

**70-649**

Number: 70-649  
Passing Score: 800  
Time Limit: 120 min



<http://www.gratisexam.com/>

## Exam A

### QUESTION 1

Your network contains a server named Server1 that runs Windows Server 2008 R2.

You have a user named User1.

You need to ensure that User1 can view the events in the Security event log. The solution must minimize the number of rights assigned to User1.

What should you do?

- A. In the Local Security Policy console, modify the Security Options.
- B. In Event viewer, configure the properties of the Security log.
- C. In Event viewer, filter the Security log.
- D. In the Registry Editor, add a Security Descriptor Definition Language (SDDL) value.

**Correct Answer: D**

**Section: (none)**

**Explanation**

#### **Explanation/Reference:**

Explanation:

Microsoft Windows uses SDDL to develop and administer object security. SDDL defines security descriptors, which are text strings or binary data structures containing security information for one or more objects, e.g., file, folder, service or unnamed process.

Security descriptors use access control lists (ACLs) to manage access and control entries and audits. Each security descriptor contains a discretionary access control list (DACL) and system access control list (SACL). The DACL controls access to an object, and the SACL controls logging of access attempts.

In addition to the object owner name, most SDDL security descriptor strings are comprised of five parts. These include DACL, SACL, group and header, which specifies inheritance level and permission.

### QUESTION 2

Your network contains a server named Server1.contoso.com. Server1 is located on the internal network.

You have a client computer named Computer1 that runs Windows 7. Computer1 is located on a public network that is connected to the Internet. Computer1 is enabled for DirectAccess.

You need to verify whether Computer1 can resolve Server1 by using DirectAccess.

<http://www.lead2pass.com/70-649.html>

Which command should you run on Computer1?

- A. netsh.exe dnsclient show state
- B. nslookup.exe Server1.contoso.com
- C. ping.exe Server1.contoso.com
- D. nbtstat.exe -a Server1.contoso.com

**Correct Answer: C**

**Section: (none)**

**Explanation**

#### **Explanation/Reference:**

Explanation:

### QUESTION 3

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

An administrator named Admin1 plans to install the Routing and Remote Access service (RRAS) role service on a server named Server1. Admin1's user account is not a member of the Domain Admins group.

You need to ensure that Server1 can authenticate users from Active Directory by using Windows authentication.

What should you do?

- A. Install the Active Directory Lightweight Directory Services (AD LDS) role on Server1.
- B. Add the computer account for Server1 to the Windows Authorization Access Group.
- C. Install the Network Policy Server (NPS) role service on a domain controller.
- D. Add the computer account for Server1 to the RAS and IAS Servers group.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Not sure if I am right on this one, since not all question is shown ;) But I guess that after adding the role by the Admin1 it says that he is not in Domain Admins group and RRAS server wont be added automatically to the RAS and IAS group, so it has to be added manually by a member of that group so server could authenticate users.

#### **QUESTION 4**

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Network Policy Server (NPS) role service installed.

You need to ensure that the NPS log files on Server1 contain information about the duration of client connections.

What should you do?

- A. Enable the Accounting requests setting.
- B. Configure the IAS (Legacy) log file format.
- C. Configure the DTS Compliant log file format.
- D. Enable the Authentication requests setting.

**Correct Answer: C**

**Section: (none)**

**Explanation**

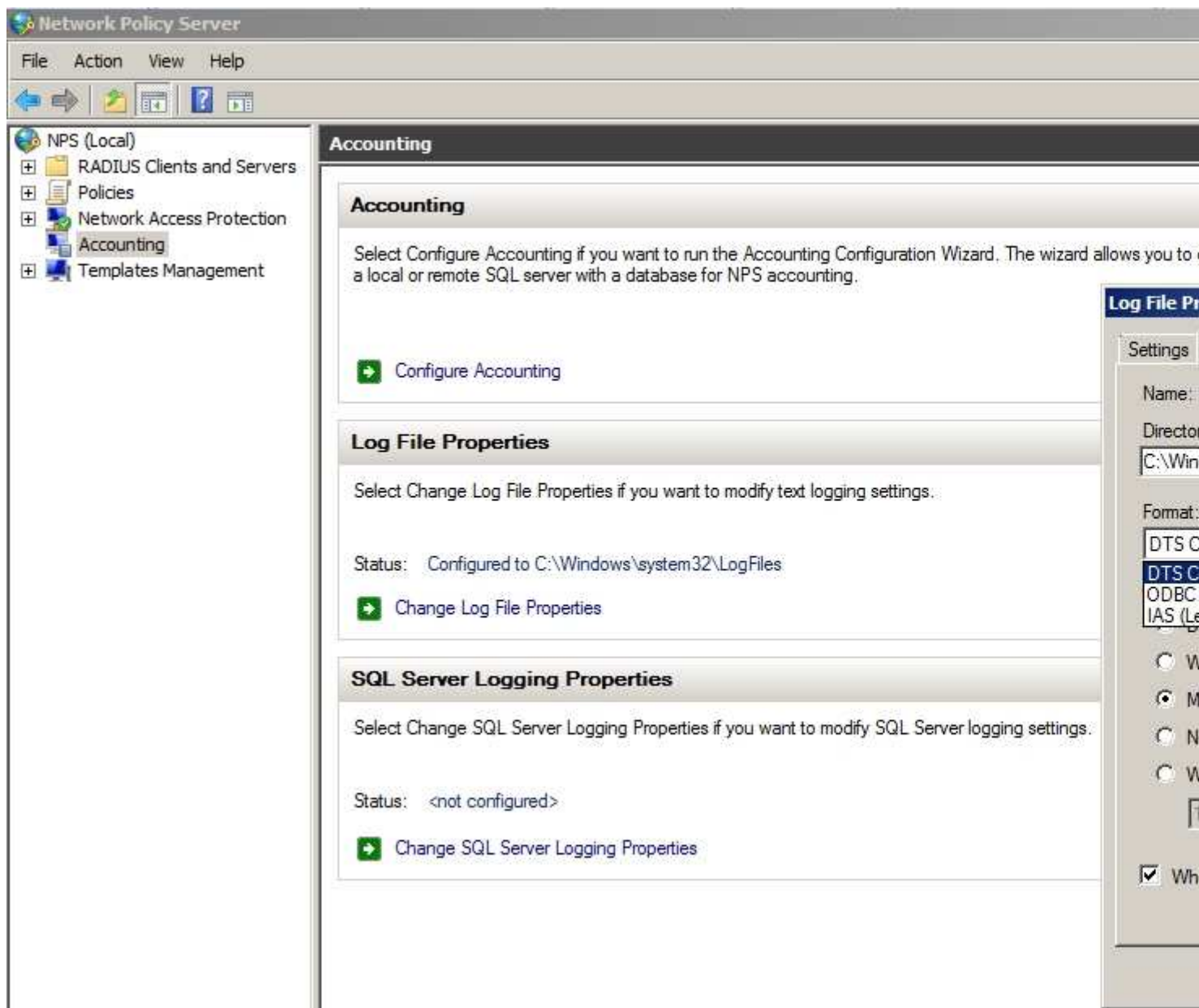
**Explanation/Reference:**

Explanation:

**The old answer was: Enable the Accounting requests setting.**

The DTS Compliant log format is the newest one and only its XML have attributes for session duration such as Acct-Session-Time = "The length of time (in seconds) for which the session has been active."  
[http://technet.microsoft.com/en-us/library/cc771748\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc771748(v=ws.10).aspx)

From **NPS Console** select **Accounting** Section.



#### QUESTION 5

Your network contains an Active Directory domain named contoso.com. Contoso.com contains two servers named Server1 and Server2 that run Windows Server 2008 R2.

DirectAccess is deployed on Server2.

You need to configure Server1 as a network location server (NLS).



<http://www.gratisexam.com/>

Which Web Server (IIS) role service should you install on Server1?

- A. IIS Client Certificate Mapping Authentication
- B. URL Authorization
- C. IP and Domain Restrictions
- D. Request Filtering

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

See steps below:

If your DirectAccess server is acting as the network location server, you must install the Web Server (IIS) server role with the IP and Domain Restrictions role service. Source: <http://technet.microsoft.com/en-us/library/ee649160%28WS.10%29.aspx>

#### **QUESTION 6**

Your company has a main office and 15 branch offices. The company has a single Active Directory domain. All servers run Windows Server 2008 R2.

You need to ensure that the VPN connections between the main office and the branch offices meet the following requirements:

- All data must be encrypted by using end-to-end encryption.
- The VPN connection must use computer-level authentication.
- User names and passwords cannot be used for authentication.

What should you do?

- A. Configure a PPTP connection to use version 2 of the MS-CHAP v2 authentication.
- B. Configure an IPsec connection to use tunnel mode and preshared key authentication.
- C. Configure a L2TP/IPsec connection to use the EAP-TLS authentication.
- D. Configure a L2TP/IPsec connection to use version 2 of the MS-CHAP v2 authentication.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

EAP-Transport Layer Security (EAP-TLS), defined in RFC 5216, is an IETF open standard, and is well supported among wireless vendors. The security of the TLS protocol is strong, provided the user understands potential warnings about false credentials. It uses PKI to secure communication to a RADIUS authentication server or another type of authentication server. So even though EAP-TLS provides excellent security, the overhead of client-side certificates may be its Achilles' heel.

EAP-TLS is the original, standard wireless LAN EAP authentication protocol. Although it is rarely deployed, it is still considered one of the most secure EAP standards available and is universally supported by all manufacturers of wireless LAN hardware and software. The requirement for a client-side certificate, however unpopular it may be, is what gives EAP-TLS its authentication strength and illustrates the classic convenience vs. security trade-off. A compromised password is not enough to break into EAP-TLS enabled systems because the intruder still needs to have the client-side private key. The highest security available is when client-side keys are housed in smart cards.[4] This is because there is no way to steal a certificate's corresponding private key from a smart card without stealing the card itself. It is significantly more likely that the physical theft of a smart card would be noticed (and the smart card immediately revoked) than a (typical) password theft would be noticed. Up until April 2005, EAP-TLS was the only EAP type vendors needed to certify for a WPA or WPA2 logo.[5] There are client and server implementations of EAP-TLS in 3Com, Apple, Avaya, Brocade

Communications, Cisco, Enterasys Networks, Foundry, HP, Juniper, and Microsoft, and open source operating systems. EAP-TLS is natively supported in Mac OS X 10.3 and above, Windows 2000 SP4, Windows XP and above, Windows Mobile 2003 and above, and Windows CE 4.2

#### QUESTION 7

Your network has Network Access Protection (NAP) policies deployed.

You need to identify the health agent compliance status of a client computer.



<http://www.gratisexam.com/>

Which command should you run?

- A. netsh nap client show config
- B. net statistics workstation
- C. netsh nap client show state
- D. net config workstation

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation: Ref: [http://technet.microsoft.com/en-us/library/cc732873\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc732873(v=ws.10).aspx)

Netsh Commands for NAP Client  
show state

Displays state information, including client access restriction state, the state of installed enforcement clients and system health agents, and the client compliance and remediation results.

#### QUESTION 8

Your network contains an Active Directory forest. The forest contains a member server named Server1 that runs Windows Server 2008 R2.

You configure Server1 as a VPN server.

You need to ensure that only client computers that have up-to-date virus definitions can establish VPN connections to Server1.

Which server role, role service, or feature should you install?

- A. windows System Resource Manager (WSRM)
- B. Routing and Remote Access service (RRAS)
- C. Connection Manager Administration Kit (CMAC)
- D. File Server Resource Manager (FSRM)
- E. Windows Server Update Services (WSUS)
- F. Windows Internal Database
- G. Services for Network File System (NFS)
- H. Simple TCP/IP Services
- I. Network Policy Server (NPS)
- J. Health Registration Authority (HRA)

- K. Group Policy Management
- L. Wireless LAN Service
- M. Network Load Balancing (NLB)

**Correct Answer: I**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

From NPS Server role Configure Health Policies:

Health Policies are used with Network Access Protection (NAP) and allow you to designate the configuration required for NAP-capable client computers to access the network.

#### **QUESTION 9**

Your network contains an Active Directory domain.

You deploy Network Access Protection (NAP).

You need to verify whether VPN clients have Windows Firewall enabled.

What should you configure?

- A. system health validators (SHVs)
- B. connection request policies
- C. the Windows Authentication authentication provider
- D. health policies
- E. the Windows Accounting accounting provider
- F. Group Policy preferences
- G. IKEv2 client connections
- H. the RADIUS Authentication authentication provider
- I. remediation server groups
- J. the RADIUS Accounting accounting provider

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 10**

Your network contains an Active Directory domain.

Your company provides VPN access for multiple organizations.

You need to configure Network Policy Server (NPS) to forward authentication requests to the appropriate organization.

What should you configure on the NPS server?

- A. Group Policy preferences
- B. health policies
- C. remediation server groups

- D. IKEv2 client connections
- E. the RADIUS Accounting accounting provider
- F. system health validators (SHVs)
- G. the Windows Authentication authentication provider
- H. connection request policies
- I. the Windows Accounting accounting provider
- J. the RADIUS Authentication authentication provider

**Correct Answer:** H

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**With NPS Installed Roles**

Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.

For NAP VPN or 802.1X, you must configure PEAP authentication in connection request policy.

### QUESTION 11

Your network contains three servers named ADFS1, ADFS2, and ADFS3 that run Windows Server 2008 R2. ADFS1 has the Active Directory Federation Services (AD FS) Federation Service role service installed.

You plan to deploy AD FS 2.0 on ADFS2 and ADFS3.

You need to export the token-signing certificate from ADFS1, and then import the certificate to ADFS2 and ADFS3.

<http://www.lead2pass.com/70-649.html>

In which format should you export the certificate?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 12

Your company has an Active Directory forest that runs at the functional level of Windows Server 2008.

You implement Active Directory Rights Management Services (AD RMS). You install Microsoft SQL Server 2005.

When you attempt to open the AD RMS administration Web site, you receive the following error message: "SQL Server does not exist or access denied."

You need to open the AD RMS administration Web site.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Restart IIS.



- B. Install Message Queuing.
- C. Start the MSSQLSVC service.
- D. Manually delete the Service Connection Point in Active Directory Domain Services (AD DS) and restart AD RMS.

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### **QUESTION 13**

Your company has a main office and a branch office.

The network contains an Active Directory domain.

The main office contains a writable domain controller named Dc1. The branch office contains a read-only domain controller (RODC) named DC2.

You discover that the password of an administrator named Admin1 is cached on DC2.

You need to prevent Admin1's password from being cached on DC2.

What should you do?

- A. Create a Password Setting object (PSO).
- B. Modify the properties of DC2's computer account.
- C. Modify the properties of the domain.
- D. Modify the NTDS Site Settings.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### **QUESTION 14**

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the DHCP server role and the Remote Desktop Session Host (RD Session Host) role service installed. Server1 hosts one RemoteApp program named App1.

You have 200 client computers that run Windows 7. The client computers obtain their IP configurations from the DHCP server.

You enable Remote Desktop IP Virtualization on Server1.

You discover that some Remote Desktop connections to App1 are assigned the same IP address.

You need to ensure that all Remote Desktop connections receive a unique IP address.

What should you do?

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

D. Reconcile the DHCP scope.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

<http://www.lead2pass.com/70-649.html>

#### QUESTION 15

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

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

Server1 and Server2 are members of an RD Session Host server farm named farm 1.contoso.com.

You configure the RD Connection Broker role service on Server3 to support farm 1.contoso.com.

You need to create DNS records to support RD Connection Broker load balancing.

Which record or records should you create for farm 1.contoso.com?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 16

You need to create a RemoteApp and Desktop Connection configuration (.wcx) file.

Which tool should you use?

- A. Remote Desktop Gateway Manager
- B. RemoteApp Manager
- C. Remote Desktop Connection Manager
- D. Remote Desktop Session Host Configuration

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

<http://www.lead2pass.com/70-649.html>

**QUESTION 17**

Your company has an Active Directory domain. A server named Server2 runs Windows Server 2008 R2. All client computers run Windows 7.

You install the Remote Desktop Services server role, RD Web Access role service, and RD Gateway role service on Server2.

You need to ensure that all client computers have compliant firewall, antivirus software, and antispyware.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

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

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Health requirement policies on the NAP health policy server determine whether a NAP-capable client is compliant or noncompliant, how to treat noncompliant NAP clients and whether they should automatically remediate their health state, and how to treat non-NAP-capable clients for different NAP enforcement methods. A health requirement policy is a combination of a connection request policy, a health policy, Network Access Protection settings, and a network policy.

**Windows Security Health Validator**

Windows Vista | Windows XP

Use the settings below to define a Windows Security Health Validator policy. Your selections define the requirements for client computers connecting to your network.

[Learn more...](#)

**Firewall**

☒ A firewall is enabled for all network connections

**Virus Protection**

☒ An antivirus application is on ☒ Antivirus is up to date

**Spyware Protection**

☒ An antispyware application is on ☒ Antispyware is up to date

**Automatic Updating**

☒ Automatic updating is enabled

**Security Update Protection**

☐ Restrict access for clients that do not have all available security updates installed

Important and above

Specify the minimum number of hours allowed since the client has checked for new security updates: 22

By default, clients can receive security updates from Microsoft Update. If additional sources are required for your deployment, select one or both of the following sources.

☐ Windows Server Update Services ☒ Windows Update

OK Cancel Apply

Source: <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=8e47649e-962c-42f8-9e6f-21c5ccdcf490&displaylang=en>

#### QUESTION 18

Your network contains a Web server named Web1 that runs Windows Server 2008 R2. Web1 is located on the perimeter network.

Web contains a Web site named Public.

You need to prevent the Public Web site from responding to requests that originate from the internal network.

Which feature should you configure?

- A. Authentication
- B. IIS Manager Permissions
- C. IP Address and Domain Restrictions
- D. Authorization Rules

**Correct Answer: C**

**Section: (none)**

## **Explanation**

### **Explanation/Reference:**

Explanation:

### **QUESTION 19**

Your network contains an Active directory domain named fabrikam.com. The domain contains a Web server named Web1 that runs Windows Server 2008 R2.

You install the SMTP Server feature on Web 1.

You need to verify whether you can establish an SMTP connection to Web1.

Which tool should you use?

- A. Internet Information Services (IIS) 6.0 Manager
- B. Internet Information Services (II) Manager
- C. Telnet
- D. Windows Firewall

**Correct Answer: C**

**Section: (none)**

**Explanation**

### **Explanation/Reference:**

Explanation:

### **QUESTION 20**

Your network contains an Active Directory domain named fabrikam.com. The domain contains a Web server named Web1 that runs Windows Server 2008 R2.

You have a Web site named Corp. The content on Corp is stored on a FAT32 partition. Corp contains a Web page named Test.html.

You need to ensure that only a user named Devi can access Test.html from the Corp Web site. All of the other content on Corp must be accessible to everyone.

Which feature should you configure?

- A. IP Address and Domain Restrictions
- B. Feature Delegation
- C. Authorization Rules
- D. IIS Manager Permissions

**Correct Answer: C**

**Section: (none)**

**Explanation**

### **Explanation/Reference:**

Explanation: Using Authorization Rules

You can grant or deny specific computers, groups of computers, or domains access to sites, applications, directories, or files on your server. For example, suppose your intranet server hosts content that is available to all employees, in addition to content that should be viewed only by members of specific groups, such as Finance or Human Resources. By configuring URL authorization rules, you can prevent employees who are not members of those specified groups from accessing restricted content.

**QUESTION 21**

Your network contains an Active directory domain named fabrikam.com. The domain contains a Web server named Web1 that runs Windows Server 2008 R2.

You install the FTP Server role service on Web1.

You need to manage the FTP server settings on Web1.

Which tool should you use?

- A. Services
- B. Internet Information Services (IIS) 6.0 Manager
- C. FTP
- D. Internet Information Services (IIS) Manager

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 22**

Your network uses Multiple Activation Key (MAK) licenses.

You perform a Server Core installation of Windows Server 2008 R2.

During the installation, you enter the license key.

You need to activate Windows Server 2008 R2 on the server.

Which command should you run?

- A. install-calpack
- B. slmgr.vbs -ato
- C. ocsetup.exe was-windowsactivationsservice
- D. slmgr.vbs -ipk

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 23**

Your corporate network has a member server named RAS1 that runs Windows Server 2008 R2.

You configure RAS1 to use the Routing and Remote Access Services (RRAS).

The company's remote access policy allows members of the Domain Users group to dial in to RAS1. The company issues smart cards to a employees.

You need to ensure that smart card users are able to connect to RAS1 by using a dial-up connection.

What should you do?

- A. Create a remote access policy that requires users to authenticate by using MS-CHAP v2.
- B. Create a remote access policy that requires users to authenticate by using SPAP.
- C. Install the Network Policy Server (NPS) server role on RAS1.
- D. Create a remote access policy that requires users to authenticate by using EAP-TLS.

**Correct Answer:** D

**Section:** (none)

**Explanation**

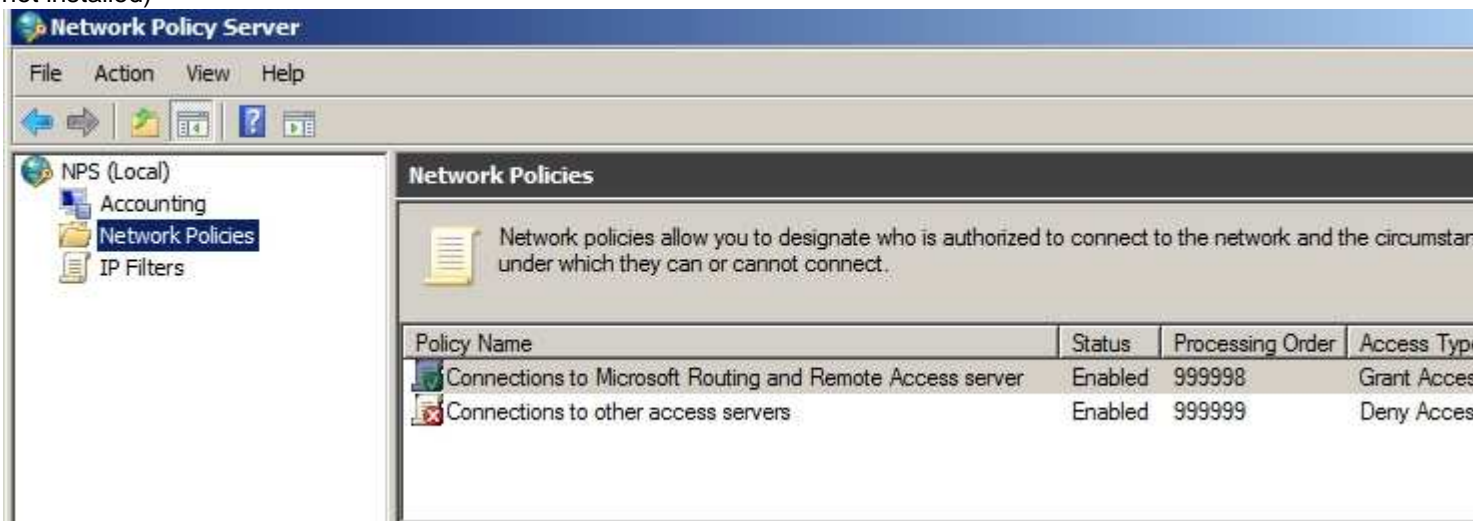
**Explanation/Reference:**

Explanation:

Not Needed to install NPS role.

You can use RRAS to Create a remote access policy that requires users to authenticate by using EAP-TLS.

Right-click on "Remote access Logging & Policies" Launch NPS (You will show only these options -- NPS roles not installed)



**QUESTION 24**

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 25**

Your network contains an Active Directory forest. The forest contains a member server named VPN1 that runs Windows Server 2008 R2.

You configure VPN1 as a VPN server.

You need to ensure that only client computers that have Windows Update enabled can establish VPN connections to VPN1.

What should you install on VPN1?

- A. Network Policy Server (NPS)
- B. Windows Server Update Services (WSUS)
- C. Connection Manager Administration Kit (CMAK)
- D. Health Registration Authority (HRA)

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

From NPS Server Configure Health Policies:

Health Policies are used with Network Access Protection (NAP) and allow you to designate the configuration required for NAP-capable client computers to access the network.

#### **QUESTION 26**

Your network has Network Access Protection (NAP) deployed. The network contains two servers named Server1 and Server2. Server1 is Network Policy Server (NPS). Server2 has a third-party antivirus solution installed.

Server1 is configured to use a custom system health validator provided by the antivirus vendor. The system health validator uses Server2 to identify the version of the current antivirus definition.

You need to ensure that NAP clients are considered noncompliant if Server1 cannot connect to Server2.

Which error code resolution setting should you configure?

- A. SHA not responding to NAP client
- B. SHV not responding
- C. SHV unable to contact required services
- D. SHA unable to contact required services



**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

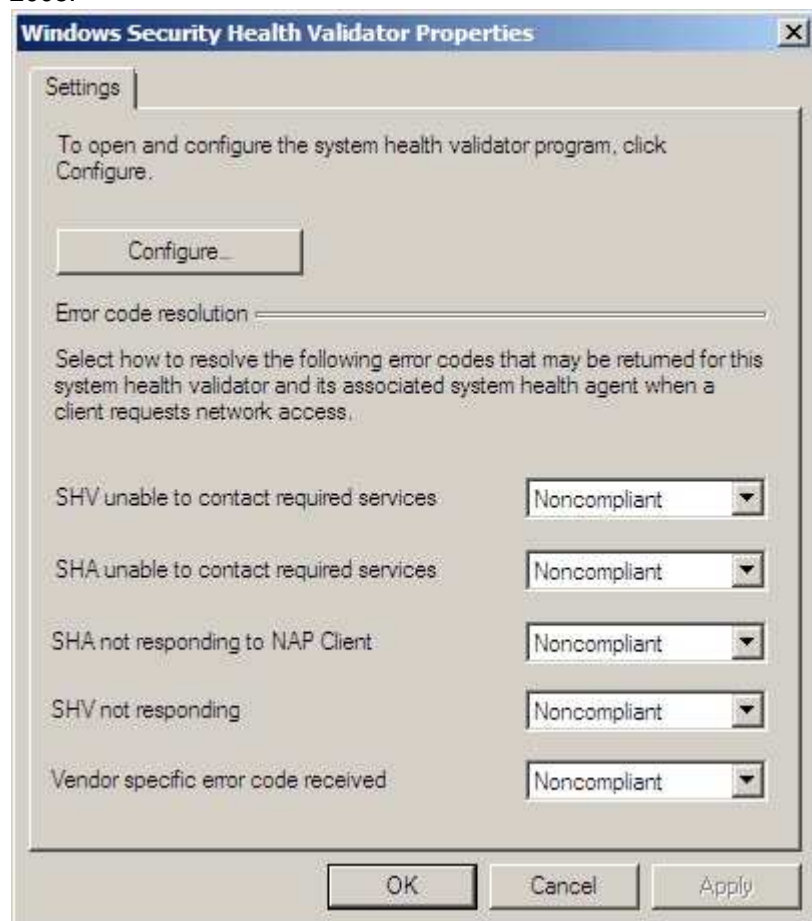
Explanation:

System health validators (SHVs) define configuration requirements for NAP client computers. Windows Security Health Validator (WSHV) is included with Windows Server 2008 and Windows Server 2008 R2.

**SHV error codes:**

All SHVs include five error code conditions. If an error code is returned to the SHV, you can choose to have the SHV evaluate the client as either compliant or noncompliant.

The following figure describes Windows Security Health Validator Properties dialog box in Windows Server 2008.



Windows Security Health Validator Properties dialog box

The following is a description of the available error codes:

**SHV unable to contact required services.** This error can occur if NPS loses connectivity to a health requirement server, such as an antivirus signature server.

**SHA unable to contact required services.** This error can occur if the SHA is unable to successfully read the client configuration.

**SHA not responding to NAP Client.** This error can occur if a SHA is not properly initialized and registered.

**SHV not responding.** This error can occur if the performance of an SHV is degraded (for example, if NPS is out of memory).

**Vendor specific error code received.** This error can occur if NPS receives an error code that is unique to the SHA or SHV vendor. Some vendors might return this code when NPS is unable to contact a health requirement server.

#### QUESTION 27

You need to document the following configurations of a server that runs Windows Server 2008 R2:

- System services
- Startup programs
- Hardware configuration
- Current CPU, network, disk, and memory utilization

Which command should you run?

- A. msinfo32.exe
- B. perfmon.exe /report
- C. systeminfo.exe
- D. mrinfo.exe local host

**Correct Answer: B**

**Section: (none)**

**Explanation**

#### Explanation/Reference:

Explanation:

Sous Windows 7 et 2008 , vous pouvez générer en tant qu'administrateur et fou d'optimisation, un rapport détaillant l'état des ressources matérielles, les temps de réponses du système et les processus sur l'ordinateur local, ainsi que les informations système et les données de configuration. Ce rapport inclut des suggestions sur les manières d'optimiser les performances et d'accélérer le fonctionnement du système. Le rapport peut être sauvegardé au format html.

#### QUESTION 28

Your network contains a domain controller named DC1 and a member server named Server1.

You save a copy of the Active Directory Web Services (ADWS) event log on Dc1. You copy the log to Server1.

You open the event log file on Server1 and discover that the event description information is unavailable.

You need to ensure that the event log file displays the same information when the file is open on

Server1 and on Dc1.

What should you do on Server1?

- A. Copy the LocaleMetaData folder from Dc1.
- B. Copy the SYSVOL folder from Dc1.
- C. Create a custom view.
- D. Import a custom view.

**Correct Answer: A**

**Section: (none)**

**Explanation**

#### Explanation/Reference:

Explanation:

#### **QUESTION 29**

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the SNMP Service installed.

You perform an SNMP query against Server1 and discover that the query returns the incorrect contact and location information.

You need to change the contact and location information returned by Server1.

What should you do?

- A. From the properties of the SNMP Trap Service, modify the Logon settings.
- B. From the properties of the SNMP Service, modify the Agent settings.
- C. From the properties of the SNMP Trap Service, modify the General settings.
- D. From the properties of the SNMP Service, modify the General settings.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 30**

Your network contains a Windows Server Update Services (WSUS) server. A Group Policy object (GPO) configures all WSUS client computers to detect updates hourly and install updates weekly.

You download a critical update.

You need to ensure that the WSUS client computers install the critical update during the next detection interval.

What should you do?

- A. From the client computers, run gpupdate.exe /force.
- B. From the client computers, run wuauclt.exe /force.
- C. From the server, configure the Synchronization Schedule options.
- D. From the server, configure the deadline settings.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Ignore maintenance windows and install immediately at deadline:

Specifies whether the software updates in the deployment are installed at the deadline regardless of a configured maintenance window.

By default, this setting is not enabled and is available only when there is a deadline configured for the deployment.

This setting is beneficial when there are software updates that must be installed on client computers as soon as possible, such as the updates in an expedited deployment.

This setting is available on the Schedule page of the Deploy Software Updates Wizard.

#### **QUESTION 31**

Your network contains a Windows Server Update Services (WSUS) server named Server1.

You need to configure all WSUS client computers to download approved updates directly from the Microsoft Update servers. The solution must ensure that all WSUS client computers report successful installation of updates to Server1.

What should you do?

