



Exam : 070-643

Title : Windows Server 2008 Applications
Infrastructure, Configuring

Ver : 01-30-2009

QUESTION 1:

Certkiller .com has a domain with Active Directory running on it. Windows Server 2008 is installed on all the servers. You plan to deploy an image to 50 computers with no operating system installed. For this you install Microsoft Windows Deployment Services on the network. When you install the image on a test computer, a driver error shows up on the screen. What would you do to change the image to include the correct driver?

- A. Configure and map the image file to the installation folder which hosts the correct driver
- B. Take the image file and mount it. Using the System Image Manager (SIM) utility, change the image file
- C. Open WDS server and update the driver through Device Manager
- D. Take the image file and mount it. Run the sysprep utility to get the correct driver
- E. None of the above

Answer: B

Explanation:

To include the correct driver, you should mount the image file and change it using System Image Manager (SIM). You need to include the correct driver in the image file so it will install with all the correct drivers.

You should not configure and map the image file to the installation folder hosting the correct driver because the image file is deployed in full. Windows Server 2008 will not consider the contents of the folder where image file resides. It will deploy the image file only with all its content

You cannot update the driver through Device Manager on WDS server. It has nothing to do with the image file.

You cannot mount the image file and run sysprep utility. Sysprep utility cannot get the correct driver for you and change the image file. Sysprep utility is related to WDS server and the deployment of images to the client computers.

QUESTION 2:

Certkiller .com has a server that runs Windows Server 2008. As an administrator at Certkiller .com, you install Microsoft Windows Deployment Service (WDS). While testing an image, you find out that the image is outdated. What should you do to remove the image from the server?

- A. Open the command prompt at WDS server and execute WDSUTIL/Remove-Image and /ImageType:install options
- B. Open the command prompt at WDS server and execute the WDSUTIL command with /Export-Image and /ImageType: install options
- C. Open the command prompt at WDS server and execute the WDSUTIL with

/Export-Image and /ImageType: boot options

D. Open the command prompt at WDS server and execute the WDSUTIL command with

/Remove-Image and /ImageType:boot options

E. All of the above

Answer: A

Explanation

To remove the image from the server, you should execute WDSUTIL/remove-image on the command prompt at WDS server. Then execute WDSUTIL/image-type:install command and install the new image. The WDSUTIL is a command specific to modify and view the images at WDS server. You need to remove the image and then install the updated one using these commands.

You cannot use the export-image parameter with WDSUTIL in this scenario. You have to remove the image not to export it to a folder.

You should not use the /image-type:boot parameter because you need to install a fresh image. You don't need to boot the service for this.

QUESTION 3:

Certkiller .com has four branch offices. To deploy the images, you install Microsoft Windows Deployment Services (WDS) on the network. Certkiller .com creates 4 images for each branch office. There are a total of 16 images for Certkiller .com. You deploy these images through WDS. A problem occurs in one branch office where the administrator reports that when he boots the WDS client computer, some of the images for his regional office does not show up in the boot menu. What should you do to ensure that every administrator can view all the images for his branch office?

A. Create separate image group for each branch office on the WDS server

B. Create unique organizational unit for each branch office and create profiles for each computer in the branch office

C. Organize a global group for each branch office and create profiles of each computer in a branch office

D. Create a Global Unique Identifier for each computer to recognize its branch office and connect it to the WDS server

E. None of the above

Answer: A

Explanation:

To ensure that every administrator can view all the images for his branch office, you should create separate image group for each branch office on WDS server. A separate image will enable all the administrators to view each image from their machine in the branch office.

You should not create an OU for each branch office. There is no logic in creating an OU for each branch office and profiles for each computer in the branch office.

You should not organize a global group for each branch office. A global group can host all the branch offices of Certkiller .com

QUESTION 4:

Microsoft Windows Deployment Services (WDS) is running on a Windows 2008 server. When you try to upload spanned image files onto WDS server, you received an error message.

What should you do to ensure that image files could be uploaded?

- A. Combine the spanned image files into a single WIM file
- B. Grant the Authenticated Users group Full Control on the \REMINST directory
- C. Run the WDSutil/Convert command from command line 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 line on WDS server
- E. None of the above

Answer: A

Explanation:

When you try to upload spanned image files onto WDS server, you received an error message because you can only mount a single WIM file once for read/write access and therefore you need to combine the spanned image files into a single WIM file to correct the problem.

Reference: The Desktop Files The Power User's Guide to WIM and ImageX / Using /mount, /mountw, and /delete

<http://technet.microsoft.com/en-us/magazine/cc137794.aspx>

QUESTION 5:

Certkiller .com has upgraded all servers in its network to Windows Server 2008. Certkiller .com also directed you to install Windows Vista on all client machines. You install Windows Vista on client machines and Windows Server 2008 on the servers. You use Multiple Activation Key (MAK) to activate the new operating systems on the network. You use proxy activation over the internet using Volume Activation Management Tool (VAMT). The Windows Vista on client computers were successfully activated using this method but the Windows Server 2008 failed to activate using VAMT. What should you do to ensure that the Windows Server 2008 is activated on all the servers?

- A. Contact Microsoft Support Center and activate the Windows server 2008 over the phone
- B. Upgrade VAMT using Windows Server 2008 RTM for VAMT to function with Windows Server 2008 Volume Licensing
- C. Upgrade VAMT using Key Management Service (KMS) for Windows Server 2008

RTM to function with Windows Server 2008 Volume Licensing

D. Contact Microsoft Support Center and activate Windows Server 2008 over the internet using MAK only

E. All of the above

Answer: B

Explanation

To ensure that the Windows Server 2008 is activated on all the servers, you should upgrade VAMT using Windows Server 2008 RTM for VAMT. You have to update VAMT at Windows Server 2008 RTM for VAMT to function with Windows Server 2008 volume licensing. VAMT (Volume Activation Management Tool) is a volume licensing tool for all flavors of Windows Vista.

There are various activation methods available for volume licensing. These methods use two types of customer specific keys: Multiple Activation Key (MAK) and Key Management Service (KMS).

The VAMT tool is used to activate the license through proxy over internet. VAMT is a tool for Windows Vista and to use it for Windows Server 2008, it needs an update.

QUESTION 6:

Certkiller .com has added 5 servers to its network. As an administrator at Certkiller .com, you install Windows Server 2008 Enterprise edition on two servers and Windows Server 2008 storage server enterprise on other two servers. You want to automatically activate both editions of Windows Server 2008 without any administrator or Microsoft intervention. You also want the activation to occur every 6months. Which volume activation service should you use to automatically activate both editions of Windows Server 2008?

A. Multiple Activation Key(MAK)

B. Volume Activation Management Tool (VAMT)

C. Volume Activation 1.0 (VA 1.0)

D. Key Management Service (KMS)

E. None of the above

Answer: D

Explanation

You should use KMS to activate both editions of Windows Server 2008. KMS automatically activates Windows Vista and Windows Server 2008. Computers that are been activated by KMS are required to reactivate by connecting to a KMS host at least once every six months.

The VL editions of Windows Serve 2008 and Windows Vista are installed as KMS clients by default. The clients can automatically discover the KMS hosts on the network with a properly configured KMS infrastructure. The clients can also activate using KMS infrastructure without administrative or user intervention.

QUESTION 7:

Certkiller has main office and a BRanch office. Main office is running 20 Windows Server 2008 computers and 125 computers running Microsoft Windows XP Professional. Branch office is running 3 Windows Server 2008 computers and 50 Windows XP Professional computers running on its network.

Computers in the main office have access to Internet. All servers are having the same security configuration and there are no plans in near future to add new servers or systems in the network.

You installed Volume Activation Management Tool (VAMT) on a server named Certkiller_DC1 in the main office and added all servers to VMAT server and configured the servers for Multiple Activation Key (MAK) independent activation. Servers at BRanch office are unable to activate Windows Server 2008. What should you do to activate Windows server 2008 on all servers?

- A. Install a Management Activation Key (MAK) server on the network
- B. Configure MAK Proxy activation on all servers in the BRanch office
- C. Configure Windows Management Instrumentation (WMI) Firewall Exception on all servers in the BRanch office
- D. Open VAMT on Certkiller_DC1 and export the Computer Information List (CIL). Send this file to Microsoft Technical support for activation
- E. None of the above

Answer: B

Explanation:

To activate Windows server 2008 on all servers, you need to configure MAK Proxy activation on all servers in the BRanch office. The MAK can be activated by using two methods, MAK Independent Activation and MAK Proxy Activation.

MAK Independent Activation is used when each computer is activated individually by connecting to Microsoft servers over the Internet or by telephone and MAK Proxy Activation is used when Volume Activation Management Tool (VAMT) is installed on a server and you need to activate multiple computers at the same time through a single connection to Microsoft servers over the Internet or phone.

Therefore, instead of MAK Independent Activation you need to use MAK Proxy activation on all servers in the BRanch office.

Reference: Frequently Asked Questions About Volume License Keys for Windows Vista and Windows Server 2008

<http://www.microsoft.com/licensing/resources/vol/ActivationFAQ/default.mspx>

QUESTION 8:

You are network administrator for Certkiller network. You configured a Windows server 2008 server named Certkiller_KM1 as Key Management Service (KMS) host. This server is also configured as Windows Sharepoint Services server. This location

has currently 18 computers having Windows Vista KMS client and you have added 10 more Windows Vista KMS client systems in the network recently. These 10 additional client computers are installed using Windows Vista image file. The KMS host is unable to activate any of the KMS client computers in the network. What should you do?

- A. Install KMS on a dedicated Windows Server 2008
- B. Run Sysprep /generalize on the Vista reference computer used to create image
- C. Run slmgr.vbs/rearm Vista reference computer used to create image
- D. Run slmgr.vbs/dli on the KMS host computer
- E. Run slmgr.vbs/cpri on the KMS host computer
- F. None of the above

Answer: B

Explanation:

To activate the KMS client computers in the network, you need to run the Sysprep /generalize on the Vista reference computer used to create image. sysprep/generalize is used to reset activation and other system-specific information as the last step before storing or capturing the VM image. If sysprep/generalize is not used, the activation timer will run down while the product is in storage and the KMS host will be unable to activate any of the KMS client computers in the network.

Reference: KMS host is unable to activate any of the KMS client computers in the network

<http://blog.windowvirtualization.com/virtualization/faq-virtualization-and-volume-activation-20>

QUESTION 9:

Certkiller .com has a server with single Active Directory domain. For security, Certkiller .com has an ISA 2006 server functioning as a firewall. You configure user access through virtual private network service by deploying the PPTP (Point-to-Point Tunneling Protocol). When a user connects to the VPN service, an error occurs. The error message says "Error 721: The remote computer is not responding." What should you do to ensure that the users connect to the VPN service?

- A. Open the port 2200 on the firewall
- B. Open the port 1423 on the firewall
- C. Open the port 1723 on the firewall
- D. Open the port 721 on the firewall
- E. All of the above

Answer: C

Explanation:

To ensure that users connect to VPN service, you should open the port 1723 on the

firewall. The port 1723 is a TCP port for PPTP tunnel maintenance traffic. For VPN connections, you need to open this port for PPTP tunnel maintenance traffic and permit IP Type 47 Generic Routing Encapsulation (GRE) packets for PPTP tunnel data to pass to your RRAS server's IP address.

You cannot open port 721. The port 721 on the firewall is a printer port so it is not related to VPN connection

QUESTION 10:

DRAG DROP

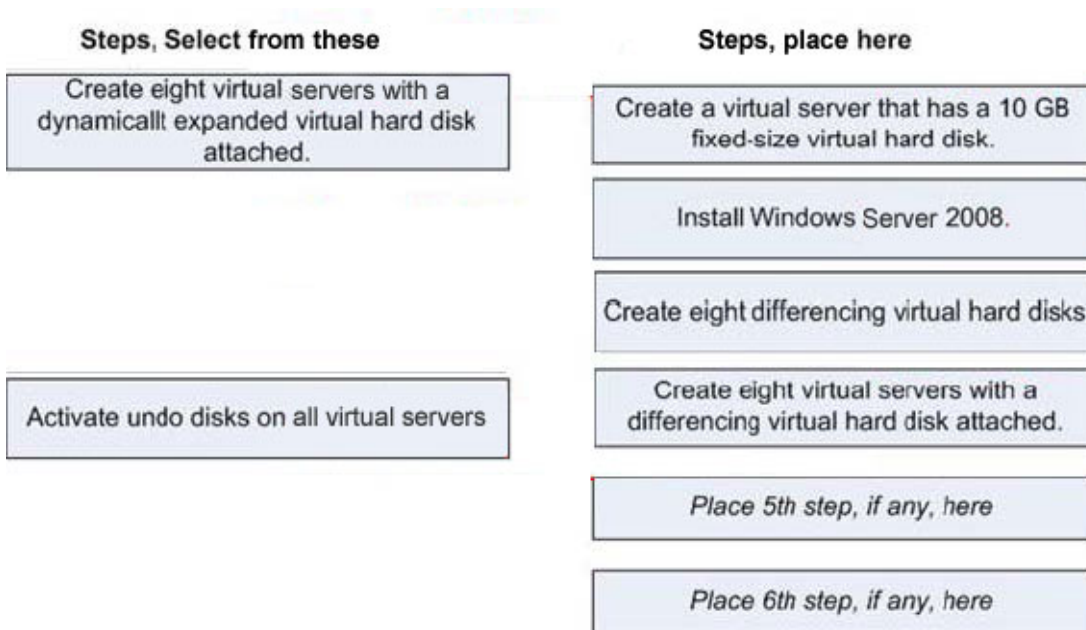
Certkiller has a server named CK1 that runs Windows Server 2008 and Microsoft Virtual Server 2005 R2.

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 in the Certkiller Lab. You discover that CK1 has only 30 GB of hard disk space that is free. You need to install the eight new virtual servers on CK1 .

From the steps shown, what steps need to be completed in a specific order?

Steps, Select from these	Steps, place here
Create eight virtual servers with a dynamically expanded virtual hard disk attached.	Place first step here
Install Windows Server 2008.	Place second step, if any, here
Create a virtual server that has a 10 GB fixed-size virtual hard disk.	Place third step, if any, here
Activate undo disks on all virtual servers	Place fourth step, if any, here
Create eight virtual servers with a differencing virtual hard disk attached.	Place 5th step, if any, here
Create eight differencing virtual hard disks	Place 6th step, if any, here

Answer:



Explanation:

To install the eight new servers on CK1 , 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 11:

When you create a virtual machine in Windows server 2008, the guest OS configuration (memory, disk, network, etc) could be saved into a file. What is the format of the file which stores the configuration details?

- A. HTML formatted file
- B. XML formatted file
- C. Text file
- D. Word file
- E. None of the above

Answer: B

Explanation:

The XML formatted file stores the guest OS configuration details such as memory, disk, and network to create the Virtual Machine.

Reference: Testing Windows Server 2008 using Virtual PC (step-by-step) / Create a Virtual Machine

<http://blogs.technet.com/josebda/archive/2007/08/05/testing-windows-server-2008-using-virtual-pc-step-by-step>

QUESTION 12:

Certkiller runs Microsoft virtual server 2005 R2 on a Windows Server 2008. This server hosts 5 virtual machines.

For some time, you are experiencing performance degradation. Upon investigation it is revealed that you are running low on disk space on the volume where virtual machine disk files are stored.

You plan to move some of the virtual disk image files onto other volume. What should you do?

- A. Shutdown virtual machine and Delete the symbolic link from the folder %systemroot%\ProgramData\Microsoft\Windows\virtualisation\Virtual Machines and then move VHD files to new volume
- B. Create a new symbolic link to the virtual machine's XML configuration file and then move VHD files to new volume
- C. Open the virtual machine's configuration file and update any references to physical paths and then move VHD files to new volume
- D. In the Windows Virtualization Management MMC console Move the virtual machines files to new volume
- E. None of the above

Answer: A

Explanation:

To move some of the virtual disk image files onto other volume, you need to shutdown virtual machine and Delete the symbolic link from the folder systemroot%\ProgramData\Microsoft\Windows\virtualisation\Virtual Machines and then move VHD files to new volume.

Windows Server 2008 Hyper-V stores a list of virtual machines in systemroot%\ProgramData\Microsoft\Windows\virtualisation\Virtual Machines folder. It also contains a set of symbolic links that are linked to the actual config files for each virtual machine. Therefore you need to shutdown virtual machine and Delete the symbolic link from the folder before moving files.

Reference: Moving a Windows Server 2008 Hyper-V virtual machine

<http://www.adopenstatic.com/cs/blogs/ken/archive/2008/01/14/15467.aspx>

QUESTION 13:

Certkiller .com has a server that runs Windows Server 2008. A server virtualization role service is installed on this server. It also hosts a virtual machine. The Virtual machine runs Windows Server 2008. You are planning to install a new application on the virtual machine. You have to ensure that you can restore the Virtual machine

to its original state if the application installation fails. What should you do to achieve this objective?

- A. Create a snapshot of the Virtual machine from the Virtualization Management Console
- B. Backup the Virtual machines using Windows Backup utility
- C. Save the state of the virtual machine through Virtualization Management Console
- D. Use a third-party backup software to backup the data on Virtual machine and put it on the server

Answer: A

Explanation

To ensure that you can restore the Virtual machine to its original state if an application installation fails, you should create a snapshot of the virtual machine using the Virtualization Management Console. You can always restore the virtual machines in its original state by using the snapshot you created.

QUESTION 14:

Certkiller .com has a server named CKS which runs Windows Server 2008 and Microsoft Hyper-V. You have installed two virtual machines on this server which runs Windows Server 2003. What should you do to configure the virtual machines to revert back to their original state in their event of system failure?

- A. Create a backup of .vmc files for each virtual machine using Windows backup utility
- B. On each virtual machine running Windows Server 2003, create a backup of all volumes
- C. Using Virtual Services Manager, take a snapshot of the virtual machines.
- D. Create restore points on each virtual machine by using the Windows Server 2003 system restore

Answer: C

Explanation

To configure the virtual machines to revert back to their original state in the event of system failure, you should create a snapshot of the virtual machines through Virtual services manager. You can revert back the VM to original state by using the snapshot you created.

QUESTION 15:

Windows Server 2008 is installed on two servers named CKS2 and CKS3. The Terminal services role is installed on both of these servers and the Terminal Services Gateway role is also installed on CKS3. Applications are published on CKS2 through Remote Desktop Connection

configuration file (.rdp file). Users download the .rdp files from CKS2 using TSWeb virtual directory.

You decide to reconfigure the applications on CKS2 to employ Terminal Services Gateway role on CKS3. You export the Remote program settings on CKS2 and import them on CKS3.

The users report that they cannot access remote applications installed on CKS3.

They can access remote applications on CKS2 through Terminal Services Gateway role on CKS3.

You try to find out the problem. During the process you have ensured that the application paths to both servers are identical. Which action should you perform to ensure that the users could access and use the remote applications on CKS3?

- A. Configure CKS3 to connect to CKS2 to access remote application files
- B. Install and configure the Terminal Services Session Directory feature on CKS3 and configure CKS2 to use this feature to for application files.
- C. Disable the User Authentication on CKS3 and implement it on CKS2
- D. Reconfigure the .rdp files on CKS3 and distribute the files to the users
- E. All of above

Answer: D

Explanation:

When you exported the Remote program settings on CKS2 and import them on CKS3, only the RemoteApp Programs list and deployment settings are exported or imported. Any .rdp files or Windows Installer packages that were created from the programs were not be exported or imported and therefore the users reported that they cannot access remote applications installed on CKS3.

To ensure that the users could access and use the remote applications on CKS3, you need to reconfigure the .rdp files on CKS3 and distribute the files to the users

Reference: Windows Server2008 Terminal Services RemoteApp Step-by-Step Guide /

To import the RemoteApp Programs list and deployment settings

http://download.microsoft.com/download/b/1/0/b106fc39-936c-4857-a6ea-3fb9d1f37063/Windows_Server_200

QUESTION 16:

You had installed Terminal services on a Windows 2008 Server. You installed several business applications on this server.

