.exe server1.contoso.com 25 again and fail to connect to Server1. You need to ensure that you can connect to the SMTP service on Server1. What should you modify first?

A. the access control settings of the SMTP Virtual Server
B. the properties of the Simple Mail Transfer Protocol (SMTP) service
C. the security settings of the SMTP Virtual Server
D. Windows Firewall on Server1

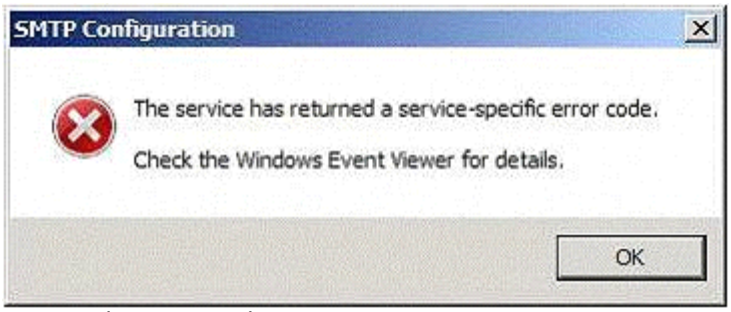
Answer: B

Explanation:



Question: 222

Your network contains an SMTP server.
You discover that the server has two SMTP Virtual Servers named SMTP1 and SMTP2.
SMTP1 starts and SMTP2 stops.
You attempt to start SMTP2 and receive the following error message.



You need to ensure that you can start SMTP2.
Which settings should you modify on SMTP2?

A. Access control
B. Advanced Delivery
C. Connection Control
D. IP address and TCP port

Answer: D

Explanation:
IP address/TCP port: All unassigned/25. You can use the General tab in the SMTP virtual server properties dialog box to change this setting. If you change this setting, you must specify an IP address/TCP port combination that is not being used by another SMTP virtual server. TCP port 25 is both the default TCP port and the recommended TCP port. More than one virtual server can use the same TCP port, provided that they are configured with different IP addresses. If you do not set a unique IP address/TCP port combination, the SMTP virtual server will not start.
Source: http://technet.microsoft.com/es-es/library/cc758440(WS.10).aspx

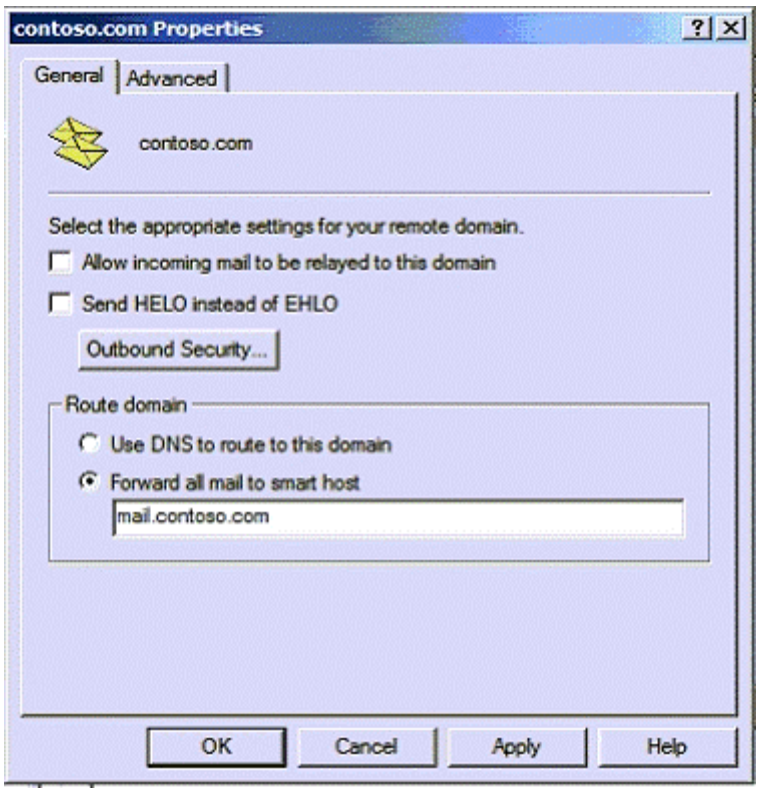
Question: 223

Your network contains an SMTP server that runs Windows Server 2008 R2. You need to ensure that all mail for contoso.com is routed through a smart host named mail.contoso.com. All other mail must be routed by using DNS name resolution. What should you configure?

A. a new SMTP domain
B. the Advanced delivery options
C. the Messages options
D. the Outbound connections options

Answer: A

Explanation:



Question: 224

Your network contains two Web servers that run Windows Server 2008 R2. Each Web server hosts three Web sites. You need to see the number of active connections to each Web site in a consolidated view. Which tool should you use?

A. Internet Information Services (IIS) Manager
B. Performance Monitor
C. Resource Monitor
D. Task Manager

Answer: B

Question: 225

Your network contains a Web server named Server1 that runs Windows Server 2008 R2. You modify the configuration of Server1. You need to restore the previous Web server configuration. What should you run?

A. appcmd.exe
B. iisback.vbs
C. iisext.vbs
D. iisreset.exe

Answer: A

Explanation:
Backup/Restore via the command line
Backing up IIS7 configuration is as simple as copying the \windows\system32\inetsrv\config directory (and subdirectories) into a backup directory, so you don't need anything special to do it. Just include this directory in whatever your OS/content back-up plan is, or write a custom script to do it. To help make managing backups easy, we've added a simple cmd-line option to AppCmd.exe that makes management of backup/restore sets easy. For example, to backup configuration, run the follow command:
%windir%\system32\inetsrv\appcmd.exe add backup "My Backup Name" to restore that backup, run this command:
%windir%\system32\inetsrv\appcmd.exe restore backup "My Backup Name" to delete a backup, run this command:
%windir%\system32\inetsrv\appcmd.exe delete backup "My Backup Name"
http://blogs.iis.net/bills/archive/2008/03/24/how-to-backup-restore-iis7-configuration.aspx

Question: 226

Your network contains a server that runs Windows 2008 R2. The disks on the server are configured as shown in the following table.

Disk Name	Disk Size	Volume Name
Disk0	50 GB	C
Disk1	50 GB	D
Disk2	100 GB	None

Volume D contains shared files and applications. You plan to install an application named App1 on the server. App1 must be installed in D:\App1. App1 requires 75 GB of disk space. You need to ensure that the server can support the planned installation of App1. The solution must minimize the impact on all users. What should you do?

A. Configure a striped volume.
B. Configure a mirrored volume.
C. Create a mount point.
D. Create a virtual hard disk (VHD).

Answer: C

Explanation:
Assign a mount point folder path to a drive
You can use Disk Management to assign a mount-point folder path (rather than a drive letter) to the drive. Mount-point folder paths are available only on empty folders on basic or dynamic NTFS volumes.
Backup Operator or Administrator is the minimum membership required.
Assigning a mount-point folder path to a drive
1. In Disk Manager, right-click the partition or volume where you want to assign the mount-point folder path, and then click Change Drive Letter and Paths.
2. Do one of the following:

To assign a mount-point folder path, click Add. Click Mount in the following empty NTFS folder , type the path to an empty folder on an NTFS volume, or click Browse to locate it. To remove the mount-point folder path, click it and then click Remove.
Source: http://technet.microsoft.com/en-us/library/cc753321.aspx

Question: 227

Your network contains an Active Directory domain. The domain contains client computers that run Windows 7. You activate Windows 7 and Microsoft Office 2010 on the client computers by using a Multiple Activation Key (MAK) key. You need to identify how many MAK activations remain. Which tool should you use?

A. Group Policy Management Console (GPMC)
B. Microsoft Office Activation Assistant (OAA)
C. the Windows Activation wizard
D. Volume Activation Management Tool (VAMT)

Answer: D

Explanation:
Volume Activation Management Tool (VAMT)
Each MAK key has a predetermined number of allowed activations, based on an organization's volume licensing agreement. Each activation with Microsoft's hosted activation services reduces the MAK activation pool by one. MAK implementations should include how your organization plans to monitor the number of MAK activations that are left. Both MAK Independent and MAK Proxy activations can use VAMT to monitor this. VAMT is a standalone application that can run on Windows XP, Windows Server 2003, or Windows Vista. It reports on the license condition of all systems using MAK activation and tracks the MAK activation count.
Source:
http://technet.microsoft.com/en-us/library/cc303276.aspx#_Volume_Activation_Management_

Question: 228

Your network contains a server that runs Windows Server 2008 R2 and has the Hyper-V server role installed. Virtual machines (VMs) are frequently added to the Hyper-V server. You need to ensure that a VM named VM1 has priority regarding the allocation of the physical CPU resources on the Hyper-V host. What should you modify?

A. the number of virtual processors for VM1
B. the relative weight of the virtual processor for VM1
C. the VM limit of the virtual processor for VM1
D. the VM reserve of the virtual processor for VM1

Answer: B

Question: 229

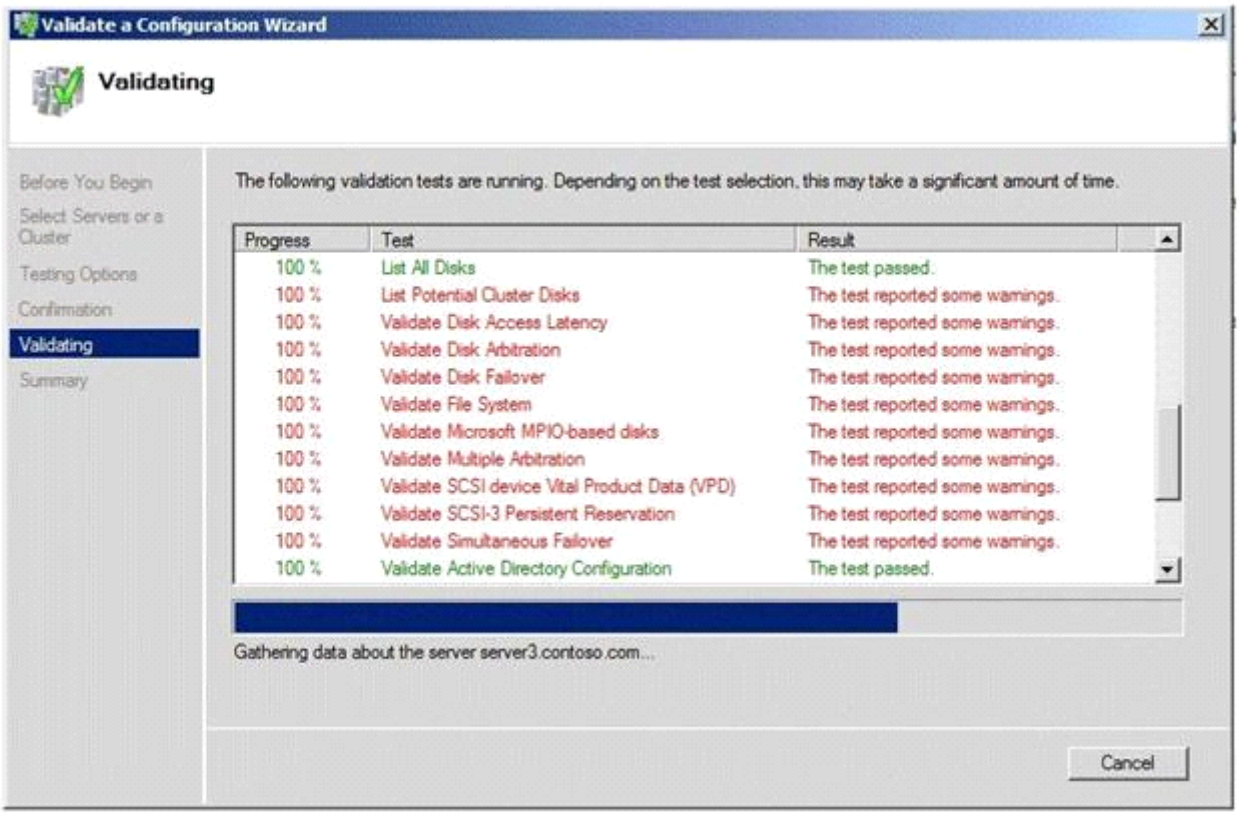
Your network contains a server that runs Windows Server 2008 R2 and has the Hyper-V server role installed. The network contains a virtual machine (VM) named VM1. The virtual hard disk (VHD) file for VM1 is stored on drive C. The snapshot files for VM1 are stored on drive D. You take several snapshots of VM1. After taking the snapshots, you discover that the state of VM1 is paused-critical. You need to ensure that you can resume VM1. The solution must prevent data loss on VM1. What should you do?

A. Change the VHD type of VM1.
B. Delete the .avhd files for VM1.
C. Increase the free disk space on drive C.
D. Increase the free disk space on drive D.

Answer: D

Question: 230

You are configuring a two-node failover cluster. The failover cluster will connect to a storage server that runs Windows Storage Server 2008. The storage server contains a raw disk. The raw disk appears in the Disk Management console for both nodes. From one of the nodes, you bring the disk online, and then you initialize the disk. You run the Validate a Configuration Wizard as shown in the exhibit. (Click the Exhibit button.)



You need to ensure that all of the tests pass when you run the Validate a Configuration Wizard. What should you do?

A. Convert the disk to a GPT disk, and then create a simple volume.
B. Convert the disk to a dynamic disk, and then take the disk offline.
C. Create a simple volume on the disk, and then take the disk offline.
D. Create a simple volume, and then convert the disk to a dynamic disk.

Answer: C

Explanation:
Now we should see our newly formatted disk as online in Disk Management. Note that if you went to any other node in the cluster, we'd still show this disk as 'offline'. This is good because we don't want more than one node to be able to see or access a disk until it's under the control of the cluster. That's the step we do next.
Source:

http://blogs.technet.com/b/askcore/archive/2009/01/14/adding-a-new-disk-to-an-existing-windows-2008-cluster.aspx

Question: 231

Your network contains a server that runs Windows Server 2008 R2. The server has two host bus adaptors (HBAs). Each HBA is attached to a different switch. The network contains a Storage Area Network (SAN). You need to configure the server to use multiple paths to access the SAN. Which tool should you use?

A. Diskpart
B. Dism
C. Mpclaim
D. Netsh

Answer: C

Explanation:
Using the MPclaim command-line tool
Multipath I/O can be managed by using the MPclaim command-line tool.
Note.
The command line is the only method of Multipath I/O configuration available on computers running a Server Core installation of Windows Server 2008.
Syntax of MPclaim mpclaim restart_option install_switch device_switch device_hwid
MPclaim parameters The following table describes the command parameters you can use with the MPclaim command to manage Multipath I/O by using a command line.
Source: http://technet.microsoft.com/en-us/library/cc725907.aspx

Question: 232

Your network contains an Active Directory domain. The domain contains a server named Server1 that has the Remote Desktop Licensing (RD Licensing) role service installed. On Server1, you enable the License server security group Group Policy setting. You need to ensure that Server1 can issue Remote Desktop Services client access licenses (RDS CALs) to a server named Server3. What should you do on Server3?

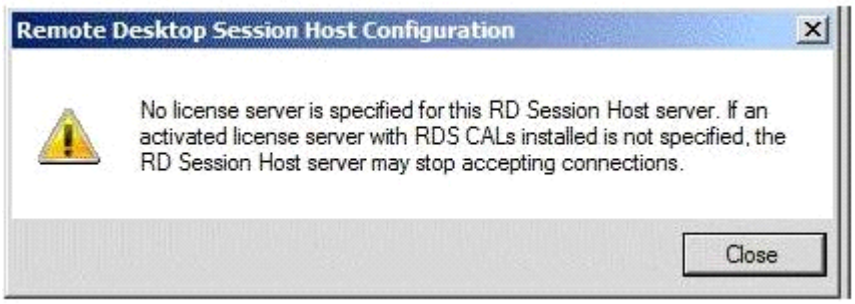
A. From Remote Desktop Licensing Manager, reactivate the server.
B. From Remote Desktop Session Host Configuration, modify the licensing mode.
C. From Computer Management, modify the members of the Terminal Server Computers group.
D. From Remote Desktop Licensing Manager, modify the connection method from the properties of the server.

Answer: C

Explanation:
Terminal Services License Server Security Group Configuration
When the TS Licensing role service is installed on the server, the Terminal Server Computers local group is created.
The license server will respond only to requests for TS CALs from terminal servers whose computer accounts are members of this group if the Computer Configuration\Administrative Templates\Windows Components\Terminal Services\TS Licensing\License server security group Group Policy setting has been enabled and applied to the license server.
By default, the Terminal Server Computers local group is empty.
Source: http://technet.microsoft.com/en-us/library/cc775331.aspx

Question: 233

Your network contains an Active Directory domain named contoso.com. Contoso.com contains a server named Server1 that has the Remote Desktop Session Host (RD Session Host) role service installed. You install the Remote Desktop Licensing (RD Licensing) role service on a server named Server2. Server2 is in a workgroup. On Server1, you attempt to configure Server2 as the RD Licensing server and receive the error shown in the following message box.



You need to ensure that you can configure Server1 to use Server2 as the RD Licensing server. What should you do first?

A. Join Server1 to the workgroup.
B. Join Server2 to the contoso.com domain.
C. On Server2, activate the server from Remote Desktop Licensing Manager.
D. On Server2, modify the membership of the Terminal Server Computers group.

Answer: C

Explanation:
Activating a Terminal Services License Server
A Terminal Services license server must be activated in order to certify the server and allow the license server to issue Terminal Services client access licenses (TS CALs). You can activate a license server by using the Activate Server Wizard in the TS Licensing Manager tool.
There are three methods by which you can activate your license server:
Internet (Automatic) This method requires Internet connectivity from the computer running TS Licensing Manager. Internet connectivity is not required from the license server itself. This method uses TCP/IP (TCP Port 443) to connect directly to the Microsoft Clearinghouse.
Web You can use the Web method when the computer running TS Licensing Manager does not have
Internet connectivity, but you have access to the Web by means of a Web browser from another computer.
The URL for the Web method is displayed in the Activate Server Wizard.
Telephone The telephone method allows you to talk to a Microsoft customer service representative to complete the activation process. The appropriate telephone number is determined by the country/region that you choose in the Activate Server Wizard and is displayed by the wizard.
When you activate the license server, Microsoft provides the server with a limited-use digital certificate that validates server ownership and identity. Microsoft uses an X.509 industry standard certificate for this purpose.
By using this certificate, a license server can make subsequent transactions with Microsoft.
If a license server is not activated, the license server can only issue temporary TS Per Device CALs, which are valid for 90 days, or TS Per User CALs.
Source: http://technet.microsoft.com/en-us/library/cc731293.aspx

Question: 234

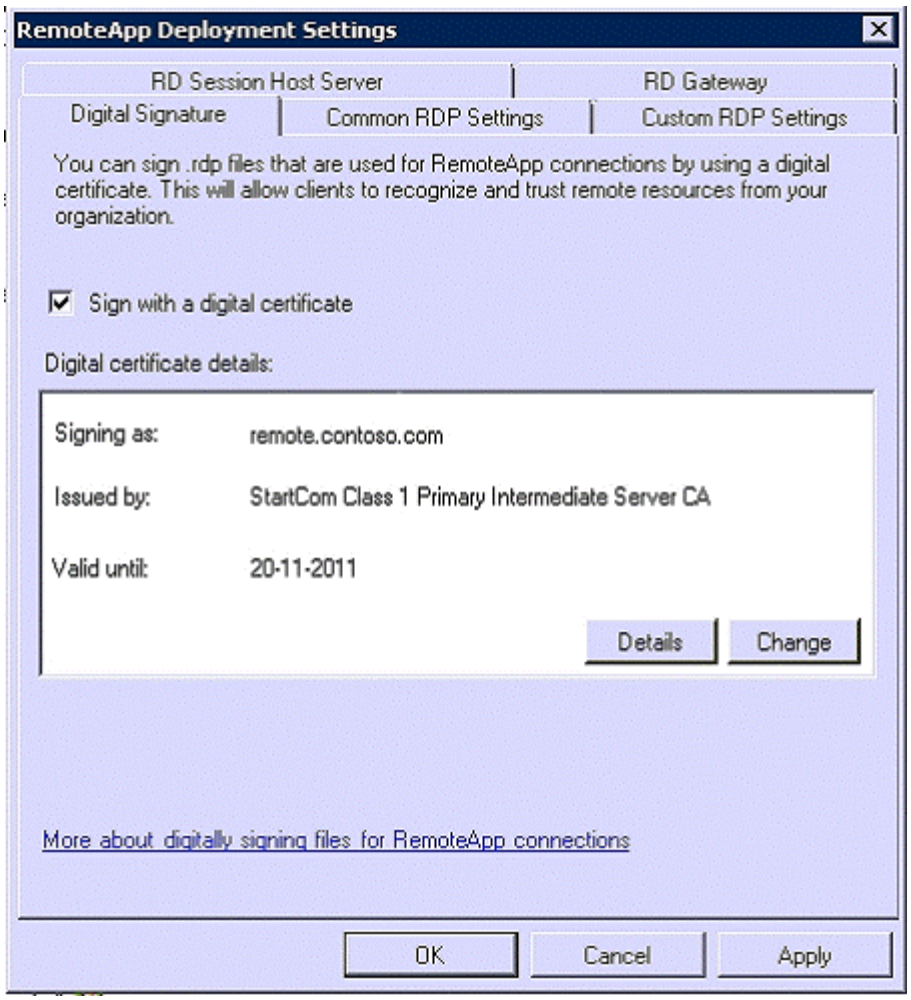
Your network contains a Remote Desktop server. The server hosts 10 RemoteApp programs.

You need to configure a digital signature for the RemoteApp programs. What should you modify?

A. the Remote Desktop connection authorization policies (RD CAPs)
B. the Remote Desktop resource authorization policies (RD RAPs)
C. the RemoteApp and Desktop Connection properties
D. the RemoteApp Deployment Settings

Answer: D

Explanation:



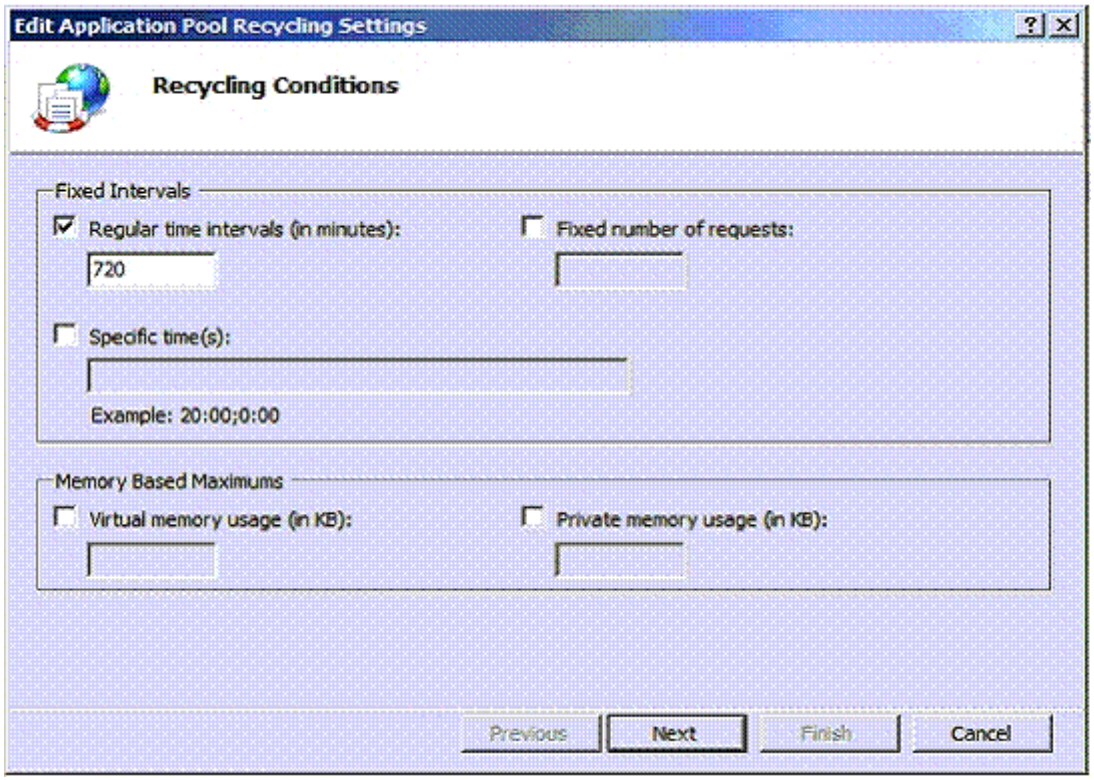
Question: 235

Your network contains a Web site named Web1. Web1 is configured to use an application pool named AppPool1. You need to ensure that the memory used by the Web site is released every 12 hours. The solution must minimize the amount of downtime for the Web site. What should you do?

A. Modify the recycling settings for AppPool1.
B. Modify the session state settings for Web1.
C. Create a scheduled task that runs tskill.exe w3svc.exe.
D. Create a scheduled task that runs iisreset.exe /noforce.

Answer: A

Explanation:



Question: 236

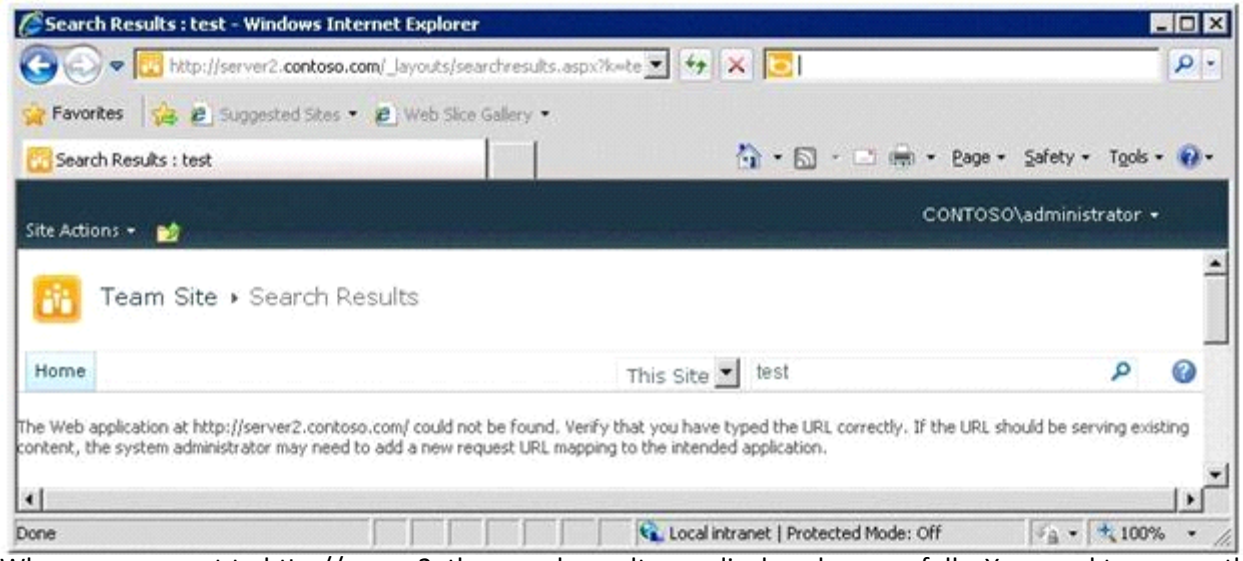
Your network contains a server named Server1 that has Microsoft SharePoint Foundation 2010 installed. Server1 contains a SharePoint site named Site1. Several users add Site1 to the SharePoint lists in Microsoft Outlook 2010. The users report that every time they open Outlook 2010, they are prompted for authentication for Server1. You need to prevent the users from being prompted for authentication when they open Outlook 2010. What should you do?

A. From Internet Explorer, add the site to the Trusted sites zone.
B. From Central Administration, configure the site to use Basic authentication.
C. From Outlook 2010, open the Trust Center and configure the Privacy Options.
D. From Outlook 2010, open the Trust Center and configure the Trusted Publishers.

Answer: A

Question: 237

Your network contains a server named Server2 that has Microsoft SharePoint Foundation 2010 installed. The server has a fully qualified domain name (FQDN) of server2.contoso.com. You connect to http://server2.contoso.com. When you attempt to search for a document, you receive the error message shown in the exhibit. (Click the Exhibit button.)



When you connect to http://server2, the search results are displayed successfully. You need to ensure that the search results display when you search from http://server2.contoso.com. What should you do?

A. From Central Administration, configure the Alternate Access Mappings.
B. From Central Administration, configure the Cross Firewall Access Zone.
C. From Internet Information Services (IIS) Manager, add a site binding.
D. From Internet Information Services (IIS) Manager, add an authorization rule.

Answer: A

Explanation:
Configure alternate access mapping
Each Web application can be associated with a collection of mappings between internal and public URLs. Both internal and public URLs consist of the protocol and domain portion of the full URL (for example, https://www.fabrikam.com). A public URL is what users type to get to the SharePoint site, and that URL is what appears in the links on the pages. Internal URLs are in the URL requests that are sent to the SharePoint site. Many internal URLs can be associated with a single public URL in multi-server farms (for example, when a load balancer routes requests to specific IP addresses to various servers in the load-balancing cluster).
Each Web application supports five collections of mappings per URL; the five collections correspond to five zones (default, intranet, extranet, Internet, and custom). When the Web application receives a request for an internal URL in a particular zone, links on the pages returned to the user have the public URL for that zone. For more information, see Plan alternate access mappings (Windows SharePoint Services).
Manage alternate access mappings
1. On the top navigation bar, click Operations.
2. On the Operations page, in the Global Configuration section, click Alternate access mappings.
Add an internal URL
1. On the Alternate Access Mappings page, click Add Internal URLs.
2. If the mapping collection that you want to modify is not specified, then choose one. In the Alternate Access Mapping Collection section, click Change alternate access mapping collection on the Alternate Access Mapping Collection menu.
3. On the Select an Alternate Access Mapping Collection page, click a mapping collection.
4. In the Add internal URL section, in the URL protocol, host and port box, type the new internal URL (for example, https://www.fabrikam.com).
5. In the Zone list, click the zone for the internal URL.
6. Click Save.
Source: http://technet.microsoft.com/en-us/library/cc288173.aspx

Question: 238

Your network contains an Active Directory forest. Microsoft Exchange Server 2010 is deployed in the forest. You have a server named Server1 that has Microsoft SharePoint Foundation installed. You need to ensure that users can receive email notifications when the SharePoint content is modified. What should you do?

A. Install the SMTP Server feature.
B. Configure the Send To Connections.
C. Configure the incoming email settings.
D. Configure the outgoing email settings.

Answer: D

Explanation:
To configure outgoing email for a farm by using Central Administration
1. Verify that you have the following administrative credentials: You must be a member of the Farm Administrators group on the computer that is running the SharePoint Central Administration Web site.
2. In Central Administration, click System Settings.
3. On the System Settings page, in the Email and Text Messages (SMS) section, click Configure outgoing email settings.
4. On the Outgoing Email Settings page, in the Mail Settings section, type the SMTP server name for outgoing email (for example, mail.example.com) in the Outbound SMTP server box.
5. In the From address box, type the email address as you want it to be displayed to email recipients.
6. In the Reply-to address box, type the email address to which you want email recipients to reply.
7. In the Character set list, select the character set that is appropriate for your language.
8. Click OK.
Source: http://technet.microsoft.com/en-us/library/cc288949.aspx

Question: 239

Your network contains a domain controller named Server1 and a server named Server2. Server2 has the Windows Deployment Services (WDS) server role installed. You open the Windows Deployment Services console and see several pending devices. You right-click one of the devices and click Name and Approve. You enter the computer name and receive the following error message: The parameter is incorrect. You need to ensure that you can create new computer accounts and update existing computer accounts. What should you do?

A. Assign the Server1 computer account permissions to the Computers container.
B. Assign the Server2 computer account permissions to the Computers container.
C. From Windows Deployment Services, change the Computer Account Location settings.
D. From Windows Deployment Services, change the PXE Response Policy to Respond only to known client computers.

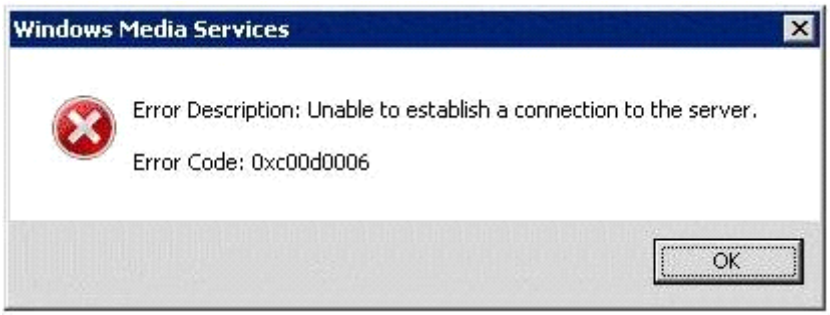
Answer: B

Explanation:
Approve a pending computer:
Read and write permissions to the C:RemoteInstall\MGMT folder (which contains Binlsvcdb.mdb). The actual account of an approved pending computer is created by using the server's authentication token, not the token of the administrator who is performing the approval. Therefore, in AD DS, you must grant rights to the Windows Deployment Services server's account (WDSSERVER$) to create computer account objects for the containers and OUs where the approved pending computers will be created.

To grant permissions to WDS to approve a pending computer
1. Open Active Directory Users and Computers.
2. Right-click the OU where you are creating prestaged computer accounts, and then select Delegate Control.
3. On the first screen of the wizard, click Next.
4. Change the object type to include computers.
5. Add the computer object of the Windows Deployment Services server, and then click Next.
6. Select Create a Custom task to delegate.
7. Select Only the following objects in the folder . Then select the Computer Objects check box, select Create selected objects in this folder, and click Next.
8. In the Permissions box, select the Write all Properties check box, and click Finish.
Source: http://technet.microsoft.com/en-us/library/cc754005(WS.10).aspx

Question: 240

Your network contains two servers named Server1 and Server2 that have the Streaming Media Services role installed. Both servers are joined to the same domain. From Server1, you open the Windows Media Services console. You attempt to connect to Server2 and receive the error shown in the following message box.

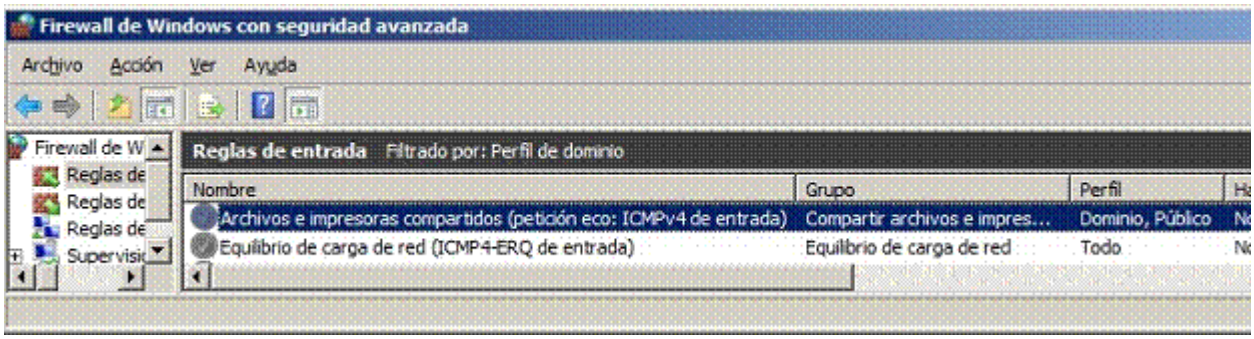


You need to ensure that you can remotely administer the Streaming Media Services on Server2 from Server1. What should you do on Server2?

A. Create an inbound firewall rule for ICMPv4.
B. Create an inbound firewall rule for TCP port 80.
C. Run winrm.exe and specify the configsddl parameter.
D. Run winrm.exe and specify the quickconfig parameter.

Answer: A

Explanation:



Question: 241

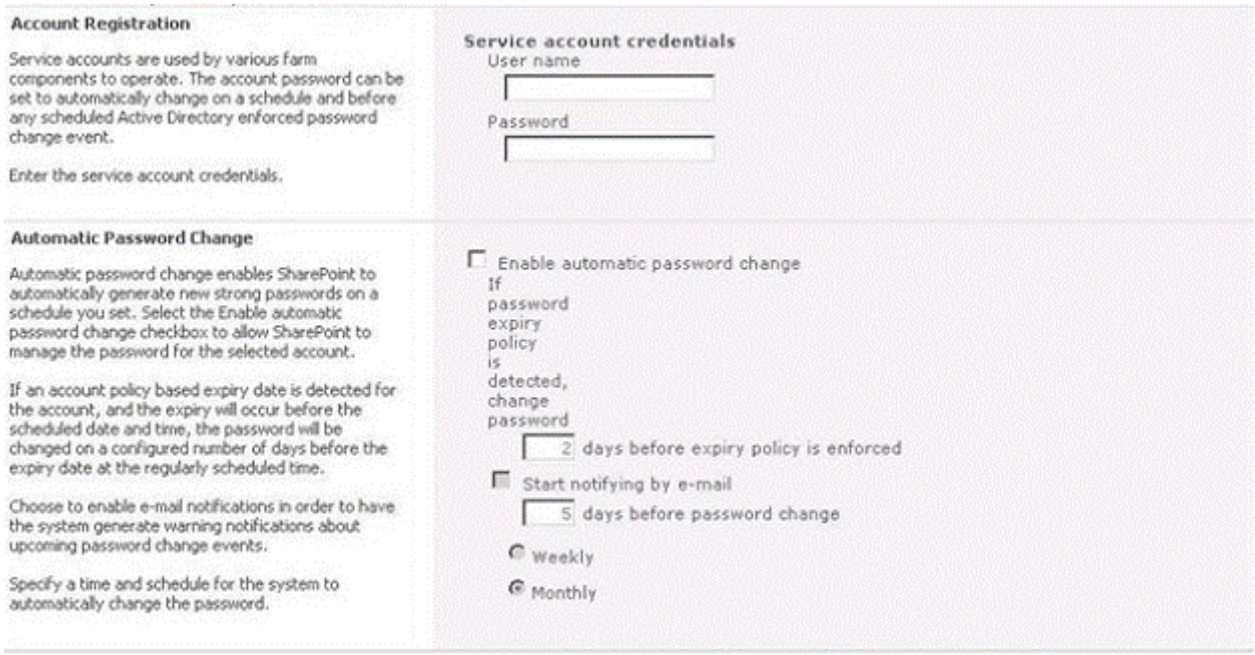
Your network contains a server that has Microsoft SharePoint Foundation 2010 installed. The farm account for the

server is named Service1. You need to automatically change that the password for Service1 every 30 days. What should you do?

A. From ADSI Edit, create a Password Settings object (PSO).
B. From Windows PowerShell, run the New-ADServiceAccount cmdlet.
C. From Windows PowerShell, run the Install-ADSserviceAccount cmdlet.
D. From Central Administration, modify the properties of the Service1 managed account.

Answer: D

Explanation:
Register Managed Accounts (SharePoint Central Administration)
To register new Managed Accounts using SharePoint Central Administration, select Security from the SharePoint Central Administration homepage.
On the Security page select Configure managed accounts under General Security.
On the Managed Accounts page select Register Managed Account.
On the Register Managed Account page specify the credentials and select the password change policies as desired.



Source: http://blogs.technet.com/b/wbaer/archive/2010/04/11/managed-accounts.aspx

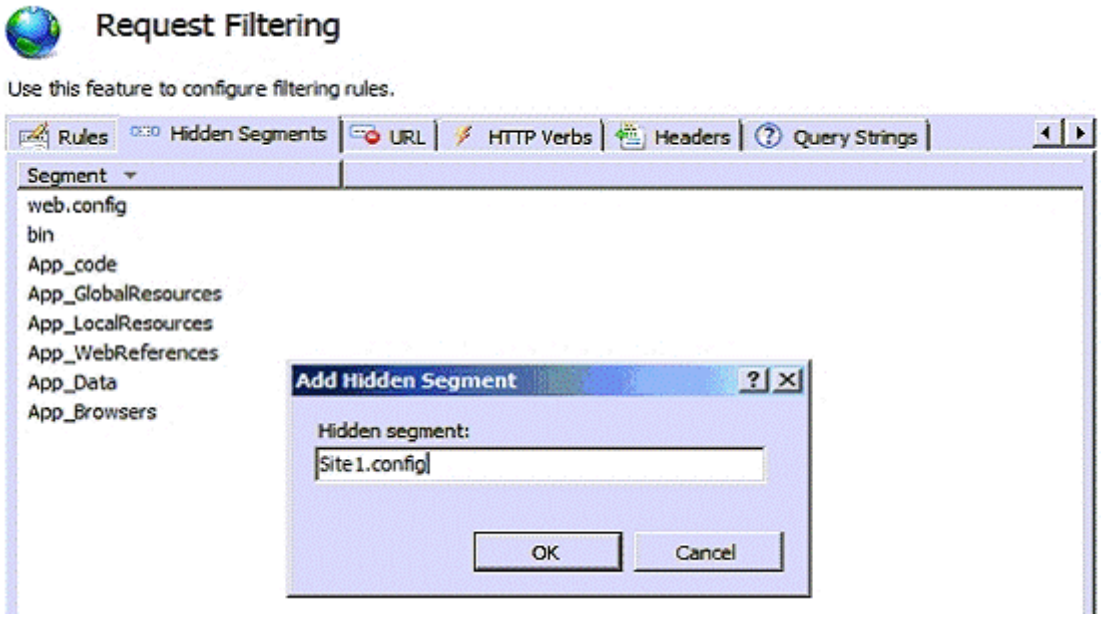
Question: 242

Your network contains a Web site. The Web site contains a configuration file named Site1.config. You need to prevent users from accessing Site1.config through the Web site. Which Internet Information Services (IIS) feature should you configure for the site?

A. Directory Browsing
B. HTTP Response Headers
C. ISAPI Filters
D. Request Filtering

Answer: D

Explanation:



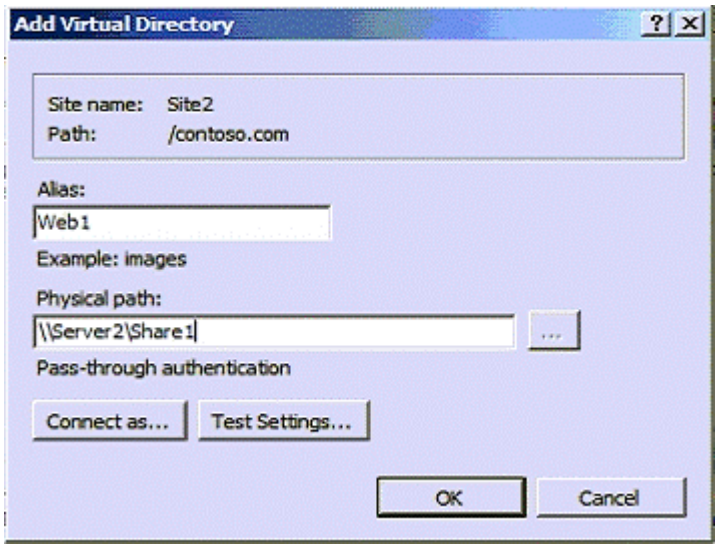
Question: 243

Your network contains two servers named Server1 and Server2 that run Windows Server 2008 R2. Server1 has the Web Server (IIS) role installed. Server2 has the File Services role installed. Server1 has a Web site named Web1. Server2 has a shared folder named Share1. You need to give users Web access to the content in Share1. What should you do on Server1?

A. Modify the connection strings of Web1 and enable directory browsing on Web1.
B. Modify the connection strings of Web1 and configure the default document of Web1.
C. Add a virtual directory to Web1 and enable directory browsing on the virtual directory.
D. Add a virtual directory to Web1 and configure the default document of the virtual directory.

Answer: C

Explanation:



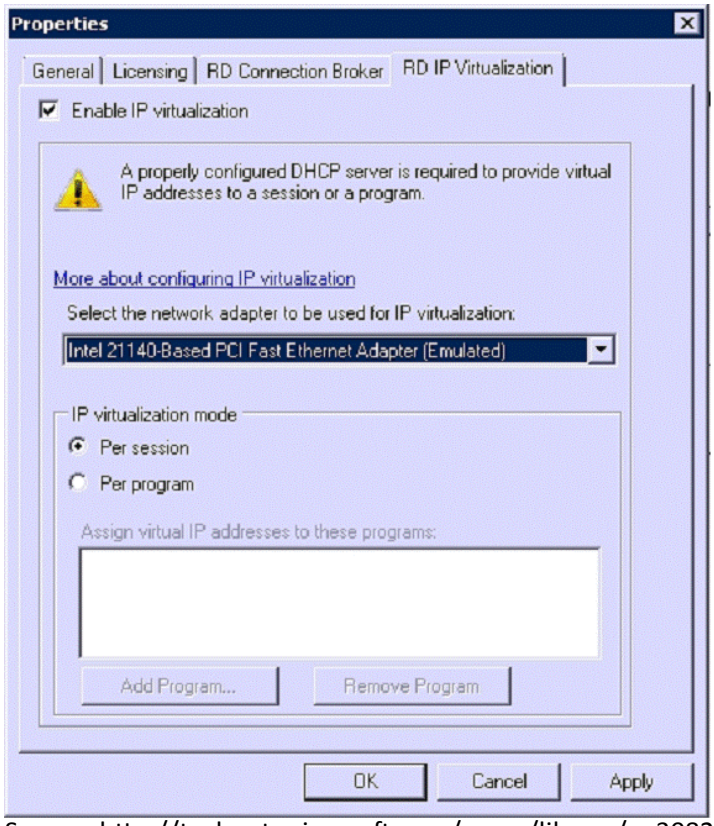
Question: 244

Your network contains a server that has the Remote Desktop Session Host (RD Session Host) role service installed. You need to ensure that each Remote Desktop connection to the server has a unique IP address. What should you do?