- A. From Server1, modify the Update Source and Proxy options.
- B. From Active Directory, deploy a Group Policy object (GPO).
- C. From Server1, modify the Update Files and Languages options.
- D. From the WSUS client computers, modify the local computer policy.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

### **QUESTION 32**

Your network contains a server that runs Windows Server 2008 R2 named Server1.

You install a new application on Server1. After the installation, you discover that Server1 frequently becomes unavailable.

You need to identify whether the issues on Server1 coincide with the installation of the application.

What should you do?

- A. From Administrative Tools, run Windows Memory Diagnostic.
- B. From Reliability Monitor, review the reliability details.
- C. From the command prompt, run the Program Compatibility Wizard.
- D. From the System Configuration utility, select Diagnostic startup.

**Correct Answer: B**

**Section: (none)**

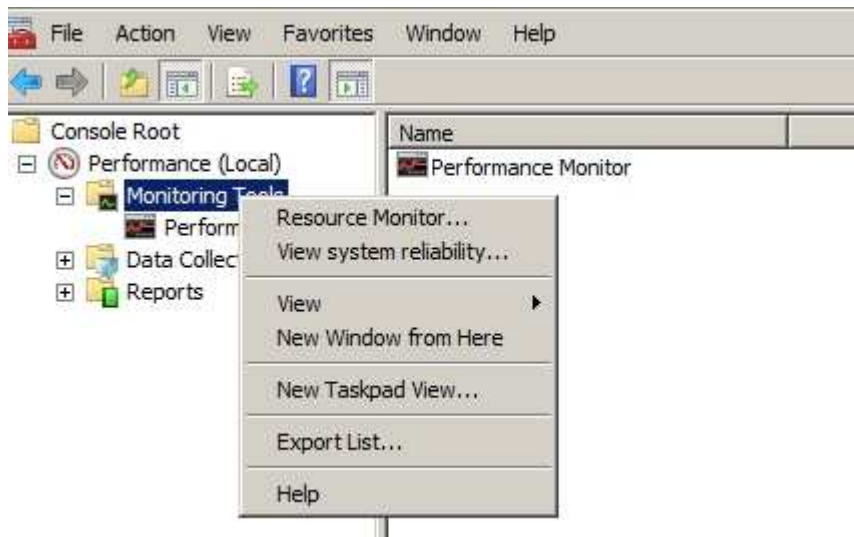
**Explanation**

**Explanation/Reference:**

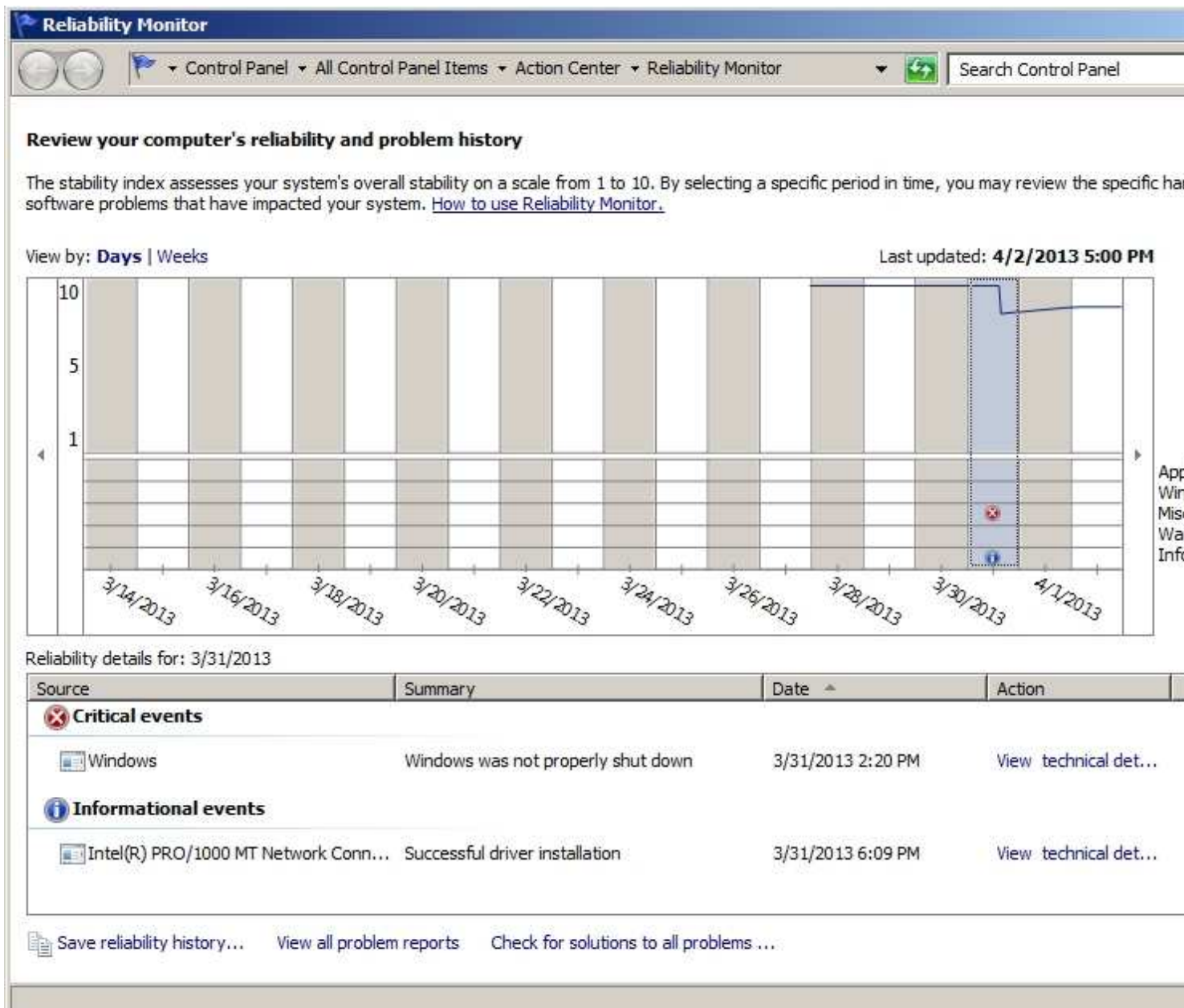
Explanation:

Enable Reliability Monitor :<http://support.microsoft.com/kb/983386/en-us>

**Use it!!**



**Click "view system reliability"**



### QUESTION 33

Your network contains an Active Directory domain. The domain contains several domain controllers.

You need to modify the Password Replication Policy on a read-only domain controller (RODC).

Which tool should you use?

- A. Computer Management
- B. Active Directory Users and Computers
- C. Group Policy Management
- D. Security Configuration Wizard
- E. Active Directory Domains and Trusts

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Reference:

<http://technet.microsoft.com/en-us/library/rodc-guidance-for-administering-the-password-replication-policy.aspx>

**Administering the Password Replication Policy**

This topic describes the steps for viewing, configuring, and monitoring the Password Replication Policy (PRP) and password caching for read-only domain controllers (RODCs).

To configure the PRP using Active Directory Users and Computers

1. Open Active Directory Users and Computers as a member of the Domain Admins group.
2. Ensure that you are connected to a writeable domain controller running Windows Server 2008 in the correct domain.
3. Click Domain Controllers, and in the details pane, right-click the RODC computer account, and then click Properties.
4. Click the Password Replication Policy tab.
5. The Password Replication Policy tab lists the accounts that, by default, are defined in the Allowed list and the Deny list on the RODC. To add other groups that should be included in either the Allowed list or the Deny list, click Add.

To add other accounts that will have credentials cached on the RODC, click Allow passwords for the account to replicate to this RODC.

To add other accounts that are not allowed to have credentials cached on the RODC, click Deny passwords for the account from replicating to this RODC.

**QUESTION 34**

Your network contains a Web server named Server1 that runs Windows Server 2008 R2. The network contains two subnets named Subnet1 and Subnet2.

Server1 contains a Web site named Site1.

You need to prevent Server1 from responding to requests that originate from Subnet2.

Which feature should you configure from Internet Information Services (IIS) Manager?

- A. Authentication
- B. Connection Strings
- C. Default Document
- D. Error Pages
- E. Feature Delegation
- F. HTTP Redirect
- G. HTTP Response Headers
- H. IIS Manager Permissions
- I. IP Address and Domain Restrictions
- J. ISAPI and CGI Restrictions

- K. ISAPI Filters
- L. Management Service
- M. Request Filtering
- N. SSL Settings
- O. Worker Processes

**Correct Answer: I**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

In IIS 7, all Internet Protocol (IP) addresses, computers, and domains can access your site by default.

To enhance security, you can limit access to your site by creating an allow rule that grants access to all IP addresses (the default), a specific IP address, a range of IP addresses, or a specific domain.

For example, if you have a site on an intranet server that is connected to the Internet, you can prevent Internet users from accessing your intranet site by allowing access only to members of your intranet.

[http://technet.microsoft.com/en-us/library/cc731598\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc731598(v=ws.10).aspx)

### **QUESTION 35**

Your network contains an Active Directory domain named fabrikam.com. The domain contains a Web Server named Web1 that runs Windows Server 2008 R2.

You create a new site named Site1.

You need to ensure that when a user enters a URL on Site1 for a resource that does not exist, a custom Web page displays.

Which feature should you configure?

- A. HTTP Redirect
- B. Authorization Rules
- C. Error Pages
- D. Default Document

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Configurability of Custom Errors

IIS 7.0 makes it easier to configure custom errors exactly how you want them. Added configuration options in the UI give administrators more flexibility and granularity; you can edit the existing configuration settings, or add completely new ones. Configuring error pages through the IIS Manager is done via the Error Pages feature in the main pane:





To edit the configuration of an existing customer error page, select the status code entry in the main pane, and choose Edit... in the Actions pane. The Edit Customer Error Page window will appear:

**Edit Custom Error Page** [?] [X]

Status code:  
  
 Example: 404 or 404.2

Response Action

☒ **Insert content from static file into the error response**

File path:

☒ Try to return the error file in the client language

☐ **Execute a URL on this site**

URL (relative to site root):  
  
 Example: /ErrorPages/404.aspx

☐ **Respond with a 302 redirect**

Absolute URL:  
  
 Example: http://www.contoso.com/404.aspx

The Add Custom Error Page looks almost the same, except the fields are blank:



<http://blogs.msdn.com/b/webtopics/archive/2008/05/28/iis-7-0-http-error-pages.aspx>

### QUESTION 36

Your network contains an Active directory domain named fabrikam.com. The domain contains a Web server named Web1 that runs Windows Server 2008 R2.

You create three application pools named AppPool1, AppPool2, and AppPool3.

You need to recycle AppPool1 without affecting AppPool2 and AppPool3.

Which tool should you use?

- A. Iisreset
- B. Internet Information Services (IIS) 6.0 Manager
- C. Internet Information Services (IIS) Manager
- D. Services

**Correct Answer: C**

**Section: (none)**

**Explanation**

### Explanation/Reference:

Explanation:

Occasionally, you may have to immediately recycle an unhealthy worker process instead of waiting for the next configured recycle. Rather than abruptly stopping the worker process, which can cause service interruptions, you can use on-demand recycling.

Overlapping recycling, the default, lets an unhealthy worker process become marked for recycling, but continues handling requests that this unhealthy process has already received.

It does not accept new requests from HTTP.sys. When all existing requests are handled, the unhealthy worker process shuts down.

1. Open IIS Manager. For information about opening IIS Manager, see Open IIS Manager (IIS 7).
2. In the Connections pane, expand the server node and click Application Pools.
3. On the Application Pools page, select the application pool you want to recycle immediately.
4. In the Actions pane, click Recycle and then click Yes.

Ref: [http://technet.microsoft.com/en-us/library/cc770764\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc770764(v=ws.10).aspx)

#### **QUESTION 37**

Your network contains an Active Directory domain named fabrikam.com. The domain contains a Web server named Web1 that runs Windows Server 2008 R2.

You create four Web sites named Site1, Site2, Site3, and Site4.

You associate each Web site to a different application pool.

You need to view the amount of memory that each application pool is currently using.

Which feature should you use?

- A. HTTP Response Headers
- B. Worker Processes
- C. Management Service
- D. Request Filtering

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 38**

Your network contains a server named WDS1 that has the Windows Deployment Services (WDS) server role installed. WDS1 is used to deploy Windows 7.

You create a virtual hard disk (VHD) file that contains an installation of Windows Server 2008 R2 Service Pack 1 (SP1),

From the Windows Deployment Services console, you attempt to add the VHD file, and you receive the error message shown in the exhibit. (Click the Exhibit button.)

You need to ensure that you can deploy the VHD file by using WDS.

What should you do?

**Exhibit:**



- A. Run wdsutil.exe and specify the update-serverfiles parameter.
- B. Run wdsutil.exe and specify the /add-image parameter.
- C. Run imagex.exe and specify the /apply parameter.
- D. Run imagex.exe and specify the /append parameter.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

To add a virtual hard disk image to the server

1. Click Start, right-click Command Prompt, and then click Run as administrator.

2. You must create an image group because .vhd images cannot be in image groups with .wim images. To create an image group for the .vhd image, use the following syntax: WDSUTIL /Add-ImageGroup /ImageGroup:<image group name>.

Example: WDSUTIL /Add-ImageGroup /ImageGroup:'VHD Image Group'

3. To add the .vhd image to the server, use the following syntax (at a minimum): WDSUTIL /Verbose /Progress /Add-Image /ImageFile:<path> /ImageType:Install /ImageGroup:<image group name>.

For differencing disks, the path to the image should be to the .vhd file of the differencing disk and not to the parent disk. Adding the differencing .vhd will add the parent .vhd file to the server, but only the differencing disk will be active (the parent .vhd will be inactive). If the differencing disk is part of chain, choose the last .vhd in the chain. In that case, the immediate parent .vhd and all preceding parent .vhd files in the chain will also be added. Full syntax: WDSUTIL /add-Image /ImageFile:<.vhd file path> [/Server:<server name>] /ImageType:install [/ImageGroup:<image group name>] [/Filename:<new image file name>] [/UnattendFile:<full path to unattend file>]

Example: WDSUTIL /Verbose /Progress /Add-Image /ImageFile:'C:\vhd\WindowsServer2008R2.vhd' / Server:MyWDSserver /ImageType:Install /ImageGroup:'VHD Image Group'

4. Repeat step 3 until you have added all of your .vhd images.

5. If you want to update the description for an image, use the following steps:

a. Run WDSUTIL /Get-ImageGroup /ImageGroup:<image group name> and note the name that the server assigned to the image. To display the full image metadata on each image in the group, append /Detailed.

Example: WDSUTIL /Get-ImageGroup /ImageGroup:'VHD Image Group'

b. To update the description for an image, use the following syntax where <image name> is the name you noted in the previous step: WDSUTIL /Set-Image /Image:<image name> /ImageType:Install / ImageGroup:<image group name> /Description:<description>.

Example: WDSUTIL /Set-Image /Image:'VHD image' /ImageType:Install /ImageGroup:'VHD Image Group' / Description:'VHD image for R2'

Source: [http://technet.microsoft.com/en-us/library/dd363560\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd363560(WS.10).aspx)

**QUESTION 39**

Your network contains a server that runs Windows Server 2008 R2 and has the Windows Deployment Services (WDS) server role installed.

The server contains an image of Windows Vista Service Pack 2 (SP2), an image of Windows 7, an image of Windows Server 2008, and an image of Windows Server 2008 R2.

You need to update the drivers in the images. You want to achieve this goal by using the minimum amount of administrative effort.

<http://www.lead2pass.com/70-649.html>

Which tool should you use?

- A. dism
- B. Pkgmgr
- C. Windows Deployment Services console
- D. Windows Driver Kit (WDK)

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

In Windows Server 2008 R2, you can use Windows Deployment Services to add driver packages to the server and configure them to be deployed to client computers along with the install image. Note that this functionality is only available when you are installing images of the following operating systems: Windows Vista with SP1, Windows Server 2008, Windows 7, and Windows Server 2008 R2.

WDS console because Dism no achieve this goal using the minimum administrative effort.

Source:[http://technet.microsoft.com/en-us/library/dd348456\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd348456(WS.10).aspx)

**QUESTION 40**

Your network contains a server named Server1 that runs Windows Server 2008 R2.

Server1 has the following Remote Desktop Services (RDS) role services installed: \* Remote Desktop Session Host (RD Session Host) \* Remote Desktop Web Access (RD Web Access)

You publish 10 RemoteApp programs on Server1 by using RD Web Access.

You need to ensure that when users log on to the RD Web Access page, they see only the RemoteApp programs assigned to them.

What should you modify from RemoteApp Manager?

- A. the properties of each RemoteApp program
- B. the RD Gateway Settings
- C. the RDP Settings
- D. The RD Session Host Server Settings

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 41**

Your network contains an Active Directory domain named contoso.com. The domain contains a server named

Server1 and a client computer named Computer1.

Server1 runs Windows Server 2008 R2.  
Computer1 runs Windows 7.

Server1 has the Remote Desktop Session Host (RD Session Host) role service and the Remote Desktop Web Access (RD Web Access) role service installed.

You need to ensure that new RemoteApp programs published on Server1 are automatically added to the Start menu on Computer1.  
What should you do?

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 42**

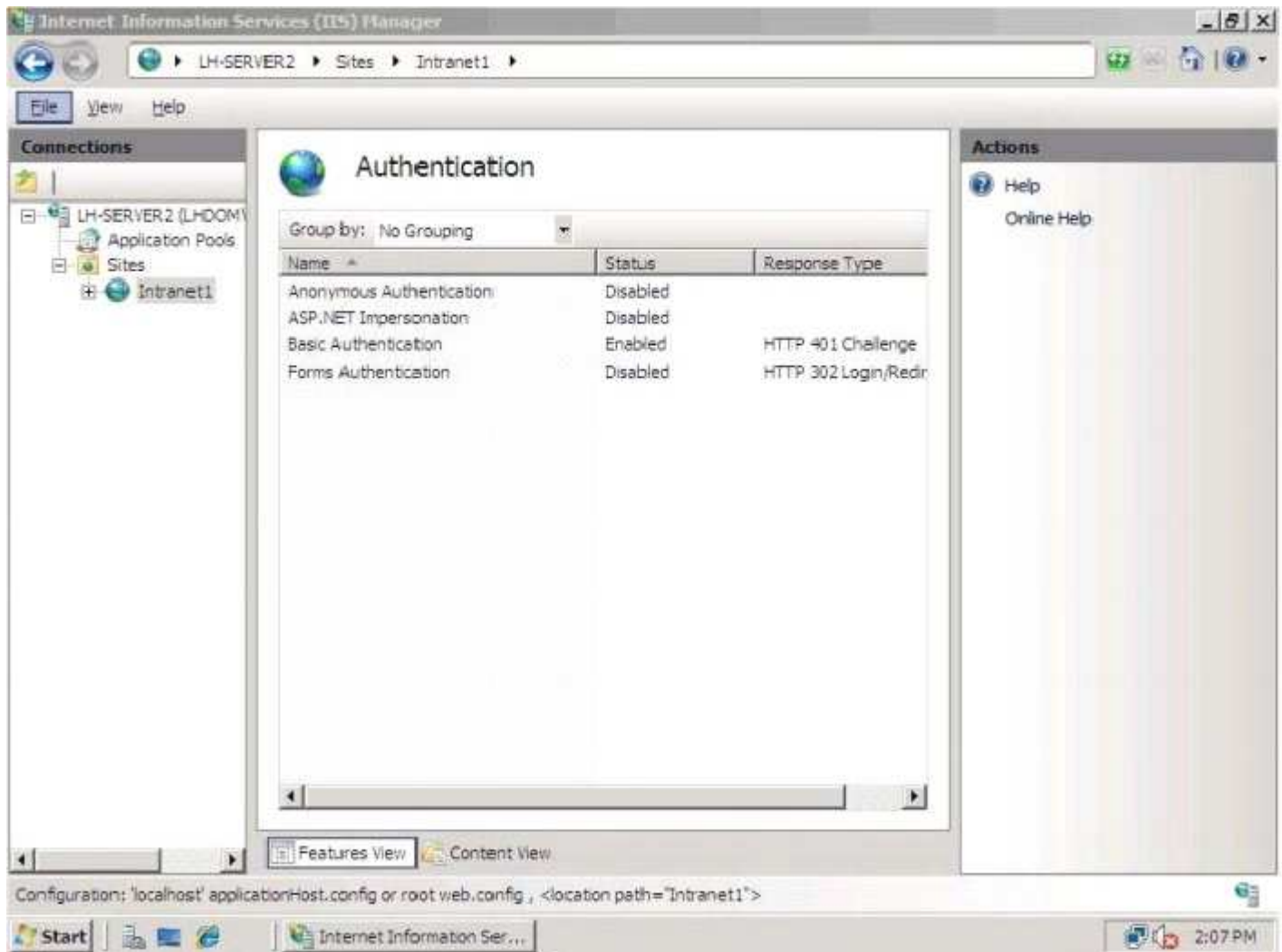
You manage a member server that runs Windows Server 2008 R2.  
The server has the Web Server (IIS) server role installed. The Web server hosts a Web site named Intranet1.

Only internal Active Directory user accounts have access to the Web site.  
The authentication settings for Intranet1 are configured as shown in the exhibit.

You need to ensure that users authenticate to the Web site by using only the:  
Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) encrypted Active Directory credentials.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

**Exhibit:**



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

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 43

Your network contains a Web server named Server1 that runs Windows Server 2008 R2. You modify the configuration of Server1.

You need to restore the previous Web server configuration. What should you run?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 44**

Your network contains an Active Directory domain. The domain contains a server named Server1. Server1 runs Windows Server 2008 R2.

You need to mount an Active Directory Lightweight Directory Services (AD LDS) snapshot from Server1.

What should you do?

- A. Run ldp.exe and use the Bind option.
- B. Run diskpart.exe and use the Attach option.
- C. Run dsdbutil.exe and use the snapshot option.
- D. Run imagex.exe and specify the /mount parameter.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

DSDBUTIL.EXE

Performs database maintenance of the Active Directory Domain Services (AD DS) store, facilitates configuration of Active Directory Lightweight Directory Services (AD LDS) communication ports, and views AD LDS instances that are installed on a computer.

#### **QUESTION 45**

Your company has a server that runs an instance of Active Directory Lightweight Directory Services (AD LDS).

You need to create new organizational units in the AD LDS application directory partition.

What should you do?

- A. Use the Active Directory Users and Computers snap-in to create the organizational units on the AD LDS application directory partition.
- B. Use the ADSI Edit snap-in to create the organizational units on the AD LDS application directory partition.
- C. Use the dsadd OU <OrganizationalUnitDN> command to create the organizational units.
- D. Use the dsmod OU <OrganizationalUnitDN> command to create the organizational units.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:



To create new OUs in the AD LDS application directory partition, you should use ADSI Edit snap-in. ADSI Edit is a snap-in that runs in a Microsoft Management Console (MMC). The default console containing ADSI Edit is Adsiedit.msc. If this snap-in is not added in your MMC, you can do it by adding through Add/Remove Snap-in menu option in the MMC or you can open Adsiedit.msc from a Windows Explorer.

#### QUESTION 46

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

Active Directory Rights Management Services (AD RMS) is deployed in contoso.com. An AD RMS trusted user domain (TUD) exists between contoso.com and adatum.com.

From the AD RMS logs, you discover that some clients that have IP addresses in the adatum.com forest are authenticating as users from contoso.com.

You need to prevent users from impersonating contoso.com users.

What should you do?

- A. Configure trusted e-mail domains.
- B. Enable lockbox exclusion in AD RMS.
- C. Create a forest trust between adatum.com and contoso.com.
- D. Add a certificate from a third-party trusted certification authority (CA).

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 47

Your company has an Active Directory forest that contains a single domain. The domain member server has an Active Directory Federation Services (AD FS) server role installed.

You need to configure AD FS to ensure that AD FS tokens contain information from the Active Directory domain.



<http://www.gratisexam.com/>

What should you do?

- A. Add and configure a new account store.
- B. Add and configure a new account partner.
- C. Add and configure a new resource partner.
- D. Add and configure a Claims-aware application.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

To configure the AD FS trust policy to populate AD FS tokens with employee's information from Active directory domain, you need to add and configure a new account store.

AD FS allows the secure sharing of identity information between trusted business partners across an extranet. When a user needs to access a Web application from one of its federation partners, the user's own organization is responsible for authenticating the user and providing identity information in the form of "claims" to the partner that hosts the Web application. The hosting partner uses its trust policy to map the incoming claims to claims that are understood by its Web application, which uses the claims to make authorization decisions. Because claims originate from an account store, you need to configure account store to configure the AD FS trust policy.

Reference: Active Directory Federation Services

<http://msdn2.microsoft.com/en-us/library/bb897402.aspx>

#### **QUESTION 48**

Your network contains an Active Directory domain named contoso.com. Contoso.com contains a domain controller named DC1 and a read-only domain controller (RODC) named RODC1.

You need to view the most recent user accounts authenticated by RODC1.

What should you do first?

- A. From Active Directory Sites and Services, right-click the Connection object for DC1, and then click Replicate Now.
- B. From Active Directory Sites and Services, right-click the Connection object for DC2, and then click Replicate Now.
- C. From Active Directory Users and Computers, right-click contoso.com, click Change Domain Controller, and then connect to DC1.
- D. From Active Directory Users and Computers, right-click contoso.com, click Change Domain Controller, and then connect to RODC1.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

[http://technet.microsoft.com/en-us/library/rodc-guidance-for-administering-the-password-replication-policy.aspx#BKMK\\_Auth2](http://technet.microsoft.com/en-us/library/rodc-guidance-for-administering-the-password-replication-policy.aspx#BKMK_Auth2)

#### **QUESTION 49**

You deploy a new Active Directory Federation Services (AD FS) federation server.

You request new certificates for the AD FS federation server.

You need to ensure that the AD FS federation server can use the new certificates.

To which certificate store should you import the certificates?

- A. Computer
- B. IIS Admin Service service account
- C. Local Administrator
- D. World Wide Web Publishing Service service account

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 50**

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**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**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 51**

Active Directory Rights Management Services (AD RMS) is deployed on your network.

You need to configure AD RMS to use Kerberos authentication.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Register a service principal name (SPN) for AD RMS.
- B. Register a service connection point (SCP) for AD RMS.
- C. Configure the identity setting of the \_DRMSAppPool1 application pool.
- D. Configure the useAppPoolCredentials attribute in the Internet Information Services (IIS) metabase.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 52**

Your company has an Active Directory Rights Management Services (AD RMS) server. Users have Windows Vista computers. An Active Directory domain is configured at the Windows Server 2003 functional level.

You need to configure AD RMS so that users are able to protect their documents.

What should you do?

- A. Install the AD RMS client 2.0 on each client computer.
- B. Add the RMS service account to the local administrators group on the AD RMS server.
- C. Establish an e-mail account in Active Directory Domain Services (AD DS) for each RMS user.
- D. Upgrade the Active Directory domain to the functional level of Windows Server 2008.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

To configure AD RMS to enable users to use it and protect their documents, you should configure an email account in Active Directory Domain Services (AD DS) for each user.

To regulate access to rights-protected content for all AD RMS users in the AD DS forest, AD RMS must use AD DS. AD RMS cannot grant licenses to publish and consume right-protected content if AD DS is not available to work with AD RMS.

You should not add and configure ADRMSADMIN account in local administrators group on the user computers because AD DS is needed for AD RMS to function properly.

Reference: <http://technet2.microsoft.com/windowsserver2008/en/library/c8f83d5b-e10d-4c31-8af9-d2afb076dbf81033.mspx>

#### **QUESTION 53**

Your company has a main office and a branch office. The branch office contains a read-only domain controller named RODC1.

You need to ensure that a user named Admin1 can install updates on RODC1. The solution must prevent Admin1 from logging on to other domain controllers.

What should you do?

- A. Run ntdsutil.exe and use the Roles option.
- B. Run dsmgmt.exe and use the Local Roles option.
- C. From Active Directory Sites and Services, modify the NTDS Site Settings.
- D. From Active Directory Users and Computers, add the user to the Server Operators group.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

RODC: USING THE DSMGMT.EXE UTILITY TO MANAGE LOCAL ADMINISTRATORS

One of the benefits of RODC is that you can add local administrators who do not have full access to the domain administration.

This gives them the ability to manage the server but not add or change active directory objects unless those roles are delegated.

Adding this type of user is done using the dsmgmt.exe utility at the command prompt.

The following graphic shows a few commands including:

adding local roles

showing local roles



```
C:\Users\Administrator.CONTOSO>dsmgmt.exe
dsmgmt.exe: local roles
local roles: add contoso Administrators
Successfully updated local role.
local roles: show role Administrators
CONTOSO\
local roles:
```

Remember, an RODC does not have all of the capabilities of a writeable domain controller.

Consequently, an RODC cannot serve as the global catalog, operations masters, or bridgehead server.

For more information see this Technet Article: [http://technet.microsoft.com/en-us/library/cc772478\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc772478(WS.10).aspx)

#### QUESTION 54

Your network contains an Active Directory domain. The domain contains two sites named Site1 and Site2. Site1 contains four domain controllers. Site2 contains a read-only domain controller (RODC).

You add a user named User1 to the Allowed RODC Password Replication Group.

The WAN link between Site1 and Site2 fails.

User1 restarts his computer and reports that he is unable to log on to the domain.

The WAN link is restored and User1 reports that he is able to log on to the domain.

You need to prevent the problem from reoccurring if the WAN link fails.

What should you do?

- A. Create a Password Settings object (PSO) and link the PSO to User1's user account.
- B. Create a Password Settings object (PSO) and link the PSO to the Domain Users group.
- C. Add the computer account of the RODC to the Allowed RODC Password Replication Group.
- D. Add the computer account of User1's computer to the Allowed RODC Password Replication Group.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 55**

Your network contains two standalone servers named Server1 and Server2 that have Active Directory Lightweight Directory Services (AD LDS) installed.

Server1 has an AD LDS instance.

You need to ensure that you can replicate the instance from Server1 to Server2.

What should you do on both servers?

- A. Obtain a server certificate.
- B. Import the MS-User.ldf file.
- C. Create a service user account for AD LDS.
- D. Register the service location (SRV) resource records.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation: [http://technet.microsoft.com/en-us/library/dd548356\(v=WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd548356(v=WS.10).aspx)

**Or/And**

#### **Considerations when using a domain-based service account with AD LDS**

By Tony Murray on Monday, April 13, 2009 9:39 PM

When creating an AD LDS instance you are prompted to specify an account to use as the service account. At this point you can specify either the Network Service account or another account. Unless you have a particular need, you should choose the built-in Network Service account. If you opt for a domain-based service account you have to jump through a whole lot of hoops to get things working. Also, you typically end up giving your domain-based service account more permissions than are strictly necessary (as described later in this article). The Network Service account on the other hand provides an easy set up option and is a good choice from a security perspective given that the account has limited access to the local computer.



So why bother to use a domain-based service account at all? Well, if you have a number of services on your server all running under the context of the Network Service account there is potential for security compromise. In this scenario you may want to consider isolating the services from each other using dedicated service accounts.

What follows is a discussion of the steps required to configure AD LDS to use a domain-based service account.

### 1. Create a user account in AD.

The account doesn't require any specific group memberships. As a service account, you may want to give some thought to the "Password Never Expires" setting, as well as password complexity.

### 2. Permission to create serviceConnectionPoint objects.

The account you have created requires the ability to create Service Connection Point objects in AD. These objects are typically created automatically as child objects of the AD LDS computer object when the service is started.