You now want all the users on the network to access these applications remotely. To achieve this, you added all applications to the RemoteApps list.

To ensure that malicious users are not able to access any applications listed in RemoteApps list what should you do?

- A. Remove the business applications from RemoteApps list
- B. Select the Do not allow users to start unlisted program on initial connection (Recommended) option in TSRemoteApp Manager on the Terminal Server tab under Connection settings

- C. Select Allow users to start both listed and unlisted program option on initial connection option in TSRemoteApp Manager on the Terminal Server tab under Connection settings.
- D. Uncheck the Make a remote desktop connection to this terminal server available in TS Web Access option on the Terminal Server tab in the RemoteApp Deployment Settings dialog box
- E. None of the above

Answer: B

Explanation:

To ensure that malicious users are not able to access any applications listed in RemoteApps list, you need to Select the Do not allow users to start unlisted program on initial connection (Recommended) option in TSRemoteApp Manager on the Terminal Server tab under Connection settings. This setting helps to protect against malicious users, or a user unintentionally starting a program from an .rdp file on initial connection
Reference: Windows Server 2008 Terminal Services RemoteApp Step-by-Step Guide / Configure terminal server settings
<http://technet2.microsoft.com/windowsserver2008/en/liBRary/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp>

QUESTION 17:

Certkiller .com has a network containing servers that run Windows Server 2008. To handle name resolution for the users, a server named CKDNS is configured as a DNS server on the network. CKDNS has an Active Directory Integrated zone that host DNS data for users on the network.

While monitoring the server, you find out that the primary zone on CKDNS contains some entries from a computer unknown and not part of the domain. What should you do to prevent this?

- A. Open the DNS server snap-in and right click on the DNS server node. Click on Scavenge resource records
- B. Set the DNS server to automatic scavenging of stale records
- C. In DNS manager snap-in and set the option to Set Aging/scavenging for all zones
- D. Open the properties of primary zone and select Secure Dynamic Updates Only option
- E. All of the above

Answer: D

QUESTION 18:

Certkiller .com has a server that runs Windows Server 2008. Terminal services role is installed on the server. As an administrator at Certkiller .com, you deploy a new application on the server. The application creates a file that has an extension of .bdc. You have to make sure that the users can launch application remotely from their

computer by double-clicking on the .bdc extension. What should you do to achieve this objective?

- A. Use Terminal Server Web Access website to configure the application as a published application
- B. Configure the remote desktop connection on the client computers to point the terminal services server
- C. Configure the Remote Desktop file to configure application as a published application
- D. Use Windows Installer package file to configure application as a published application

Answer: D

Explanation

To make sure that the users can launch application remotely from their computer by double-clicking on the .bdc extension, you should use Windows Installer package file to configure application as a published application

QUESTION 19:

Certkiller .com has an Active Directory domain. There are two servers named CKS1 and CKS2 that have Windows Server 2008 as their operating system. Terminal Services gateway role is active on CKS1 and Terminal Services role is active on CKS2.

The printers in the network support PostScript only. Users must have the facility to print on the printers that do not have prime driver support. What should you do to make sure that the Terminal Services provide primary printer support automatically?

- A. Configure a new group policy that supports terminal server fallback printer driver behavior as a setting and turn it to Default to PS if the server is unable to find any driver. Set the policy on all client machines in the domain
- B. Configure all printers to use PostScript on CKS2 and create a new group policy to support the printer instances. Add the policy on all client machines in the domain
- C. Delete the PostScript and install the driver for all the printers on all the client machines. Create a group policy that adds the printer automatically to all the servers and instate the policy on all client machines
- D. Configure a new group policy object (GPO) that supports Specify terminal server fallback printer driver behavior setting to Default to PS if one is not found option. Apply the GPO to CKS2
- E. None of the above

Answer: D

Explanation:

To make sure that the Terminal Services provide primary printer support automatically, you need to configure a new group policy object (GPO) that supports Specify terminal

server fallback printer driver behavior setting to Default to PS if one is not found option. Apply the GPO to CKS2. This setting allows the use of Adobe PostScript (PS) fallback printer driver by Terminal Server if no suitable printer driver can be found.

Reference: Terminal Services in Windows Server 2003 Service Pack 1 / New fallback printer driver capability

<http://technet2.microsoft.com/windowsserver/en/liBRary/2284b19b-30a6-42b5-9bd1-ff301f7248b01033.msp?m>

Reference: Terminal Services Printing / What existing functionality is changing

<http://technet2.microsoft.com/windowsserver2008/en/liBRary/484d57e7-feb4-4dcc-9d13-152c053516471033.msp>

QUESTION 20:

Terminal Services role is installed on two Windows 2008 servers named Srv1 and Srv2. Srv2 is running Terminal Services Gateway role.

Applications on Srv1 are published using a Remote Desktop Connection configuration file (.rdp file). Users download the .rdp files from the TSrvWeb virtual directory on Srv1.

You reconfigure the applications on Srv1 to use the Terminal Services Gateway role on Srv2 and export the Remote Program settings from Srv1 and import them to Srv2.

Users are complaining that they cannot access the remote applications on Srv2. Users can access the remote applications on Srv1 by using the Terminal Services Gateway on Srv2. You already verified that the application paths on both servers are identical. In order to ensure that users can access the applications on Srv2. What should you do?

- A. Disable the Network level Authentication feature on Srv2
- B. Re-create the .rdp files on Srv2 and redistribute the files to the users
- C. Copy the .rdp files from Srv1 to a new TSrvWeb virtual directory on Srv2
- D. Configure and activate the Terminal Server Session Directory feature on Srv2, configure Srv1 to use the Terminal Server Session Directory feature
- E. None of the above

Answer: B

Explanation:

When you exported the Remote program settings on Srv1 and import them on Srv2, only the RemoteApp Programs list and deployment settings are exported or imported. Any .rdp files or Windows Installer packages that were created from the programs were not be exported or imported and therefore the users reported that they cannot access remote applications installed on Srv2.

To ensure that the users could access and use the remote applications on Srv2, you need Re-create the .rdp files on Srv2 and redistribute the files to the users

Reference: Windows Server2008 Terminal Services RemoteApp Step-by-Step Guide /

To import the RemoteApp Programs list and deployment settings

http://download.microsoft.com/download/b/1/0/b106fc39-936c-4857-a6ea-3fb9d1f37063/Windows_Server_200

QUESTION 21:

Terminal Services role is installed on two Windows 2008 servers named Srv1 and Srv2. Srv2 is running Terminal Services Gateway role. Applications on Srv1 are published using a Remote Desktop Connection configuration file (.rdp file). Users download the .rdp files from the TSrvWeb virtual directory on Srv1. You reconfigure the applications on Srv1 to use the Terminal Services Gateway role on Srv2 and export the Remote Program settings from Srv1 and import them to Srv2. Users are complaining that they cannot access the remote applications on Srv2. Users can access the remote applications on Srv1 by using the Terminal Services Gateway on Srv2. You have already verified that the application paths on both servers are identical. In order to ensure that users can access the applications on Srv2. What should you do?

- A. Disable the Network level Authentication feature on Srv2
- B. Re-create the .rdp files on Srv2 and redistribute the files to the users
- C. Copy the .rdp files from Srv1 to a new TSrvWeb virtual directory on Srv2
- D. Configure and activate the Terminal Server Session Directory feature on Srv2, configure Srv1 to use the Terminal Server Session Directory feature.
- E. None of the above

Answer: B

QUESTION 22:

The corporate network of Certkiller consists of 10 servers that run Windows Server 2008. You have recently enabled RDP on the servers to provide remote administration to the servers. All the computers that will be used to provide remote administration run Windows Vista.

You configured RDP on server with default security settings. However, you are not satisfied with the default security setting and need to ensure that the RDP connections are as secure as possible.

Which of the following two actions would you perform to configure secure RDP connections? (Each correct answer presents a part of the solution. Select two).

- A. Acquire user certificates.
- B. Block port 3389 of the firewall on each server.
- C. Set the security layer for each server to the RDP Security Layer.
- D. Configure each server to allow connections only to RDP client computers that use Network Level Authentication.

Answer: A, D

Explanation:

To configure secure RDP connections, you need to first Acquire user certificates and then configure each server to allow connections only to Remote Desktop client computers that use Network Level Authentication.

The Network Level Authentication is selected on each server to allow connections to Remote Desktop client computers because only Vista clients are used to connect to the Terminal Server

Reference: Configuring the Windows Server 2008 Terminal Services Gateway (Part 1)

<http://www.windowsecurity.com/articles/Configuring-Windows-Server-2008-Terminal-Services-Gateway-Part1>

QUESTION 23:

Certkiller .com has a server that hosts an Active Directory domain. A server at Certkiller .com named CK2 has Terminal services role and Terminal Services web access role installed. It also has a server called CKSA that runs ISA Server 2006. You are assigned the task to deploy Terminal Services Gateway (TS Gateway) role on a new server called CK4 . Certkiller .com. Certkiller .com wants to employ ISA as the SSL endpoint for Terminal Server connections. After doing the necessary configurations, you succeed in deploying TS Gateway role on CK4 . Certkiller .com. Now you have to configure the ISA for TS connections. To do this you need to configure the TS gateway on CK4 to use ISA 2006 on CK2 . What should you do to achieve this objective?

- A. On CK4 , configure the Terminal Services Connection Authorization Policy store to use CK2 as the Central network policy server
- B. Design an SSL certificate from CK4 and export it to install the SSL certificate on CK2 . Set the ISA service on CK2 to use SSL certificate on CK4
- C. Set the TS gateway to use SSL HTTPS-HTTP bridging
- D. Export an SSL certificate on CK4 and install it on CK2 . Set the TS gateway to accept SSL certificate from CK2

Answer: C

Explanation:

To configure the TS gateway on CK4 to use ISA 2006 on CK2 , you have to configure the TS gateway to use SSL HTTPS-HTTP bridging. The HTTPS-HTTP bridging works when the TS gateway client initiates an SSL (HTTPS) request to the SSL bridging device. A new HTTP request to the TS Gateway server is started by the SSL bridging device.

QUESTION 24:

Certkiller .com runs Terminal services on an Active Directory domain. As an administrator of Certkiller .com, you configure the main office printer as the default printer on Terminal server.

Certkiller .com has a stringent security policy which states that all the remote client

computers must meet the following requirements:

- * The default printer on client computers must be the main office printer
- * Users must also be able to access their local printers during a terminal session

To meet the company policy, you have to set a Group Policy Object by using the Terminal Services Printer Redirection template. What should you do to achieve this objective?

- A. In a session options, set the 'Do not set default client printer' to default printer Enabled. Apply GPO to the Terminal Server
- B. Set the Terminal services option on print to default printer and disable Easy printer driver. Apply the GPO to the Terminal Server
- C. Apply the GPO to all the client computers and configure their printer options to Set default printer for office printer and local printers as user printers
- D. Configure Easy Printer driver and disable the first option. Apply the GPO to the Terminal Server
- E. None of the above

Answer: A

Explanation:

To set a Group Policy Object by using the Terminal 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 Terminal 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 terminal session so if the default printer is busy or has any problem, the next available printer (user printer) will automatically print the required document.

QUESTION 25:

The Certkiller is running Windows Server 2003 and Windows Server 2008 servers on their corporate network domain. The Terminal Service Gateway role is installed on a Windows Server 2008 server named Serv1.

The Terminal Service role is installed on servers named Serv2 and Serv3, which are running Windows Server 2003. Serv2 and Serv3 are configured in a load balancing terminal Server Farm name Certkiller TSLoad.

A Terminal Server Broker Service is installed on a Windows Server 2008 server named Serv4 and Certkiller TSLoad farm is added to the Terminal Server Broker Service configuration on Serv4.

You configured some applications to use TS Session Load Balancing Service and found that TSSession Broker Load Balancing is not providing load balancing for Serv2 and Serv3.

What do you need to do to enable TS Session Broker Load Balancing Service on Serv2 and Serv3?

- A. Add Serv2 and Serv3 to the Session Broker Computers local group on Serv4
- B. Load Balancing Service cannot be configured on Serv2 and Serv3 servers because Windows Server2003-based terminal servers cannot use the TSSession Broker Load Balancing feature
- C. Run remote Desktop Connection (RDC) version5.2 on clients connecting to Serv2 and Serv3
- D. None of the above

Answer: B

Explanation:

The TS Session Broker Load Balancing Service is not providing load balancing for Serv2 and Serv3 because Windows Server2003-based terminal servers cannot use the TSSession Broker Load Balancing feature.

Reference: Windows Server 2008 TS Session Broker Load Balancing Step-by-Step Guide

<http://technet2.microsoft.com/windowsserver2008/en/liBRary/f9fe9c74-77f5-4bba-a6b9-433d823bbfbd1033.msp>

QUESTION 26:

Certkiller network domain is running Windows Server 2003 and Windows Server 2008 servers. The Terminal Service Gateway role is installed on a Windows 2008 server.

The Terminal Service role is installed on servers named New1, New2 and New3 and configured in a load balancing terminal Server Farm name NewTSLoad.

New2 and New 3 are running Windows Server 2003. A Terminal Server Broker Service is installed on a new server named New1 and NewTSLoad farm is added to the Terminal Server Broker Service configuration on New1.

When you check event logs, you find an event ID: 1023 is getting generated. The event ID description indicates TS session Broker farm service is in inconsistent state. What should you do?

- A. Install Terminal Server Broker Service on Windows Server 2008 servers.
- B. Move Terminal server BRoker service on Windows server 2003 named New2 or New3.
- C. Enable Terminal server BRoker service on Windows 2003 servers
- D. Disable Terminal server BRoker service for Windows 2003 servers
- E. None of the above

Answer: A

Explanation:

The Event ID: 1023 is getting generated and the event ID description indicates that TS session Broker farm service is in inconsistent state because Terminal servers that are running Microsoft Windows Server 2003 do not support TS Session Broker load balancing and therefore for load balancing you need to install Terminal Server Broker

Service on Windows Server 2008 servers .

Reference: Windows Server 2008 TS Session Broker Load Balancing Step-by-Step Guide

<http://technet2.microsoft.com/windowsserver2008/en/liBRary/f9fe9c74-77f5-4bba-a6b9-433d823bbfbd1033.msp>

QUESTION 27:

Certkiller .com has a server that runs Windows Server 2008. There are four terminal servers installed. They are named CK2 , CK3 , CK4 , CK5 . As an administrator at Certkiller .com, you install the Terminal Server Session Broker role service on CK2 . What tool should you use to configure load balancing for the four terminal servers? You also have to make sure that CK3 is the preferred server for TS sessions.

- A. TS Gateway Manager
- B. Group Policy Manager
- C. Terminal Services Manager
- D. Terminal Services Configuration.

Answer: D

Explanation

You should use Terminal Services Configuration to configure load balancing for the four terminal servers. It will also make CK3 the preferred server for TS sessions. Using NBL with Terminal Services provide increased availability, scalability, and load-balancing performance, as well as the ability to distribute a large number of Terminal Services clients over a group of terminal servers.

QUESTION 28:

As an administrator at Certkiller .com, you install a member server named ebms1 that has Windows Server 2008 as its primary operating system. The Terminal Services role is installed on the ebms1.

The Terminal Server user profiles are in a folder named as UPT on a server called CKTS. On CKTS3, a home folder is placed for each user. As you monitor CKTS, you find out that there is only 5% of hard disk space remaining because the users are saving their files on their profiles on CKTS instead of using their home folders. You have to limit the amount of disk space allocated to each user to 200 MB. What should you do to achieve that?

- A. On the ebms1, configure a group policy object. Configure a default quota limit to 200 MB and set a warning level policy
- B. Create a new group policy object and link it to the CKTS. Configure the UPT folder to limit the disk space quota to allocate 200 MB to all users.
- C. Configure the disk quotas for the volume that hosts UPT folder. Limit the users to use only 200 MB of space.

- D. Configure each profile by activating disk quota on each profile. Apply folder redirection settings to redirect the users to save their files on CKTS3
- E. None of the above

Answer: C

Explanation:

To limit the amount of disk space allocated to each user to 200 MB, you need to configure the disk quotas for the volume that hosts UPT folder and then limit the users to use only 200 MB of space.

Configuring a quota limit through group policy will not help in Terminal services scenario. Also disk quotas cannot be configured for each user profile rather it is configured on a volume or a folder.

Reference: Working with Quotas

<http://technet2.microsoft.com/windowsserver2008/en/liBRary/31790148-eaf1-4115-8a50-4ce7a4503d211033.msp>

Reference: Setting Up File Sharing Services

http://safari.phptr.com/9780596514112/setting_up_file_sharing_services

QUESTION 29:

In Windows Server 2008, Windows System resource manager (WSRM) uses resource-allocation policies to determine how computer resources, such as CPU and memory, are allocated to processes running on the computer.

Name the two resource-allocation policies that are specifically designed for computers running Terminal Services in Windows sever 2008 Terminal services environment?

- A. Equal-Per-User and Equal-Per-Session
- B. Per_user_Equal and Per_Session_Equal
- C. Equal_Per_User and Equal_Per_Session
- D. User_Per_Equal and Session_Per_Equal
- E. None of the above

Answer: C

Explanation:

The two resource-allocation policies that are specifically designed for computers running Terminal Services in Windows sever 2008 Terminal services environment are Equal_Per_User and Equal_Per_Session

Reference: Terminal Services and Windows System Resource Manager

/Resource-Allocation Policies

<http://technet2.microsoft.com/windowsserver2008/en/liBRary/a25ed552-a42d-4107-b225-fcb40efa8e3c1033.msp>

QUESTION 30:

There is an Active Directory domain at Certkiller .com's corporate network. On the member server, CK1 , terminal services are installed and on a new test server called CK2 in a workgroup environment, the Terminal Licensing role is installed. On CK2 , you wanted to enable the Terminal Services per User Client Access License (CAL) mode but you were not allowed to do so. What should you do to ensure that you could employ Terminal Services per User CAL mode on CK2 ?

- A. Connect CK2 to the Active Directory domain
- B. Configure Terminal Service Per User CAL on CK1 and connect CK2 to CK1
- C. Configure the license keys obtained from Microsoft Clearinghouse and enter these into the licensing server
- D. Configure a group policy object for CK1 to sue CK2 for licensing. Apply the GPO on CK1
- E. None of the above

Answer: A

Explanation:

To ensure that you could employ Terminal Services per User CAL mode on CK2 , you need to connect CK2 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.msp>

QUESTION 31:

The Terminal Services role is installed on a member server named Srv1. The Terminal Services Licensing role is installed on a new test server named TestSrv in a workgroup.

You cannot enable the Terminal Services Per User Client Access License (CAL) mode in the Terminal Services Licensing role on TestSrv.

What should you do to ensure that you could use the Terminal Services Per User CAL mode on test server?

- A. Join TestSrv to the domain.
- B. Obtain license keys from Microsoft Clearinghouse. Enter the keys into the Licensing server.
- C. Configure Srv1 to use TestSrv for the Terminal Services Licensing role. Reconfigure Test Server for the Terminal Services Per User CAL mode
- D. Install the Terminal Services Gateway role on Srv1. Configure a group policy object that configures Server1 to use test Server for licensing. Apply the policy to Srv1
- E. None of the above

Answer: A

Explanation:

To ensure that you could employ Terminal Services per User CAL mode on CK2 , you need to connect CK2 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.msp>

QUESTION 32:

Certkiller .com has a server that runs Windows Server 2003. It has an Active Directory domain. There is a server on the network that runs Windows Server 2008. It is called CK7 . Another server named CK9 runs Windows Server 2006. The terminal services role is installed on CK7 and the Terminal Services Licensing role service is installed on CK9 . You have to set the Terminal Services Per User Client Access License (TS Per User CAL) tracking and reports to work on both the servers. What should you do to achieve this objective?

