Vendor: Microsoft

Exam Code:70-649

Exam Name:TS: Upgrading Your MCSE on Windows Server 2003 to Windows Server 2008, Technology Specialist

Version: Demo

QUESTION 1

Your network contains a server named Server1. Server1 has three hard disk drives. Two hard disk drives named C and E are configured as simple volumes. The third hard disk drive contains 500 GB of unallocated space.

Drive E hosts a shared folder named Folder1.

Users report that they fail to save files to Folder1.

You discover that drive E has no free space.

You need to ensure that users can save files to Folder1.

What should you do?

A. From the Share and Storage Management console, run the Provision Storage Wizard.

B. From the Disk Management console, run the Add Mirror wizard.

C. From the Share and Storage Management console, run the Provision a Shared Folder Wizard.

D. From the Disk Management console, run the Extend Volume Wizard.

Correct Answer: D

Extend a Simple or Spanned Volume

A spanned volume is a dynamic volume that consists of disk space on more than one physical disk. If a simple volume is not a system volume or boot volume, you can extend across additional disks. If you extend a simple volume across

multiple disks, it becomes a spanned volume.

You can extend a volume only if it does not have a file system or if it is formatted using the NTFS file system.

You cannot extend volumes formatted using FAT or FAT32. Backup Operator or Administrator is the minimum membership required to complete the actions below.

Extending a simple or spanned volume

1.

In Disk Management, right-click the simple or spanned volume you want to extend.

2.

Click Extend Volume.

3.

Follow the instructions on your screen. Source: http://technet.microsoft.com/en-us/library/cc753058.aspx

---

QUESTION 2

Your network contains an Active Directory forest. The forest contains a member server named Server1 that runs Windows Server 2008 R2. You need to configure Server1 as a network address translation (NAT) server. Which server role, role service, or feature should you install?

A. windows System Resource Manager (WSRM)

B. Simple TCP/IP services Wireless LAN Service

C. Connection Manager Administration Kit (CMAK)

D. Routing and Remote Access service (RRAS)

E. Group Policy Management

F. File Server Resource Manager (FSRM)

G. Services for Network File System (NFS)

H. Network Load Balancing (NLB)

I. Windows Server Update Services (WSUS)

J. Health Registration Authority (HRA)

K. Network Policy Server (NPS)

L. Windows Internal Database

Correct Answer: D

QUESTION 3

Your network contains an Active Directory domain. The domain contains a server that runs Windows Server 2008 R2.

The server has the Remote Desktop Session Host (RD Session Host) role service and the Remote Desktop Web Access (RD Web Access) role service installed.

When domain users run RemoteApp programs from the RD Web Access page, they are prompted for their credentials.

You need to ensure that the domain users can run the RemoteApp programs without being prompted for their credentials.

What should you do?

A. FromRemoteApp Deployment Settings, configure the Common RDP Settings.

B. FromRemoteApp Deployment Settings, configure the Digital Signature Settings.

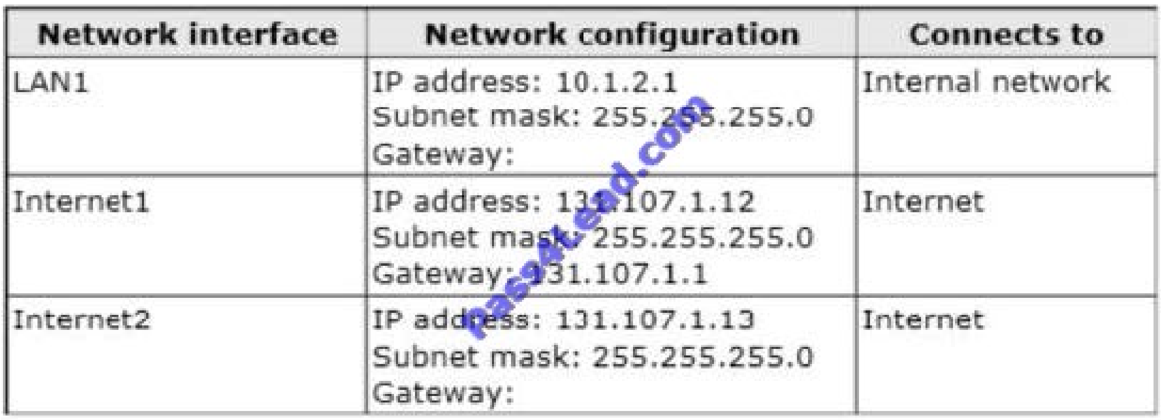
C. On each client computer, add the URL of the RD Web Access Web site to the Trusted sites zone.