A. Enable IP virtualization per session
B. Enable IP virtualization per program
C. Configure the network adapter to have multiple IP addresses
D. Configure the network adapter to obtain an IP address automatically

Answer: A

Explanation:
Deploying Remote Desktop IP Virtualization
In Windows Server 2008 R2, RD Session Host supports per program and per session Remote Desktop IP Virtualization for Winsock applications. When using per program Remote Desktop IP Virtualization, you choose which programs to use with Remote Desktop IP Virtualization. When using per session Remote Desktop IP Virtualization, all Winsock applications are virtualized with Remote Desktop IP Virtualization. Remote Desktop IP Virtualization allows you to assign a unique IP address to a user session, which helps to avoid application compatibility issues by simulating a local desktop.
To configure Remote Desktop IP Virtualization for per program virtualization
1. Log on to RD Session Host as an Administrator.
2. Click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Session Host Configuration.
3. Under the RD IP Virtualization heading, double-click IP Virtualization.
4. Click the Enable IP virtualization check box.
5. In the Select the network adapter to be used for IP virtualization box, select the appropriate network adapter.
6. Under the IP virtualization mode heading, ensure that the Per Session option is selected.
Important If your computer has more than one network adapter, you must choose per program. Using per session Remote Desktop IP Virtualization with more than one network adapter installed on the computer is not supported.
7. Click OK.



Source: http://technet.microsoft.com/en-us/library/ee308293.aspx

Question: 245

Your network contains an FTP server that runs Windows Server 2008 R2. You need to configure SSL security for the FTP connections. The solution must meet the following requirements:

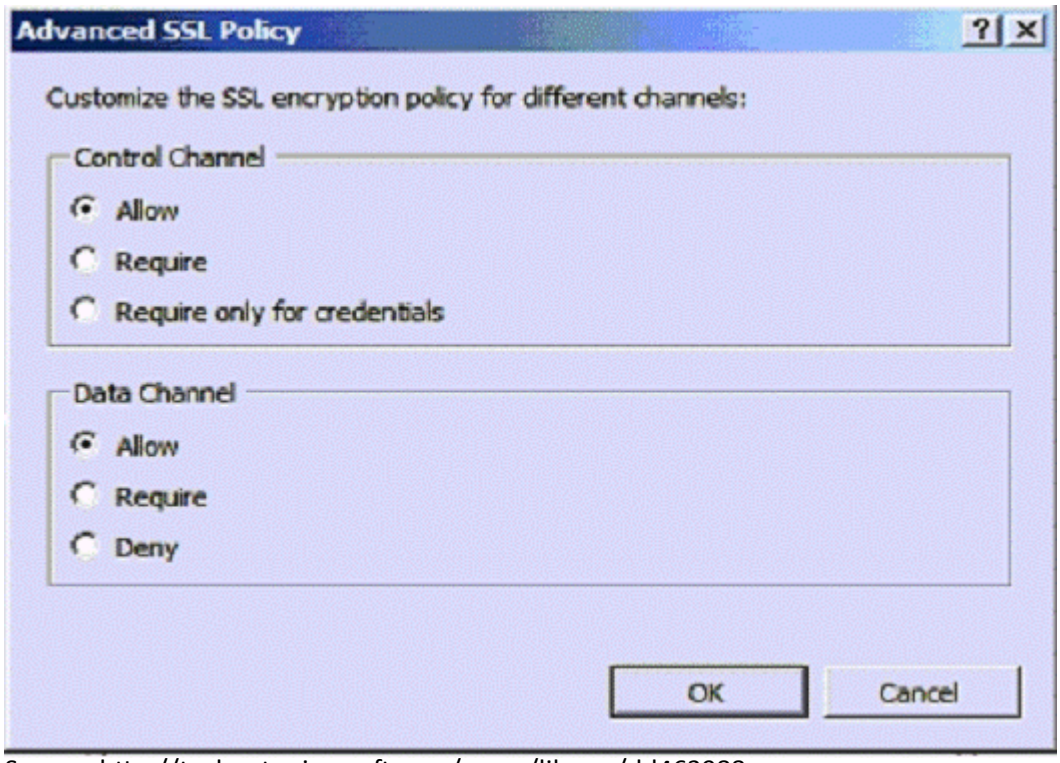
- All user names and passwords must be encrypted.
- The anonymous user identity must be allowed to establish a connection without requiring encryption. What should you configure?

A. the Control Channel setting to Allow
B. the Control Channel setting to Require only for credentials
C. the Data Channel setting to Allow
D. the Data Channel setting to Require

Answer: B

Explanation:
Configure the FTP SSL Encryption Policy for the Control Channel and Data Channel
Configure a custom SSL encryption policy when you want to specify an SSL encryption policy for the control channel and data channel separately. For example, you might encrypt the control channel to avoid passing user credentials in cleartext. Or you might encrypt the data channel to protect sensitive information from being disclosed or changed.
To configure the SSL encryption policy for the control channel and data channel
1. Open IIS Manager.
2. In the Connections pane, select the server node.
3. In Features View, double-click FTP SSL Settings.
4. Under SSL Policy, select Custom and then click Advanced.
5. In the Advanced SSL Policy dialog box, under Control Channel select one of the following options for SSL encryption

over the control channel:
Allow: Requires SSL encryption for all users, but gives the anonymous user identity the ability to establish a connection without encryption.
Require: Requires SSL encryption for all users, including the anonymous user identity.
Require only for credentials: Requires SSL encryption for all users, but does not allow the anonymous user identity to establish an encrypted connection.
6. Under Data Channel, select one of the following options for SSL encryption over the data channel:
Allow: When an encrypted connection is established, data transfer is encrypted but requests for metadata (using the DIR command) return a non-encrypted reply.
Require: Requires SSL encryption over the data channel.
Deny: Denies SSL encryption over the data channel.
7. Click OK.
8. In the Actions pane, click Apply.



Source: http://technet.microsoft.com/en-us/library/dd463988.aspx

Question: 246

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the SMTP Server feature installed and has one SMTP Virtual Server named SMTP1. You need to configure Server1 to meet the following requirements:
Relay email messages for contoso.com.
Relay email messages for nwtraders.com.
Prevent the relaying of email messages to other domains.
What should you do?

A. Configure two alias domains to SMTP1.
B. Configure two remote domains to SMTP1.
C. Modify the relay restrictions list of SMTP1.
D. Modify the connection control settings of SMTP1.

Answer: B

Explanation:
Configuring SMTP Virtual Server Relay for Remote Domains
You can configure an SMTP virtual server to relay incoming mail to your SMTP/POP3 server. The SMTP virtual server can also accept and relay mail to other domains within your organization.
Specifying a relay server overrides the smart host setting in the Advanced Delivery box of the SMTP virtual server.
Procedures
To configure an SMTP virtual server to relay mail to a remote domain
1. In IIS Manager, double-click the SMTP virtual server that you want to configure, right-click Domains, point to New, and then click Domain. The New SMTP Domain Wizard starts.
2. Click Remote, and then click Next.
3. In the Name box, type a name for the remote domain, and then click Finish.
4. In IIS Manager, right-click the new remote domain, and then click Properties.
5. On the General tab, select the Allow incoming mail to be relayed to this domain check box to allow the SMTP server to act as a mail relay.
6. On the General tab under Route domain, click Forward all mail to smart host, and then type the fully qualified domain name or the IP address of the internal network corporate mail server through which you would like to route messages for this remote domain.
7. Click OK, and then stop and restart the SMTP virtual server.
After you configure the remote domain, all mail that is addressed to the remote domain is relayed to the smart host that you configured. Mail that is not deliverable is stored in the Inetpub\Mailroot\Badmail folder.

Source: http://technet.microsoft.com/en-us/library/cc775967.aspx

Question: 247

Your network contains a server that has the Hyper-V server role installed. The server hosts a virtual machine (VM) named VM1. VM1 runs Windows Server 2008 R2 and has the file server role installed. You need to add more disk space to VM1. The solution must minimize the amount of downtime for VM1. What should you do first on VM1?

A. Add a virtual disk to IDE controller 0.
B. Add a virtual disk to IDE controller 1.
C. Add a virtual disk to the SCSI controller.
D. Add a pass-through disk to IDE controller 0.

Answer: C

Question: 248

Your network contains two servers that have the Hyper-V server role installed. You install the Failover Clustering feature on both servers. You add both servers as nodes in the cluster. You need to ensure that you can perform live migrations of individual virtual machines (VMs) between the nodes. The solution must minimize the number of

volumes required to host the VMs. What should you do first?

A. From Failover Cluster Manager, enable Cluster Shared Volumes.
B. From Failover Cluster Manager, modify the quorum settings of the cluster.
C. From Hyper-V Manager on each server, modify the default location for the virtual hard disks (VHDs).
D. From Hyper-V Manager on each server, modify the default location for the virtual machine configuration files.

Answer: A

Explanation:
Cluster Shared Volumes, a feature available with some versions of failover clustering, simplifies the configuration and management of clustered virtual machines. With Cluster Shared Volumes, multiple clustered virtual machines can use the same LUN (disk) while still being able to fail over (or move from node to node) independently of one another.
Note In Windows ServerR 2008 R2, the Cluster Shared Volumes feature included in failover clustering is only supported for use with the Hyper-V server role. The creation, reproduction, and storage of files on Cluster Shared Volumes that were not created for the Hyper-V role, including any user or application data stored under the ClusterStorage folder of the system drive on every node, are not supported and may result in unpredictable behavior, including data corruption or data loss on these shared volumes. Only files that are created for the Hyper-V role can be stored on Cluster Shared Volumes. An example of a file type that is created for the Hyper-V role is a Virtual Hard Disk (VHD) file.
Before installing any software utility that might access files stored on Cluster Shared Volumes (for example, an antivirus or backup solution), review the documentation or check with the vendor to verify that the application or utility is compatible with Cluster Shared Volumes.
Overview of Cluster Shared Volumes
Cluster Shared Volumes is available in versions of Windows ServerR 2008 R2 and of MicrosoftR Hyper-V™ Server 2008 R2 that include the Failover Clustering feature. Volumes that are configured as Cluster Shared Volumes can be accessed by all nodes of a failover cluster. Each node can open and manage files on the volumes. Therefore, different nodes can host different virtual machines that all have files on the same volume.
This design has many advantages, including the following:
Easier storage management: When virtual machines share volumes, fewer LUNs need to be configured and managed to host the same number of virtual machines.
Independent failover of virtual machines : Although multiple virtual machines are sharing the same volume, each virtual machine can fail over, or be moved or migrated, independently of other virtual machines. No drive letter restrictions: Cluster Shared Volumes do not need to be assigned a drive letter, so you are not restricted by the number of available drive letters, and you do not have to manage volumes using GUIDs.
Enhanced availability: The Cluster Shared Volumes feature is designed to detect and handle many problems that would otherwise cause the storage to be unavailable to virtual machines. This includes detecting and handling storage connection problems (Cluster Shared Volumes reroutes the storage access through another node).
Efficient use of storage: You can make better use of disk space, because you do not need to place each Virtual Hard Disk (VHD) file on a separate disk with extra free space set aside just for that VHD file. Instead, the free space on a Cluster Shared Volume can be used by any VHD file on that LUN. This reduces the total amount of space that must be set aside for expansion, and simplifies capacity planning
Source: http://technet.microsoft.com/en-us/library/dd630633(WS.10).aspx

Question: 249

Your network contains a server that has the Streaming Media Services role installed. The server contains a publishing point. You need to configure the publishing point to meet the following requirements:
Authenticate users by using Kerberos authentication.
Only allow users from a virtual local area network (VLAN) named VLAN1 to access the publishing point.
What should you configure?

A. WMS Digest Authentication and WMS IP Address Authorization
B. WMS Digest Authentication and WMS Publishing Points ACL Authorization
C. WMS Negotiate Authentication and WMS IP Address Authorization
D. WMS Negotiate Authentication and WMS Publishing Points ACL Authorization

Answer: C

Explanation:
WMS Negotiate Authentication
The WMS Negotiate Authentication plug-in grants access to the server based upon the user's network logon approval. This plug-in uses an encrypted challenge/response scheme to authenticate users. It is a secure form of authentication because the user name and password are not sent across the network; the player acknowledges the password by using a cryptographic exchange with the Windows Media server. Because this plug-in relies upon established user logon credentials, the player and server must be on the same domain or on trusted domains. Negotiate authentication does not work across proxy servers or other firewall applications.
Source: http://technet.microsoft.com/en-us/library/cc730972.aspx
WMS IP Address Authorization
The WMS IP Address Authorization plug-in is used to control access to your content based on client Internet
Protocol (IP) addresses. You can add specific IP addresses or ranges of IP addresses for which you want to allow or restrict access. You can configure the following options on the General tab for this plug-in.
Source: http://technet.microsoft.com/en-us/library/cc770273.aspx

Question: 250

You plan to stream media content over the Internet. You need to configure PlayReady DRM to support HTTP streaming. What should you install?

A. Microsoft IIS Media Services
B. Microsoft Office Communications Server
C. Microsoft SharePoint Foundation 2010
D. Streaming Media Services

Answer: A

Explanation:
IIS Media Services to Include a Version of PlayReady DRM for HTTP Streaming
Some big news today for customers who are interested in easy to use, robust content protection for HTTP streaming scenarios using IIS Media Services…
Today we're announcing that IIS Media Services will support a version of PlayReady DRM to enable protected HTTP streaming. The PlayReady DRM IIS Media Services solution will deploy on a single box to secure your media assets for online streaming using the IIS Smooth Streaming and PlayReady DRM technology, directly within IIS Media Services - no additional license fees or royalties required.
File-based encryption is the most robust way to secure high value content – much more so than stream encryption, which only secures the communication stream. The PlayReady DRM IIS Media Services solution will bring full file-based encryption into IIS Media Services with the ease of use of traditional stream encryption. And the solution of course will use Microsoft PlayReady technology, which is widely supported in the industry and draws on the experience gained from more than a decade of investment that Microsoft has made in the development of DRM technology.
For customers needing to apply PlayReady DRM protection to content for offline scenarios, or apply customized

business rules to the use of protected content in purchase/rental/subscription scenarios, of course that functionality will remain available, as it is today, via the use of a PlayReady Server.
Source: http://team.silverlight.net/announcement/iis-media-services-to-include-a-version-of-playready-drm-for-http-streaming/

Question: 251

Your network contains a server that has Microsoft SharePoint Foundation 2010 installed. Users report that it takes as many as five minutes to receive an email notification when content on the SharePoint site is changed. You need to reduce the amount of time it take for users to receive the email notifications. What should you modify?

A. the incoming email settings
B. the outgoing email settings
C. the Task Scheduler Library
D. the timer job definitions

Answer: D

Explanation:
Timer job reference (SharePoint Foundation 2010)
This article describes the default timer jobs for SharePoint Foundation 2010. A timer job runs in a specific Windows service for SharePoint Foundation. Timer jobs also perform infrastructure tasks for the Timer service, such as clearing the timer job history and recycling the Timer service; and tasks for Web applications, such as sending email alerts. A timer job contains a definition of the service to run and specifies how frequently the service is started. The SharePoint 2010 Timer service (SPTimerv4) runs timer jobs. Many features in SharePoint Foundation rely on timer jobs to run services according to a schedule.
Manage timer jobs You can check the status of a timer job and edit the timer job definition.
For the general administration of all jobs, the SharePoint Central Administration Web site has a Timer Job Status page and a Job Definitions page. You can find these pages in Central Administration, on the Monitoring page, in the Timer Jobs section.
From the View menu, you can filter the timer jobs at the following levels:
All Displays all timer jobs for the farm.
Service Displays all the timer jobs for a particular service. If you select this command, use the Service menu to select the service by which you want to filter the listed jobs.
Web Application Displays all the timer jobs for a Web application. If you select this option, use the Web Application menu to select the Web application by which you want to filter the listed jobs.
Server Displays all the timer jobs for the specified server. If you select this command, use the Server menu to select the server by which you want to filter the listed jobs.
Job Definition Displays all the timer jobs for the specified job definition. On the Timer Job Status page, use the Job Definition menu to select the job definition by which you want to filter the listed jobs.
Failed Jobs Displays all the timer jobs on the farm that have failed to finish.
The SharePoint 2010 Timer service (SPTimerv4) is based on the Gregorian calendar for scheduling. For every job that you schedule, you specify when the timer job will run, specified in a 24-hour time format. You must specify the time in local time instead of as an offset from Coordinated Universal Time (UTC). The time is stored in that format. Daily, weekly, and monthly schedules also include a window of execution. The timer service will select a random time within this interval to start executing the job on each applicable server. This feature is appropriate for high-load jobs that run on multiple servers on the farm. Running this kind of job on all the servers at the same time might place an unreasonable load on the farm. Timer job schedules can be specified by using Windows PowerShell.
Default timer jobs
The following table lists the default timer jobs for SharePoint Foundation 2010.
Immediate Alerts Sends out immediate and scheduled alerts.

Source: http://technet.microsoft.com/en-us/library/ff808317.aspx

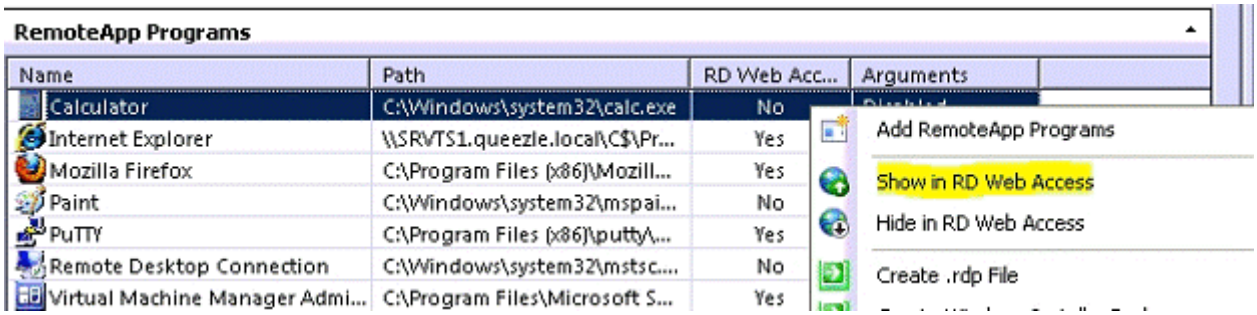
Question: 252

Your network contains a Remote Desktop server named Server1. The network contains a RemoteApp named App1 that is published to all users. You need to ensure that App1 is available through the Remote Desktop Web Access (RD Web Access) Web site. What should you modify on Server1?

A. the RemoteApp Properties
B. the Remote Desktop connection authorization policy (RD CAP)
C. the Remote Desktop resource authorization policy (RD RAP)
D. the Remote Desktop server properties

Answer: A

Explanation:



Question: 253

Your network contains a server named Server1 that has the Remote Desktop Session Host (RD Session Host) role service installed. A user named User1 connects to Server1 and starts an application named App1.exe. User1 reports that App1.exe is unresponsive and cannot be closed. You need to terminate App1.exe for User1 only. Which tool should you do?

A. Qprocess
B. Quser
C. Rwinsta
D. Tskill

Answer: D

Explanation:
Tskill Ends a process.
Syntax tskill {ProcessID | ProcessName} [/server:ServerName] [{/id:SessionID | /a}] [/v]
Parameters ProcessID : The ID of the process you want to end.
ProcessName : The name of the process you want to end. You can use wildcards to specify this parameter.
/server: ServerName : Specifies the terminal server containing the process you want to end. Otherwise, the current terminal server is used.
/id: SessionID : Ends the process running in the specified session.
/a : Ends the process running in all sessions.
/v : Displays information about the actions being performed.
/? : Displays help at the command prompt.

tskill App1.exe /server:Server1 /id:<SessionID of User1>
Source: http://technet.microsoft.com/en-us/library/bb490806.aspx

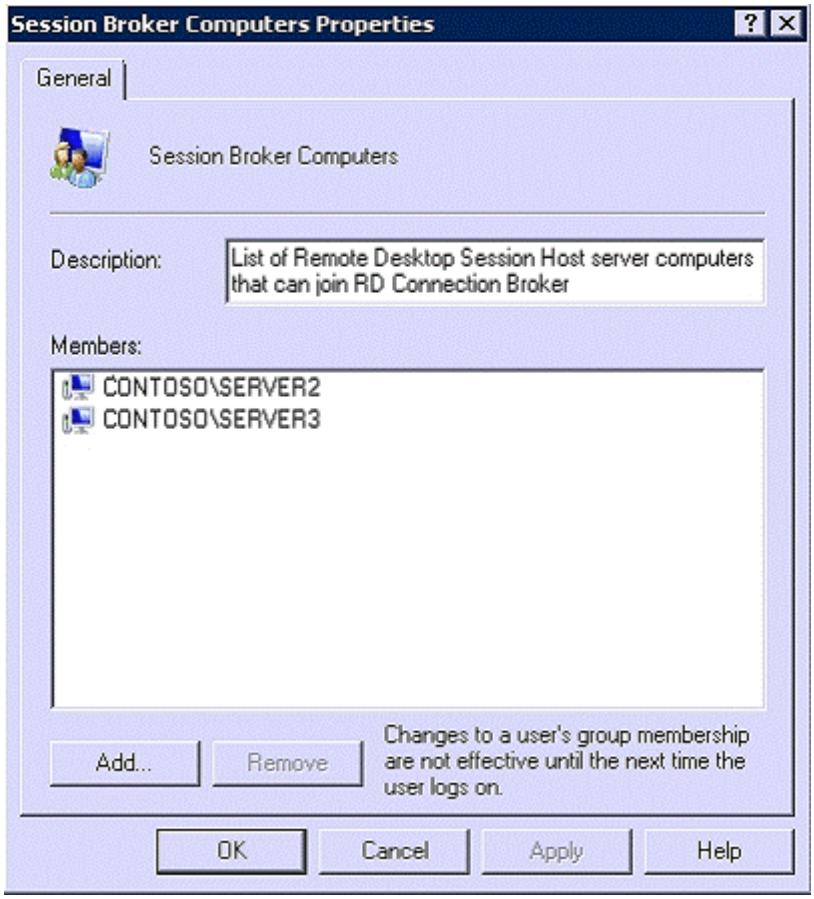
Question: 254

Your network contains a server named Server1 that has the Remote Desktop Connection Broker (RD Connection Broker) role service installed. You deploy two new servers named Server2 and Server3. On Server2 and Server3, you install the Remote Desktop Session Host (RD Session Host) role service. From the Remote Desktop Session Host Configuration snap-in, you configure Server2 and Server3 as server farm members. You need to ensure that all Remote Desktop sessions are distributed between Server2 and Server3. What should you do?

A. On Server2 and Server3, add the Server1 computer account to the Remote Desktop Users group.
B. On Server1, add the Server2 computer account and the Server3 computer account to the Session Broker Computers group.
C. On Server1, install the Remote Desktop Gateway (RD Gateway) role service. Add Server1 as an RD Gateway server farm member.
D. On Server1, install the Remote Desktop Gateway (RD Gateway) role service. Add Server2 and Server3 as RD Gateway server farm members.

Answer: B

Explanation:



Question: 255

Your network contains a Web server that runs Windows Server 2008 R2. The server has a Web site named Site1. You

need to ensure that Web developers can update the Web content on Site1 by using HTTP. What should you do first?

A. Modify the Feature Delegation settings.
B. Install the ASP Web Server (IIS) role service.
C. Install the WebDAV Publishing Web Server (IIS) role service.
D. Modify the Microsoft ASP.NET pages and control settings for the Web site.

Answer: C

Explanation:
About WebDAV
Web Distributed Authoring and Versioning (WebDAV) extends the HTTP/1.1 protocol to allow clients to publish, lock, and manage resources on the Web.
Integrated into IIS, WebDAV allows clients to do the following:
Manipulate resources in a WebDAV publishing directory on your server. For example, users who have been assigned the correct rights can copy and move files around in a WebDAV directory.
Modify properties associated with certain resources. For example, a user can write to and retrieve a file's property information.
Lock and unlock resources so that multiple users can read a file concurrently. However, only one person can modify the file at a time.
Search the content and properties of files in a WebDAV directory.
Setting up a WebDAV publishing directory on your server is as straightforward as setting up a virtual directory through IIS Manager. After you have set up your publishing directory, users who have been assigned the correct rights can publish documents to the server and manipulate files in the directory.
Source: http://technet.microsoft.com/en-us/library/cc781730.aspx

Question: 256

Your network contains a Web server. The Web server is configured as shown in the following table.

Site name	Application pool	Microsoft .NET Framework version
Site1	AppPool1	No managed code
Site2	AppPool1	2.0
Site3	AppPool1	2.0

Site1 fails intermittently. You need to isolate Site1 from the other sites. What should you do?

A. Assign Site1 to a new application pool.
B. Add a managed handler to the Handler Mappings of Site1.
C. Install and configure Windows System Resource Manager (WSRM).
D. Upgrade the Site1 applications to use .NET Framework version 2.0.

Answer: A

Explanation:
An application belongs to an application pool, which isolates the application from applications in other application pools on the server. In the case of managed code applications, make sure to associate your application together with an application pool that is running the .NET Framework version that your application requires.
http://technet.microsoft.com/en-us/library/cc771654.aspx

Question: 257

Your network contains a Web server that runs Windows Server 2008 R2. The Web server has a Web site named Web1. Web1 hosts several HTML Web pages located in the C:\inetpub\wwwroot folder. Windows authentication is enabled for Web1. You need to prevent some users from accessing one of the HTML Web pages. What should you do?

A. From Windows Explorer, modify the NTFS permissions.
B. From Windows Explorer, modify the share permissions.
C. From Internet Information Services (IIS) Manager, modify the Authentication settings.
D. From Internet Information Services (IIS) Manager, modify the Request Filtering settings.

Answer: A

Question: 258

Your network contains a Web server named Server1 that runs Windows Server 2008 R2. Server1 contains a Web site named Web1. Users access Web1 by using the URL http://www.contoso.com. You plan to request a SSL certificate for Web1 from a trusted certification authority (CA). You need to create a certificate request for Web1. The solution must ensure that users do not receive certificate related error messages when they access the Web site. What should you specify as the common name value in the certificate request?

A. server1.contoso.com
B. web1
C. www
D. www.contoso.com

Answer: D

Question: 259

Your network contains a server named Server1 that has Microsoft SharePoint Foundation 2010 installed. You install the SMTP Server feature on Server1. You configure the incoming email settings from Central Administration. You mail-enable a document library. From an external email account, you attempt to send an email message to the document library and you receive a non-delivery report (NDR). You need to ensure that you can send email messages to the document library. What should you do?

A. Create a Mailbox (MB) record in DNS.
B. Create a Mail Exchanger (MX) record in DNS.
C. Configure the outgoing email settings in Central Administration.
D. Configure the connection control settings of the SMTP virtual server.

Answer: B

Question: 260

Your network contains a server named Server1 that has Microsoft SharePoint Foundation 2010 installed. Server1 contains a SharePoint site collection named Site1. You install Office Web Apps on Server1. Users report that when they click on a link for a Microsoft Word document in Site1, the document opens in Internet Explorer. You need to configure Server1 to meet the following requirements:

- If a user has Word installed locally, Word documents must open in Word by default.

- If a user does not have Word installed, Word documents must open in Internet Explorer.

What should you do?

A. Deactivate Office Web Apps.
B. Modify the site collection features.
C. Modify the Default Programs settings on Server1.
D. Modify the Default Programs settings on the client computers.

Answer: B

Explanation:
Activate the Office Web Apps Feature for a site collection
The Office Web Apps Feature should be activated on every site collection for which any of the Web apps will be available. Typically, you activate the Office Web Apps Feature on a site collection during the deployment phase after you run setup and activate the services; however, in some cases, you can decide to later activate only on particular site collections and deactivate on other site collections.
To activate the Office Web Apps Feature on a site collection on the Site collection features page
1. In a browser, in the SharePoint site, click Site Actions, and then click Site Settings.
2. On the Site Settings page, in Site Collection Administration, click Site Collection Features.
3. On the Features page, for Office Web Apps, click Activate.
Source: http://technet.microsoft.com/en-us/library/ee837418.aspx
Configure the default open behavior for documents
In SharePoint, you can configure whether browser-enabled documents are opened in a client application or in the browser. By default, when Office Web Apps is installed, Office documents will open in the browser. You can override this setting using the SharePoint OpenInClient feature. The OpenInClient feature can be configured in Central Administration or by using the SPFeature cmdlet in Windows PowerShell.
How documents open in SharePoint varies depending on whether the OpenInClient feature is present, and either enabled or disabled:
If the OpenInClient feature is not present and Office Web Apps is not installed, documents will open in the client application (SharePoint default). If the OpenInClient feature is not present, Office Web Apps is installed and Office Web Apps service applications are activated, documents will open in the browser (Office Web Apps default).
If the OpenInClient Feature is present and enabled, and Office Web Apps service applications are activated, documents will open in the client application.
If the OpenInClient Feature is present and disabled, and Office Web Apps service applications are activated, documents in will open in the browser.
To set the default open behavior for site collections by using Central Administration
1. In SharePoint Central Administration, click Site Actions, and then click Site Settings.
2. On the Site Settings page, under Site Collection Administration, click Site Collection Features.
3. On the Features page, for the Open Documents in Client Applications by Default feature, click Activate
(OpenInClient Feature is enabled) to open documents in the client application. Click Deactivate
(OpenInClient Feature is disabled) to open documents in the browser.
Source: http://technet.microsoft.com/en-us/library/ee837425.aspx

Question: 261

Your network contains a server named Server1 that runs Windows Server 2008 R2. You have a Microsoft Application Virtualization (App-V) application named App1. You need to publish App1 as a RemoteApp program. Which role service should you install on Server1?

A. Remote Desktop Gateway (RD Gateway)
B. Remote Desktop Session Host (RD Session Host)

C. Remote Desktop Virtualization Host (RD Virtualization Host)
D. Remote Desktop Web Access (RD Web Access)

Answer: B

Question: 262

Your network contains an Active Directory domain. You deploy a server named Server1 that has the Remote Desktop Connection Broker (RD Connection Broker) role service installed. You need to ensure that all servers that have the Remote Desktop Session Host (RD Session Host) role service installed are automatically configured to use Server1 as an RD Connection Broker. What should you do?

A. Register a service principal name (SPN) for Server1.
B. Register a service location (SRV) record for Server1.
C. Use a Group Policy to configure the Restricted Groups settings.
D. Use a Group Policy to configure the Remote Desktop Services settings.

Answer: D

Explanation:
RD Connection Broker
Policy settings in this node control configuration of a Remote Desktop Session Host server that is a member of a load-balanced Remote Desktop Session Host server farm.
The full path of this node in the Group Policy Management Console is
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\RD Connection Broker.
Available policy settings Join RD Connection Broker
This policy setting allows you to specify whether the RD Session Host server should join a farm in RD Connection Broker. RD
Connection Broker tracks user sessions and allows a user to reconnect to their existing session in a load-balanced RD Session Host server farm. To participate in RD Connection Broker, the Remote Desktop Session Host role service must be installed on the server.
If the policy setting is enabled, the RD Session Host server joins the farm that is specified in the Configure RD Connection Broker Farm Name setting. The farm exists on the RD Connection Broker server that is specified in the Configure RD Connection Broker
Server name policy setting.
If you disable this policy setting, the server does not join a farm in RD Connection Broker, and user session tracking is not performed. If the setting is disabled, you cannot use either the Remote Desktop Session Host Configuration tool or the Terminal
Services WMI provider to join the server to RD Connection Broker.
If the policy setting is not configured, the setting is not specified at the Group Policy level. In this case, you can configure the server
to join RD Connection Broker by using the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider.
If you enable this setting, you must also enable the "Configure RD Connection Broker Farm Name" and Configure RD Connection Broker Server name policy settings, or configure these settings by using either the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider.
Configure RD Connection Broker farm name
This policy setting allows you to specify the name of a farm to join in RD Connection Broker. RD Connection Broker uses the farm name to determine which RD Session Host servers are in the same RD Session Host server farm.

Therefore, you must use the same farm name for all RD Session Host servers in the same load-balanced farm. The farm name does not have to correspond to a name in Active Directory Domain Services.
If you specify a new farm name, a new farm is created in RD Connection Broker. If you specify an existing farm name, the server joins that farm in RD Connection Broker.
If you enable this policy setting, you must specify the name of a farm in RD Connection Broker.
If you disable or do not configure this policy setting, the farm name is not specified by Group Policy. In this case, you can adjust the farm name by using the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider.
This setting is not effective unless both the Join RD Connection Broker and the Configure RD Connection Broker server name settings are enabled and configured by using Group Policy, the Remote Desktop Session Host Configuration tool, or the Terminal Services WMI provider.
Configure RD Connection Broker server name
This policy setting allows you to specify the RD Connection Broker server that the RD Session Host server uses to track and redirect user sessions for a load-balanced RD Session Host server farm. The specified server must be running the Remote Desktop Connection Broker service. All RD Session Host servers in a load-balanced farm should use the same RD Connection Broker server.
If you enable this policy setting, you must specify the RD Connection Broker server, using either its host name, IP address, or fully qualified domain name. If you specify a name or IP address for the RD Connection Broker server that is not valid, an error message is logged in Event Viewer on the RD Session Host server.
If you disable or do not configure this policy setting, you can adjust the RD Connection Broker server name or IP address by usin the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider.
This policy setting is not effective unless the Join RD Connection Broker policy setting is enabled or the RD Session Host server is configured to join RD Connection Broker by using the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider.
To be an active member of an RD Connection Broker-enabled RD Session Host server farm, the computer account for each RD Session Host server in the farm must be a member of the Session Directory Computers local group on the RD Connection Broker server.
Use RD Connection Broker load balancing
This policy setting allows you to specify whether to use the RD Connection Broker load balancing feature to balance the load between servers in an RD Session Host server farm.
If you enable this policy setting, RD Connection Broker redirects users who do not have an existing session to the RD Session Host server in the farm with the fewest sessions. Redirection behavior for users with existing sessions is not affected. If the server is configured to use RD Connection Broker, users who have an existing session are redirected to the RD Session Host server where their session exists.
If you disable this policy setting, users who do not have an existing session log on to the first RD Session Host server to which they connect.
If you do not configure this policy setting, you can configure the RD Session Host server to participate in RD Connection Broker load balancing by using the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider.
If you enable this policy setting, you must also enable the Join RD Connection Broker, the Configure RD Connection Broker farm name, and the Configure RD Connection Broker server name policy settings.
Source: http://technet.microsoft.com/en-us/library/ee791821.aspx

Question: 263

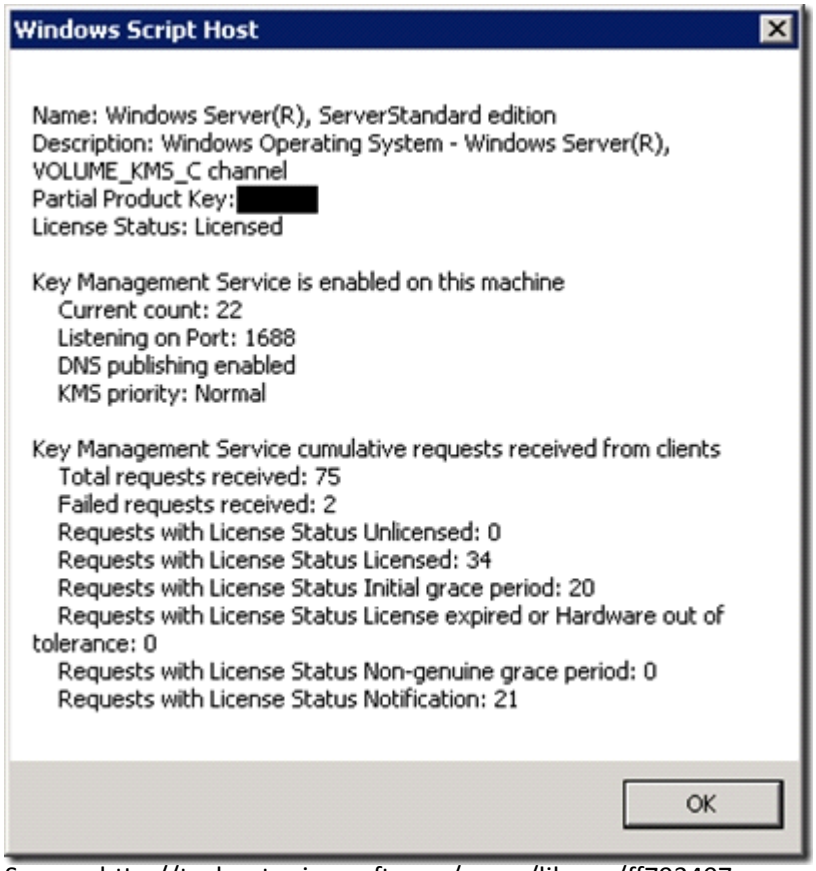
You have a server named Server1 that runs Windows Server 2008 R2. Server1 has the Key Management Service (KMS) installed. You need to identify how many computers were activated by Server1. What should you run?

A. cliconfg.exe
B. mrinfo.exe Server1
C. slmgr.vbs / dli

D. slui.exe

Answer: C

Explanation:
slmgr.vbs /dli - Retrieves the current KMS activation count from the KMS host.



Source: http://technet.microsoft.com/en-us/library/ff793407.aspx

Question: 264

Your network contains 10 servers that have the Remote Desktop Session Host (RD Session Host) role service installed. You install the Remote Desktop Gateway (RD Gateway) role service on a new server. You need to ensure that users can access the RD Session Host servers by using the RD Gateway. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Create a Remote Desktop resource authorization policy (RD RAP).
B. Create a Remote Desktop connection authorization policy (RD CAP).
C. Install the RD Session Broker role service.
D. Install the Remote Desktop Web Access (RD Web Access) role service.

Answer: A, B

Question: 265

Your company has an Active Directory domain. The company runs Remote Desktop Services. You configure the main office printer as the default printer on the Remote Desktop Session Host Server. The company policy states that all

remote client computers must meet the following requirements: The main office printer must be the default printer of the client computers. Users must be able to access their local printers during a remote desktop session. You need to create a Group Policy object (GPO) by using the Remote Desktop Session Host Printer Redirection template to meet the company policy. What should you do?

A. Set the Use Remote Desktop Easy Print printer driver first option to Disabled. Apply the GPO to the Remote Desktop Session Host Server.
B. Set the Use Remote Desktop Easy Print printer driver first option to Disabled. Apply the GPO to all the client computers.
C. Set the Do not set default client printer to be default printer in a session option to Enabled. Apply the GPO to the Remote Desktop Session Host Server.
D. Set the Do not set default client printer to be default printer in a session option to Enabled. Apply the GPO to all the client computers.

Answer: C

Explanation:
Do not set default client printer to be default printer in a session
This policy setting allows you to specify whether the client default printer is automatically set as the default printer in a Terminal Services session.
By default, Terminal Services automatically designates the client default printer as the default printer in a Terminal Services session. You can use this policy setting to override this behavior.
If you enable this policy setting, the default printer is the printer specified on the remote computer.
If you disable this policy setting, the terminal server automatically maps the client default printer and sets it as the default printer upon connection.
If you do not configure this policy setting, the default printer is not specified at the Group Policy level. However, an administrator can configure the default printer for client sessions by using the Terminal Services Configuration tool.
Source: http://technet.microsoft.com/en-us/library/cc731963(WS.10).aspx

Question: 266

Your network contains two servers that have the Remote Desktop Web Access (RD Web Access) role service installed. Each server hosts three different RemoteApp programs. You deploy a new server that has the Remote Desktop Connection Broker (RD Connection Broker) role service installed. Users report that when they connect to one of the RD Web Access servers, they see only three applications. You need to ensure that the users see all six RemoteApp programs when they connect to an RD Web Access server. Which two actions should you perform? (Each correct answer present part of the solution. Choose two.)

A. From RemoteApp Manager, configure the RD Gateway Settings
B. From RemoteApp Manager, configure the Digital Signature Settings.
C. From Remote Desktop Connection Manager, add RemoteApp sources.
D. From Remote Desktop Connection Manager, add RD Web Access servers.

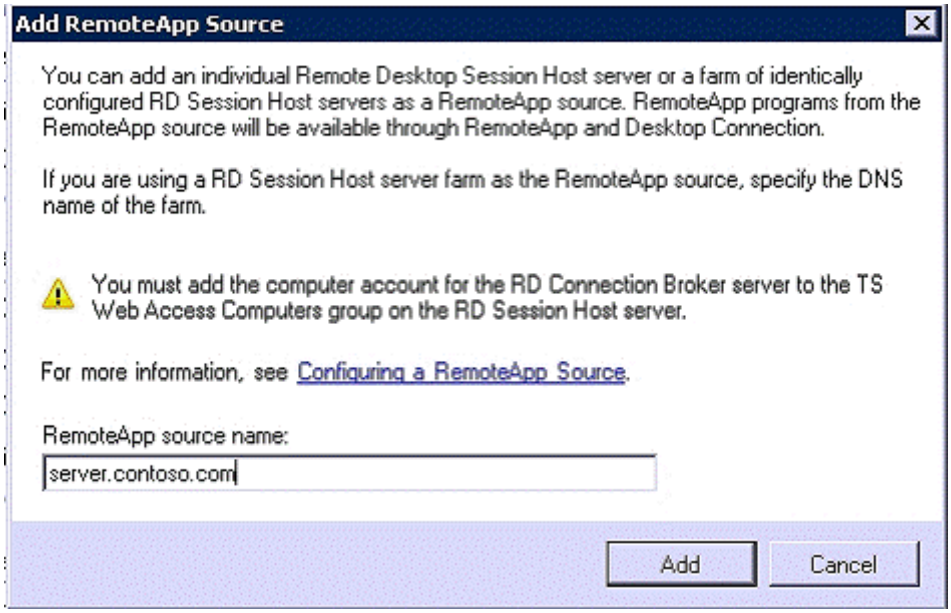
Answer: C, D

Explanation:
To add a RD Web Access Server by using Remote Desktop Connection Manager
1. Log on to Remote Desktop Connection Broker as CONTOSO\Administrator.
2. Click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Connection Manager.

3. I the Actions pane, click Add RD Web Access Server.
4. In the Server name box, type the computer name and then click Add.

To add a RemoteApp source by using Remote Desktop Connection Manager

1. Log on to Remote Desktop Connection Broker as CONTOSO\Administrator.
2. Click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Connection Manager.
3. In the Actions pane, click Add RemoteApp Source.
4. In the RemoteApp source name box, type the computer name and then click Add.



Question: 267

Your network contains a server that has the Remote Desktop Session Host (RD Session Host) role service installed. You need to ensure that the Remote Desktop sessions of administrators are more responsive than other sessions when the server is under a heavy load. What should you do?

A. From the RDP-Tcp properties, modify the Client Settings.
B. From the RDP-Tcp properties, modify the Sessions settings.
C. Install and configure the RD Session Broker role service.
D. Install and configure Windows System Resource Manager (WSRM).

Answer: D

Question: 268

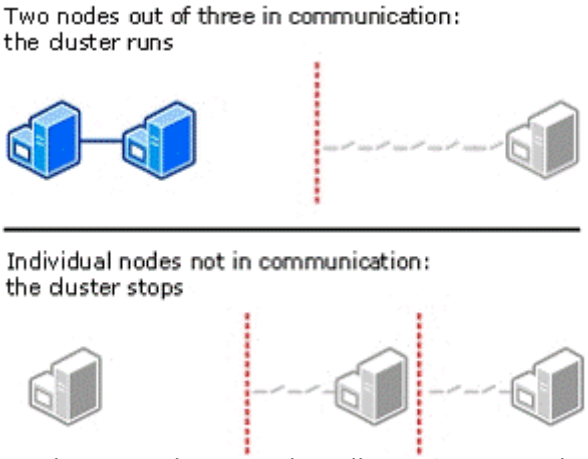
Your network contains two servers that run Windows Server 2008 R2. The servers are located on different IP subnets. You plan to configure the servers in a two-node failover cluster. You need to select the quorum model for the cluster. The solution must ensure that users can access the cluster resources if a single node fails. Which quorum model should you select?