- A. On CK9 , uninstall the terminal services licensing role and install it on CK7 . Then, configure TS Per User CAL tracking and reporting on CK9
- B. Configure the CK7 by adding terminal services licensing role on it. Install terminal services role on CK9 and activate Tracking and reporting
- C. Configure the Terminal Services Licensing Server on CK9
- D. Add CK7 in the Windows Server 2003 Terminal services licensing service

Answer: A

Explanation

To set the Terminal Services Per User CAL tracking and reports to work on both the servers, you should uninstall the terminal services licensing role on CK9 and install it on CK7 . After that, you should configure TS Per User CAL tracking and reporting on CK9 .

QUESTION 33:

Certkiller .com is running Windows Server 2008 on a server called CKS2. The Terminal Services are installed on CKS2.

You installed a new Terminal Services application on CKS2. The new application vendor assured you that the application can be installed in Terminal Services environment. He also informed you that the application does not use Windows Installation packages for installation and that it makes changes in the user registry during installation process.

After the installation, the users complained that application is not responding.

When you diagnosed the problem, you found that the sessions are disconnected and that the application is not accepting multiple sessions. What should you do to make

sure that the application accepts multiple sessions?

- A. Execute the command chguser/install on CKS2 and install the application. Execute the chgusr/execute after installing the application on the CKS2
- B. Execute chgusr/disable on CKS2 and install the application. Run the chgusr on user computers to allow multiple sessions
- C. Execute chglogon/execute command after installing the application on the CKS2 and execute chglogon/multiplesessions on each client computer
- D. Run mstsc/v:CKS2/enable command on the client computer and then install the application
- E. None of the above

Answer: A

Explanation:

To make sure that the application accepts multiple sessions on a terminal server, you need to execute the command chguser/install on CKS2 and install the application.

Execute the chgusr/execute after installing the application on the CKS2. IF you install an application using chuser/install command the application will be installed for multiple users to be able to use them, other wise they will be installed in single user mode and can only be run directly from the server itself by the local admin.

Reference: Forums / Topic Title: Why reinstall apps after Terminal Server installation?

<http://forums.windowsitpro.com/web/forum/messageview.aspx?catid=45&threadid=83425&enterthread=y>

QUESTION 34:

Certkiller network has a terminal server named TERM1 running on Windows server 2008.

You are running some business applications on the terminal server for the remote users in the BRanch office of the company, who will be remotely accessing these applications from this terminal server. You have configured the user accounts to provide them a Terminal Services-specific profile and a home folder.

While testing connection, you realized that the Terminal server profile has failed to load and the event ID: 1046 has been generated and logged to the event viewer.

What should you do now?

- A. Specify a new location for the Terminal Services profile path, ensuring that the path does not exceed 256 characters
- B. Specify the Terminal Services profile path by using Group Policy
- C. Establish a remote session with the terminal server and check that the user's desktop and other settings
- D. None of the above

Answer: A

Explanation:

The event ID: 1046 generates when the profile path is less than 256 characters in length. Therefore to resolve the problem, you need to specify a new location for the Terminal Services profile path, ensuring that the path does not exceed 256 characters.
Reference: Event ID 1046 - Terminal Services User Configuration
<http://technet2.microsoft.com/windowsserver2008/en/liBRary/f4c0f0c3-19c9-4220-b1c6-07c3590db9f41033.msp>

QUESTION 35:

Certkiller .com has a server that runs Terminal Services. As an administrator at Certkiller .com, you plan to install an application update for an application named tsap.exe on the Terminal Server (TS). While checking the application, you find out that instances of tsap.exe process are running even after the users have disconnected.

In order to perform an application update, you have to terminate all instances of tsap.exe process. Which two actions would you perform to achieve this objective? (Choose two answers. Each answer is a part of a complete solution)

- A. Open Terminal Services Manager Console and end all instances of tsap.exe
- B. Execute the TSapp - getprocess command on Terminal server
- C. End all instances of the tsap.exe and restart the server. Execute a appkill command to stop the application immediately
- D. On the Terminal Server, execute Tskill tsap/a command
- E. None of the above

Answer: A, D

Explanation:

To terminate all instances of tsap.exe process, you have to end all instances of tsap.exe process by accessing the Terminal Services Manager Console. The processes are displayed there. You kill the unwanted process by terminating a process. Use Microsoft Management Console to access the Terminal Services Manager console snap-in. After doing this, you have to execute a Tskill tsap/a command to end active processes. You can end the process by right-clicking on the process in the processes tab in Terminal Services Manager and clicking End process or you can use tskill command to do this. If you end a process through this command, no notification will be sent to the user. The process is ended immediately.

QUESTION 36:

Certkiller .com has servers with Windows Server 2008 installed as a primary operating system. The servers are in an Active Directory domain. CKS1 is a server, which has Terminal Services gateway role installed. The Terminal Services role is installed on CKS2 and CKS3. Both servers are added in a load balancing terminal server farm called TSF.

Another administrator installs Terminal service BRoker on a new server called

CKS4 and configures TSF farm to be added to the Terminal Server Broker Service configuration on CKS4.

Due to a requirement, you setup the published applications to employ Terminal Server Broker Service. You find out that CKS2 and CKS3 are not accepted in Terminal Server Broker service. What should you do to ensure that Terminal Server Broker Service accepts the CKS2 and CKS3 connections?

- A. Open the Session Broker Computers local group on CKS4 and add CKS2 and CKS3
- B. Configure and set a Group Policy Object and set the Allow reconnection option to True for Terminal services security section and apply it to the CKS2 and CKS3
- C. Configure and set a GPO to set the Deny reconnection option to True for Terminal Server Broker Service and apply it to CKS2 and CKS3
- D. Configure the Windows Authorization Access domain for CKS3 and add CKS2 and CKS4 in the Active Directory domain
- E. None of the above

Answer: A

Explanation:

For terminal servers to use TSSession Broker, you must add the computer account for each terminal server in the farm to the Session Directory Computers local group on the TSSession Broker server. Therefore to ensure that Terminal Server Broker Service accepts the CKS2 and CKS3 connections, you need to open the Session Broker Computers local group on CKS4 and add CKS2 and CKS3.

Reference: Windows Server 2008 TS Session Broker Load Balancing Step-by-Step Guide / Add each terminal server in the farm to the Session Directory Computers local group

<http://technet2.microsoft.com/windowsserver2008/en/liBRary/f9fe9c74-77f5-4bba-a6b9-433d823bbfbd1033.msp>

QUESTION 37:

Certkiller .com has an Active Directory domain. It has Terminal services installed on the Windows Server 2008 computers in the domain. All client machines have Windows Vista as their operating system.

Due to a nature of work, users are required to view some training videos on Windows Media Player 11 during Terminal Services session. What should you do to ensure that the users could run Windows Media Player 11 during the Terminal services session?

- A. On the terminal server, install the Quality Audio Video feature.
- B. Open the Terminal server settings and enable the 'allow desktop applications to run on session'. Disable the default settings
- C. Install and configure the Desktop Experience feature on the terminal server
- D. Create a group policy object that allows Windows Media Player 11 to set the differential services code point value to 10 and apply the policy to the client machines

that want to use Windows Media Player 11
E. All of the above

Answer: C

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 38:

As an administrator at Certkiller .com, you manage a member server having Windows Server 2008. A Terminal Services role is installed on the server along with Microsoft Windows System Resource Manager (WSRM).

Users are complaining about degradation in performance on Terminal Server. You find out that a single user is consuming 100% of the processor time. To rectify the problem, you create a resource-allocation policy named Policy1 which limits each user to 30% of the total processor time. Still, there is no improvement in the performance. What should you do to configure WSRM to force Policy1?

- A. Configure each user account to allocate a resource quota on WSRM application
- B. Configure Policy1 to accept the WSRM resource quota for each user
- C. Restart the Server and the Terminal Services configuration service
- D. Configure policy1 as the Managing Policy
- E. None of the above

Answer: D

Explanation:

To configure WSRM to force Policy1, you should configure policy1 and Managing policy. You can set a policy as managing policy by accessing Resource Allocation Policies node in the left-hand pane. You can click on the policy and set it as managing policy by click on "Set as Managing Policy" link in the right pane.

QUESTION 39:

Certkiller .com has a server that runs Windows Server 2008. Certkiller .com has WSUS (Windows Server Update Services) installed on this server. This server is located on the Certkiller .com's intranet. It is installed on the default website. Due to a company policy, you configured the update and statistics servers to employ SSL (Secure Socket Layer). Which URLs should you use to configure a group policy

object (GPO) that specifies the intranet update locations on a default port?

- A. https://server1: 80
- B. http://server1: 1073
- C. https://server1: 8080
- D. https://server1
- E. None of the above

Answer: D

Explanation:

To configure a group policy object (GPO) that specifies the intranet update locations on a default port, you need to use https://server1. You must include a URL for a secure port that the WSUS server is listening on. Because you cannot require SSL on the server, the only way to ensure that client computers use a secure channel is to make sure they use a URL that specifies HTTPS. If you are using any port other than 443 for SSL, you must include that port in the URL, too.

Reference: WSUS SSL Client Configuration

<http://www.techsupportforum.com/microsoft-support/windows-nt-2000-2003-server/115983-wsus-ssl-client-con>

Reference: Specify Intranet Microsoft Update Service Location

<http://technet2.microsoft.com/windowsserver/en/library/ac90c1de-9e04-46fd-b8ab-0bb4ab8515461033.mspx?m>

QUESTION 40:

Certkiller .com has a server that runs Windows Server 2008. This server is running IIS 7.0 and one .ASP NET application for Sales department users.

You had previously another version of ASP NET installed on this server. You want that new application should use the specific version of ASP NET at virtual directory\ASP.NET application level.

What you should do to choose the specific version of .ASP NET for a specific application?

- A. In IIS management console, navigate to the Website or ASP.NET application folder, in the Properties tab go to ASP NET tab and choose the version to use
- B. Run Aspnet_regiis.exe tool to check version of ASP.NET
- C. You need to uninstall previous version of ASP.NET before installing a new version
- D. None of the above

Answer: A

Explanation:

To choose the specific version of .ASP NET for a specific application, you need to open the IIS management console, and then navigate to the Website or ASP.NET application folder. In the Properties tab go to ASP NET tab and choose the version to use.

Reference: Configure a Web Application to Use a Specific Version of ASP.NET /
Configuring an ASP.NET Application to Use a Specific Version of ASP.NET
http://www.codeguru.com/csharp/.net/net_asp/miscellaneous/article.php/c10879/

QUESTION 41:

Certkiller .com uses Windows Server 2008 on all its servers. An active directory domain is acting as a Certkiller network named CK1 .com. The network also has a web server named CK2 .com. The users on the domains access the web server by using http:// CK2 .com.

To implement SSL, you generate a self-signed certificate for CK2 .com and configure it to use Secure Socket Layer (SSL).

After the implementation, users complain that when they try to connect to the web server using http:// CK2 .com, they get a warning message. What should you do to ensure that the users are able to connect to CK2 .com without getting warning messages?

- A. Export the self-signed certificate to CK2 .cer file by accessing the certificate from the certificates console on CK1 . Install the CK2 .cer file on all computers in the domain
- B. Configure the security zones on all computers in the domain. Put http:// CK2 .com in the trusted zone.
- C. Configure the DNS host records on CK2 .com and reissue the self-signed certificate. Ask users to connect to CK2 . CK1 .com to access resources on http:// CK2 .com
- D. Connect the CK2 .com to CK1 server and reissue the certificate. Ask the users to use https:// CK2 .com instead of http:// CK2 .com

Answer: A

Explanation:

To ensure that the users can connect to CK2 .com without getting warning messages, you should export the self-signed certificate to a CK2 .cer file. Then, you install the CK2 .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 42:

Certkiller .com has a Windows Server 2008 installed on a server that runs IIS server role. Users complain that when they try to connect to the IIS server, they receive an error message. You check the server and receive the following message:

"The maximum number of worker processes is reached or out of resources."

Which command should you execute to identify the website that is causing this problem?

- A. Execute `appcmd list wp`

- B. Execute appcmd list site
- C. Execute cmd command and list the IIS server running on the computer
- D. Execute apppool.exe to identify the website causing problem
- E. None of the above

Answer: A

Explanation:

To identify the website that is causing this problem, you need to Execute appcmd list wp
AppCmd.exe is the single command line tool for managing IIS 7.0 without using a graphical administration tool

The LISTcommand is used to display the objects on the machine. An optional <ID> can specify a unique object to list, or one or more parameters can be specified to match against object properties.

You can use the WP (worker process) object to list running worker processes and thereby identifying the website that is causing this problem.

Reference: Overview of Command Line Administration - AppCmd.exe

<http://www.iis.net/954/SinglePageArticle.ashx>

QUESTION 43:

Exhibit:

Setting Name	Value
Site name	certkiller
ID	2
Location	80
Post header	www.certkiller.com

Certkiller .com has a server that runs Windows Server 2008. You install an IIS server role on this server. Certkiller .com has decided to add a new website to the IIS server. The settings of the new site are shown in the exhibit. What would you do to setup the new website according to the settings shown in the exhibit?

- A. Open the command prompt on the server and execute appcmd set app /app.name: Certkiller /[path='/'].physicalPath:d:\ Certkiller _content_ID2 command
- B. Open the command prompt on the server and execute theappcmd add site /name: Certkiller /id:45 /physicalPath: f:\ Certkiller _content /binding:http:80: www. Certkiller .com command
- C. Open the command prompt on the server and execute theappcmd add app /app.name: Certkiller /[path='/']
- D. Execute the command set-location/ Certkiller -new website port: 80 by utilizing the MS Windows command prompt utility
- E. None of the other alternatives apply

Answer: E

Explanation:

To setup the new website according to the settings shown in the exhibit, you need to run the following command on the server:

```
appcmd add site /name: Certkiller /id:2 /physicalPath: d:\ Certkiller _content  
/binding:http/*:80: www. Certkiller .com.
```

To add a site, you need to use the following syntax:

```
appcmd add site /name:string /id:uint /physicalPath:string /bindings:string
```

Reference: IIS 7.0: Create a Web Site / Command Line

<http://technet2.microsoft.com/windowsserver2008/en/liBRary/f6c26eb7-ad7e-4fe2-9239-9f5aa4ff44ce1033.mspx>

QUESTION 44:

Certkiller .com has a member server that has Windows Server 2008. An IIS Server role is installed on the member server. This member server hosts an intranet website. Windows Authentication is setup on the website and it is the only authentication method that is active on the server. You decide to create a virtual directory named /tm/. This directory has content that can be accessed only by the Technical management global group. What should you do to configure options on the website to allow only the Technical management group to access the /tm/ virtual directory?

- A. Reconfigure the default Authorization rule on /tm/ directory
- B. Configure a deny authorization rule on /hr/ virtual directory that denys all anonymous users and allow only users in Technical management global group
- C. Configure the Allow Authorization rule on /tm/ directory. Set the roles and user groups setting and allow Technical management users group to access the directory
- D. Add a Deny Authorization rule on the user groups for all other groups and set the allow option for technical management group in the user roles
- E. None of the above

Answer: C

Explanation:

To configure options on the website to allow only the Technical management group to access the /tm/ virtual directory, you need to configure the Allow Authorization rule on /tm/ directory. Select the Specified users setting and add Technical management group name. The Authorization rule allows you to add additional authentication and authorization settings for the specific user accounts for a website.

Reference: Creating a New FTP Site / Step 2: Adding Additional FTP Security Settings
<http://learn.iis.net/page.aspx/301/creating-a-new-ftp-site/>

QUESTION 45:

Certkiller .com provides Web hosting services. AS an administrator, you manage the server that has Windows Server 2008 installed on it as its operating system. An IIS server role is installed on this server. The server has multiple websites running. You have to configure a new website for a new client on the IIS server. While deploying the website on the server, you find out that the website looks like an FTP download page instead of the normal HTTP page that presents the content without letting anyone to download it. You have to setup the website to present the content through HTTP and make sure the files are not downloaded by the users. Which two actions should you perform to complete this task? (Choose two answers. Each answer is a part of the complete solution.)

- A. Match the webpage file to the website by configure the default document setting
- B. Configure the website to use the application pool
- C. Execute the appcmd set config/section:directoryBrowse/enabled: false command
- D. Configure the directory that hosts website to grant Allow, read and execute permission to the users of the website content
- E. Configure a DNS zone for the domain that hosts website and create a CNAME record

Answer: A, C

Explanation:

To setup the website to present the content through HTTP and make sure the files are not downloaded by the users, you need to first match the web page file to the website by configuring the Default document setting and then executing the appcmd set config/section: directoryBrowse/enabled: false command.

Configuring default document setting will allow you to hide the document name while showing its content. The default document specifies what file to serve. The appcmd set config/section: directoryBrowse/enabled: false command will allow you to turn off the directory Browsing on the website.

Reference: Default Documents

<http://learn.iis.net/page.aspx/203/default-documents/>

Reference: Getting Started with AppCmd.exe / Controlling Location of Configuration

<http://learn.iis.net/page.aspx/114/getting-started-with-appcmdexe/>

QUESTION 46:

Certkiller .com has a server that runs Windows Server 2008. A Web Server (IIS) role is installed on the server which is used to host multiple websites.

You are assigned to release memory for a single website. You have to configure the server automatically to release memory. What should you do to achieve this objective without affecting other websites hosted on the same Web server?

- A. Change the Recycling options from the application pool defaults
- B. Edit the bindings for the website by creating a new website

- C. Create and configure a virtual directory. Link the physical path credentials to the website
- D. Associate the website to an application pool by creating a new application pool
- E. None of the above

Answer: D

Explanation:

To configure the server automatically to release memory without affecting other website hosted on the same web server, you should associate the website to an application pool by creating a new application pool. Application pools helps isolate the applications running on a web server. Each application pool has its own worker process in the system. By adding an application to a specific pool, the application never affects on applications in other pools. Even if the application process crashes, only the pool which is hosting it will be affected. The web server and other pools will continue to run normally.

QUESTION 47:

You are an administrator of a Server that runs Windows Server 2008. It is named as CKFSVE. This server is dedicated to a FTP service. According to the Certkiller .com policy, the FTP server should only be available for selected authorized projects. What should you do to make sure that FTP service unavailable after restarting the server?

- A. Execute the iisftp/stop command on CKFSVE
- B. Execute the netsrvr32/stop ftp: CKFSVE command on CKFSVE
- C. Run the WMIC /NODE: CKFSVE SERVICE WHERE the caption="FTP Publishing Service" CALL ChangeStartMode "Disabled" command on this particular Certkiller FTP server
- D. Execute iisreset ftp. Certkiller .com command on the CKFSVE server
- E. Execute WMIC/node: CKFSVE command on publishing service command on the server
- F. None of the above

Answer: C

Explanation:

To make sure that FTP service unavailable after restarting the server, you need to Run the WMIC /NODE: CKFSVE SERVICE WHERE the caption="FTP Publishing Service" CALL ChangeStartMode "Disabled" command on this particular Certkiller 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: wmic

[http://msdn2.microsoft.com/en-us/liBRary/aa394531\(VS.85\).aspx](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 48:

The Windows server 2008 FTP service no longer uses metadata and the new configuration store in IIS 7.0 uses files to store configuration details. What is the format of new configuration files?

- A. .TXT files
- B. HTTP files
- C. CGI script files
- D. .NET XML based files
- E. None of the above

Answer: D

Explanation:

The format of new configuration files is .NET XML based files. The IIS 7.0 has a Brand-new administration interface which uses a new FTP instead of the old IIS 6 metabase. The new configuration store is based on the .NET XML-based *.config format.

Reference: Microsoft FTP Service for IIS 7.0 (x86) / Integration with IIS 7.0

<http://www.microsoft.com/downloads/details.aspx?familyid=2ECCF14A-5C4F-4CFB-9153-CFE1204B346A&d>

QUESTION 49:

Certkiller .com has a server that runs Windows Server 2008. You install the FTP role service on the server. After installing the FTP service, you allow users to use it. Users complain that they receive an error message when they attempt to use FTP site to upload files. What should you do to allow authenticated users to access the FTP sites to upload files?