D. On each client computer, add the URL of the RD Web Access Web site to the Local intranet zone.

Correct Answer: B

QUESTION 4

Your network contains a server named Server1 that runs Windows Server 2008 R2. The network for Server1 is configured as shown in the table.



Network interface	Network configuration	Connects to
LAN1	IP address: 10.1.2.1 Subnet mask: 255.255.255.0 Gateway:	Internal network
Internet1	IP address: 131.107.1.12 Subnet mask: 255.255.255.0 Gateway: 131.107.1.1	Internet
Internet2	IP address: 131.107.1.13 Subnet mask: 255.255.255.0 Gateway:	Internet

You plan to deploy DirectAccess on Server1.

You need to configure the network interfaces on Server1 to support DirectAccess.

What should you do?

A. Remove the IP address of 131.107.1.13 from Internet2, and then add the address to LAN1.

B. Add the IP address of 10.1.2.2 to LAN1.

C. Remove the IP of address 131.107.1.13 from Internet2, and then add the address to Internet1.

D. Add the default gateway of 131.107.1.1 to Internet2.

Correct Answer: C

QUESTION 5

Your network contains an Active Directory domain named contoso.com.

You publish a RemoteApp named Appl. The Remote Desktop Connection (.rdp) file for App1 is unsigned.

When a user named User1 runs App1 from the Remote Desktop Web Access (RD Web Access) website, User1 is prompted for credentials.

You need to prevent users from being prompted for credentials when they run Appl.

What should you do?

A. Enable the Allow Delegating Default Credentials Group Policy setting.

B. Configure the SSL Settings for the RDWeb virtual directory.

C. Enable the Assign a default domain for logon Group Policy setting.

D. Modify the Authentication Settings for the RDWeb virtual directory.

Correct Answer: A

When applied to Terminal Services, Single Sign-On means using the credentials of the currently logged on user (also called default credentials) to log on to a remote computer. If you use the same user name and password logging on to your

local computer and connecting to a Terminal Server, enabling Single Sign-On will allow you to do it seamlessly, without having to type in your password again. Locally logged on credentials are used for connecting to TS Web Access,

however, they cannot be shared across TS Web Access and TS or TS Gateway. Thus you will need to enable the Group Policy settings described below in order to use locally logged on credentials for TS or TS Gateway connections.

How to enable Single Sign-On?

Single sign-On can be enabled using domain or local group policy.

1.

Log on to your local machine as an administrator.

2.

Start Group Policy Editor - "gpedit.msc".

3.

Navigate to "Computer Configuration\Administrative Templates\System\Credentials Delegation".

4.

Double-click the "Allow Delegating Default Credentials" policy.

5.

Enable the policy and then click on the "Show" button to get to the server list.

6.

Add "TERMSRV/" to the server list. You can add one or more server names. Using one wildcard (*) in a name is allowed. For example to enable Single Sign-On to all servers in "MyDomain.com" you can type "TERMSRV/*.MyDomain.com". (Notice the "Concatenate OS defaults with input above" checkbox on the picture above. When this checkbox is selected your servers are added to the list of servers enabled by OS by default. For Single Sign-On this default list is empty, so the checkbox has no effect.)

7.