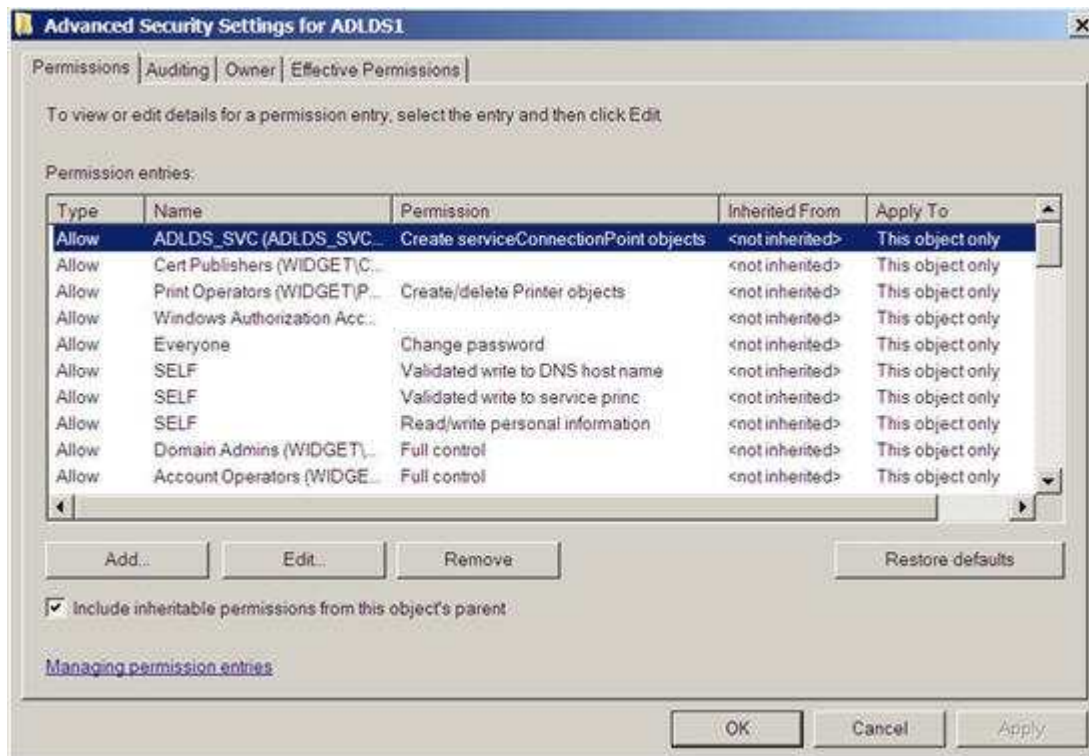
The simplest method is to set the permission using DSACLs. You could alternatively use the security editor from within dsa.msc or adsiedit.msc, but you would first need to edit the `%systemroot%\system32\lssec.dat` file to expose the serviceConnectionPoint object. Here's the syntax using DSACLs:

```
C:\>dsacl <DN_of_AD LDS_server> /G <Domain\User>:CC;"serviceConnectionPoint"
```

e.g.  

```
C:\>dsacl "CN=AD LDS1,OU=Servers,DC=Widget,DC=com" /G MyDom\AD LDS_SVC:CC;"serviceConnectionPoint"
```

The setting should appear similar to that shown in the screenshot below.



### 3. Permission to create servicePrincipalName objects.

Your service account also needs permissions to create Service Principal Name (SPN). The SPNs are generated automatically as attributes of the service account itself in AD when the service is first started. Note that this is different from the behaviour when running the service under the Network Service account. When using Network Service, the SPNs are created as attributes of the AD LDS server's computer object.

To set the permissions, assign the SELF account Read/Write servicePrincipalName. The permissions are applied onto *This object only* on the service account object. Here's an example using DSACLs.

```
C:\>dsacl <DN_of_Service_Account> /G SELF:RPWP;"servicePrincipalName"
```

e.g.

```
C:\>dsacl "CN=AD LDS_SVC,OU=Service Account,DC=Widget,DC=com" /G  
SELF:RPWP;"servicePrincipalName"
```

The screenshot below shows how the permissions should appear.





#### 4. Grant "Log on as a service" user rights

The service account requires Log on as service user rights on the server running the AD LDS instance. You don't normally have to assign this right in advance because you will be prompted when creating the instance using the setup wizard.

If you have to set this right manually, use the Group Policy Editor to edit the local policy, or alternatively use the GPMC to edit an appropriate domain policy. The location of the setting is:

Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment.

The screenshot below shows the setting.



## 5. Membership of the local Administrators group.

At the time of writing, the AD LDS product documentation indicates that the service account is not required to be a member of the local Administrators group on server running the AD LDS instance. However, my experience is that without this, the following error is generated in the event log corresponding to the instance each time the service is re-started.

*Log Name: ADAM (instance1)*

*Source: ADAM [instance1] General*

*Date: 6/04/2009 11:22:08 a.m.*

*Event ID: 1168*

*Task Category: Internal Processing*

*Level: Error*

*Keywords: Classic*

*User: ANONYMOUS LOGON*

*Computer: ADLDS1.widget.com*

*Description:*

*Internal error: An Active Directory Lightweight Directory Services error has occurred.*

*Additional Data*

*Error value (decimal):*

*-1073741790*

*Error value (hex):*

*c0000022*

*Internal ID:*

*3000715*

The fact that the service account requires membership of the local Administrators group makes the choice to use Network Service even more compelling. The Network Service account has a lower level of privilege on the local machine than that of members of the Administrators group. This implies the potential for compromise is lower when using Network Service.

## Conclusion

As you can see, using domain-based service accounts for your AD LDS instances requires a fair amount of extra work during setup. I recommend that you use Network Service unless your circumstances require you to use a domain account.

#### QUESTION 56

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 is configured as an Active Directory Federation Services (AD FS) 2.0 standalone server.

You plan to add a new token-signing certificate to Server1.

You import the certificate to the server as shown in the exhibit. (Click the Exhibit button.)

When you run the Add Token-Signing Certificate wizard, you discover that the new certificate is unavailable.

You need to ensure that you can use the new certificate for AD FS.

What should you do?

**Exhibit:**



- A. From the properties of the certificate, modify the Certificate purposes setting.
- B. From the properties of the certificate, modify the Certificate Policy OIDs setting.
- C. Import the certificate to the local computer personal certificate store.
- D. Import the certificate to the AD FS 2.0 windows Service personal certificate store.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 57

You install a read-only domain controller (RODC) named RODC1.

You need to ensure that a user named User1 can administer RODC1. The solution must minimize the number of permissions assigned to User1.

Which tool should you use?

- A. Active Directory Administrative Center
- B. Active Directory Users and Computers
- C. Dsadd
- D. Dsmgmt

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**The old answer was: Dsmgmt**

There are a couple of ways to achieve this and two of them are mentioned in the listed answers, Active Directory Users and Computers and Dsmgmt.

Referenced below are two Technet articles. The first explains the different ways to implement Administrator Role Separation on an RODC, and why the use of Active Directory Users is recommended over Dsmgmt. The second reference is now a kind of bonus, explaining how to use dsmgmt for this task. (In version 1 of this dump I used it to explain why dsmgmt should be the answer.)

Reference 1:

<http://technet.microsoft.com/en-us/library/cc755310.aspx>

**Delegating local administration of an RODC**

Administrator Role Separation (ARS) is an RODC feature that you can use to delegate the ability to administer an RODC to a user or a security group. When you delegate the ability to log on to an RODC to a user or a security group, the user or group is not added the Domain Admins group and therefore does not have additional rights to perform directory service operations.

**Steps and best practices for setting up ARS**

You can specify a delegated RODC administrator during an RODC installation or after it. To specify the delegated RODC administrator after installation, you can use either of the following options:

Modify the Managed By tab of the RODC account properties in the **Active Directory Users and Computers** snap-in, as shown in the following figure. You can click Change to change which security

principal is the delegated RODC administrator. You can choose only one security principal. Specify a security group rather than an individual user so you can control RODC administration permissions most efficiently. This method changes the managedBy attribute of the computer object that corresponds to the RODC to the SID of the security principal that you specify. This is the recommended way to specify the delegated RODC administrator account because the information is stored in AD DS, where it can be centrally managed by domain administrators.

**RODC1 Properties**

General | Operating System | Member Of | Delegation  
 Password Replication Policy | Location | Managed By | Dial-in

Name:

The [selected group](#) can administer this RODC

Office:

Street:

City:

State/province:

Country/region:

Telephone number:

Fax number:

Use the `ntdsutil` local roles command or the **`dsmgmt`** local roles command. You can use this command to view, add, or remove members from the Administrators group and other built-in groups on the RODC. [See also the second reference for more information on how to use `dsmgmt`.]

**Using `ntdsutil` or `dsmgmt` to specify the delegated RODC administrator account is not recommended** because the information is stored only locally on the RODC. Therefore, when you use `ntdsutil` local roles to delegate an administrator for the RODC, the account that you specify does not appear on the Managed By tab of the RODC account properties. As a result, using the Active Directory Users and Computers snap-in or a similar tool will not reveal that the RODC has a delegated administrator. In addition, if you demote an RODC, any security principal that you specified by using `ntdsutil` local roles remains stored in the registry of the server. This can be a security concern if you demote an RODC in one domain and then promote it to be an RODC again in a different domain. In that case, the original security principal would have administrative rights on the new RODC in the different domain.

Reference 2:

<http://technet.microsoft.com/en-us/library/cc732301.aspx>

### Administrator Role Separation Configuration

This section provides procedures for creating a local administrator role for an RODC and for adding a user to that role.

To configure Administrator Role Separation for an RODC

1. Click Start, click Run, type `cmd`, and then press ENTER.
2. At the command prompt, type **`dsmgmt.exe`**, and then press ENTER.
3. At the DSMGMT prompt, type **`local roles`**, and then press ENTER.
4. For a list of valid parameters, type `?`, and then press ENTER.

By default, no local administrator role is defined on the RODC after AD DS installation. To add the local administrator role, use the Add parameter.

5. Type add <DOMAIN>\<user> <administrative role>  
For example, type add CONTOSO\testuser administrators

#### QUESTION 58

Your network contains an Active Directory forest. The forest contains an Active Directory site for a remote office. The remote site contains a read-only domain controller (RODC).

You need to configure the RODC to store only the passwords of users in the remote site.

What should you do?

- A. Create a Password Settings object (PSO).
- B. Modify the Partial-Attribute-Set attribute of the forest.
- C. Add the user accounts of the remote site users to the Allowed RODC Password Replication Group.
- D. Add the user accounts of users who are not in the remote site to the Denied RODC Password Replication Group.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 59

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

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

You need to limit the display quality of Remote Desktop connections.

What should you do?

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 60

Your network contains a server that has the Remote Desktop Session Host (RD Session Host) role service installed.

You need to increase the bandwidth that is allocated for printing and for file transfers between the RD Session Host server and the Remote Desktop clients.

What should you do?

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Display data prioritization

Display data prioritization automatically controls virtual channel traffic so that display, keyboard, and mouse data is given a higher priority over other virtual channel traffic, such as printing or file transfers. This prioritization is designed to ensure that your screen performance is not adversely affected by bandwidth intensive actions, such as large print jobs. The default bandwidth ratio is 70:30. Display and input data will be allocated 70 percent of the bandwidth, and all other traffic, such as clipboard, file transfers, or print jobs, will be allocated 30 percent of the bandwidth.

You can adjust the display data prioritization settings by making changes to the registry of the terminal server. You can change the value of the following entries under the

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TermDD subkey:

FlowControlDisable

FlowControlDisplayBandwidth

FlowControlChannelBandwidth

FlowControlChargePostCompression

If these entries do not appear, you can add them. To do this, right-click TermDD, point to New, and then click

DWORD (32-bit) Value.

You can disable display data prioritization by setting the value of FlowControlDisable to 1. If display data prioritization is disabled, all requests are handled on a first-in-first-out basis.

The default value for FlowControlDisable is 0.

You can set the relative bandwidth priority for display (and input data) by setting the FlowControlDisplayBandwidth value.

The default value is 70; the maximum value allowed is 255. You can set the relative bandwidth priority for other virtual channels (such as clipboard, file transfers, or print jobs) by setting the FlowControlChannelBandwidth value. The default value is 30; the maximum value allowed is 255. The bandwidth ratio for display data prioritization is based on the values of FlowControlDisplayBandwidth and FlowControlChannelBandwidth. For example, if FlowControlDisplayBandwidth is set to 150 and FlowControlChannelBandwidth is set to 50, the ratio is 150:50, so display and input data will be allocated 75 percent of the bandwidth.

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

**QUESTION 61**

Your network contains an Active Directory domain. The domain contains an enterprise certification authority (CA) named Server1 and a server named Server2.

On Server2, you deploy Network Policy Server (NPS) and you configure a Network Access Protection (NAP) enforcement policy for IPSec.

From the Health Registration Authority snap-in on Server2, you set the lifetime of health certificates to four hours.

You discover that the validity period of the health certificates issued to client computers is one year.

You need to ensure that the health certificates are only valid for four hours.

What should you do?

- A. On Server1, run certutil.exe -setreg policy\editflags + editf\_attributeenddate.
- B. On Server1, run certutil.exe - setreg dbflags +dbflags\_enablevolatilerequests.
- C. Modify the Request Handling settings of the certificate template used for the health certificates.
- D. Modify the Issuance Requirements settings of the certificate template used for the health certificates.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 62**

Your network contains one Active Directory domain. You have a member server named Server1 that runs Windows Server 2008 R2. The server has the Routing and Remote Access Services role service installed.

You implement Network Access Protection (NAP) for the domain.

You need to configure the Point-to-Point Protocol (PPP) authentication method on Server1.

Which authentication method should you use?

- A. Challenge Handshake Authentication Protocol (CHAP)
- B. Extensible Authentication Protocol (EAP)
- C. Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2)
- D. Password Authentication Protocol (PAP)

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 63**

Your company has 10 servers that run Windows Server 2008 R2. The servers have Remote Desktop Protocol (RDP) enabled for server administration. RDP is configured to use default security settings. All administrators' computers run Windows 7.

You need to ensure the RDP connections are as secure as possible.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Set the security layer for each server to the RDP Security Layer.
- B. Configure the firewall on each server to block port 3389.
- C. Acquire user certificates from the internal certification authority.
- D. Configure each server to allow connections only to Remote Desktop client computers that use Network Level Authentication.

**Correct Answer:** CD

**Section:** (none)

**Explanation**



**Explanation/Reference:**

Explanation:

**QUESTION 64**

Your network contains an Active Directory domain named contoso.com. The network has DirectAccess deployed.

You deploy a new server named Server1 that hosts a management application.

You need to ensure that Server1 can initiate connections to DirectAccess client computers.

Which settings should you modify from the DirectAccess Setup console?

- A. Application Servers
- B. DirectAccess Server
- C. Infrastructure Servers
- D. Remote Clients

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Read the guide here:

<http://blog.concurrency.com/infrastructure/uag-directaccess-infrastructure-servers-wizard/>

**QUESTION 65**

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

You have a standalone Network Policy Server (NPS) named NPS1.

You have a VPN server named VPN1. VPN1 is configured as a RADIUS client to NPS1.

You need to ensure that users from both forests can establish VPN connections by using their own domain accounts.

What should you do?

- A. On NPS1, configure remediation server groups.
- B. On NPS1, configure connection request policies.
- C. On VPN1, modify the DNS suffix search order.
- D. On VPN1, modify the IKEv2 Client connection controls.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.

For NAP VPN or 802.1X, you must configure PEAP authentication in connection request policy.

**QUESTION 66**

Your network contains a server named Server1 that runs Windows Server 2008 R2.

Server1 has the Hyper-V server role installed.

Server1 hosts a virtual machine (VM) named VM1.

You take a snapshot of VM1 at 05:00 and at 19:00.

You use Hyper-V Manager to delete the snapshot taken at 05:00.

You need to ensure that the files created by the 05:00 snapshot are deleted from the hard disk on Server1.  
What should you do?

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 67

Your network contains an Active Directory domain.

The domain contains two servers named Server1 and Server2.

You connect Server1 and Server2 to a logical unit number (LUN) on a Storage Area Network (SAN).

You need to ensure that you can use the LUN in a failover cluster.  
What should you do?

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 68

Your network contains an Active Directory domain. The relevant servers in the domain are configured as shown in the following table:

Server name	Operating System	Server role
Server1	Windows 2008	Domain controller
Server2	Windows 2008 R2	Enterprise root certification authority (CA)
Server3	Windows 2008 R2	Network Device Enrollment Service (NDES)

You need to ensure that all device certificate requests use the MD5 hash algorithm.

What should you do?

- A. On Server2, run the Certutil tool.
- B. On Server1, update the CEP Encryption certificate template.
- C. On Server1, update the Exchange Enrollment Agent (Offline Request) template.
- D. On Server3, set the value of the HKLM\Software\Microsoft\Cryptography\MSCEP\HashAlgorithm\HashAlgorithm registry key.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 69

.

Your network contains an Active Directory domain.

You have a server named Server1 that runs Windows Server 2008 R2. Server1 is an enterprise root certification authority (CA).

You have a client computer named Computer1 that runs Windows 7. You enable automatic certificate enrollment for all client computers that run Windows 7. You need to verify that the Windows 7 client computers can automatically enroll for certificates.

Which command should you run on Computer1?

- A. certreq.exe retrieve
- B. certreq.exe submit
- C. certutil.exe getkey
- D. certutil.exe pulse

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 70

.

Your network contains two Active Directory forests named contoso.com and adatum.com. The functional level of both forests is Windows Server 2008 R2. Each forest contains one domain. Active Directory Certificate Services (AD CS) is configured in the contoso.com forest to allow users from both forests to automatically enroll user certificates.

You need to ensure that all users in the adatum.com forest have a user certificate from the contoso.com certification authority (CA).

What should you configure in the adatum.com domain?

- A. From the Default Domain Controllers Policy, modify the Enterprise Trust settings.
- B. From the Default Domain Controllers Policy, modify the Trusted Publishers settings.
- C. From the Default Domain Policy, modify the Certificate Enrollment policy.

D. From the Default Domain Policy, modify the Trusted Root Certification Authority settings.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

## QUESTION 71

You have a server named Server1 that has the following Active Directory Certificate Services (AD CS) role services installed:

- Enterprise root certification authority (CA)
- Certificate Enrollment Web Service
- Certificate Enrollment Policy Web Service

You create a new certificate template.

External users report that the new template is unavailable when they request a new certificate.

You verify that all other templates are available to the external users.

You need to ensure that the external users can request certificates by using the new template.

What should you do on Server1?

- A. Run iisreset.exe /restart.
- B. Run gpupdate.exe /force.
- C. Run certutil.exe dspublish.
- D. Restart the Active Directory Certificate Services service.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

## QUESTION 72

Your network contains an enterprise root certification authority (CA). You need to ensure that a certificate issued by the CA is valid.

What should you do?

- A. Run syskey.exe and use the Update option.
- B. Run sigverif.exe and use the Advanced option.
- C. Run certutil.exe and specify the -verify parameter.
- D. Run certreq.exe and specify the -retrieve parameter.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

certutil.exe -verify - verify certifcate, CRL, or chain

### QUESTION 73

.

You have an enterprise subordinate certification authority (CA). The CA issues smart card logon certificates.

Users are required to log on to the domain by using a smart card. Your company's corporate security policy states that when an employee resigns, his ability to log on to the network must be immediately revoked.

An employee resigns. You need to immediately prevent the employee from logging on to the domain.

What should you do?

- A. Revoke the employee's smart card certificate.
- B. Disable the employee's Active Directory account.
- C. Publish a new delta certificate revocation list (CRL).
- D. Reset the password for the employee's Active Directory account.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

dsmod userUserDN-disabled yes

### QUESTION 74

.

You add an Online Responder to an Online Responder Array. You need to ensure that the new Online Responder resolves synchronization conflicts for all members of the Array.

What should you do?

- A. From Network Load Balancing Manager, set the priority ID of the new Online Responder to 1.
- B. From Network Load Balancing Manager, set the priority ID of the new Online Responder to 32.
- C. From the Online Responder Management Console, select the new Online Responder, and then select Set as Array Controller.
- D. From the Online Responder Management Console, select the new Online Responder, and then select Synchronize Members with Array Controller.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

<http://www.lead2pass.com/70-649.html>

### QUESTION 75

.

Your network contains a server that runs Windows Server 2008 R2. The server is configured as an enterprise root certification authority (CA).

You have a Web site that uses x.509 certificates for authentication. The Web site is configured to use a many-to-one mapping.

You revoke a certificate issued to an external partner. You need to prevent the external partner from accessing

the Web site.

What should you do?

- A. Run certutil.exe -crl.
- B. Run certutil.exe -delkey.
- C. From Active Directory Users and Computers, modify the membership of the IIS\_IUSRS group.
- D. From Active Directory Users and Computers, modify the Contact object for the external partner.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 76**

Your network contains a server named Server1 that has the Hyper-V server role installed.

Server1 hosts a virtual machine (VM) named VM1 that runs Windows Server 2003 Service Pack 2 (SP2). VM1 is configured to use a 127-GB dynamically-expanding virtual hard disk (VHD).

You need to add 500 GB of disk space to VM1. The solution must minimize the amount of downtime for VM1.

What should you do?

- A. Increase the size of the VHD drive.
- B. Add a new VHD drive to an IDE controller.
- C. Convert the VHD to a fixed-size disk.
- D. Add a new VHD drive to a SCSI controller.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

Source:<http://technet.microsoft.com/en-us/library/dd446676.aspx>

#### **QUESTION 77**

You are evaluating whether to purchase Windows Server 2008 R2 Service Pack 1 (SP1).

Several weeks ago, you installed Windows Server 2008 R2 SP1 on a server. During the installation, you did not enter a product key.

You need to identify how many days remain until the license status of the server will change to Unlicensed.

Which tool should you use?

- A. Slmgr.vbs
- B. Action Center

- C. Wevutil.exe
- D. System Configuration

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:  
slmgr.vbs -dli

Display license information.

By default, /dli displays the license information for the installed active Windows edition. Specifying the [Activation ID] parameter displays the license information for the specified edition associated with that Activation ID. Specifying the [All] as the parameter will display all applicable installed products' license information. This operation does not require elevated privileges.

#### **QUESTION 78**

Your network contains two servers named Server1 and Server2 that run Windows Server 2008 R2. Server1 and Server2 have the Hyper server role and the Failover Clustering feature installed.

You deploy a new virtual machine (VM) named VM1 on Server1.

You need to ensure that VM1 is available if one of the Hyper-V servers fails.

What should you do?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 79**

Your network contains a server that runs Windows Server 2008 R2 and has the Hyper-V server role installed.

Virtual machines (VMs) are frequently added to the Hyper-V server.

You need to ensure that a VM named VM1 has priority regarding the allocation of the physical CPU resources on the Hyper-V host.

What should you modify?

- A. The VM reserve of the virtual processor for VM1
- B. The VM limit of the virtual processor for VM1
- C. The number of virtual processors for VM1
- D. The relative weight of the virtual processor for VM1

**Correct Answer:** D

**Section:** (none)

## Explanation

### Explanation/Reference:

Explanation:

The relative weight given to the resource needs of this virtual machine compared to all other virtual machines. A virtual machine with a higher relative weight is dynamically allocated additional resources as needed from other virtual machines that have lower relative weights.

By default, all virtual machines have a relative weight of 100, so that their resource requirements are equal, and none is given preference.

You can assign each virtual machine a relative weight from 1 through 10,000.

In most cases, this is the only setting that you will need to configure.

### QUESTION 80

Your network contains a single Active Directory domain. The domain contains a server named Server1 that runs Windows Server 2008 R2.

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 `mpclaim.exe -l -m 6`.

**Correct Answer: C**

**Section: (none)**

**Explanation**

### Explanation/Reference:

Explanation:

**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 R2 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](http://technet.microsoft.com/en-us/library/ee619734(WS.10).aspx)

#### **QUESTION 81**

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Windows Deployment Services (WDS server role installed).

You need to copy a default Windows 7 image to Server1.

Which type of image should you add?

- A. Boot
- B. Install
- C. Capture
- D. Discover

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 82**

You are configuring a two-node failover cluster. The failover cluster will connect to a storage server that runs Windows Storage Server 2008. The storage server contains a raw disk.

The raw disk appears in the Disk Management console for both nodes.

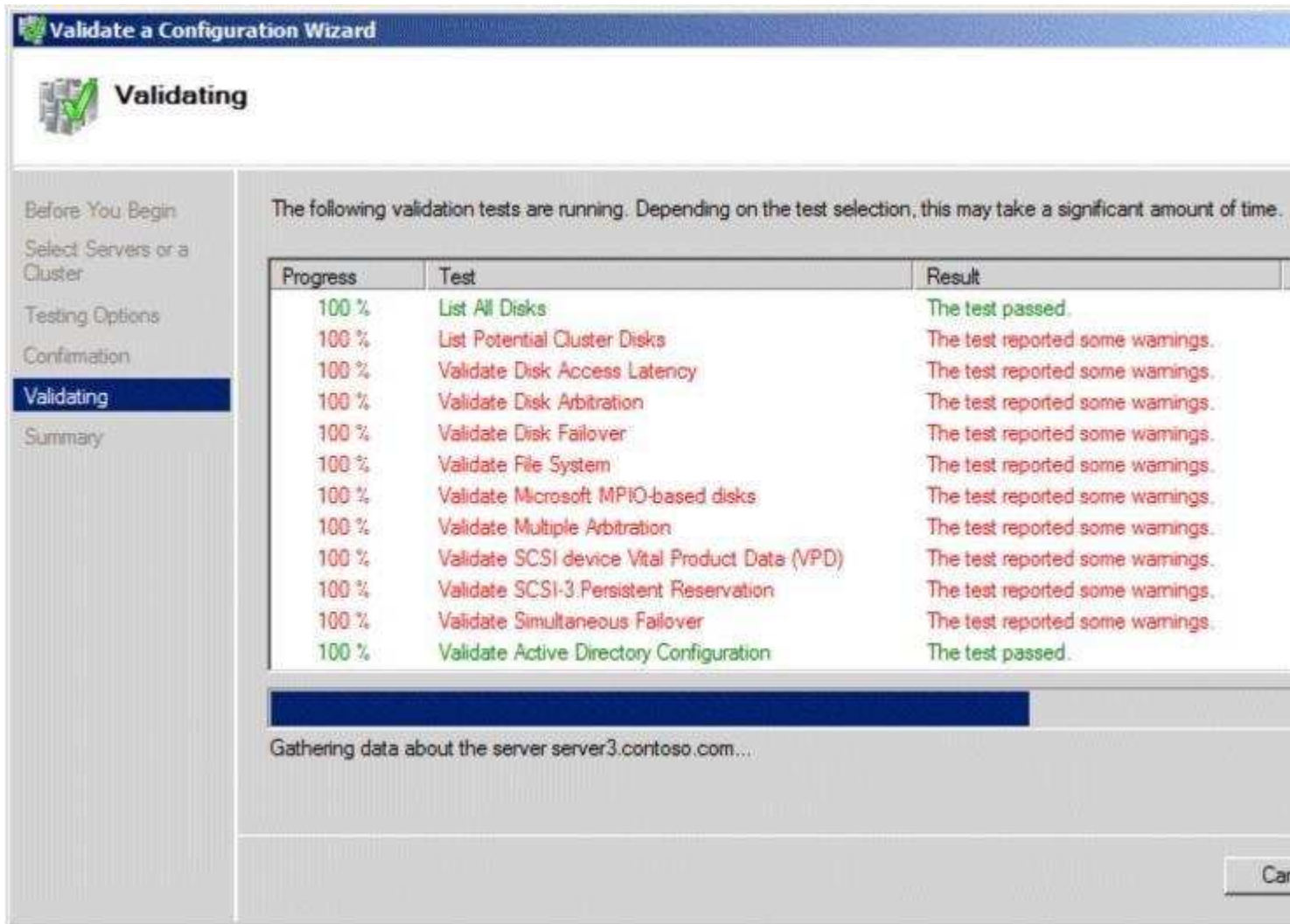
From one of the nodes, you bring the disk online, and then you initialize the disk.

You run the Validate a Configuration Wizard as shown in the exhibit. (Click the Exhibit button.)

You need to ensure that all of the tests pass when you run the Validate a Configuration Wizard.

What should you do?

**Exhibit:**



- A. Convert the disk to a GPT disk, and then create a simple volume.
- B. Create a simple volume, and then convert the disk to a dynamic disk.
- C. Create a simple volume on the disk, and then take the disk offline.
- D. Convert the disk to a dynamic disk, and then take the disk offline.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 83

**Note:** This question is part of a series of question that use the same set of answer choices. Each answer choice may be used once, more than once, or not at all.

You manage a Web server named Server1 that runs Window Server 2008 R2. Server1 hosts five Web sites.

You discover that the CPU utilization of Server1 is abnormally high.

**You need to view the amount of CPU resources that each Web site is using.**



<http://www.gratisexam.com/>

Which tool should you use ?

- A. Component Services
- B. IISreset
- C. Internet Information Services (IIS) Manager
- D. Internet Information Services (IIS) 6.0 Manager
- E. FTP
- F. Local Security Policy
- G. Performance Monitor
- H. Security Configuration wizard (SCW)
- I. Services
- J. System Configuration
- K. Telnet
- L. Windows Firewall

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**The old answer was: Performance Monitor**

Performance Monitor – it is not better tool than IIS Manager, because it provides same functionality as “Worker processes” tab of IIS Manager, but in Performance Monitor you need to configure list of counters before you see their values unlike as in IIS Manager, which displays all application pools and their CPU usage in one click. PS. “Web site” is not equal to “application pool”, and I did not find any possibility to track “web site CPU usage” in Windows Server 2008R2.

#### **QUESTION 84**

**Note: This question is part of a series of questions that use the same set of answer choices. Each answer choice may be used once, more than once, or not at all.**

Your network contains a Web server named Server1 that runs Windows Server 2008 R2.

**You need to ensure that Server1 only processes HTTP URLs that are shorter than 2,048 bytes.**

Which feature should you configure from Internet Information Services (IIS) Manager?