- A. Execute the `ftp -a <IP address>` command on the Windows Server 2008
- B. Set write permission on the FTP site. On the FTP destination folder, set the NTFS permissions for Authenticated Users group to allow Read/write attributes
- C. Configure the FTP settings to allow Authenticated users to connect to the FTP server using the port 26.
- D. Configure the FTP settings to allow Authenticated users to connect to the FTP server by using their account logins and passwords
- E. None of the above

Answer: B

Explanation:

To allow authenticated users to access FTP sites to upload files, you have to set write permission on the FTP site and set the NTFS permissions for Authenticated Users group on FTP designation folder to allow Read/write attributes. By setting the write permission on FTP site, users will be able to upload files on FTP and adding Authenticated Users group in NTFS permissions will enable the users to upload files without getting any warning messages.

QUESTION 50:

Certkiller .com has a web hosting service. It hosts websites for 40 customers. An SMTP server is dedicated for each website.

You changed the server and installed the IIS server role and SMTP server on the new server that is running Windows Server 2008. Certkiller .com has acquired a new client. You create their website and install the SMTP server for the new client.

However, the SMTP server fails to start.

What should you do to configure the new SMTP server to start on the IIS server?
(Select all that apply)

- A. Configure the SMTP server to integrate the IIS server role
- B. Use a different IP address for the new SMTP server
- C. Configure the SMTP server by using the iiscnfg/enable command on the IIS server
- D. Add the SMTP server IP address in the IIS Server SMTP settings
- E. Use a different port for the new SMTP server

Answer: B, E

Explanation:

To configure the new SMTP server to start on the IIS server, you need to either use a different IP address for the new SMTP server or use a different port for the new SMTP server. This is because more than one virtual server can use the same TCP port if all servers are configured by using different IP addresses.

Reference: IIS 7.0: Configure SMTP E-mail

<http://technet2.microsoft.com/windowsserver2008/en/liBRary/e56b93b1-8521-48ab-a902-e47b0ee4408b1033.ms>

QUESTION 51:

You are running a SMTP server on a Windows server 2008. Some of the developers want to create a set of web pages that let a user type a message in a form and mail it to techsupport@mail. Certkiller .com. The form creates a text file with the proper SMTP headers. In which folder should the file be copied?

- A. Mailroot\Delivery
- B. Mail\Queue
- C. Mailroot\Pickup
- D. Mailroot\Queue

E. None of the above

Answer: C

The file should be copied to Mailroot\Pickup folder because all the files copied to the Mailroot\Pickup folder are processed and delivered as regular mail.

Reference: SMTP and IIS / OVERVIEW OF THE MESSAGE DELIVERY PROCESS

<http://www.windowsitlibrary.com/Content/141/09/1.html>

QUESTION 52:

Certkiller .com has a server named CK1 which runs Windows Server 2008. An IIS role and an SMTP server feature are also installed on CK1 . You are assigned a task to configure the new SMTP server to forward all mails to the mail server of the ISP (Internet Service Provider). What should you do to achieve this objective?

- A. Execute the adprep/dm: getfromiis command
- B. Configure the local host to use smart host setting
- C. Configure the SMTP delivery setting to open ports assigned by ISP for SMTP service
- D. Set smart host setting to employ the mail server of ISP
- E. None of the above

Answer: D

Explanation:

To configure the new SMTP server to forward all mails to the mail server of the ISP, you should set smart host setting to use the ISP mail server. A smart host server helps you in delivering all your mail. IT processes bounce-backs, retries and general mail delivery. Due to the processor-intensive nature of the mail delivery system with millions of spam messages, a server can get overwhelmed processing mails. It doesn't have enough time to do normal web serving. To address this issue, you should use smart host on your ISP mail server to manage the mail delivery and the related tasks.

QUESTION 53:

As an administrator at Certkiller .com, you installed and configured an IIS server on CKS1 and added the file server role on a server named CKS2.

The hard disk installed in CKS1 hosts the Certkiller /apps virtual directory. You discovered that the hard disk is running out of space. So you moved the data on hard disk at CKS1 to a new volume, which has a new-shared directory on CKS2. You named the directory as CKWCKAPP.

What should you do to ensure that applications use CKWCKAPP?

- A. Execute the Appcmd set vdir/vdir.name: CKWCKAPP/APPS/TTO/physicalpath:\\CKS2\CKWCKAPP command on CKS1
- B. Execute Appcmd set vdir/vdir.name: Certkiller /apps/physicalPath:\\CKS2\CKWCKAPP command on CKS1

- C. Execute Appcmd set vdir /vdir.name: Contoso/Apps /physicalPath:C:\WebApp command on Server2.
- D. Execute Appcmd set vdir /vdir.name: CKS2/Apps /physicalPath:C:\WebApp command on CKS2.
- E. None of the above

Answer: B

Explanation:

To ensure that applications use CKWCKAPP, you need to execute Appcmd set vdir/vdir.name: Certkiller /apps/ physicalPath:\\CKS2\ CKWCKAPP command on CKS1.

To change the path of a virtual directory's content, you need to use the following syntax:
appcmd set vdir /vdir.name:string /physicalPath:string

The variable vdir.namestring is the virtual path of the virtual directory, and physicalPathstring is the physical path of the application's content.

Reference: IIS 7.0: Change the Physical Path of Virtual Directory Content

<http://technet2.microsoft.com/windowsserver2008/en/liBRary/836c7fa3-e7fe-4134-a970-b9ae1034f2311033.mspx>

QUESTION 54:

You are an administrator at Certkiller .com managing a member server that has Windows Server 2008 installed. An IIS Server role is installed on this member server.

The IIS server hosts a restricted website that only Certkiller .com executives can access. According to the company's policy, it is necessary for the executives to use user certificates to access the restricted website.

While monitoring the Server, you found out that the executives are accessing the secured website by using their usernames and passwords. What should you do to ensure that the executives can access the secured website only through user certificates?

- A. Open the secure website properties dialog box and modify the SSL settings to accept 128-bit of SSL certificate for authentication
- B. Install and configure a Group Policy Object to define a Certificate Trust list. Link the GPO to the IIS server to accept user certificates as login type.
- C. Modify the Client Certificate settings to Require on SSL Settings for the secured website
- D. Modify the Client Certificate setting to Accept in SSL settings for the secured website.
- E. All of the above

Answer: C

Explanation:

By default, client certificates are ignored. If you want the clients to verify their identity before they access the content of a website, you need to configure client certificates.

Therefore to ensure that the executives can access the secured website only through user certificates you need to modify the Client Certificate settings to Require on SSL Settings for the secured website

Reference: IIS 7.0: Specify Whether to Use Client Certificates

<http://technet2.microsoft.com/windowsserver2008/en/liBRary/5adc0029-8875-4390-a717-e5eb2eba97781033.msp>

QUESTION 55:

Certkiller .com has a server that runs on Windows Server 2008. The server also has an instance of Active Directory Lightweight Directory Services (AD LDS) running. In order to test AD LDS, you need to replicate the AD LDS instance on a test computer located on the network. What should you do to achieve this objective?

- A. Execute AD LDS Setup wizard on the test computer to create and install a replica of AD LDS.
- B. Execute repadmin/bs <servername> command on the test computer
- C. Install and configure a new AD LDS instance on the test computer by copy and pasting the entire partition on the test computer
- D. Execute the Dsmgmt command on the test computer and create a naming context

Answer: A

Explanation

To replicate the AD LDS instance on a test computer located on the network, you should execute AD LDS setup wizard on the test computer to create and install a replica of AD LDS. This is the only way to replicate the AD LDS instance on another computer on the network. The setup wizard has the option to replicate the AD LDS instance on another computer.

QUESTION 56:

Certkiller .com has a server named CK1 . CK1 runs Windows Server 2008. A web server (IIS) role is also installed on CK1 .

A public website is hosted on CK1 . While monitoring the traffic on the public site, you notice an unusual high volume of traffic on the website. You need to find the source of the traffic. What should you do to achieve this objective?

- A. Open the IIS server manager and enable website logging to filter the logs for the source IP address
- B. Install a third-party traffic analysis software to view the source IP address of the traffic
- C. Execute net session - at command on the server
- D. Execute net stat/all command to view the traffic statistics
- E. None of the above

Answer: A

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 57:

Exhibit:



Certkiller .com has a member server that is under your control. The member server has Windows Server 2008 installed as its prime operating system. An IIS server role is installed on the server, which also hosts an intranet website of Certkiller .com's. The website authentication settings are shown in the exhibit. Certkiller .com has a BRanch office that accesses the intranet through a proxy server. All client machines in the BRanch office and the main office use Microsoft Internet explorer. Users on the corporate network in the main office have no problems to get authenticated to the intranet website while the users in the BRanch office are unable to

authenticate and access the website. The authentication process is encrypted on the IIS server to enhance the performance.

What should you do to configure the website to support authentication for the users in the main office and the users in the BRanch office?

- A. Enable the Basic authentication settings and Disable the Windows Authentication setting for the users. After that select Require SSL through website properties
- B. Configure each client machine in the BRanch office and deselect Integrated Windows authentication option in the Internet Options Advanced settings dialog box.
- C. Add the Digest Authentication role service to the IIS server. Configure the Digest Authentication setting to Enabled.
- D. Add and enable the Host Credential Authorization Protocol role service on the IIS server
- E. None of the above

Answer: C

Explanation:

The users in the BRanch office are unable to authenticate and access the website because they were accessing the intranet through a proxy server and the authentication method configured (Windows Authentication) was not supporting proxy server.

To configure the website to support authentication for the users in the main office and the users in the BRanch office, you need to add the Digest Authentication role service to the IIS server and then configure the Digest Authentication setting to Enabled.

Digest Authentication works by sending a password hash to a Windows domain controller to authenticate users. When you need improved security over Basic authentication, consider using Digest authentication, especially if users who must be authenticated access your Web site from behind firewalls and proxy servers.

Reference: Available Role Services in IIS 7.0 / Security Features

<http://technet2.microsoft.com/windowsserver2008/en/liBRary/1ec80c97-4455-4829-a319-30e1e1c081691033.msp>

QUESTION 58:

You are running a Windows server 2008 with IIS server role installed. The web server is hosting the Intranet site and using Windows Authentication as the only authentication method that is set to Enabled. You need to create a new virtual directory /Sales/ which holds contents that can be accessed only by the members of SalesUsers global group. What should you do?

- A. Remove the Default Allow Authorization rule the /Sales/ virtual directory
- B. Modify the Default Allow Authorization rule on the /Sales/ virtual directory. Select the specified roles or user groups setting and add the SalesUsers group name
- C. Add a new Deny Allow Authorization rule on the /Sales/ virtual directory that applies to all anonymous users. Remove the Default Allow Authorization rule on the /Sales/ virtual directory

- D. Modify the Default Allow Authorization rule on the /Sales/ virtual directory. Select the specified roles or user groups setting and add the SalesUsers group name. Add a new Deny Authorization rule that applies to all users on the /Sales/ virtual directory.
- E. None of the above

Answer: B

Explanation:

To create a new virtual directory /sales/ which holds contents that can be accessed only by the members of SalesUsers global group, you should modify the Default Allow Authorization rule on the /Sales/ virtual directory. Then, select the specified roles or user groups setting and add the SalesUsers group name

QUESTION 59:

As the network administrator of Certkiller , it was your responsibility to ensure that all computers on the corporate network are always updated with Microsoft updates. To ensure that all computers get latest updates, you installed WSUS on a server called Certkiller 10 that runs Windows Server 2008.

To ensure the secure communication between the WSUS administrative Web site and the server administrator's computer, you decided to encrypt the traffic between them. What of the following options would you choose to accomplish this task?

- A. On the Certkiller 10 execute the netdom trust /SecurePasswordPrompt command from the command prompt.
- B. Configure the Certkiller 10 to require Integrated Windows Authentication (IWA) when user connects to it.
- C. Configure SSL encryption on the WSUS server web site on Certkiller 10.
- D. Configure the NTFS permissions on the content directory of Certkiller 10 to Deny Full Control permission to the Everyone group.
- E. None of the above

Answer: B

Explanation:

To ensure that the traffic between the WSUS administrative Web site and the server administrator's computer is encrypted, you need to first configure IIS to disable anonymous access to the ServerSyncWebService virtual directory and then enable Integrated Windows authentication.

You cannot set up the entire WSUS Web site to require SSL. This would mean that all traffic to the WSUS site would have to be encrypted, whereas WSUS only encrypts metadata traffic.

Reference: Plan and Assess: Using Windows Server Update Services (WSUS)
<http://technet.microsoft.com/en-us/updatesmanagement/bb245871.aspx>

QUESTION 60:

Certkiller .com offers Web hosting services. As an administrator you manage a member server that has Windows Server 2008 as its operating system.

The server named Exbla1 has an IIS server role actively running. Exbla1 hosts 5 client companies. You are setting up a website for a new client company called WXYZ inc. on the IIS server.

You put content for the WXYZ website on IIS server and store the HTML content documents on the virtual directory of the website, which is on a Windows Server 2008 remote server called CK3 .

The content directory is named WXYZ_VDIR. On CK3 , you grant share and NTFS permission to a user account called WXYZ_ADMIN for that virtual directory. The user complains that he is unable to access the content in the directory although he has access to the main website.

What should you do to enable the user to access the content in the virtual directory?

- A. Configure the WXYZ_ADMIN user account by accessing the account settings and enabling Connect on demand to the virtual directory
- B. Open the virtual directory options and select Edit permissions. On the customize tab, set Use this folder type as a template setting to documents
- C. Create a Group Policy Object and link it to the virtual directory. Configure the GPO to enable the WXYZ_ADMIN to access the virtual directory on CK3 .
- D. Open the properties of Virtual directory and click Connect As button and then configure the specific user setting to WXYZ_ADMIN
- E. All of the above

Answer: D

Explanation:

To enable the user to access the content in the virtual directory, you need to open the properties of Virtual directory and click Connect As button and then configure the specific user setting to WXYZ_ADMIN

The Connect As dialog box can be used to specify credentials that have permission to access the physical path. If you do not use specific credentials, select the Application user (pass-thru authentication) option in the Connect As dialog box

Reference: IIS 7.0: Create a Virtual Directory

<http://technet2.microsoft.com/WindowsServer2008/f/?en/LiBRary/32c434c0-5c5f-43eb-bd92-7302b95e43dd1033>

QUESTION 61:

Certkiller provides web-hosting services. You are running a Windows server 2008 with IIS server role installed.

The server hosts websites of 10 partner companies. You are configuring a website for a new partner named Flexinet on IIS server. Contents of Flexinet web site will

be stored on IIS server.

The HTML content documents for a virtual directory for the website would be stored on a remote Windows server 2008 named FI_Serv1. The contents folder is a shared folder named Flexinet_VDIR.

You granted the share and NTFS permission to a user account named Flexinet_admin in the virtual directory content on FI_Serv1. Users are unable to access the contents of virtual directory although they can access main website. What should you do to enable the users to access to the contents of virtual directory?

- A. Add the Flexinet_admin user account to the Domain Administrator global security group
- B. Add the Flexinet_admin user account to the Windows Authorization Access Domain local security group
- C. Configure the Specific user setting to Flexinet_admin in the Connect As dialog box in the properties of the virtual directory
- D. Select the Edit Permissions option for the virtual directory. Set the use this folder type as Template setting to Documents on the Customize tab
- E. None of the above

Answer: C

Explanation:

To enable the users to access to the contents of virtual directory, you need to configure the specific user settings to Flexinet_admin in the Connect As dialog box in the properties of the virtual directory

The Connect As dialog box can be used to specify credentials that have permission to access the physical path. If you do not use specific credentials, select the Application user (pass-thru authentication) option in the Connect As dialog box

Reference: IIS 7.0: Create a Virtual Directory

<http://technet2.microsoft.com/WindowsServer2008/f/?en/LiBRary/32c434c0-5c5f-43eb-bd92-7302b95e43dd1033>

QUESTION 62:

Certkiller .com has a Windows Server 2008 server with a single Active Directory domain installed on it. You are the administrator of a server name CKWDS which runs Windows Server 2008. You install the Windows Deployment Services (WDS) role on CKWDS. You are instructed to deploy the image of a reference computer on 30 client computers. After capturing the reference computer image, you find out that all the client computers have the same name. What should you do to ensure that each client computer receives a unique security identifier?

- A. Open the WDS snap-in and create an image group. Redeploy the image on all client computers
- B. Execute wdsutil/nickname:yes command on CKWDS server command prompt and redeploy the image on all client computers

- C. Execute wdsutil/ser-server/prestageusingMAC:yes command on the CKWDS server command prompt and redeploy the image on all client computers
- D. Execute imagex/securityid:yes command on the CKWDS server command prompt and redeploy the image to the client computers

Answer: C

Explanation:

To ensure that each client computer receives a unique security identifier, you should execute wdsutil/ser-server/prestageusingMAC:yes command on the CKWDS server command prompt and redeploy the image on all client computers. Unique security identifier is a data structure of variable length that identifies user, group, and computer accounts. Every account on a network is issued a unique SID when the account is first created. Internal processes in Windows refer to an account's SID rather than the account's user or group name.

Reference: www.guardianedge.com/resources/glossary/active-directory.php

QUESTION 63:

Certkiller .com has a server that runs Windows Server 2008. You installed Windows Deployment Services (WDS) role on the server. You decide to install Windows Vista on a computer that does not support Preboot Execution Environment (PXE). The Windows Vista image is stored on the WDS server. You have to start the computer and install the Windows Vista image stored on the WDS server. What should you create to achieve this task?

- A. Image Boost
- B. Discover image
- C. PXE drivers image
- D. WDS image
- E. None of the above

Answer: B

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.msp>

QUESTION 64:

Certkiller .com has a server that runs Windows Server 2008. You installed Windows Deployment Services (WDS) role on the server. You decide to install Windows Vista on a computer that does not support Preboot Execution Environment (PXE). The Windows Vista image is stored on the WDS server. You have to start the computer and install the Windows Vista image stored on the WDS server. What should you create to achieve this task?

- A. Image Boost
- B. Discover image
- C. PXE drivers image
- D. WDS image

Answer: B

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.msp>

QUESTION 65:

Certkiller .com has an Active Directory domain. You are an administrator at Certkiller .com. You administer a server named CKKMS that runs Windows Server 2008. Certkiller .com has instructed you to deploy Windows Server 2008 on 12 new servers. You install first two servers. The servers fail to activate Windows Server 2008 using CKKMS. You have to activate the new server through KMS server. What should you do to achieve this task?

- A. Configure the Windows Firewall to have Windows Management Instrumentation exceptions on the new servers.
- B. Complete the installation of the remaining 10 servers
- C. Install Volume Activation Management Tool (VAMT) on the CKKMS server and

- configure Multiple Activation Key (MAK) service
D. Install VAMT and configure MAK independent activation
E. All of the above

Answer: B

Explanation:

To activate the new server through KMS server, you should complete the installation of the remaining 10 servers. The Key Management Service is a Windows service. KMS is a trusted mechanism that, once the KMS host is activated, allows volume client computers within the enterprise to activate themselves without any interactions with Microsoft. KMS activation of Windows Server 2008 follows a hierarchical structure. Each successive product group can activate all the groups below it, and the KMS can be hosted on any edition that it can activate.

QUESTION 66:

Certkiller .com has a single Active Directory domain called certkiller.com. All servers in the domain run Windows Server 2008. There are two domain controllers in the network: ED1 and ED2 and the DNS service is installed on the domain controllers. Both DNS servers host Active Directory integrated zones that are configured to allow the most secured updates. ED1 has a Key Management Services (KMS) installed and activated. During maintenance, you find that the service locator records from the certkiller.com zone hosted on CK2 and CK2 are missing. You have to force registration of the KMS service locator records in the Certkiller .com zone. What should you do to correct this problem?