A. No Majority: Disk Only
B. Node and Disk Majority
C. Node and File Share Majority
D. Node Majority

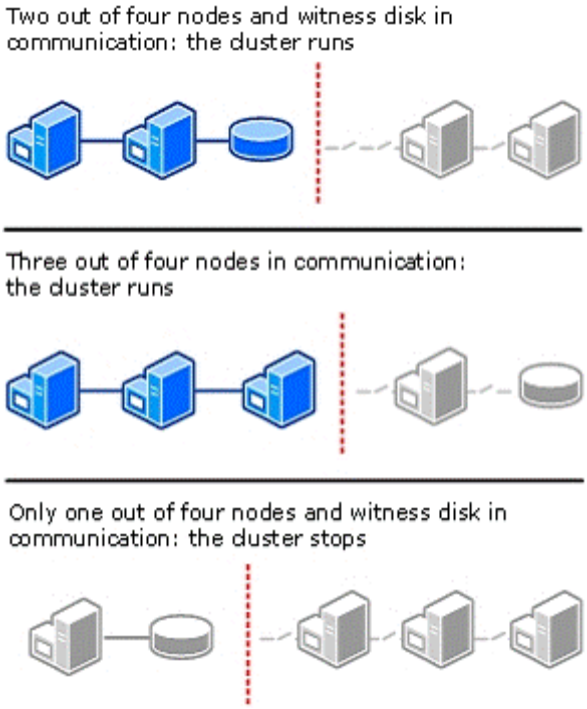
Answer: C

Explanation:
Quorum configuration choices
You can choose from among four possible quorum configurations:
Node Majority (recommended for clusters with an odd number of nodes)
Can sustain failures of half the nodes (rounding up) minus one. For example, a seven node cluster can sustain three

node failures.
Node and Disk Majority (recommended for clusters with an even number of nodes) Can sustain failures of half the nodes (rounding up) if the disk witness remains online. For example, a six node cluster in which the disk witness is online could sustain three node failures. Can sustain failures of half the nodes (rounding up) minus one if the disk witness goes offline or fails. For example, a six node cluster with a failed disk witness could sustain two (3-1=2) node failures.
Node and File Share Majority (for clusters with special configurations)
Works in a similar way to Node and Disk Majority, but instead of a disk witness, this cluster uses a file share witness.
Note that if you use Node and File Share Majority, at least one of the available cluster nodes must contain a current copy of the cluster configuration before you can start the cluster. Otherwise, you must force the starting of the cluster through a particular node. For more information, see "Additional considerations" in Start or Stop the Cluster Service on a Cluster Node.
No Majority: Disk Only (not recommended) Can sustain failures of all nodes except one (if the disk is online). However, this configuration is not recommended because the disk might be a single point of failure.
Illustrations of quorum configurations
The following illustrations show how three of the quorum configurations work. A fourth configuration is described in words, because it is similar to the Node and Disk Majority configuration illustration.
Note:
In the illustrations, for all configurations other than Disk Only, notice whether a majority of the relevant elements are in communication (regardless of the number of elements). When they are, the cluster continues to function.
When they are not, the cluster stops functioning.



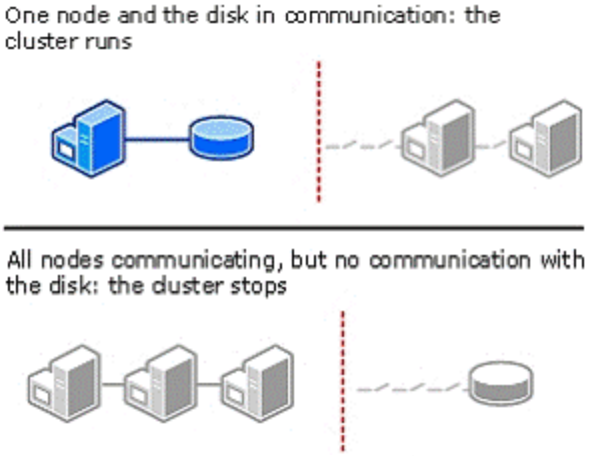
As shown in the preceding illustration, in a cluster with the Node Majority configuration, only nodes are counted when calculating a majority.



As shown in the preceding illustration, in a cluster with the Node and Disk Majority configuration, the nodes and the disk witness are counted when calculating a majority.

Node and File Share Majority Quorum Configuration

In a cluster with the Node and File Share Majority configuration, the nodes and the file share witness are counted when calculating a majority. This is similar to the Node and Disk Majority quorum configuration shown in the previous illustration, except that the witness is a file share that all nodes in the cluster can access instead of a disk in cluster storage.



In a cluster with the Disk Only configuration, the number of nodes does not affect how quorum is achieved. The disk is the quorum. However, if communication with the disk is lost, the cluster becomes unavailable.

Source: http://technet.microsoft.com/en-us/library/cc731739.aspx

Question: 269

Your network contains a two-node Hyper-V cluster that hosts 10 virtual machines (VMs). You discover that when a failover occurs, all of the VMs fail over simultaneously. You need to modify the cluster so that you can fail over each VM individually. What should you do first?

A. Add a third node to the cluster.
B. Create a Clustered Shared Volume.

C. Add a new disk to the failover cluster.
D. Modify the properties of the cluster failover.

Answer: B

Question: 270

Your network contains a server that runs Windows Server 2008 R2 Standard. The server is configured to native boot from a virtual hard disk (VHD). All hard disks on the server are configured as basic disks that use an MBR. A new corporate security policy states that all of the hard disks on the server must use Windows BitLocker Drive Encryption (BitLocker). You need to ensure that the server meets the corporate security policy. What should you do first?

A. Configure the disks to use a GPT.
B. Convert the disks to dynamic disks.
C. Upgrade the server to Windows Server 2008 R2 Enterprise.
D. Back up the server and restore the server to a physical volume.

Answer: D

Explanation:
Applies To: Windows 7, Windows Server 2008 R2
Configuring native VHD boot if the host volume is protected by BitLocker. You can save a VHD file on a file system that is protected by BitLocker™, but you cannot use the VHD for native boot or enable Bitlocker on the volume(s) that are contained inside a VHD.
Source: http://technet.microsoft.com/en-us/library/dd440865(WS.10).aspx

Question: 271

Your network contains a virtual machine (VM) named VM1. VM1 contains two virtual hard disks (VHDs). One VHD is a dynamically expanding disk and the other VHD is a fixed disk. You need to manually copy the VHDs. The solution must minimize the amount of downtime for VM1. What should you do first?

A. From Hyper-V Manager, reset VM1.
B. From Hyper-V Manager, pause VM1.
C. Run the Export-VM PowerShell cmdlet.
D. Run the Unmount-VHD PowerShell cmdlet.

Answer: B

Question: 272

Your network contains a server that runs Windows Server 2008 R2 and has the Windows Deployment Services (WDS) server role installed. You have a .vhd file that contains an installation of Windows 7. You need to deploy the Windows 7 installation by using WDS. You want to achieve this goal by using the minimum amount of administrative effort. What should you do first?

A. From Disk Management, mount the .vhd file.
B. From Windows Deployment Services, add a capture image.
C. Run the imagex.exe command and specify the /export parameter.

D. Run the wdsutil.exe command and specify the /add-image parameter.

Answer: D

Explanation:
To add a virtual hard disk image to the server
1. Click Start, right-click Command Prompt, and then click Run as administrator.
2. You must create an image group because .vhd images cannot be in image groups with .wim images. To create an image group for the .vhd image, use the following syntax: WDSUTIL /Add-ImageGroup /ImageGroup:
<image group name>.
Example: WDSUTIL /Add-ImageGroup /ImageGroup:"VHD Image Group"
3. To add the .vhd image to the server, use the following syntax (at a minimum): WDSUTIL /Verbose /Progress /
Add-Image /ImageFile:<path> /ImageType:Install /ImageGroup:<image group name>.
For differencing disks, the path to the image should be to the .vhd file of the differencing disk and not to the parent disk. Adding the differencing .vhd will add the parent .vhd file to the server, but only the differencing disk will be active (the parent .vhd will be inactive). If the differencing disk is part of chain, choose the last .vhd in the chain. In that case, the immediate parent .vhd and all preceding parent .vhd files in the chain will also be added.
Full syntax: WDSUTIL /add-Image /ImageFile:<.vhd file path> [/Server:<server name>] /ImageType:install [/
ImageGroup:<image group name>] [/Filename:<new image file name>] [/UnattendFile:<full path to unattend
file>]
Example: WDSUTIL /Verbose /Progress /Add-Image /ImageFile:"C:\vhd
\WindowsServer2008R2.vhd" /Server:MyWDSServer /ImageType:Install /ImageGroup:"VHD
Image Group"
4. Repeat step 3 until you have added all of your .vhd images.
5. If you want to update the description for an image, use the following steps:
a. Run WDSUTIL /Get-ImageGroup /ImageGroup:<image group name> and note the name that the server assigned to the image. To display the full image metadata on each image in the group, append /Detailed.
Example: WDSUTIL /Get-ImageGroup /ImageGroup:"VHD Image Group"
b. To update the description for an image, use the following syntax where <image name> is the name you noted in the previous step: WDSUTIL /Set-Image /Image:<image name> /ImageType:Install /ImageGroup:<image
group name> /Description:<description>.
Example: WDSUTIL /Set-Image /Image:"VHD image" /ImageType:Install /ImageGroup:"VHD Image Group" /
Description:"VHD image for R2"
Source: http://technet.microsoft.com/en-us/library/dd363560(WS.10).aspx

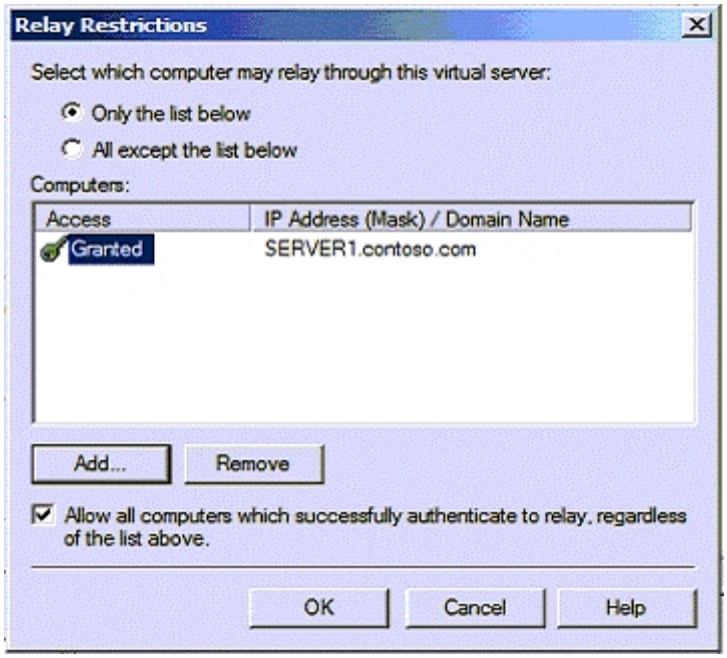
Question: 273

Your network contains an Active Directory domain. The domain contains a server named Server1 that has Microsoft SharePoint Foundation 2010 installed. You install the SMTP Server feature on a server named SMTP1. From Central Administration on Server1, you configure SMTP1 as the outbound mail server for the SharePoint farm. You need to ensure that SMTP1 can deliver all email messages sent from Server1. What should you do?

A. On Server1, create an inbound firewall rule.
B. On Server1, create an outbound firewall rule.
C. On SMTP1, configure the Authentication settings.
D. On SMTP1, configure the Relay Restrictions settings.

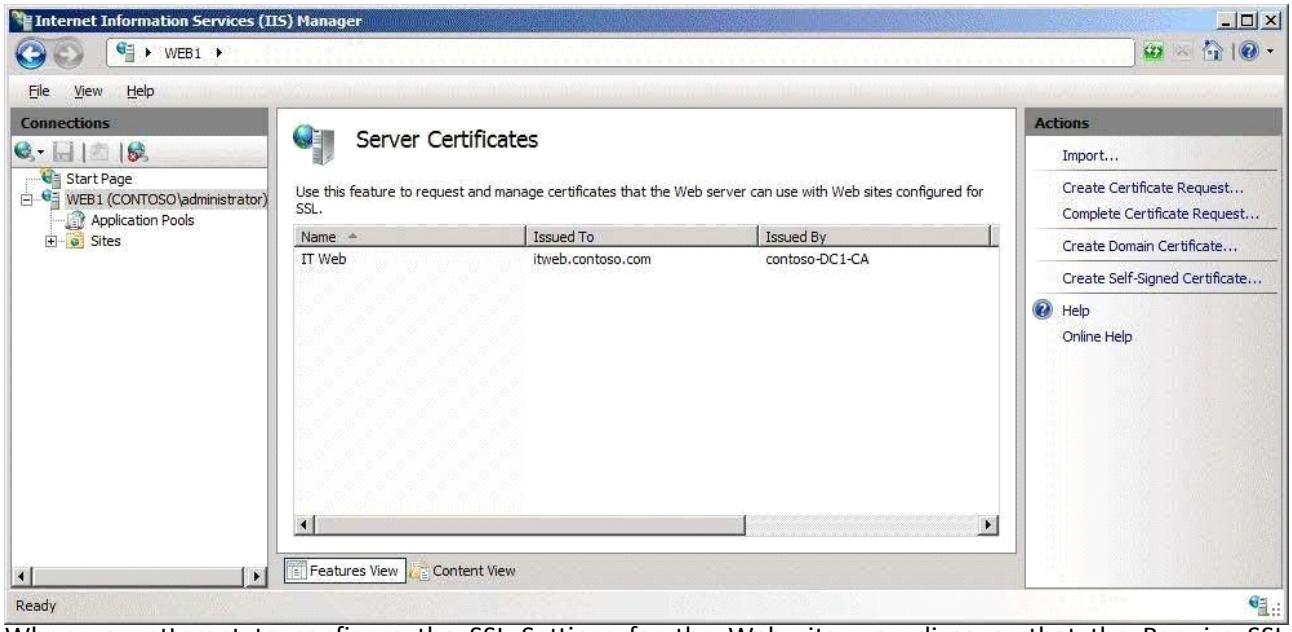
Answer: D

Explanation:



Question: 274

Your network contains a server named Web1 that runs Windows Server 2008 R2. Web1 has the Web Server (IIS) role installed. Web1 hosts a Web site that is accessed by using the URL http://itweb.contoso.com. The server certificates for Web1 are shown in the exhibit. (Click the Exhibit button.)

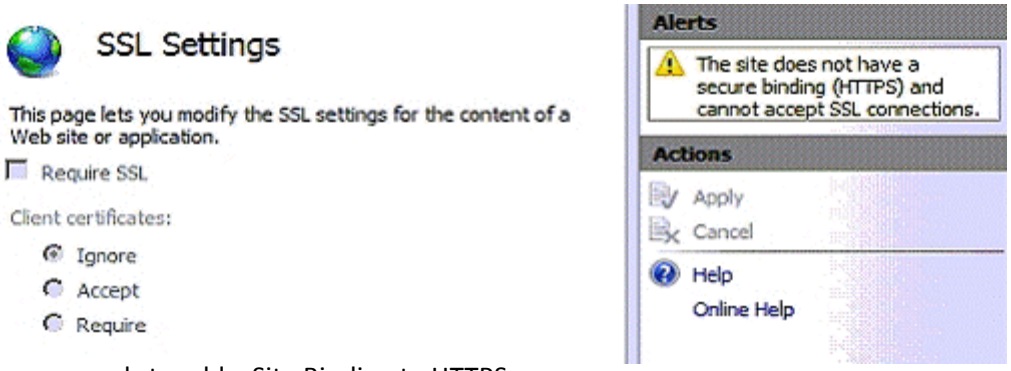


When you attempt to configure the SSL Settings for the Web site, you discover that the Require SSL option is unavailable. You need to ensure that you can require SSL for the Web site. What should you do?

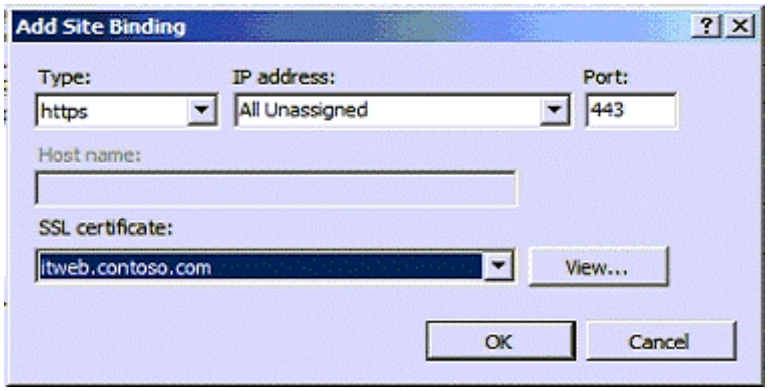
A. Run iisreset.exe /force.
B. Configure the bindings for the Web site.
C. Request a new domain certificate and specify Web1 as the common name.
D. Request a self-signed certificate and specify itweb.contoso.com as the friendly name.

Answer: B

Explanation:



So one needs to add a Site Binding to HTTPS:



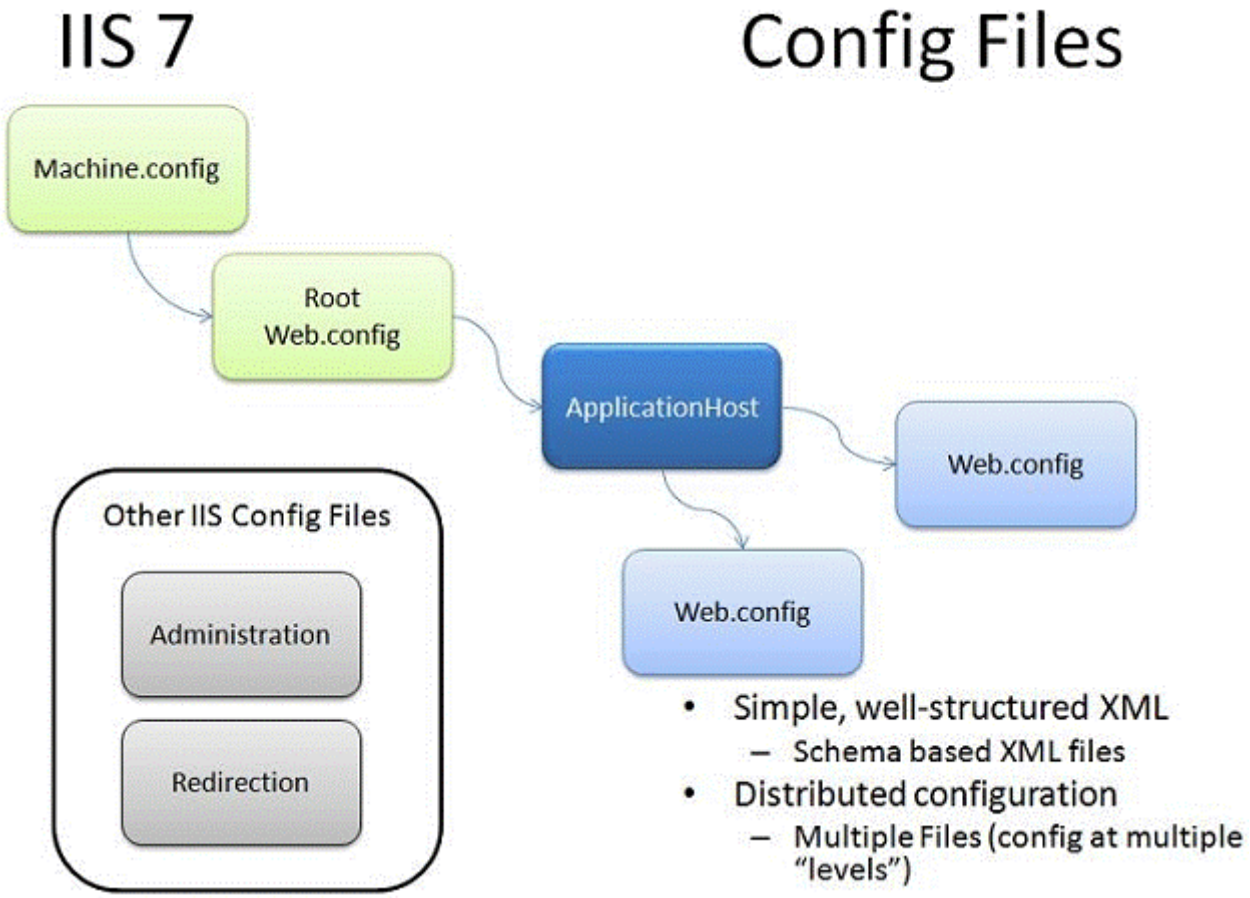
Question: 275

Your network contains a Web server that runs Windows Server 2008 R2. The server contains 10 Web sites. You need to back up the Microsoft ASP.NET configuration settings of one Web site. The solution must minimize the size of the backup. What should you do?

A. Perform a system state backup.
B. Copy the Web.config file.
C. Copy the ApplicationHost.config file.
D. Copy the %systemdrive%\inetpub folder.

Answer: B

Explanation:
In the web content directories, there may be optional web.config files that control the behavior for their level of the hierarchy and downward. They could be local or remote (if the content directory is on a UNC share, for example). They may contain IIS, ASP.NET or any other .NET framework configuration settings that can be specified at their level. By default there are no web.config files.



Source: http://learn.iis.net/page.aspx/282/the-configuration-system-in-iis-7/

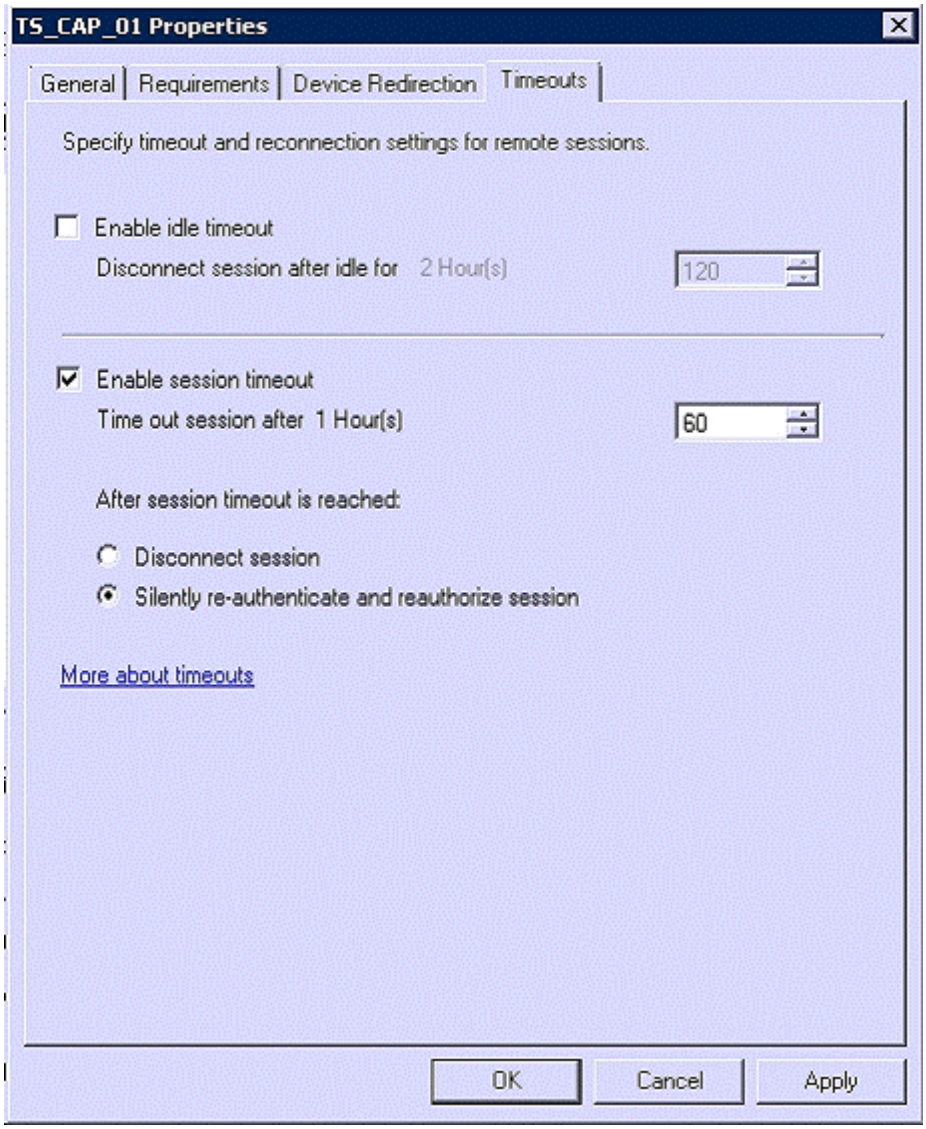
Question: 276

Your network contains a server that has the Remote Desktop Gateway (RD Gateway) role service installed. You plan to modify the Remote Desktop resource authorization policies (RD RAPs). You need to ensure that the new RD RAP settings are applied to all Remote Desktop sessions within one hour. What should you do?

A. Configure the General settings of the Remote Desktop resource authorization policies (RD RAPs).
B. Configure the Timeouts settings of the Remote Desktop connection authorization policies (RD CAPs).
C. Configure the Network Resource settings of the Remote Desktop resource authorization policies (RD RAPs).
D. Configure the Requirements settings of the Remote Desktop connection authorization policies (RD CAPs).

Answer: B

Explanation:
Section: Remote Desktop Services (RDS)



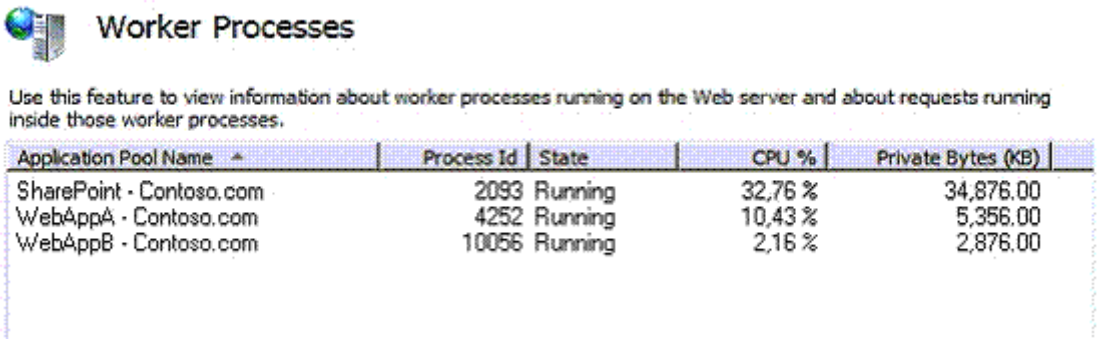
Question: 277

Your network contains a Web server that runs Windows Server 2008 R2. The Web server contains 100 application pools. You need to identify which application pool is using the most CPU resources.
Which tool should you use?

A. Appcmd
B. Internet Information (IIS) Manager
C. Resource Monitor
D. Task Manager

Answer: B

Explanation:



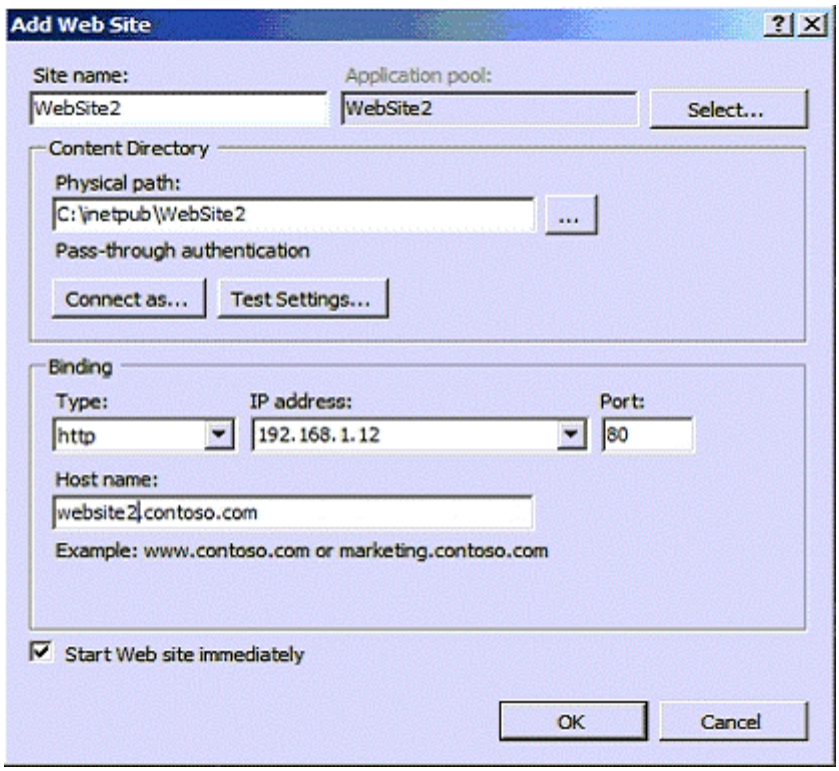
Question: 278

Your network contains a Web server that runs Windows Server 2008 R2. The server has a single IP address. You plan to create several Web sites. You need to ensure that each Web site is accessible over TCP port 80. What should you configure?

A. the application pools for the server
B. the bindings for each site
C. the ISAPI Filters for each site
D. the Request Filtering settings for the server

Answer: B

Section: Internet Information Server (IIS)
Explanation:



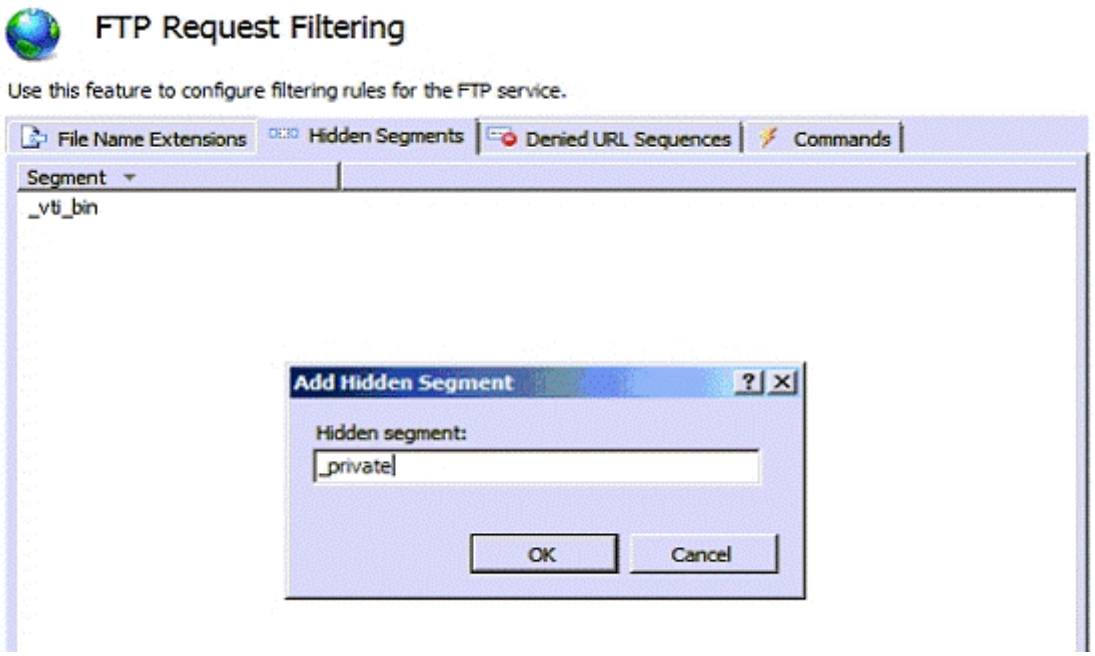
Question: 279

Your network contains an FTP server that runs Windows Server 2008 R2. You need to prevent FTP users from viewing all folders named _private. What should you configure?

A. FTP Authorization Rules
B. FTP Directory Browsing
C. FTP IPv4 Address and Domain Restrictions
D. FTP Request Filtering

Answer: D

Section: Internet Information Server (IIS)
Explanation:



Question: 280

Your network contains an FTP server that runs Windows Server 2008 R2. The server has two FTP sites. The sites are configured as shown in the following table.

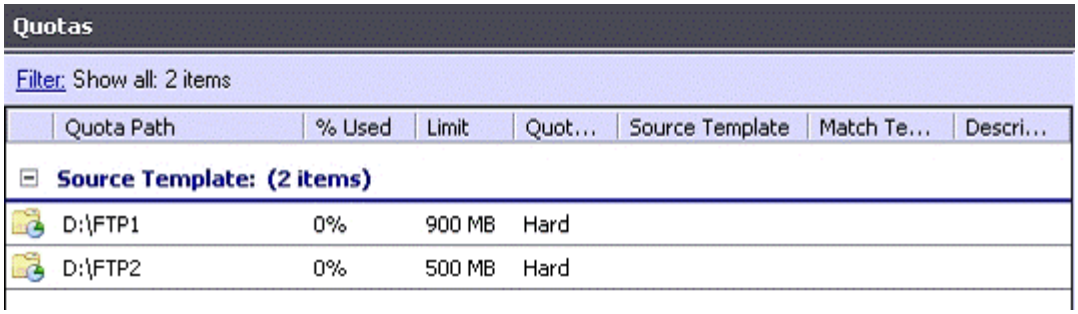
Site Name	Site Root	User isolation mode
FTP1	D:\FTP1	Disabled
FTP2	D:\FTP2	Enabled

You need to prevent users from storing more than 500 MB of data on FTP2. The users must be able to store at least 900 MB of data on FTP1. What should you do?

A. Modify the properties of the FTP1 site.
B. Modify the properties of the FTP2 site
C. Create a disk quota from Windows Explorer.
D. Install File Server Resource Manager (FSRM) and create a quota.

Answer: D

Explanation:



Question: 281

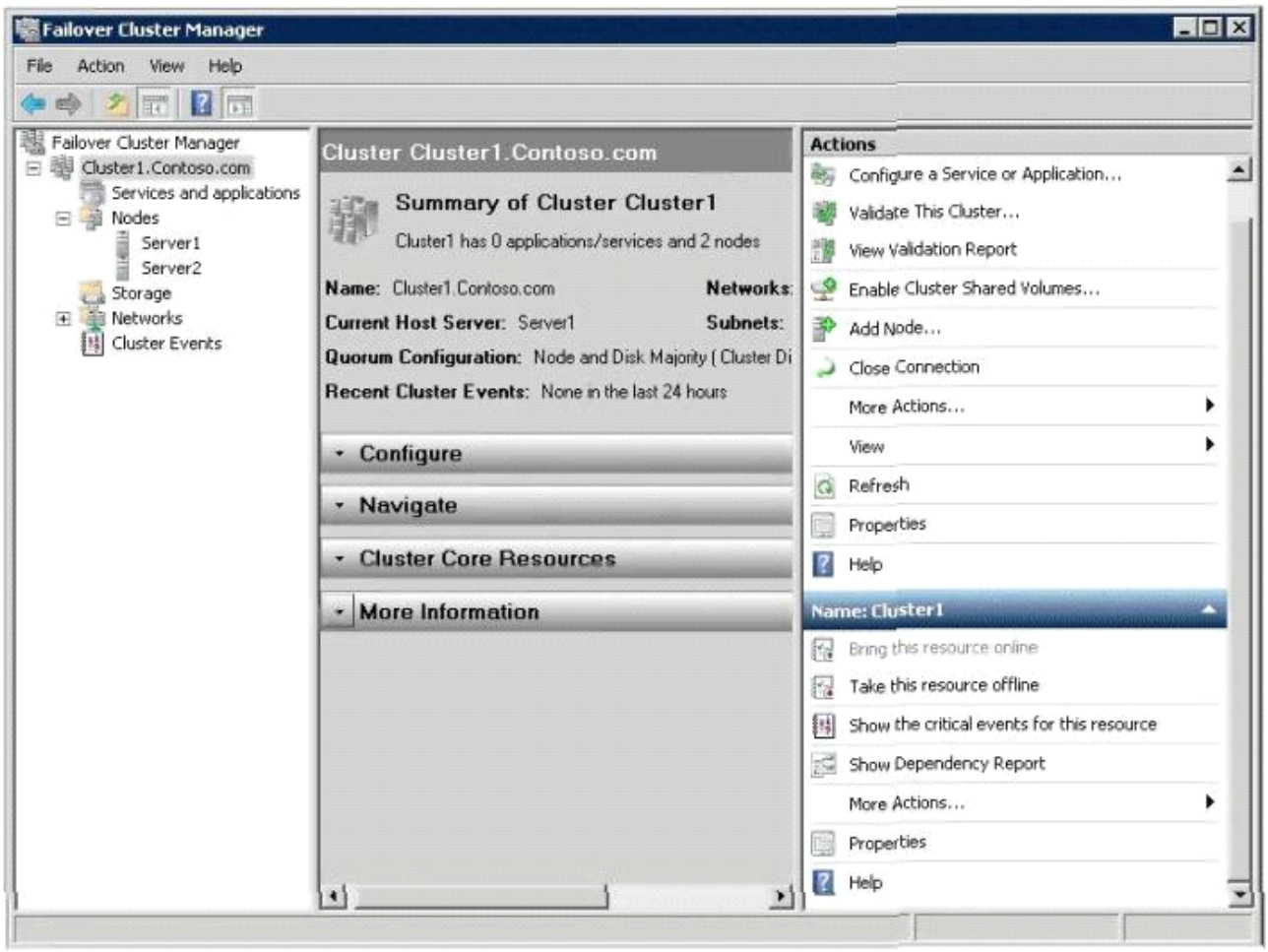
Your network contains an Active Directory domain. The domain contains a member server named Server1. Server1 has the Windows Deployment Services (WDS) server role installed. You need to ensure that only approved client computers receive a boot image from Server1. Which settings should you modify on Server1?

A. Computer Account Location
B. PXE Boot Policy
C. Client Naming Policy
D. PXE Response Policy

Answer: D

Question: 282

Your network contains two Hyper-V hosts named Server1 and Server2. Server1 and Server2 belong to a failover cluster. Server1 and Server2 are connected to the same 2-terabyte logical unit number (LUN). You open Failover Cluster Manager as shown in the exhibit. (Click the Exhibit button.)



The cluster will host 20 highly available virtual machines (VMs). You need to ensure that the VMs can fail over independently. Which action should you select from Failover Cluster Manager?

A. validate This Cluster
B. Add Node
C. Enable Cluster Shared Volumes
D. Configure a Service or Application

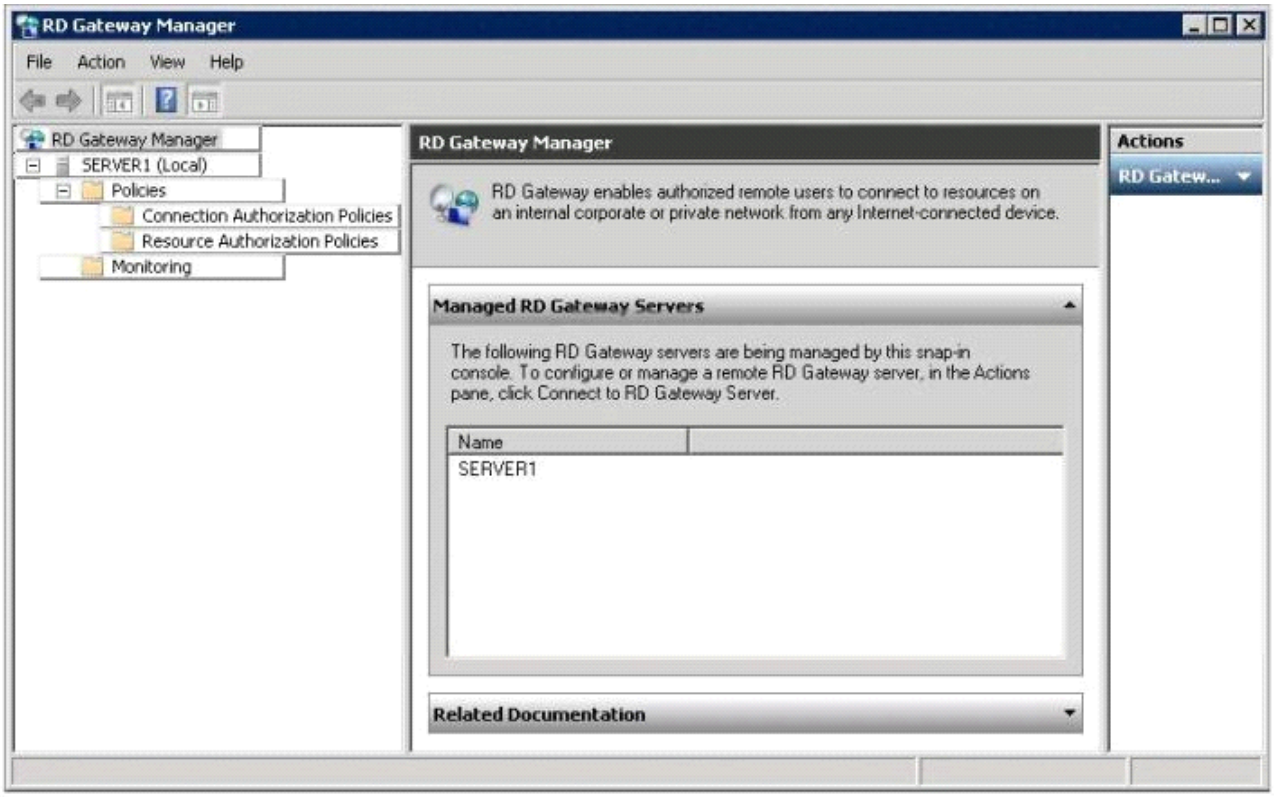
Answer: C

Question: 283
HOTSPOT

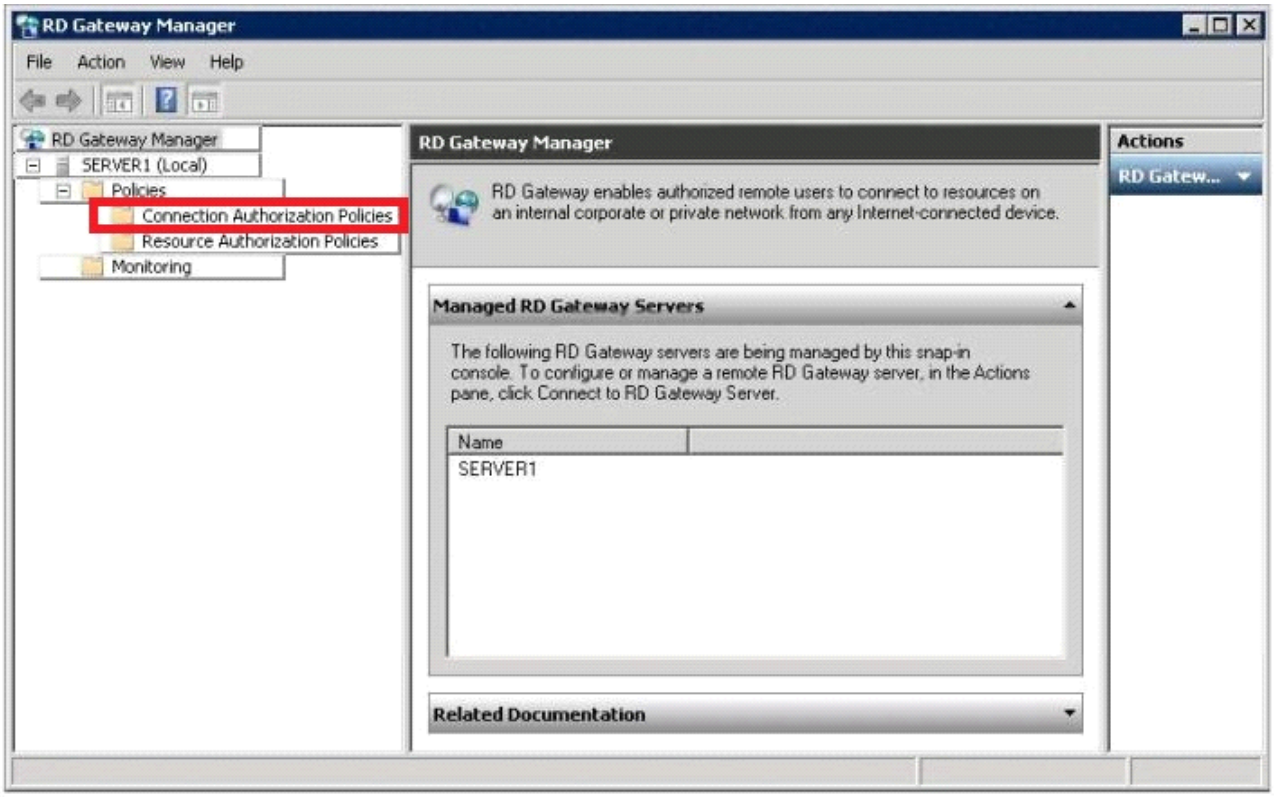
Your network contains three servers. The servers are configured as shown in the following table.

Server name	Role service
Server1	Remote Desktop Gateway (RD Gateway)
Server2	Remote Desktop Session Host (RD Sessions Host)
Server3	Remote Desktop Session Host (RD Sessions Host)

You need to allow only certain users to establish Remote Desktop connections through the RD Gateway server. Which node from RD Gateway Manager should you use to achieve this task? To answer, select the appropriate node in the answer area.



Answer:



Question: 284

Your network contains three servers named Server1, Server2, and Server3. Server1 is located on a perimeter network.

Server2 and Server3 are accessible from the internal network only. Users connect to Server2 and Server3 to run RemoteApp programs. You need to ensure that remote users can run the RemoteApp programs on Server2 and Server3. The solution must minimize the number of ports that must be opened on the internal firewall. Which role service should you install on Server3?