- A. Authentication
- B. Authorization Rules
- C. Connection Strings
- D. Default Document
- E. Error Pages
- F. Feature Delegation
- G. HTTP Redirect
- H. HTTP Response Headers

- I. IIS Manager Permissions
- J. IP Address and Domain Restrictions
- K. ISAPI and CGI Restrictions
- L. ISAPI Filters
- M. Management Service
- N. Request Filtering

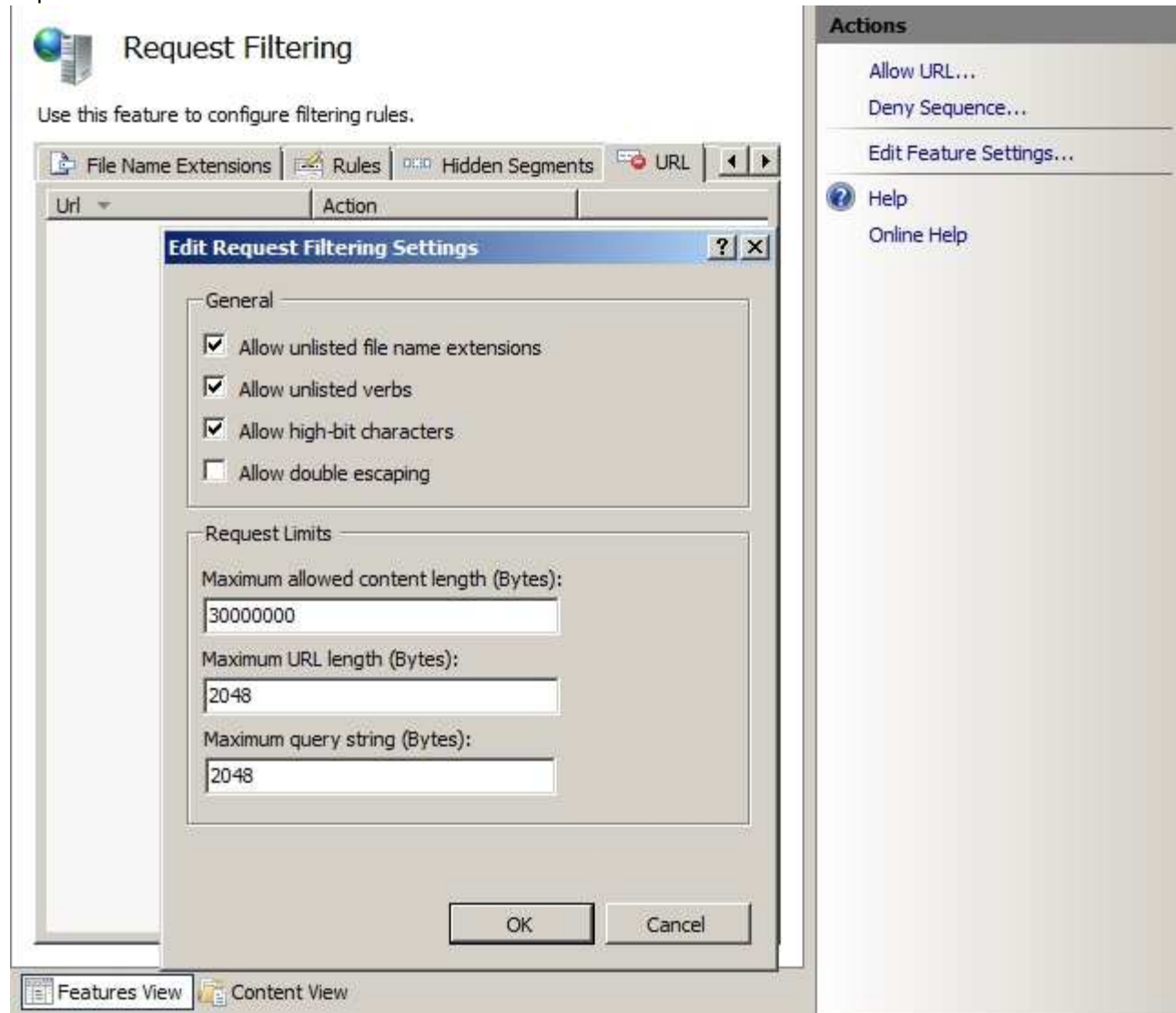
**Correct Answer:** N

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:



#### QUESTION 85

Your network contains an Active Directory domain. The domain contains several VPN servers that run Windows Server 2008 R2.

You need to log the time and the date users establish VPN connections to the network. The log must be stored in a central location.

What should you configure on the VPN servers?

- A. The Windows Accounting accounting provider
- B. The RADIUS Accounting accounting provider
- C. Connection request policies
- D. Health policies

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

RADIUS Accounting is used to record service usages such as connection time and network use, then based on these records the user is billed

## Exam B

### QUESTION 1

Your network contains an Active Directory domain.

You deploy Network Access Protection (NAP).

You need to verify whether VPN clients have antivirus software enabled.

What should you configure?

- A. Connection request policies
- B. Group Policy preferences
- C. System health Validators (SHVs)
- D. Health policies

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 2

Your company is implementing Network Access Protection (NAP) with DHCP enforcement.

You need to define which network resources non-compliant client computers can access.

What should you configure?

- A. System health validators (SHVs)
- B. Connection request policies
- C. Health policies
- D. Remediation server groups

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Remediation server groups are used to specify servers that are available to noncompliant Network Access Protection (NAP) clients for the purpose of remediating their health state to comply with health requirements. The type of remediation servers that are required depend on your health requirements and network access methods.

<http://technet.microsoft.com/en-us/library/dd759158.aspx>

### QUESTION 3

Your company has a main office and five branch offices. The branch offices connect to the main office by using a WAN link.

Each branch office has 100 client computers that run Windows XP or Windows Vista. All servers run Windows Server 2008 R2.

The main office has a Windows Server Update Services (WSUS) server.

You need to minimize the amount of WAN traffic used to download updates from the WSUS server.

What should you do?

- A. From a Group Policy, enable Allow BITS Peercaching.
- B. From Windows Explorer, enable Offline Files.
- C. From a Group Policy, enable the Set BranchCache Hosted Cache mode setting.
- D. From a Group Policy, enable the Set BranchCache Distributed Cache mode setting.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Windows Update and Microsoft Update use the Background Intelligent Transfer Service (BITS) to download updates. You can optimize download performance by configuring BITS through Group Policy.

Peer caching is a feature of BITS that enables peer computers to share files. Peer computers are computers that have the peer caching feature enabled and that are located in the same subnet. If peer caching is enabled on a computer, Automatic Updates instructs BITS to make downloaded files available to the computer's peers. When updates are downloaded, BITS caches them. When another peer caching-enabled computer tries to download the same update, BITS sends a multicast request to all peers. If peer computers respond to the request, BITS downloads the file from the first peer computer to respond. If the download from the peer computer fails or takes too long, BITS continues the download from the WSUS server or from Microsoft Update.

Peer caching can optimize bandwidth in the following ways:

- Decreases the data that is transferred from the WSUS server to client computers because computers in the same subnet will usually download the updates from each other.
- Decreases the data that is transferred across the WAN when some or all of the client computers of a WSUS server are located in different locations.
- Decreases the data that is transferred across the Internet if WSUS client computers that are located in the same subnet are configured to download updates from Microsoft Update. [http://technet.microsoft.com/en-us/library/dd939927\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd939927(v=ws.10).aspx)

#### **QUESTION 4**

Your network contains a file server named Server1 that runs Windows Server 2008 R2.

You enable IPsec on Server1.

You need to identify which client computers have active IPsec associations to Server1.

Which administrative tool should you use to achieve this task?

- A. Windows Firewall with Advanced Security
- B. Performance Monitor
- C. Event Viewer
- D. Share and Storage Management

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 5**

Your network contains a DNS server named DN51 that runs Windows Server 2008 R2.

You need to be notified by e-mail if the DNS service logs errors or warnings. The solution must minimize the number of e-mail notifications you receive.

<http://www.lead2pass.com/70-649.html>

What should you do?

- A. Select the DNS Server log from Event Viewer and attach a task to the log.
- B. Run the Configure a DNS Server Wizard.
- C. Create a custom view from Event Viewer and attach a task to the custom view.
- D. Create an alert in Performance Monitor.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

The question states: The solution must minimize the number of e-mail notifications you receive.

If you would do answer A (select the DNS server log and attach a task to the log) you would be flooded with e-mails from 'Information' events etc.

**Filter Current Custom View**

Filter XML

Logged: Any time

Event level: ☐ Critical ☒ Warning ☐ Verbose ☒ Error ☐ Information

☒ By log Event logs: DNS Server

☐ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Clear

OK Cancel



**QUESTION 6**

Your company has a server named DC1 that runs Windows Server 2008 R2. Server1 has the DHCP Server server role installed.

You find that a desktop computer named Computer1 is unable to obtain an IP configuration from the DHCP server.

You install the Microsoft Network Monitor 3.0 application on Server1. You enable P-mode in the Network Monitor application configuration. You plan to capture only the DHCP server-related traffic between Server1 and Computer1.

The network interface configuration for the two computers is shown in the following table.

	Server1	Computer1
IP address	192.168.2.1	169.254.15.84
MAC address	00-0A-5E-1C-7F-67	00-17-31-D5-5E-FF

You need to build a filter in the Network Monitor application to capture the DHCP traffic between Server1 and Computer1.

Which filter should you use?

- A. IPv4.Address == 169.254.15.84 && DHCP
- B. IPv4.Address == 192.168.2.1 && DHCP
- C. Ethernet.Address == 0x000A5E1C7F67 && DHCP
- D. Ethernet.Address == 0x001731D55EFF &&. DHCP

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 7**

You create a Data Collector Set (DCS).

You need prevent the DCS from logging data if the server has less than 1 GB of available disk space.

What should you do?

- A. Modify the Stop Conditions settings of the DCS.
- B. Create a passive file screen.
- C. Create an active file screen.
- D. Modify the Data Manager settings of the DCS.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

The screenshot shows the 'Data Manager' tab in the WSUS console. It contains several settings for managing update data:

- Minimum free disk:** 200 MB
- Maximum folders:** 100
- Resource policy:** Delete largest
- Apply policy before the data collector set starts:** Checked
- Maximum root path size:** 1024 MB
- Report file name:** report.html
- Event file name:** (empty)
- Enable data management and report generation:** Checked

At the bottom, there are buttons for OK, Cancel, Apply, and Help.

### QUESTION 8

Your network contains a Windows Server Update Services (WSUS) server named Server1. Server1 provides updates to client computers in two sites named Site1 and Site2.

A WSUS computer group named Group1 is configured for automatic approval.

You need to ensure that new client computers in Site2 are automatically added to Group1.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Configure a Group Policy object (GPO) that enables client-side targeting.
- B. Modify the Computers Options in the Update Services console.
- C. Create a new automatic approval update rule.
- D. Modify the Automatic Approvals options in the Update Services console.

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Reference: [http://technet.microsoft.com/en-us/library/cc720433\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc720433(WS.10).aspx)

Explanation:

WSUS enables you to target updates to groups of client computers. This capability can help you ensure that specific computers get the right updates at the most convenient times on an ongoing basis. For example, if all computers in one department of your organization have a specific configuration (such as all computers in the

Accounting team), you can determine what updates those computers get, at what time, and then use WSUS reporting features to evaluate the success of update activity for that computer group.

By default, each computer is already assigned to the All Computers group. Computers will also be assigned to the Unassigned Computers group until you assign them to another group.

Regardless of the group you assign a computer to, it will also remain in the All Computers group. A computer can be in only one other group in addition to the All Computers group.

You can assign computers to computer groups by using one of two methods, server-side targeting or client side targeting, depending on whether or not you want to automate the process. With server-side targeting, you use the Move the selected computer task on the Computers page to move one or more client computers to one computer group at a time. With client-side targeting, you use Group Policy or edit the registry settings on client computers to enable those computers to automatically add themselves into the computer groups. You must specify which method you will use by selecting one of the two options on the Computers Options page.

#### Note

If your WSUS server is running in replica mode, you will not be able to create computer groups on that server, you will only inherit the computer groups created on the administration server from which your server inherits its settings. For more information about replica mode, see [Running in Replica Mode](#).

**Server-side Targeting** With server-side targeting, you use the WSUS console to both create groups and then assign computers to the groups. Server-side targeting is an excellent option if you do not have many client computers to update and you want to move client computers into computer groups manually.

To enable server-side targeting on your WSUS server, click the Use the Move computers task in Windows Server Update Services option on the Computers Options page.

**Client-side Targeting** With client-side targeting, you enable client-computers to add themselves to the computer groups you create in the WSUS console. You can enable client-side targeting through Group Policy (in an Active Directory network environment) or by editing registry entries (in a non-Active Directory network environment) for the client computers. When the client computers connect to the WSUS server, they will add themselves into the correct computer group. Client-side targeting is an excellent option if you have many client computers and want to automate the process of assigning them to computer groups. To enable client-side targeting on your WSUS server, click the Use Group Policy or registry settings on client computers option on the Computers Options page.

## QUESTION 9

Your network contains a server that runs Windows Server 2008 R2 Standard. The server is

configured to native boot from a virtual hard disk (VHD). All hard disks on the server are configured as basic disks that use an MBR.

A new corporate security policy states that all of the hard disks on the server must use Windows BitLocker Drive Encryption (BitLocker).

You need to ensure that the server meets the corporate security policy.

What should you do first?

- A. Convert the disks to dynamic disks.
- B. Upgrade the server to Windows Server 2008 R2 Enterprise.
- C. Back up the server and restore the server to a physical volume.
- D. Configure the disks to use a GPT.

**Correct Answer: C**

**Section: (none)**

## **Explanation**

### **Explanation/Reference:**

Explanation:

Applies To: Windows 7, Windows Server 2008 R2

Configuring native VHD boot if the host volume is protected by BitLocker. You can save a VHD file on a file system that is protected by BitLockerTM, but you cannot use the VHD for native boot or enable Bitlocker on the volume(s) that are contained inside a VHD.

Source: [http://technet.microsoft.com/en-us/library/dd440865\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd440865(WS.10).aspx)

### **QUESTION 10**

Your network contains a Windows Server 2003 server cluster named Cluster1. Cluster1 hosts a print server instance named Print1.

You deploy a Windows Server 2008 R2 failover cluster named Cluster2.

You configure Cluster2 to use the physical disk resource used by Print1.

From Cluster2, you run the Migrate a Cluster Wizard to migrate Print1 to Cluster2.

You need to ensure that Print1 runs on Cluster2.

What should you do first?

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

**Correct Answer: B**

**Section: (none)**

### **Explanation**

### **Explanation/Reference:**

Explanation:

### **QUESTION 11**

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

You publish a RemoteApp named Webapp1. The Remote Desktop Connection (.rdp) file for Webapp1 is unsigned.

When a user named User1 runs Webapp1 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 Webapp1.**

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**

## Section: (none)

### Explanation

#### Explanation/Reference:

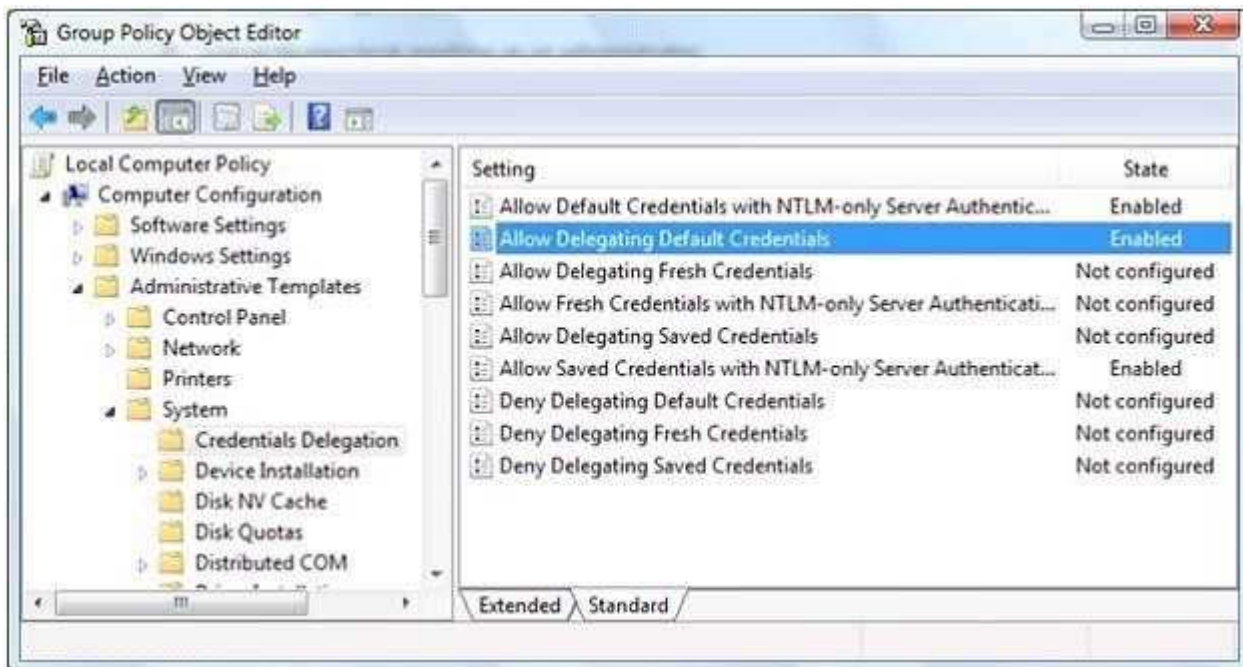
Explanation:

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.

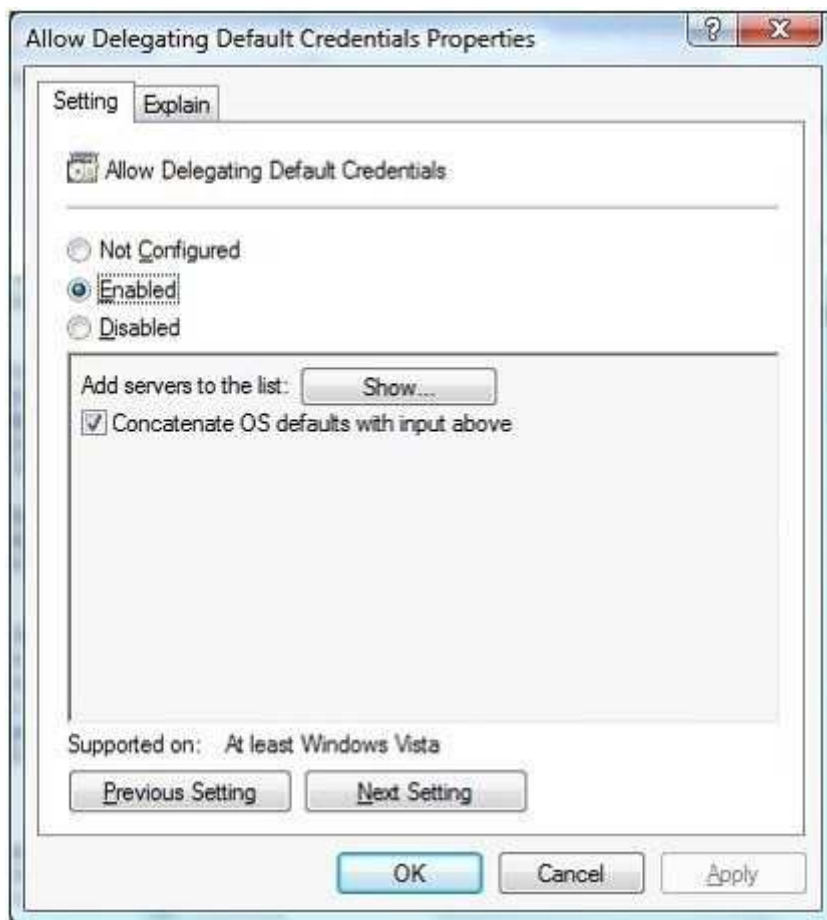
How to enable Single Sign-On?

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

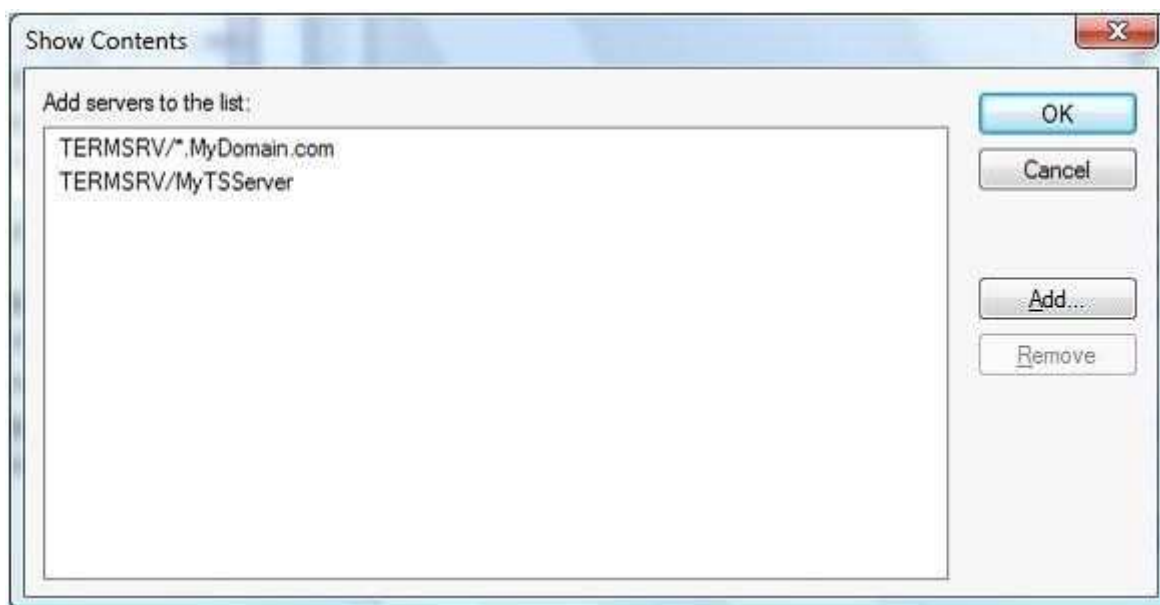
1. Log on to your local machine as an administrator.
2. Start Group Policy Editor - "gpedit.msc".
3. Navigate to "Computer Configuration\Administrative Templates\System\Credentials Delegation".



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/<Your server name>" 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>

#### **QUESTION 12**

Your company has an Active Directory domain. The company has a server named Server1 that has the Remote Desktop Services server role and the RD Web Access role service installed. The company has a server named Server2 that runs ISA Server 2006.

The company deploys the Remote Desktop Gateway (RD Gateway) role on a new server named Server3. The company wants to use ISA as the SSL endpoint for Remote Desktop connections.

You need to configure the RD Gateway role on Server3 to use ISA 2006 on Server2.

What should you do?

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

#### **Explanation/Reference:**

Explanation:

To enhance security for an RD Gateway server, you can configure Microsoft Internet Security and Acceleration (ISA) Server or a non-Microsoft product to function as a Secure Sockets Layer (SSL) bridging device. The SSL bridging device can enhance security by terminating SSL sessions, inspecting packets, and re-establishing SSL sessions. You can configure ISA Server communication with the RD Gateway server in either of the two following ways:

**HTTPS-HTTPS bridging.**In this configuration, the RD Gateway client initiates an SSL (HTTPS) request to the SSL bridging device. The SSL bridging device initiates a new HTTPS request to the RD Gateway server, for maximum security.

**HTTPS-HTTP bridging.**In this configuration, the RD Gateway client initiates an SSL (HTTPS) request to the SSL bridging device. The SSL bridging device initiates a new HTTP request to the RD Gateway server. To use HTTPS-HTTPS or HTTPS-HTTP bridging, you must enable the `Use SSL Bridging` setting on the RD Gateway server.

Source: <http://technet.microsoft.com/en-us/library/cc772387.aspx>

#### **QUESTION 13**

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

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

On Server1, you configure a virtual desktop pool named Pool1. Pool1 contains a Windows 7 virtual machine (VM) named Computer1.

You need to ensure that when a user logs off of Computer1, all of the changes made to Computer1 are discarded.

What should you do?

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

To enable rollback on a virtual machine

1. Log on to RD Virtualization Host using an Administrator account.
2. Open Hyper-V Manager. To open Hyper-V Manager, clickStart, point toAdministrative Tools, and then clickHyper-V Manager.
3. UnderVirtual Machines, right-click the virtual machine to enable rollback, and then click Snapshot.
4. UnderSnapshots, right-click the snapshot of the virtual machine, and then clickRename.
5. TypeRDV\_Rollbackand then press ENTER.
6. Close Hyper-V Manager.
7. Repeat these steps for each virtual machine.

Source:[http://technet.microsoft.com/en-us/library/ff710411\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ff710411(WS.10).aspx)

#### QUESTION 14

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

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



You install 100 Remote Desktop Services Per User client access licenses (RDS Per User CALs) on Server1.  
<http://www.lead2pass.com/70-649.html>

You discover that when users connect to Remote Desktop Services (RDS) on Server2, they receive temporary licenses.

You need to ensure that users receive permanent licenses when they connect to Server2.

What should you do?

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

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

Source: <http://technet.microsoft.com/en-us/library/cc732416.aspx>

## **QUESTION 15**

Your company has an Active Directory domain. The company runs Remote Desktop services.

Standard Users who connect to the Remote Desktop Sessions Host Server are in an organizational unit (OU) named OU1. Administrative users are in OU1. No other users connect to the Remote Desktop Session Host Server.

**You need to ensure that only members of OU1 can run Remote Desktop Protocol files.**

What should you do?

- A. Create a Group Policy object (GPO) that configures the Allow .rdp files from valid publishers and user's default .rdp settings policy setting in the Remote Desktop Client Connection template to **Enabled**. Apply the GPO to OU1.
- B. Create a Group Policy object (GPO) that configures the Specify SHA1 thumbprints of certificates represting trusted .rdp publishers policy setting in the Remote Desktop Client Connection template to **Enabled**. apply the GPO to OU1.
- C. Create a Group Policy object (GPO) that configures the Allow .rdp files from unknown publishers policy setting in the Remote Desktop Client Connection template to **Disabled**. Apply the GPO to OU1.
- D. Create a Group Policy object (GPO) that configures the Allow .rdp files from valid publishers and user's default .rdp settings policy setting in the Remote Desktop Client Connection template to **Disabled**. Apply the GPO to OU1.

**Correct Answer: B**

**Section: (none)****Explanation****Explanation/Reference:****Explanation:**

To ensure that only members of the TermSerAdmin OU can run the Remote Desktop Protocol files, you need to enable the Allow .rdp files from valid publishers and users default .rdp settings policy setting in the Remote Desktop Client Connection template.

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

If you enable this policy setting, users can run .rdp files that are signed with a valid certificate. Users can also start an RDP session with default .rdp settings by directly opening the RDC client. When a user starts an RDP session, the user is asked to confirm whether they want to connect.

If you disable this policy setting, users cannot run .rdp files that are signed with a valid certificate. Additionally, users cannot start an RDP session by directly opening the RDC client and specifying the remote computer name. When a user tries to start an RDP session, the user receives a message that the publisher has been blocked.

Reference: Remote Desktop Connection Client

<http://technet2.microsoft.com/windowsserver2008/en/library/76fb7e12-b823-429b-9887-05dc70d28d0c1033.mspx?mfr=true>

other ref:

Using Group Policy settings to control client behavior when opening a digitally signed .rdp file

You can use Group Policy settings to configure clients to always trust RemoteApp programs from a particular publisher. You can also configure whether clients will block RemoteApp programs and remote desktop connections from external or unknown sources. By using these policy settings, you can reduce the number and complexity of security decisions that users face. This reduces the chances of inadvertent user actions that may lead to security vulnerabilities.

The relevant Group Policy settings are located in the Local Group Policy Editor at the following location, in the Computer Configuration node and in the User Configuration node:

Administrative Templates\Windows Components\Terminal Services\Remote Desktop Connection Client

The available policy settings include the following:

Specify SHA1 thumbprints of certificates representing trusted .rdp publishers

This policy setting allows you to specify a list of Secure Hash Algorithm 1 (SHA1) certificate thumbprints that represent trusted .rdp file publishers. If you enable this policy setting, any certificate with a SHA1 thumbprint that matches a thumbprint on the list is trusted.

Allow .rdp files from valid publishers and user's default .rdp settings

This policy setting allows you to specify whether users can run .rdp files from a publisher that signed the file with a valid certificate. This policy setting also controls whether the user can start an RDP session by using default .rdp settings, such as when a user directly opens the RDC client without specifying an .rdp file.

Allow .rdp files from unknown publishers

This policy setting allows you to specify whether users can run unsigned .rdp files and .rdp files from unknown publishers on the client computer.

**QUESTION 16**

Your network consists of a single Active Directory domain. The network contains a Remote Desktop Session Host Server that runs Windows Server 2008 R2, and client computers that run Windows 7. All computers are members of the domain.

You deploy an application by using the RemoteApp Manager. The Remote Desktop Session Host Server's security layer is set to Negotiate.

You need to ensure that domain users are not prompted for credentials when they access the application.

What should you do?

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

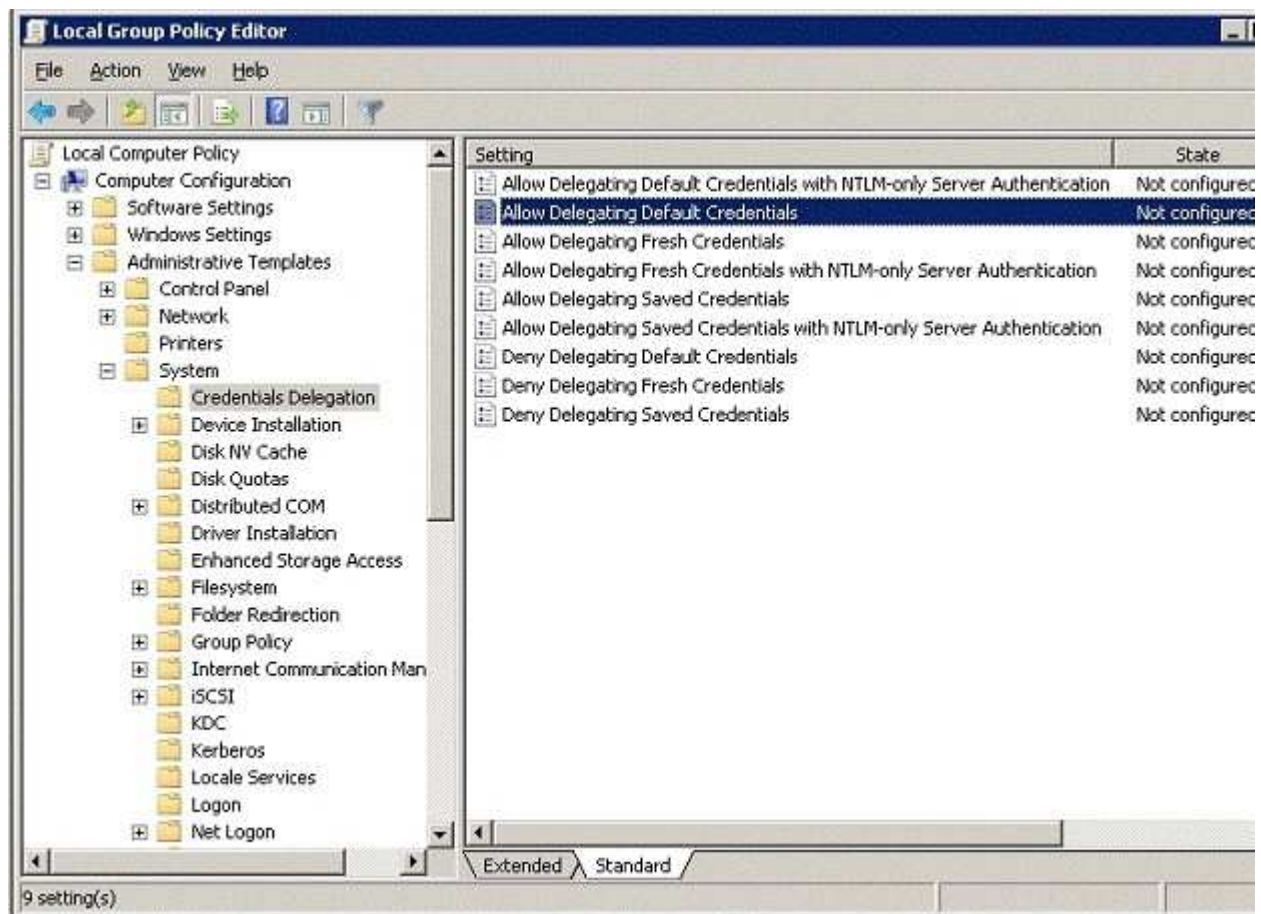
Explanation:

Configuration

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

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

One needs to enable the policy on the client computers, because one want to allow the client computer to reuse the credentials.