- A. Execute slmgr.vbs script on ED1 at the command prompt
- B. Configure non-secure updates on certkiller.com
- C. Execute the net stop netlogon command on ED2 and run net start logon command
- D. At the command prompt on ED1, run net stop sppsvc command and after that execute the net start sppsvc command

Answer: D

Explanation:

To force registration of the KMS service locator records in the Certkiller .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 Certkiller .com zone.

QUESTION 67:

Certkiller .com has an Active Directory domain. You are the administrator of a server named CKKMS that runs Windows Server 2008. You install and configure Key Management Service (KMS) on KMS1. You plan to deploy Windows Server

2008 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 to achieve this task?

- A. Configure Windows Management Instrumentation (WMI) exceptions in Windows Firewall on the new servers.
- B. Install Volume Activation Management Tool (VAMT) on the KMS server and configure Multiple Activation Key (MAK) Proxy Activation.
- C. Install Volume Activation Management Tool (VAMT) on the KMS server and configure Multiple Activation Key (MAK) Independent Activation.
- D. Complete the installation of the remaining eight servers.
- E. None of the above

Answer: D

Explanation:

To activate the new servers using KMS server, you should complete the installation of the remaining eight servers. The Key Management Service is a Windows service. KMS is a trusted mechanism that, once the KMS host is activated, allows volume client computers within the enterprise to activate themselves without any interactions with Microsoft. KMS activation of Windows Server 2008 follows a hierarchical structure. Each successive product group can activate all the groups below it, and the KMS can be hosted on any edition that it can activate.

QUESTION 68:

Certkiller .com has a server named CKV1 which runs Windows Server 2008 and Microsoft Hyper-V. 30 virtual machines are hosted on CKV1. Certkiller .com has instructed you to configure CKV1 to shut down each virtual machine running on it before it shut downs itself. What should you do to achieve this task?

- A. Open the Automatic stop action properties on each virtual machine and Enable the Shut down the guest operating system option.
- B. Write a custom shutdown script for each virtual machine
- C. Open the Automatic stop action properties on each virtual machine and Disable the Never shut down option.
- D. Open the general properties of each virtual machine and Enable the Shut down on Prompt option.
- E. None of the above

Answer: A

Explanation:

To ensure that each virtual machines running on the server shuts down before the server shutdown, you should enable the Shut down the guest operation system option in the Automatic stop action properties on each virtual machine. When you enable the Shut

down the guest operating system option, the server turns off the virtual machines before shutting down itself. It is very important to shut down the virtual machines before shutting down the server because it can corrupt the virtual machine files. The Automatic Stop action properties can be accessed on the virtual machine.

QUESTION 69:

Certkiller .com has a Windows Server 2008 server that has a Windows Server Virtualization (WSv) server role installed on it. You create a new virtual machine. You have to configure the network communications between the virtual machines and the host server. You also need to configure it to prevent communications with other network servers. What should you do first to achieve this task?

- A. Configure a Microsoft Loopback Adapter
- B. Configure the interface card to broadcast a unique IP address for the virtual machine
- C. Create and configure a virtual network switch
- D. Configure the Internet Connection Sharing
- E. None of the above

Answer: C

Explanation:

To configure the network communications between the virtual machines and the host server and prevent communications with other network server, you have to create and configure a virtual network switch. Like traditional network security switches, the virtual switch integrates network policy enforcement and access control. The product features virtual network partitioning, a firewall, and virtual network discovery capabilities. It also secures communication between virtual environments and enables policy based switching and traffic monitoring.

Reference:http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1307117,00.html

QUESTION 70:

Certkiller .com hosts a single Active Directory domain. All servers have Windows Server 2008. You are instructed to install an iSCSI storage area network (SAN) for a group of file servers. Corporate security policy requires that all data communication to and from iSCSI SAN must be very secure. You are assigned the task to implement the highest security available for communications to and from the iSCSI SAN. What should you do to achieve this task?

- A. Create a Group Policy Object (GPO) to enable System objects
- B. Create a Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv2) authentication in iSCSI Initiator Properties.
- C. Open iSCSI Initiator Properties and implement IPsec security. Set up inbound and outbound rules by using Windows Firewall
- D. Open iSCSI Initiator Properties and implement Secure Mode transition. Set outbound

and inbound rules by using Windows Defender

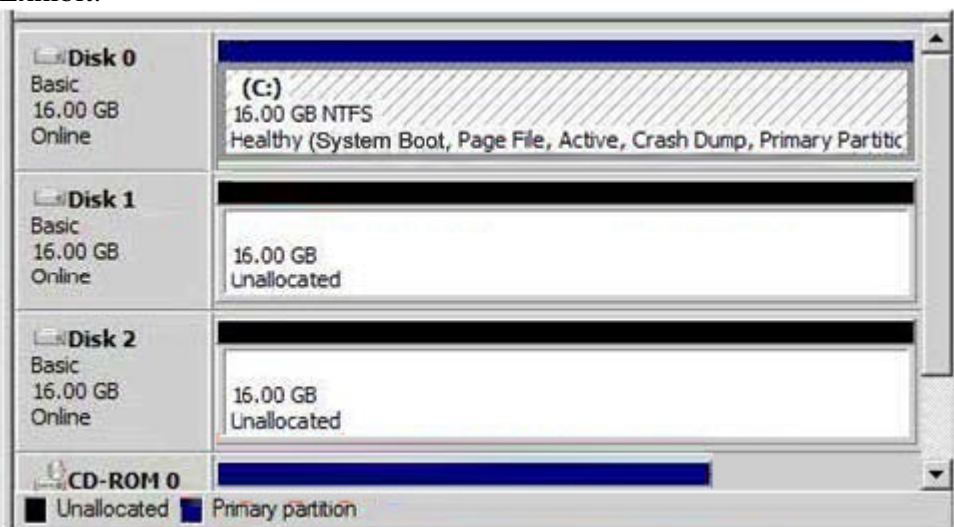
Answer: C

Explanation:

To implement the highest security available for communication to and from iSCSI SAN, you should implement IPSec security. You can access the IPSec security by opening the iSCSI Initiator Properties. After that you need to set inbound and outbound rules by using Windows Firewall.

QUESTION 71:

Exhibit:



Certkiller .com has servers that run Windows Server 2008. It also has a single Active Directory domain. You are an administrator of a server called EFS. A file services role is installed on EFS. Certkiller .com requires the data disk drives to provide redundancy. The disks are configured as shown in the exhibit. You have to configure the hard disk drives to support RAID 1. What should you do to achieve this task? (Choose two answers. Each answer is the part of a complete solution)

- A. Create a group volume by using Disk1 and Disk 0
- B. Create Disk1 and Disk 2 as dynamic drives
- C. Create and configure a striped volume across Disk1 and Disk2
- D. Using the Disk 1 and Disk 2, create a new mirrored volume

Answer: B, D

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.msp

QUESTION 72:

Certkiller .com has a server running Windows Server 2008. Windows Server Virtualization role service is installed on this server. For maximum storage capacity you need to merge a parent disk and a differencing disk. What should you do to achieve this task?

- A. Edit the differencing disk
- B. Edit parent disk
- C. Configure the Merge settings on differencing disk
- D. Configure the Merge settings on Parent disk

Answer: A

Explanation:

For maximum storage capacity, you need to merge a parent disk and a differencing disk by editing the differencing disk. A differencing disk is a child and it can be merged with the parent disk. The differencing disk stores all changes that would otherwise be made to the parent disk if the differencing disk was not being used. The differencing disk provides an ongoing way to save changes without altering the parent disk. You can use the differencing disk to store changes indefinitely, as long as there is enough space on the physical disk where the differencing disk is stored. The differencing disk expands dynamically as data is written to it and can grow as large as the maximum size allocated for the parent disk when the parent disk was created.

Reference:

<http://technet2.microsoft.com/windowsserver/en/library/d9ef5bd9-6ca2-488b-a960-f3f8ecd6ecc51033.msp>

QUESTION 73:

DRAG DROP

Certkiller .com has a server that runs Windows Server 2008 and has Microsoft Hyper-V installed on it. It is called CKVS. CKVS hosts 10 virtual servers. One of the virtual servers named VSV has one 64 GB fixed size virtual hard disk (VHD). The VHD file is named disk0.vhd.

While testing the VSV, you find out that it utilizes only 5 GB of the VHD. You turn off the VSV to make the disk1.vhd file as small as possible. What should you do to achieve this task? (To answer, move the appropriate tasks from the list of tasks to the answer area and arrange them in the correct order.)

Steps, Select from these	Steps, place here
Create a new difference VHD file named disk2.vhd that has disk1.vhd as a parent disk.	Place first step here
Compact the disk2.vhd file	Place second step, if any, here
Delete the disk1.vhd file. Rename disk2.vhd to disk1.vhd	Place third step, if any, here
Convert the disk1.vhd file to a new dynamically expanding VHD file named disk2.vhd	Place fourth step, if any, here
Convert the disk2.vhd file to a new fixed-size VHD file named disk1.vhd.	Place 5th step, if any, here

Answer:

QUESTION 74:

Certkiller .com has a Terminal Server running Windows Server 2008. Through Terminal Services RemoteApp (TS RemoteApp), you create a Windows Installer package for the Microsoft Office Word 2007. After installing the package on a client machine, you double-click on a Word document and receive the error, "Windows cannot open this file". You have to make sure that you can open the Word Document by double clicking on the file. What should you do to solve this problem?

- A. use msixexec.exe to install the windows installer package
- B. Delete the windows installer package and re-create a new one
- C. Change the file association on the TSRemoteApp server
- D. Create the Windows installer package again by using TSRemoteApp

Answer: C

Explanation:

To make sure you can open the Word document file after installing MS Word 2007 on the client machine using Terminal services RemoteApp, you should change the file association on the TSRemoteApp server.

Reference:<http://forums.technet.microsoft.com/fr-FR/winserverTS/thread/213c907c-7d0c-43d7-970c-2226>

QUESTION 75:

You are an administrator at Certkiller .com. You manage a server named CK2 that

runs Windows Server 2008. You are instructed to publish an application using Terminal Services. All users must be able to connect to the Terminal Services application by using Remote Desktop Protocol. To achieve this, you install and configure the Terminal Services Gateway (TS Gateway) role service on CK2 . You also configure a default domain policy to enable the Enable Connection through TS gateway setting. But Users report that they cannot connect to the Terminal Services application. What should you do to ensure that the users can access the Terminal Services application on the intranet from the Internet?

- A. Disable the Enable Connection through TS Gateway Group Policy setting
- B. Configure the Remote Desktop connection on each client computer to Always Connect even if the server authentication fails.
- C. Create a GPO and link the TS Gateway server authentication to the domain
- D. Create and configure the Set TS Gateway server address Group Policy and also configure the IP address of the TS Gateway server. Link the configured GPO to the domain

Answer: D

Explanation:

To ensure that the users can access the Terminal Services application on the intranet from the internet, you should create and configure the Set TS Gateway server address group policy and also configure the IP address of the TS Gateway server. After that, link the configure GPO to the domain.

[QUESTION 76:](#)

Certkiller .com has an Active Directory domain. All servers in the domain run Windows Server 2008. You install a Terminal Services Gateway (TS Gateway) role service on a server named S11. The Terminal services role is installed on servers called S2 and S3. Both of these servers are configured in a load balancing Terminal Server farm named as TSFrm. You install and configure the Terminal Services (TS) Session Broker service on a new server named S4. You need to configure S2 and S3 to join the TS Session Broker. What should you do to achieve this task?

- A. Create a new Group Policy object (GPO) that assigns S4 to S2 and S3 as their session broker server. Apply the GPO to S2 and S3.
- B. Configure a Group Policy object (GPO) to set the Set TS Gateway server address option in the Terminal Services Security section to Server1. Apply the GPO to all client computers.
- C. Configure S2 and S3 to use the TS Gateway role service to access TS Session Broker.
- D. Configure a Group Policy object (GPO) to set require secure RPC communications option in the Terminal Services Security section to False. Apply the GPO to S2 and S3.

Answer: A

Explanation

To configure S2 and S3 to join the TS session broker, you should create a new GPO that assigns S2, S3 and S4 as their session broker server. After that you can apply the GPO to S2 and S3. The Group Policy Object will enable all three servers to act as session broker server and when you apply the GPO to the S2 and S3 server, both servers join the TS session broker.

QUESTION 77:

Certkiller .com has an active directory domain. You are the administrator of ES1, a server that runs Windows Server 2008 and has Terminal Services role and the Terminal Services Web Access role service installed on it. You install Terminal Services Gateway role on ES1 and create the Terminal Services connection authorization policy. Users are reporting that they cannot access ES1. What should you do to ensure that the users can connect to ES1?

- A. Install and configure the Terminal Services Resource Authorization Policy (RAP) on ES1
- B. Configure the Network Access Protection on ES1 and start the Terminal services gateway service
- C. Create a Terminal Services Group Policy Object and allow users to connect remotely to the Terminal services setting on the GPO. Link the GPO to the domain controller
- D. Create a Terminal services GPO and Set the TS Roaming profiles setting on the GPO
- E. None of the above

Answer: A

Explanation:

To ensure that the users can connect to ES1, you should install and configure the Terminal Services Resource Authorization Policy on ES1. RAP's are used to control which Terminal Servers can be accessed through the Terminal Services Gateway.

Reference:

<http://www.windowsecurity.com/articles/Configuring-Windows-Server-2008-Terminal-Services-Gateway-Part2>

QUESTION 78:

You are an Administrator at Certkiller .com. you manage a member server that runs Windows Server 2008. The Terminal Server Gateway (TS Gateway) is also installed on the member server. You want to find out whether a group of users have ever connected to their workstations remotely through TS Gateway server. What should you do to achieve this task?

- A. Open the TS gateway console and view the events in the monitoring field
- B. View the Windows Server 2008 Event Viewer for TS Gateway connections
- C. View Event Viewer security log
- D. View the Event Viewer Terminal Services-gateway log

Answer: D

Explanation:

To find out whether a group of users have ever connected to their workstations remotely through TS Gateway Server, you should check the Event View Terminal Services-gateway log. You can access the Event Viewer Terminal Services-gateway log through the Windows Event Viewer. The log will tell you about the connections made to the workstation through TS Gateway server.

QUESTION 79:

Certkiller .com has an Active Directory domain installed on a server that runs Windows Server 2008. Another server named S3 also runs Windows Server 2008. All client machines have Windows Vista. Certkiller .com has instructed you to install the Terminal Services role, Terminal Services Gateway role and Terminal Services Web Access role service on S3. To protect the network, you want to ensure that all client machines have firewall, antivirus software and anti-spyware software installed. Which actions should you perform to achieve this task? (Select two answers. Each answer is a part of a complete solution)

- A. Configure Windows Authorization Access domain local security group and add Terminal Services client computers
- B. Configure Terminal Services client computers to access the Terminal Services health policy.
- C. Set the Request clients to send a health option statement in the Terminal Services client access policy
- D. Install and configure Network Access Protection (NAP) on the server in the domain

Answer: C, D

Explanation

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

QUESTION 80:

Certkiller .com has an Active Directory domain. Terminal Services is installed on a server. All terminal services accounts are configured to allow session takeover without permission. A user logged on to a server named S2 using an account named U1. The terminal session ID for U1 is 1209. Which command should you run to perform a session takeover for Terminal session ID 1209?

- A. Beown/U U1 1209, and the execute TSconnection 1209
- B. Tsdicon 1209, and then Tscon 1209
- C. Chgport/U U1 1209

- D. chguser 1209, Tscon 1209
- E. None of the above

Answer: B

Explanation:

To perform a session takeover for the Terminal session ID 1209, you should run Tsdicon 1209 and then Tscon 1209. You can use the tsdiscon command to disconnect an active Terminal Services session. The session remains attached to the Terminal Services server in a disconnected state. Programs that are currently in use continue to run. When you reconnect to the Terminal Services server, you can reconnect by using the same session from which you disconnected. You can resume working without any loss of data in the programs that were running when you disconnected. You can use the tscon command to connect to another Terminal Services user session. You can connect to sessions that are in an active or disconnected state. When you connect to another session, you are disconnected from your previous session. If you create more than one session on a server, you can use this option to switch between the sessions.

Reference: <http://support.microsoft.com/kb/321703> -

<http://support.microsoft.com/kb/321705>

QUESTION 81:

As an administrator at Certkiller .com, you install Web server (IIS) role on a server that runs Windows Server 2008. You created a new site called Certkiller .com. You need to install an application on the website called webcontent. You copy the application to the server. What should you do to add the application on the website?

- A. Create a virtual directory and copy the website contents in it. Copy the application in the directory and install it
- B. Execute appcmd command on the command prompt on the server
- C. Open the IIS Manager Console and select the website. Select Add Application
- D. Execute appcmd -t on the command prompt on the server
- E. None of the above

Answer: C

Explanation

To add the application on the website, you should use IIS Manager Console and select the website. The website is listed in the IIS Manager Console and you can access it through the navigation tree. Right-click on the website name and select 'Add Application'. The wizard will walk you through the process of adding the application to a website.

Reference: www.tech-faq.com/securing-webservers.shtml

QUESTION 82:

Certkiller .com has a server running Windows Server 2008. The Web Server (IIS)

server role is also installed on it. The IIS server hosts a Website. You are instructed to ensure that the cookies sent from the Website are encrypted on users' computer. Which website feature should you configure to achieve this task?

- A. Controls and Pages
- B. Authorization Rules
- C. Machine Key
- D. IIS Secure Socket Layer configuration
- E. None of the above

Answer: C

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 web servers may be in no affinity mode.

Reference:

<http://www.codeproject.com/KB/web-security/HttpCookieEncryption.aspx>

QUESTION 83:

Certkiller .com has a server that runs Windows Server 2008. You install the Web Server (IIS) role on this server. The server hosts company's default website with an IP address of 23.52.10.1. Certkiller .com has instructed you to add a Website on the server named Customer Service. After doing necessary configurations, you find out that the Customer Service Website cannot be started. What should you do to configure and start Customer Service website?

- A. Configure Customer Service Website to use a host header
- B. Execute iisreset/enable command on the server
- C. Execute iisconfig/renew command and add /name: Customer Service/id:1/physicalPath: c:\Customer Service/binding: port 50
- D. Execute the iisreset/start Customer Service:8080 command on the server

Answer: A

Explanation:

To get the customer website started, you need to configure the website to use a host header. 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.Certkiller.com> is www.Certkiller.com.

Reference: <http://www.visualwin.com/host-header/>

QUESTION 84:

Certkiller .com has a server that runs Windows Server 2008. You have installed the Web Server (IIS) role on it. Certkiller plans to host multiple websites on the server. To achieve this you configure a single IP address on the server. You also configure all websites to be registered in DNS to point to the single IP address configured on the server. You have to make sure that each and every website responds only to the name requests from all client machines. What should you do to achieve this task?

- A. Configure the primary and secondary DNS to point to the server's IP address
- B. Configure a network address for each website
- C. Assign a unique port for each website
- D. Configure and assign a unique Host Header to each website

Answer: D

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.Certkiller.com> is www.Certkiller.com.

Reference: <http://www.visualwin.com/host-header/>

QUESTION 85:

You are an administrator at Certkiller .com. You are instructed to implement a member server that runs Windows Server 2008. Web Server (IIS) role is also installed on the member server. The primary purpose of the member server is to host intranet websites. The company policy dictates that a server should:

1. use encryption for all authentication traffic to the intranet website
2. Avoid SSL on the web server for performance reasons
3. Authenticate users through Active Directory credentials

What should you do to configure all websites on the server according to the company policy? (Choose three answers. Each answers is a part of the complete solution)

- A. Enable the Active Directory Client Certificate Authentication on the server
- B. Disable the Basic Authentication setting on the server
- C. Enable Digest Authentication setting on the server
- D. Enable Windows Authentication setting on the server
- E. Disable Anonymous Authentication setting on the server

Answer: C, D, E

Explanation

To configure all website on the server according to the company policies, you should first disable Anonymous Authentication setting on the server and then enable Digest Authentication and Windows Authentication settings on the server.