A. Remote Desktop Connection Broker (RD Connection Broker)
B. Remote Desktop Web Access (RD Web Access)
C. Remote Desktop Gateway (RD Gateway)
D. Remote Desktop Session Host (RD Session Host)

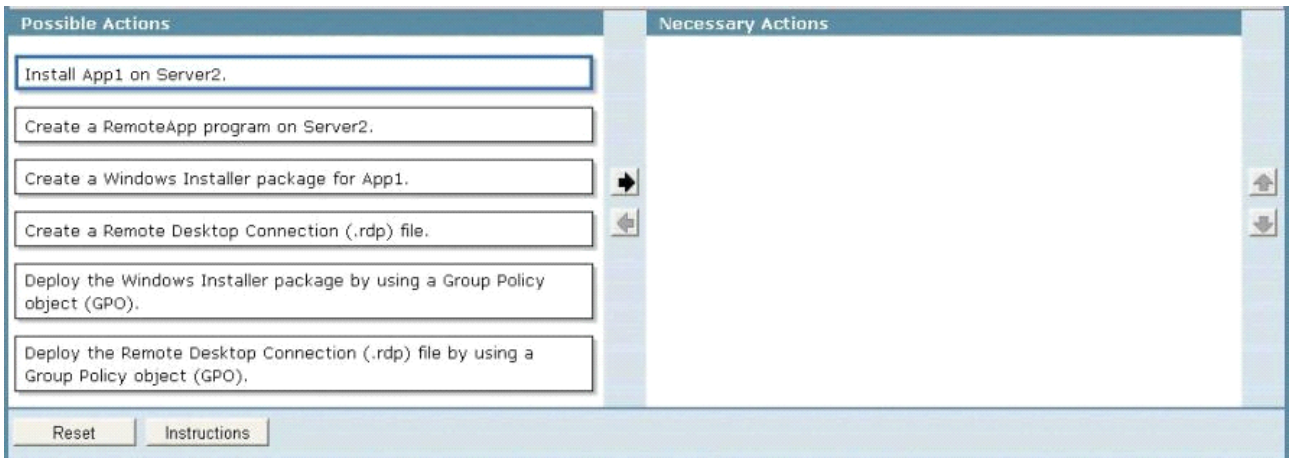
Answer: C

Question: 285

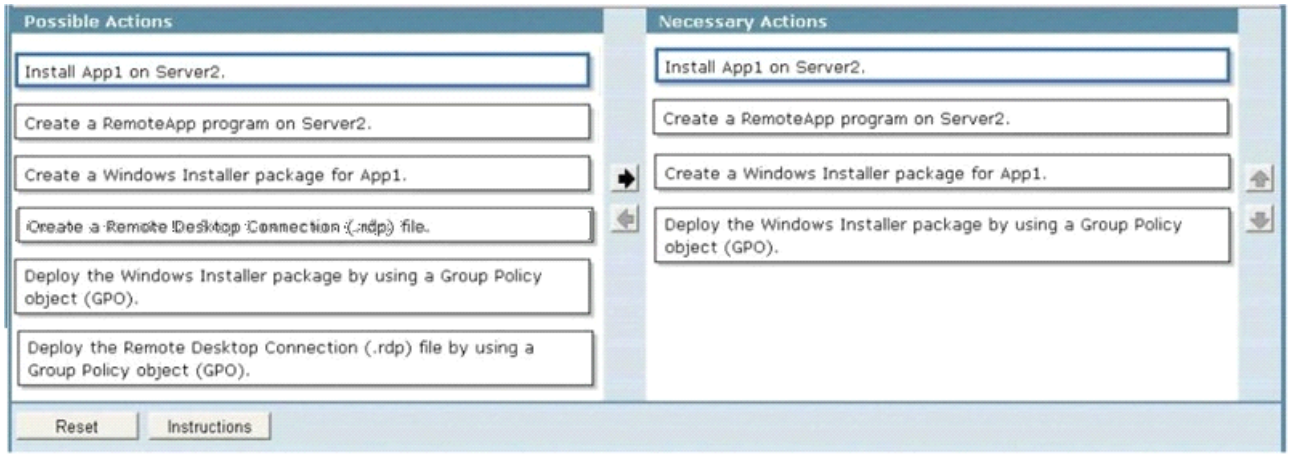
DRAG DROP
Your network contains three servers. The servers are configured as shown in the following table.

Server name	Server configuration
Server1	Windows Server 2008 R2 Enterprise (64-bit) Remote Desktop Web Access (RD Web Access)
Server2	Windows Server 2008 R2 Enterprise (64-bit) Remote Desktop Session Host (RD Session Host)
Computer1	Windows 7 Enterprise (32-bit)

All client computers run the 32-bit version of Windows 7. You have a 64-bit application named Appl. App1 is associated with the .kfa file extension. You need to ensure that when users open files that have the .kfa file extension, App1 automatically opens. What should you do? To answer, move the appropriate actions from the Possible Actions list to the Necessary Actions area and arrange them in the correct order.



Answer:



Question: 286

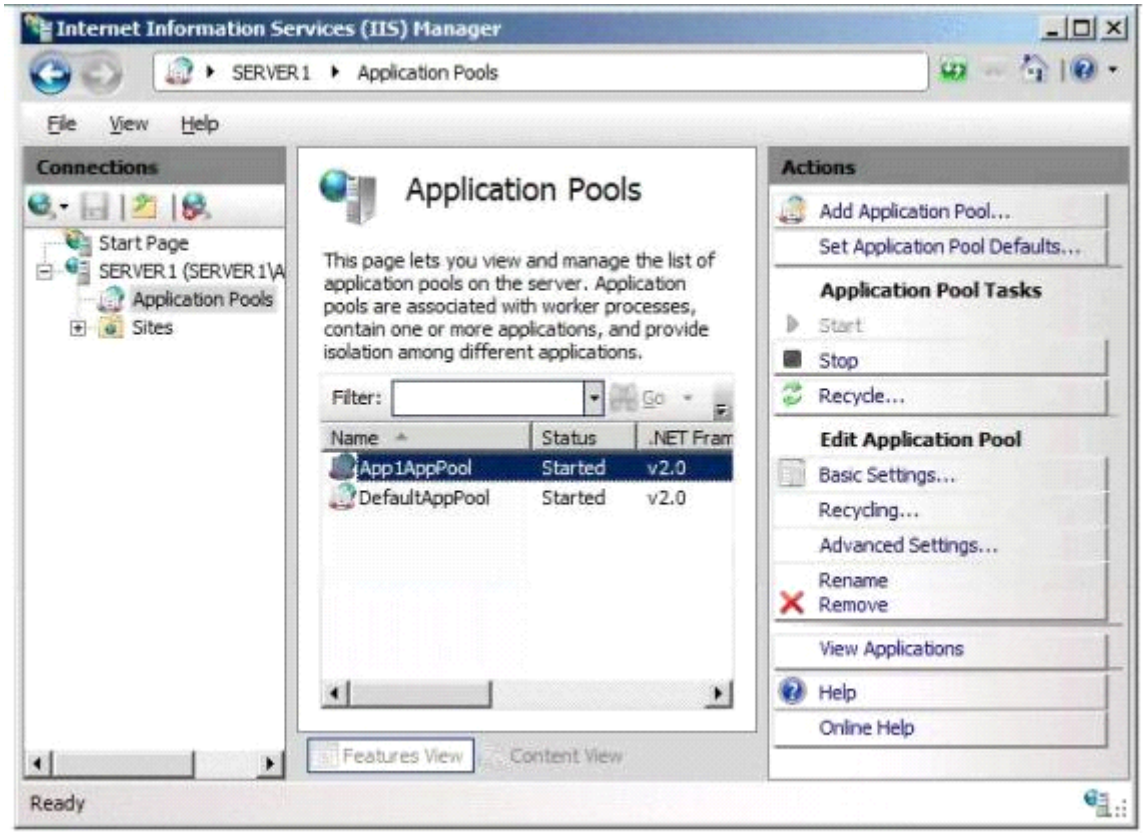
You need to create a RemoteApp and Desktop Connection configuration (.wcx) file. Which tool should you use?

A. Remote Desktop Gateway Manager
B. Remote Desktop Connection Manager
C. RemoteApp Manager
D. Remote Desktop Session Host Configuration

Answer: B

Question: 287
HOTSPOT

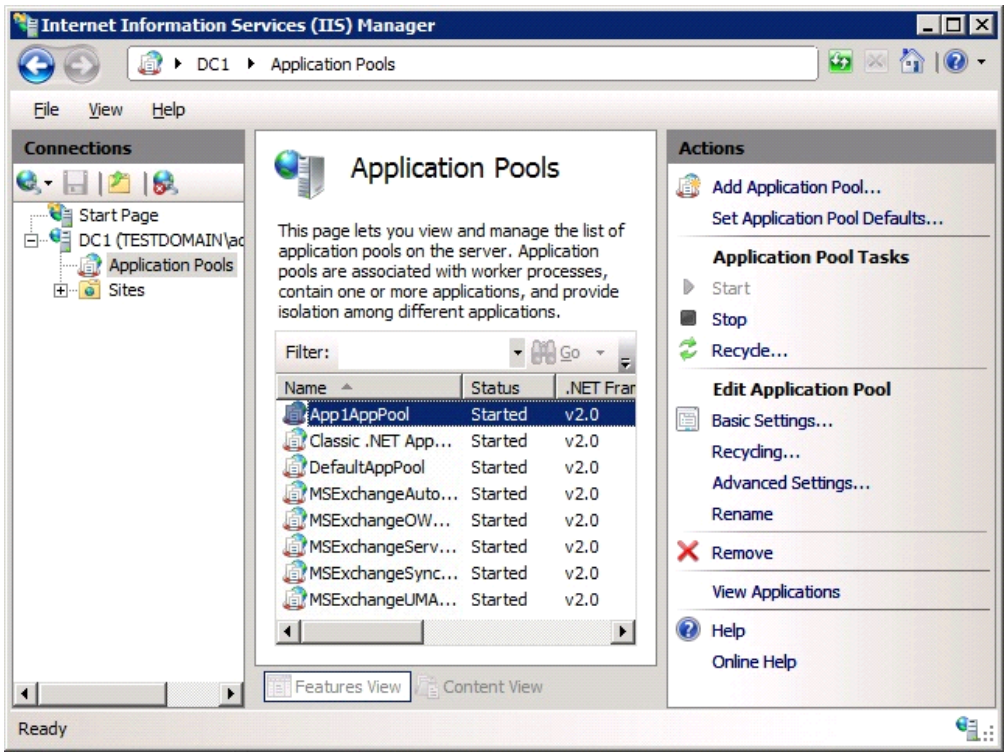
Your network contains a Web server named Served. Served has an application pool named ApplAppPool. You need to configure ApplAppPool to restart automatically when the application pool uses more than 100 MB of virtual memory. What should you do from Internet Information Services (IIS) Manager?

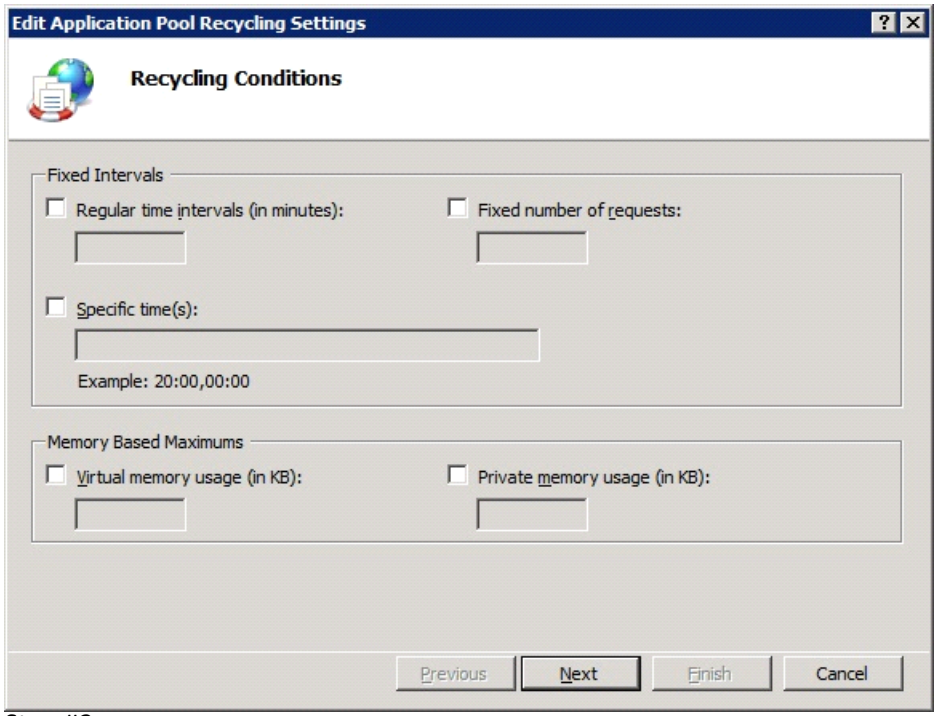


To answer, select the appropriate action in the answer area.

Answer:

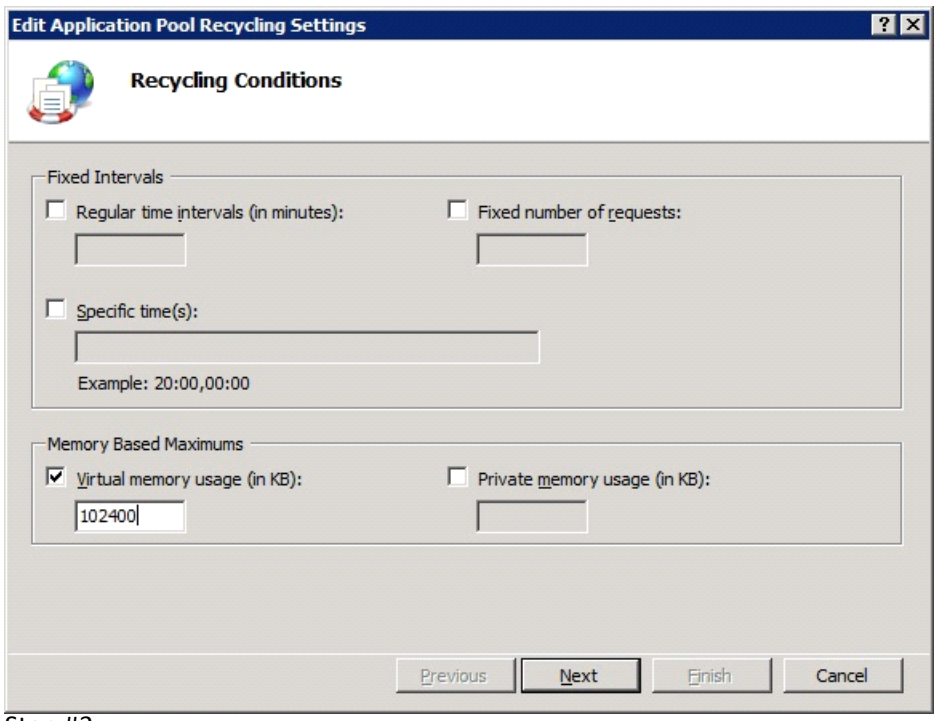
Step #1.
Click on the "Recycling" link in Actions pane to bring up the dialog box shown below.





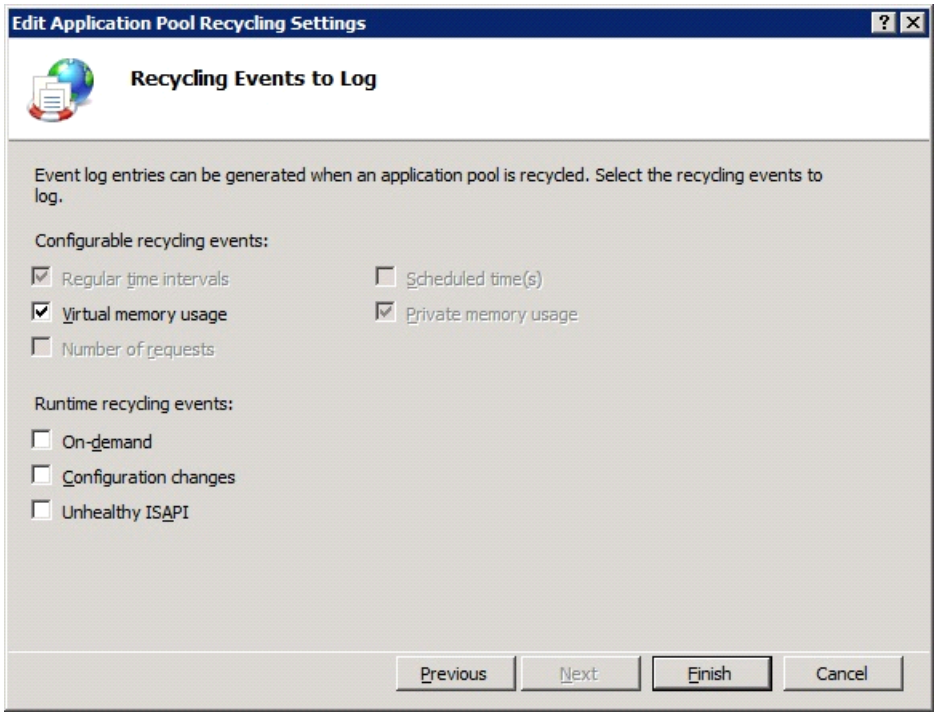
Step #2.

Select the Virtual Memory check box and enter 102400 then click Next. (102400KB = 100MB).



Step #3.

Leave the default selections and click Finish.



Question: 288

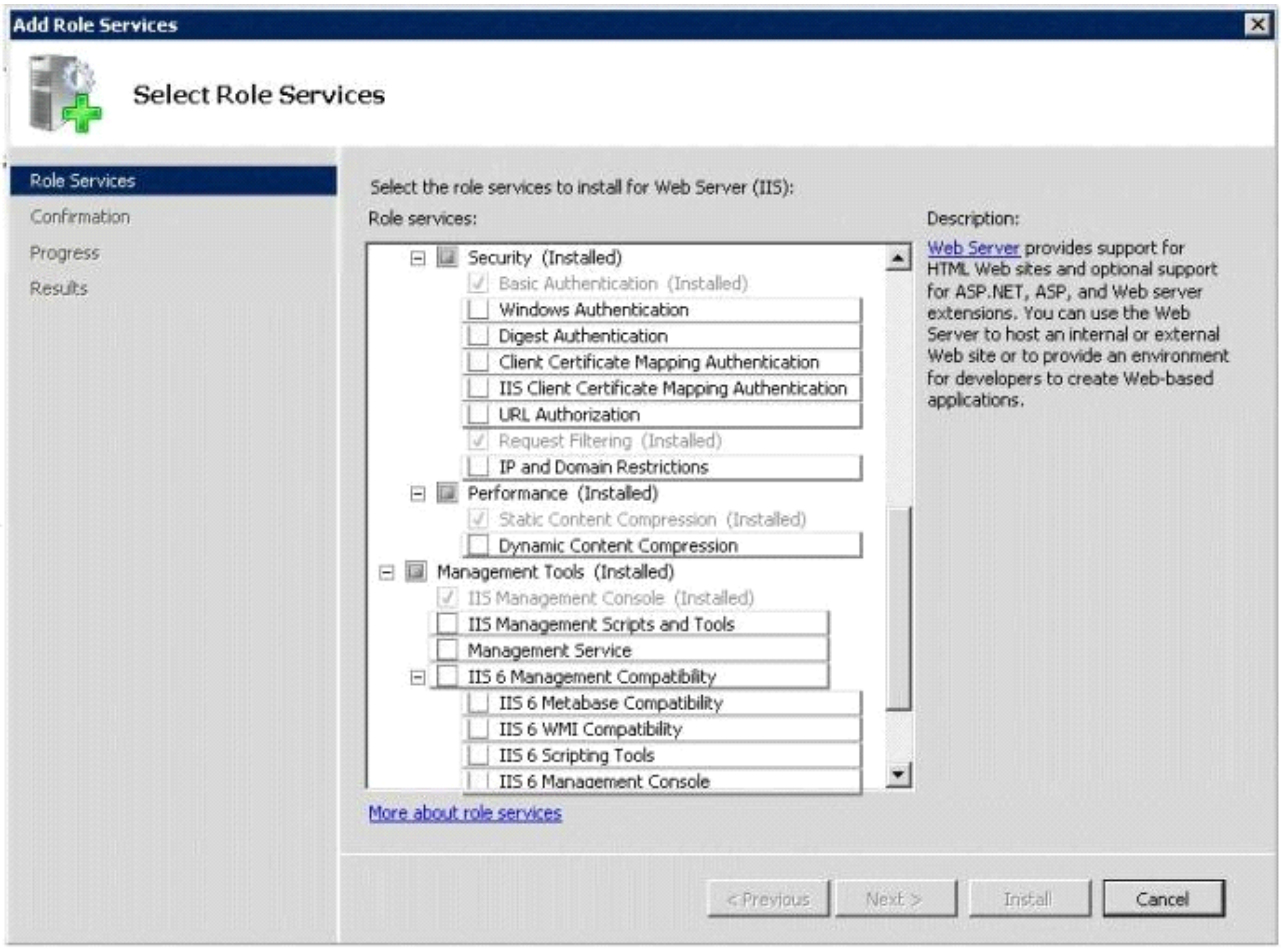
Your network contains a Web server named Web1. You install a server certificate on Web1, and then you create a new site named Site1. You need to ensure that users can access Site1 over HTTPS. Which settings should you modify?

A. HTTP Redirect
B. SSL Settings
C. Site Bindings
D. Handler Mappings

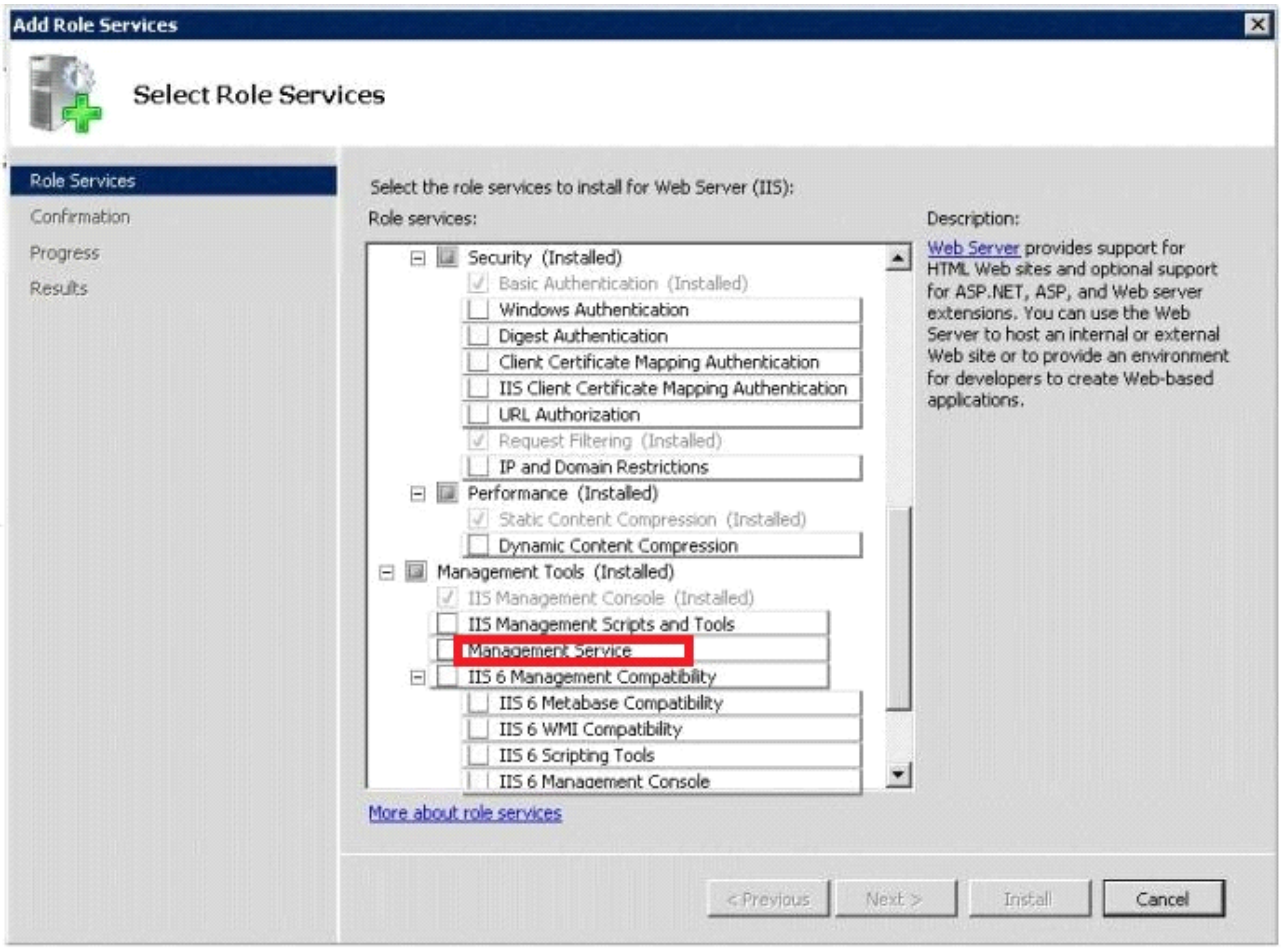
Answer: C

Question: 289
HOTSPOT

Your network contains two servers named Server1 and Server2 that have the Web Server (US) server role installed. You need to ensure that you can administer Server2 from Server1 by using Internet Information Services (IIS) Manager. The solution must minimize the number of role services installed on Server2. What should you install on Server2?
To answer, select the appropriate role service or role services from the Add Role Services dialog box in the answer area.


Add Role Services
Select Role Services
Role Services
Confirmation
Progress
Results
Select the role services to install for Web Server (IIS):
Role services:
Security (Installed)
Basic Authentication (Installed)
Windows Authentication
Digest Authentication
Client Certificate Mapping Authentication
IIS Client Certificate Mapping Authentication
URL Authorization
Request Filtering (Installed)
IP and Domain Restrictions
Performance (Installed)
Static Content Compression (Installed)
Dynamic Content Compression
Management Tools (Installed)
IIS Management Console (Installed)
IIS Management Scripts and Tools
Management Service
IIS 6 Management Compatibility
IIS 6 Metabase Compatibility
IIS 6 WMI Compatibility
IIS 6 Scripting Tools
IIS 6 Management Console
More about role services
Description:
Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
< Previous
Next >
Install
Cancel

Answer:



Question: 290

Your network contains an Active directory domain named fabrikam.com. The domain contains a Web server named Web1 that runs Windows Server 2008 R2. You install the SMTP Server feature on Web1. You need to create an SMTP virtual server on Web1. Which tool should you use?

A. Internet Information Services (IIS) Manager
B. System Configuration
C. Services
D. Internet Information Services (IIS) 6.0 Manager

Answer: D

Question: 291

Your network contains an Active Directory domain named contoso.com. The domain contains a member server named WDS1. You install the Windows Deployment Services (WDS) server role on WDS1. You have a reference computer named Server1 that runs windows Server 2008 R2. You need to capture an image of Server1 to WDS1. What should you do first?

A. Add a boot image to WDS1.
B. Add an install image to WDS1.
C. Start Server1 from the Windows 7 installation media.

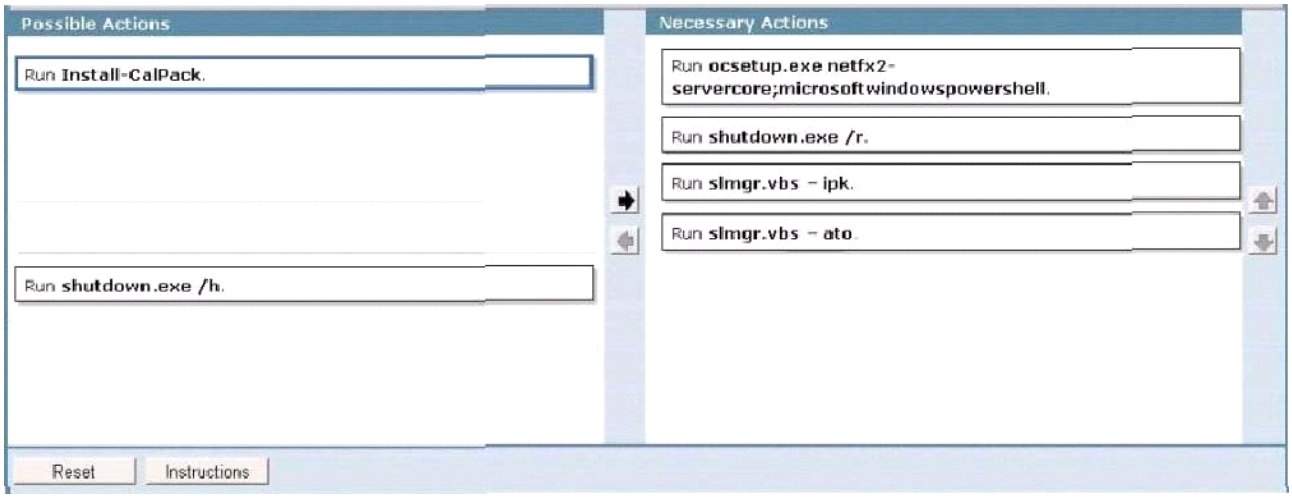
D. Add an image group to WDS1.

Answer: A

Question: 292

DRAG DROP
Your network uses Multiple Activation Key (MAX) licenses. A network technician performs a Server Core installation of Windows Server 2008 R2. Dunng the installation, the technician does not enter the license key. You need to activate Windows Server 2008 R2 on the server. What should you do?
To answer, move the appropriate actions from the Possible Actions list to the Necessary Actions area and arrange them in the correct order.

Answer:



Question: 293 DRAG DROP

Your network contains a Network Load Balancing (NLB) cluster named NLB01. NLB01 contains two servers named Server1 and Server2 that run Windows Server 2008 B2.
Server1 and Server2 are configured:

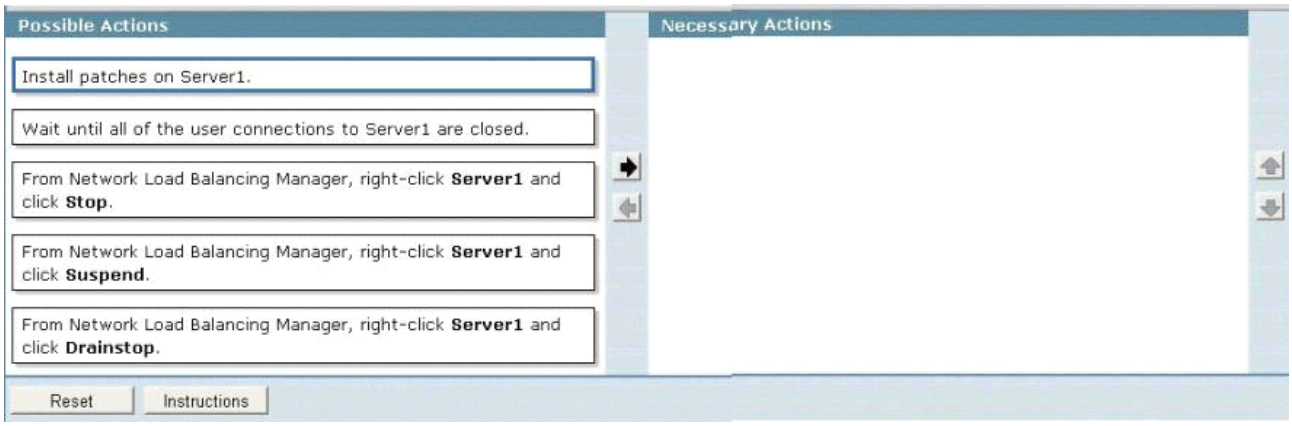
Server setting	Server configuration
Initial host state	Started
Retain suspended state after computer starts	Enabled

You need to install Windows updates on Server1 to meet the following requirements:

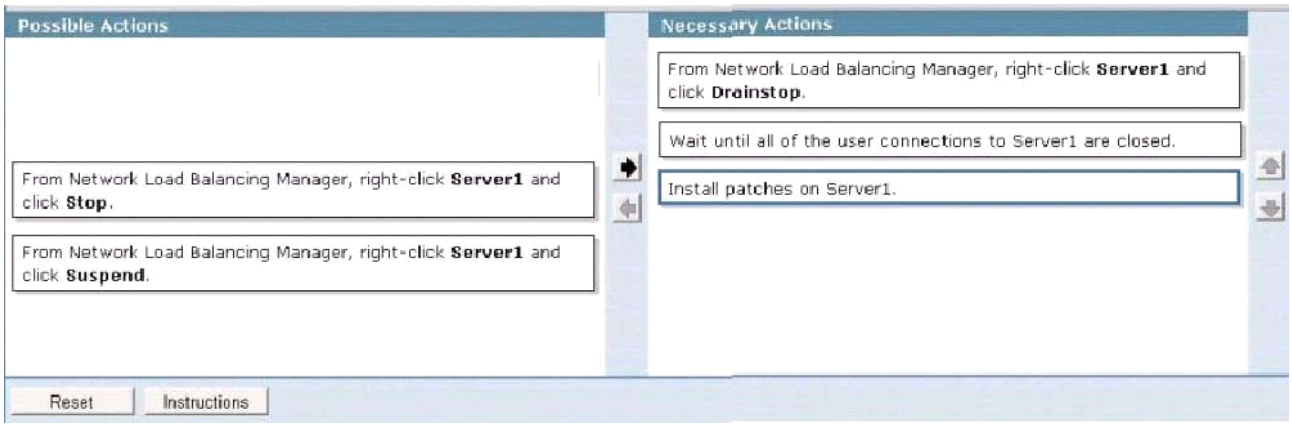
- Prevent new connections to Server1 while the updates are installed.
- Provide connected users with the ability to complete their session on server1 before the updates are installed.

What should you do?

To answer, move the appropriate actions from the Possible Actions list to the Necessary Actions area and arrange them in the correct order.

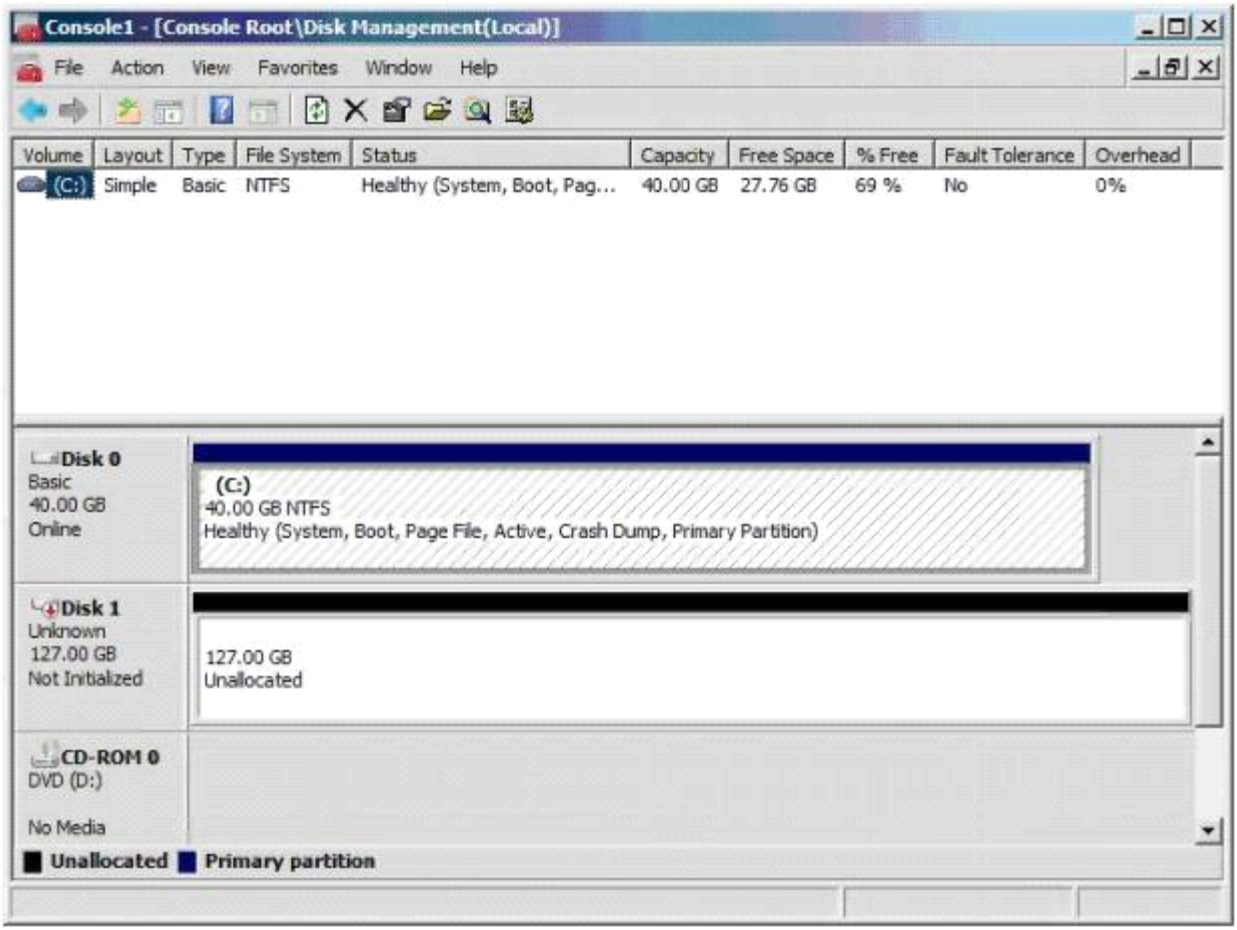


Answer:

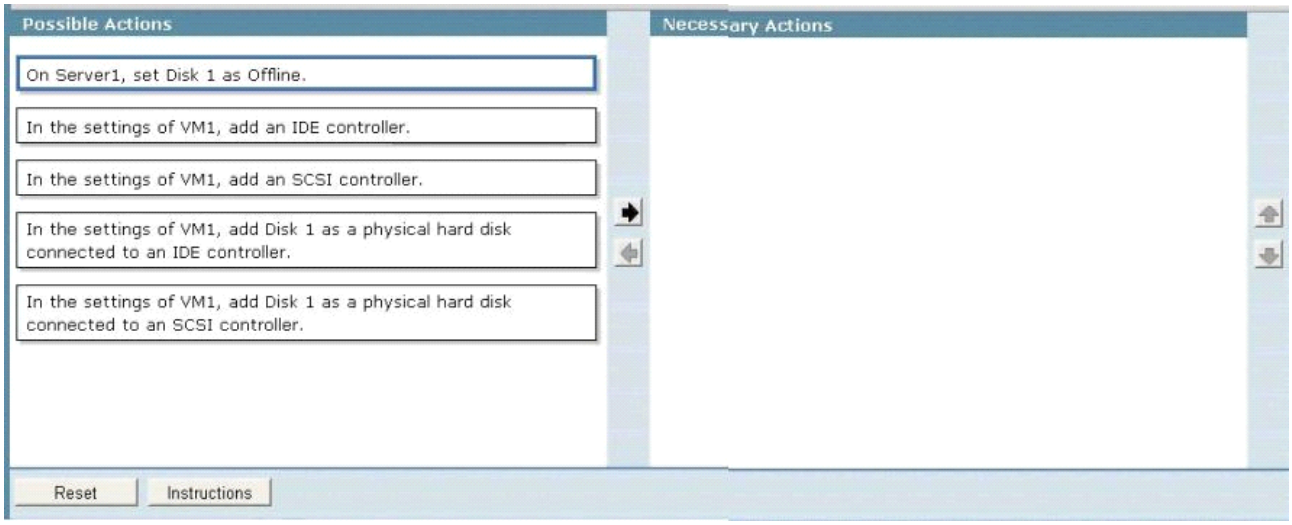


Question: 294 DRAG DROP

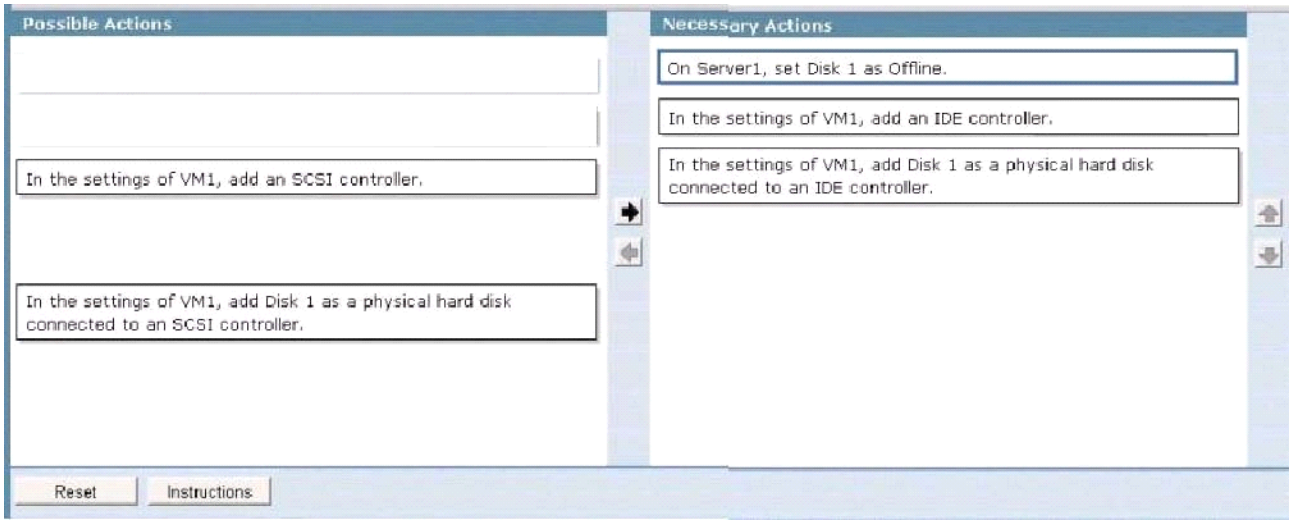
Your network contains a Hyper-V host named Server1 that runs Windows Server 2008 R2. The disks on Server1 are configured as shown in the exhibit. (Click the Exhibit button.)



You create a virtual machine (VM) named VM1. You deploy Windows Server 2008 R2 to VM1. You need to configure VM1 to use Disk l as a pass-through disk. The solution must minimize downtime on VM1. What should you do?
To answer, move the appropriate actions from the Possible Actions list to the Necessary Actions area and arrange them in the correct order.



Answer:



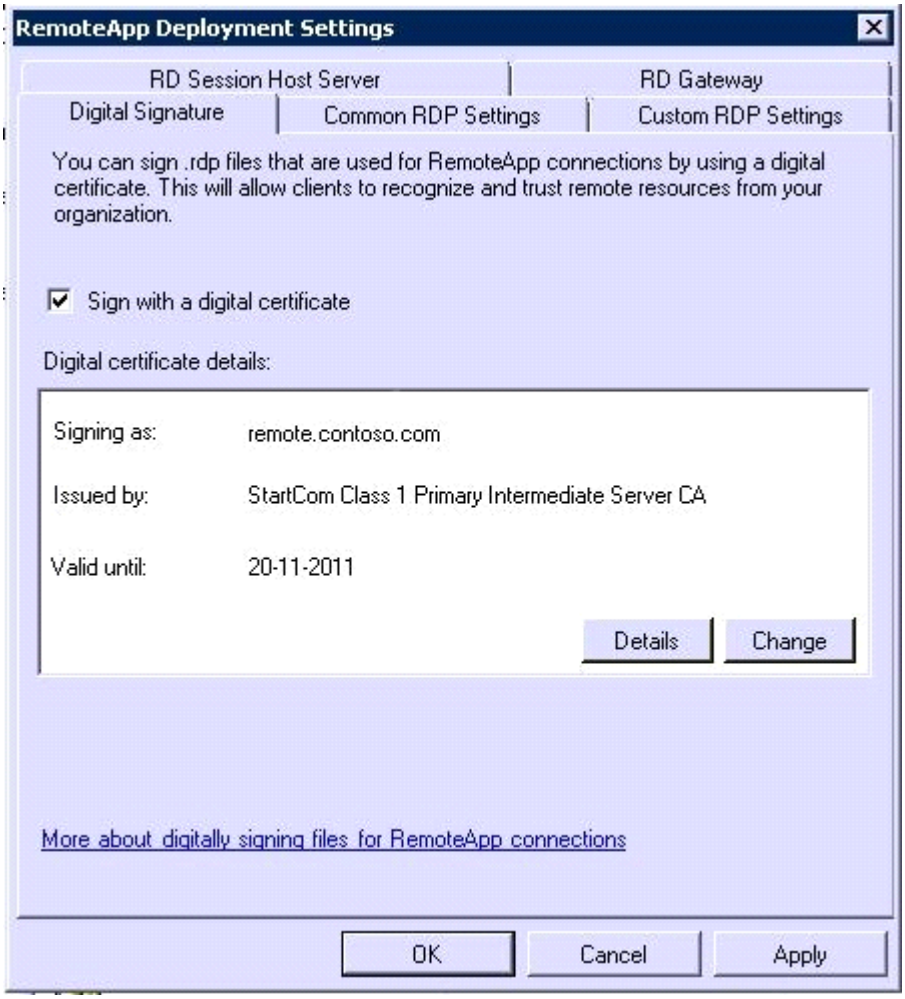
Question: 295

Your network contains an Active Directory domain. The domain contains a server that runs Windows Server 2008 R2. The server has the Remote Desktop Session Host (RD Session Host) role service and the Remote Desktop Web Access (RD Web Access) role service installed. When domain users run RemoteApp programs from the RD Web Access page, they are prompted for their credentials. You need to ensure that the domain users can run the RemoteApp programs without being prompted for their credentials. What should you do?

A. From RemoteApp Deployment Settings, configure the Digital Signature Settings.
B. On each client computer, add the URL of the RD Web Access Web site to the Trusted sites zone.
C. From RemoteApp Deployment Settings, configure the Common RDP Settings.
D. on each client computer, add the URL of the RD Web Access Web site to the Local intranet zone.

Answer: A

Explanation:



Question: 296

Your network contains four servers that run Windows Server 2008 R2. The servers are configured as shown in the following table:

Server name	Role service
Server1	Remote Desktop Web Access (RD Web Access)
Server2	Remote Desktop Session Host (RD Session Host)
Server3	Remote Desktop Session Host (RD Session Host)
Server4	Remote Desktop Connection Broker (RD Connection Broker)

Server2 and Server3 are configured as RemoteApp sources on Server4. You need to ensure that the RemoteApp programs are listed on the RD Web Access Web page on Server1. What should you do?