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

**Allow Delegating Default Credentials**

☐ Not Configured    Comment:

☒ Enabled

☐ Disabled

Supported on:

Options:

Add servers to the list:

☒ Concatenate OS defaults with input above

Help:

This policy setting applies to applications using the Cred SSP component (for example: Terminal Server).

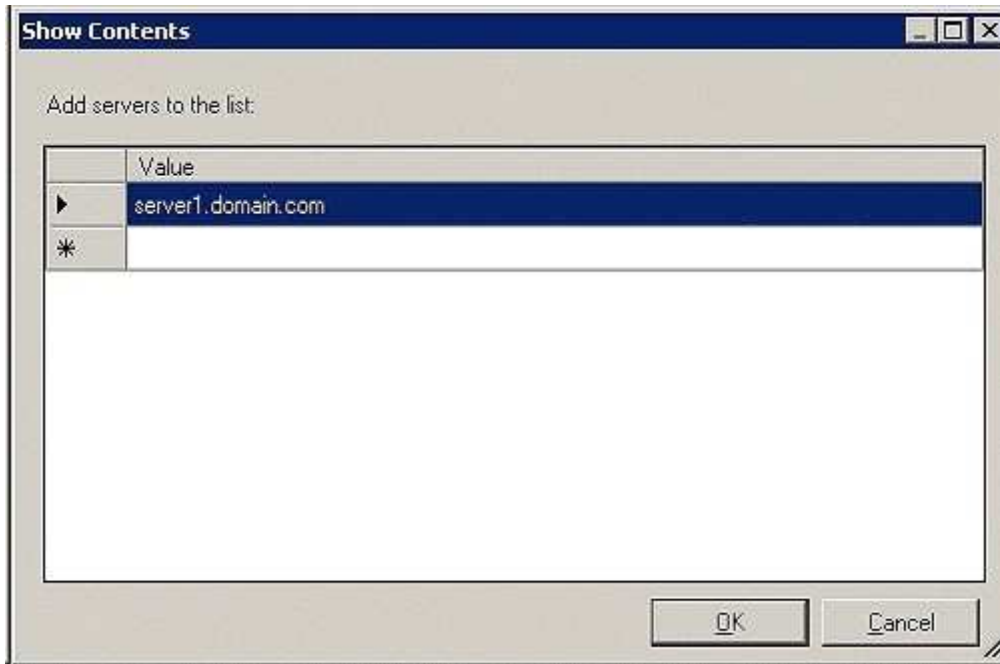
This policy applies when server authentication was achieved via a trusted X509 certificate or Kerberos.

If you enable this policy setting you can specify the servers to which the user's default credentials can be delegated (default credentials are those that you use when first logging on to Windows).

If you disable or do not configure (by default) this policy setting, delegation of default credentials is not permitted to any machine.

Note: The "Allow Delegating Default Credentials" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN.

For Example:  
TERMSRV/host.humanresources.fabrikam.com Terminal server



Add all servers who are trusted for Credential Delegation.

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

#### QUESTION 17

Your network contains a server that has the Remote Desktop Session Host (RD Session Host) role service installed.

You need to ensure that the Remote Desktop sessions of administrators are more responsive than other sessions when the server is under a heavy load.

What should you do?

- A. From the RDP-Tcp properties, modify the Sessions settings.
- B. Install and configure the RD Session Broker role service.
- C. From the RDP-Tcp properties, modify the Client Settings.
- D. Install and configure Windows System Resource Manager (WSRM).

**Correct Answer: D**

**Section: (none)**

**Explanation**

#### Explanation/Reference:

Explanation:

Manage system resources (processor and memory) with pre configured policies, or create custom policies that allocate resources per process, per user, per Remote Desktop Services session, or per Internet Information Services (IIS) application pool.

When the Weighted Remote Sessions resource allocation policy is managing the system, the processes are grouped according to the priority assigned with the user account.

For example, if three users are remotely connected, the user assigned Premium priority will receive highest priority access to the CPU, the user assigned Standard priority will receive second priority to the CPU, and the user assigned Basic priority will receive lowest priority to the CPU.

This policy is for use with RD Session Host servers.

**QUESTION 18**

A corporate network includes two servers named File1 and File2 that run Windows Server 2008 R2.

You need to ensure that a specific user can schedule Data Collector Sets (DCSs) on File2. The solution must minimize the number of rights assigned to the user.

What should you do?

- A. Add the user to the Performance Monitor Users group on File2.
- B. Assign the Profile single process user right to the user on File2.
- C. Add the user to the Performance Log Users group on File2.
- D. Assign the Bypass traverse checking user right to the user on File2.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 19**

Your network contains a server that has the SNMP Service installed.

You need to configure the SNMP security settings on the server.

Which tool should you use?

- A. Services console
- B. Secedit
- C. Scw
- D. Local Security Policy

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 20**

Your network contains 200 servers that run Windows Server 2008 R2.

You need to archive the Security log for each server on a daily basis.

Which tool should you use?

- A. Secedit
- B. Netsh
- C. Wecutil
- D. Wevtutil

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Enables you to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, to run queries, and to export, archive, and clear logs  
wevtutil al <FileName.evtx> [/l:<LocaleString>]

[http://technet.microsoft.com/en-us/library/cc732848\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc732848(v=ws.10).aspx)

<http://technet.microsoft.com/en-us/library/cc749339.aspx>

#### **QUESTION 21**

Your network contains a server named Server1.

An administrator named Admin1 installs the Windows Server Update Services (WSUS) server role on Server1.

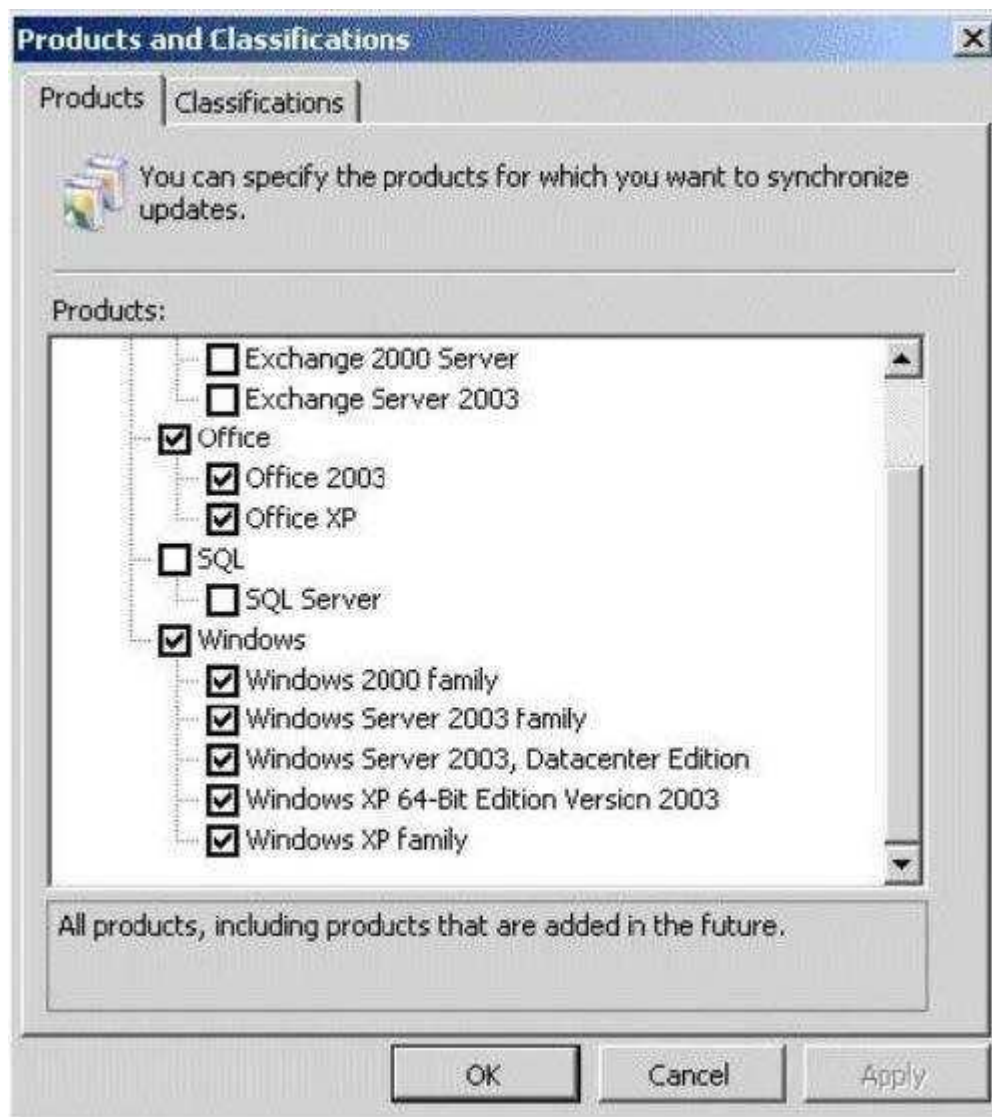
You open the Windows Server Update Services console and view the Products and Classifications options as shown in the exhibit. (Click the Exhibit button.)

You need to ensure that you can select updates for Windows Server 2008 R2 Service Pack 1 (SP1) from the Products and Classifications options.

What should you do?

**Exhibit:**





- A. From the Service console, restart the Update Services service.
- B. From the WSUS Administration console, synchronize Server1.
- C. From a command prompt, run `gupdate /force`.
- D. From a command prompt, run `wuauctl /detectnow`.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Synchronization involves the WSUS server contacting Microsoft Update.

After making contact, WSUS determines whether any new updates have been made available since the last time you synchronized.

Because this is the first time you are synchronizing the WSUS server, all of the updates are available and are ready for your approval for installation.

The initial synchronization may take a fairly long time.

**QUESTION 22**

You perform a security audit of a server named CRM1. You want to build a list of all DNS requests that are

initiated by the server.

You install the Microsoft Network Monitor 3.0 application on CRM1. You capture all local traffic on CRM1 for 24 hours. You save the capture file as data.cap. You find that the size of the file is more than 1 GB.

You need to create a file named DNSdata.cap from the existing capture file that contains only DNS-related data.

What should you do?

- A. Add a new alias named DNS to the aliases table and save the file as DNSdata.cap.
- B. Apply the capture filter DNS and save the displayed frames as a DNSdata.cap file.
- C. Run the nmcap.exe /inputcapture data.cap /capture DNS /file DNSdata.cap command.
- D. Apply the display filter !DNS and save the displayed frames as a DNSdata.cap file.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Below is a sample i created :

```
C:\Users\Administrator\Documents\Network Monitor 3\Captures>nmcap.exe /inputcapture data.cap /capture  
DNS /file dnsdata.cap
```

```
Network Monitor Command Line Capture (nmcap) 3.4.2350.0 Loading Parsers ... [INFO] sparser.npb:001.000
```

```
Successfully unserialized NPL parser 'C:\ProgramData\Microsoft\Network Monitor 3\NPL\NetworkMonitor
```

```
Parsers\Profiles\64BAA24A-0AAD-44 e6-9846- 3BE43D698FF6\sparser.npb. (0x83008006)
```

```
Saving info to: C:\Users\Administrator\Documents\Network Monitor 3\Captures\dnsdata. cap - using circular  
buffer of size 20.00 MB.
```

```
ATTENTION: Conversations Enabled: consumes more memory (see Help for details) Note:
```

```
Process Filtering Enabled.
```

```
Exit by Ctrl+C
```

```
Processing | Received: 4045 Saved: 23 | Time: 0 seconds.
```

```
Closing generated capture files ...
```

```
Completed | Received: 4045 Saved: 23 | Time: 0 seconds.
```

```
C:\Users\Administrator\Documents\Network Monitor 3\Captures>'\' is not recognized as an internal or external  
command, operable program or batch file.
```

### QUESTION 23

Your network contains a server named Server1 that runs Windows Server 2008 R2.

You need to ensure that you can log performance counter data from Server1 to a SQL database.

Which tool should you use?

- A. Data Sources (ODBC)
- B. Storage Explorer
- C. Share and Storage Management
- D. Component Services

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 24

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Routing and Remote Access service (RRAS) role service installed.

You need to view all inbound VPN packets. The solution must minimize the amount of data collected.

What should you do?

- A. At the command prompt, run netsh.exe ras set tracing rasauth enabled.
- B. From Network Monitor, create a capture filter.
- C. From the Registry Editor, configure file tracing for RRAS.
- D. From RRAS, create an inbound packet filter.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 25**

Your network contains an Active Directory forest. The functional level of the forest is Windows Server 2008 R2.

You plan to deploy DirectAccess.

You need to configure the DNS servers on your network to support DirectAccess.

What should you do?

- A. Modify the EnableGlobalNamesSupport registry key and restart the DNS Server service.
- B. Create a trust anchor that uses a certificate issued by a publicly trusted certification authority (CA).
- C. Modify the GlobalQueryBlockList registry key and restart the DNS Server service.
- D. Create a trust anchor that uses a certificate issued by an internal certification authority (CA).

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

To remove ISATAP from the DNS global query block list

1. Click Start, click All Programs, click Accessories, rightclick Command Prompt, and then click Run as administrator.

2. In the Command Prompt window, type dnscmd /config / globalqueryblocklist wpad, and then press ENTER.

3. Close the Command Prompt window.

OR

To remove ISATAP from the DNS global query block list on a DNS server 1- Click Start, type regedit.exe, and then press ENTER.

2- In the console tree, open

Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DNS \Parameters.

3- In the contents pane, double-click the GlobalQueryBlockList value. 4- In the Edit Multi-String dialog box, remove the name ISATAP from the list, and then click OK.

5- Start a command prompt as an administrator.

6- In the Command Prompt window, run the following commands:

net stop dns

net start dns

[http://technet.microsoft.com/en-us/library/ee649158\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/ee649158(v=ws.10).aspx)

#### **QUESTION 26**

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

A partner organization has an Active Directory domain named fabrikam.com.

Your company plans to provide VPN access for fabrikam.com users.

You need to configure Network Policy Server (NPS) to forward authentication requests to fabrikam.com.

What should you configure on the NPS server?

- A. Health policies
- B. Connection request policies
- C. System health validators (SHVs)
- D. Remediation server groups

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Connection request policies are sets of conditions and settings that allow network administrators to designate which Remote Authentication Dial-In User Service (RADIUS) servers perform the authentication and authorization of connection requests that the server running Network Policy Server (NPS) receives from RADIUS clients. Connection request policies can be configured to designate which RADIUS servers are used for RADIUS accounting.

Ref:<http://technet.microsoft.com/en-us/library/cc753603.aspx>

#### **QUESTION 27**

Your network contains an Active Directory domain named contoso.com. Contoso.com contains three servers.

The servers are configured as shown in the following table.

Server name	Server operating system	Server role
DC1	Windows Server 2003 Service Pack 2 (SP2)	Domain controller DNS server
Server1	Windows Server 2003 Service Pack 2 (SP2)	Certificate services
Server2	Windows Server 2008	File server
Server3	Windows Server 2008 R2	None

You plan to give users access to the file shares on Server2 by using DirectAccess.

You need to ensure that you can deploy DirectAccess on Server3.

What should you do?

- A. Upgrade DC1 to Windows Server 2008 R2.
- B. Add a static IPv6 address to DC1.
- C. Add a static IPv6 address to Server2.
- D. Upgrade Server2 to Windows Server 2008 R2.

**Correct Answer: A**

**Section: (none)****Explanation****Explanation/Reference:**

Explanation:

DirectAccess requires the following:

One or more DirectAccess servers running Windows Server 2008 R2 (with or without UAG) with two network adapters: one that is connected directly to the Internet and one that is connected to the intranet. DirectAccess servers must be a member of an AD DS domain.

On the DirectAccess server, at least two consecutive, public IPv4 addresses assigned to the network adapter that is connected to the Internet.

DirectAccess client computers that are running Windows 7 Enterprise or Windows 7 Ultimate. DirectAccess clients must be members of an AD DS domain.

At least one domain controller and DNS server that is running Windows Server 2008 SP2 or Windows Server 2008 R2. When UAG is used, DirectAccess can be deployed with DNS servers and domain controllers that are running Windows Server 2003 when NAT64 functionality is enabled.

A public key infrastructure (PKI) to issue computer certificates, and optionally, smart card certificates for smart card authentication and health certificates for NAP. For more information, see Public Key Infrastructure on the Microsoft Web site.

Without UAG, an optional NAT64 device to provide access to IPv4-only resources for DirectAccess clients. DirectAccess with UAG provides a built-in NAT64.

[http://technet.microsoft.com/en-us/library/ee344835\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/ee344835(v=ws.10).aspx)

**QUESTION 28**

Your network contains a Network Policy Server (NPS) named Server1. You need to configure a network policy for a VLAN.

Which RADIUS attributes should you add?

- A. ·Login-LAT-Service  
·Login-LAT-Node  
·Login-LAT-Group  
·NAS-Identifier
- B. ·Tunnel-Assignment-ID  
·Tunnel-Preference  
·Tunnel-Client-Auth-ID  
·NAS-Port-Id
- C. ·Tunnel-Client-Endpt  
·Tunnel-Server-Endpt  
·NAS-Port-Type  
·Tunnel-Password
- D. ·Tunnel-Medium-Type  
·Tunnel-Pvt-Group-ID  
·Tunnel-Type  
·Tunnel-Tag

**Correct Answer: D**

**Section: (none)****Explanation****Explanation/Reference:**

Explanation:

[http://technet.microsoft.com/en-us/library/cc754422\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc754422(v=ws.10).aspx)

#### QUESTION 29

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**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Use connection request policies from Network Policy Server (NPS)

Ref:

<http://www.windowsnetworking.com/articles-tutorials/windows-server-2008/Understanding-new-Windows-Server-2008-Network-Policy-Server.html>

#### QUESTION 30

Your network contains an Active Directory forest. The forest contains a member server named VPN1 that runs Windows Server 2008 R2.

You need to configure VPN1 as a VPN server.

What should you install on VPN1?

- A. Network Policy Server (NPS)
- B. Simple TCP/IP Services
- C. Routing and Remote Access service (RRAS)
- D. Connection Manager Administration Kit (CMAK)

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation: <http://technet.microsoft.com/en-us/library/cc754378.aspx>

### QUESTION 31

Your network contains a Key Management Service (KMS) host named Server1.

On a client computer named Computer1 that runs Windows 7, you discover the following error message in the Event log: "0xC004F00F. The Software Licensing Server reported that the hardware ID binding is beyond level of tolerance."

You need to prevent the error message from appearing on Computer1.

What should you do from Computer1?

- A. Run slmgr.vbs /xpr.
- B. Run slmgr.vbs /ato.
- C. Restart the Windows Process Activation Service.
- D. Restart the Windows Update service.

**Correct Answer: B**

**Section: (none)**

**Explanation**

#### **Explanation/Reference:**

Explanation: Error message: The Software Licensing Server reported that the hardware ID binding is beyond level of tolerance.

Cause: The hardware has changed, or the drivers were updated on the system.

Troubleshooting steps: For the MAK, reactivate the system during the "Out of Tolerance" grace period by using online or telephone activation.

For

KMS, run the slmgr.vbs -ato command.

<http://technet.microsoft.com/en-us/library/ff793399.aspx>

### QUESTION 32

Your network contains a server named Server1 that has the Hyper-V server role installed. Server1 has two network adapters.

You need to configure Server1 to meet the following requirements:

- All virtual machines (VMs) on Server1 must be able to communicate with other computers on the network.
- The number of virtual network connections must be minimized.

What should you do?

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

#### **Explanation/Reference:**

Explanation:

External virtual networks. Use this type when you want to provide virtual machines with access to a physical network to communicate with externally located servers and clients. This type of virtual network also allows virtual machines on the same virtualization server to communicate with each other. This type of network may also be available for use by the management operating system, depending on how you configure the networking. (The management operating system runs the Hyper-V role.) For more information, see "A closer look at external virtual networks" later in this topic.

Source:<http://technet.microsoft.com/en-us/library/cc816585%28WS.10%29.aspx>

### QUESTION 33

Your network contains a server that runs Windows Server 2008 R2. The server has two host bus adaptors (HBAs). Each HBA is attached to a different switch.

The network contains a Storage Area Network (SAN).

You need to configure the server to use multiple paths to access the SAN.

Which tool should you use?

- A. Dism
- B. Mpclaim
- C. Diskpart
- D. Netsh

**Correct Answer: B**

**Section: (none)**

**Explanation**

#### **Explanation/Reference:**

Explanation:

Install MPIO on Windows Server 2008 R2

MPIO is an optional feature in Windows Server 2008 R2, and is not installed by default.

Install MPIO on Server Core installations of Windows Server 2008 R2

Because the Server Core installation of Windows Server 2008 R2 does not include the Server Manager interface, you must install MPIO by using a command prompt. Until you enable MPIO by using the DISM tool, you cannot use the mpclaim command.

Open a command prompt to run the following commands. After typing a command, press ENTER.

Enable MPIO:

Dism /online /enable-feature:MultipathIo

[http://technet.microsoft.com/en-US/library/ee619752\(v=ws.10\).aspx](http://technet.microsoft.com/en-US/library/ee619752(v=ws.10).aspx)

Using the MPclaim command-line tool

Multipath I/O can be managed by using the MPclaim command-line tool.

Note The command line is the only method of Multipath I/O configuration available on computers running a Server Core installation of Windows Server 2008.

Syntax of MPclaim

mpclaim restart\_option install\_switch device\_switch device\_hwid

MPclaim parameters

The following table describes the command parameters you can use with the MPclaim command to manage Multipath I/O by using a command line.

Source: <http://technet.microsoft.com/en-us/library/cc725907.aspx>

### QUESTION 34

Your network contains a server named Server1 that has the Hyper-V server role installed. Server1 hosts a virtual machine (VM) named VM1.

You add an additional hard disk to Server1. The hard disk is configured as a basic disk. You need to configure VM1 to use the new hard disk as a pass-through disk.



What should you do before you configure the pass-through disk?

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Pass-through Disk Configuration

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

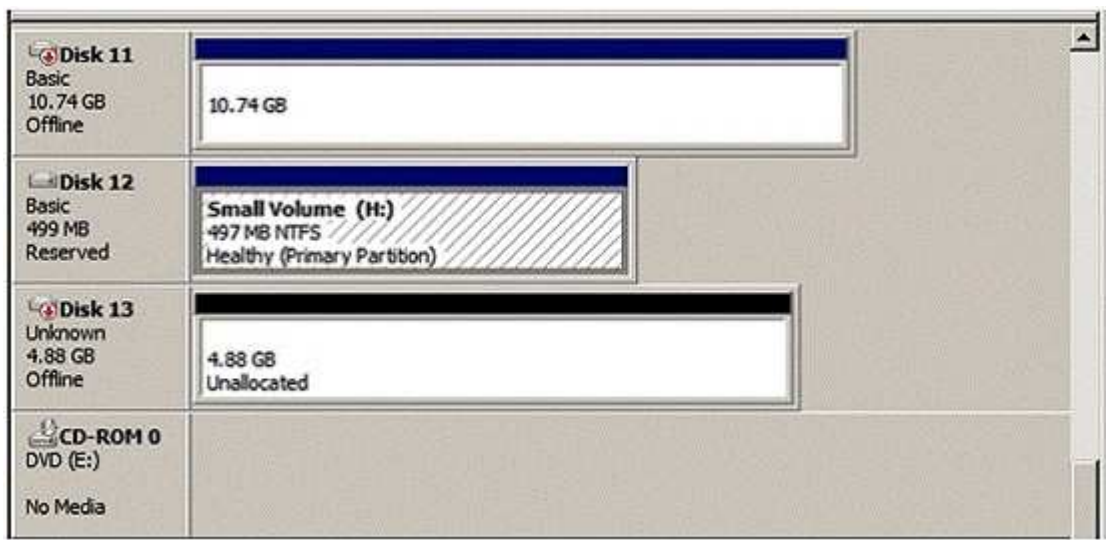


Figure 1: Raw disk is Offline



Figure 1-1 SAN Mode determination using diskpart.exe

I stated earlier that a disk must be Offline from the Hyper-V servers' perspective in order for the Guest to have exclusive access. However, a raw volume must first be initialized before it can be

used. To accomplish this in the Disk Management interface, the disk must first be brought Online. Once Online, the disk will show as being Not Initialized (Figure 2).

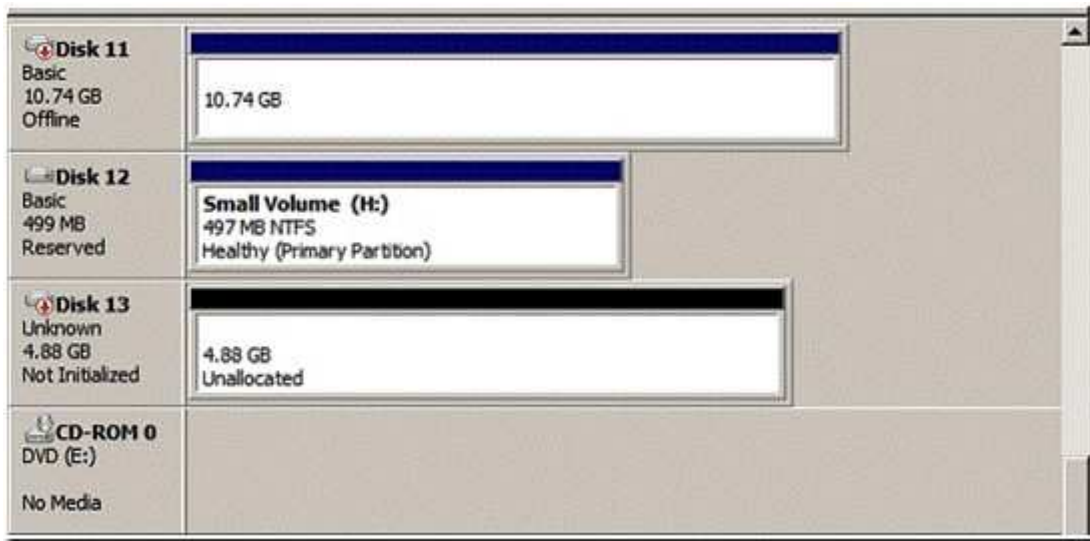


Figure 2: Disk is Online but Not Initialized  
Right-click on the disk and select Initialize Disk (Figure 3)

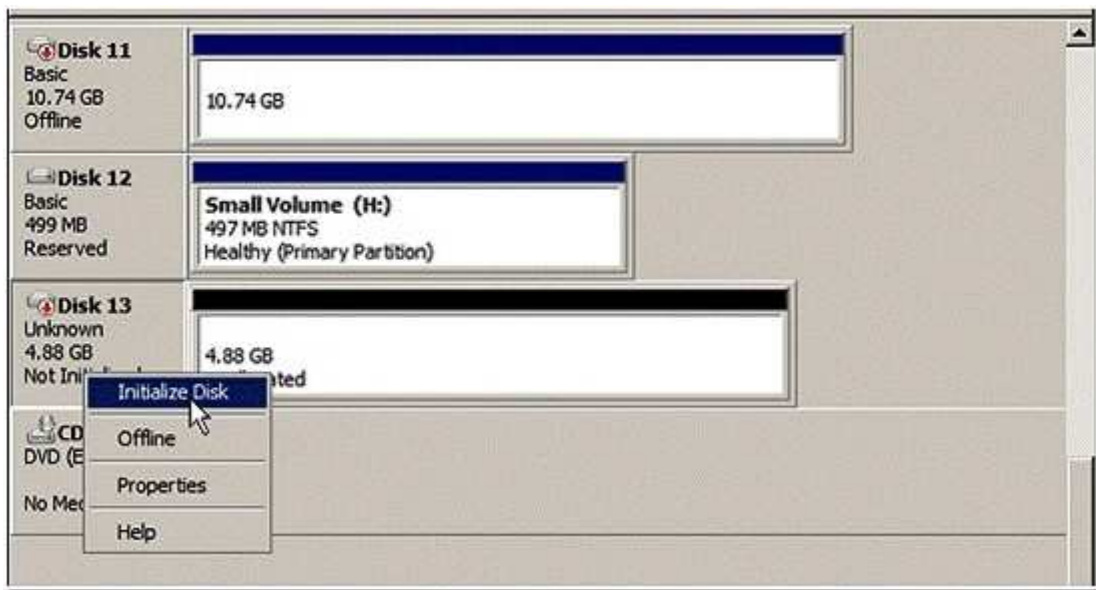


Figure 3: Initialize the disk

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



Figure 4: Selecting a partition type

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

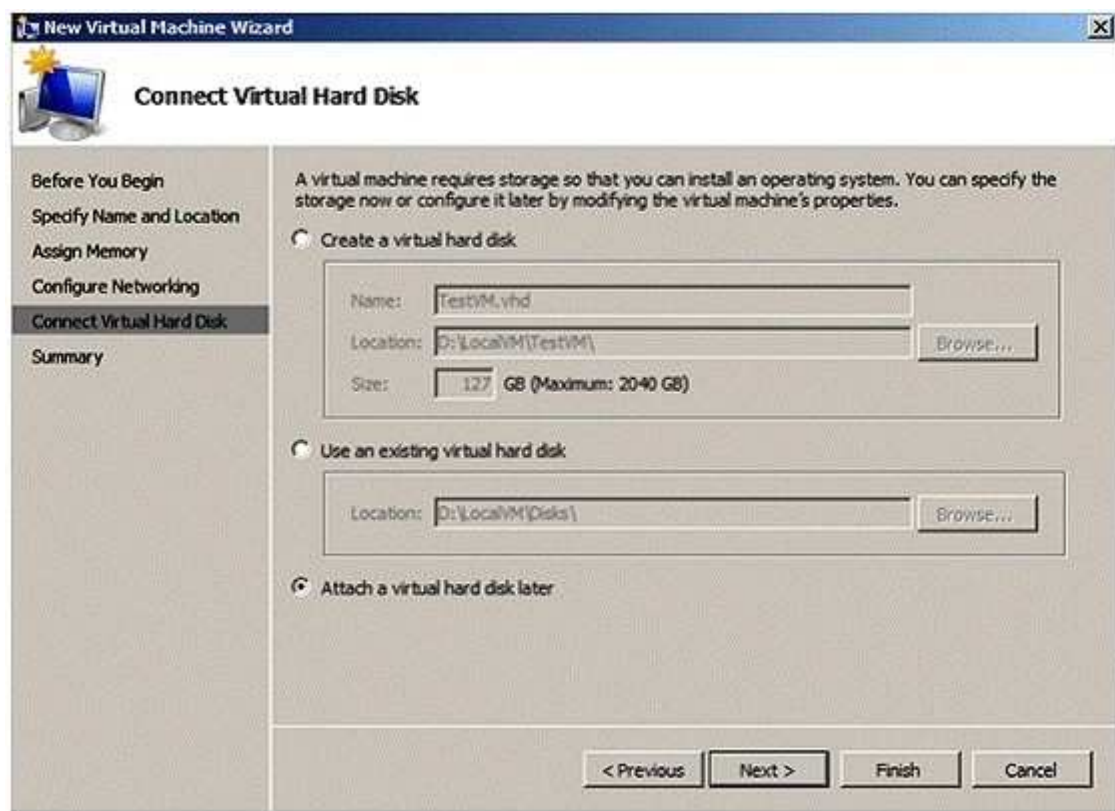


Figure 5: Choosing to attach a virtual disk later

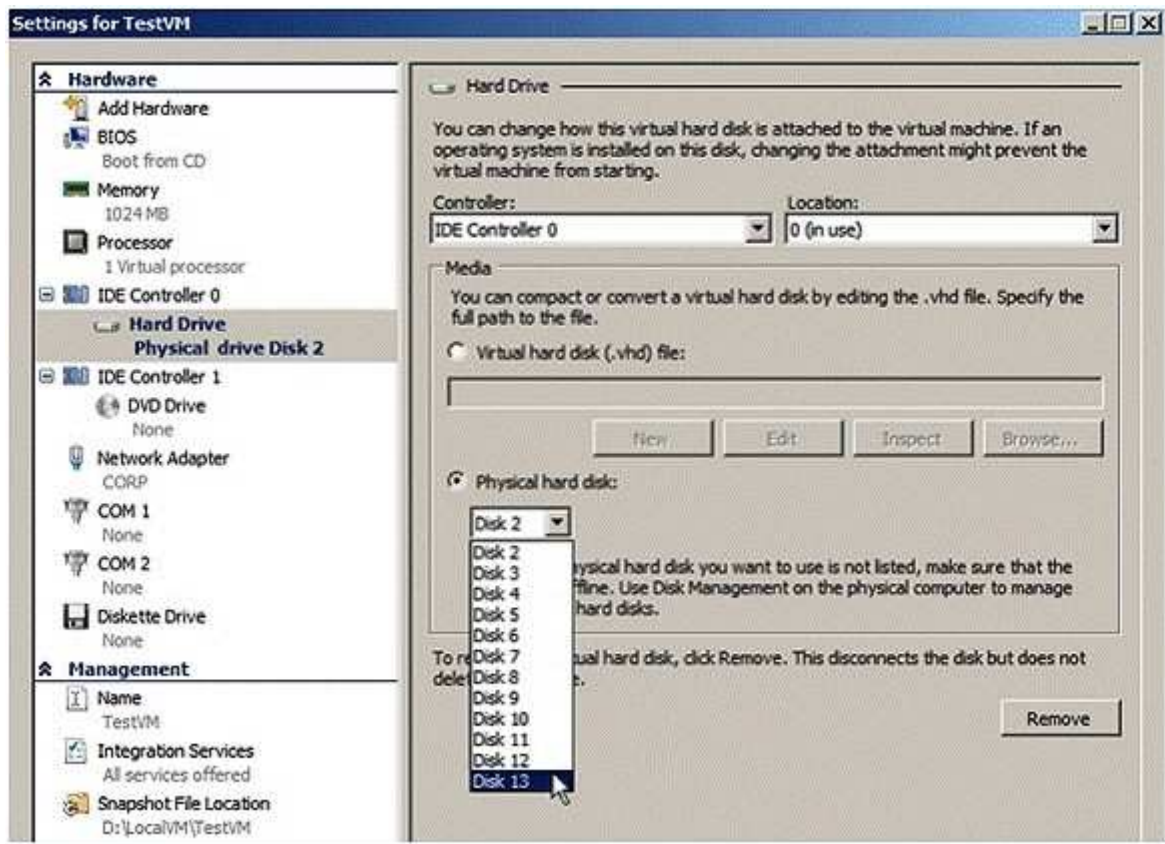


Figure 6: Attaching a pass-through disk to an IDE Controller Note: If the disk does not appear in the drop down list, ensure the disk is Offline in the Disk Management interface (In Server CORE, use the diskpart.exe CLI). Once the Pass-through disk is configured, the Guest can be started and data can be placed on the drive. If an operating system will be installed, the installation process will properly prepare the disk. If the disk will be used for data storage, it must be prepared in the Guest operating system before data can be placed on it.