Reference: <http://support.microsoft.com/kb/810572>

QUESTION 86:

Certkiller .com has a server that runs Windows Server 2008. A Web Server (IIS) server role is installed on the server. The server hosts a website that is configured to use only Windows Authentication. The company has a security group named EG1 which contains 50 user accounts. You need to prevent this group from accessing the website while allowing all other to access the website. Which website feature should you configure to achieve this task?

- A. Group Access Policy
- B. Authorization Rules
- C. IIS group permissions
- D. SSL certificates
- E. None of the above

Answer: B

Explanation:

To prevent a group from accessing the website while allowing all others to access it, you should configure Authorization rules for the website.

Authorization rules are scripts, written in VBScript or JScript that you can include in role definitions and task definitions. An authorization rule determines whether the role or task is allowed. For information about role definitions and task definitions

Reference:

<http://technet2.microsoft.com/windowsserver/en/library/8f2db3a0-feb4-4b7f-91fe-dcb29899a10d1033.msp>

QUESTION 87:

Certkiller .com has a server that runs Windows Server 2008. You install the FTP role service on the server. Users complain that they receive an error message while uploading files to the FTP site. You have to allow authenticated users to upload files to the FTP site. What should you do to achieve this task?

- A. Execute the FTP -authenticate 192.168.10.23 command on the Windows Server 2008 server
- B. Set write permission on the FTP site. Configure the NTFS permission on the FTP destination folder for the Authenticated users group
- C. Set the Write permissions on the FTP site. Set NTFS permission on the FTP

destination folder for the Authenticated Users group to Allow-Modify
D. Execute appcmd -ftp command on the server to unlock Config.txt file

Answer: C

Explanation:

To allow authenticated users to upload files to the FTP site, you should set the Write Permission on the FTP site folder and set NTFS permission on the FTP destination folder for the Authenticated Users group to Allow-Modify. By setting the write permission on the FTP site folder, you will enable the authenticated users to access the FTP site. By setting NTFS permission on the FTP destination folder, you allow the Authenticated Users group to modify the files and add or delete them.

QUESTION 88:

Certkiller .com has a Windows Server 2008 server named S1. You have installed Web Server (IIS) server role on S1. The server has an SMTP gateway that connects to the internet. You have an internal firewall installed on the network which prevents all client machines from establishing a connection to the internet except the SMTP gateway over TCP port 25. You configure the SMTP gateway to relay e-mail for S1. What should you do to configure a website on S1 to send email to internet users?

- A. Install and configure SMTP server feature on S1
- B. Configure the SMTP email feature for the website on S1
- C. Create a DNS server on S1 and configure the SMTP mail service
- D. Create an MX record for the SMTP gateway on an internal DNS server
- E. None of the above

Answer: B

Explanation:

To configure a website on a server to send email to the internet users, you should configure the SMTP email feature for the website on that server. The Simple Message Transfer Protocol allows the emails to be sent to a specific address.

Reference:

<http://technet2.microsoft.com/windowsserver2008/en/library/4ade618d-ff7a-4359-b6ba-4982f0bdf4a51033>

QUESTION 89:

You are an administrator at Certkiller .com. You have been instructed to install Web Server (IIS) on a new Windows Server 2008 server. After installing IIS, you install Microsoft .NET framework 1.0 application on a website hosted on the server. You also have to make sure that all applications must run on a minimum level of permission according to the company security policy. You should configure the website application to have permissions to execute without creating other content or

accessing Windows Server 2008 system components. What should you do to achieve this task?

- A. Configure the .NET Framework website trust level to low
- B. Configure the .NET Framework website trust level to High
- C. Configure the .NET Framework website trust level to Full
- D. Configure the .NET Framework website trust level to Medium
- E. Configure the .NET Framework website trust level to Optimal

Answer: C

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:

1. My Computer - The application code is hosted directly on the user's computer.
2. Local Intranet - The application code runs from a file share on the user's intranet.
3. Internet - The application code runs from the Internet.
4. Trusted Sites - The application code runs from a Web site that is defined as "Trusted" in Internet Explorer.
5. 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 90:

Certkiller .com has 20 servers that run Windows Server 2008. All servers have Web server (IIS) server role installed. Being the members of a server farm, all servers host the same website. Certkiller .com has instructed you to configure the servers to meet the minimized administrative effort policy. You need to configure the servers to allow web server configuration changes been made on one server to be made on all the servers in the farm. You have to make sure that the administrative effort to perform the configuration changes is minimized. What should you do to achieve this task?

- A. Create a scheduled task on a single server and copy the Inetpub folder and put it on all the servers
- B. Configure the shared configuration group policy and apply it on all the servers
- C. Create a script that enables a single server to impose its configuration settings on all other servers
- D. Configure the Shared Configurations setting on all servers

E. None of the above

Answer: D

Explanation:

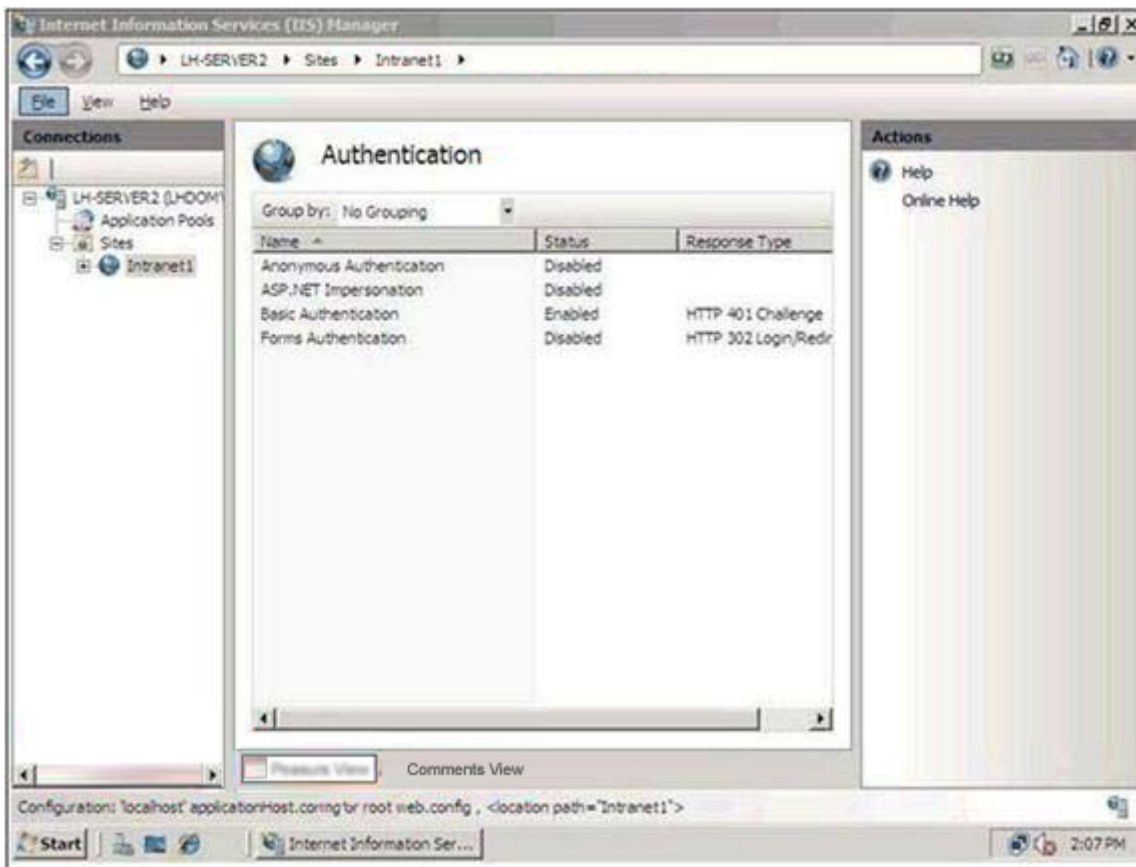
To ensure that the administrative effort to perform the configuration changes is minimized, you should configure the shared configurations setting on all servers. This will allow a Config file to be shared among other servers and they can use that file to update their configuration settings.

Reference:

<http://technet2.microsoft.com/windowsserver2008/en/library/8941cb68-2833-4788-9ef3-8714fe9113001033.msp>

QUESTION 91:

Exhibit:



As an administrator at Certkiller .com, you manage a member server that runs Windows Server 2008. The Web Server (IIS) role is also installed on the member server. The web server hosts an intranet website called intranet-e. The intranet-e is only accessed by internal active directory users. As shown in the exhibit, the authentication settings for intranet-e are basic. You have to ensure that the users accessing the website are authenticated through Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) encrypted Active Directory

credentials. What should you do to achieve this task? (Choose two answers. each answer is the part of a complete solution)

- A. Add Windows Authentication role service to the IIS server. Enable the Windows Authentication settings in the intranet-e properties
- B. Configure Digest Authentication role service on IIS server and add URL authentication role service to the server.
- C. Disable the basic authentication and set the Anonymous Authentication to enabled in the intranet-e properties
- D. Add the internal Active Directory users to the IIS Access Permissions and use Basic Authentication in Intranet-e properties
- E. Disable the basic authentication setting in the intranet-e properties

Answer: A, E

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 92:

As an administrator at Certkiller .com, you have installed a new server named MS12 that runs Windows Server 2008. This server should be used for steaming media purposes. So you install Streaming Media Services role on the server. Since all client machines have Windows Vista as their operating system and they only use Windows Media Player 11 application, you configure a Publishing Point and assign source of content that has video media. Users report that they are unable to pause and rewind the video using Windows Media Player 11. What should you do to ensure that users have full playback control of the streaming media?

- A. Set and configure Real Time Streaming Protocol (RTSP) on MS12
- B. Reconfigure the Publishing Point as an on-demand publishing point
- C. Uninstall and then reinstall the Publishing Point
- D. Configure the MS12 server to use Simple Object Access Protocol (SOAP) instead of Publishing Point
- E. None of the above

Answer: B

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.msp>

QUESTION 93:

Certkiller .com has instructed you to install Windows Server 2008 on a new server. You are instructed to install Streaming Media Services role on the server. Users have both Windows Vista and MAC machines. They use Windows Media Player on both Windows and MAC computers. What should you do install Streaming Media Services role on the server with the support for both media players?

- A. Install and configure Simple Object Access Protocol (SOAP) on the server
- B. Install HTTPS on the server and use RPC
- C. Install and configure Windows Media Streaming Protocol (WMSP)
- D. Install and configure Real Time Streaming Protocol (RTSP)
- E. None of the above

Answer: A

Explanation:

To install Streaming Media Services role on the server with the support for both media players, you should install and configure Simple Object Access Protocol (SOAP) on the server. SOAP is a lightweight protocol for exchange of information in a decentralized, distributed environment. It is an XML based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses. SOAP can potentially be used in combination with a variety of other protocols; however, the only bindings defined in this document describe how to use SOAP in combination with HTTP and HTTP Extension Framework.

Reference: <http://whitepapers.techrepublic.com.com/abstract.aspx?docid=17638>

QUESTION 94:

Certkiller .com has a server that runs Windows Server 2008. You plan to publish an

audio file on the internet. You install Windows Media Services server role on the server to publish the audio file using Media Server. To protect the file, you need to create a license for the audio file. What should you do first to achieve this task?

- A. Create a new site and publish the audio file
- B. Use Media Rights Manager to package the audio file
- C. Publish the audio file on Windows Media Services server
- D. Create a MPEG server on Windows Media services server and package the file with Windows Installer application
- E. None of the above

Answer: B

Explanation:

To create a license for the audio file, you need to use Media Rights Manager to package the audio file. When a consumer acquires an encrypted digital media file from a Web site, he or she must also acquire a license that contains a key to unlock the file before the content can be played. Content owners can easily set these licenses and keys in motion by protecting their content files with Microsoft(r) Windows Media(r) Rights Manager and then distributing the content to consumers.

Reference:<http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx>

QUESTION 95:

As a senior administrator at Certkiller .com, you manage a server named ERA1 that runs Windows Server 2008. It has the Windows SharePoint Services (WSS) role installed in a standalone mode. You also manage another server called ERA2. For a big project, you install WSS role on ERA2. You indicate during the installation that the ERA2 must be the member of a WSS server farm. But you are unable to connect to ERA1 in the WSS server farm. What should you do to configure both ERA1 and ERA2 in the WSS server farm?

- A. reduce the Microsoft .NET Framework Trust Level to Low on both ERA1 and ERA2
- B. Reconfigure the Web Management Service on ERA1
- C. Set the Microsoft .NET Framework Trust Level to High on both ERA1 and ERA2
- D. Uninstall the WSS on ERA1 and select the server farm mode while reinstalling it.
- E. None of the above

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.mspix?mfr=true>

QUESTION 96:

Certkiller .com has a server that runs Windows Server 2008. You have installed Windows SharePoint Services (WSS) role on the Windows Server 2008 server. You want to configure WSS to support SMTP. What should you do to achieve this task?

- A. Reinstall the WSS role
- B. Open the Server Manager console and install Application Server
- C. Configure port 25 for WSS role
- D. Open the Server Manager console and install the SMTP Server feature
- E. None of the above

Answer: D

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 e-mail 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 97:

You manage a server that runs Windows Server 2008. You have installed the Windows SharePoint Services (WSS) server role on the server. The server is configured to accept incoming mail. To streamline the process, you create a new document library. You have to make sure that any user can send email to the document library. What should you do to achieve this task?

- A. Change the incoming email settings for the document library
- B. Enable basic user authentication for the document library
- C. Modify the document library settings to accept emails from SMTP servers
- D. Change the permissions for the document library

Answer: A

Explanation:

To ensure that any user can send email to the document library, you should change the incoming mail settings for the document library.

Reference: [http://technet.microsoft.com/en-us/library/cc262947\(TechNet.10\).aspx](http://technet.microsoft.com/en-us/library/cc262947(TechNet.10).aspx)

QUESTION 98:

You are an enterprise administrator for Certkiller .com. All the servers on the network run Windows Server 2008. The network consists of a server called Certkiller Server1 that runs Microsoft Hyper-V and hosts three virtual machines. To fulfill a network requirement, you need to configure all of the virtual machines to connect to each other. However, the company policy states that the virtual machines must not connect to the company network.

Which of the following options would you choose to ensure that all the virtual machines connect to each other and you meet the company policy also?

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

Answer: B

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.msp>

QUESTION 99:

You are an enterprise administrator for Certkiller .com. The company runs Windows Server 2008 on all the servers on the network. The Windows Server virtualization role service installed on two servers called Certkiller Server1 and Certkiller Server2.

Which of the following options would you choose to remotely manage the virtualization settings of Certkiller Server2 from Certkiller Server1?

- A. From the Virtualization Management Console, right-click Virtualization Services and then click Connect to Server.
- B. Run vmconnect.exe Certkiller Server2.
- C. Run vmconnect.exe Certkiller Server1 Certkiller Server2.
- D. From the Virtualization Management Console, right-click Certkiller Server1 on the left pane, point to New, and then click Virtual machine.

Answer: A

Explanation:

To remotely manage the virtualization settings of Certkiller Server2 from Certkiller 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 100:

You are an enterprise administrator for Certkiller .com. All the servers on the network run Windows Server 2008. The network consists of a Server that has the Windows Server virtualization role service installed.

You create a new virtual machine, installed Windows Server 2008 on it, and configure it to use the physical network card of the host server. After this installation and configuration the virtual machine, you were unable to access network resources from the virtual machine.

Which of the following options would you choose to ensure that the virtual host can connect to the physical network?

- A. Install the MS Loopback adapter on the virtual machine.
- B. Enable the Multipath I/O feature on the host server.
- C. Install Windows Server virtualization Guest Integration Components on the virtual machine.
- D. Install the MS Loopback adapter on the host server.
- E. None of the above

Answer: C

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=6&paged=3>

QUESTION 101:

You are an enterprise administrator for Certkiller .com. The corporate network of the company consists of an Active Directory domain. All the servers on the network run Windows Server 2008. The network runs Terminal services to enable remote users to run commonly required applications from their terminal.

A remote user logged on to the Terminal Server, required some help on the application he wanted to run. However, when you connect to the Terminal Server session, you cannot operate any applications. Which of the following options would you choose to ensure that you can assist any user on the Terminal Server?

- A. From the Terminal Server, run the Chgusr /execute command and then reconnect to the session.
- B. In the RDP-Tcp Properties on the Terminal Server, enable the Use remote control option with default user settings.
- C. In the RDP-Tcp Properties on the Terminal Server, enable the Use remote control with the following settings option and then configure the Level of control policy setting to Interact with the session. Ask the user to log off and log back on.
- D. From the Terminal Server, run the Tscon /v command and then reconnect to the session.

Answer: C

Explanation:

To ensure that you can assist any user on the Terminal Server, you need to enable the Use remote control with the following settings option and then configure the Level of control policy setting to Interact with the session. Ask the user to log off and log back on. You can configure remote control with the Level of control to Interact with the session. When this option is selected, the user's session can be actively controlled with your keyboard and mouse.

Reference

: Need to monitor a terminal services session? Use Shadow. / How to Configure Remote Control Settings

<http://www.myitforum.com/articles/16/view.asp?id=5808>

QUESTION 102:

You are an enterprise administrator for Certkiller .com. The corporate network of the company consists of an Active Directory domain. All the servers on the network run Windows Server 2008. The network runs a Terminal server named Certkiller Server2 to enable remote users to run commonly required applications from their terminal.

You have recently been asked to deploy a Terminal Services application called App1 on Certkiller Server2. To deploy the application, you first confirmed from the application vendor that the application can be deployed in a Terminal Services environment.

The features of App1 are that it does not use Microsoft Windows Installer packages for installation and makes changes to the current user registry during installation.

Which of the following options would you choose to install the application to support multiple user sessions? (Select all that apply)

- A. Run the change user /install command on Certkiller Server2
- B. Install the application.
- C. Run the change user /execute command on Certkiller Server2.
- D. Run the change logon /disable command on Certkiller Server2.
- E. Run the change logon /enable command on Certkiller Server2.
- F. Run the mstsc /v: Certkiller Server2/console command from the client computer to log on to Certkiller Server2.

Answer: A, B, C

Explanation:

To install the application to support multiple user sessions in the above scenario, you need to first run the change user /install command on Certkiller Server2 because You must put a Terminal Services server in Install mode to install or remove programs on the server. You can put a Terminal Services server in Install mode either by using the Add/Remove Programs tool in Control Panel to add or remove a program, or by using the change user command at a command prompt. You need to then install the application. When you are finished installing the program, you need to return the Terminal Services server to Execute mode, to execute the application. Therefore, to return to the Execute mode, you need to run the change user /execute command on Certkiller Server2.

Reference: HOW TO: Use the CHANGE USER Command to Switch to Install Mode in Windows 2000 Terminal Services

<http://support.microsoft.com/kb/320185>

QUESTION 103:

You are an enterprise administrator for Certkiller .com. The corporate network of the company consists of a single Active Directory domain. All the servers on the network run Windows Server 2008 and all the client computers run Windows Vista. All computers are members of the domain. The network runs a Terminal server named Certkiller Server2.

You have recently deployed an application called App1 by using the TS RemoteApp

Manager. You set the Terminal Servers security layer to Negotiate. Which of the following options would you choose to ensure that domain users are not prompted for credentials when they access the application?

- A. Modify the Password Policy settings in the local Group Policy on all the client computers.
- B. Modify the Credential Delegation settings in the local Group Policy on all client computers.
- C. Modify the Credential Delegation settings in the local Group Policy on the terminal server, Certkiller Server2.
- D. Modify the Password Policy settings in the local Group Policy on the terminal server, Certkiller Server2.
- E. None of the above

Answer: B

Explanation:

To ensure that domain users are not prompted for credentials when they access the application, you need to modify the Credential Delegation settings in the local Group Policy on all client computers.