A. On Server4, add Server1 to the Session Broker Computers group.
B. On Server1, add Server4 to the TS Web Access Administrators group.
C. On Server4, add Server1 to the TS Web Access Computers group.
D. On Server1, add Server2 and Server3 to the TS Web Access Administrators group.

Answer: C

Question: 297

Your network contains an Active Directory domain named fabnkam.com. The domain contains a Web Server named Web1 that runs Windows Server 2008 R2. You create a new site named Site1. You need to ensure that when a user enters a URL on site1 for a resource that does not exist, a custom web page displays. Which feature should you configure?

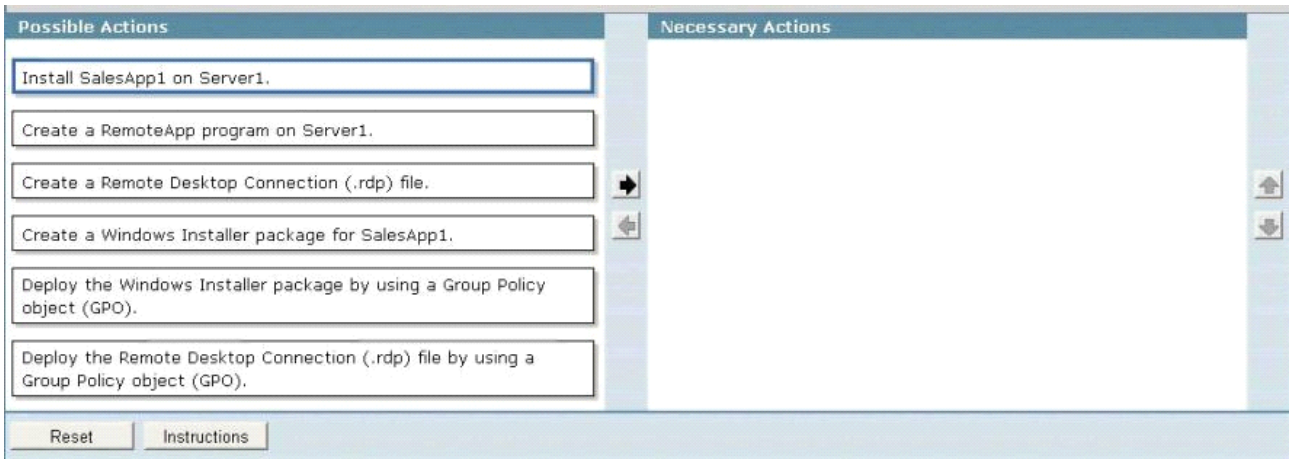
A. Default Document
B. Error Pages
C. HTTP Redirect
D. Authorization Rules

Answer: B

Server name	Server configuration
Server1	Windows Server 2008 R2 Enterprise (64-bit) Remote Desktop Session Host (RD Session Host)
Server2	Windows Server 2008 R2 Enterprise (64-bit) Remote Desktop Web Access (RD Web Access)

Question: 298

DRAG DROP
Your network contains two servers. The servers are configured as shown in the following table All client computers run the 32-bit version of Windows Vista. Your company purchases a new sales application named SalesAppl. SalesAppl is a 64-bit application. SalesAppl is associated with the .abc file I extension. You need to ensure that when users in the sales department open files that have the .abc file extension, SalesAppl automatically opens. What should you do?
To answer, move the appropriate actions from the Possible Actions list to the Necessary Actions area and arrange them in the correct order.

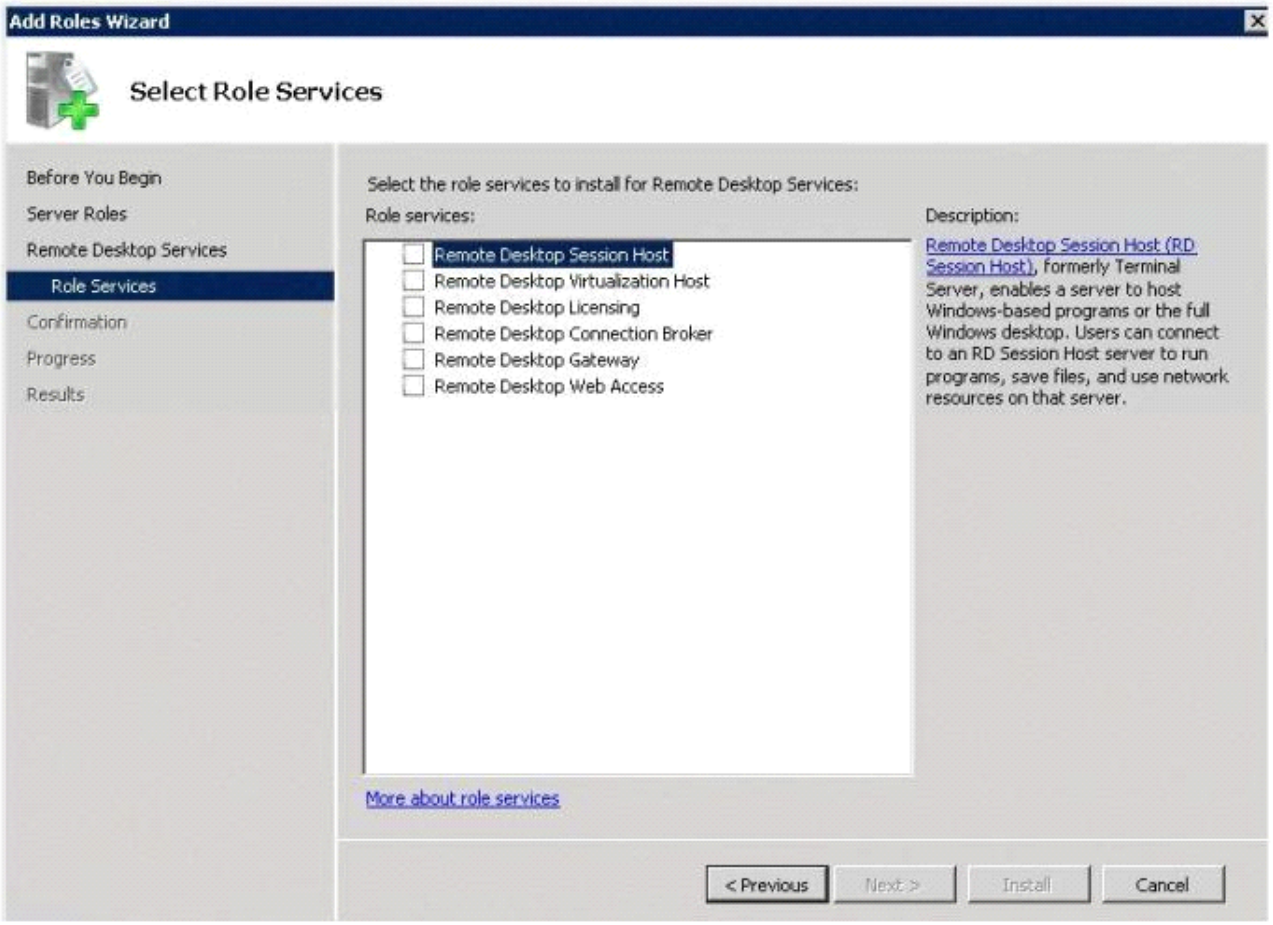


Answer:

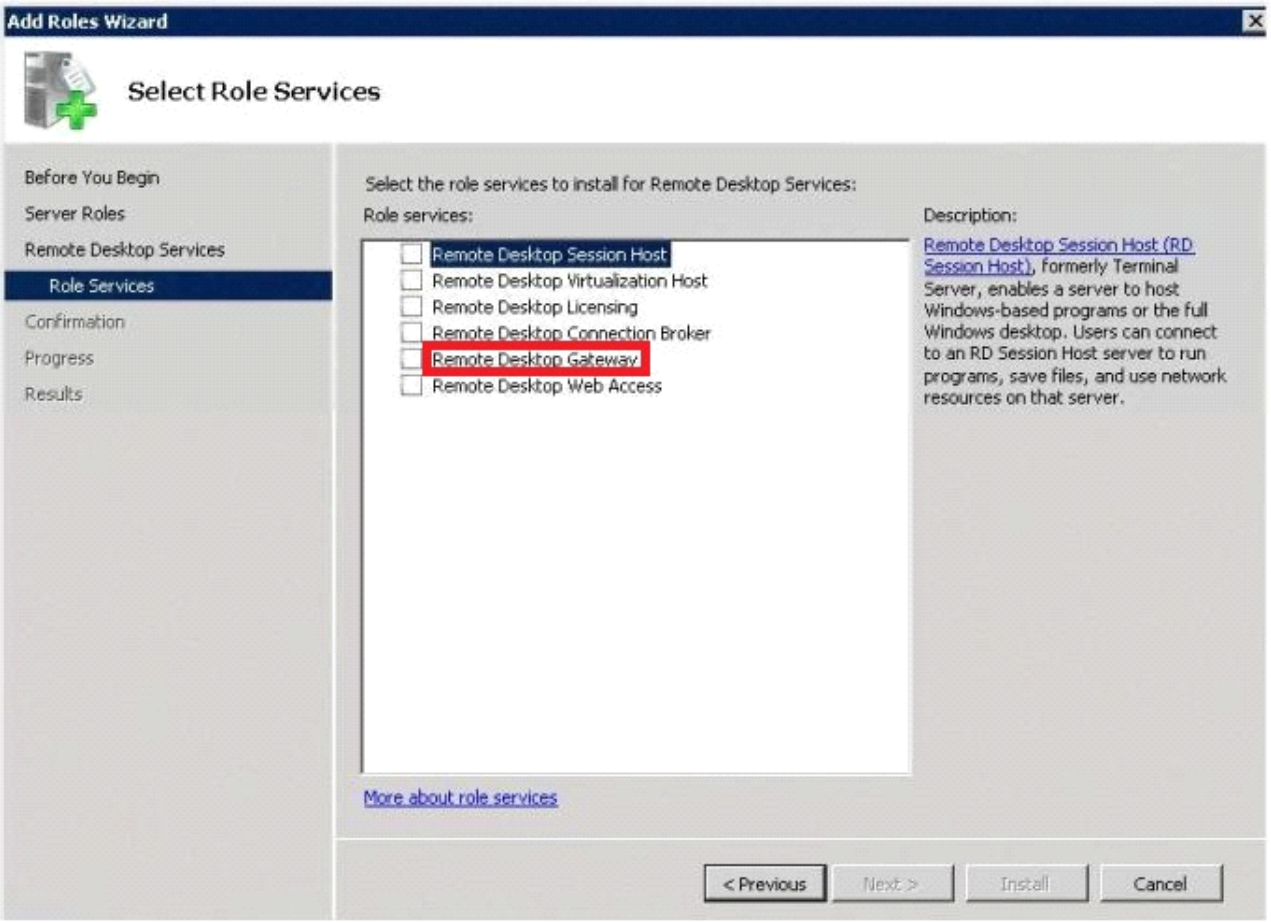
Install SalesApp1 on Server2
Create a RemoteApp program on Server2
Create a Windows Installer package for SalesApp1
Deploy the Windows Installer package by using a Group Policy object (GPO)

Question: 299
HOTSPOT

Your network contains three servers named Server1, Server2, and Server3. Server1 and Server2 are accessible from the internal network only. Server3 is located on a perimeter network. Users connect to Server1 and Server2 to run RemoteApp programs. You need to ensure that remote users can run the RemoteApp programs on Server1 and Server. The solution must minimize the number of ports that must be opened on the internal firewall. Which role service or role services from the Add Roles Wizard should you install on Server3? To answer, select the appropriate role service or role services in the answer area. Select only the required role service or role services.

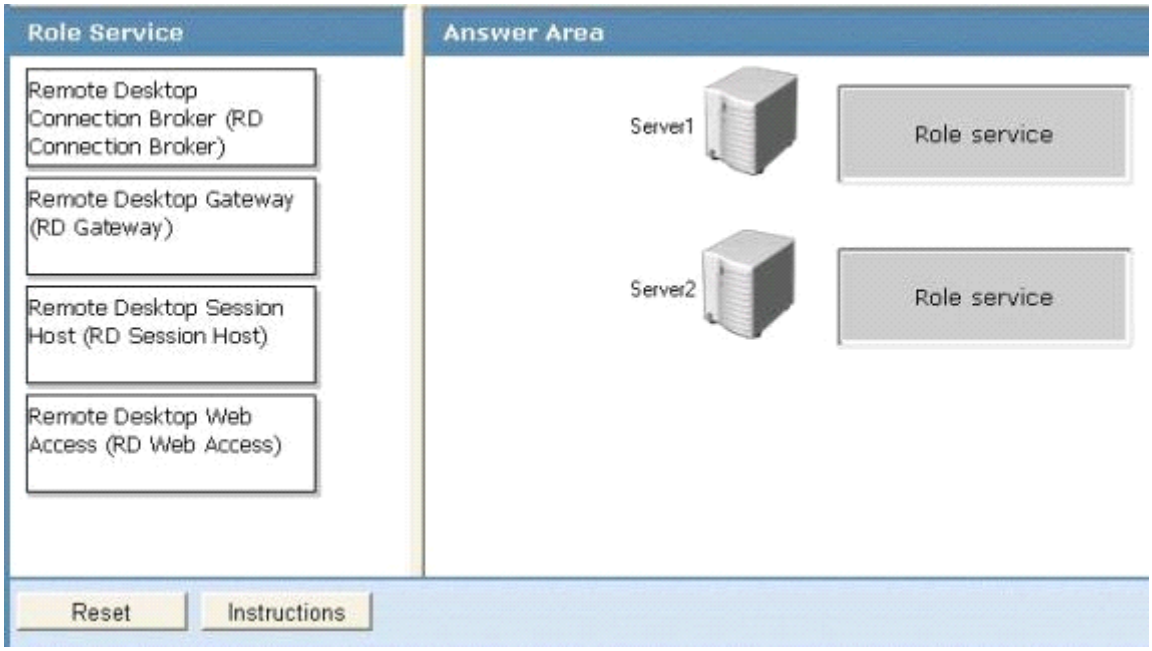


Answer:

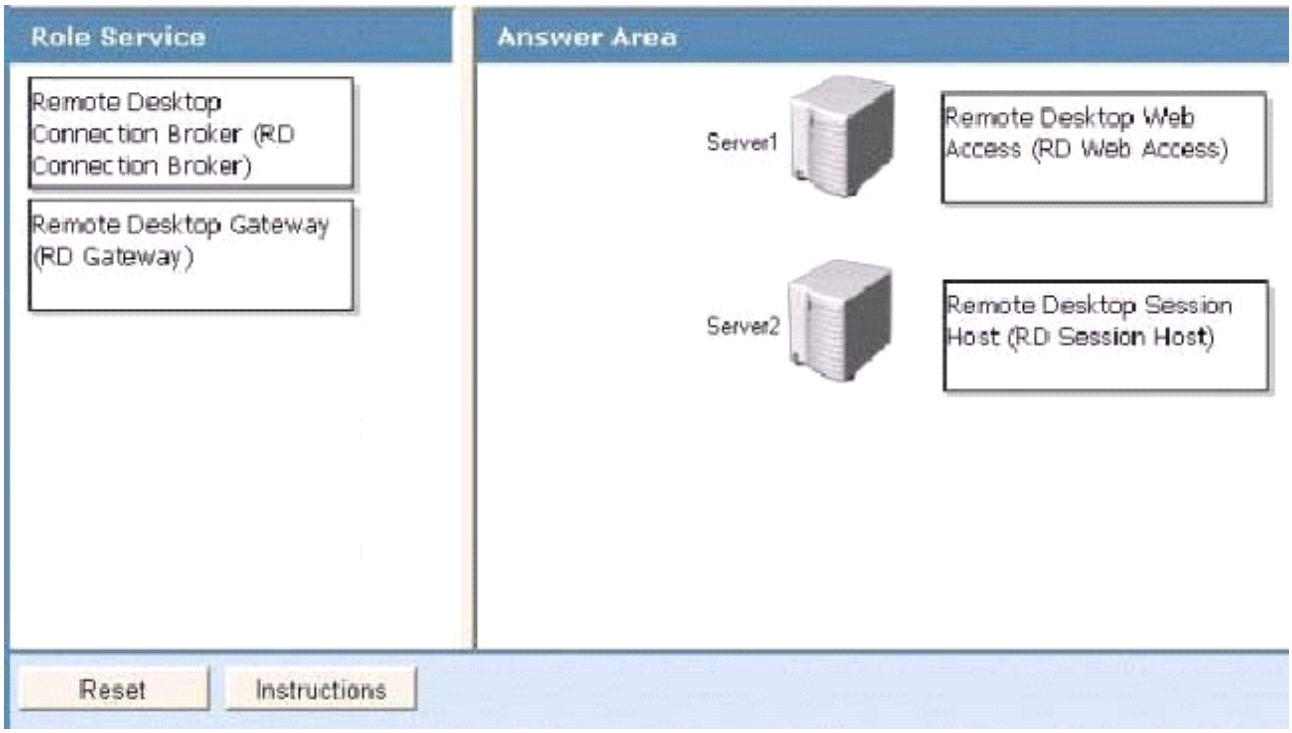


Question: 300

DRAG DROP
Your network contains two servers named Server1 and Server2 that run Windows Server 2008 R2. You plan to publish a RemoteApp program named App1 to Server2. You need to ensure that App1 appears as a RemoteApp program when you connect to https://serverl/rdweb. Which role services should you install on Server1 and Server2?
To answer, drag the appropriate role service to the correct server in the answer area.



Answer:



Question: 301

Your network contains a Web server named Server1 that runs Windows Server 2008 R2. The network contains two subnets named Subnet1 and Subnet2. Server1 contains a Web site named Site1. You need to prevent Server1 from responding to requests that originate from subnet2. Which feature should you configure from Internet Information Services (IIS) Manager?

A. Default Document
B. Authorization Rules

C. Feature Delegation
D. ISAPI and CGI Restrictions
E. Connection strings
F. HTTP Response Headers
G. Error Pages
H. IP Address and Domain Restrictions
I. Management Service
J. Request Filtering
K. Worker Processes
L. SSL Settings
M. ISAPI Filters
N. Authentication
O. HTTP Redirect
P. IIS Manager Permissions

Answer: H

Question: 302

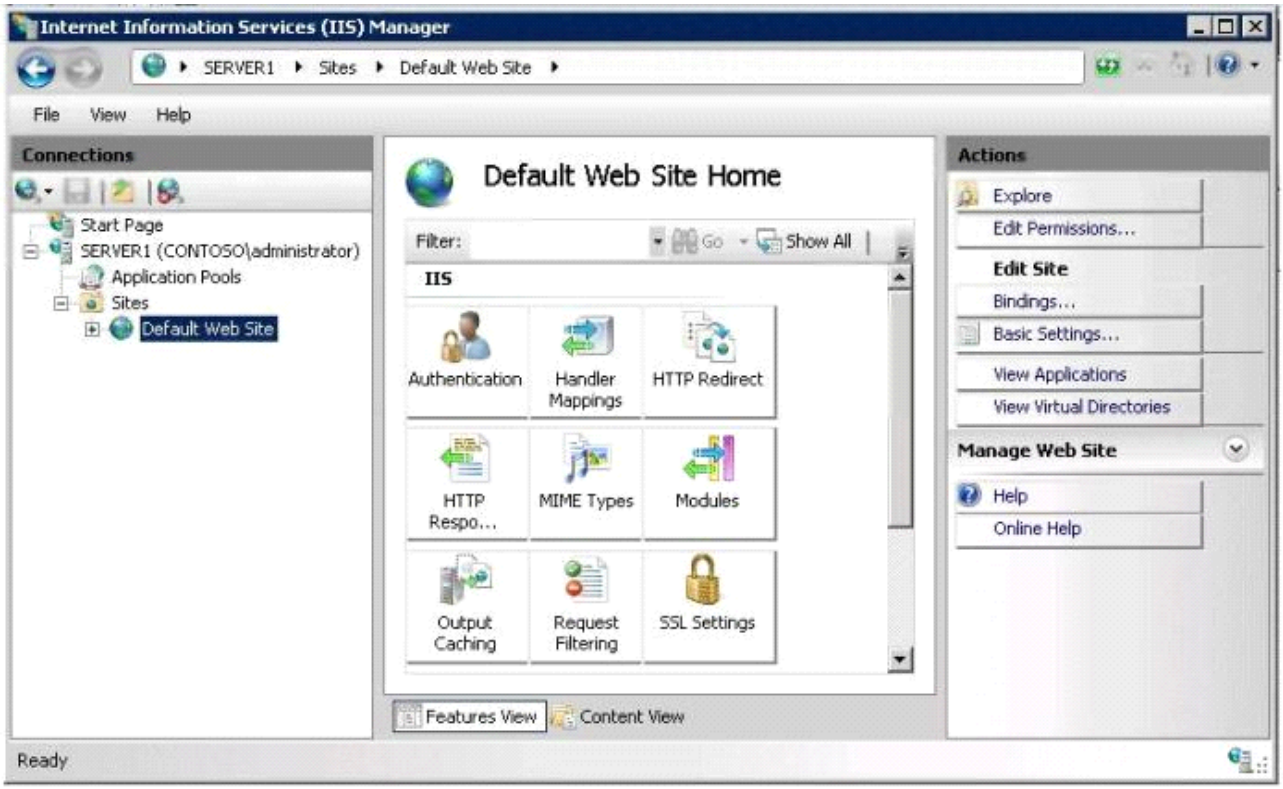
Your network contains a Web server that runs Windows Server 2008 R2. You need to log all of the configuration changes made from Internet Information Services (IIS) Manager. Which tool should you use?

A. Performance Monitor
B. Appcmd
C. Event viewer
D. Netsh

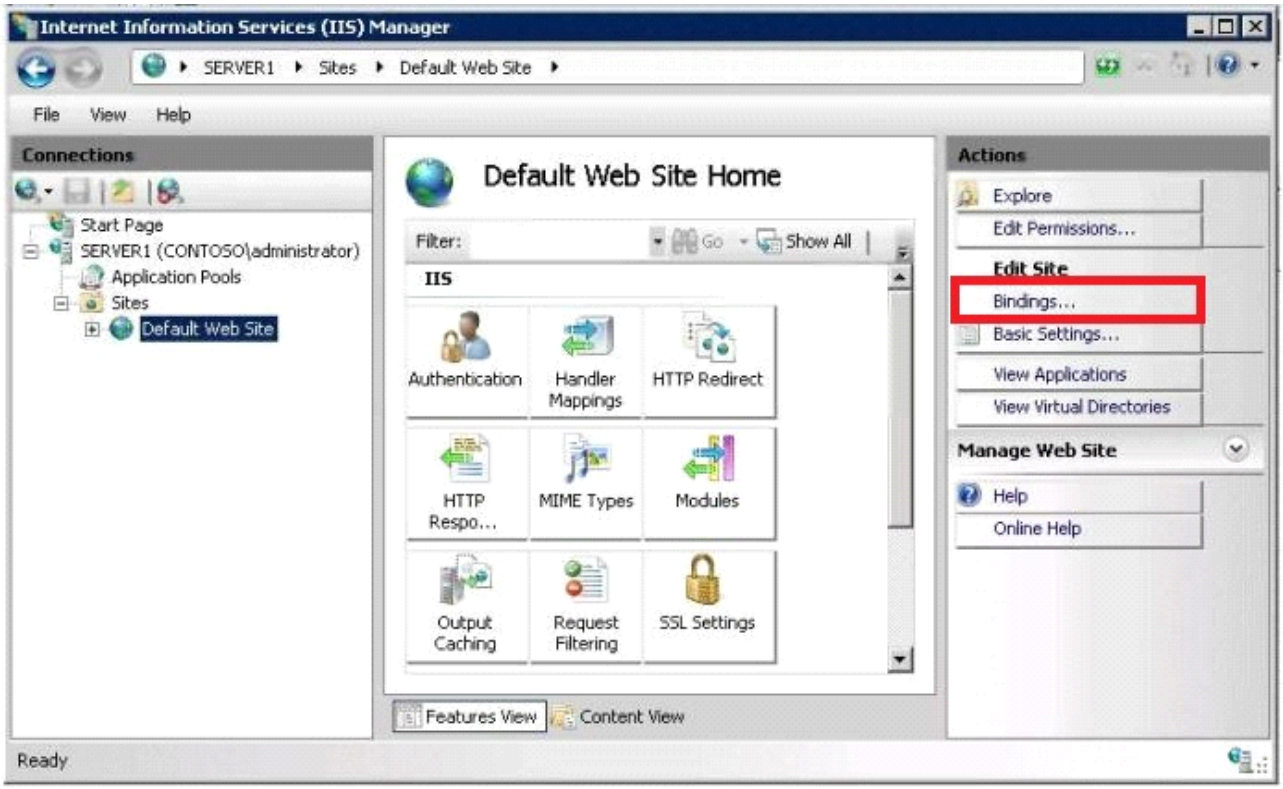
Answer: B

Question: 303
HOTSPOT

Your network contains a Web server named Server1. You install a server certificate on Server1. You need to ensure that users can access the default Web site over HTTPS. What should you configure from Internet Information Services (IIS) Manager? To answer, select the appropriate component or action in the answer area.

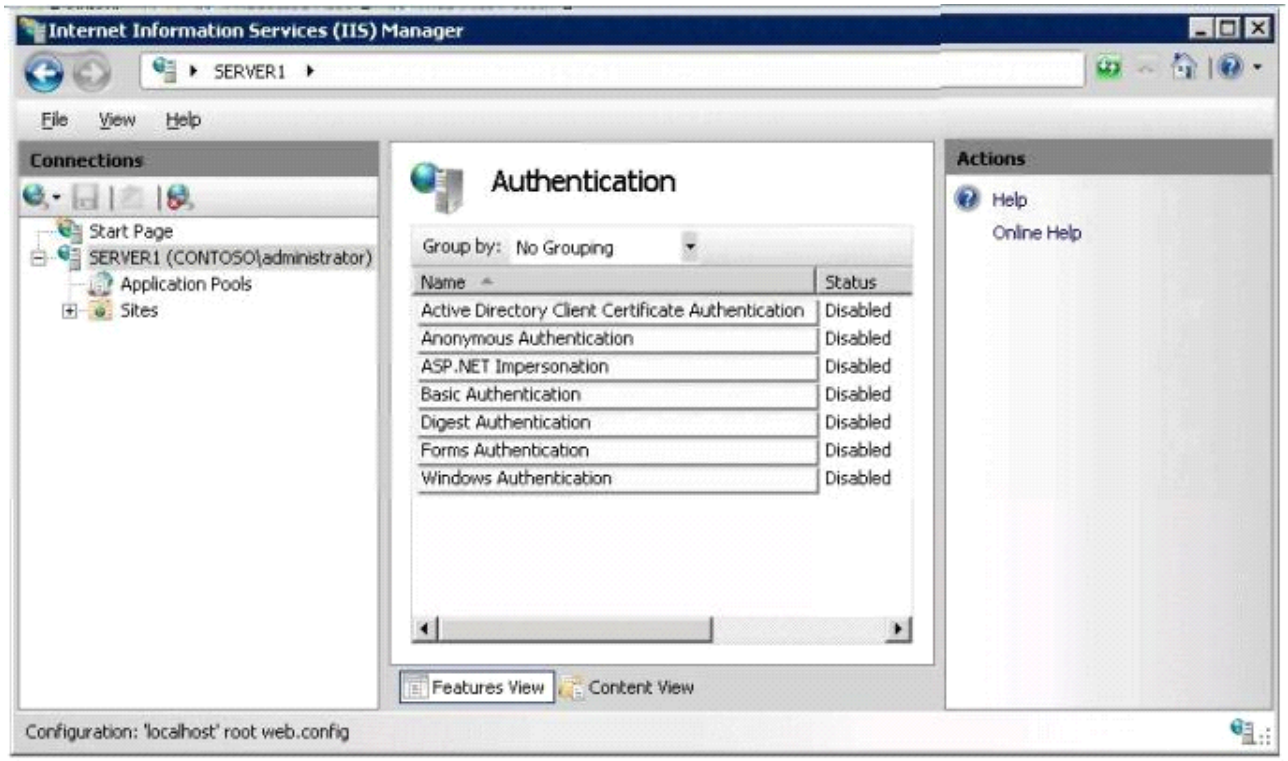


Answer:

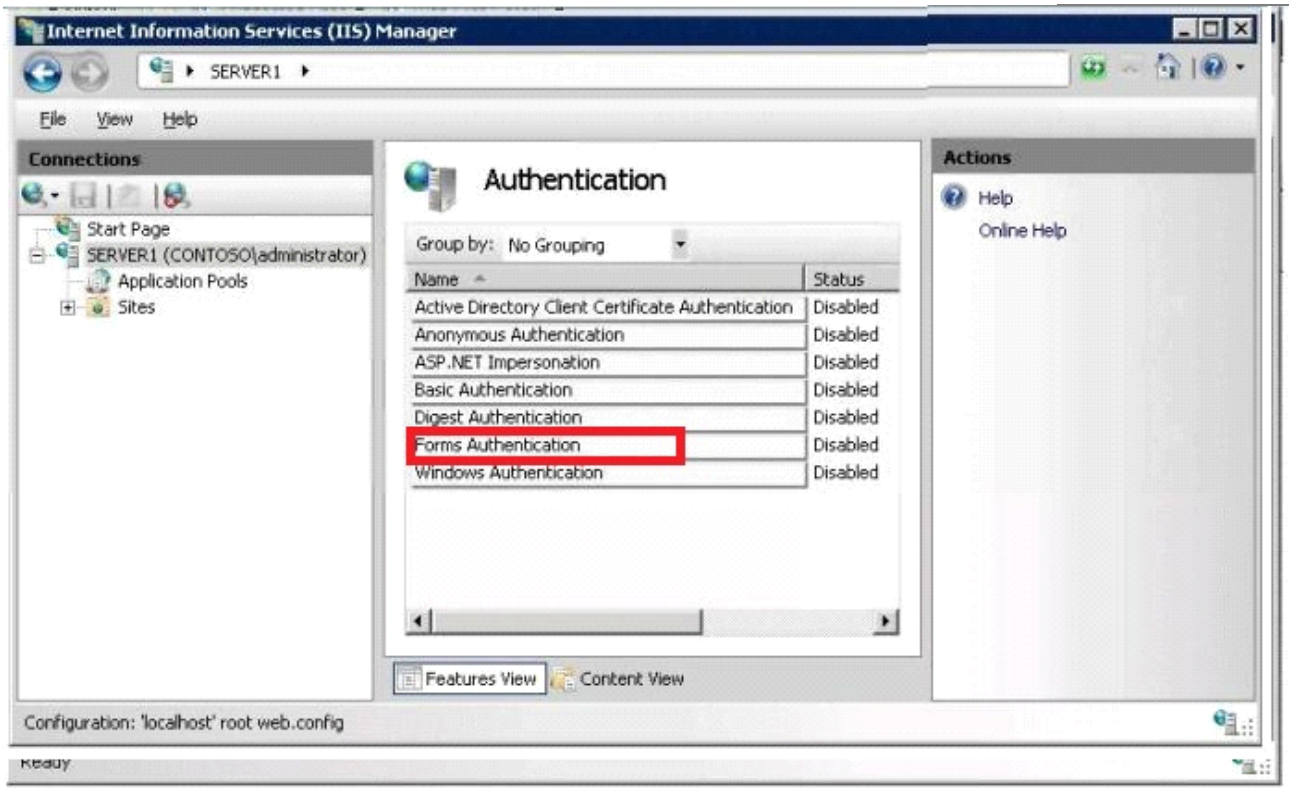


Question: 304
HOTSPOT

Your network contains a Web server named Server1. You need to ensure that Server1 authenticates users by using a custom Web page. Which authentication method should you enable from (IIS) Manager? To answer, select the appropriate authentication method in the answer area.



Answer:

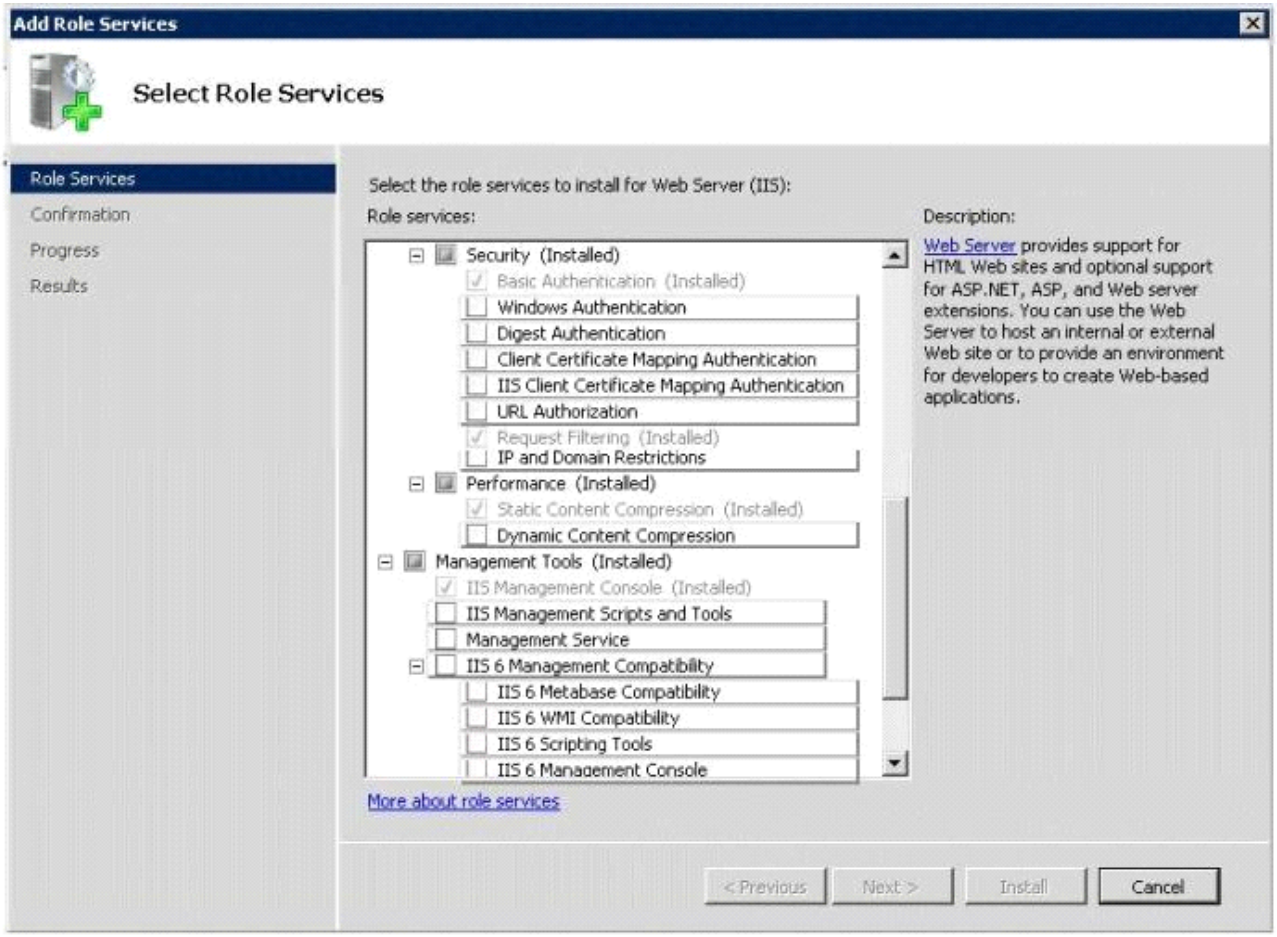


Question: 305

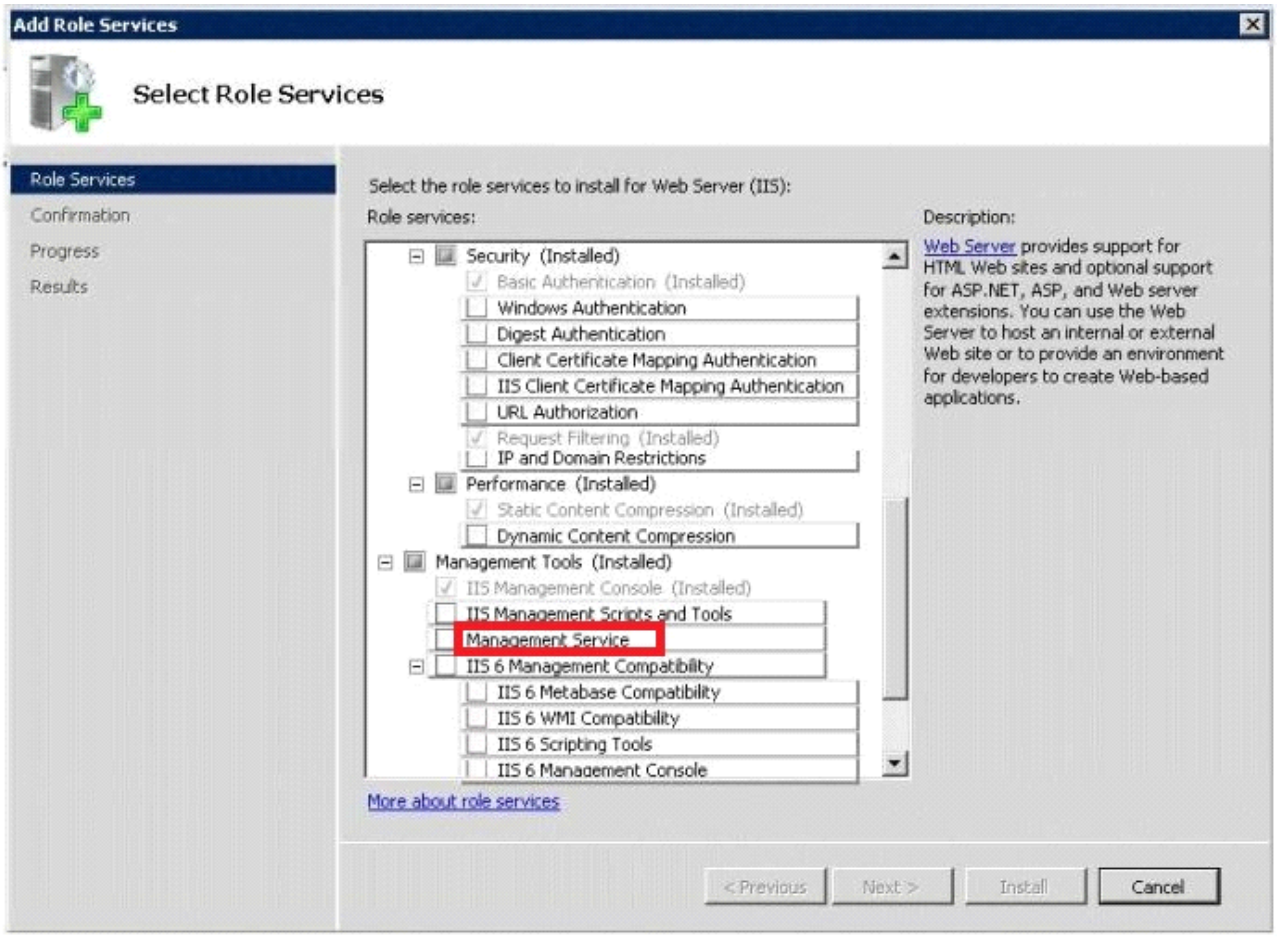
HOTSPOT

Your network contains a server named Server1 that has the web Server (HS) server role installed. The network contains a computer named Computer1 that runs Windows 7. Computer1 has the Remote Server Administration Tools (RSAT) installed. You need to ensure that you can administer Server1 from Computer1 by using Internet Information Services (IIS) Manager. The solution must minimize the number of role services installed on Server1. What should you install on Server1?

To answer, select the appropriate role service or role services from the Add Role Services dialog box in the answer area.



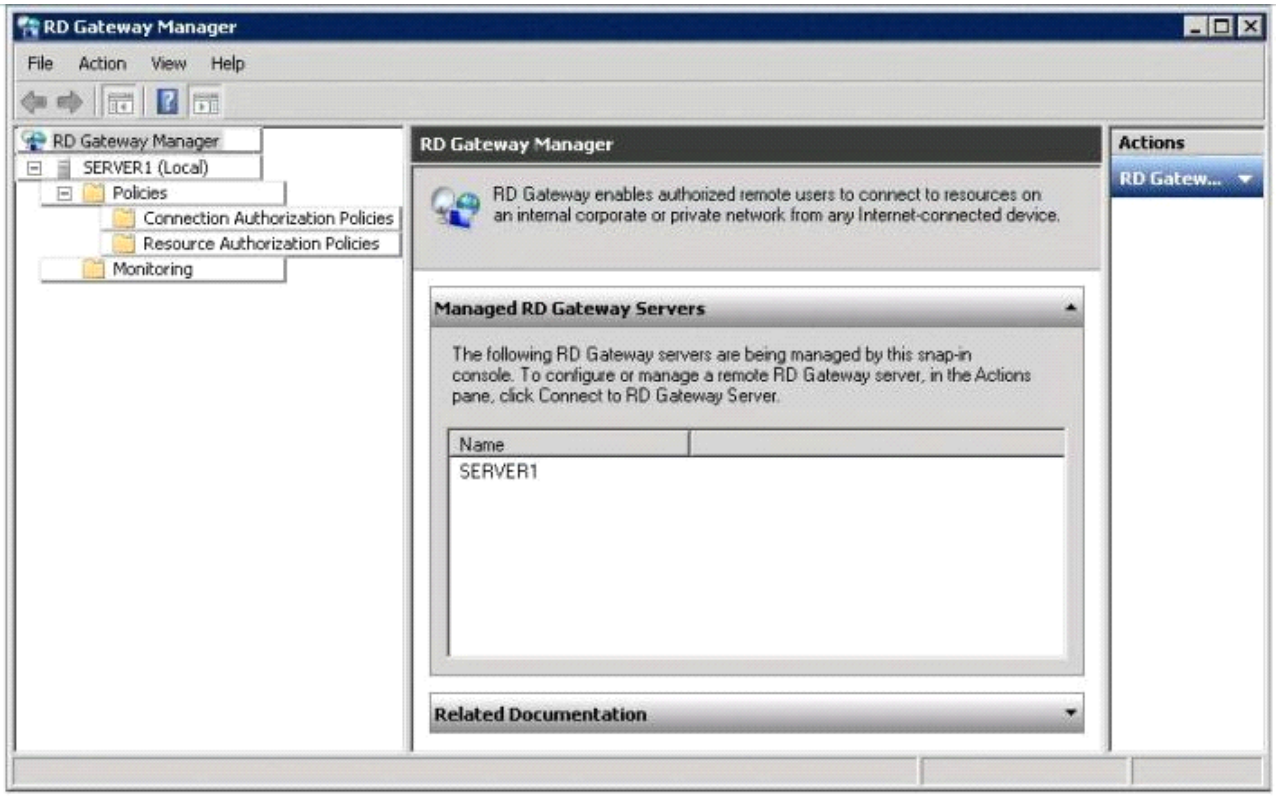
Answer:



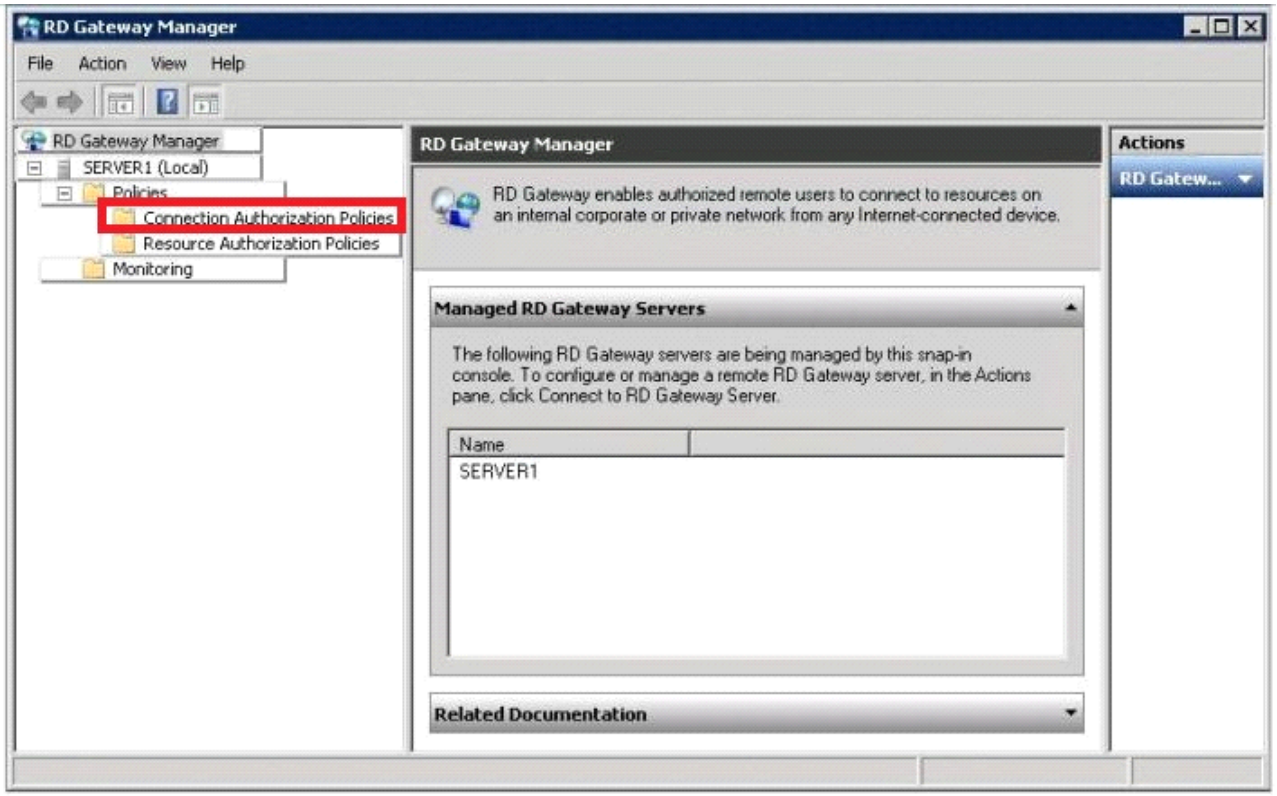
Question: 306
HOTSPOT

Server name	Role service
Server1	Remote Desktop Gateway (RD Gateway)
Server2	Remote Desktop Session Host (RD Sessions Host)
Server3	Network Policy Server (NPS)

Your network contains three servers. The servers are configured as shown in the following table. You need to configure Server1 to use Network Access Protection (NAP) for all client connections. Which node from RD Gateway Manager should you use to make this configuration? To answer, select the appropriate node in the answer area.