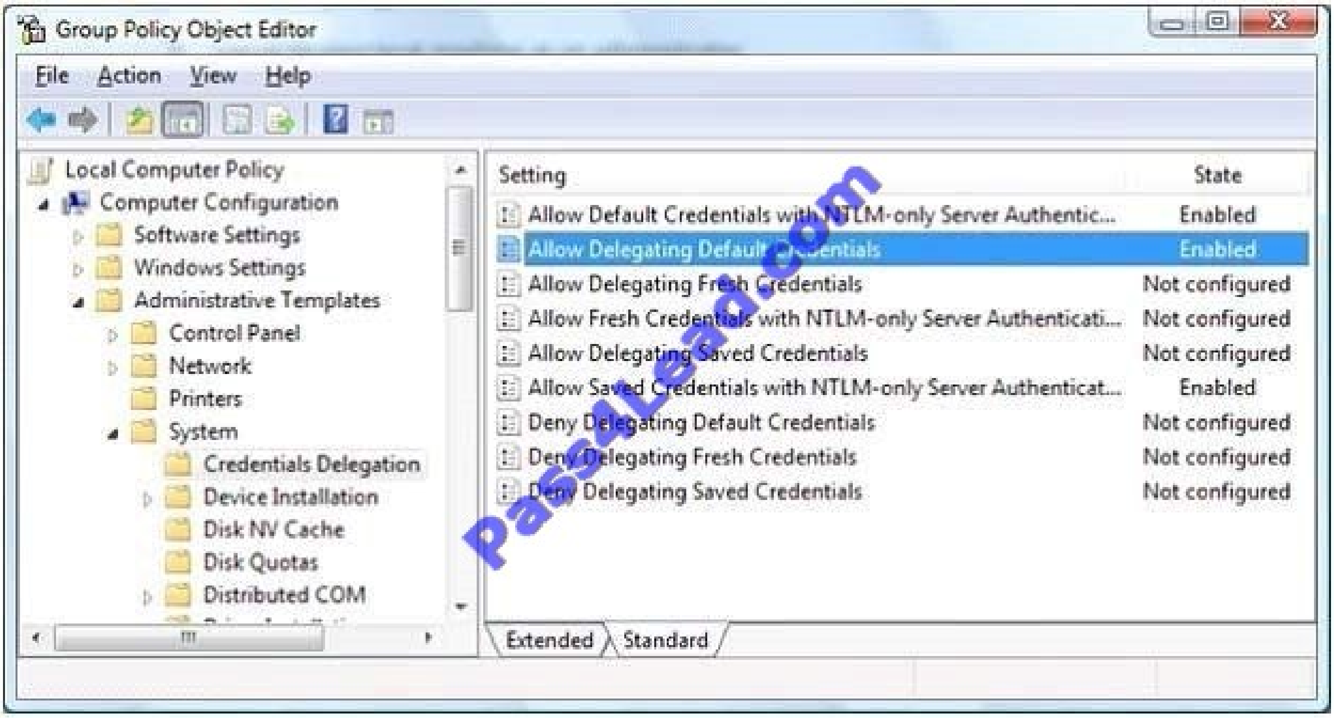
Confirm the changes by clicking on the "OK" button until you return back to the main Group Policy Object Editor dialog.

8.

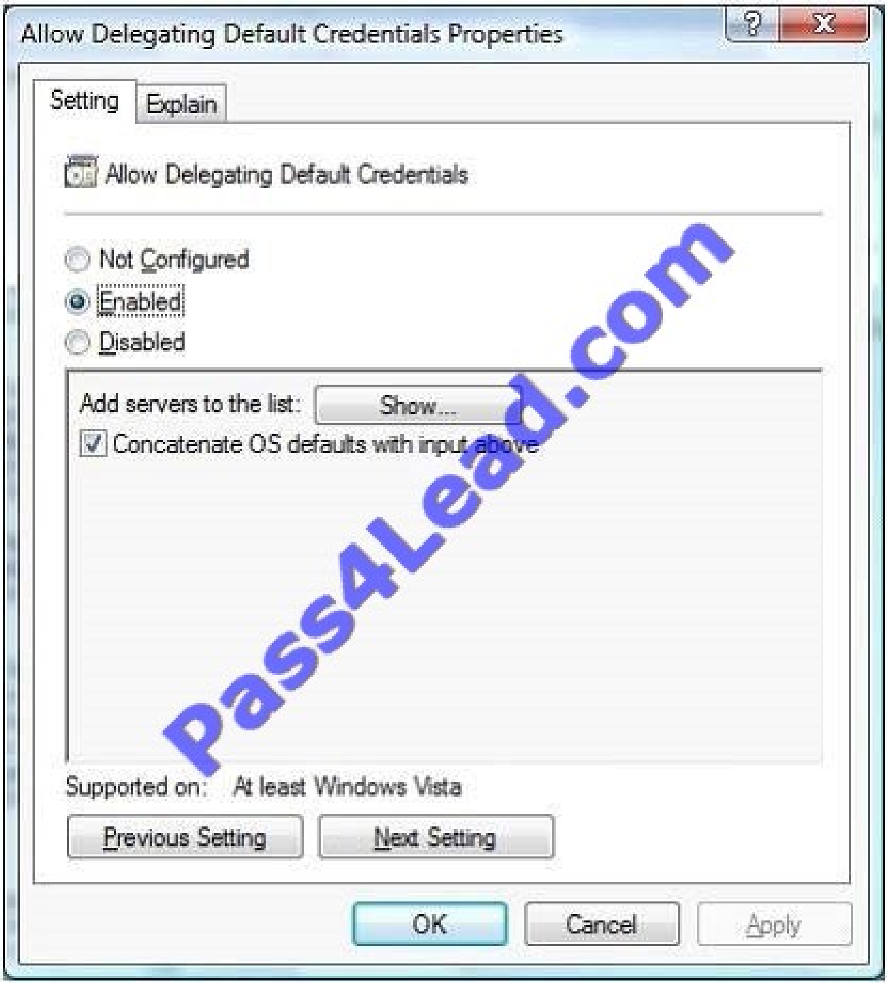
At a command prompt, run "gpupdate" to force the policy to be refreshed immediately on the local machine.