Windows Vista introduces a new authentication package called the Credential Security Service Provider, or CredSSP, that provides a single sign-on (SSO) user experience when starting new Terminal Services sessions. CredSSP enables applications to delegate users' credentials from the client computer (by using the client-side security service provider) to the target server (through the server-side security service provider) based on client policies. CredSSP policies are configured via Group Policy, and delegation of credentials is turned off by default.

In addition, a few of the policy settings might increase or decrease the risk. For example, the Allow Default Credentials with NTLM-only Server Authentication and Allow Fresh Credentials with NTLM-only Server Authentication policy settings remove the restriction to require the Kerberos authentication protocol for authentication between the client and server.

Reference: Credential Security Service Provider and SSO for Terminal Services Logon
<http://technet2.microsoft.com/WindowsVista/en/library/6b6bf605-0b9f-45ed-9900-12aca2a0f2a21033.msp?mfr>

QUESTION 104:

You are an enterprise administrator for Certkiller .com. The corporate network of the company consists of a single Active Directory domain. All the servers on the network run Windows Server 2008 and all the client computers run Windows XP Service Pack 2 (SP2). All computers are members of the domain.

The network runs a server named Certkiller Server1 on which the Terminal Services role and the Terminal Services Web Access role are installed. The Network Level Authentication is enabled on the server. The Terminal Services Web Access role uses Active Directory Domain Services (AD DS).

You have been assigned the task to deploy and publish an application called App1 on Certkiller Server1. Which of the following options would you choose to ensure that the users can launch App1 on Certkiller Server1 from the Terminal Services Web Access Web page?

- A. Publish App1 on Certkiller Server1 as a Microsoft Windows Installer package. Distribute the Windows Installer package to the users.
- B. Install the Terminal Services Gateway (TS Gateway) role on Certkiller Server1 and then reconfigure the remote application publishing for App1 to reflect the change.
- C. Disable publishing to AD DS for the App1.
- D. Install the Remote Desktop Client 6.1 application on the client computers.
- E. None of the above

Answer: D

Explanation:

To ensure that the users can launch App1 on Certkiller 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 Certkiller 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 105:

You are an enterprise administrator for Certkiller .com. The company runs Windows Server 2008 on all the servers on the network. The company has many remote users

One of the servers on the network called Certkiller Server1 has the Terminal Services Gateway (TS Gateway) role installed on it. The remote users of the company need to connect remotely to desktop computers located in their offices through the gateway.

To ensure secure connection to the gateway, you created a security group named RemoteUsersGrp1 for the remote users who need to connect to computers in their offices. Which of the following options would you choose to enable the remote users to connect to the TS Gateway? (Select two. Both the selected options will form a part of the answer.)

- A. Create a resource authorization policy.
- B. Create a client authorization policy.
- C. Create a Group Policy object enable the Set TS Gateway authentication method properties to Ask for credentials, use Basic protocol.

- D. Add the RemoteUsersGrp1 security group and enable Device redirection.
- E. Add the RemoteUsersGrp1 security group to the local remote desktop users group on the TS Gateway server.
- F. Add the RemoteUsersGrp1 security group and enable Users to connect to any resource.
- G. Apply the policy to the TS Gateway server.

Answer: B, D

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>

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 106:

You are an enterprise administrator for Certkiller .com. The company runs Windows Server 2008 on all the servers on the network. One of the servers, Certkiller Server1 has the Terminal Services Gateway (TS Gateway) role installed on it.

Which of the following options would you choose to provide a security group access to the TS Gateway server?

- 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 groups that can access Terminal Server through the TS Gateway through a Resource Authorization Policy.
- D. Create and configure groups that can access Terminal Server through the TS Gateway through a Connection Authorization Policy.
- E. None of the above

Answer: D

Explanation:

To provide a security group access to the TS Gateway server, you need to create and

configure a Connection Authorization Policy. A connection authorization policy (CAP) allows you to control who can connect to the Terminal Server through the Terminal Services Gateway. You can configure what groups can access the Terminal Server through the TS Gateway.

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>

QUESTION 107:

You are an enterprise administrator for Certkiller .com. The corporate network of the company consists of a single Active Directory domain. All the servers on the network run Windows Server 2008. The network consists of four servers configured as follows:

1. Certkiller Server1: The Terminal Services Gateway role service is installed.
2. Certkiller Server2: The Terminal Services role is installed and is configured in a load balancing Terminal Server farm named TSLoad.
3. Certkiller Server3: The Terminal Services role is installed is configured in a load balancing Terminal Server farm named TSLoad.
4. Certkiller Server4: Recently been perfectly configured with the Terminal Services (TS) Session Broker service that works correctly.

To handle the load distribution to the Terminal Server farm you have recently deployed a hardware load balancing device that has specialized support for terminal servers and routing tokens to the Terminal Server farm.

However, after this installation, you discovered that the TS Session Broker service has started failing. Which of the following options would you choose to ensure that the TS Session Broker works correctly?

Group Policy object (GPO) should you create and apply to the Terminal Server farm to?

- A. Create a GPO that enables the Use TS Session Broker Load Balancing policy setting in the Session Directory section of the Terminal Server Group Policy template and apply it to the Terminal Server farm.
- B. Create a GPO that disables the Use IP Address Redirection policy setting in the TS Session Broker section of the Terminal Server Group Policy template and apply it to the Terminal Server farm.
- C. Create a GPO that enables the Use IP Address Redirection policy setting in the Session Directory section of the Terminal Server Group Policy template and apply it to the Terminal Server farm.
- D. Create a GPO that disables the Use TS Session Broker Load Balancing policy setting in the Session Directory section of the Terminal Server Group Policy template and apply it to the Terminal Server farm.
- E. None of the above

Answer: B

Explanation:

To ensure that the TS Session 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 TS Session Broker section of the Terminal Server Group Policy template.

The TS Session Broker service is failing because you have recently deployed a hardware load balancing device that has specialized support for terminal servers and routing tokens to the Terminal Server farm. When routing tokens are used the IP address of the terminal 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: TS Session Broker

<http://technet2.microsoft.com/windowsserver2008/en/library/8a46c71e-cc7d-4bf0-82cc-8261f7c3069c1033.msp>

QUESTION 108:

You are an enterprise administrator for Certkiller .com. The company runs Windows Server 2008 on all the servers on the network. On the corporate network a Network Load Balancing cluster named nlb. Certkiller .com is configured. The two hosts of the cluster are named as Certkiller Web1 and Certkiller Web2.

A single port rule has been configured for the cluster according to which all HTTP traffic is evenly distributes between both the hosts.

Which of the following options would you choose to configure the cluster in such a way that Certkiller Web2 handles all HTTPS traffic for nlb. Certkiller .com while ensuring the even distribution of HTTP traffic between Certkiller Web1 and Certkiller Web2? (Choose two. Each correct answer presents part of the solution.)

- A. Change the Handling priority option for the TCP 443 port rule to the value of 0 in the properties for Certkiller Web1
- B. Create a new port rule for port TCP 443 that has the Filtering mode option set to Single host in the properties for the cluster.
- C. Change the Handling priority option for the TCP 443 port rule to the value of 1 in the properties for Certkiller Web2.
- 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: B, C

Explanation:

To configure the cluster so that Certkiller Web2 handles all HTTPS traffic for nlb. Certkiller .com evenly distribute the HTTP traffic between Certkiller Web1 and Certkiller Web2: You need to create a new port rule for port TCP 443 that has the Filtering mode option set to Single host in the properties for the cluster. The Single Host filtering mode directs the specified network traffic to a single host. For example, in an IIS

Web farm in which only one server contains the SSL certificate for a secure Web site, the single host port rule will direct port TCP 443 (SSL port) traffic to that particular server. And then in the properties for Certkiller Web2, change the Handling priority option for the TCP 443 port rule to the value of 1

In Host Parameters, the Priority (Unique host identifier) specifies the handling priority option. This parameter specifies a unique ID for each host. The host with the lowest numerical priority among the current members of the cluster handles all of the cluster's network traffic that is not covered by a port rule. You can override these priorities or provide load balancing for specific ranges of ports by specifying rules on the Port rules tab of the Network Load Balancing Properties dialog box. In this scenario there are two hosts, so the value 1 will equally distribute the load.

Reference: Network Load Balancing Step-by-Step Guide: Configuring Network Load Balancing with Terminal Services To create an NLB cluster

<http://technet2.microsoft.com/windowsserver2008/en/library/6e3fc3a6-ef42-41cf-afed-602a60f562001033.mspx>

Reference: Network Load Balancing Overview

<http://www.tech-faq.com/network-load-balancing.shtml>

QUESTION 109:

You are an enterprise administrator for Certkiller .com. All the servers on the network run Windows Server 2008. The network consists of 20 servers on which the Terminal Services role and the Microsoft Windows System Resource Manager (WSRM) features are installed.

On one of the servers called Certkiller Server1, you have recently configured a resource-allocation policy with all the required custom settings. Which of the following options would you choose to configure the WSRM settings on all the servers to match the WSRM settings on Certkiller Server1?

- A. Configure the Remote WSRM accounting option of Certkiller Server1 on each server by enabling the Accounting function on each server.
- B. Export the registry key, HKLM\SYSTEM\CurrentControlSet\Services\WSRM on Certkiller Server1 and import the registry key on other servers.
- C. Using the WSRM console on Certkiller Server1, export the WSRM settings to a shared folder and then import the WSRM settings from others servers using the WSRM console from the shared folder.
- D. Backup the system state data on and then restore the System State data on each server.
- E. None of the above

Answer: C

Explanation:

To configure the WSRM settings on all the servers to match the WSRM settings on Certkiller Server1, you need to use the WSRM console on Certkiller Server1 to export the WSRM information to a shared folder. Use the WSRM console to import the WSRM information from the shared folder. The WSRM settings can be imported or exported

using command line or WSRM console.

Enabling accounting function will not help also, you cannot copy the registry settings from one system to another to duplicate the WSRM settings. You also cannot use Backup tool for this purpose because you cannot copy the system state from the system to another to duplicate the WSRM settings from one computer to another.

Reference: Implementing Windows System Resource Manager/ Running WSRM in a clustered Environment

<http://www.docstoc.com/docs/284328/redp3701>

QUESTION 110:

You are an enterprise administrator for Certkiller .com. The corporate network of the company consists of an Active Directory domain. All the servers on the network run Windows Server 2008. The network runs a Terminal services role on a server to enable remote users to run commonly required applications from their terminal.

A Terminal Services application called App1 that runs on the server has suddenly stopped responding. To diagnose the problem, you monitored the memory usage on the server for a week and discover that App1 application has a memory leak.

To resolve the problem, you first looked for a patch but that was not currently available. So you created a new resource-allocation policy in Microsoft Windows Server Resource Manager and configured a Process Matching Criteria named TrackMem for the application.

Which of the following options would you choose to terminate the application when the application consumes more than half of the available memory on the server?

(Select two. Each selected answer will form a part of the answer)

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

Answer: B, D

Explanation:

To terminate the application when the application consumes more than half of the available memory on the server, you need to configure the resource-allocation policy and set the maximum committed memory option to half the available memory on the server and then set the new policy as a Managing Policy.

A memory limit should be set when an application is leaking memory from the Memory tab. Select the Use Maximum Committed Memory For Each Process check box. In Maximum Committed Memory Limit Per Process, you can type a value in megabytes. The Maximum Committed Memory Limit Per Process field allows you to limit the memory on per process basis.

Now you're ready to set the new resource allocation policy to manage the computer. In

the console tree, click Resource Allocation Policies. In the details pane, right-click the resource allocation policy you want to set, and then click Set As Managing Policy. This is because this policy is for computer management and not for profile management.

Reference: Use Windows System Resource Manager to control a server's powers

http://articles.techrepublic.com.com/5100-10878_11-5054954.html

QUESTION 111:

You are an enterprise administrator for Certkiller .com. The corporate network of the company consists of a single Active Directory domain. All the servers on the network run Windows Server 2008. The network consists of two servers configured as follows:

1. Certkiller Server1 (Member server): The Terminal Services role is installed.
2. Certkiller Server2 (Test server in a workgroup environment): The Terminal Services Licensing role service is installed.

You wanted to use Terminal Services Per User Client Access License (TS Per User CAL) mode on Certkiller Server2. However, you were not able to enable the TS Per User CAL mode in the Terminal Services Licensing role service on Certkiller Server2.

Which of the following options would you choose to ensure that you can use TS Per User CAL mode on Certkiller Server2?

- A. Disjoin Certkiller Server1 from the domain.
- B. Extend the schema to add attributes for Terminal Services Licensing.
- C. Join Certkiller Server2 to the domain.
- D. Create a Group Policy object (GPO) that configures Certkiller Server1 to use Certkiller Server2 for licensing.
- E. None of the above

Answer: C

Explanation:

To ensure that you can use TS Per User CAL mode on Certkiller Server2, you need to join Certkiller Server2 to the domain. This is because the TS Per User CAL tracking and reporting is supported only in domain-joined scenarios (the terminal server and the license server are members of a domain) and is not supported in workgroup mode.

Reference: Terminal Services Licensing (TS Licensing)/ Are there any special considerations about TSLicensing?

<http://technet2.microsoft.com/windowsserver2008/en/library/04bf6206-1546-4326-a9a0-b32bc50aeb8d1033.msp>

QUESTION 112:

You are an enterprise administrator for Certkiller .com. The company runs Windows Server 2008 on all the servers on the network. The corporate network consists of a web server called Certkiller Server1, which uses an SSL certificate from

a public certification authority (CA). The users access the server through Internet using URLs: <http://www.Certkiller.com> and <https://www.Certkiller.com>. Due to heavy traffic on the server, the company has decided to configure Network Load Balancing cluster on the network so that the traffic can be load balanced between two servers.

To implement the idea, an additional Web server called Certkiller Server2 was installed and Network Load Balancing cluster is configured using both the servers to distribute the incoming HTTP and HTTPS traffic between both the Web servers. Which of the following options would you choose to configure an SSL certificate on Certkiller Server2 to support HTTPS connections so that all users can connect to <https://www.Certkiller.com> without receiving security warnings?

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

Answer: A

Explanation:

To configure an SSL certificate on Certkiller Server2 also to support HTTPS connections so that all users can connect to <https://www.Certkiller.com> without receiving security warnings, you need to configure the same certificate that exists on Certkiller Server1 to Certkiller Server2 also. To do this you need to export the SSL certificate to a .pfx file and import the .pfx file to Certkiller 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>

QUESTION 113:

You are an enterprise administrator for Certkiller .com. All the servers on the network run Windows Server 2008. The network consists of a Terminal Server. Which of the following options would you choose to configure the Terminal Server to end any sessions that are inactive for more than one hour?

- A. Modify the RDP-Tcp settings from Terminal Services Configuration.
- B. Modify the User logon mode setting from Terminal Services Configuration.
- C. Create a new group from Terminal Services Manager.
- D. Delete the inactive sessions from Terminal Services Manager.

Answer: A

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 114:

You are an enterprise administrator for Certkiller .com. The corporate network of the company consists of a single Active Directory domain. All the servers on the network run Windows Server 2008. The network consists of a server called Certkiller Server1 that has the Terminal Services role is installed on it.

You have recently deployed a remote application called APP1 on the Terminal server. You need to ensure that the company's security policy that states that users should not be allowed to copy and paste information to a local computer during a Terminal Services session, requirements must be met while configuring Terminal Services.

Which of the following options would you choose to accomplish this task?

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

Answer: B

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?mf>

Reference: Frequently Asked Windows Terminal Services Questions! / New Features and Improvements

<http://www.msterialservices.org/faq/WindowsTerminalServices/?page=5>

QUESTION 115:

You are an enterprise administrator for Certkiller .com. The corporate network of the company consists of an Active Directory domain. All the servers on the network run Windows Server 2008. The network runs Terminal services to enable remote users to run commonly required applications from their terminal.

An organizational unit (OU) called TermSerUsers have been configured for the standard users who connect to the Terminal Server and an OU called TermSerAdmin is configured for the administrative users.

Besides these two types of users, no other user can connect to the Terminal Server. Which of the following options would you choose to ensure that only members of the TermSerAdmin OU can run the Remote Desktop Protocol files?

- A. Create a GPO and disabled the Allow .rdp files from unknown publishers policy setting in the Remote Desktop Client Connection template. Apply the GPO to the TermSerUsers OU.
- B. Create a GPO) and enable the Allow .rdp files from valid publishers and users default .rdp settings policy setting in the Remote Desktop Client Connection template. Apply the GPO to the TermSerUsers OU.
- C. Create a GPO and enable the Allow .rdp files from valid publishers and users default .rdp settings policy setting in the Remote Desktop Client Connection template. Apply the GPO to the TermSerAdmin OU.
- D. Create a GPO and enable the Specify SHA1 thumbprints of certificates representing trusted .rdp publishers policy setting in the Remote Desktop Client Connection template. Apply the GPO to the TermSerAdmin OU.

Answer: B

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.ms>

QUESTION 116:

You are an enterprise administrator for Certkiller .com. The corporate network of the company consists of an Active Directory domain. All the servers on the network run Windows Server 2008. The network runs a Terminal server named Certkiller Server2 to enable remote users to run commonly required applications from their terminal.

Which of the following options would you choose to prevent new sessions on the Terminal Server without affecting current user sessions?

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

Answer: D

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.msp?mf>

QUESTION 117:

You are an enterprise administrator for Certkiller .com. The company runs Windows Server 2008 on all the servers on the network. One of the servers, Certkiller Server1 has the Web Server (IIS) role installed on it. A web developer of the company created a website that run a web application called App1 using ASP.NET 3.0 and hosted it on Certkiller Server1.

The Certkiller Server1 was already running other ASP.NET applications. The new web application App1 must run under a security context that is separate from any

other ASP.NET application on the Web server.

To fulfill this requirement, you create a local user account and grant account rights and permissions to run App1. Which of the following options would choose to configure authentication for the new website to support App1?

- A. Enable the ASP.NET Impersonation setting and specify the new local user account by editing the ASP.NET Impersonation setting.
- B. Enable the Windows Authentication setting.
- C. Enable the Forms Authentication setting and retain all the default settings.
- D. Configure the ASP.NET State service to log on to the new local user account by using the Services console.

Answer: A

Explanation:

To configure authentication for the new website to support App1 so that it may run under a security context that is separate from any other ASP.NET application on the Web server, you need to enable the ASP.NET Impersonation setting and specify the new local user account by editing the ASP.NET Impersonation setting.

Impersonation is when ASP.NET executes code in the context of an authenticated and authorized client. By default, ASP.NET does not use impersonation and instead executes all code using the same user account as the ASP.NET process, which is typically the ASPNET account. Using impersonation, ASP.NET applications can optionally execute the processing thread using the identity of the client on whose behalf they are operating.

Reference: ASP.NET Impersonation

[http://msdn.microsoft.com/en-us/library/aa292118\(VS.71\).aspx](http://msdn.microsoft.com/en-us/library/aa292118(VS.71).aspx)

QUESTION 118:

You are an enterprise administrator for Certkiller .com. The company runs Windows Server 2008 on all the servers on the network. One of the servers, Certkiller Server1 has the Web Server (IIS) role installed.

The server hosts a Web application called App1 that uses a custom application pool, which is set to recycle every 1,440 minutes. The App1 does not support multiple worker processes. Which of the following options would you choose to configure the application pool to ensure that users can access App1 after the application pool is recycled?

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

Answer: A

Explanation:

To configure the application pool to ensure that users can access App1 after the application pool is recycled, you need to set the Disable Overlapped Recycling option to True.

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.

Reference: IIS Process Recycling / Considerations When Recycling Applications
<http://msdn.microsoft.com/en-us/library/ms525803.aspx>

QUESTION 119:

You are an enterprise administrator for Certkiller .com. The company runs Windows Server 2008 on all the servers on the network. One of the servers, Certkiller Server1 has the Web Server (IIS) role installed on it.