If a Pass-through disk, being used to support an operating system installation, is brought Online before the Guest is started, the Guest will fail to start. When using Pass-through disks to support an operating system installation, provisions must be made for storing the Guest configuration file in an alternate location. This is because the entire Pass-through disk is consumed by the operating system installation. An example would be to locate the configuration file on another internal drive in the Hyper-V server itself. Or, if it is a cluster, the configuration file can be hosted on a separate cluster providing highly available file services. Be aware that Pass-through disks cannot be dynamically expanded. Additionally, when using Pass-through disks, you lose the capability to take snapshots, and finally, you cannot use differencing disks with Pass-through disks.

Note: When using Pass-through disks in a Windows Server 2008 Failover Cluster, you must have the update documented in KB951308: Increased functionality and virtual machine control in the Windows Server 2008 Failover Cluster Management console for the Hyper-V role installed on all

nodes in the cluster.

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

### QUESTION 35

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

Which SRV record should you create?

A. `_mskms._tcp.contoso.com`



- B. \_vlmcs.\_tcp.contoso.com
- C. \_kms.\_tcp.\_msdcs.contoso.com
- D. \_kms.\_tcp.contoso.com

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Manually Create SRV Records in DNS

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

Table 2 SRV Resource Record

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

**QUESTION 36**

You manage 20 servers that run Windows Server 2008 R2. The Remote Desktop Services server role and the Windows System Resource Manager (WSRM) feature are installed on all the servers.

You create and configure a resource-allocation policy that has the required custom settings on a server named TS01.

You need to configure the WSRM settings on all the servers to match the WSRM settings on TS01.

What should you do?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### Import or Export Criteria, Policies, and Schedules

You can import or export Windows System Resource Manager configuration information between computers. Configuration information stored includes process matching criteria, resource allocation policies, calendar events and schedules, and conditional policies. In this way, you can create management scenarios and then deploy them on other computers without performing the configuration multiple times.

#### Files Created and Imported

The files created by or imported by Windows System Resource Manager are:

#### Exporting and Importing Configuration Information

To export configuration information

1. Open Windows System Resource Manager.
2. In the navigation tree, right-click Windows System Resource Manager, and then click Export WSRM Information.
3. In Location, type a directory path where you want to save the configuration information, or click Browse to find the directory you want to use. When you have entered the directory information, click OK.
4. Windows System Resource Manager creates four XML documents in the specified directory that contain information about criteria, policies, and schedules.

To import configuration information

1. Open Windows System Resource Manager.
2. In the navigation tree, right-click Windows System Resource Manager, and then click Import WSRM Information.
3. In Location, type a directory path where the configuration information you want to import is located, or click Browse to find the directory you want to use. When you have entered the directory information, click OK.
4. Windows System Resource Manager loads the XML files into its current configuration, overwriting any previous configuration data.

Source:[http://technet.microsoft.com/en-us/library/cc771960\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc771960(WS.10).aspx)

### QUESTION 37

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

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

Server1 has Remote Desktop Services Per Device client access licenses (RDS Per Device CALs) installed. Server2 and Server3 are members of a Remote Desktop Connection Broker (RD Connection Broker) farm.

Four months after Server2 and Server3 are deployed, you discover that users can no longer establish Remote Desktop sessions on Server3.

You verify that Server3 is online and that all required services on Server3 run properly. You verify that the users can establish Remote Desktop sessions on Server2.

You need to ensure that the users connecting to the RD Connection Broker farm can establish sessions on Server3.

What should you do?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

You must configure RD Licensing correctly in order for your RD Session Host server to accept connections from clients. To allow ample time for you to deploy a license server, Remote Desktop Services provides a licensing grace period for the RD Session Host server during which no license server is required. During this grace period, an RD Session Host server can accept connections from unlicensed clients without contacting a license server. The grace period begins the first time the RD Session Host server accepts a client connection. A permanent RDS CAL is issued by a license server to a client connecting to the RD Session Host server. The number of days in the grace period is exceeded.

The length of the grace period is based on the operating system running on the RD Session Host server.

The grace periods are as follows:

Source:<http://technet.microsoft.com/en-us/library/cc725933.aspx>

### **QUESTION 38**

Your network contains two separate subnets named Subnet1 and Subnet2. Subnet1 contains a Windows Server Update Services (WSUS) server named Server1.

Computers on Subnet1 can access resources on the Internet. Subnet2 is an isolated subnet.

You deploy a new WSUS server named Server2 in Subnet2.

You need to replicate the metadata from Server1 to Server2.

What should you do on Server1?

- A. Run wsusutil.exe and specify the export parameter.
- B. Run wsusutil.exe and specify the move content parameter.
- C. Run wbadmin.exe and specify the start backup parameter.
- D. Run wbadmin.exe and specify the start system state backup parameter.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

<http://technet.microsoft.com/en-us/library/cc720437%28WS.10%29.aspx>

### **QUESTION 39**

Your network contains a single Active Directory domain. All servers run Windows Server 2008 R2. A DHCP server is deployed on the network and configured to provide IPv6 prefixes.

You need to ensure that when you monitor network traffic, you see the interface identifiers derived from the Extended unique Identifier (6UI)-64 address.

Which command should you run?

- A. netsh.exe interface ipv6 set global addressmaskreply-disabled
- B. netsh.exe interface ipv6 set global dhcpmediasense = enabled
- C. netsh.exe interface ipv6 set global randomizeidentifiers = disabled
- D. netsh.exe interface ipv6 set privacy state = enabled

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 40**

Your network contains a server that runs a Server Core installation of Windows Server 2008 R2. You need to log the CPU utilization of the server.

Which tool should you use?

- A. logman.exe
- B. oclist.exe
- C. relog.exe
- D. sc.exe

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation: <http://technet.microsoft.com/en-us/library/bb490956.aspx>

Manages and schedules performance counter and event trace log collections on local and remote systems.

#### **QUESTION 41**

You need to capture the HTTP traffic to and from a server every day between 09:00 and 10:00.

What should you do?

- A. Create a scheduled task that runs the Netsh tool.
- B. Create a scheduled task that runs the Nmcap tool.
- C. From Network Monitor, configure the General options.
- D. From Network Monitor, configure the Capture options.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

nmcap /networks \* /capture LDAP /file c:\file.cap

If you want a timer add the following

/startwhen /timeafter x hours

#### **QUESTION 42**

Your company runs Windows Server Update Services (WSUS) on a server named Server1. Server1 runs Windows Server 2008 R2. Server1 is located on the company intranet.

You configure the WSUS Web site to use SSL.

You need to configure a Group Policy object (GPO) to specify the intranet update locations.

Which URLs should you use?



- A. http://SERVER1
- B. http://Server1:8080
- C. https://SERVER1
- D. https://Server1:8080

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 43**

Your network contains a Windows Server Update Services (WSUS) Server infrastructure that has three servers named WSUS1, WSUS2, and WSUS3. WSUS2 is a downstream replica server of WSUS1. WSUS3 is a downstream replica server of WSUS2.

You need to ensure that the Update Services console on WSUS2 only displays computers that receive updates from WSUS2.

What should you configure on WSUS2?

- A. downstream servers
- B. Personalization
- C. reporting rollup
- D. synchronizations

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 44**

Your company has a network that has 100 servers. A server named Server1 is configured as a file server. Server1 is connected to a SAN and has 15 logical drives.

You want to automatically run a data archiving script if the free space on any of the logical drives is below 30 percent.

You need to automate the script execution.

You create a new Data Collector Set.

What should you do next?

- A. Add the Event trace data collector.
- B. Add the Performance counter alert.
- C. Add the Performance counter data collector.
- D. Add the System configuration information data collector.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Refer to below Step by step guide:

<http://technet.microsoft.com/en-us/library/cc722414.aspx>

**QUESTION 45**

Your network contains a server named Server1 that runs Windows Server 2008 P2.

You have a user named User1.

You need to ensure that User1 can schedule Data Collector Sets (DCSs) on Server1. The solution must minimize the number of rights assigned to User1.

What should you do?

- A. Add User1 to the Performance Log Users group.
- B. Add User1 to the Performance Monitor Users group.
- C. Assign the Profile single process user right to User1.
- D. Assign the Bypass traverse checking user right to User1.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Both A and B are valid users group but:

Performance Log users group : Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to

this computer Performance Monitor users group : Members of this group can access performance counter data locally and remotely.

Hence answer is "A".

**QUESTION 46**

Your network contains a Windows Server Update Services (WSUS) server.

You have an organizational unit (OU) named Sales. The Sales OU contains all of the computer objects for the sales department. You enable client side targeting for the Sales OU and set the target group name to Sales-Computers.

You restart a sales computer.

You discover that the computer is not added to the Sales-Computer computer group in WSUS.

You need to ensure that all sales computers are added to the Sales-Computers group.

Which options should you configure?

- A. Automatic Approvals
- B. Computers
- C. Personalization
- D. Products and Classifications

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 47**

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Web Server (IIS) role installed.

You need to review the contents of the US-Configuration Analytic event log on Server1.

You configure Event Viewer to show the Analytic log.

What should you do next?

- A. Attach a task to the log.
- B. Create a custom view to the log.
- C. Modify the Subscriptions list for the log.
- D. Modify the General properties of the log.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Analytic event logs, and not only for IIS are not enabled by default. You are enable it. You should enable them from "General Tab" of properties of log "Log of services and applications\Microsoft\Windows\IIS-Configuration\Analytic" to start logging

**QUESTION 48**

Your network contains a server that runs Windows Server 2008 R2.

You plan to create a custom script.

You need to ensure that each time the script runs, an entry is added to the Application event log.

Which tool should you use?

- A. Eventcreate
- B. Eventvwr
- C. Wecutil
- D. Wevtutil

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

You can create custom events in an event log by using the Eventcreate utility. This can be useful as a diagnostic tool in scripts when you record an error or event directly into the logs without using VBScript or another language to log the event.

<http://support.microsoft.com/kb/324145>

**QUESTION 49**

Your network contains two servers named Server1 and Server2 that run a Server Core installation of Windows Server 2008 R2. Server1 has the SNMP Service installed.

You need to ensure that Server2 can send SNMP traps to Server1.

What should you do?

- A. On Server1, run `oclist snmp-sc`.
- B. On Server2, run `oclist snmp-sc`.
- C. On Server1, run `dism /online /enable-feature /featurename:snmp-sc`.
- D. On Server2, run `dism /online /enable-feature /featurename:snmp-sc`.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

<http://tweaks.com/windows/40255/manage-windows-features-from-command-line-with-dism/>

### QUESTION 50

Your company has a network that has an Active Directory domain. The domain has two servers named DC1 and DC2.

You plan to collect events from DC2 and transfer them to DC1. You configure the required subscriptions by selecting the Normal option for the Event delivery optimization setting and by using the HTTP protocol.

You discover that none of the subscriptions work.

You need to ensure that the servers support the event collectors.

Which three actions should you perform? (Each correct answer presents part of the solution. Choose three.)

- A. Run the `wecutil qc` command on DC1.
- B. Run the `wecutil qc` command on DC2.
- C. Run the `winrm quickconfig` command on DC1.
- D. Run the `winrm quickconfig` command on DC2.
- E. Add the DC2 account to the Administrators group on DC1.
- F. Add the DC1 account to the Administrators group on DC2.

**Correct Answer:** ADF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 51

Network Access Protection (NAP) is configured for the corporate network.

Users connect to the corporate network by using portable computers.

The company policy requires confidentiality of data when the data is in transit between the portable computers and the servers.

You need to ensure that users can access network resources only from computers that comply with the company policy.

What should you do?

- A. Create an IPSec Enforcement Network policy.
- B. Create an 802.1X Enforcement Network policy.
- C. Create a Wired Network (IEEE 802.3) Group policy.
- D. Create an Extensible Authentication Protocol (EAP) Enforcement Network policy.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

<http://www.lead2pass.com/70-649.html>

#### **QUESTION 52**

Your network contains an Active Directory forest. The forest contains two domains named contoso.com and eu.contoso.com.

You install a Network Policy Server (NPS) named Server1 in the contoso.com domain.

You need to ensure that Server1 can read the dial-in properties of the user accounts in the eu.contoso.com domain.

<http://www.lead2pass.com/70-649.html>

What should you do?

- A. In the contoso.com domain, add Server1 to the RAS and IAS Servers group.
- B. In the contoso.com domain, add Server1 to the Windows Authorization Access group.
- C. In the eu.contoso.com domain, add Server1 to the RAS and IAS Servers group.
- D. In the eu.contoso.com domain, add Server1 to the Windows Authorization Access group.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

C is correct, Servers in this group can access remote access properties of users

#### **QUESTION 53**

Your network contains a computer named Computer1 that runs Windows 7.

You need to verify if Computer1 has active DirectAccess connections to the network.

What should you do?

- A. From Network Connections, right-click the active network connection, and then click Status.
- B. From Network Connections, select the active network connection, and then click Diagnose this connection.
- C. From Windows Firewall with Advanced Security, click Monitoring, and then click Connection Security Rules.
- D. From Windows Firewall with Advanced Security, click Monitoring, click Security Associations, and then click Main Mode.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 54**

Your network contains a single Active Directory domain. The domain contains five read-only domain controllers (RODCs) and five writable domain controllers. All servers run Windows Server 2008.

You plan to install a new RODC that runs Windows Server 2008 R2.

You need to ensure that you can add the new RODC to the domain. You want to achieve this goal by using the minimum amount of administrative effort.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. From Active Directory Domains and Trusts, raise the functional level of the domain.
- B. From Active Directory Users and Computers, pre-stage the RODC computer account.
- C. At the command prompt, run `adprep.exe /forestprep`.
- D. At the command prompt, run `adprep.exe /rodcprep`.
- E. At the command prompt, run `adprep.exe /domainprep`.

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 55**

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 56**

Active Directory Rights Management Services (AD RMS) is deployed on your network.

Users who have Windows Mobile 6 devices report that they cannot access documents that are protected by AD RMS.

You need to ensure that all users can access AD RMS protected content by using Windows Mobile 6 devices.

What should you do?

- A. Modify the security of the `MobileDeviceCertification.asmx` file.
- B. Modify the security of the `ServerCertification.asmx` file.

- C. Enable anonymous authentication for the \_wmcs virtual directory.
- D. Enable anonymous authentication for the certification virtual directory.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 57

Your network contains an Active Directory forest named adatum.com. All domain controllers currently run Windows Server 2003 Service Pack 2 (SP2). The functional level of the forest and the domain is Windows Server 2003.

You need to deploy a read-only domain controller (RODC) that runs Windows Server 2008 R2.

What should you do first?

- A. Raise the functional level of the forest to Windows Server 2008.
- B. Deploy a writable domain controller that runs Windows Server 2008 R2.
- C. Raise the functional level of the domain to windows Server 2008.
- D. Run adprep.exe.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

They mean the first action ==> Adprep /forestprep and Adprep /domainprep

Second action in this case is to "Deploy a writable domain controller that runs Windows Server 2008 R2"  
Because RODC need 2K8 Writable domain Controller to replicate.

#### QUESTION 58

Your network contains a server named Server1. The Active Directory Rights Management Services (AD RMS) server role is installed on Server1. An administrator changes the password of the user account that is used by AD RMS.

You need to update AD RMS to use the new password.

Which console should you use?

- A. Active Directory Users and Computers
- B. Local Users and Groups
- C. Services
- D. Active Directory Rights Management Services

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 59

Your network contains two servers named Server1 and Server2 that run Windows Server 2008 R2. Server1 has Active Directory Federation Services (AD FS) 2.0 installed.

Server1 is a member of an AD FS farm. The AD FS farm is configured to use a configuration database that is stored on a separate Microsoft SQL Server.

You install AD FS 2.0 on Server2.

You need to add Servers to the existing AD FS farm.

What should you do?

- A. On Server2, run fsconfig.exe.
- B. On Server1, run fsconfigwizord.exe
- C. On Server1, run fsconfig.exe.
- D. On Server2, run fsconfigwizord.exe.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

To configure a new federation server using the command line

Open a Command Prompt window. To open a command prompt, click Start, click Run, type cmd, and then click OK.

Change the directory to the path where AD FS 2.0 was installed. For example, if the default path of %ProgramFiles%\Active Directory Federation Services 2.0 was used as the install path, type the following command, and then press ENTER:

```
cd %programfiles%\Active Directory Federation Services 2.0
```

To configure this computer as a federation server, type the applicable syntax using either of the following command parameters, and then press ENTER:

```
fsconfig.exe {StandAlone|CreateFarm|CreateSQLFarm|JoinFarm|JoinSQLFarm} [deployment specific parameters]
```

Parameter	Description
StandAlone:	Sets up this computer as a stand-alone federation server for evaluation purposes or for a small production environment. To see details about this option, type fsconfig StandAlone /help.
CreateFarm:	Creates a new federation server farm and uses the Windows Internal Database to store AD FS 2.0 configuration settings. To see details about this option, type fsconfig CreateFarm /help.
CreateSQLFarm:	Creates a new federation server farm and uses Microsoft SQL Server® to store AD FS 2.0 configuration settings. To see details about this option, type fsconfig CreateSQLFarm /help.
JoinFarm:	Joins this computer to an existing federation server farm that is using the Windows Internal Database. To see details about this option, type fsconfig JoinFarm /help.
JoinSQLFarm:	Joins this computer to an existing federation server farm that is using SQL Server. To see details about this option, type fsconfig JoinSQLFarm /help.

## QUESTION 60

Your company runs Remote Desktop Services. You plan to install an application update for the lobapp.exe application on the Remote Desktop Session Host Server. You find instances of the lobapp.exe processes left behind by users who have disconnected.

You need to terminate all instances of the lobapp.exe processes so that you can perform an application update.

What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two.)

- A. Run the Tasklist /fi "IMAGENAME eq lobapp.exe" command on the Remote Desktop Session Host Server.



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

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

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

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



**Wrong Answers:**

Tasklist

Displays a list of currently running processes on the local computer or on a remote computer.

Tasklist replaces the tlist tool.

Source: [http://technet.microsoft.com/en-us/library/cc730909\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc730909(WS.10).aspx) Get-Process Although the following will work for a single instance:

(Get-Process lobapp).Kill()

```
Administrator: C:\Windows\system32\cmd.exe - powershell
C:\>powershell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\> (Get-Process lobapp)

Handles      NPM(K)      PM(K)      WS(K)      UM(M)      CPU(s)      Id ProcessName
-----
        68         8       1256       5712        71         0.16     1132 lobapp

PS C:\> (Get-Process lobapp).Kill()
PS C:\> (Get-Process lobapp)
Get-Process : Cannot find a process with the name "lobapp". Verify the process
name and call the cmdlet again.
At line:1 char:13
+ <Get-Process <<<< lobapp>
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (lobapp:String) [Get-Process], P
rocessCommandException
+ FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.
Commands.GetProcessCommand

PS C:\> _
```

This will not work on multiple instances:  
(Get-Process lobapp).Kill()

```
Administrator: C:\Windows\system32\cmd.exe
C:\>powershell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\> (Get-Process lobapp)

Handles      NPM(K)      PM(K)      WS(K)      UM(M)      CPU(s)      Id ProcessName
-----
        68         8       1260       5644        71         0.09         920 lobapp
        68         8       1256       5704        71         0.14       1132 lobapp
        68         8       1260       5708        71         0.11       3080 lobapp
        68         8       1260       5652        71         0.11       3992 lobapp

PS C:\> (Get-Process lobapp).Kill()
Method invocation failed because [System.Object[]] doesn't contain a method nam
ed 'Kill'.
At line:1 char:26
+ <Get-Process lobapp>.Kill <<<< <>
+ ~~~~~
+ CategoryInfo          : InvalidOperation: (Kill:String) [], RuntimeExcep
tion
+ FullyQualifiedErrorId : MethodNotFound

PS C:\>
```

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

```
Administrator: C:\Windows\system32\cmd.exe - powershell
C:\>powershell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\> Get-Process lobapp

Handles      NPM(K)      PM(K)      WS(K)      VM(M)      CPU(s)      Id ProcessName
-----
        68          8       1256       5676        71         0.08      2524 lobapp
        68          8       1260       5700        71         0.09      2544 lobapp
        68          8       1260       5720        71         0.08      2920 lobapp
        69          8       1256       5784        71         0.06      3492 lobapp

PS C:\> Get-Process lobapp | ForEach-Object { $_.Kill() }
PS C:\> Get-Process lobapp
Get-Process : Cannot find a process with the name "lobapp". Verify the process
name and call the cmdlet again.
At line:1 char:13
* Get-Process <<<< lobapp>
+ CategoryInfo          : ObjectNotFound: (lobapp:String) [Get-Process], P
rocessCommandException
+ FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.
Commands.GetProcessCommand