9.

Once the policy is enabled you will not be asked for credentials when connecting to the specified servers. http://blogs.msdn.com/b/rds/archive/2007/04/19/how-to-enable-single-sign-on-for-my- terminal-serverconnections.aspx



Setting	State
Allow Default Credentials with NTLM-only Server Authentic...	Enabled
Allow Delegating Default Credentials	Enabled
Allow Delegating Fresh Credentials	Not configured
Allow Fresh Credentials with NTLM-only Server Authenticati...	Not configured
Allow Delegating Saved Credentials	Not configured
Allow Saved Credentials with NTLM-only Server Authenticat...	Enabled
Deny Delegating Default Credentials	Not configured
Deny Delegating Fresh Credentials	Not configured
Deny Delegating Saved Credentials	Not configured



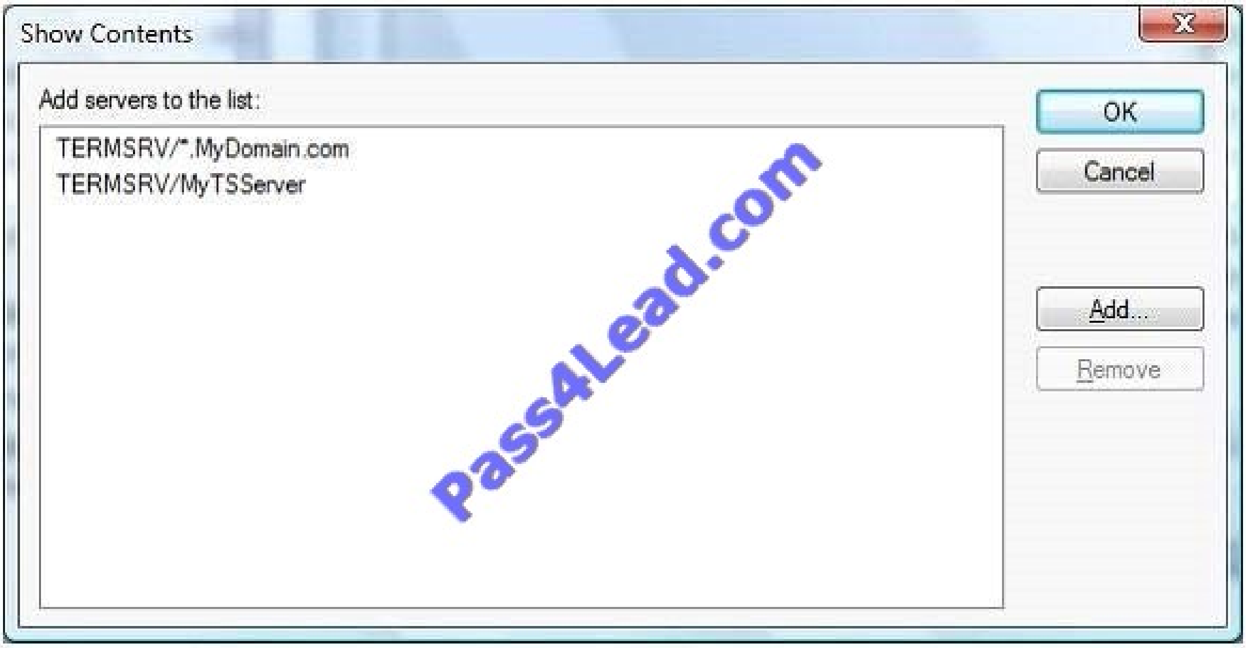
Allow Delegating Default Credentials

○ Not Configured
● Enabled
○ Disabled

Add servers to the list:

☑ Concatenate OS defaults with input above

Supported on: At least Windows Vista



Show Contents

Add servers to the list:

TERMSRV/*.MyDomain.com
TERMSRV/MyTSServer

QUESTION 6

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1. The Active Directory Federation Services (AD FS) role is installed on Server1. Contoso.com is defined as an account

store.