Which of the following commands would you choose to create a virtual directory on the company website www.Certkiller.com/sl for the Sales department?

- A. `appcmd add site /name:sl /physicalPath:c:\websites\sl`
- B. `appcmd set vdir /vdir.name:sl /path:/sl /physicalPath:c:\websites\sl`
- C. `appcmd add app /app.name: Certkiller /path:/sl /physicalPath:c:\websites\sl`
- D. `appcmd add vdir /app.name: Certkiller /path:/sl /physicalPath:c:\websites\sl`
- E. None of the above

Answer: D

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.name:string` 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 `path:string` is the virtual path of the virtual directory, such as `/sl`, and `physicalPath:string` 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 `Certkiller`, you need to type the following command prompt

`appcmd add vdir /app.name: Certkiller / 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.msp>

QUESTION 120:

Exhibit:

Application	Web location	Original location	New location
CertKillerApp	certkiller/CertKillerApp	D:\CertKillerApp	f:\CertKillerApp

You are an enterprise administrator for Certkiller .com. The company runs

Windows Server 2008 on all the servers on the network. One of the servers, Certkiller Server1 has the Web Server (IIS) role installed on it. A web developer configured a Web site named Certkiller .com and a Web application named Certkiller App on the Web server.

However, after this configuration, the Web server runs out of disk space. So to resolve the problem, you move Certkiller App to another drive on the Web server. The exhibit shows the current application configuration.

After moving Certkiller App to another drive on the Web server, the users reported that they cannot access Certkiller App. Which of the following options would you choose to enable users to access Certkiller App?

- A. Run `appcmd add app /site.name: Certkiller /path:/ Certkiller App /physicalPath:d:\ Certkiller App` command on the server
- B. Run `appcmd set app /site.name: Certkiller /path:/ Certkiller App /physicalPath:d:\ Certkiller App` command on the server
- C. Run `appcmd set app /site.name: Certkiller /path:/ Certkiller App /physicalPath:f:\ Certkiller App` command on the server
- D. `appcmd add app /site.name: Certkiller /path:/ Certkiller App /physicalPath:f:\ Certkiller App` command on the server

Answer: C

Explanation:

To enable users to access Certkiller App on another drive on the Web server, you need to run `appcmd set app /site.name: Certkiller /path:/ Certkiller App /physicalPath:f:\ Certkiller App` command on the server.

Reference: IIS 7.0: Appcmd.exe

<http://technet2.microsoft.com/windowsserver2008/en/library/ec52c53b-6aff-4d76-995e-3d222588bf321033.msp>

QUESTION 121:

You are an enterprise administrator for Certkiller .com. The company runs Windows Server 2008 on all the servers on the network. One of the servers, Certkiller Server1 has the Web Server (IIS) role installed on it. The Certkiller Server1 hosts multiple websites. Which of the following options would you choose to configure the server to automatically release memory for a single website without affecting the other Web sites?

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

Answer: D

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.ms>

Reference: IIS 7.0: Configuring Recycling Settings for an Application Pool

<http://technet2.microsoft.com/windowsserver2008/en/library/0d5770e3-2f6f-4e11-a47c-9bab6a69ebc71033.msp>

QUESTION 122:

You are an enterprise administrator for Certkiller .com. The company runs Windows Server 2008 on all the servers on the network. One of the servers, Certkiller Server1 has the Web Server (IIS) role installed on it.

A public website has recently been hosted on Certkiller Server1. After a few days, you noticed an unusual high traffic volume on the website. Which of the following options would you choose to identify the source of the traffic?

- A. Run the netstat -an command on Certkiller Server1.
- B. Using IIS Server Manager, first enable the website logging and then filter the logs for the source IP address.
- C. Enable Web scripting on Certkiller Server1.
- D. Using Event Viewer, filter information from the security log by creating a custom view in it.

Answer: B

Explanation:

To identify the source of the traffic, you need to first enable the website logging using IIS Server Manager and then filter the logs for the source IP address so that the source of high traffic can be found out.

The Internet Services Manager, available within the Administrative Tools folder on your Start menu, is the primary tool you'll use to administer your Web server. It allows you to enable logging on your web site. The IIS log files then can be used to identify performance issues in performance testing.

The Client IP address filtering allows you to filter the IP address of the machine that accessed your web site. Although IP addresses aren't necessarily unique to any one visitor (as most visitors surf the web via a dynamic IP address provided by their ISP and

not their own dedicated static IP and pipe), the IP address can still be useful in partitioning the log file into visitor sessions.

The netstat -an command cannot be used because it is used to check various TCP/IP connections. The web scripting is used to enhance your browsing experience. Event logs are special files that record significant events on your computer, such as when a user logs on to the computer or when a program encounters an error. Therefore all these options cannot be used to detect the source of high traffic.

Reference: How To Use IIS Log Files In Performance Testing

<http://www.codeplex.com/PerfTesting/Wiki/Print.aspx?title=How%20To%3A%20Use%20IIS%20Log%20Files>

Reference: Web Wizardry: Putting the Internet to Work on Windows 2000

<http://mcpmag.com/features/print.asp?EditorialsID=94>

Reference: Dissecting Log Files

http://www.clicktracks.com/insidetrack/articles/dissecting_log_files.php

QUESTION 123:

You are an enterprise administrator for Certkiller .com. The company runs Windows Server 2008 on all the servers on the network. One of the servers, Certkiller Server1 has the Web Server (IIS) role installed.

An application called App1 runs on Certkiller Server1. Due to some requirement, you need to make some configuration changes to App1. However, after those changes, the users report that the application fails.

To diagnose the problem, you checked the event log and discovered an error message saying "503 Service Unavailable" appearing. Which of the following options would you choose to ensure that users are able to connect to App1?

- A. Run appcmd stop apppool on Certkiller Server1
- B. Run appcmd set config on Certkiller Server1
- C. Run appcmd start apppool on Certkiller Server1
- D. Run appcmd set apppool on Certkiller Server1

Answer: C

Explanation:

To ensure that users are able to connect to App1, you need to run appcmd start apppool on Certkiller Server1.

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_22

QUESTION 124:

You are an enterprise administrator for Certkiller .com. The company runs Windows Server 2008 on all the servers on the network. One of the servers, Certkiller Server1 has the Web Server (IIS) role installed and all the Web Server role services on it.

Which of the following features would you configure on the server to provide a user the ability to administer a website?

- A. Configure .Net Users feature on Certkiller Server1
- B. Configure .Net Roles feature on Certkiller Server1
- C. Configure IIS Manager Permissions feature on Certkiller Server1
- D. Configure Authentication feature on Certkiller Server1

Answer: C

Explanation:

To provide a user the ability to administer a website, you need to configure IIS Manager Permissions feature on Certkiller Server1.

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/33aacc94-c0cb-4402-b91e-a5e3b9c3e0e01033.msp>

QUESTION 125:

You are an enterprise administrator for Certkiller .com. The company runs Windows Server 2008 on all the servers on the network. One of the servers, Certkiller Server1 has the Web Server (IIS) role installed.

The server hosts a Web application called App1 that uses a custom application pool, which is set to recycle every 1,440 minutes. The App1 does not support multiple worker processes. Which of the following options would you choose to configure the application pool to ensure that users can access App1 after the application pool is recycled?

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

Answer: A

Explanation:

To configure the application pool to ensure that users can access App1 after the application pool is recycled, you need to set the Disable Overlapped Recycling option to True.

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.

Reference: IIS Process Recycling / Considerations When Recycling Applications

<http://msdn.microsoft.com/en-us/library/ms525803.aspx>

QUESTION 126:

You are an enterprise administrator for Certkiller .com. The company runs Windows Server 2008 on all the servers on the network. One of the servers, Certkiller Server1 has the Web Server (IIS) role installed on it.

Which of the following options would you choose to activate SSL for the default Web site on the server? (Choose two. Each correct answer presents part of the solution.)

- A. Select the Generate Key option in the Machine Key dialog box for the default Web site.
- B. Create an HTTPS binding on the default Web site.
- C. Install the Digest Authentication component for the Web server
- D. Obtain an appropriate server certificate.

Answer: B, D

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 requires storing 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 7.0 sends 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 127:

You are an enterprise administrator for Certkiller .com. The company runs Windows Server 2008 on all the servers on the network. One of the servers, Certkiller Server1 has the Web Server (IIS) role installed on it. The Certkiller Server1 hosts an Internet-accessible Web site called Certkiller .com that has a virtual directory named /Salesorders/. A Web server certificate is installed and an SSL listener has been configured for the Web site.

Which of the following options would you choose to configure the /salesorders/ virtual directory to meet the company policy requirements that states that the /salesorders/ virtual directory must be accessible to authenticated users only and it should allow authentication types to support all browsers?

Besides it should encrypt all authentication traffic by using HTTPS and all other directories of the Website must be accessible to anonymous users and be available without SSL. (Select all that apply. Each correct answer presents part of the solution.)

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

Answer: D, E, G

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>

Reference: Basic access authentication

http://en.wikipedia.org/wiki/Basic_access_authentication

QUESTION 128:

You are an enterprise administrator for Certkiller .com. The company runs Windows Server 2008 on all the servers on the network. One of the servers, Certkiller Server1 has the Windows Media Services server role installed on it. You have been assigned the task to distribute a video file on DVD media. The video file should be viewed by the users on computers even when the users are not connected to the Internet.

Which of the following options would you choose to accomplish the desired task while making sure that the video file is protected from unauthorized use and illegal distribution?

- A. Advertise the video using Windows Media Services and then create a DVD that contains the HTML and ASPX files for the advertised video.
- B. Package and advertise the video on the corporate Web site using Windows Media Digital Rights Manager.
- C. Publish the video as streaming content, and then burn the video to a DVD using Windows Media Services.
- D. 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.

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 129:

You are an enterprise administrator for Certkiller .com. The company runs Windows Server 2008 on all the servers on the network. Two servers on the network were configured as follows:

Certkiller Server1: Windows Media Services server role installed

Certkiller server2: Windows Media Services server role installed and is also configured a License Clearing House.

You published an audio file, which is licensed by Certkiller Server2 on Certkiller Server1. Which of the following options would you choose to ensure that users are allowed to use the audio file for only two days?

- A. Modify the license on Certkiller server2.
- B. Modify the key ID on Certkiller Server1.
- C. Create a new package on Certkiller server2.
- D. Modify the license key seed on Certkiller Server1.

Answer: A

Explanation:

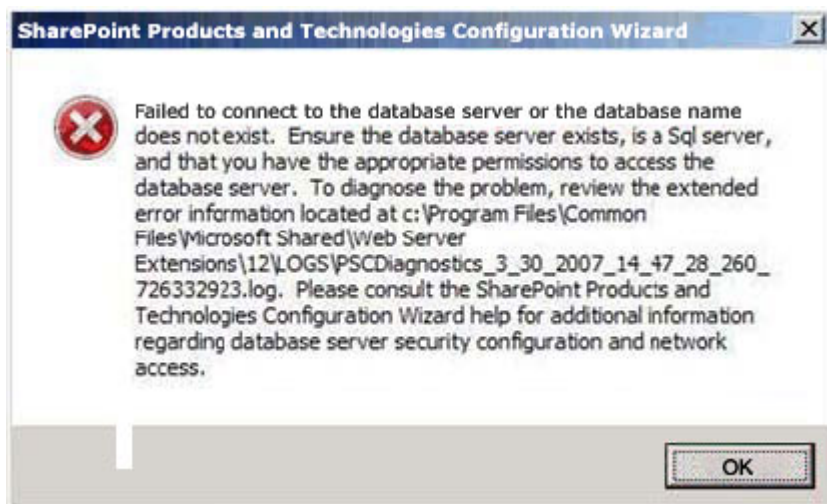
To ensure that users are allowed to use the audio file for only two days, you need to modify the license on Certkiller server2. Windows Media Rights Manager lets content providers deliver songs, videos, and other digital media content over the Internet in a protected, encrypted file format. The licenses in Windows Media Rights Manager can support a wide range of different business rules, including the number of times a file can be played.

Reference: Architecture of Windows Media Rights Manager

<http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx>

QUESTION 130:

Exhibit:



You are an enterprise administrator for Certkiller .com. All the servers on the

corporate network run Windows Server 2008. A new server farm has recently been created on the network. The company uses Public folders and Web Distributed Authoring and Versioning.

You have been assigned the task to install Microsoft Windows SharePoint Services (WSS) as a server in a new server farm. However, when you started the installation by starting the SharePoint Products and Technologies Configuration Wizard, you receive an error message that states "Failed to connect to the database server or the database name does not exist", as shown in the exhibit.

Which of the following server/services would install to configure WSS to start SharePoint Services 3.0 Central Administration?

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

Answer: A

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 131:

You are an enterprise administrator for Certkiller .com. The corporate network of the company consists of a single Active Directory domain. All the servers on the network either run Windows Server 2008 or Windows Server 2003.

The network consists of a Windows Server 2003 server called Certkiller Server2 that runs Microsoft SQL Server 2005 SP2 and Microsoft Windows SharePoint Services (WSS) 2.0. The network consists of another server called Certkiller Server3 that runs Windows Server 2008.

You have been assigned the task to migrate to SharePoint Services (WSS) 3.0. from Certkiller Server2 to Certkiller Server3 with all the configuration and content. Which of the following options would you choose to accomplish this task?

- A. Install WSS 2.0 on Certkiller Server3. Back up the WSS 2.0 configuration and content

from Certkiller Server2 and restore the backup from Certkiller Server2 to Certkiller Server3. Perform an in-place upgrade of WSS 2.0 to WSS 3.0 on Certkiller Server3.

B. Upgrade Certkiller Server2 to Windows Server 2008. Back up the SharePoint configuration and content from Certkiller Server2. Install WSS 3.0 on Certkiller Server3 and then restore the backup from Certkiller Server2 to Certkiller Server3.

C. Back up the SQL Server 2005 configuration and the WSS 2.0 databases from Certkiller Server2. Install SQL Server 2005 on Certkiller Server3 and then restore the SQL Server 2005 backup from Certkiller Server2 to Certkiller Server3.

D. Back up the SharePoint configuration and content from Certkiller Server2. Install WSS 3.0 on Certkiller Server3 and then restore the backup from Certkiller Server2 to Certkiller Server3.

Answer: A

Explanation:

To migrate to SharePoint Services (WSS) 3.0. from Certkiller Server2 to Certkiller Server3 with all the configuration and content, you need to install WSS 2.0 on Certkiller Server3.

Back up the WSS 2.0 configuration and content from Certkiller Server2 and restore the backup from Certkiller Server2 to Certkiller Server3. Perform an in-place upgrade of WSS 2.0 to WSS 3.0 on Certkiller Server3.

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](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](http://technet.microsoft.com/en-us/library/cc263447(TechNet.10).aspx)

QUESTION 132:

You are an enterprise administrator for Certkiller .com. All the servers on the network run Windows Server 2008. The network consists of a server called Certkiller Server1 on which Windows SharePoint Services (WSS) role is installed. A group of users need to access the WSS server. However, you want to restrict the users to view items, open items, and view versions on the WSS server. To accomplish this task, you created a group called SPUsers that will access content on the WSS server.

Which of the following permissions would you configure for the SPUsers group to restrict the permissions of the group to viewing items, opening items, and viewing versions?

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

Answer: C

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 133:

You are an enterprise administrator for Certkiller .com. All the servers on the network run Windows Server 2008. The network consists of two servers configured as follows:

1. Certkiller Server1: The Windows SharePoint Services (WSS) 3.0 is installed.
2. Certkiller Server2: The SMTP feature is installed.

Which of the following options would you choose to configure the outgoing e-mail settings on Certkiller Server1 to use the SMTP service on Certkiller Server2 and ensure that e-mail messages from Certkiller Server1 are forwarded to users?

- A. Create a new application pool on Certkiller Server2 and then associate the application pool with a new website.
- B. Create a new application pool on Certkiller Server1 and on an internal DNS server, create a new MX record for Certkiller Server2.
- C. Create a new application pool on Certkiller Server1 and on an internal DNS server, create a new MX record for Certkiller Server1.
- D. On Certkiller Server2, configure the SMTP service to accept anonymous connections and to relay e-mail messages.

Answer: D

Explanation:

You can configure the SMTP service to accept relayed e-mail from servers in your farm. You can decide to accept relayed e-mail from all servers except those you specifically exclude. Alternatively, you can block e-mail 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 e-mail relaying but by doing this, you increase the possibility that the SMTP server will be used to relay unsolicited commercial e-mail (spam).

Reference: Configure outgoing e-mail settings (Windows SharePoint Services)

[http://technet.microsoft.com/en-us/library/cc288949\(TechNet.10\).aspx](http://technet.microsoft.com/en-us/library/cc288949(TechNet.10).aspx)

QUESTION 134:

You are an enterprise administrator for Certkiller .com. The corporate network consists of a single Active Directory domain. The company runs Windows Server 2008 on all the servers on the network. One of the servers, Certkiller Server1 has the Windows SharePoint Services (WSS) server role installed on it.

Which of the following options would you choose to configure WSS server in such a way that it allow users to create distribution lists from a SharePoint site?

- A. Modify the outgoing mail character set.
- B. Configure the SharePoint site to accept messages from authenticated users only.
- C. Enable the SharePoint Directory Management Service on Certkiller Server 1.
- D. Use the default Rights Management server in Active Directory Domain Services to configure the SharePoint site.

Answer: C

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 Certkiller Server 1. A distribution list contains the e-mail addresses of existing address lists as well as the e-mail 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 e-mail-enabled site collection are automatically e-mail-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 e-mail/ New site creation walkthrough

<http://office.microsoft.com/en-us/help/HA100823061033.aspx>

QUESTION 135:

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 136:

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 137:

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 138:

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 139:

You have a server that runs Windows Server 2008 and has the Windows Server Virtualization (WSv) 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 with other network servers.

What should you do first?

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

Answer: B

QUESTION 140:

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 141:

Your company named Certkiller 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. Certkiller .com.

You discover that Certkiller users can see the Network Load Balancing cluster in the network neighborhood and can connect to various services by using the web. Certkiller .com name. The web. Certkiller .com Network Load Balancing cluster is configured with only one port rule.

You need to configure the web. Certkiller .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

QUESTION 142:

You have two servers named FC1 and FC2 that run Windows Server 2008 Enterprise Edition. 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

QUESTION 143:

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 144:

Your company has an Active Directory domain. The company runs Terminal Services. All Terminal 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. Tsdicon 1337, and then Chgport /U User1 1337
- D. Tsdicon 1337, and then Tscon 1337

Answer: D

QUESTION 145:

You have the Web Server (IIS) role installed on a server that runs Windows Server 2008.

You create a Web site named Certkiller .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

QUESTION 146:

You have a Windows Server 2008 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

QUESTION 147:

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

QUESTION 148:

You install the FTP role service on a server that runs Windows Server 2008. 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 149:

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:PickupDirectoryFromIis` command.
- D. Configure the SMTP delivery setting to Attempt direct delivery before sending to smart host.

Answer: B

QUESTION 150:

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

QUESTION 151:

You have 10 servers that run Windows Server 2008. 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 Inetpub 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

QUESTION 152:

Your company named Certkiller has a Web server named WEB1.

The Web server runs Windows Server 2008. The fully qualified domain name of WEB1 is web1. Certkiller .com. The public DNS server has an alias record named owa. Certkiller .com that maps to web1. Certkiller .com. Users access WEB1 from the Internet by using http://owa. Certkiller .com.

The new company security policy states that the owa. Certkiller .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. Certkiller
- B. owa. Certkiller .com
- C. WEB1
- D. web1. Certkiller .com

Answer: B

QUESTION 153:

You implement a member server that runs Windows Server 2008. 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 154:

You manage a new server that runs Windows Server 2008. You plan to install the Streaming Media Services role on the server.

Users will access content on the new server by using Windows Media Player for Windows Vista and Windows Media Player for Mac.

You need to install the Streaming Media Services 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