Answer:



Question: 307

Your network uses Multiple Activation Key (MAK) licenses. You perform a Server Core installation of Windows Server 2008 R2. During the installation, you enter the license key. You need to activate Windows Server 2008 R2 on the

server. Which command should you run?

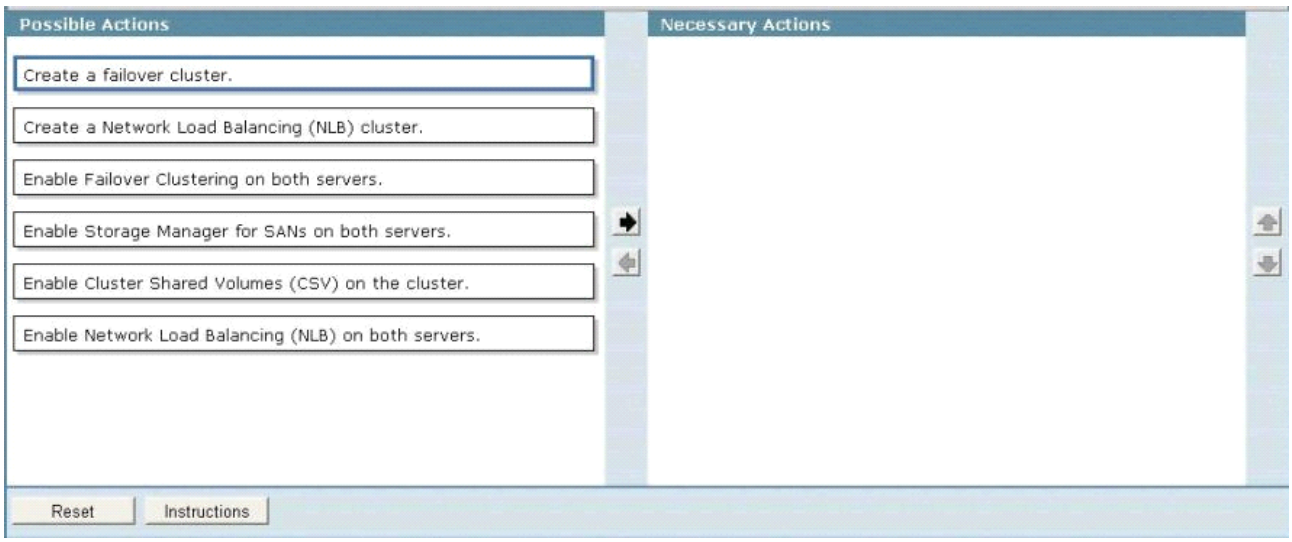
A. slmgr.vbs -ipk
B. install-callpack
C. ocsetup.exe was-windowsactivationservice
D. slmagr.vbs -ato

Answer: D

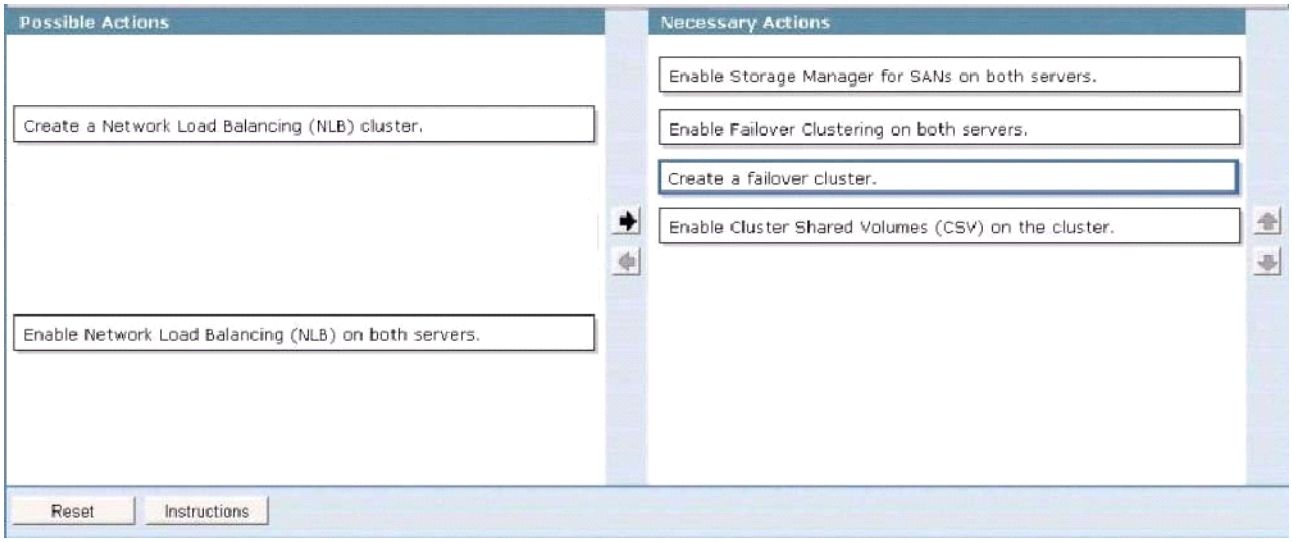
Explanation:
(If you already entered the product key during Windows Setup, you can skip this first step.)
Then, type the following command to perform the actual activation:
slmgr –ato
You can also use Slmgr command to activate a remote installation. For more information, type slmgr at a command prompt.

Question: 308

DRAG DROP
Your network contains two servers named Server1 and Server2. Server1 and Server2 run Windows Server 2008 R2 Enterprise and have the Hyper-V server role installed. You need to deploy a Hyper-V host cluster. The solution must ensure that if one of the hosts is disconnected from the shared storage device, all of the virtual machines (VMs) running on the host will continue to run. What should you do?
To answer, move the appropriate actions from the Possible Actions list to the Necessary Actions area and arrange them in the correct order.

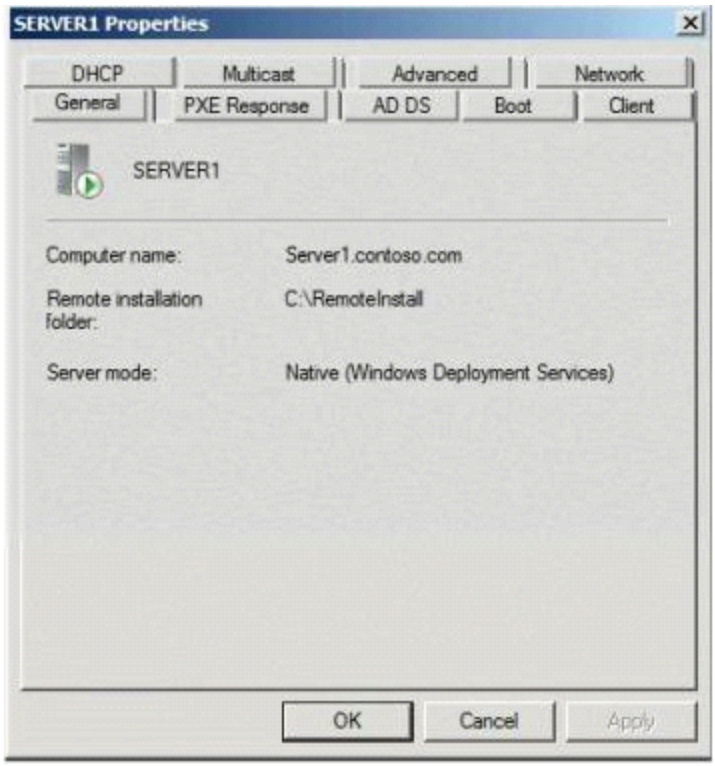


Answer:



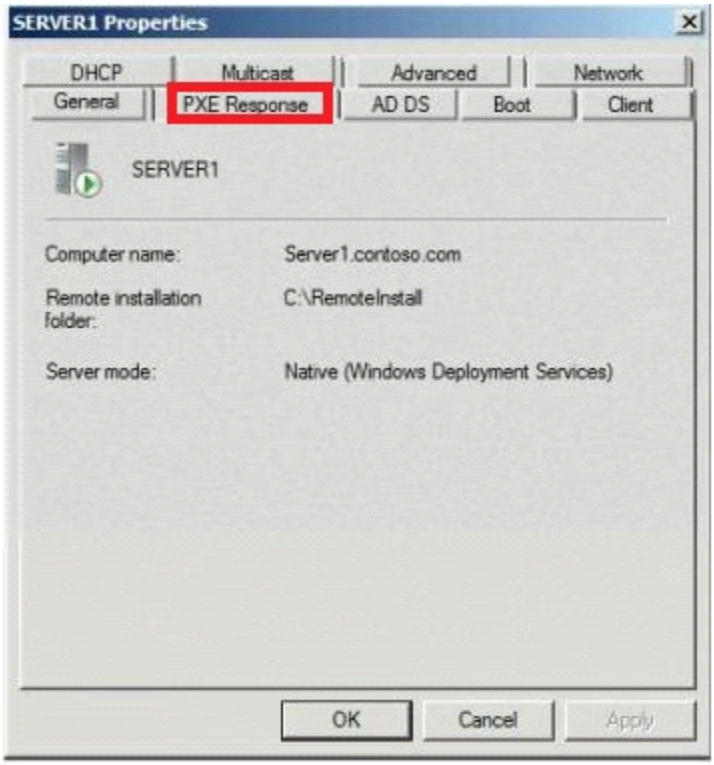
Question: 309
HOTSPOT

Your network contains an Active Directory domain. The domain contains a member server named Server1. Server1 has the windows Deployment Services (WDS) server role installed. You need to ensure that only approved client computers receive a boot image from Server1. Which tab should you select from the Server1 Properties dialog box to make the configuration?



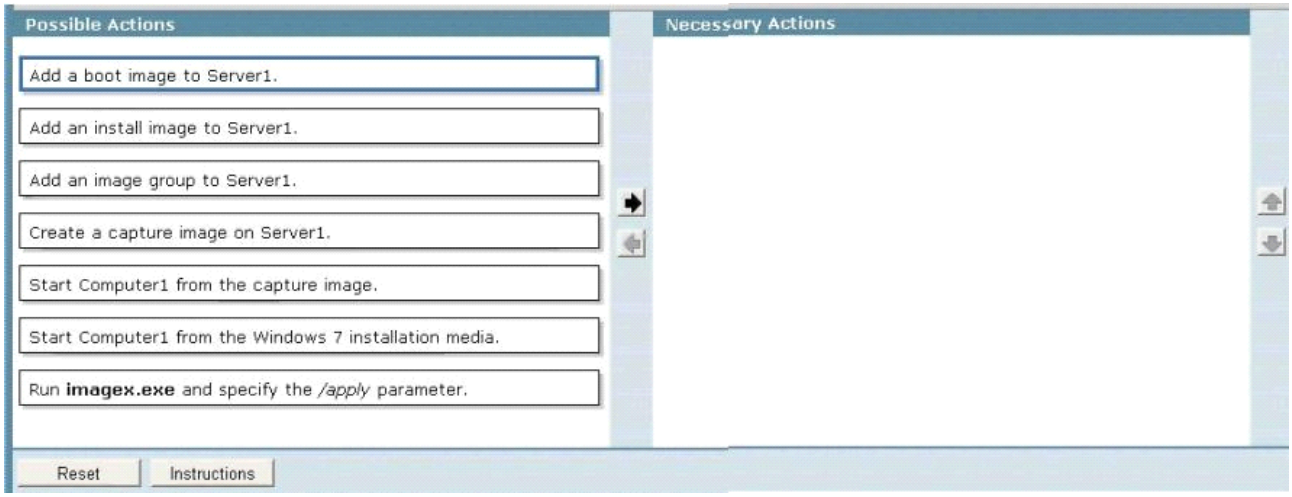
To answer, select the appropriate tab in the answer area.

Answer:

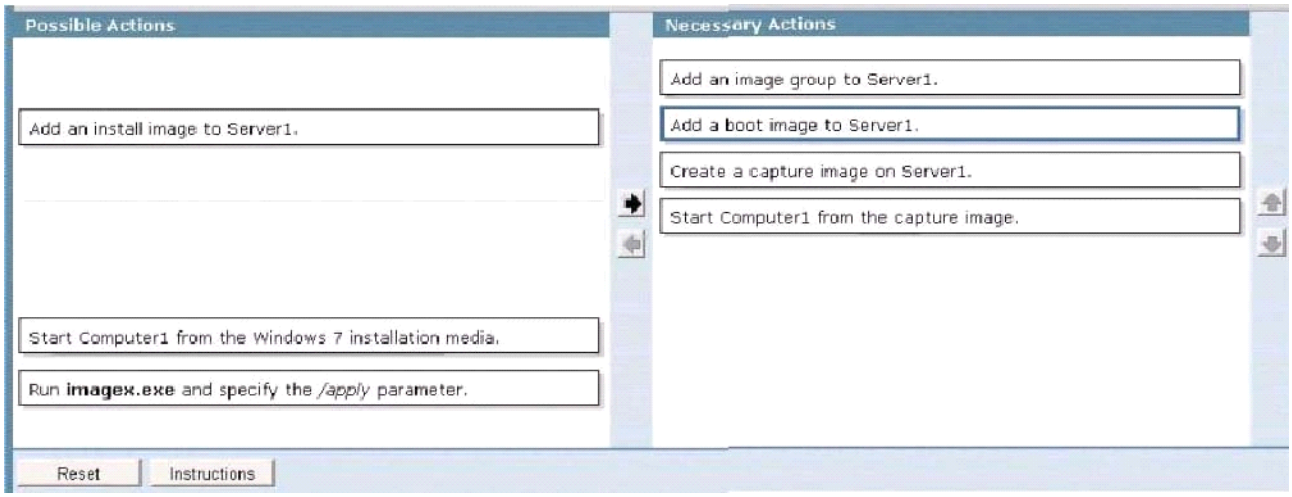


Question: 310 DRAG DROP

Your network contains an Active Directory domain. The domain contains a member server named Server1. You install the Windows Deployment Services (WDS) server role on Server1. You have a reference computer named Computer1 that runs Windows 7. You need to capture an image of Computer1 to WDS. What should you do?
To answer, move the appropriate actions from the Possible Actions list to the Necessary Actions area and arrange them in the correct order.



Answer:



Question: 311

Server setting	Server configuration
Initial host state	Started
Retain suspended state after computer starts	Enabled

Your network contains a Network Load Balancing (NLB) cluster named NLB01. NLB01 contains two servers named Node1 and Node2 that run Windows Server 2008 R2. Node1 and Node2 are configured as shown in the following table:
You need to install Windows updates on Node1 to meet the following requirements:

- Prevent new connections to Node1 while the updates are installed.
- Provide connected users with the ability to complete their session on Node1 before the updates are installed.

What should you do first?

A. From Network Load Balancing Manager, right-click Model and click Drainstop.
B. From Network Load Balancing Manager, right-click Node1 and click Suspend.
C. From the Services console, right-click Workstation and click Pause.
D. From the Services console, right-click Server and click Pause.

Answer: A

Question: 312

Your network contains a server named Server1 that runs a Server Core installation of Windows Server 2008 R2. The network contains a server named Server2 that runs a full installation of Windows Server 2008 R2. Server1 has the Streaming Media Services role installed. You need to administer the Streaming Media Services on Server1 from Server2. What should you do on Server2?

A. Download and install Windows Media Services 2008 for Windows Server 2008 R2.
B. Install the Remote Server Administration Tools (RSAT) feature.
C. Download and install Microsoft IIS Media services 3.0 - 64-bit.
D. Install the Quality Windows Audio video Experience (qWave) feature.

Answer: A

Explanation:

Managing a Windows Media server
Windows Media Services includes the following management interfaces:
On the full installation option for Windows Server 2008, you can use the Windows Media Services snap-in for Microsoft Management Console (MMC) to manage the local Windows Media server. To open the snap-in, click Start, click All Programs, click Administrative Tools, and then click Windows Media Services.
You can install the optional Web-based Administration role service on the local Windows Media server and then manage the server by opening the Windows Media Administration site (http://server_name:8080/default.asp) in a Web browser on a remote computer. For more information, see Administering Windows Media servers remotely.
You can install Remote Server Administration Tools for Windows Media Services on a computer that runs Windows Vista® or Windows® 7 and then manage your remote Windows Media server from the client computer. To start the Windows Media Services snap-in for MMC on the client computer, click Start, click Run, and then type wmsadmin.
Source: http://technet.microsoft.com/en-us/library/ee822833.aspx

Question: 313

Your network contains a Web server named Web1. You need to configure Web1 to authenticate users by using a custom Web page. Which authentication method should you enable on Web1?

A. Forms Authentication
B. Basic Authentication
C. ASP.NET Impersonation
D. Digest Authentication

Answer: A

Question: 314

You manage a Web server named Server1 that runs Windows Server 2006 R2. Server1 hosts five Web sites. You discover that the CPU utilization of Server1 is abnormally high. You need to view the amount of CPU resources that each web site is using. Which tool should you use?

A. Local Security Policy
B. Telnet
C. Services
D. windows Firewall
E. System Configuration
F. Ftp
G. Security Configuration Wizard (SCW)
H. Performance Monitor
I. Internet Information Services (IIS) Manager
J. Internet information services (IIS) 6.0 Manager
K. Component Services
L. lisreset

Answer: H

Question: 315

You manage a Web server named Server1 that runs Windows Server 200B R2. Server1 has five application pools. You need to recycle one application pool without affecting the other application pools. Which tool should you use?

A. System Configuration
B. Iisreset
C. Component Services
D. Internet Information Services (IIS) 6.0 Manager
E. Internet Information Services (IIS) Manager
F. Local Security Policy
G. Windows Firewall
H. Ftp
I. Security Configuration Wizard (SCW)
J. Telnet
K. Performance Monitor
L. Services

Answer: E

Question: 316

Your network contains an Active Directory domain named fabnkam.com. The domain contains a Web server named Web1 that runs Windows Server 2008 R2. You have a Web site named Corp. The content on Corp is stored on a FAT32 partition. Corp contains a Web page named Test.html. You need to ensure that only a user named Devi can access Test.html from the Corp Web site. All of the other content on Corp must be accessible to everyone. Which feature should you configure?

A. Feature Delegation
B. Authorization Rules
C. IP Address and Domain Restrictions
D. us Manager Permissions

Answer: B

Question: 317

Your network contains a server that has the Remote Desktop Session Host (RD Session Host) role service installed. You need to prevent administrators from logging other administrators off of the console session. What should you do?

A. From the RDP-Tcp properties of the RD Session Host server, modify the Sessions settings.
B. From the Computer Configuration Group Policy settings, modify the Remote Desktop Session Host settings.
C. From the User Configuration Group Policy settings, modify the Remote Desktop Connection Client settings.
D. From the RDP-Tcp properties of the RD Session Host server, modify the Client Settings.

Answer: B

Explanation:
Connections
Policy settings in this node control connection settings on a Remote Desktop Session Host server.
The full path of this node in the Group Policy Management Console is Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections.
Deny logoff of an administrator logged in to the console session

This policy setting determines whether an administrator attempting to connect remotely to the console of a server can log off an administrator currently logged on to the console.
This policy is useful when the currently connected administrator does not want to be logged off by another administrator. If the connected administrator is logged off, any data not previously saved is lost.
If you enable this policy setting, logging off the connected administrator is not allowed.
If you disable or do not configure this policy setting, logging off the connected administrator is allowed.
Note
The console session is also known as Session 0. Console access can be obtained by using the /console switch from Remote Desktop Connection in the computer field name or from the command line
Source: http://technet.microsoft.com/en-us/library/ee791922.aspx

Question: 318

Your network contains a server named Server1 that runs Windows Server 2008 R2. You have a Microsoft Application Visualization (App-V) application named Appl. You need to publish App1 as a RemoteApp program. Which role service should you install on Server1?

A. Remote Desktop Gateway (RD Gateway)
B. Remote Desktop Visualization Host (RD Visualization Host)
C. Remote Desktop Web Access (RD Web Access)
D. Remote Desktop Session Host (RD Session Host)

Answer: D

Question: 319

Your network contains an Active Directory domain named fabnkam.com. The domain contains a Web server named Web1 that runs Windows Server 2008 R2. You create a new site named Site1. You need to prevent Web1 from accepting HTTP URLs that are longer than 1,024 bytes. Which feature should you configure?

A. Connection Strings
B. Authorization Rules
C. Request Filtering
D. HTTP Response Headers

Answer: C

Question: 320

Your network contains a Web server named Server1 that runs Windows Server 2008 R2. Server1 has four application pools. You need to view a list of the CPU and memory resources used by each application pool. Which feature should you configure from internet Information Services (IIS) Manager?

A. Request Filtering
B. Error Pages
C. SSL Settings
D. Default Document
E. ISAPI and CGI Restrictions
F. HTTP Response Headers
G. Feature Delegation

H. Authentication
I. IIS Manager Permissions
J. Connection Strings
K. IP Address and Domain Restrictions
L. Management Service
M. HTTP Redirect
N. worker Processes
O. ISAPI Filters
P. Authorization Rules

Answer: N

Question: 321

Your network contains a server that runs Windows Server 2008 R2 and has the Windows Deployment Services (WDS) server role installed. The server contains an image of Windows Vista Service Pack 2 (SP2), an image of Windows 7, an image of Windows Server 2008, and an image of Windows Server 2008 R2. You need to update the drivers in the images. You want to achieve this goal by using the minimum amount of administrative effort. Which tool should you use?

A. Dism
B. Pkgmgr
C. Windows Deployment Services console
D. Windows System Image Manager (Windows SIM)

Answer: C

Explanation:
In Windows Server 2008 R2, you can use Windows Deployment Services to add driver packages to the server and configure them to be deployed to client computers along with the install image. Note that this functionality is only available when you are installing images of the following operating systems: Windows Vista with SP1, Windows Server 2008, Windows 7, and Windows Server 2008 R2. WDS console because Dism no archieve this goal using the minimum administrative effort.
Source: http://technet.microsoft.com/en-us/library/dd348456(WS.10).aspx

Question: 322

Your network contains a server named Server1. Server1 has the Web Server (IIS) server role installed and all of the Web Server (IIS) role services installed. You install the SMTP Server feature on Server1. You need to configure size limits for messages processed by the SMTP server. Which tool should you use? (Each correct answer presents a complete solution. Choose two.)

A. Internet Information Services (IIS) Manager
B. Computer Management
C. Internet Information Services (IIS) 6.0 Manager
D. ADsutil.vbs
E. Netsh.exe
F. Services.msc

Answer: A, B

Question: 323

Your network contains a server named Server1 that has the Streaming Media Services server role installed. Server1 has the WMS Http Server Control Protocol plug-in and the WMS Server RTSP Control Protocol plug-in enabled. All client computers run Windows 7. The corporate website contains links to on-demand media content that is hosted on Server1. You install the Web Server (IIS) server role on Server1 by using the default settings. You change the port of the WMS HTTP Server Control Protocol plug-in to 1450. Users report that the links on the corporate website no longer work. You need to ensure that the users can access the on-demand media content by clicking the links on the corporate website. What should you do? (Each correct answer presents a complete solution. Choose three.)

A. On Server1, bind the HTTP protocol of the Default Web Site to port 1450.
B. On Server1, disable the Default Web Site
C. On the corporate website, change the URLs of the links to use rtsp://server1.
D. On the corporate website, change the URLs of the links to use mms://server1.
E. On Server1, disable the WMS Server RTSP Control Protocol plug-in.
F. On the corporate website, change the URLs of the links to use http://server1:1450.

Answer: A, B, C

Question: 324

Your network contains three servers named Server2, Server3, and Server4 that run Windows Server 2008 R2 Service Pack 1 (SP1). Each server has the Streaming Media Services server role installed. Server2 is configured as an origin server, Server3 and Server4 are cache/proxy servers. You need to prevent Server2 from streaming more than 500 kilobits per second (Kbps) to the cache/proxy servers. The Solution must also prevent individual users from streaming more than 250 Kbps from Server2. Which two limits should you configure on Server2? (Each correct answer presents part of the solution. Choose two.)

A. Limit aggregate outgoing distribution bandwidth (Kbps)
B. Limit bandwidth per player connection (Kbps)
C. Limit bandwidth per outgoing distribution connection (Kbps)
D. Limit aggregate player bandwidth (Kbps)
E. Limit outgoing distribution connections
F. Limit player connections

Answer: A, B

Question: 325

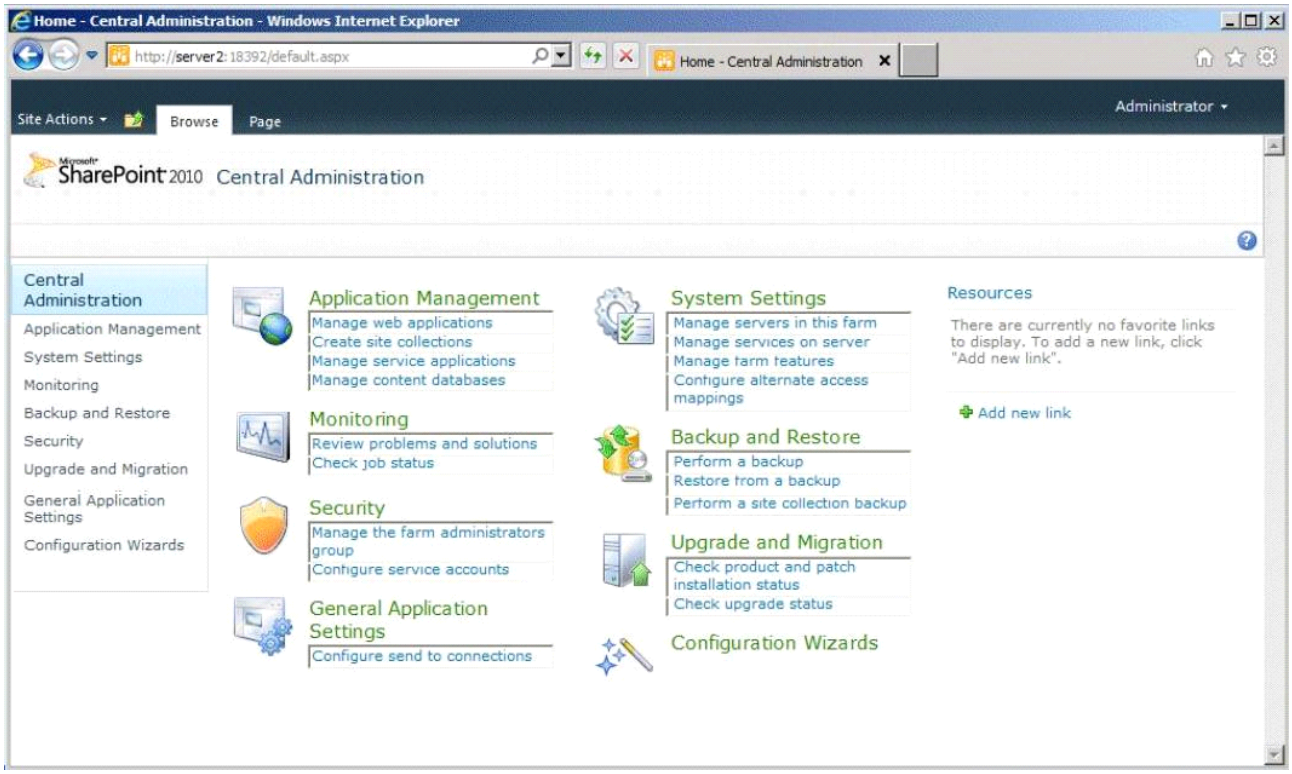
Your network contains a server named Server1 that runs Windows Server 2008 R2 Service Pack 1 (SP1). You install the SMTP Server feature on Server1. You verify that Server1 receives email messages. You restart Server1. You discover that Server1 no longer receives email messages. You need to ensure that Server1 can receive email messages after the restart. What should you do on Server1?

A. From Internet Information Services (IIS) 6.0 Manager, configure the Relay Restrictions settings
B. From the Services console, modify the startup type of the Message Queuing feature.
C. From Internet Information Services (IIS) 6.0 Manager, configure the Security settings.
D. From the Services console, modify the startup type of the Simple Mail Transfer Protocol (SMTP) service.

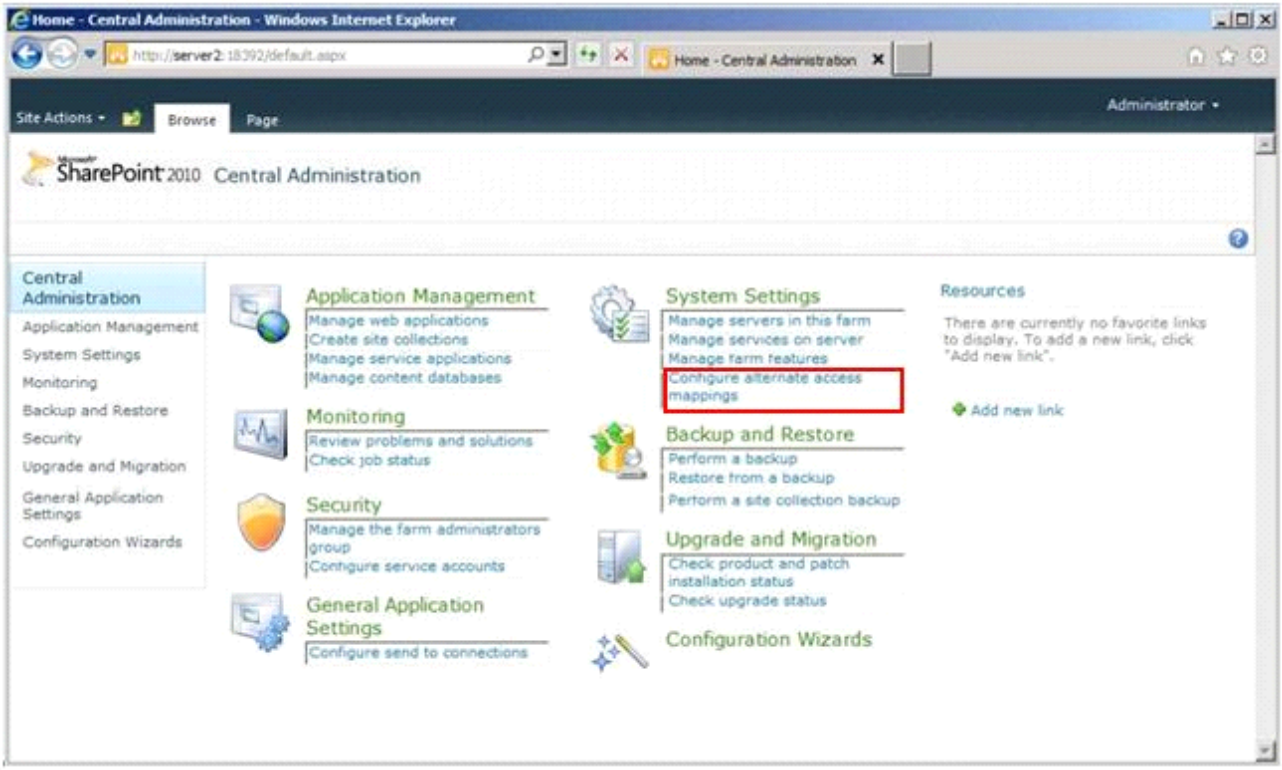
Answer: A

Question: 326
HOTSPOT

Your network contains a server named Server2 that has Microsoft SharePoint Foundation 2010 Service Pack 1 (SP1) installed. Server2 has a web application named Web1. Web1 contains a site collection named Site1.
Users access Site1 by using the URL http://server2.contoso.com.
You need to ensure that the users can access Site1 by using the URL http://site1.contoso.com.
The solution must not create additional Internet Information Services (IIS) websites. What should you configure? To answer, select the appropriate link in the answer area.



Answer:



Question: 327

Your network contains a Remote Desktop Session Host (RD Session Host) server named Server1. You need to prevent users from running a application named App1 in Remote Desktop sessions. The solution must ensure that the users can run other applications from Remote Desktop sessions on Server1. What should you do? (Each correct answer presents part of the solution. Choose three.)

A. Start the Application Management service, and then set up the startup to Automatic.
B. From th Local Group Policy console, set the security level of the software restriction policy to Basic user.
C. From the Local group Policy Editor, create the default AppLocker executable rules and a deny AppLocker executable rule.
D. Start the Application Identity service, and then set the startup type to Automatic.
E. From the Local group Policy Editor, modify the AppLocker Enforcement settings.

Answer: A, B, C

Question: 328

You have a Remote Desktop Services (RDS) server farm named farm.contoso.com. The farm contains five servers. The Servers are configured as shown in the following table.

Server Name	IP Address	Role service and configuration
Server1	192.168.0.10	Remote Desktop Connection Broker (RD Connection Broker)
Server2	192.168.0.75	Remote Desktop Session Host (RD Session Host) in virtual machine redirection mode
Server3	192.168.0130	Remote Desktop Session Host (RD Session Host)
Server4	192.168.0.195	Remote Desktop Web Access (RD Web Access)
Server5	192.168.1.100	Remote Desktop Virtualization Host (RD Virtualization Host)

The farm is configured to host virtual desktops. All users access the virtual desktops by using RD Web Access. Users who use Remote Desktop Connection 6.1 report that they cannot connect to their personal virtual desktop by using RD Web Access. You verify that the users who use Remote Desktop Connection 7.0 can access their personal virtual desktop by using RD Web Access. What should you do? (Each correct answer presents part of the solution. Choose two.)

A. Create a canonical name (CNAME) record for server2.contoso.com.
B. From Remote Desktop Connection Manager, configure an alternative server name.
C. Create a host (A) record named Redirect that points to 192.168.1.100
D. Create a host (A) record named Redirect that points to 192.168.0.75
E. From Remote Desktop Session Host Configuration, configure Server2 for dedicated farm redirection.
F. Create a canonical name (CNAME) record for server5.contoso.com.

Answer: E, F

Question: 329

Your network contains an Active Directory domain named adatum.com. the domain contains a server named Server5 that has the Remote Desktop Services (RDS) server role installed and all of the RDS role services installed. You have two support Administrators named Admin1 and Admin2, Admin1 and Admin2 connect to Server5 by using Remote Desktop Connections, to run network managementtools. You need to identify which processes currently run in Admin1's remote Desktop session. Which tool should you use?

A. Regedit
B. Remote Desktop Gateway Manager
C. Dism
D. Rdpsign
E. Netsh
F. Remote Desktop Services Manager
G. Windows System Resource Manager (WSRM)
H. Rdpinit
I. Mstsc
J. Remote Desktop Connection Manager
K. Remote Desktop Session Host Configuration

Answer: J

Question: 330

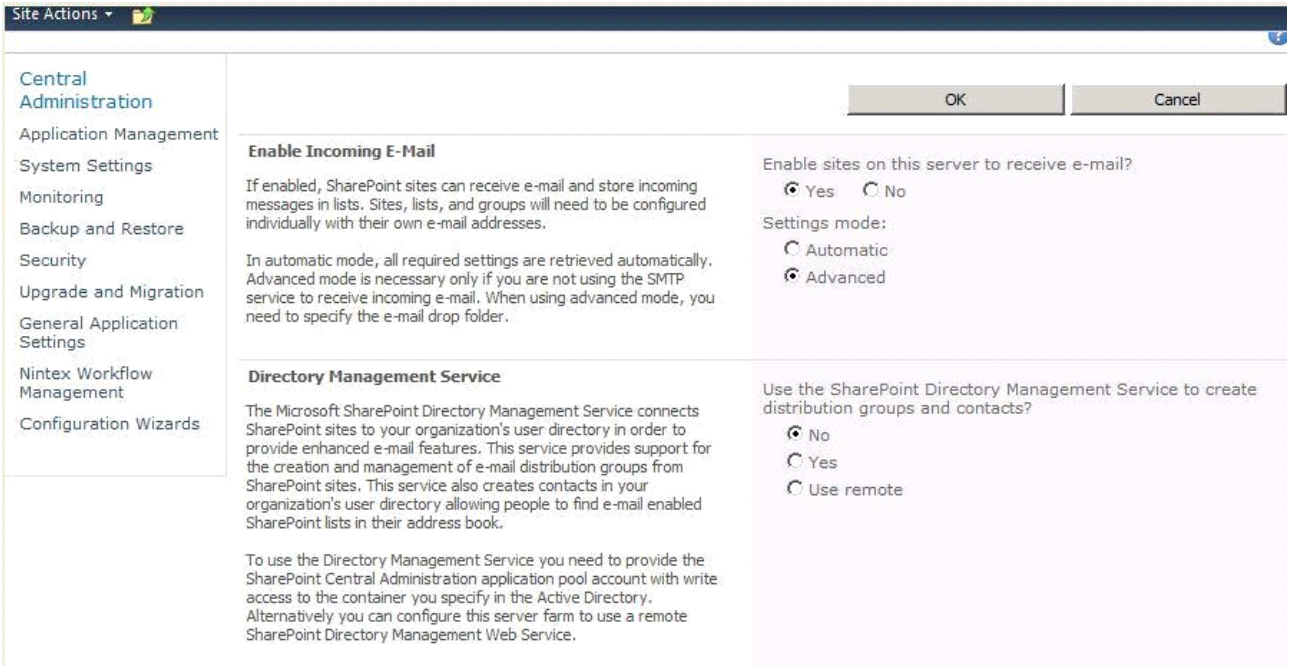
You have a Remote Desktop Session Host (RD Session Host) server named SRV4. You Open Remote Desktop Services Manager as shown in the exhibit (Click the Exhibit button.) You need to take remote control of the session of User1. What should you do first?

A. From Remote Desktop Connection, connect to Server4.
B. From local Users and Groups, add user1 to the Remote Desktop Users group.
C. From Remote Desktop Services Manager, disconnect the session of User1.
D. From Local Users and Groups, add the built-in Administrator account to the Remote Desktop Users group.

Answer: A

Question: 331

Your network contains a server named Web1 that has Microsoft SharePoint Foundation 2010 installed. You open Configure the incoming email settings as shown in the exhibit. (Click the Exhibit button.).

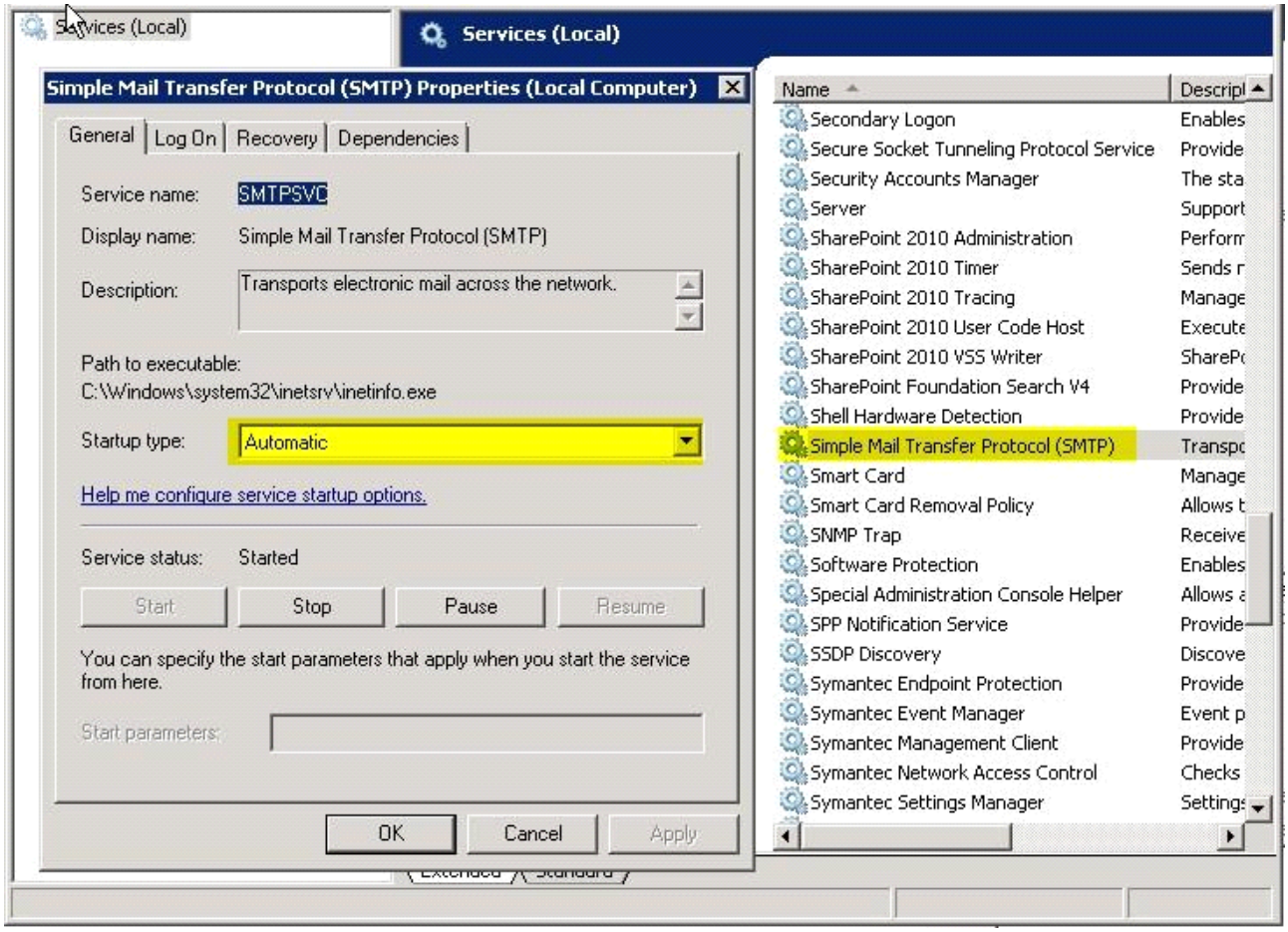


You need to configure the incoming email settings to use automatic mode. What should you do first?

A. Configure the outgoing email settings.
B. Install the SMTP Server feature.
C. Activate the email Integration with Content Organizer feature.
D. Install the Message Queuing feature.

Answer: B

Explanation:



Question: 332

Your network contains an Active Directory domain named fabrikam.com. The domain contains a Web server named Web1 that runs Windows Server 2008 R2. You install the FTP Server role service on Web1. You need to manage the FTP server settings on Web1. Which tool should you use?

A. Services
B. Internet Information Services (IIS) Manager
C. Internet Information Services (IIS) 6.0 Manager
D. Ftp

Answer: C

Question: 333

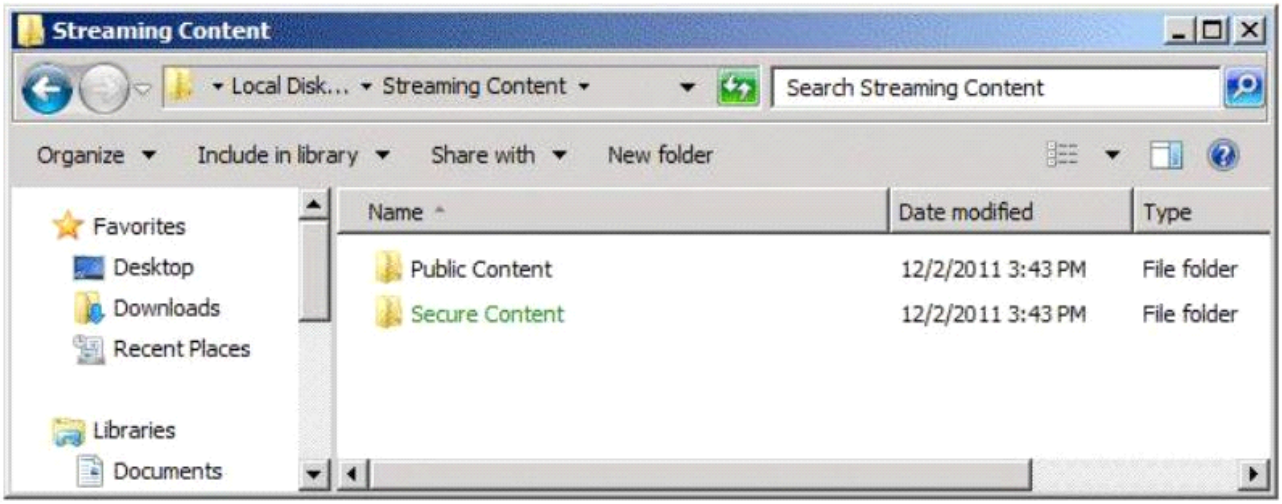
Your network contains a server named Server1 that runs Windows Server 2008 R2. You add a new 1TB hard disk to Server1. You need to minimize the risk of file system corruption or loss on the new volume in the event of a system failure. What should you do?