PS C:\>
```

#### QUESTION 61

Your network contains an Active Directory domain.

You deploy a server named Server1 that has the Remote Desktop Connection Broker (RD Connection Broker) role service installed.

You need to ensure that all servers that have the Remote Desktop Session Host (RD Session Host) role service installed are automatically configured to use Server1 as an RD Connection Broker.

What should you do?

- A. Register a service principal name (SPN) for Server1.
- B. Register a service location (SRV) record for Server1.
- C. Use a Group Policy to configure the Restricted Groups settings.
- D. Use a Group Policy to configure the Remote Desktop Services settings.

**Correct Answer: D**

**Section: (none)**

**Explanation**

#### Explanation/Reference:

Explanation:

RD Connection Broker

Policy settings in this node control configuration of a Remote Desktop Session Host server that is a member of a load-balanced Remote Desktop Session Host server farm. The full path of this node in the Group Policy Management Console is Computer Configuration\Policies\Administrative Templates\Windows Components\Remote

Desktop Services\Remote Desktop Session Host\RD Connection Broker.

Available policy settings Join RD Connection Broker

This policy setting allows you to specify whether the RD Session Host server should join a farm in RD Connection Broker. RD

Connection Broker tracks user sessions and allows a user to reconnect to their existing session in a load-balanced RD Session Host server farm. To participate in RD Connection Broker, the Remote Desktop Session

Host role service must be installed on the server. If the policy setting is enabled, the RD Session Host server joins the farm that is specified in the Configure RD Connection Broker Farm Name setting. The farm exists on the RD Connection Broker server that is specified in the Configure RD Connection Broker Server name policy setting.

If you disable this policy setting, the server does not join a farm in RD Connection Broker, and user session tracking is not performed. If the setting is disabled, you cannot use either the Remote Desktop Session Host Configuration tool or the Terminal

Services WMI provider to join the server to RD Connection Broker.

If the policy setting is not configured, the setting is not specified at the Group Policy level. In this case, you can configure the server

to join RD Connection Broker by using the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider.

If you enable this setting, you must also enable the "Configure RD Connection Broker Farm Name" and Configure RD Connection Broker Server name policy settings, or configure these settings by using either the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider.

**Configure RD Connection Broker farm name**

This policy setting allows you to specify the name of a farm to join in RD Connection Broker. RD Connection Broker uses the farm name to determine which RD Session Host servers are in the same RD Session Host server farm. Therefore, you must use the same farm name for all RD Session Host servers in the same load-balanced farm. The farm name does not have to correspond to a name in Active Directory Domain Services. If you specify a new farm name, a new farm is created in RD Connection Broker. If you specify an existing farm name, the server joins that farm in RD Connection Broker. If you enable this policy setting, you must specify the name of a farm in RD Connection Broker. If you disable or do not configure this policy setting, the farm name is not specified by Group Policy. In this case, you can adjust the farm name by using the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider. This setting is not effective unless both the Join RD Connection Broker and the Configure RD Connection Broker server name settings are enabled and configured by using Group Policy, the Remote Desktop Session Host Configuration tool, or the Terminal Services WMI provider.

**Configure RD Connection Broker server name**

This policy setting allows you to specify the RD Connection Broker server that the RD Session Host server uses to track and redirect user sessions for a load-balanced RD Session Host server farm. The specified server must be running the Remote Desktop Connection Broker service. All RD Session Host servers in a load-balanced farm should use the same RD Connection Broker server.

If you enable this policy setting, you must specify the RD Connection Broker server, using either its host name, IP address, or fully qualified domain name. If you specify a name or IP address for the RD Connection Broker server that is not valid, an error message is logged in Event Viewer on the RD Session Host server.

If you disable or do not configure this policy setting, you can adjust the RD Connection Broker server name or IP address by using the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider.

This policy setting is not effective unless the Join RD Connection Broker policy setting is enabled or the RD Session Host server is configured to join RD Connection Broker by using the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider. To be an active member of an RD Connection Broker-enabled RD Session Host server farm, the computer account for each RD Session Host server in the farm must be a member of the Session Directory Computers local group on the RD Connection Broker server.

**Use RD Connection Broker load balancing**

This policy setting allows you to specify whether to use the RD Connection Broker load balancing feature to balance the load between servers in an RD Session Host server farm. If you enable this policy setting, RD Connection Broker redirects users who do not have an existing session to the RD Session Host server in the farm with the fewest sessions. Redirection behavior for users with existing sessions is not affected. If the server is configured to use RD Connection Broker, users who have an existing session are redirected to the RD Session Host server where their session exists.

If you disable this policy setting, users who do not have an existing session log on to the first RD Session Host server to which they connect.

If you do not configure this policy setting, you can configure the RD Session Host server to participate in RD

Connection Broker load balancing by using the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider. If you enable this policy setting, you must also enable the Join RD Connection Broker, the Configure RD Connection Broker farm name, and the Configure RD Connection Broker server name policy settings.

Source:<http://technet.microsoft.com/en-us/library/ee791821.aspx>

### QUESTION 62

Your network contains a server named Server1 that has the Remote Desktop Session Host (RD Session Host) role service installed.

A user named User1 connects to Server1 and starts an application named App1.exe.

User1 reports that App1.exe is unresponsive and cannot be closed.

You need to terminate App1.exe for User1 only.

Which tool should you do?

- A. Tskill
- B. Qprocess
- C. Rwinsta
- D. Quser

**Correct Answer: A**

**Section: (none)**

**Explanation**

#### Explanation/Reference:

Explanation:

Tskill Ends a process.

Syntax tskill {ProcessID | ProcessName} [/server:ServerName] [{/id:SessionID | /a}] [/v] Parameters ProcessID : The ID of the process you want to end. ProcessName : The name of the process you want to end. You can use wildcards to specify this parameter.

/server: ServerName : Specifies the terminal server containing the process you want to end.

Otherwise, the current terminal server is used.

/id: SessionID : Ends the process running in the specified session.

/a : Ends the process running in all sessions.

/v : Displays information about the actions being performed.

/? : Displays help at the command prompt.

tskill App1.exe /server:Server1 /id:<SessionID of User1>

Source:<http://technet.microsoft.com/en-us/library/bb490806.aspx>

### QUESTION 63

Your company has an Active Directory domain. The company runs Remote Desktop Services. You configure the main office printer as the default printer on the Remote Desktop Session Host Server.

The company policy states that all remote client computers must meet the following requirements:

- The main office printer must be the default printer of the client computers.
- Users must be able to access their local printers during a remote desktop session.

You need to create a Group Policy object (GPO) by using the Remote Desktop Session Host Printer Redirection template to meet the company policy.

What should you do?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Do not set default client printer to be default printer in a session This policy setting allows you to specify whether the client default printer is automatically set as the default printer in a Terminal Services session. By default, Terminal Services automatically designates the client default printer as the default printer in a Terminal Services session. You can use this policy setting to override this behavior. If you enable this policy setting, the default printer is the printer specified on the remote computer. If you disable this policy setting, the terminal server automatically maps the client default printer and sets it as the default printer upon connection. If you do not configure this policy setting, the default printer is not specified at the Group Policy level. However, an administrator can configure the default printer for client sessions by using the Terminal Services Configuration tool.

Source:[http://technet.microsoft.com/en-us/library/cc731963\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc731963(WS.10).aspx)

#### **QUESTION 64**

Your network contains an Active Directory domain. The domain contains a server named Server1 that has the Remote Desktop Licensing (RD Licensing) role service installed.

On Server1, you enable the License server security group Group Policy setting.

You need to ensure that Server1 can issue Remote Desktop Services client access licenses (RDS CALs) to a server named Server3.

What should you do on Server3?

- A. From Server1 Computer Management, modify the members of the Terminal Server Computers group.
- B. From Remote Desktop Session Host Configuration, modify the licensing mode.
- C. From Remote Desktop Licensing Manager, modify the connection method from the properties of the server.
- D. From Remote Desktop Licensing Manager, reactivate the server.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Terminal Services License Server Security Group Configuration When the TS Licensing role service is installed on the server, the Terminal Server Computers local group is created.

The license server will respond only to requests for TS CALs from terminal servers whose computer accounts are members of this group if the Computer Configuration\Administrative Templates\Windows Components\Terminal Services\TS Licensing\License server security group Group Policy setting has been enabled and applied to the license server. By default, the Terminal Server Computers local group is empty. Source: <http://technet.microsoft.com/en-us/library/cc775331.aspx>

**QUESTION 65**

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**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 66**

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the SMTP Server feature installed and has one SMTP Virtual Server named SMTP1.

You need to configure Server1 to meet the following requirements:

- Relay e-mail messages for contoso.com.
- Relay e-mail messages for nwtraders.com.
- Prevent the relaying of e-mail messages to other domains.

What should you do?

- A. Modify the connection control settings of SMTP1.
- B. Configure two alias domains to SMTP1.
- C. Modify the relay restrictions list of SMTP1.
- D. Configure two remote domains to SMTP1.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Configuring SMTP Virtual Server Relay for Remote Domains You can configure an SMTP virtual server to relay incoming mail to your SMTP/POP3 server. The SMTP virtual server can also accept and relay mail to other domains within your organization. Specifying a relay server overrides the smart host setting in the Advanced Delivery box of the SMTP virtual server.

Procedures

To configure an SMTP virtual server to relay mail to a remote domain

1. In IIS Manager, double-click the SMTP virtual server that you want to configure, right-click Domains, point to New, and then click Domain. The New SMTP Domain Wizard starts.
2. Click Remote, and then click Next.
3. In the Name box, type a name for the remote domain, and then click Finish.
4. In IIS Manager, right-click the new remote domain, and then click Properties.



5. On the General tab, select the Allow incoming mail to be relayed to this domain check box to allow the SMTP server to act as a mail relay.
6. On the General tab under Route domain, click Forward all mail to smart host, and then type the fully qualified domain name or the IP address of the internal network corporate mail server through which you would like to route messages for this remote domain.
7. Click OK, and then stop and restart the SMTP virtual server. After you configure the remote domain, all mail that is addressed to the remote domain is relayed to the smart host that you configured. Mail that is not deliverable is stored in the Inetpub\Mailroot\Badmail folder.



Source:<http://technet.microsoft.com/en-us/library/cc775967.aspx>

#### QUESTION 67

Your network contains a virtual machine (VM) named VM1. VM1 contains two virtual hard disks (VHDs). One VHD is a dynamically expanding disk and the other VHD is a fixed disk.

You need to manually copy the VHDs. The solution must minimize the amount of downtime for VM1.

What should you do first?

- A. From Hyper-V Manager, reset VM1.
- B. Run the Export-VM PowerShell cmdlet.
- C. From Hyper-v Manager, pause VM1.
- D. Run the Unmount-VHD PowerShell cmdlet.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 68

Your network contains a server named Server1 that runs Windows Server 2008 R2. The network contains two sites named Site1 and Site2 that are separated by a firewall. Server1 is configured as a Key Management Service (KMS) host located in Site1.

You need to configure the firewall so that computers in Site2 can activate Windows by using Server1.

Which TCP port should you allow through the firewall?

- A. 443
- B. 135
- C. 1688
- D. 1433



**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

KMS requires a firewall exception on the KMS host. If using the default TCP port, enable the KMS Traffic exception in Windows Firewall. If using a different firewall, open TCP port 1688. If using a non-default port, open the custom TCP port in the firewall.

Source:<http://technet.microsoft.com/en-us/library/ff793409.aspx>

#### **QUESTION 69**

Your network contains a server that runs windows Server 2008 R2 and has the Windows Deployment Services (WDS) server role installed.

You have a .vhd file that contains an installation of Windows 7.

You need to deploy the Windows 7 installation by using WDS. You want to achieve this goal by using the minimum amount of administrative effort.

What should you do first?

- A. From Windows Deployment Services, add a capture image.
- B. From Disk Management, mount the .vhd file.
- C. Run the imagex.exe command and specify the /export parameter.
- D. Run the wdsutil.exe command and specify the /add-image parameter.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

To add a virtual hard disk image to the server

1. Click Start, right-click Command Prompt, and then click Run as administrator.

2. You must create an image group because .vhd images cannot be in image groups with .wim images. To create an image group for the .vhd image, use the following syntax: WDSUTIL /Add- ImageGroup / ImageGroup:

<image group name>.

Example: WDSUTIL /Add-ImageGroup /ImageGroup:"VHD Image Group"

3. To add the .vhd image to the server, use the following syntax (at a minimum): WDSUTIL /Verbose / Progress /

Add-Image /ImageFile:<path> /ImageType:Install /ImageGroup:<image group name>. For differencing disks, the path to the image should be to the .vhd file of the differencing disk and not to the parent disk. Adding the differencing .vhd will add the parent .vhd file to the server, but only the differencing disk will be active (the parent .vhd will be inactive). If the differencing disk is part of chain, choose the last .vhd in the chain. In that case, the immediate parent .vhd and all preceding parent .vhd files in the chain will also be added. Full syntax: WDSUTIL /add-Image /ImageFile:<.vhd file path> [/Server:<server name>]

/ImageType:install [/

ImageGroup:<image group name>] [/Filename:<new image file name>] [/UnattendFile:<full path to unattend file>]

Example: WDSUTIL /Verbose /Progress /Add-Image /ImageFile:"C:\vhd \WindowsServer2008R2.vhd" / Server:MyWDSserver /ImageType:Install /ImageGroup:"VHD Image Group"

4. Repeat step 3 until you have added all of your .vhd images.

5. If you want to update the description for an image, use the following steps:

a. Run WDSUTIL /Get-ImageGroup /ImageGroup:<image group name> and note the name that the server assigned to the image. To display the full image metadata on each image in the group, append /Detailed.

Example: WDSUTIL /Get-ImageGroup /ImageGroup:"VHD Image Group" b. To update the description for an image, use the following syntax where <image name> is the name you noted in the previous step: WDSUTIL /Set-Image /Image:<image name> /ImageType:Install /ImageGroup:<image group name> /Description:<description>.

Example: WDSUTIL /Set-Image /Image:"VHD image" /ImageType:Install /ImageGroup:"VHD Image Group" /Description:"VHD image for R2"

Source:[http://technet.microsoft.com/en-us/library/dd363560\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd363560(WS.10).aspx)

#### QUESTION 70

Your network contains a server named Server1 that has two volumes named C and D.

You add a new volume.

You need to ensure that you can access data on the new volume by using the path D:\data.

What should you do?

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

#### Explanation/Reference:

Explanation:

Assign a mount point folder path to a drive

You can use Disk Management to assign a mount-point folder path (rather than a drive letter) to the drive.

Mount-point folder paths are available only on empty folders on basic or dynamic NTFS volumes. Backup Operator or Administrator is the minimum membership required.

Assigning a mount-point folder path to a drive

1. In Disk Manager, right-click the partition or volume where you want to assign the mount-point folder path, and then click Change Drive Letter and Paths.

2. Do one of the following:

To assign a mount-point folder path, click Add. Click Mount in the following empty NTFS folder, type the path to an empty folder on an NTFS volume, or click Browse to locate it. To remove the mount-point folder path, click it and then click Remove.

Additional considerations

If you are administering a local or remote computer, you can browse NTFS folders on that computer.

When assigning a mount-point folder path to a drive, use Event Viewer to check the system log for any Cluster service errors or warnings indicating mount point failures. These errors would be listed as ClusSvc in the Source column and Physical Disk Resource in the Category column.

Source:<http://technet.microsoft.com/en-us/library/cc753321.aspx>

#### QUESTION 71

You manage a Web server named Server1 that runs Windows Server 2008 R2. Server1 has five application pools. You need to recycle one application pool without affecting the other application pools. Which tool should you use?

- A. Internet Information Services (IIS) Manager
- B. Telnet
- C. Windows Firewall
- D. Performance Monitor
- E. Ftp
- F. Services
- G. Internet Information Services (IIS) 6.0 Manager
- H. Security Configuration Wizard (SCW)
- I. Iisreset
- J. Component Services
- K. Local Security Policy
- L. System Configuration

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 72**

You manage a Web server named Server1 that runs Windows Server 2008 R2. Server1 has the FTP Server role service installed.

You need to manage the FTP server settings on Server1.

Which tool should you use?

- A. Services
- B. Local Security Policy
- C. Performance Monitor
- D. Internet Information Services (IIS) Manager
- E. Ftp
- F. System Configuration
- G. Iisreset
- H. Component Services
- I. Telnet
- J. Windows Firewall
- K. Security Configuration Wizard (SCW)
- L. Internet Information Services (IIS) 6.0 Manager

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 73**

Your network contains a Web server named Server1 that runs Windows Server 2008 R2. Server1 contains a Web site named Site1. Site1 contains a Web page named Priv.aspx.

The Web page is stored on a FAT partition.

You need to ensure that only a user named User1 can access Priv.aspx. All other content on Site1 must be accessible to everyone.

Which feature should you configure from Internet Information Services (IIS) Manager?

- A. Authorization Rules
- B. ISAPI and CGI Restrictions
- C. Authentication
- D. Connection Strings
- E. IP Address and Domain Restrictions
- F. HTTP Response Headers
- G. Management Service
- H. Error Pages
- I. HTTP Redirect
- J. ISAPI Filters
- K. Worker Processes
- L. Feature Delegation
- M. Request Filtering
- N. IIS Manager Permissions
- O. SSL Settings
- P. Default Document

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Ref:<http://www.iis.net/ConfigReference/system.webServer/security/authorization>

#### QUESTION 74

Your network contains a server named Server1 that runs Windows Server 2008 R2.

You need to ensure that an administrator is notified by e-mail if the Event Viewer logs any error.

What should you do from the Event Viewer console?

- A. From the System log, select an Error event, and then click the Attach Task to This Event action.
- B. Create a custom view, and then click the Attach Task to This Custom view action.
- C. Create a custom view, and then click the Filter Current Custom view action.
- D. From the System log, click the Filter Current Log action.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 75

You perform a security audit of a server named DC1. You install the Microsoft Network Monitor 3.0 application on DC1.

You plan to capture all the LDAP traffic that comes to and goes from the server between 20:00 and 07:00 the next day and save it to the E:\data.cap file.

You create a scheduled task. You add a new Start a program action to the task.

You need to add the application name and the application arguments to the new action.

What should you do?

- A. Add nmcap.exe as the application name. Add the /networks \* /capture LDAP /file e:\data.cap /stopwhen / timeafter 11hours line as arguments.
- B. Add netmon.exe as the application name. Add the /networks \*/capture LDAP /file e:\data.cap /stopwhen / timeafter 11hours line as arguments.
- C. Add nmcap.exe as the application name. Add the /networks \* /capture !LDAP /file e:\data.cap / stopwhen / timeafter 11hours line as arguments.
- D. Add nmconfig.exe as the application name. Add the /networks \* /capture &LDAP /file e:\data.cap / stopwhen /timeafter 11hours line as arguments.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 76**

Your company has a network that has 100 servers. You install a new server that runs Windows Server 2008 R2. The server has the Web Server (IIS) server role installed.

After a week, you discover that the Reliability Monitor has no data, and that the Systems Stability chart has never been updated.

You need to configure the server to collect the Reliability Monitor data.

What should you do?

- A. Run the perfmon.exe /sys command on the server.
- B. Configure the Secondary Logon service to start automatically.
- C. Configure the Remote Registry service to start automatically.
- D. Configure the Task Scheduler service to start automatically.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 77**

Your network contains an Active directory domain named fabrikam.com. The domain contains a Web server named Web1 that runs Windows Server 2008 R2. Web1 contains three Web sites

named Corp, Sales, and Marketing.

You discover that the CPU utilization of Web1 is abnormally high.

You need to identify the amount of memory that each Web site is using.

Which tool should you use?

- A. Component Services
- B. Internet Information Services (IIS) Manager
- C. System Configuration
- D. Performance Monitor

**Correct Answer: B**

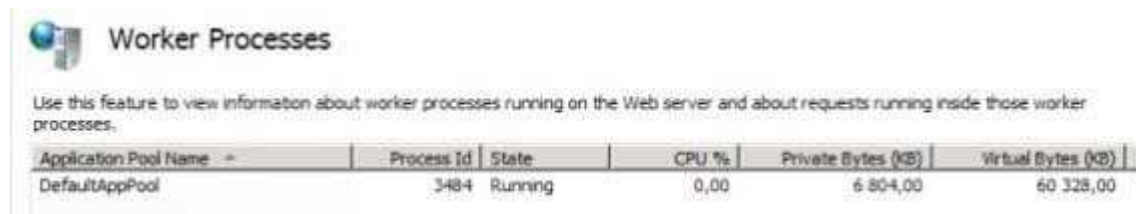
**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Performance Monitor - it is not better tool than IIS Manager, because it provides same functionality as "Worker processes" tab in IIS Manager, but in Performance Monitor you need to configure list of counters before you see their values unlike as in IIS Manager, which displays all application pools and they cpu usage in one click. PS. "Web site" is not equal to "application pool", therefore you need to assign separate application pools for each web site.



Application Pool Name	Process Id	State	CPU %	Private Bytes (KB)	Virtual Bytes (KB)
DefaultAppPool	3484	Running	0,00	6.804,00	60.328,00

#### QUESTION 78

Your network contains a server named Server1 that runs Windows Server 2008 R2.

You need to configure Server1 as a Key Management Service (KMS) host.

What should you do first?

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

To install a KMS host on a Windows Vista or Windows Server 2008 computer

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

5. After activation is complete, restart the Software Licensing Service using the Service application

Source:[http://technet.microsoft.com/en-us/library/cc303280.aspx#\\_Install\\_KMS\\_Hosts](http://technet.microsoft.com/en-us/library/cc303280.aspx#_Install_KMS_Hosts)

#### **QUESTION 79**

Your network contains two servers that run Windows Server 2008 R2. The servers are located on different IP subnets.

You plan to configure the servers in a two-node failover cluster.

You need to select the quorum model for the cluster. The solution must ensure that users can access the cluster resources if a single node fails.

Which quorum model should you select?

- A. Node and Disk Majority
- B. Node Majority
- C. No Majority: Disk Only
- D. Node and File Share Majority

**Correct Answer: D**

**Section: (none)**

**Explanation**

#### **Explanation/Reference:**

Explanation:

Quorum configuration choices

You can choose from among four possible quorum configurations:

Node Majority(recommended for clusters with an odd number of nodes) Can sustain failures of half the nodes (rounding up) minus one. For example, a seven node cluster can sustain three node failures.

Node and Disk Majority(recommended for clusters with an even number of nodes) Can sustain failures of half the nodes (rounding up) if the disk witness remains online. For example, a six node cluster in which the disk witness is online could sustain three node failures. Can sustain failures of half the nodes (rounding up) minus one if the disk witness goes offline or fails. For example, a six node cluster with a failed disk witness could sustain two ( $3-1=2$ ) node failures. Node and File Share Majority(for clusters with special configurations) Works in a similar way to Node and Disk Majority, but instead of a disk witness, this cluster uses a file share witness. Note that if you use Node and File Share Majority, at least one of the available cluster nodes must contain a current copy of the cluster configuration before you can start the cluster. Otherwise, you must force the starting of the cluster through a particular node. For more information, see "Additional considerations" in Start or Stop the Cluster Service on a Cluster Node. No Majority: Disk Only(not recommended) Can sustain failures of all nodes except one (if the disk is online). However, this configuration is not recommended because the disk might be a single point of failure.

Illustrations of quorum configurations

The following illustrations show how three of the quorum configurations work. A fourth configuration is described in words, because it is similar to the Node and Disk Majority configuration illustration.

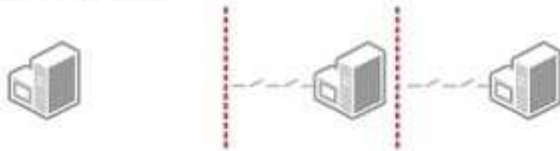
Note:

In the illustrations, for all configurations other than Disk Only, notice whether a majority of the relevant elements are in communication (regardless of the number of elements). When they are, the cluster continues to function. When they are not, the cluster stops functioning.

Two nodes out of three in communication:  
the cluster runs

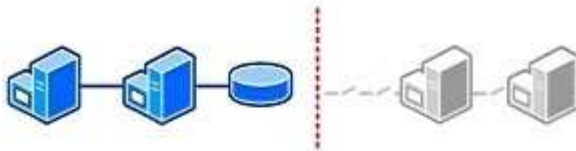


Individual nodes not in communication:  
the cluster stops

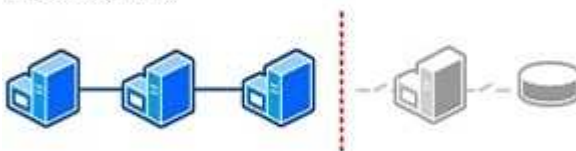


As shown in the preceding illustration, in a cluster with the Node Majority configuration, only nodes are counted when calculating a majority.

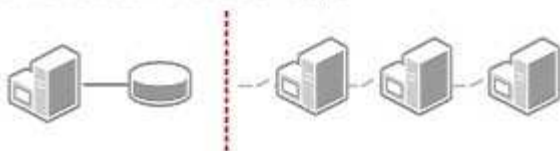
Two out of four nodes and witness disk in  
communication: the cluster runs



Three out of four nodes in communication:  
the cluster runs



Only one out of four nodes and witness disk in  
communication: the cluster stops



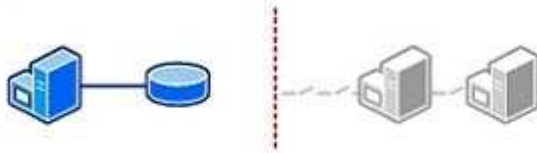
As shown in the preceding illustration, in a cluster with the Node and Disk Majority configuration, the nodes and the disk witness are counted when calculating a majority.

#### Node and File Share Majority Quorum Configuration

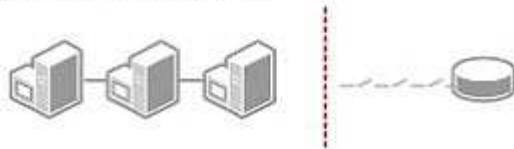
In a cluster with the Node and File Share Majority configuration, the nodes and the file share witness are counted when calculating a majority. This is similar to the Node and Disk Majority quorum configuration shown in the previous illustration, except that the witness is a file share that all nodes in the cluster can access instead of a disk in cluster storage.



One node and the disk in communication: the cluster runs



All nodes communicating, but no communication with the disk: the cluster stops



In a cluster with the Disk Only configuration, the number of nodes does not affect how quorum is achieved. The disk is the quorum. However, if communication with the disk is lost, the cluster becomes unavailable.

Source: <http://technet.microsoft.com/en-us/library/cc731739.aspx>

## QUESTION 80

Your company has a main office and five branch offices that are connected by WAN links. The company has an Active Directory domain named contoso.com. Each branch office has a member server configured as a DNS server. All branch office DNS servers host a secondary zone for contoso.com.

You need to configure the contoso.com zone to resolve client queries for at least four days in the event that a WAN link fails.

What should you do?

- A. Configure the Expires after option for the contoso.com zone to 4 days.
- B. Configure the Retry interval option for the contoso.com zone to 4 days.
- C. Configure the Refresh interval option for the contoso.com zone to 4 days.
- D. Configure the Minimum (default) TTL option for the contoso.com zone to 4 days.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

<http://technet.microsoft.com/en-us/library/bb727018.aspx>

## DNS Config

**Expires After** The period of time for which zone information is valid on the secondary server. If the secondary server can't download data from a primary server within this period, the secondary server lets the data in its cache expire and stops responding to DNS queries. Setting Expires After to seven days allows the data on a secondary server to be valid for seven days.

## QUESTION 81

Your company has an Active Directory domain named contoso.com. The company network has two DNS servers named DNS1 and DNS2.

The DNS servers are configured as shown in the following table:

DNS1	DNS2
_msdcs.contoso.com contoso.com	.(root) _msdcs.contoso.com contoso.com

Domain users, who are configured to use DNS2 as the preferred DNS server, are unable to connect to Internet Web sites.

You need to enable Internet name resolution for all client computers.

What should you do?

- A. Create a copy of the .(root) zone on DNS1.
- B. Update the list of root hints servers on DNS2.
- C. Update the Cache.dns file on DNS2. Configure conditional forwarding on DNS1.
- D. Delete the .(root) zone from DNS2. Configure conditional forwarding on DNS2.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 82

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1. Server1 has the Active Directory Federation Services (AD FS) role installed.

You have an application named App1 that is configured to use Server1 for AD FS authentication.

You deploy a new server named Server2. Server2 is configured as an AD FS 2.0 server.

You need to ensure that App1 can use Server2 for authentication.

What should you do on Server2?

- A. Create a relaying provider trust.
- B. Create a relaying party trust.<http://www.lead2pass.com/70-649.html>
- C. Add an attribute store.
- D. Create a claims provider trust.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

To create a relaying party trust manually

Click Start, point to Programs, point to Administrative Tools, and then click AD FS 2.0 Management.

Under AD FS 2.0\Trust Relationships, right-click Relying Party Trusts, and then click Add Relying Party Trust to open the Add Relying Party Trust Wizard.

On the Welcome page, click Start.

On the Select Data Source page, click Enter data about the relying party manually, and then click Next.

On the Specify Display Name page type a name in Display name, under Notes type a description for this relying party trust, and then click Next.

On the Choose Profile page, do one of the following:  
Click AD FS 2.0 profile, click Next, and then move to step 7.

Click AD FS 1.0 and 1.1 profile, click Next, and then go to step 9.

If you know you will require interoperability with older Active Directory Federation Services (AD FS) federation, as provided in Windows Server 2003 R2, click AD FS 1.0 and 1.1 profile. Otherwise, use the default AD FS 2.0 profile.

On the Configure Certificate page, click Browse to locate a certificate file, and then click Next.

On the Configure URL page, do one or both of the following, click Next, and then go to step 10:

Select the Enable support for the WS-Federation Passive protocol check box. Under Relying party WS-Federation Passive protocol URL, type the URL for this relying party trust, and then click Next.

Select the Enable support for the SAML 2.0 WebSSO protocol check box. Under Relying party SAML 2.0 SSO service URL, type the Security Assertion Markup Language (SAML) service endpoint URL for this relying party trust, and then click Next.

Click the Help button on this page for more information about which of these options apply to the needs of your organization.

On the Configure URL page, under WS-Federation Passive URL, type the URL for this relying party trust, and then click Next.

On the Configure Identifiers page, specify one or more identifiers for this relying party, click Add to add them to the list, and then click Next.

On the Choose Issuance Authorization Rules page, select either Permit all users to access this relying party or Deny all users access to this relying party, and then click Next.

On the Ready to Add Trust page, review the settings, and then click Next to save your relying party trust information.

On the Finish page, click Close. This action automatically displays the Edit Claim Rules dialog box. For more information about how to proceed with adding claim rules for this relying party trust, see Additional references.

### QUESTION 83

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

The network has a branch office site that contains a read-only domain controller (RODC) named RODC1. RODC1 runs Windows Server 2008 R2.

A user logs on to a computer in the branch office site.

You discover that the user's password is not stored on RODC1.

You need to ensure that the user's password is stored on RODC1 when he logs on to a branch office site computer.

What should you do?

- A. Add RODC1's computer account to the built-in Allowed RODC Password Replication Group on RODC1.
- B. Modify the RODC's password replication policy by removing the entry for the Allowed RODC Password Replication Group.
- C. Modify the RODC's password replication policy by adding RODC1's computer account to the list of allowed users, groups, and computers.
- D. Add the user's user account to the built-in Allowed RODC Password Replication Group on RODC1.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 84**

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**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

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 licenser certificate, of the AD RMS installation to trust, to the trusting AD RMS installation.

**QUESTION 85**

Your network contains a server named Server1 that runs Windows Server 2008 R2.

You create an Active Directory Lightweight Directory Services (AD LDS) instance on Server1.

You need to create an additional AD LDS application directory partition in the existing instance.

Which tool should you use?

- A. Dsmod
- B. Ldp
- C. Dsadd
- D. Adaminstall

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

## Exam C

### QUESTION 1

Your network contains two servers named Server1 and Server2 that run Windows Server 2008 R2. Server1 has the Active Directory Federation Services (AD FS) Federation Service role service installed.

You plan to deploy AD FS 2.0 on Server2.

You need to export the token-signing certificate from Server1, and then import the certificate to Server2.

Which format should you use to export the certificate?

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation: [http://technet.microsoft.com/en-us/library/cc784075\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc784075(v=ws.10).aspx)