A partner company has a Web-based application that uses AD FS authentication. The partner company plans to provide users from contoso.com access to the Web application.

You need to configure AD FS on contoso.com to allow contoso.com users to be authenticated by the partner company.

What should you create on Server1?

A. a new application

B. a resource partner

C. an account partner

D. an organization claim

Correct Answer: D

The old answer was: a resource partner

Since the account store has already been configured, what needs to be done is to use the account store to map an AD DS global security group to an organization claim (called group claim extraction). So that\\'s what we need to create for

authentication: an organization claim.

Creating a resource/account partner is part of setting up the Federation Trust.

Reference 1:

http://technet.microsoft.com/en-us/library/dd378957.aspx Configuring the Federation Servers

[All the steps for setting up an AD FS environment are listed in an extensive step-by-step guide, too long to post here.]

Reference 2:

http://technet.microsoft.com/en-us/library/cc732147.aspx

Add an AD DS Account Store

If user and computer accounts that require access to a resource that is protected by Active Directory Federation Services (AD FS) are stored in Active Directory Domain Services (AD DS), you must add AD DS as an account store on a

federation server in the Federation Service that authenticates the accounts.

Reference 3:

http://technet.microsoft.com/en-us/library/cc731719.aspx Map an Organization Group Claim to an AD DS Group (Group Claim Extraction) When you use Active Directory Domain Services (AD DS) as the Active Directory Federation Services

(AD FS) account store for an account Federation Service, you map an organization group claim to a security group in AD DS. This mapping is called a group claim extraction.

QUESTION 7

Your network contains three servers named Server1, Server2, and Server3. Server1 is located on a perimeter network. Server2 and Server3 are accessible from the internal network only.

Users connect to Server2 and Server3 to run RemoteApp programs.

You need to ensure that remote users can run the RemoteApp programs on Server2 and Server3. The solution must minimize the number of ports that must be opened on the internal firewall. Which role service should you install on Server3?

A. Remote Desktop Gateway (RD Gateway)

B. Remote Desktop connection Broker (RD connection Broker)

C. Remote Desktop Web Access (RD Web Access)

D. Remote Desktop Session Host (RD Session Host)

Correct Answer: A

QUESTION 8

Your network contains two Active Directory forests named contoso.com and nwtraders.com.

Active Directory Rights Management Services (AD RMS) is deployed in each forest.

You need to ensure that users from the nwtraders.com forest can access AD RMS protected content in the contoso.com forest.

What should you do?

A. Create an external trust from nwtraders.com to contoso.com.

B. Add a trusted user domain to the AD RMS cluster in the nwtraders.com domain.

C. Create an external trust from contoso.com to nwtraders.com.

D. Add a trusted user domain to the AD RMS cluster in the contoso.com domain.

Correct Answer: D

A trusted user domain, often referred as a TUD, is a trust between AD RMS clusters that instructs a licensing server to accept rights account certificates (the certificates identifying users) from another AD RMS server in a different Active Directory forest. An AD RMS trust is not the same as an Active Directory trust, but it is similar in that it refers to the ability of one environment to accept identities from another environment as valid subjects. As a TUD is a trust between AD RMS infrastructures, it requires that each forest (whether in the same company or in different companies) has its own AD RMS infrastructure. Using trusted user domains, AD RMS can process requests for use licenses from users whose rights account certificates were issued by an AD RMS installation in a different Active Directory forest; in other words, from a different certification cluster. Trusted user domains are added by importing the server licensor certificate, of the AD RMS installation to trust, to the trusting AD RMS installation.

QUESTION 9

Your network contains a single Active Directory domain. The domain contains a server named Server1 that runs Windows Server 2008 IC

Server1 has an SCSI host bus adapter that connects to an iSCSI target.

You install an additional iSCSI host bus adapter on Server1.

You need to ensure that Server1 can access the iSCSI target if a host bus adapter fails.

What should you do first?

A. Install the Internet Storage Name Server (iSNS) feature.

B. Bridge the iSCSI host bus adapters.

C. Install the Multipath I/O feature.

D. At the command prompt, run mpclairn.exe -I -m 6.

Correct Answer: C

The old answer was: Bridge the iSCSI host bus adapters. About MPIO

Microsoft Multipath I/O (MPIO) is a Microsoft-provided framework that allows storage providers to develop multipath solutions that contain the hardware-specific information needed to optimize connectivity with their storage arrays. These modules are called device- specific modules (DSMs). The concepts around DSMs are discussed later in this document.