A. Initialize the disk as a GUID partition Table (GPT) disk.
B. Initialize the disk as a Master Boot Record (MBR) disk.
C. Disable write caching for the hard disk.
D. Disable direct memory access (DMA) for the hard disk controller.

Answer: A

Question: 334

Your network contains a server named Server1 that has the Streaming Media Services server role installed. Server1 streams content from two folders as shown in the exhibit. (Click the Exhibit button.)



You discover that you can stream content from the public Content folder, but you cannot stream content from the Secure Content folder. You need to ensure that you can stream content from both folders. What should you configure?

A. the Windows Audio Endpoint Builder service
B. the WMS negotiate Authentication plug-in at the publishing point level
C. the WMS NTFS ACL Authorization plug-in at the publishing point level
D. the Windows Media Services service
E. the WMS Negotiate Authentication plug-in at the server level
F. the WMS NTFS ACL Authorization plug-in at the server level

Answer: D

Question: 335

Your network contains an Active Directory domain named adatum.com. The domain contains a server named Server5 that runs Windows Server 2008 R2 Service Pack 1 (SP1). You install the Remote Desktop Services (RDS) server role and all of the RDS role services on Server5. You create universal security group named Support.yYou add 10 user accounts to the Support group. You need to ensure that Remote Desktop sessions established by members of the Support group receive the highest possible CPU allocation on Server5. Which tool should you use?

A. Regedit
B. Remote Desktop Gateway Manager
C. Dism
D. Rdpsign
E. Netsh
F. Remote Desktop Services Manager
G. Windows System Resource Manager (WSRM)
H. Rdpinit
I. Mstsc
J. Remote Desktop Connection Manager

K. Remote Desktop Session Host Configuration

Answer: G

Question: 336

Your network contains an Active Directory domain named adatum.com. The domain contains a server named Server5 that has the Remote Desktop Services (RDS) server role installed and all of the RDS role services installed. Server5 is configured as a file server and a Remote Desktop Services client access licences (RDS CALS) on Server5. Which tool should you use?

A. Regedit
B. Remote Desktop Gateway Manager
C. Dism
D. Rdpsign
E. Netsh
F. Remote Desktop Services Manager
G. Windows System Resource Manager (WSRM)
H. Rdpinit
I. Mstsc
J. Remote Desktop Connection Manager
K. Remote Desktop Session Host Configuration

Answer: F

Question: 337

Your network contains an Active Directory domain named adatum.com. The domain contains a server named Server5 that has the Remote Desktop Services (RDS) server role installed and all of the RDS role services installed. Server5 is configured as a file server and a Remote Desktop services server. You configure a remote Desktop Connection named server5.rdp. You plan to deploy server5.rdp to all users in the domain. You need to ensure that server5.rdp cannot be used by any user if the content of the file has been modified Which tool should you use?

A. Regedit
B. Remote Desktop Gateway Manager
C. Dism
D. Rdpsign
E. Netsh
F. Remote Desktop Services Manager
G. Windows System Resource Manager (WSRM)
H. Rdpinit
I. Mstsc
J. Remote Desktop Connection Manager
K. Remote Desktop Session Host Configuration

Answer: D

Question: 338

You manage a Web server named Server1 that runs Windows 2008 R2 Server1 has the SMTP Server feature installed. You need to verify whether you can connect to Server1 over port 25 Which tool should you use?

A. Ftp
B. Services
C. Security Configuration Wizard (SCW)
D. Internet Information Services (IIS) 6.0 Manager
E. Internet Information Services (IIS) Manager
F. Iisreset
G. Performance Monitor
H. Windows Firewall
I. Telnet
J. Local Security Policy
K. System Configuration
L. Component Services

Answer: I

Question: 339

Your network contains a server named Serverl that has the Remote Desktop Services (RDS) server role installed and all of the RDS role services installed. You need to install the RemoteFX cap driver on Server1. Which tool should you use?

A. Remote Desktop Session Host Configuration
B. Remote Desktop Connection Manager
C. Remote Desktop Services Manager
D. Dism
E. Windows System Resource Manager (WSRM)
F. Netsh
G. Mstsc
H. Remote Desktop Gateway Manager
I. Rdpinit
J. Regedit
K. Rdpsign

Answer: D

Explanation:
Ref:
http://technet.microsoft.com/en-us/library/gg607270(v=ws.10)

Question: 340

Your network contains a server named Server1 that has the Remote Desktop Services (RDS) server role installed and all of the RDS role services installed. You need to identify which processes each Remote Desktop session runs currently. Which tool should you use?

A. Remote Desktop Gateway Manager
B. Windows System Resource Manager (WSRM)
C. Remote Desktop Session Host Configuration

D. Regedit
E. Remote Desktop Services Manager
F. Dism
G. Rdpinit
H. Mstsc
I. Rdpsign
J. Remote Desktop Connection Manager
K. Netsh

Answer: E

Explanation:
Ref:
http://technet.microsoft.com/en-us/library/cc754930

Question: 341

You manage a Web server named Server1 that runs Windows Server 2008 R2. Server1 has the FTP Server role service installed. You need to manage the FTP server settings on Server1, Which tool should you use?

A. System Configuration
B. Performance Monitor
C. Internet Information Services (IIS) Manager
D. Local Security Policy
E. Security Configuration Wizard (SCW)
F. Ftp
G. Telnet
H. Component Services
I. Services
J. Windows Firewall
K. Iisreset
L. Internet Information Services (IIS) 6.0 Manager

Answer: C

Explanation:
Ref:
http://technet.microsoft.com/en-us/library/dd722761(WS.10).aspx
http://support.orcsweb.com/KB/a338/create-an-iis-75-ftp-site-windows-server-2008-r2.aspx

Question: 342

Your network contains three servers named Server2, Server3, and Server4 that run Windows Server 2008 R2 Service Pack 1 (SP1). Each server has the Streaming Media Services server role installed. Server2 is configured as an origin server. Server3 and Server4 are cache/proxy servers. You need to configure the limits on Server2 to meet the following requirements:

- Prevent Server3 from streaming more than 500 Kbps from Server2.
- Prevent Server4 from streaming more than 500 Kbps from Server2.
- Prevent individual users from streaming more than 250 Kbps from Server2.

Which two limits should you configure on Server2? (Each correct answer presents part of the solution. Choose two.)

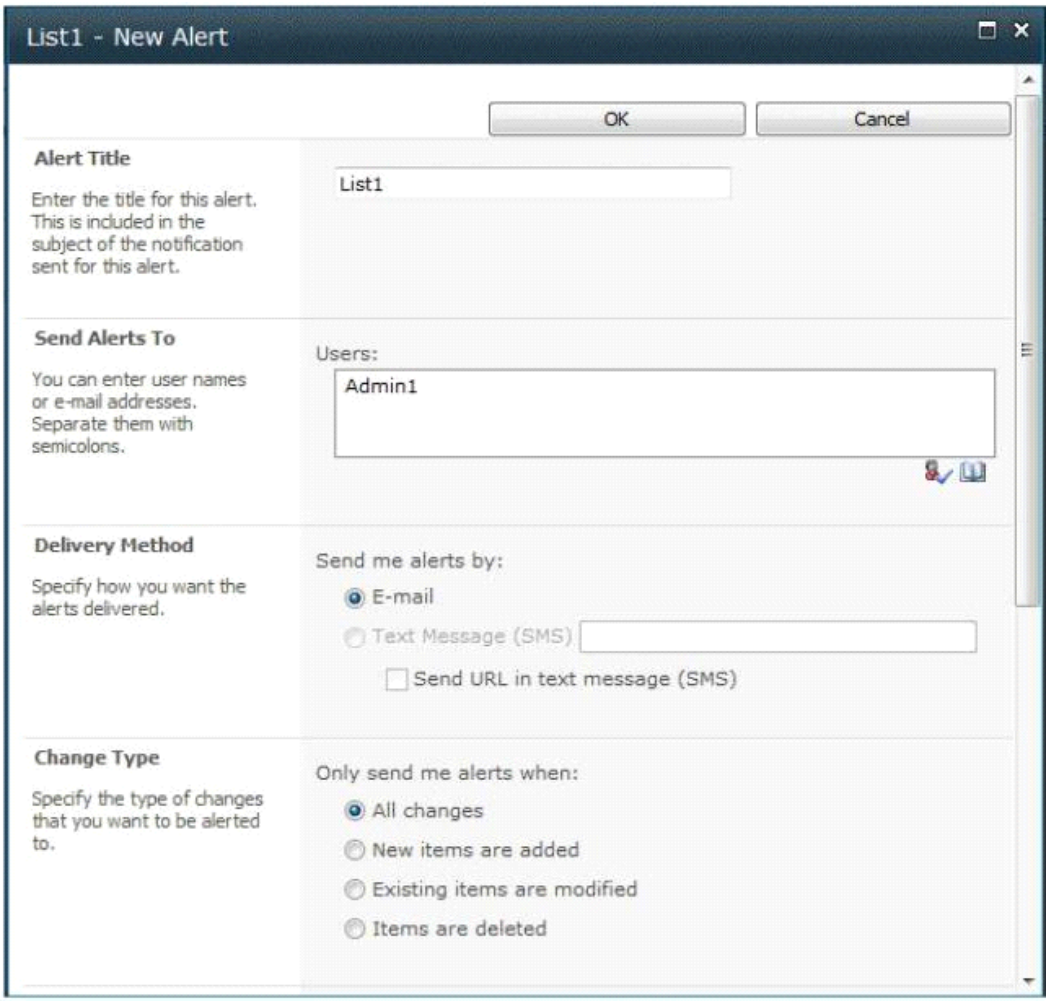
A. Limit player connections
B. Limit outgoing distribution connections
C. Limit bandwidth per outgoing distribution connection (Kbps)
D. Limit bandwidth per player connection (Kbps)
E. Limit aggregate outgoing distribution bandwidth (Kbps)
F. Limit aggregate player bandwidth (Kbps)

Answer: C, D

Explanation:
Ref:
http://technet.microsoft.com/en-us/library/cc754690
http://technet.microsoft.com/en-us/library/cc731216

Question: 343

Your network contains a server named Web1 that has Microsoft SharePoint Foundation 2010 installed. Web1 has a site named Site1. You attempt to create an alert as shown in the exhibit. (Click the Exhibit button.)



You need to ensure that alerts can be sent as text messages. What should you do?

A. From Central Administration, create a new trust relationship.
B. From Site Settings, modify the RSS settings.

C. From Site Settings, modify the site permissions.
D. From Central Administration, modify the mobile account settings.

Answer: D

Explanation:
Ref:
http://technet.microsoft.com/en-us/library/ee428292

Question: 344
HOTSPOT

Your network contains a server named Web1 that has Microsoft SharePoint Foundation 2010 installed. You need to configure Web1 to use Information Rights Management (IRM). Which link should you use? To answer, select the appropriate link from the answer area.

Answer:

Explanation:
Ref:
http://technet.microsoft.com/en-us/library/hh545613.aspx

Question: 345

Your network contains a server named Server1 that has the Streaming Media Services server role installed. Server1 is located in the perimeter network. A firewall named Firewall1 connects the perimeter network and the Internet. You need to ensure that clients from the Internet can access streaming content from Server1 by using RTSP. The solution must minimize the number of open ports on Firewall1. Which two inbound firewall ports should you open on Firewall1? (Each correct answer presents part of the solution. Choose two.)

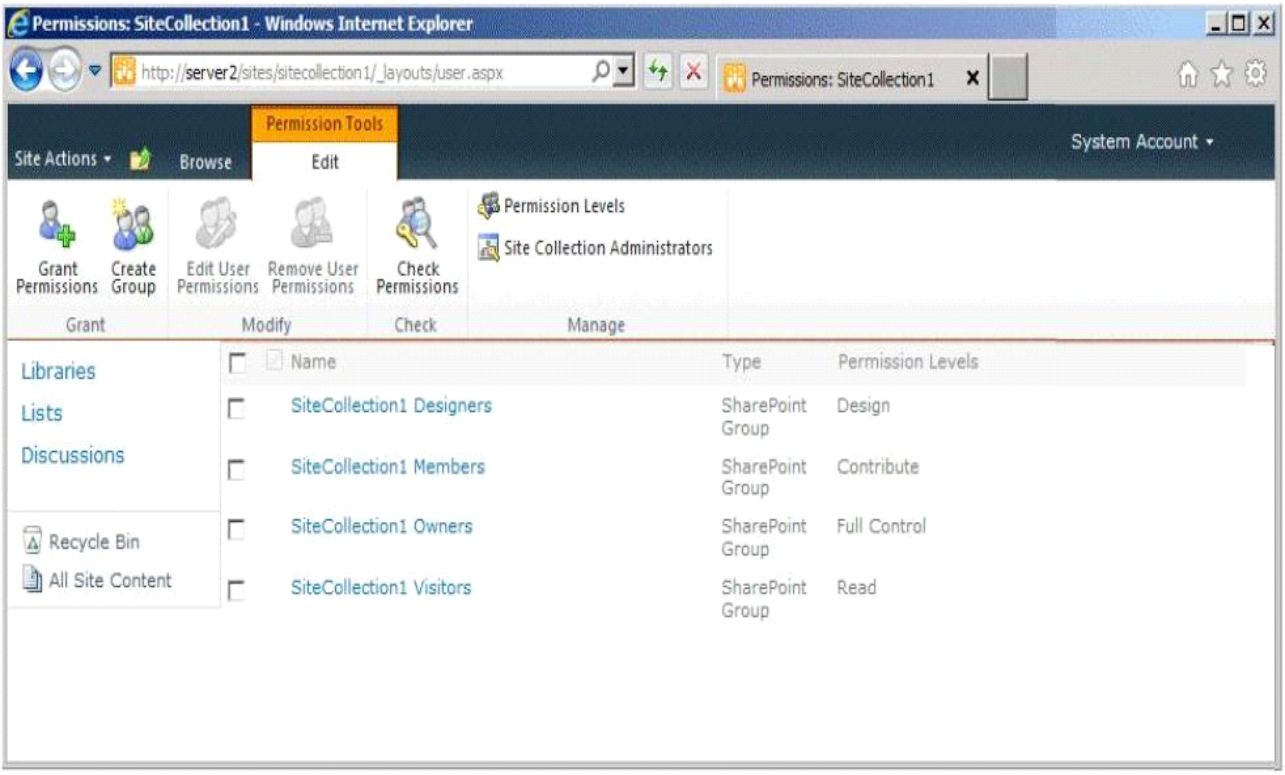
A. TCP 6881
B. UDP 8080
C. TCP 1755
D. TCP 554
E. UDP 5005

Answer: D, E

Explanation:
Ref:
http://www.microsoft.com/windows/windowsmedia/forpros/serve/firewall.aspx

Question: 346

Your network contains a server named Server2 that has Microsoft SharePoint Foundation 2010 Service Pack 1 (SP1) installed. You have a site collection named SiteCollection1. The groups in SiteCollection1 are shown in the exhibit. (Click the Exhibit button.)



You need to ensure that a user named User1 can create and delete lists in SiteCollection1. The solution must minimize the number of permissions assigned to User1. To which group should add User1?

A. SiteCollection1 Visitors
B. SiteCollection1 Owners
C. SiteCollection1 Designers
D. SiteCollection1 Members

Answer: C

Explanation:
Ref:
http://technet.microsoft.com/library/cc288074(office.14).aspx

Question: 347

Your network contains a Web server named Server1 that runs Windows Server 2008 R2. You need to ensure that Server1 only processes HTTP URLs that are shorter than 2,048 bytes. Which feature should you configure from Internet Information Services (IIS) Manager?

A. HTTP Response Headers
B. IP Address and Domain Restrictions
C. Default Document
D. SSL Settings
E. Worker Processes
F. Authentication
G. Connection Strings
H. IIS Manager Permissions
I. Request Filtering

J. ISAPI and CGI Restrictions
K. Feature Delegation
L. Error Pages
M. Authorization Rules
N. ISAPI Filters
O. HTTP Redirect
P. Management Service

Answer: I

Explanation:
Ref:
http://www.iis.net/ConfigReference/system.webServer/security/requestFiltering

Question: 348

You are evaluating whether to purchase Windows Server 2008 R2 Service Pack 1 (SP1). Several weeks ago, you installed Windows Server 2008 R2 SP1 on a server. During the installation, you did not enter a product key. You need to identify how many days remain until the license status of the server will change to Unlicensed. Which tool should you use?

A. System Configuration
B. Windows Activation
C. Action Center
D. Act.exe

Answer: B

Explanation:
Ref:
http://www.windowsvalley.com/is-windows-activated-check-windows-activation-status/

Question: 349

Your network contains a server that runs Windows Server 2008 R2 and has the Windows Deployment Services (WDS) server role installed. The server contains an image of Windows Vista Service Pack 2 (SP2), an image of Windows 7, an image of Windows Server 2008, and an image of Windows Server 2008 R2. You need to update the drivers in the images. You want to achieve this goal by using the minimum amount of administrative effort. Which tool should you use?

A. Windows Deployment Services console
B. Pkgmgr
C. Dism
D. Windows Driver Kit (WDK)

Answer: A

Explanation:
In Windows Server 2008 R2, you can use Windows Deployment Services to add driver packages to the server and configure them to be deployed to client computers along with the install image. Note that this functionality is only

available when you are installing images of the following operating systems: Windows Vista with SP1, Windows Server 2008, Windows 7, and Windows Server 2008 R2.
WDS console because Dism no archieve this goal using the minimum administrative effort.
Source: http://technet.microsoft.com/en-us/library/dd348456(WS.10).aspx

Question: 350

Your network contains a server named Server1 that has the Remote Desktop Session Host (RD Session Host) role service installed. You enable Plug and Play device redirection for Server1 by using a Group Policy. You verify that the Group Policy is applied to Server1. From a client computer, you configure Remote Desktop Connection as shown in the exhibit. (Click the Exhibit button.)

You discover that when you establish a Remote Desktop session to Serverl, Plug and Play devices are not redirected. You need to ensure that Plug and Play devices are redirected during Remote Desktop sessions to Server1. What should you do? (Each correct answer presents part of the solution. Choose two.)

A. On Server1, modify the Sessions settings of the RDP-Tcp Properties.
B. On Server1, install the Desktop Experience feature.
C. From the client computer, modify the Experience settings of Remote Desktop Connection.
D. On Server1, install the Quality Windows Audio Video Experience feature.
E. On Server1, modify the Client Settings of the RDP-Tcp Properties.

Answer: B, E

Explanation:
Ref:
http://technet.microsoft.com/en-us/library/cc725887(v=ws.10).aspx

Question: 351

Your network contains an Active Directory domain named adatum.com. You publish a RemoteApp named WebApp5. The Remote Desktop Connection (.rdp) file for WebApp5 is unsigned. When a user named User5 runs WebApp5 from the Remote Desktop Web Access (RD Web Access) website, Users is prompted for credentials. You need to prevent users from being prompted for credentials when they run WebApp5. What should you do?

A. Enable Forms-based authentication for the Remote Desktop Web Access website.
B. Enable the Allow Delegating Default Credentials Group Policy setting.
C. Add a Managed Module for the RDWeb virtual directory.
D. Enable the Assign a default domain for logon Group Policy setting.

Answer: B

Explanation:
Ref:
http://technet.microsoft.com/en-us/library/cc742808.aspx

Question: 352

Your company contains an Active Directory domain named adatum.com. The domain contains a server named Servers that runs Windows Server 2008 R2 Service Pack 1 (SP1). Server5 is configured as a file and print server. Server5 contains three dynamic disks named HardDisk1, HardDisk2 and HardDisk3. HardDisk1 has a volume that contains critical data. HardDisk2 and HardDisk3 do not contain any volumes. You need to create a mirror of the volume on HardDisk1. Which Diskpart command should you run?

A GPT
B. online
C. list
D. filesystems
E. merge vdisk
F. create
G. attach vdisk
H. automount
I. retain
J. assign
K. add
L. compact vdisk
M. extend
N offline
O. break
P. attributes
Q. remove
R. recover
S. format
T. rescan
U. repair
V. active
W. expand vdisk

X. detach vdisk

Answer: K

Explanation:
Ref:
http://technet.microsoft.com/en-us/library/cc754384(v=ws.10).aspx

Question: 353

Your network contains a server named Server1 that runs Windows Server 2008 R2 Service Pack 1 (SP1). You have a new server that contains one dynamic disk. You plan to install Windows Server 2008 R2 Service Pack 1 (SP1) on the server. You attempt to select the dynamic disk during the installation and you receive the following error message: "Windows cannot be installed to this hard disk space. The partition contains one or more dynamic volumes that are not supported for installation." You need to install Windows Server 2008 R2 SP1 on the disk. Which Diskpart command should you run?

A. merge vdisk
B. compact vdisk
C. create
D. filesystems
E. rescan
F. expand vdisk
G. repair
H. online
I. offline
J. GPT
K. assign
L. remove
M. break
N. automount
O. format
P. active
Q. retain
R. detach vdisk
S. add
T. recover
U. extend
V. attach vdisk
W. list
X. attributes

Answer: Q

Explanation:
Ref:
http://technet.microsoft.com/en-us/library/cc755127(v=ws.10)

Question: 354

Your network contains a server named Server1 that has the Web Server (IIS) server role installed. You need to ensure that the IIS configuration of Server1 is backed up daily. The solution must minimize the size of the backup. What should you do?

A. Create a scheduled task that runs Get-WebConfiguration.
B. From Windows Server Backup, create a custom backup configuration that backs up drive C.
C. From Windows Server Backup, create a custom backup configuration that backs up the C:\Inetpub folder.
D. Create a scheduled task that runs appcmd.exe.

Answer: D

Explanation:
Ref:
http://learn.iis.net/page.aspx/114/getting-started-with-appcmdexe/#Managing
(Managing Backups section)

Question: 355

Your network contains a server named Web1 that has the Web Server (IIS) server role installed. Web1 has a web application named SalesApp. SalesApp runs in an application pool named AppPool1. Only SalesApp runs in AppPool1. You need to ensure that SalesApp automatically releases all memory resources every day at 06:00. What should you do?

A. From Internet Information Services (IIS) Manager, modify the Advanced Settings of SalesApp.
B. From Internet Information Services (IIS) Manager, modify the Advanced Settings of AppPool1.
C. From Windows System Resource Manager, add a conditional policy.
D. From Windows System Resource Manager, add a profiling resource allocation policy.

Answer: B

Explanation:
Ref:
http://technet.microsoft.com/en-us/library/dd349270(WS.10).aspx

Question: 356

Your network contains a server named Web1 that has Microsoft SharePoint Foundation 2010 installed. You install the SMTP Server feature on Web1, and then you configure the outgoing email settings from Central Administration. You verify that users can receive SharePoint alerts by email. During routine maintenance, you restart Web1. You discover that the users no longer receive SharePoint alerts by email. You need to ensure that Web1 can send SharePoint alerts by email. What should you do on Web1?

A. From Internet Information Services (IIS) 6.0 Manager, configure the Security settings.
B. From Internet Information Services (IIS) 6.0 Manager, configure the Relay Restrictions settings.
C. From the Services console, modify the startup type of the Message Queuing feature.
D. From the Services console, modify the startup type of the Simple Mail Transfer Protocol (SMTP) service.

Answer: D

Question: 357

Your network contains a Web server named Server1 that runs Windows Server 2008 R2. You need to ensure that when a user attempts to connect to a page on Server1 that does not exist, Server1 displays a custom page that contains a site map. Which feature should you configure from Internet Information Services (IIS) Manager?

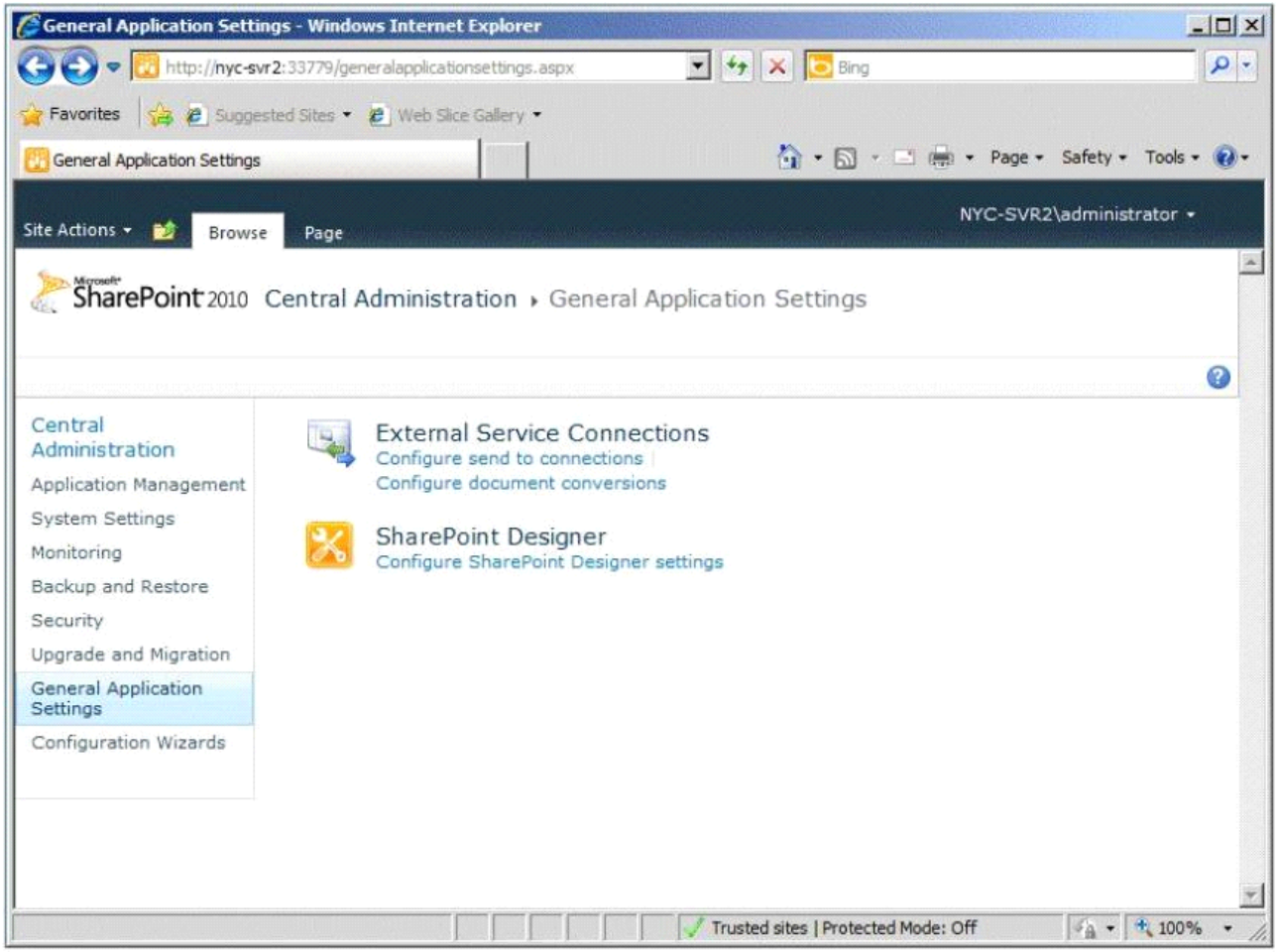
A. ISAPI Filters
B. HTTP Response Headers
C. Connection Strings
D. IP Address and Domain Restrictions
E. Error Pages
F. SSL Settings
G. Authorization Rules
H. Feature Delegation
I. Worker Processes
J. Default Document
K. ISAPI and CGI Restrictions
L IIS Manager Permissions
M. Authentication
N. HTTP Redirect
O. Request Filtering
P. Management Service

Answer: E

Explanation:
Ref:
http://stackoverflow.com/questions/11334142/non-existing-url-path-throws-standard-iis-404-page

Question: 358

Your network contains a server that runs Windows Server 2008 R2 Service Pack 1 (SP1). The server has Microsoft SharePoint Foundation 2010 installed. When you open General Application Settings, you see the webpage shown in the exhibit. (Click the Exhibit button.)



You need to configure report server integration. What should you do first?

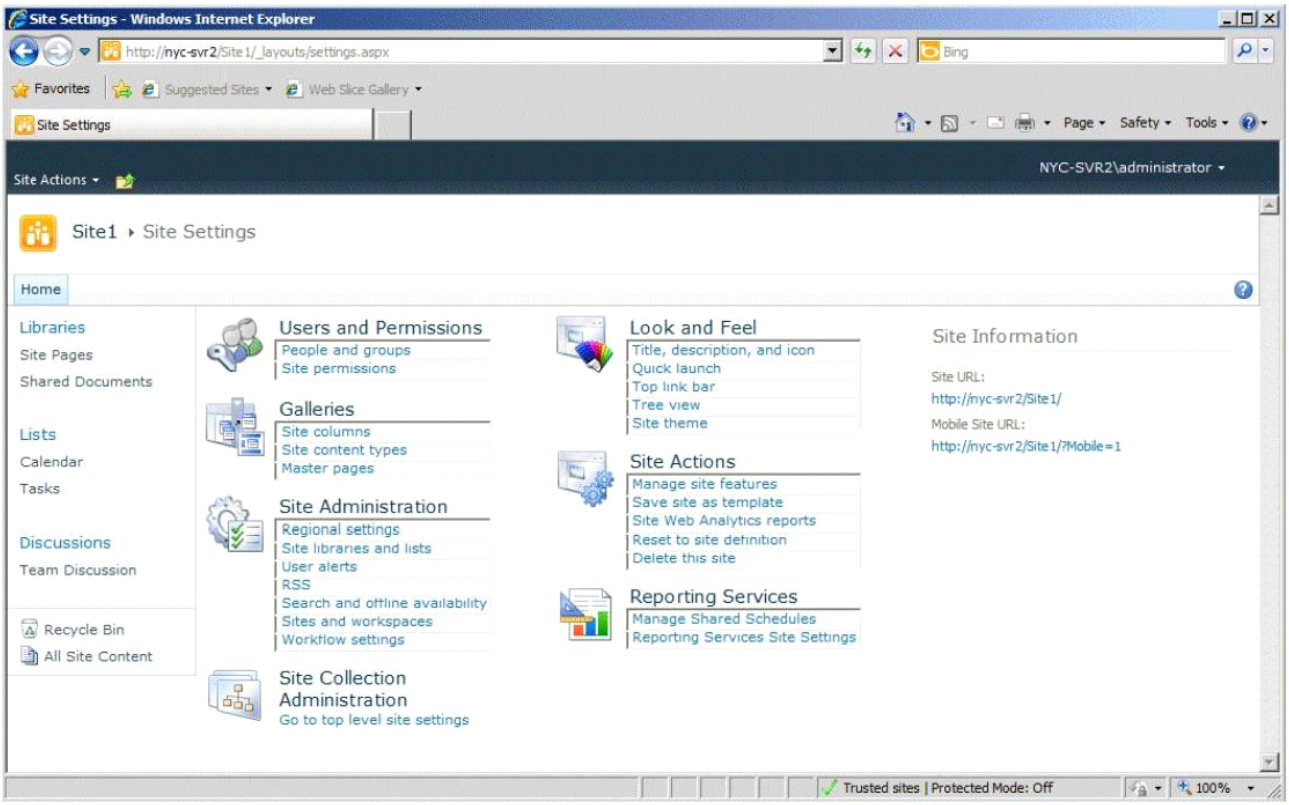
A. Configure the service accounts.
B. Add a new web application.
C. Add a new service application.
D. Manage the server farm features.

Answer: B

Explanation:
Ref:
http://msdn.microsoft.com/en-us/library/bb283190(v=sql.105).aspx

Question: 359
HOTSPOT

Your network contains a server that has Microsoft SharePoint Foundation 2010 installed. The server has a site named Site1. You need to prevent the content of Site1 from being indexed. What should you configure?
To answer, select the appropriate link in the answer area.



Answer: Select "Search and offline availability" in the Site Administration section.

Question: 360

Your network contains a server named Server1 that has the Web Server (IIS) server role installed. You need to ensure that the IIS configuration of Server1 is backed up daily. The solution must minimize the size of the backup. What should you do?

A. Create a scheduled task that runs appcmd.exe.
B. Create a scheduled task that runs Get-WebConfiguration.
C. Create a scheduled task that runs iisbback.vbs.
D. Create a scheduled task that runs iisconfig.vbs.

Answer: A

Explanation:
Ref:
http://learn.iis.net/page.aspx/114/getting-started-with-appcmdexe/#Managing
(Managing Backups section)

Question: 361

Your network contains an Active directory domain named fabrikam.com. The domain contains a Web server named Web1 that runs Windows Server 2008 R2. You create three application pools named AppPool1, AppPool2, and AppPool3. You need to recycle AppPool1 without affecting AppPool2 and AppPool3. Which tool should you use?

A. Services
B. Internet Information Services (IIS) Manager
C. Internet Information Services (IIS) 6.0 Manager
D. Iisreset

Answer: B

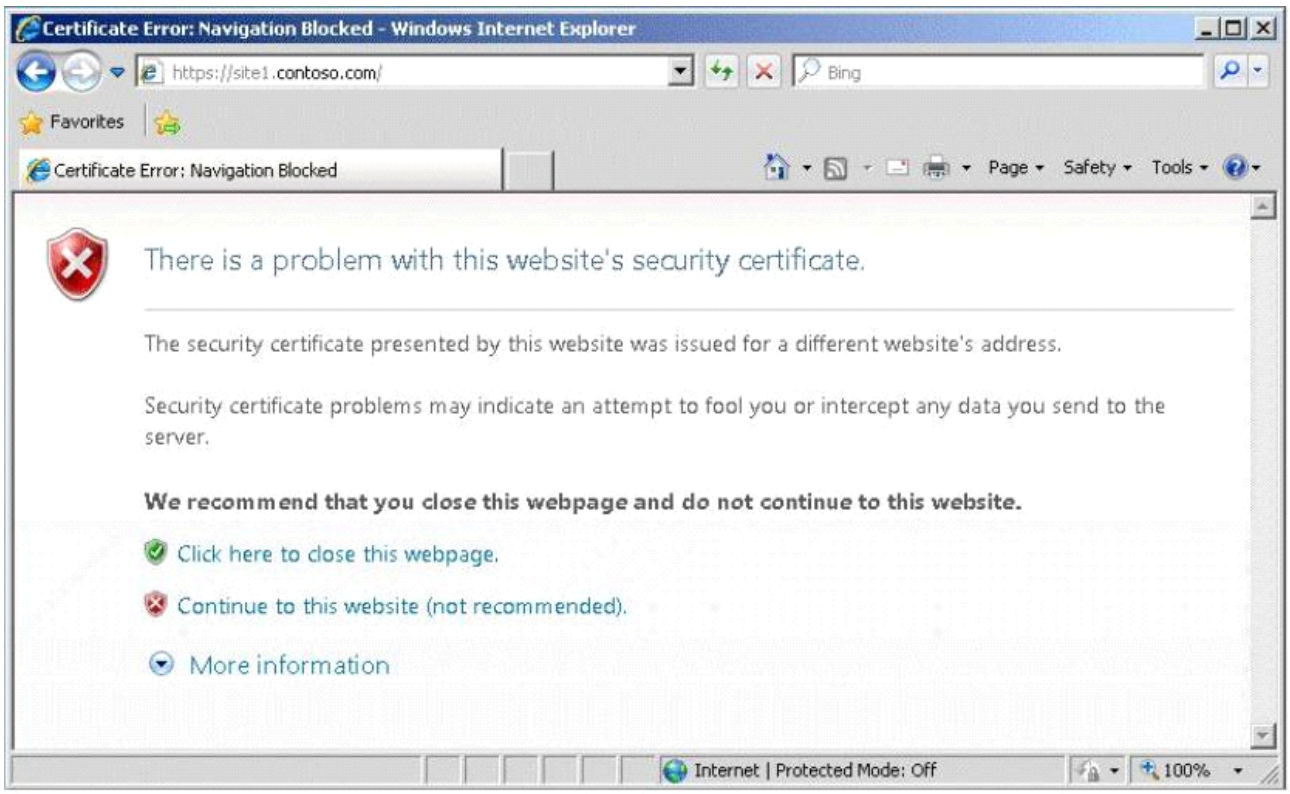
Explanation:
Ref:
http://technet.microsoft.com/en-us/library/cc770764(v=ws.10).aspx

Question: 362

Your network contains an enterprise certification authority (CA). You have a server named Server1 that has the Web Server (IIS) server role installed. Server1 has a website named Site1. Users access the website by using the following URLs:

- https://web
- https://sitel.contoso.com

The users report that they receive the error message shown in the exhibit. (Click the Exhibit button.)



You need to request a Subject Alternative Name (SAN) certificate for Server1. Which tool should you use?

A. Internet Information Services (IIS) 6.0 Manager
B. Local Security Policy
C. Certificates
D. Internet Information Services (IIS) Manager

E. Certification Authority

Answer: C

Explanation:
Ref:
http://technet.microsoft.com/library/ff625722.aspx

Question: 363

You have a failover cluster that uses Cluster Shared Volumes (CSV). The cluster hosts two virtual machines (VMs) named VM1 and VM2. The cluster contains five networks. The networks are configured as shown in the following table.

Network name	Metric
Network1	1,000
Network2	1,100
Network3	1,200
Network4	10,000
Network5	10,100

You need to ensure that all of the network traffic related to Hyper-V live migration of the VMs occurs on Network3. What should you do?

A. Set the metric of Network3 to 500.
B. Set the metric of Network3 to 10,200.
C. From Hyper-V Manager, modify the properties of VM1 and VM2.
D. From Failover Cluster Manager, modify the properties of VM1 and VM2.

Answer: D

Explanation:
Ref:
http://technet.microsoft.com/en-us/library/ff182335(v=ws.10).aspx
http://marckean.wordpress.com/2011/04/12/hyper-v-cluster-network-configuration/

Question: 364

You are evaluating whether to purchase Windows Server 2008 R2 Service Pack 1 (SP1). Several weeks ago, you installed Windows Server 2008 R2 SP1 on a server. During the installation, you did not enter a product key. You need to identify how many days remain until the license status of the server will change to Unlicensed. Which tool should you use?

A. Wevutil.exe
A. Windows Activation
C. Computer Management
D. Action Center

Answer: B

Explanation:

Ref:
http://www.windowsvalley.com/is-windows-activated-check-windows-activation-status/

Question: 366

Your network contains an Active Directory domain named adatum.com. The domain contains a server named Servers that runs Windows Server 2008 R2 Service Pack 1 (SP1). Server5 is configured as a file and print server. Server5 contains a RAIDS volume named Volume1. Volume1 contains four disks. You replace one of the disks in Volume1. You need to ensure that the new disk is added to Volume1. Which Diskpart command should you run?

A. create
B. online
C. break
D. filesystems
E. list
F. compact vdisk
G. rescan
H. assign
I. GPT
J. remove
L. merge vdisk
M. recover
N. repair
O. add
P. retain
Q. attach vdisk
R. offline
S. expand vdisk
T. extend
U. attributes
V. active
W. automount
X. format

Answer: N

Explanation:
Ref:
http://technet.microsoft.com/en-us/library/cc766465(v=ws.10)

Question: 367

You have a Remote Desktop Session Host (RD Session Host) server farm. All of the RD Session Host servers use Per Device licensing mode. You have 100 Remote Desktop Services client access licenses (RDS CALs). Your network contains 100 users. Each user has a desktop computer. Twenty client computers run Windows XP Professional Edition, 20 client computers run Windows Vista Professional, and 60 client computers run Windows 7 Enterprise. All of the users use RemoteApps that are published in the RD Session Host farm. You replace the Window XP client computers with new desktop computers that run Windows 7 Professional. You replace the Windows Vista client computers with new desktop computers that run Windows 7 Enterprise. Your company hires 10 new employees. For each new employee, the company purchases a new laptop that run Windows Vista Ultimate. You need to identify the total

number of RDS CALs the company must purchase to ensure that all of the client computer are licensed to access the Remote Desktop servers. The solution must minimize costs. How many RDS CALs should the company purchase?

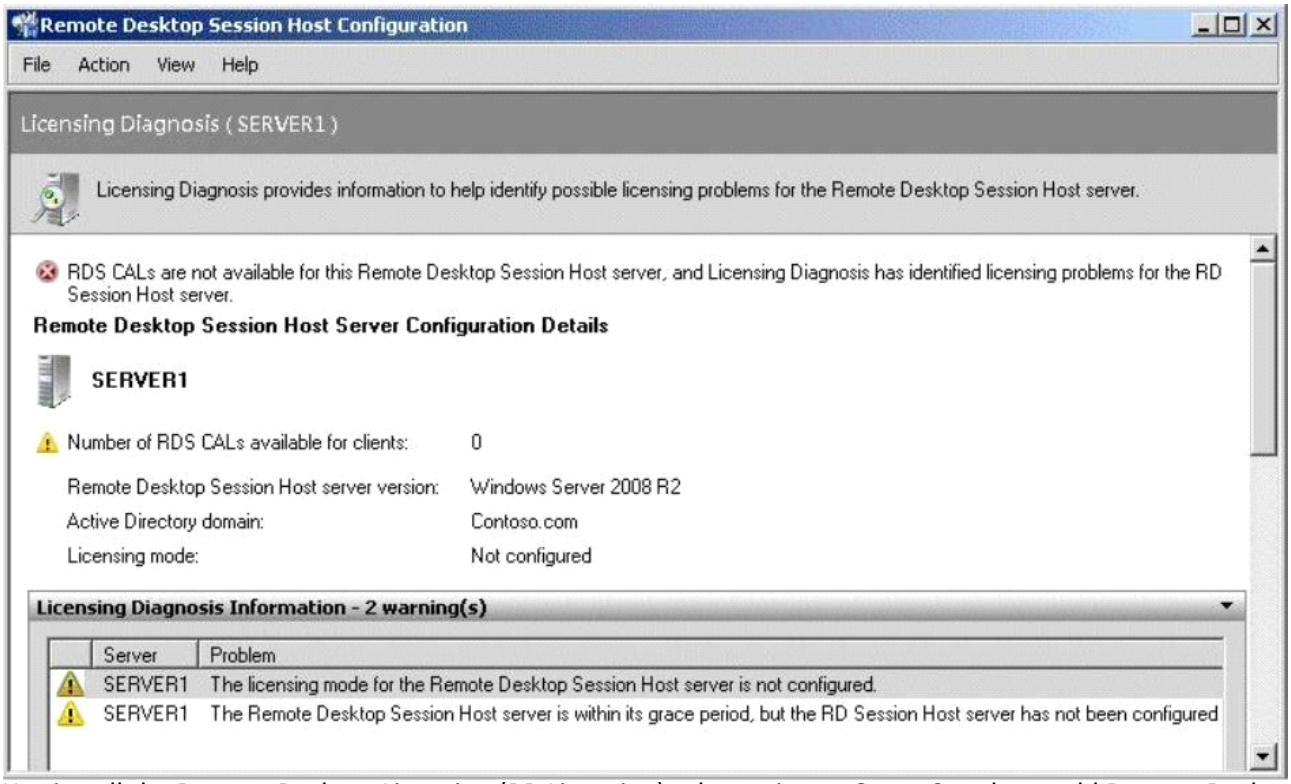
A. 50
B. 20
C. 10
D. 30

Answer: C

Explanation:
Every device needs an RDS-CAL whatever operating system it's running. The company will end up with 110 computers so 10 additional CALs are required.
Explanation:
Ref:
http://www.microsoft.com/en-us/server-cloud/windows-server/remote-desktop-services-buy.aspx

Question: 368

Your network contains an Active Directory domain named contoso.com. The domain contains two member servers named Server1 and Server2. You install the Remote Desktop Session Host (RD Session Host) role service on Server1. You open Remote Desktop Session Host Configuration as shown in the exhibit. (Click the Exhibit button.)



You install the Remote Desktop Licensing (RD Licensing) role service on Server2 and you add Remote Desktop Services client access licenses (RDS CALs) to Server2. You need to resolve the licensing error on Server1. Which tool should you use?

A. Remote Desktop Licensing Manager
B. Remote Desktop Connection Manager
C. Remote Desktop Session Host Configuration

D. Remote Desktop Services Manger

Answer: C

Explanation:
Ref:
http://technet.microsoft.com/en-us/library/cc754487.aspx

Question: 369

Your network contains a server named Server1 that has the Remote Desktop Services (RDS) server role installed and the Remote Desktop Session Host (RD Session Host) role service installed. You have a line-of-business application named App1 that runs on Server1. App1 accesses a database application named App2. App2 does not support multiple connections from the same IP address. Users access App1 by using Remote Desktop sessions. You discover that only one user can access App1 at a time. You need to ensure that at least 10 users can access App1 simultaneously. What should you do? (Each correct answer presents part of the solution. Choose two.)

A. Configure Server1 to use 10 static IP addresses.
B. Add a DHCP server to the same subnet as Server1.
C. On Server1, enable Remote Desktop IP Virtualization.
D. On Server1, configure the RDP-Tcp Properties.
E. Configure Server1 to obtain an IP address automatically.

Answer: A, C

Explanation:
Ref:
http://technet.microsoft.com/en-us/library/dd759263.aspx

Question: 370

Your network contains a server named Server1 that has the Web Server (IIS) server role installed. You need to ensure that the IIS configuration of Server1 backed up daily. The solution must minimize the size of the backup. What should you do?

A. From Windows Server Backup, create a custom bsckup configuration that backs up the system state.
B. Create a scheduled task that runs Get-WebConfiguration.
C. Create a scheduled task that runs iisbback.vbs.
D. From Windows Server Backup, create a custom bsckup configuration that backs up the %Windows%\system32\Inetsrv\config folder.

Answer: D

Question: 371

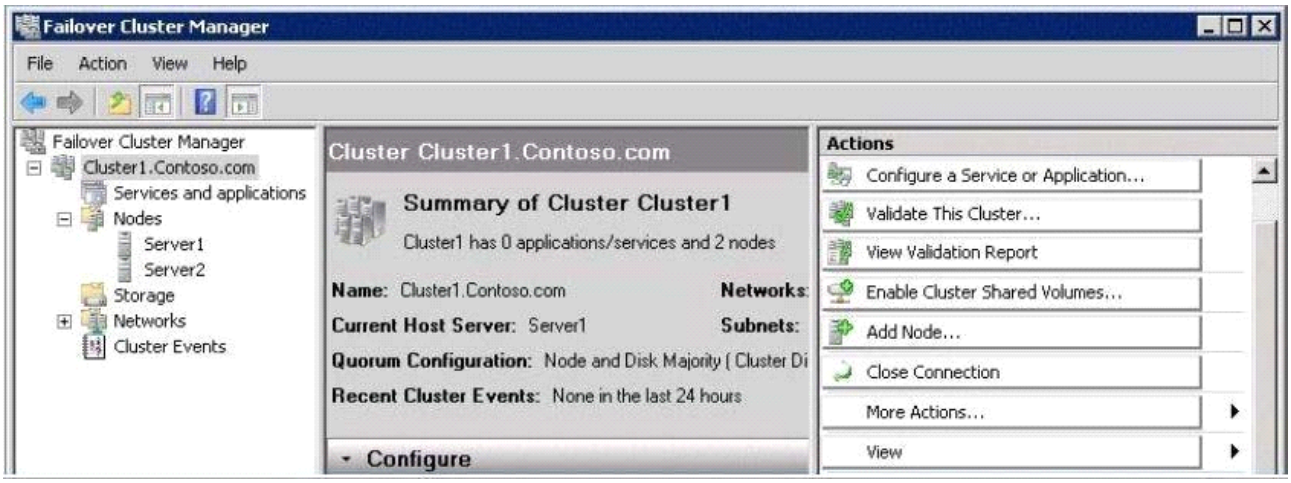
You are evaluating whether to purchase Windows Server 2008 R2 Service Pack 1 (SP1). Several weeks ago, you installed Windows Server 2008 R2 SP1 on a server. During the installation, you did not enter a product key. You need to identify how many days remain until the license status of the server will change to Unlicensed. Which tool should you use?

A. Slmgr.vbs
B. Computer management
C. Wevutil.exe
D. System Configuration

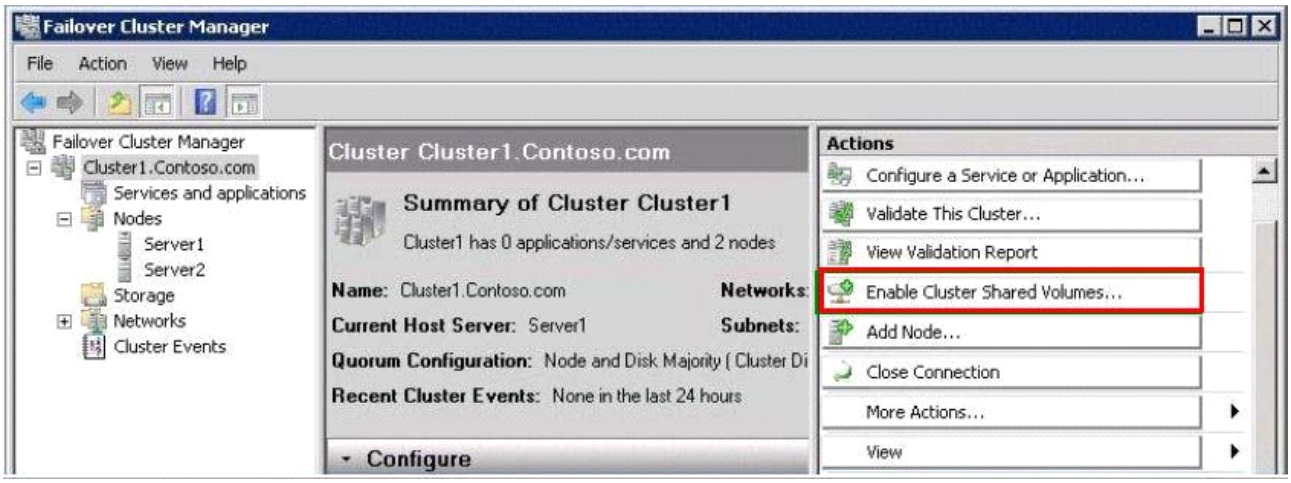
Answer: A

Question: 372
HOTSPOT

Your network contains two Hyper-V hosts named Server1 and Server2. Server1 and Server2 belong to a failover cluster. Server1 and Server2 are connected to the same 2-terabyte logical unit number (LUN). The cluster will host 20 highly available virtual machines (VMs). You need to ensure that the VMs can fail over independently. Which action should you select from Failover Cluster Manager?
To answer, select the appropriate action in the answer area.

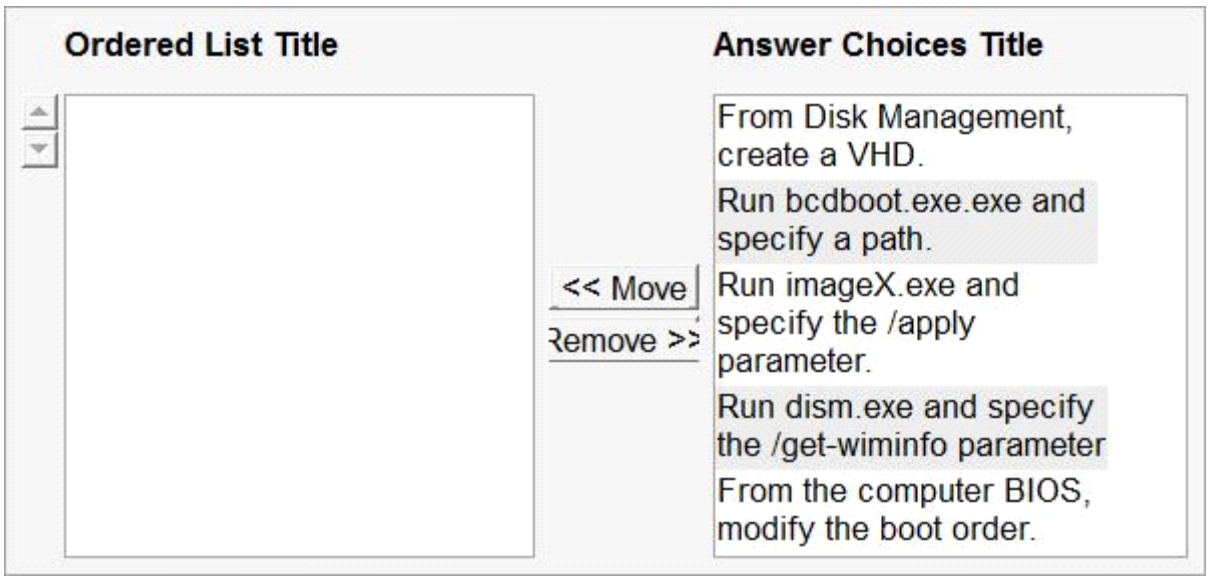


Answer:



Question: 373 DRAG DROP

You have a test computer named Server1 that runs Windows Server 2008 R2 Service pack 1 (SP1) Standard. The Windows Server 2008 R2 SP1 installation media is available on Server1. You need to configure Server1 to dual boot to Windows Server 2008 R2 SP1 Enterprise by using a virtual hard disk (VHD). What should you do?
To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

From Disk Management, create a VHD.
Run imageX.exe and specify the /apply parameter.
Run bcdboot.exe and specify a path.

Question: 374

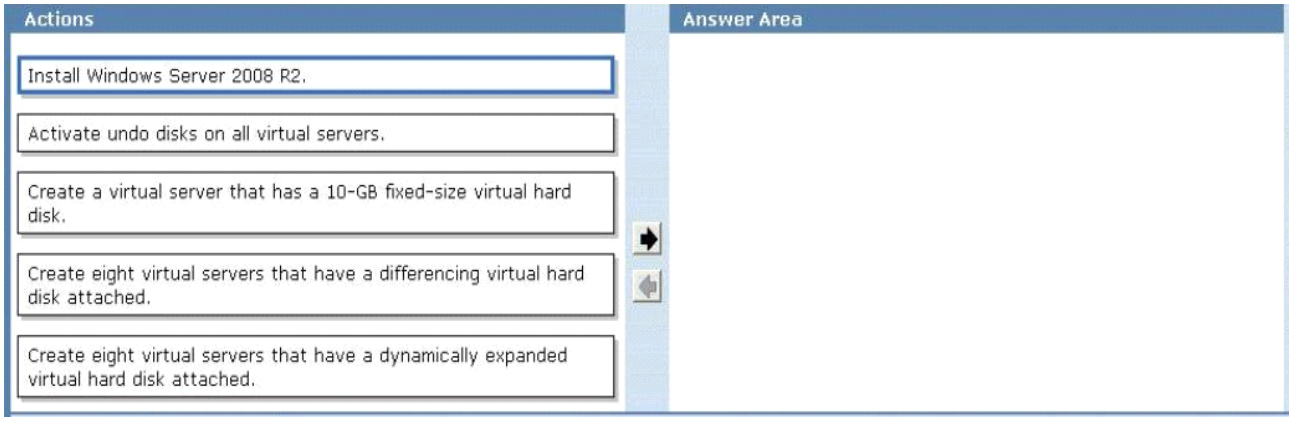
Your network contains an Active Directory forest. Microsoft Exchange Server 2010 is deployed in the forest. You have a server named Server1 that has Microsoft SharePoint Foundation installed. You need to ensure that users can receive e-mail notifications when the SharePoint content is modified. What should you do?

A. Install the SMTP Server feature.
B. Configure the Send To Connections.
C. Configure the outgoing e-mail settings.
D. Configure the incoming e-mail settings.

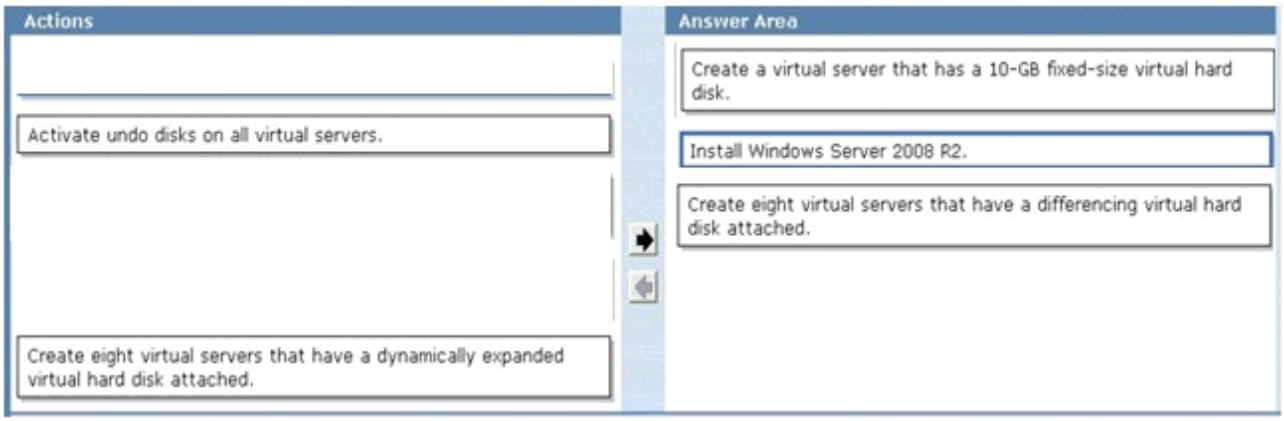
Answer: C

Question: 375

DRAG DROP
Your company has a server named VS1 that runs Windows Server 2008 R2 and Hyper-V. You want to create eight virtual servers that run Windows Server 2008 R2 and configure the virtual servers as an Active Directory forest for testing purposes. You discover that VS1 has only 30 GB of free hard disk space. You need to install the eight new virtual servers on VS1. What should you do? (To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.)



Answer:



Question: 376

You are evaluating whether to purchase Windows Server 2008 R2 Service Pack 1 (SP1). Several weeks ago, you installed Windows Server 2008 R2 SP1 on a server. During the installation, you did not enter a product key. You need to identify how many days remain until the license status of the server will change to Unlicensed. Which tool should you use?

A. Wevutil.exe
B. Slmgr.vbs
C. Msinfo32.exe
D. Act.exe

Answer: B

Question: 377

Your network contains a server named Server1 that runs Windows Server 2008 R2 Service Pack 1 (SP1). Server1 contains two dynamic disks named Disk1 and Disk2. Disk1 has a volume that contains critical data. Disk2 does not contain a volume. You need to create a mirror of the volume on Disk1. Which Diskpart command should you run?

A. format
B. retain
C. merge vdisk

D. attributes
E. add
F. break
G. GPT
H. compact vdisk
I. recover
J. active
K. rescan
L. extend
M. detach vdisk
N. offline
O. repair
P. automount
Q. remove
R. online
S. filesystems
T. assign
U. list
U. expand vdisk
V. create
W. attach vdisk

Answer: V

Reference: http://technet.microsoft.com/en-us/library/gg252557%28v=ws.10%29.aspx

Question: 378

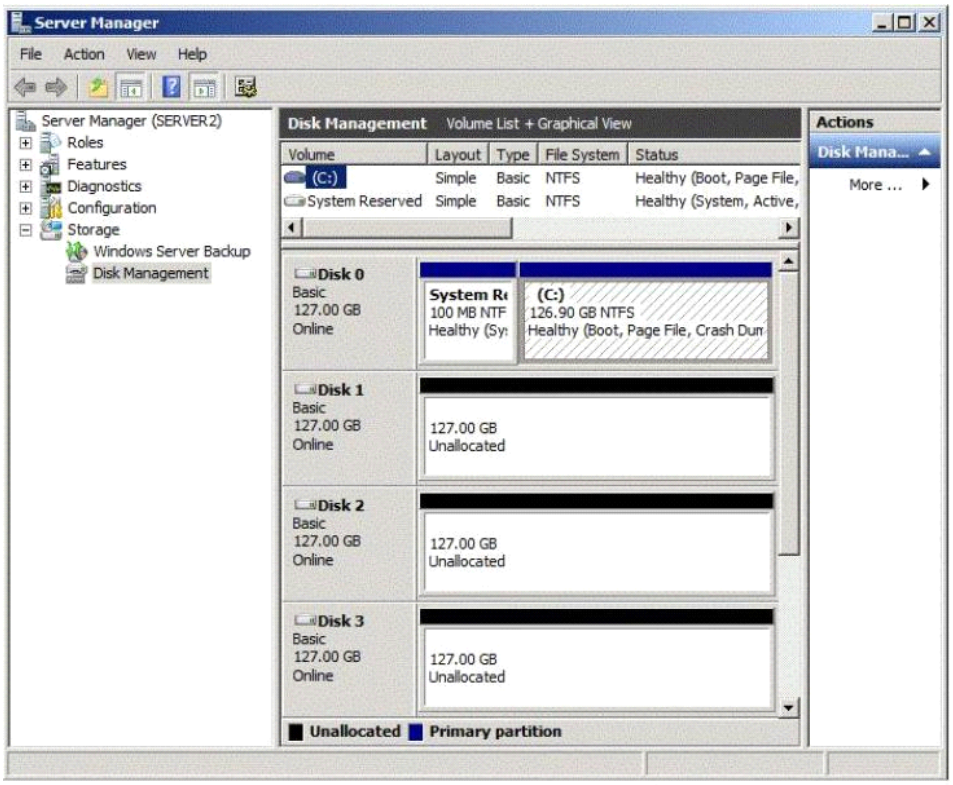
A server that runs Windows Server 2008 R2 has the Hyper-V server role installed. You create a new virtual machine (VM) and perform an installation of Windows Server 2003 on the VM. You need to ensure that you can access files on the Hyper-V server from the VM. You must also prevent access to the external network from the VM. What should you do?

A. On the VM, install the Microsoft Loopback adapter.
B. On the Hyper-V server, enable the Multipath I/O feature.
C. On the VM, install Microsoft Hyper-V Integration Components.
D. On the Hyper-V server, install the Microsoft Loopback adapter.

Answer: C

Question: 379

Your network contains a server named Server2 that runs Windows Server 2008 R2 Service Pack 1 (SP1). Server2 has the Hyper-V server role installed. The disks on Server2 are configured as shown in the exhibit. (Click the Exhibit button.)



You create a new virtual machine (VM) named VM1. You plan to install Windows Server 2008 R2 SP1 on VM1. You need to configure Disk 2 on Server2 as the system drive of VM1. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. On VM1, add a virtual hard disk (VHD) to an IDE controller.
B. On VM1, add a virtual hard disk (VHD) to an SCSI controller.
C. Convert Disk 2 to a dynamic disk.
D. On VM1, add a physical hard disk to an SCSI controller.
E. On VM1, add a physical hard disk to an IDE controller.
F. Take Disk 2 offline.
G. Convert Disk 2 to a GPT disk.

Answer: AF

Question: 380

Your network contains an Active Directory domain named contoso.com. You publish a RemoteApp named Appl. The Remote Desktop Connection (.rdp) file for App1 is unsigned. When a user named User1 runs App1 from the Remote Desktop Web Access (RD Web Access) website, User1 is prompted for credentials. You need to prevent users from being prompted for credentials when they run Appl. What should you do?

A. Enable the Allow Delegating Default Credentials Group Policy setting.
B. Enable the Assign a default domain for logon Group Policy setting.
C. Configure the SSL Settings for the RDWeb virtual directory.
D. Modify the Authentication Settings for the RDWeb virtual directory.

Answer: A

Question: 381

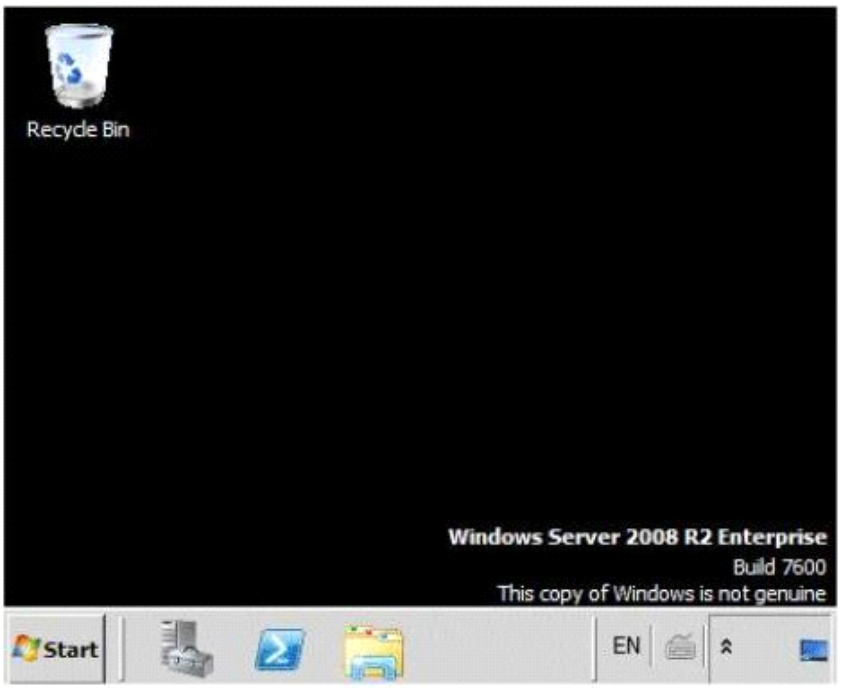
Your network contains an Active Directory domain named contoso.com. The domain contains five Remote Desktop Session Host (RD Session Host) servers and one Remote Desktop license server. You need to ensure that all of the RD Session Host servers use Per User licensing mode. What should you do? (Each correct answer presents a complete solution. Choose two.)

A. On the Remote Desktop license server, modify the discovery scope.
B. On each RD Session Host, modify the license settings.
C. On the Remote Desktop license server, modify the connection method.
D. On each RD Session Host, modify the user logon mode setting.
E. From a Group Policy object (GPO), enable the Set the Remote Desktop licensing mode setting.

Answer: AE

Question: 382

Your network contains an Active Directory domain. The domain contains a Key Management Service (KMS) host. The network has a perimeter network and an internal network. The network contains 1,000 client computers. All of the client computers receive their IP address from a DHCP server. You deploy a new server named Server1 by using a corporate image of Windows Server 2008 R2 Service Pack 1 (SP1). You configure Server1 as a member of a workgroup. You move Server1 to the perimeter network and you configure Server1 to use an external DNS server. Six months later, when you log on to Server1, you discover a message on the lower-right corner of the desktop as shown in the exhibit. (Click the Exhibit button.)



You need to ensure that the message does not appear on the desktop. What should you do?

A. From the command prompt, run djoin.exe.
B. From Windows Activation, click Activate Windows online now.
C. From Desktop Background, change the desktop background to solid white.
D. From the command prompt, run slmgr.vbs.

Answer: D

Question: 383

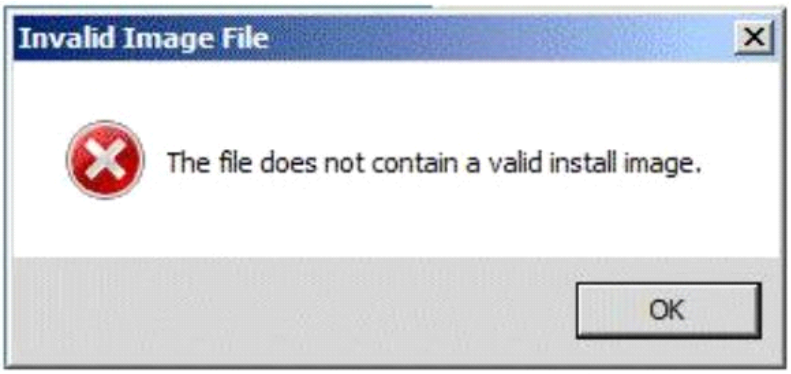
You are evaluating whether to purchase Windows Server 2008 R2 Service Pack 1 (SP1). Several weeks ago, you installed Windows Server 2008 R2 SP1 on a server. During the installation, you did not enter a product key. You need to identify how many days remain until the license status of the server will change to Unlicensed. Which tool should you use?

A. Computer Management
B. Msinfo32.exe
C. Action Center
D. Slmgr.vbs

Answer: B

Question: 384

Your network contains a server named WDS1 that has the Windows Deployment Services (WDS) server role installed. WDS1 is used to deploy Windows 7. You create a virtual hard disk (VHD) file that contains an installation of Windows Server 2008 R2 Service Pack 1 (SP1), From the Windows Deployment Services console, you attempt to add the VHD file, and you receive the error message shown in the exhibit. (Click the Exhibit button.)



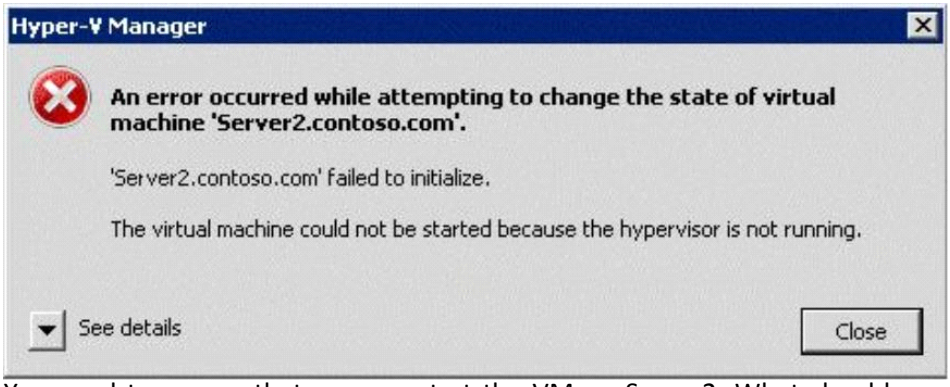
You need to ensure that you can deploy the VHD file by using WDS. What should you do?

A. Run vvdsutil.exe and specify the update-serverfiles parameter.
B. Run wdsutil.exe and specify the add-image parameter.
C. Run imagex.exe and specify the /apply parameter.
D. Run imagex.exe and specify the /append parameter.

Answer: B

Question: 385

Your network contains a server named Server2 that has the Hyper-V server role installed. Server2 has a single-core x64 processor, 4 GB of RAM, and a 500-GB hard disk drive. You create a virtual machine (VM) on Server2 and you assign the VM 1 GB of memory. When you attempt to start the VM, you receive the error message shown in the exhibit. (Click the Exhibit button.)



You need to ensure that you can start the VM on Server2. What should you do on Server2? (Each correct answer presents part of the solution. Choose two.)

A. Add more physical memory.
B. Enable hardware-assisted visualization in the system BIOS.
C. Add an additional hard disk drive.
D. Enable Data Execution Prevention (DEP) in the system BIOS.
E. Modify the Data Execution Prevention (DEP) settings from the system properties.
F. Create one virtual network.

Answer: CD

Question: 386

Your network contains a server named Server1 that runs Windows Server 2008 R2 Service Pack 1 (SP1). Server1 has a RAID5 volume. One of the disks in the RAID5 volume fails. You install a new disk on Server1. You need to add the new disk to the RAIDS volume. Which Diskpart command should you run?

A. active
B. add
C. assign
D. attach vdisk
E. attributes
F. automount
G. break
H. repair
I. compact vdisk
J. retain
K. create
L. detach vdisk
M. expand vdisk
N. extend
O. filesystems
P. format
Q. GPT
R. list
S. merge vdisk
T. offline
U. online
V. recover

W. remove
X. rescan

Answer: H

Question: 387

Your network contains a server named Server1 that runs Windows Server 2008 R2 Service Pack 1 (SP1). You attempt to create a folder on a volume and you receive the following error message:
"The media is write protected."
You need to ensure that you can create files and folders on the volume.
Which Diskpart command should you run?

A. active
B. add
C. assign
D. attach vdisk
E. attributes
F. automount
G. break
H. repair
I. compact vdisk
J. retain
K. create
L. detach vdisk
M. expand vdisk
N. extend
O. filesystems
P. format
Q. GPT
R. list
S. merge vdisk
T. offline
U. online
V. recover
W. remove
X. rescan

Answer: E

Question: 388

Your network contains an Active Directory domain named fabrikam.com. The domain contains a Web server named Web1 that runs Windows Server 2008 R2. You create four Web sites named Site1, Site2, Site3, and Site4. You associate each Web site to a different application pool. You need to view the amount of memory that each application pool is currently using. Which feature should you use?

A. Management Service
B. HTTP Response Headers
C. Worker Processes

D. Request Filtering

Answer: C

Question: 389

Your network contains a Web server that runs Windows Server 2008 R2. The server has a single IP address. You plan to create several Web sites. You need to ensure that each Web site is accessible over TCP port 80. What should you configure?

A. the ISAPI Filters for each site
B. the Request Filtering settings for the server
C. the host headers for each site
D. the bindings for each site

Answer: C

Question: 390

Your network contains a Web server named Web1 that runs Windows Server 2008 R2. Web1 is located on the perimeter network. Web contains a Web site named Public. You need to prevent the Public Web site from responding to requests that originate from the internal network. Which feature should you configure?

A. IP Address and Domain Restrictions
B. Authorization Rules
C. Authentication
D. IIS Manager Permissions

Answer: A

Question: 391

Your network contains an Active Directory domain named adatum.com. The domain contains a server named Servers that has the Remote Desktop Services (RDS) server role installed and all of the RDS role services installed. Servers is configured as a file server and a Remote Desktop services server. You need to identify the number of Remote Desktop Services client access licenses (RDS CALs) on Servers. Which tool should you use?

A. Regedit
B. Mstsc
C. Netsh
D. Rdpinit
E. Dism
F. Rdpsign
G. Remote Desktop Connection Manager
H. Remote Desktop Session Host Configuration
I. Remote Desktop Gateway Manager
J. Windows System Resource Manager (WSRM)
K. Remote Desktop Services Manager

Answer: H

Question: 392

Your network contains a server named Server1 that has the Streaming Media Services server role installed. Server1 has the WMS HTTP Server Control Protocol plug-in and the WMS Server RTSP Control Protocol plug-in enabled. All client computers run Windows 7. Server1 hosts an on-demand publishing point that contains a welcome video for new employees. When a new employee is hired, the human resources department sends an email message to the employee. The message contains a link to the welcome video. You install the Web Server (IIS) server role on Server1 by using the default settings. You change the port of the WMS HTTP Server Control Protocol plug-in to 1450. Human resources reports that the link to the welcome video no longer works. You need to ensure that the new employees can access the welcome video by using the link in the email message. What should you do? (Each correct answer presents a complete solution. Choose three.)

A. Instruct human resources to update the link in the email message to use http://serverl: 1450.
B. On Server1, disable the Default Web Site.
C. Instruct human resources to update the link in the email message to use rtsp://serverl.
D. Instruct human resources to update the link in the email message to use mms://serverl.
E. On Server1, bind the HTTP protocol of the Default Web Site to port 1450.
F. On Server1, disable the WMS Server RTSP Control Protocol plug-in.

Answer: ABC

Question: 393

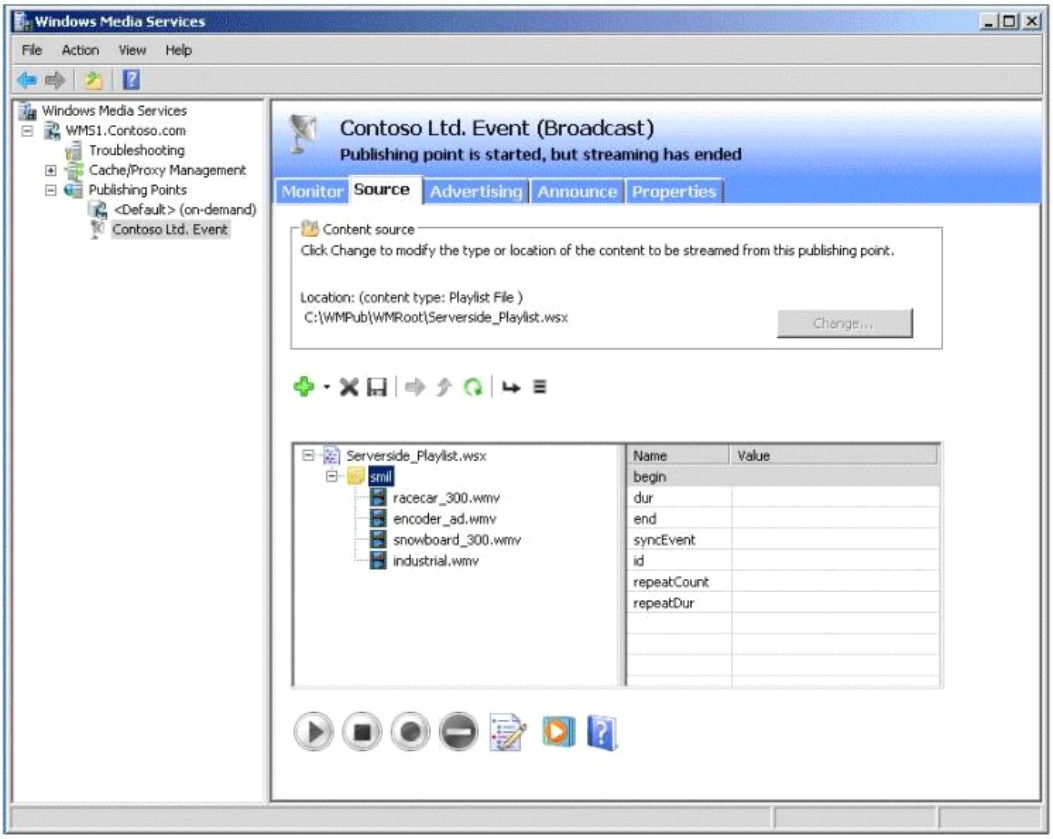
Your network contains a server named Server1 that has Microsoft SharePoint Foundation 2010 installed. You discover that users who access the SharePoint sites on Server1 by using a Windows Phone device are redirected to the desktop version of the sites rather than the mobile version. You need to ensure that the Windows Phone users are redirected automatically to the mobile version of the sites. What should you modify from Server1?

A. the site collection settings
B. the Web.config file
C. the site settings
D. the Compat.browsers file

Answer: D

Question: 394

Your network contains a server named WMS1 that has the Streaming Media Services server role installed. You have a publishing point as shown in the exhibit. (Click the Exhibit button.)



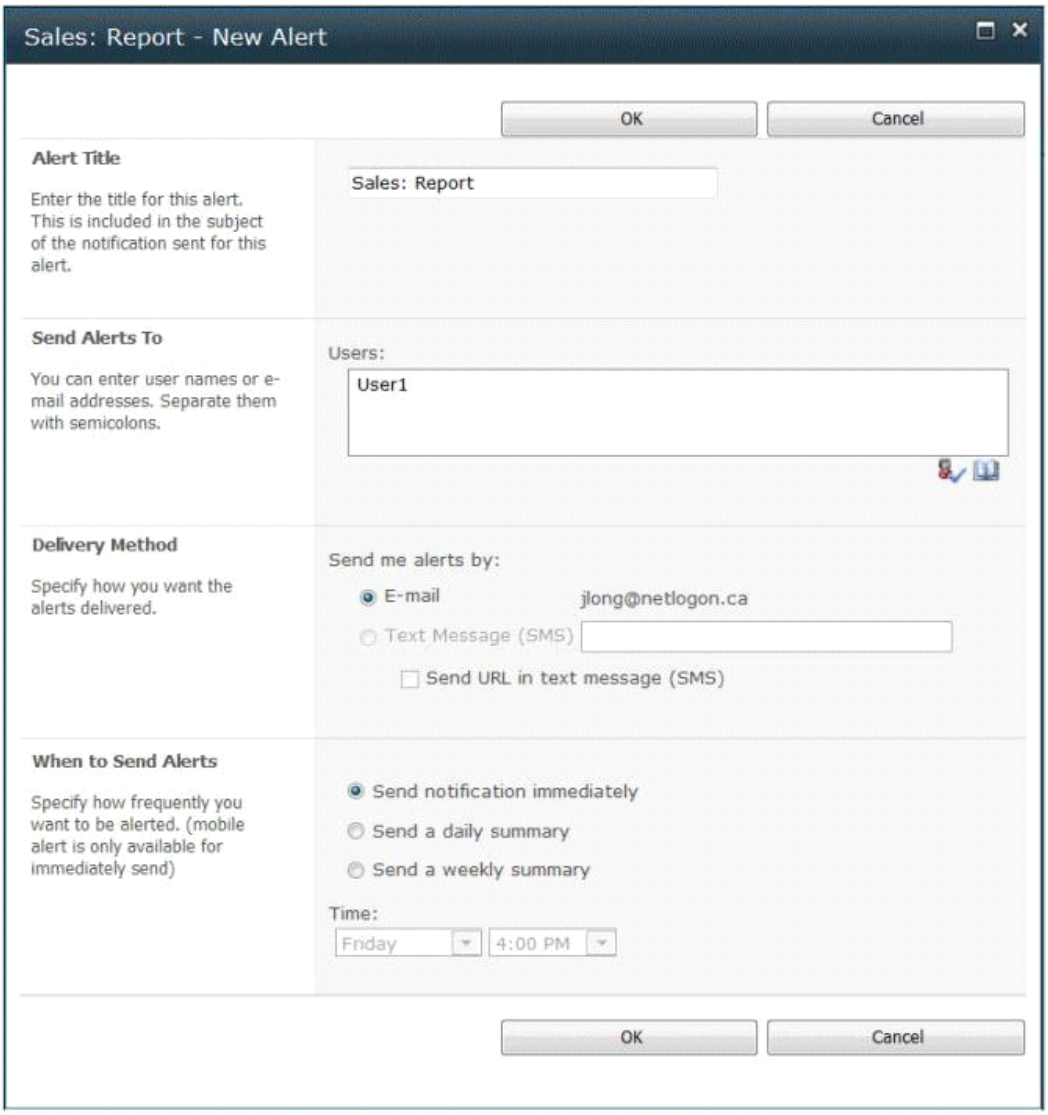
You create a new playlist named Contoso_Promo.wsx. You need to configure the Contoso Ltd. Event publishing point to use the Contoso_Promo.wsx playlist. What should you do first?

A. Disconnect all of the connections to the publishing point.
B. Stop the publishing point.
C. Configure stream splitting.
D. Stop Windows Media Services.

Answer: B

Question: 395

Your network contains a server named Server1 that has Microsoft SharePoint Foundation 2010 installed. Server1 has a site named Intranet. Intranet contains a custom list named Sales. A user named User1 attempts to create an alert for a list item in the Sales list as shown in the exhibit. (Click the Exhibit button.)



You need to ensure that Users1 can create alerts that are sent by text message. What should you do?

A. From Central Administration, create a new trust relationship.
B. From Central Administration, modify the mobile account settings.
C. From Site Settings, modify the site permissions.
D. From Site Settings, modify the RSS settings.

Answer: B

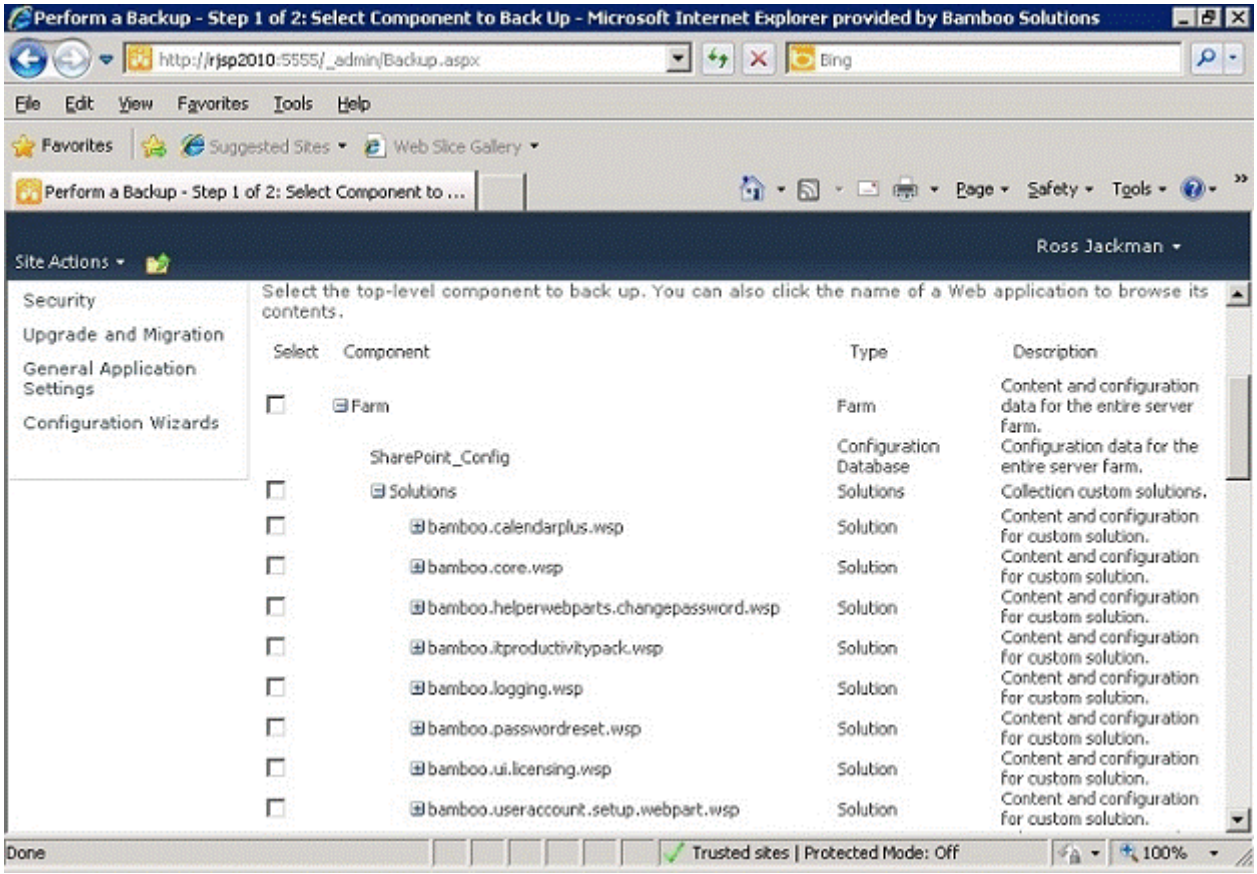
Question: 396

Your network contains a server that has Microsoft SharePoint Foundation 2010 installed. You need to back up the server farm configuration. The solution must minimize the size of the backup. What should you select from Backup and Restore in Central Administration?

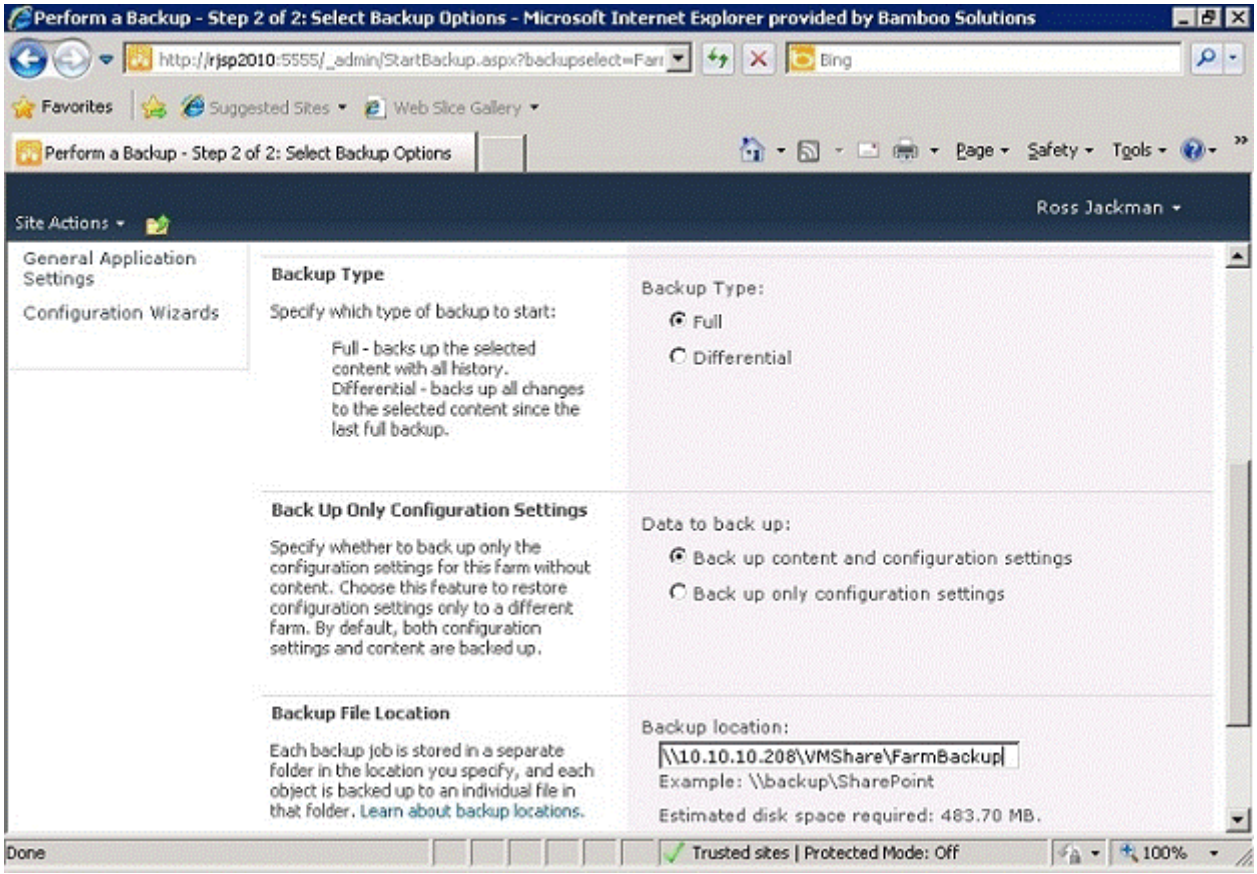
A. From Granular Backup, click Export a site or list.
B. From Granular Backup, click Perform a site collection backup.
C. From Farm Backup and Restore, click Perform a backup.
D. From Farm Backup and Restore, click Configure backup settings.

Answer: C

Explanation:
From Central Administration -> Backup and Restore -> Farm Backup and Restore, click Perform a Backup:



On this page, components to be included in the farm backup are selected.
A description of each component is included in the right-hand column.
Select the components to be backed up, then click Next.



Source:
http://community.bamboosolutions.com/blogs/sharepoint-2010/archive/2010/12/03/sharepoint-2010-cookbook-backing-up-datapart-1-farm-backup.aspx

Question: 397

Your network contains 20 servers that run Windows Server 2008 R2 and 800 client computers that run Windows 7 Enterprise. The network contains a server named Server1 that has the Key Management Service (KMS) installed. You discover that the Windows 7 client computers are not added to the current count on the KMS host. You need to ensure that all client computers are added to the KMS current count on Server1. What should you do?

A. On Server1, run slmgr.vbs /ato.
B. On Server1, run slmgr.vbs /rearm.
C. On each client computer, run slmgr.vbs /ato.
D. On each client computer, run slmgr.vbs /rearm.

Answer: D

Explanation:
Clients are not adding to the KMS count:
You need to run sysprep /generalize or slmgr.vbs /rearm to reset the client computer ID (CMID) and other product activation information. Otherwise, each client computer looks identical and the KMS host does not count them as separate KMS clients.
Source: http://technet.microsoft.com/en-us/library/cc303695.aspx