MPIO is protocol-independent and can be used with Fibre Channel, Internet SCSI (iSCSI), and Serial Attached SCSI

(SAS) interfaces in Windows Server- 2008 and Windows Server 2008 R2. Multipath solutions in Windows Server 2008 R2 When running on Windows Server 2008 R2, an MPIO solution can be deployed in the following ways:

*

By using a DSM provided by a storage array manufacturer for Windows Server 2008 R2 in a Fibre Channel, iSCSI, or SAS shared storage configuration.

*

By using the Microsoft DSM, which is a generic DSM provided for Windows Server 2008 R2 in a Fibre Channel, iSCSI, or SAS shared storage configuration.

High availability through MPIO

MPIO allows Windows- to manage and efficiently use up to 32 paths between storage devices and the Windows host operating system. MPIO provides fault tolerant connectivity to storage. By employing MPIO users are able to mitigate the

risk of a system outage at the hardware level.

MPIO provides the logical facility for routing I/O over redundant hardware paths connecting server to storage.

These redundant hardware paths are made up of components such as cabling, host bus adapters (HBAs), switches, storage controllers, and possibly even power. MPIO solutions logically manage these redundant connections so that I/O requests can be rerouted if a component along one path fails.

As more and more data is consolidated on storage area networks (SANs), the potential loss of access to storage resources is unacceptable. To mitigate this risk, high availability solutions, such as MPIO, have now become a requirement. Source: http://technet.microsoft.com/en-us/library/ee619734(WS.10).aspx

---

QUESTION 10

Your network contains a server named Server1 that runs a Server Core installation of Windows Server 2008 R2. The network contains a client computer named Computer1 that runs Windows 7.

You need to ensure that you can collect events from Server1 on Computer1.

What should you run on Server1?

A. net config server

B. eventcreate /so

C. wecutilcs

D. winrmquickconfig

Correct Answer: D

Explanation: http://technet.microsoft.com/en-us/library/cc748890(v=WS.10).aspx

---

QUESTION 11

You deploy an Active Directory Federation Services (AD FS) Federation Service Proxy on a server named Server1.

You need to configure the Windows Firewall on Server1 to allow external users to authenticate by using AD FS.

Which protocol should you allow on Server1?

A. SMB

B. RPC

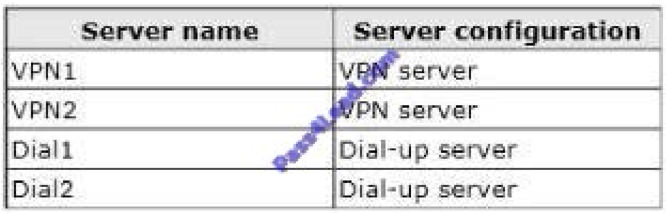
C. Kerberos

D. SSL

Correct Answer: D

QUESTION 12

Your network contains an Active Directory forest. The forest contains the member servers configured as shown in the following table.



Server name	Server configuration
VPN1	VPN server
VPN2	VPN server
Dial1	Dial-up server
Dial2	Dial-up server

All servers run Windows Server 2008 R2.

You deploy a new server named Server1.

You need to configure Server1 to provide central authentication for all dial-up connections and all VPN connections.

What should you install on Server1?

A. Routing and Remote Access service (RRA5)

B. Active Directory Lightweight Directory Services (AD LDS)

C. Active Directory Federation Services (AD FS)

D. Network Policy Server (NPS)

Correct Answer: D

Use connection request policies from Network Policy Server (NPS) Ref: http://www.windowsnetworking.com/articles_tutorials/understanding-new-windows- server- 2008-networkpolicy-server.html

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

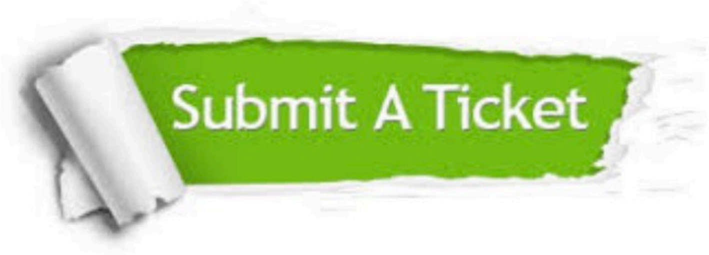
Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



One Year Free Update

Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee

To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.