Every federation server in an Active Directory Federation Services (ADFS) server farm must have access to the private key of the token-signing certificate. If you are implementing a server farm of federation servers that share a single, exportable private key certificate that is issued by an enterprise certification authority (CA), the private key portion of the existing token-signing certificate must be exported to make it available for importing into the certificate store on the new server.

### QUESTION 2

Your company has a main office and 40 branch offices. Each branch office is configured as a separate Active Directory site that has a dedicated read-only domain controller (RODC).

An RODC server is stolen from one of the branch offices.

You need to identify the user accounts that were cached on the stolen RODC server.

Which utility should you use?

- A. Dsmode.exe
- B. Ntdsutil.exe
- C. Active Directory Sites and Services
- D. Active Directory Users and Computers

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 3

Your network contains a server named Server1 that runs Windows Server 2008 R2.

On Server1, you create an Active Directory Lightweight Directory Services (AD LDS) instance named Instance1.

You connect to Instance1 by using ADSI Edit.

You run the Create Object wizard and you discover that there is no User object class.

You need to ensure that you can create user objects in Instance1.

What should you do?

- A. Run the AD LDS Setup Wizard.
- B. Modify the schema of Instance1.
- C. Modify the properties of the Instance1 service.
- D. Install the Remote Server Administration Tools (RSAT).

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 4**

Your company has a server that runs Windows Server 2008 R2. The server runs an instance of Active Directory Lightweight Directory Services (AD LDS).

You need to replicate the AD LDS instance on a test computer that is located on the network.

<http://www.lead2pass.com/70-649.html>

What should you do?

- A. Run the repadmin /kcc <servername> command on the test computer.
- B. Create a naming context by running the Dsmgmt command on the test computer.
- C. Create a new directory partition by running the Dsmgmt command on the test computer.
- D. Create and install a replica by running the AD LDS Setup wizard on the test computer.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 5**

Your network contains an Active Directory domain named contoso.com. The network contains client computers that run either Windows Vista or Windows 7. Active Directory Rights Management Services (AD RMS) is deployed on the network.

You create a new AD RMS template that is distributed by using the AD RMS pipeline. The template is updated every month.

You need to ensure that all the computers can use the most up-to-date version of the AD RMS template. You want to achieve this goal by using the minimum amount of administrative effort.

What should you do?

- A. Upgrade all of the Windows Vista computers to Windows 7.
- B. Upgrade all of the Windows Vista computers to Windows Vista Service Pack 2 (SP2).

- C. Assign the Microsoft Windows Rights Management Services (RMS) Client Service Pack 2 (SP2) to all users by using a Software Installation extension of Group Policy.
- D. Assign the Microsoft Windows Rights Management Services (RMS) Client Service Pack 2 (SP2) to all computers by using a Software Installation extension of Group Policy.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 6**

Your network contains a single Active Directory domain. Active Directory Rights Management Services (AD RMS) is deployed on the network.

A user named User1 is a member of only the AD RMS Enterprise Administrators group.

You need to ensure that User1 can change the service connection point (SCP) for the AD RMS installation. The solution must minimize the administrative rights of User1.



<http://www.gratisexam.com/>

To which group should you add User1?

- A. AD RMS Auditors
- B. AD RMS Service Group
- C. Domain Admins
- D. Schema Admins

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

The AD RMS SCP can be registered automatically during AD RMS installation, or it can be registered after installation has completed.

To register the SCP you must be a member of the local **AD RMS Enterprise Administrators group** and the **Active Directory Domain Services (AD DS) Enterprise Admins group**, or you must have been given the appropriate authority.

If the user account installing AD RMS does not have permission to register the SCP you will see an Event ID: 190 in the Event Viewer .

You can manually register the SCP in the AD RMS console.

Open SCP tab in the cluster's Properties box and select the Change SCP check box.

#### **QUESTION 7**

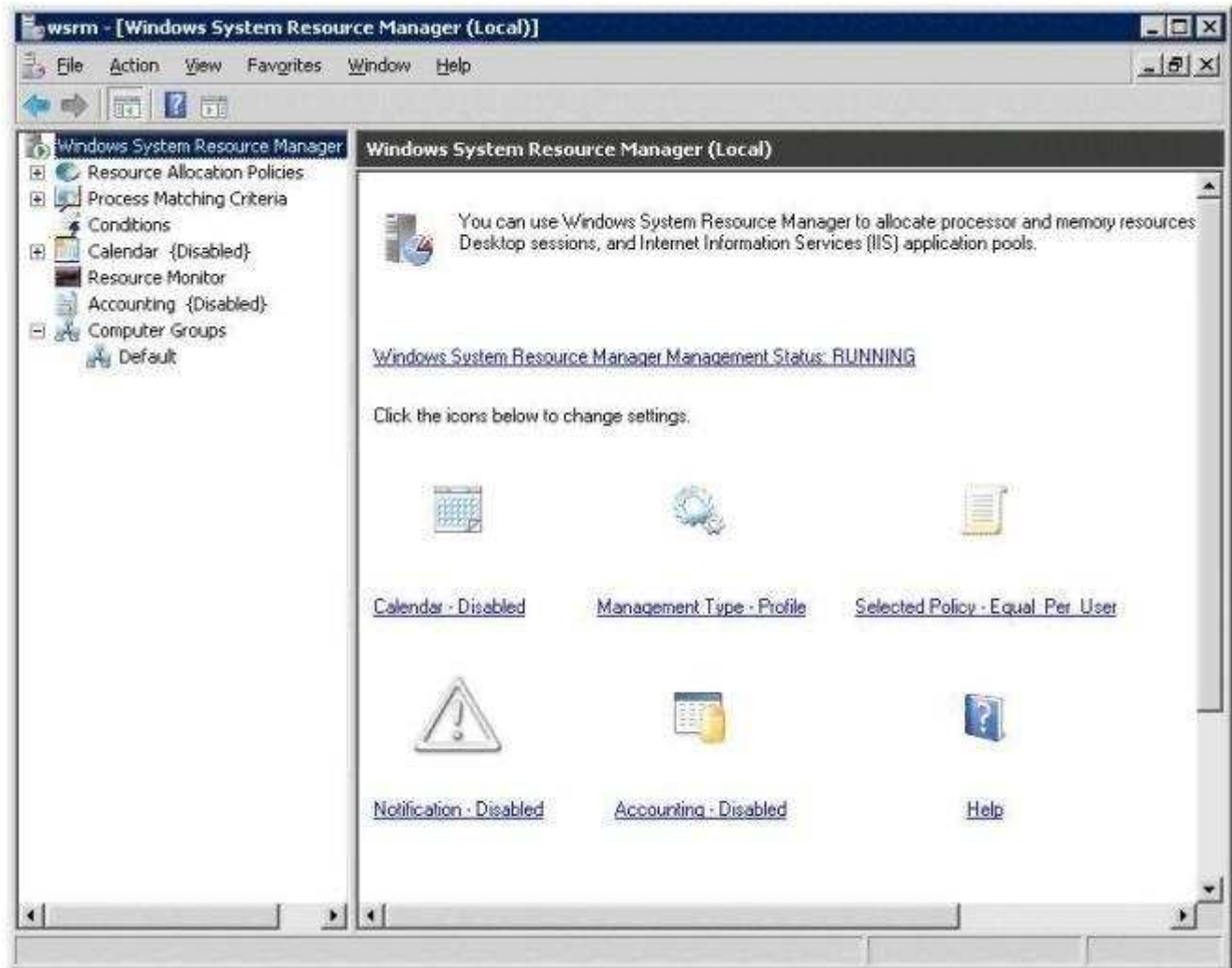
Your network contains a server named Server1 that runs Windows Server 2008 R2. Server 1 has the Remote Desktop Session Host (RD Session Host) role service installed.

On server1, you install and configure the Windows System Resource Manager (WSRM) feature as shown in the exhibit. (Click the Exhibit button.)

You need to ensure that WSRM enforces the allocation of CPU capacity between users.

What should you do?

**Exhibit:**



- A. Enable Accounting.
- B. Change the Management type to Manage.
- C. Add Server1 to the Default computer group.
- D. Change the resource allocation policy to Equal\_per\_process.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 8**

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



the following table.

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

The network contains 100 client computers that connect to Remote Desktop Services (RDS) on Server2. Server1 has 100 Remote Desktop Services Per Device client access licenses (RDS Per Device CALs) installed.

You exchange 10 client computers for 10 new client computers.

You need to ensure that the RDS Per Device CALs allocated to the old client computers can be immediately reallocated to the new client computers.

What should you do?

- A. From the Remote Desktop Session Host Configuration console on Server2, modify the Licensing settings.
- B. From the Remote Desktop Licensing Manager tool on Server1, run the Manage RDS CALs wizard and click the Migrate action.
- C. From the Remote Desktop Licensing Manager tool on Server1, navigate to the Windows Server 2008 R2 - Installed RDS Per Device CALs node and run the Install Licenses wizard.
- D. From the Remote Desktop Licensing Manager tool on Server1, navigate to the Windows Server 2008 R2 - Installed RDS Per Device CALs node and click the Revoke RDS CAL action.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Revoke a Remote Desktop Services Per Device Client Access License When a Remote Desktop Session Host (RD Session Host) server is configured to use Per Device licensing mode, and a client computer or device connects to an RD Session Host server for the first time, the client computer or device is issued a temporary license by default. When a client computer or device connects to an RD Session Host server for the second time, if the Remote Desktop license server is activated and enough RDS Per Device CALs are available, the license server issues the client computer or device a permanent RDS Per Device CAL. If the license server is not activated or does not have any RDS Per Device CALs available, the device continues to use the temporary license. The temporary license is valid for 90 days. In some circumstances, you might want or need to return an RDS Per Device CAL that has been issued back to the available pool on the license server before the automatic expiration period has been reached. For example, you might want to do this if the client computer or device is no longer a part of your environment.

You can revoke an RDS Per Device CAL by using the Remote Desktop Licensing Manager tool. After you have revoked the RDS Per Device CAL, that RDS Per Device CAL is immediately available to be issued to another client computer or device. Revocation is not a substitute for ensuring that you have enough RDS Per Device CALs to support your environment. You can only revoke up to twenty percent of the number of RDS Per Device CALs of a particular version installed on your license server.

Source:<http://technet.microsoft.com/en-us/library/cc732416.aspx>

**QUESTION 9**

Your network contains a Remote Desktop server. The server hosts 10 RemoteApp programs. You need to configure a digital signature for the RemoteApp programs.

What should you modify?

- A. the Remote Desktop connection authorization policies (RD CAPs)

- B. the Remote Desktop resource authorization policies (RD RAPs)
- C. the RemoteApp and Desktop Connection properties
- D. the RemoteApp Deployment Settings

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

To configure the digital certificate to use

In the Actions pane of Gestionnaire RemoteApp TS, click Digital Signature Settings. (Or, in the Overview pane, next to Digital Signature Settings, click Change.)

Select the Sign with a digital certificate check box.

In the Digital certificate details box, click Change.

In the Select Certificate dialog box, select the certificate that you want to use, and then click OK

#### **QUESTION 10**

Your network contains a server that has the Remote Desktop Session Host (RD Session Host) role service installed.

You need to prevent administrators from logging other administrators off of the console session.

<http://www.lead2pass.com/70-649.html>

What should you do?

- A. From the RDP-Tcp properties of the RD Session Host server, modify the Client Settings.
- B. From the RDP-Tcp properties of the RD Session Host server, modify the Sessions settings.
- C. From the Computer Configuration Group Policy settings, modify the Remote Desktop Session Host settings.
- D. From the User Configuration Group Policy settings, modify the Remote Desktop Connection Client settings.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Connections

Policy settings in this node control connection settings on a Remote Desktop Session Host server.

The full path of this node in the Group Policy Management Console is

Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections.

Deny logoff of an administrator logged in to the console session

This policy setting determines whether an administrator attempting to connect remotely to the console of a server can log off an administrator currently logged on to the console.

This policy is useful when the currently connected administrator does not want to be logged off by another administrator. If the connected administrator is logged off, any data not previously saved is lost.

If you enable this policy setting, logging off the connected administrator is not allowed.

If you disable or do not configure this policy setting, logging off the connected administrator is allowed.

Note The console session is also known as Session 0. Console access can be obtained by using the /console switch from Remote Desktop Connection in the computer field name or from the command line

Source: <http://technet.microsoft.com/en-us/library/ee791922.aspx>

#### **QUESTION 11**

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Remote

Desktop Gateway (RD Gateway) role service installed.

You add the Domain Users group to a connection authorization policy named TS\_CAP\_01.

You need to ensure that only client computers that have Windows Firewall enabled can connect to Remote Desktop resources through the RD Gateway.

What should you do?

- A. From Remote Desktop Gateway Manager, modify the properties of the TS\_RAP\_01 resource authorization policy.
- B. From Remote Desktop Gateway Manager, modify the properties of the TS\_CAP\_01 connection authorization policy.
- C. From the Network Policy Server console, modify the properties of the TS\_CAP\_01 network policy.
- D. From the Network Policy Server console, modify the properties of the TS\_GATEWAY\_AUTHORIZATION\_POLICY connection request policy.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation: [http://technet.microsoft.com/en-us/library/cc754252\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc754252(v=ws.10).aspx)

1. Install the TS Gateway role service

Follow these steps to install the TS Gateway role service. Optionally, during the role service installation process, you can select an existing certificate (or create a new self-signed certificate), and you can create a TS CAP and a TS RAP.

To install the TS Gateway role service

Open Server Manager. To open Server Manager, click Start, point to Administrative Tools, and then click Server Manager.

If the Terminal Services role is not already installed:

In Server Manager, under Roles Summary, click Add roles.

In the Add Roles Wizard, if the Before You Begin page appears, click Next. This page will not appear if you have already installed other roles and you have selected the Skip this page by default check box.

On the Select Server Roles page, under Roles, select the Terminal Services check box, and then click Next.

On the Terminal Services page, click Next.

On the Select Role Services page, in the Role services list, select the TS Gateway check box.

If prompted to specify whether you want to install the additional role services required for TS Gateway, click Add Required Role Services.

On the Select Role Services page, confirm that TS Gateway is selected, and then click Next.

If the Terminal Services role is already installed:

Under Roles Summary, click Terminal Services.

Under Role Services, click Add Role Services.

On the Select Role Services page, select the TS Gateway check box, and then click Next.

If prompted to specify whether you want to install the additional role services required for TS Gateway, click Add Required Role Services.

On the Select Role Services page, click Next.

On the Choose a Server Authentication Certificate for SSL Encryption page, specify whether to choose an existing certificate for SSL encryption (recommended), create a self-signed certificate for SSL encryption, or choose a certificate for SSL encryption later. If you are completing an installation for a new server that does not yet have certificates, see 2. Obtain a certificate for the TS Gateway server for certificate requirements and information about how to obtain and install a certificate.

Under the Choose an existing certificate for SSL encryption (recommended) option, only certificates that have the intended purpose (server authentication) and Enhanced Key Usage (EKU) [Server Authentication (1.3.6.1.5.5.7.3.1)] that are appropriate for the TS Gateway role service will appear in the list of certificates. If you select this option, click Import, and then import a new certificate that does not meet these requirements, the imported certificate will not appear in the list.

On the Create Authorization Policies for TS Gateway page, specify whether you want to create authorization policies (a TS CAP and a TS RAP) during the TS Gateway role service installation process or later. If you select Later, follow the procedures in 4. Create a TS CAP for the TS Gateway server to create this policy. If you select Now, do the following:

On the Select User Groups That Can Connect Through TS Gateway page, click Add to specify additional user groups. In the Select Groups dialog box, specify the user group location and name, and then click OK as needed to check the name and to close the Select Groups dialog box.

To specify more than one user group, do either of the following: Type the name of each user group, separating the name of each group with a semi-colon; or add additional groups from different domains by repeating the first part of this step for each group.

After you finish specifying additional user groups, on the Select User Groups that Can Connect Through TS Gateway page, click Next.

On the Create a TS CAP for TS Gateway page, accept the default name for the TS CAP (TS\_CAP\_01) or specify a new name, select one or more supported Windows authentication methods, and then click Next.

On the Create a TS RAP for TS Gateway page, accept the default name for the TS RAP (TS\_RAP\_01) or specify a new name, and then do one of the following: Specify whether to allow users to connect only to computers in one or more computer groups, and then specify the computer groups; or specify that users can connect to any computer on the network. Click Next.

On the Network Policy and Access Services page (which appears if this role service is not already installed), review the summary information, and then click Next.

On the Select Role Services page, verify that Network Policy Server is selected, and then click Next.

On the Web Server (IIS) page (which appears if this role service is not already installed), review the summary information, and then click Next.

On the Select Role Services page, accept the default selections for Web Server (IIS), and then click Next.

On the Confirm Installation Options page, verify that the following roles, role services, and features will be installed:

Terminal Services\TS Gateway

Network Policy and Access Services\Network Policy Server

Web Server (IIS)\Web Server\Management Tools

RPC over HTTP Proxy

Windows Process Activation Service\Process Model\Configuration APIs

Click Install.

On the Installation Progress page, installation progress will be noted.

If any of these roles, role services, or features has already been installed, installation progress will be noted only for the new roles, role services, or features that are being installed.

On the Installation Results page, confirm that installation for these roles, role services, and features was successful, and then click Close.

## QUESTION 12

You have a Remote Desktop Services farm that contains several Remote Desktop Session Host Servers.

You need to configure one of the Remote Desktop Session Host Servers as a dedicated redirector.

You configure the appropriate DNS records.

What should you do next?

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 13**

Your network contains a Web server that runs Windows Server 2008 R2. The Web server has a Web site named Web1. Web1 hosts several HTML Web pages located in the C:\inetpub\wwwroot folder,

Windows authentication is enabled for Web1.

You need to prevent some users from accessing one of the HTML Web pages.

What should you do?

- A. From Windows Explorer, modify the NTFS permissions.<http://www.lead2pass.com/70-649.html>
- B. From Windows Explorer, modify the share permissions.
- C. From Internet Information Services (IIS) Manager, modify the Authentication settings.
- D. From Internet Information Services (IIS) Manager, modify the Request Filtering settings.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 14**

Your network contains a Web site named Web1. Web1 is configured to use an application pool named AppPool1.

You need to ensure that the memory used by the Web site is released every 12 hours. The solution must minimize the amount of downtime for the Web site.

What should you do?

- A. Modify the recycling settings for AppPool1.
- B. Modify the session state settings for Web1.
- C. Create a scheduled task that runs `tskill.exe w3svc.exe`.
- D. Create a scheduled task that runs `iisreset.exe /noforce`.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 15**

Your company hosts a Web site on a server that runs Windows Server 2008 R2. The server has the Web Server (IIS) server role installed. SSL is configured on the Web site for virtual directories that require encryption.

You are implementing a new Web application on the Web site. The new application has its own logon page named User1ogin.aspx. You enable Forms Authentication in the Web site properties.

You need to configure the Web site to use User1ogin.aspx to authenticate user accounts.

What should you do?

- A. Configure the Forms Authentication Settings to Require SSL.
- B. Configure the Name property of the Cookie Settings to the User1ogin.aspx filename.
- C. Configure the Login URL property for the Forms Authentication Settings to the User1ogin.aspx filename.
- D. Configure the Default Document setting to add the User1ogin.aspx filename in the Web site properties.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

<http://www.lead2pass.com/70-649.html>

#### **QUESTION 16**

Your network contains a server that runs Windows Server 2008 R2. The server has the Web Server (IIS) role installed.

The server has a Web application that uses HTTP. All authentication methods are enabled for the Web application.

You need to prevent passwords from being sent over the network in clear text.

Which two authentication methods should you disable? (Each correct answer presents part of the solution. Choose two.)

- A. Anonymous
- B. Basic
- C. Digest
- D. Forms
- E. Windows Integrated

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Configure Basic Authentication (IIS 7)

Basic authentication requires that users provide a valid user name and password to access content. This authentication method does not require a specific browser, and all major browsers support it. Basic authentication also works across firewalls and proxy servers. For these reasons, it is a good choice when you want to restrict access to some, but not all, content on a server.

However, the disadvantage of Basic authentication is that it transmits unencrypted base64- encoded passwords across the network. You should use Basic authentication only when you know that the connection between the client and the server is secure. The connection should be established either over a dedicated line or by using Secure Sockets Layer (SSL) encryption and Transport Layer Security (TLS). For example, to use Basic authentication with Web Distributed Authoring and Versioning (WebDAV), you should configure SSL encryption.

[http://technet.microsoft.com/en-us/library/cc772009\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc772009(WS.10).aspx) Configuring Forms Authentication (IIS 7)

Forms authentication uses client-side redirection to forward unauthenticated users to an HTML form where they can enter their credentials, which are usually a user name and password. After the credentials are validated, users are redirected to the page they originally requested. Because Forms authentication sends the user name and password to the Web server as plain text, you should use Secure Sockets Layer (SSL) encryption for the logon page and for all other pages in your application except the home page.

[http://technet.microsoft.com/en-us/library/cc771077\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc771077(WS.10).aspx) Check this link on MSDN for a nice comparison of all authentication methods:

<http://msdn.microsoft.com/en-us/library/aa292114.aspx>

#### **QUESTION 17**

Your network contains an FTP server named Server1. Server1 has an FTP site named FTP1.

You need to hide all of the files in FTP1 that have an .exe file extension. The solution must ensure that users can list other files in FTP1.

What should you modify?

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 18**

Your network contains two standalone servers named Server1 and Server2. Server1 has Microsoft SQL Server 2008 Reporting Services installed. Server2 has the SMTP Server feature installed.

You configure the Reporting Services on Server1 to send reports by using Server2.

You need to ensure that Server2 sends the reports.

What should you do on Server2?

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

**Correct Answer: C**

**Section: (none)**

## Explanation

### Explanation/Reference:

Explanation:

To change the SMTP Virtual Server Relay Restrictions, one needs to use the Internet Information Servers (IIS) 6.0 Manager.

This is an IIS Role Service that needs to be installed (IIS 6 Management Console)

### QUESTION 19

Your network contains a Web server that runs Windows Server 2008 R2. You need to back up all Web site content.

Which tool should you use?

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

**Correct Answer: D**

**Section: (none)**

### Explanation

### Explanation/Reference:

Explanation:

Wbadmin

Backups are usually done with Windows Server Backup;

Wbadmin is the command-line counterpart to Windows Server Backup. You use Wbadmin to manage all aspects of backup configuration that you would otherwise manage in Windows Server Backup. This means that you can typically use either tool to manage backup and recovery. Source: <http://technet.microsoft.com/en-us/magazine/dd767786.aspx> To not only backup the website content but also the IIS configuration backup the systemstate:

The -systemState parameter:

For Windows7 and Windows Server 2008 R2, creates a backup that includes the system state in addition to any other items that you specified with the -include parameter. The system state contains boot files (Boot.ini, NTLDR, NTDetect.com), the Windows Registry including COM settings, the SYSVOL (Group Policies and Logon Scripts), the Active Directory and NTDS.DIT on Domain Controllers and, if the certificates service is installed, the Certificate Store. If your server has the Web server role installed, the IIS Metadirectory will be included. If the server is part of a cluster, Cluster Service information will also be included.

Source: [http://technet.microsoft.com/en-us/library/cc742083\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc742083(WS.10).aspx)

Appcmd

The backup feature of Appcmd only backs up the configuration of the IIS server, not the websites:

After you install IIS 7.0, you can backup your configuration by using the built-in command-line tool,

AppCmd.exe. You can run AppCmd.exe to create a backup of your Web server before you have changed any configuration.

Files configuration IIS server:

Administration.config

ApplicationHost.config

Redirection.config

MBSchema.xml

MetaBase.xml

To create a backup using AppCmd.exe



1. Open a command prompt as administrator and change to the %windir%\system32\inetsrv\ directory.
2. At the command prompt, type appcmd add backup "FirstBackup" and then press Enter.
3. This creates a backup with the name "FirstBackup". At a later date, if you need to restore the backup, use appcmd restore backup "FirstBackup"

Source:<http://learn.iis.net/page.aspx/199/create-a-backup-with-appcmd/>

#### QUESTION 20

Your network contains a Web server named Server1 that runs Windows Server 2008 R2.

Server1 contains a Web site named Web1. Users access Web1 by using the URL <http://www.contoso.com>.

You plan to request a SSL certificate for Web1 from a trusted certification authority (CA).

You need to create a certificate request for Web1. The solution must ensure that users do not receive certificate-related error messages when they access the Web site.

What should you specify as the common name value in the certificate request?

- A. Server1.contoso.com
- B. web1
- C. www
- D. www.contoso.com

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 21

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

Disk name	Disk size	Volume name
Disk0	50 GB	C
Disk1	50 GB	D
Disk2	100 GB	None

Volume D contains shared files and applications.

You plan to install an application named App1 on the server. App1 must be installed in D:\Appl. App1 requires 75 GB of disk space.

You need to ensure that the server can support the planned installation of Appl. The solution must minimize the impact on all users.

What should you do?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Assign a mount point folder path to a drive

You can use Disk Management to assign a mount-point folder path (rather than a drive letter) to the drive.

Mount-point folder paths are available only on empty folders on basic or dynamic NTFS volumes. Backup Operator or Administrator is the minimum membership required.

Assigning a mount-point folder path to a drive

1. In Disk Manager, right-click the partition or volume where you want to assign the mount-point folder path, and then click Change Drive Letter and Paths.

2. Do one of the following:

To assign a mount-point folder path, click Add. Click Mount in the following empty NTFS folder, type the path to an empty folder on an NTFS volume, or click Browse to locate it. To remove the mount-point folder path, click it and then click Remove.

Source:<http://technet.microsoft.com/en-us/library/cc753321.aspx>

**QUESTION 22**

Your network contains two servers named Server1 and Server2 that run Windows Server 2008 R2. Server1 and Server2 are configured as a failover cluster named Cluster1.

Cluster1 hosts a clustered application named App1. App1 has a physical disk resource named Cluster Disk 1.

You need to use the Chkdsk tool to fix all of the errors on Cluster Disk 1.

What should you do first?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Run a Disk Maintenance Tool Such as Chkdsk on a Clustered Disk To run a disk maintenance tool such as Chkdsk on a disk or volume that is configured as part of a clustered service, application, or virtual machine, you must use maintenance mode. When maintenance mode is on, the disk maintenance tool can finish running without triggering a failover. If you have a disk witness, you cannot use maintenance mode for that disk.

Maintenance mode works somewhat differently on a volume in Cluster Shared Volumes than it does on other disks in cluster storage, as described in Additional considerations, later in this topic. Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure

To run a disk maintenance tool such as Chkdsk on a clustered disk

1. In the Failover Cluster Manager snap-in, if the cluster is not displayed, in the console tree, right-click Failover Cluster Manager, click Manage a Cluster, and select or specify the cluster you want.

2. If the console tree is collapsed, expand the tree under the cluster that uses the disk on which you want run a disk maintenance tool.

3. In the console tree, click Storage.

4. In the center pane, click the disk on which you want to run the disk maintenance tool.

5. Under Actions, click More Actions, and then click the appropriate command:

If the disk you clicked is under Cluster Shared Volumes and contains multiple volumes, click Maintenance, and then click the command for the appropriate volume. If prompted, confirm your action.

If the disk you clicked is under Cluster Shared Volumes and contains one volume, click Maintenance, and then click Turn on maintenance mode for this volume . If prompted, confirm your action.

If the disk you clicked is not under Cluster Shared Volumes, click Turn on maintenance mode for this disk.

6. Run the disk maintenance tool on the disk or volume. When maintenance mode is on, the disk maintenance tool can finish running without triggering a failover.

7. When the disk maintenance tool finishes running, with the disk still selected, under Actions, click More Actions, and then click the appropriate command:

If the disk you clicked is under Cluster Shared Volumes and contains multiple volumes, click Maintenance, and then click the command for the appropriate volume. If the disk you clicked is under Cluster Shared Volumes and contains one volume, click Maintenance, and then click Turn off maintenance mode for this volume. If the disk you clicked is not under Cluster Shared Volumes, click Turn off maintenance mode for this disk.

Source:<http://technet.microsoft.com/en-us/library/cc772587.aspx>

### QUESTION 23

You have two servers that run Windows Server 2008 R2 Enterprise. Both servers have the Failover Clustering feature installed. You configure the servers as a two-node cluster. The cluster nodes are named NODE1 and NODE2.

You have an application named PrintService that includes a print spooler resource.

You need to configure the cluster to automatically return the PrintService application to NODE1 after a failover.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

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

**Correct Answer:** BC

**Section:** (none)

**Explanation**

#### Explanation/Reference:

Explanation:

Preferred nodes list defined

If you define a complete preferred nodes list for a group (that is, one listing all the nodes in the cluster), then the Cluster service uses this defined list as its internal list. However, if you define a partial preferred nodes list for a group, then the Cluster service uses this defined list as its internal list and appends any other installed nodes not on the preferred list, ordered by their node IDs. For example, if you created a 5-node cluster (installing the nodes in the order Node1, Node2, Node3, Node4, and Node5) and defined Node3, Node4, and Node5 as preferred owners for the resource group, PRINTGR1, the Cluster service would maintain this ordered list for PRINTGR1: Node3, Node4, Node5, Node1, Node2. How the Cluster service uses this list depends on whether the resource group move is due to a resource/node failure or a manual move group request.

Preferred lists and resource or node failures

For resource group or node failures, the group fails over to the node next to the current owner on the preferred nodes list. In the example above, if the resource group PRINTGR1 on Node3 fails, then the Cluster service would fail that group over to the next node on the list, Node4. If you allow fallback for that group, then when Node3 comes up again, the Cluster service will fail back PRINTGR1 to that node.

Source:<http://technet.microsoft.com/en-us/library/cc737785.aspx>

### QUESTION 24

Your network contains an Active Directory domain named contoso.com- All servers run Windows Server 2008 R2.

A server named Server1 has the Windows Deployment Services (WDS) server role installed. A custom

Windows 7 image is available for download from Server1.

A server named Server2 has the Hyper-V server role installed.

You create a virtual machine (VM) named VM1 on Server2.

You need to deploy the Windows 7 image from Server1 to VM1.

What should you do first?

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 25**

Your company has a single Active Directory domain. The company network is protected by a firewall.

Remote users connect to your network through a VPN server by using PPTP.

When the users try to connect to the VPN server, they receive the following error message:

"Error 721: The remote computer is not responding."

You need to ensure that users can establish a VPN connection.

What should you do?

- A. Open port 3389 on the firewall.
- B. Open port 1723 on the firewall.
- C. Open port 1423 on the firewall.
- D. Open port 6000 on the firewall.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

You need to make sure TCP port 1723 (for PPTP) or UDP port 500 (for IPsec) is open for the VPN to communicate through the firewall.

#### **QUESTION 26**

Your company's corporate network uses Network Access Protection (NAP).

Users are able to connect to the corporate network remotely.

You need to ensure that data transmissions between remote client computers and the corporate network are as secure as possible.

What should you do?

- A. Apply an IPsec NAP policy.
- B. Restrict Dynamic Host Configuration Protocol (DHCP) clients by using NAP.
- C. Configure a NAP policy for 802.1X wireless connections.
- D. Configure VPN connections to use MS-CHAP v2 authentication.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 27**

Your company has a main office and a branch office. The branch office has three servers that run a Server Core installation of Windows Server 2008 R2.

The servers are named Server1, Server2, and Server3.

You want to configure the Event Logs subscription on Server1 to collect events from Server2 and Server3.

You discover that you cannot create a subscription on Server1 from another computer.

You need to configure a subscription on Server1.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Run the `wecutil cs subscription.xml` command on Server1.
- B. Create a custom view on Server1 by using Event Viewer.  
Export the custom view to a file named `subscription.xml`.
- C. Create an event collector subscription configuration file.  
Name the file `subscription.xml`.
- D. Run the `wevtutil im subscription.xml` command on Server1.

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 28**

Your network contains 100 servers that run Windows Server 2008 R2.

A server named Server1 is deployed on the network. Server1 will be used to collect events from the Security event logs of the other servers on the network.

You need to define the Custom Event Delivery Optimization settings on Server1.

Which tool should you use?

- A. Wevtutil
- B. Wecutil
- C. Task Scheduler
- D. Event Viewer

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Wecutil.exe is a Windows Eventviewer Collector utility that enables an administrator to create and manage subscriptions to events forwarded from remote event sources that support the WS-Management protocol. Commands, options, and option values are case-insensitive for this utility.

**QUESTION 29**

Your network consists of a single Active Directory domain. All servers run Windows Server 2008 R2. You have a server named Server1 that hosts shared documents. Users report extremely slow response times when they try to open the shared documents on Server1.

You log on to Server1 and observe real-time data indicating that the processor is operating at 100 percent of capacity.

You need to gather additional data to diagnose the cause of the problem.

What should you do?

- A. In Event viewer, open and review the application log for Performance events.
- B. In Resource Monitor, use the Resource view to see the percentage of processor capacity used by each application.
- C. In Performance Monitor, create performance counter alert that will be triggered when processor usage exceeds 80 percent for more than five minutes on Server1.
- D. In the Performance Monitor console, create a counter log to track processor usage.

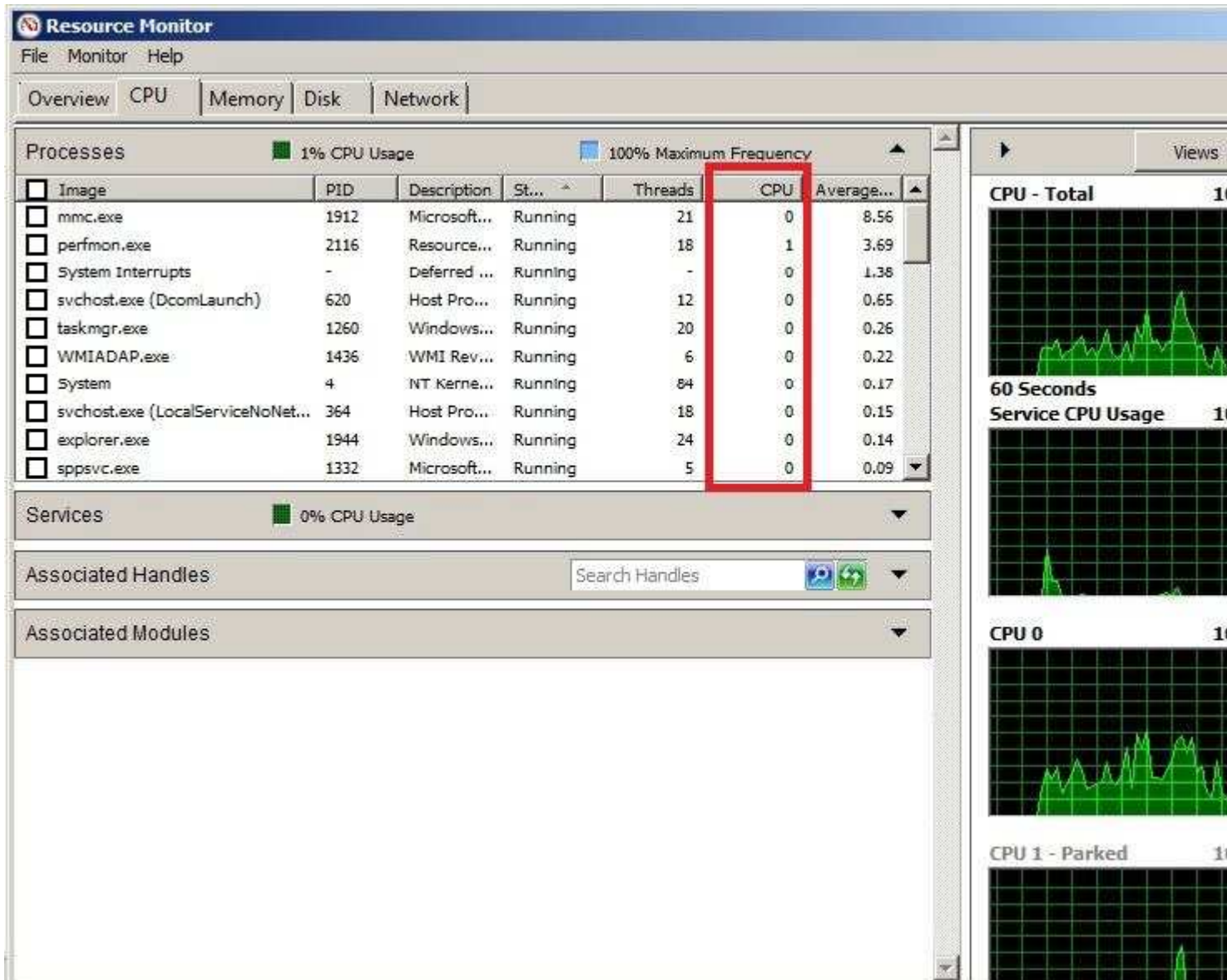
**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:



### QUESTION 30

Your network contains two servers named Server1 and Server2 that run Windows Server 2008 R2.

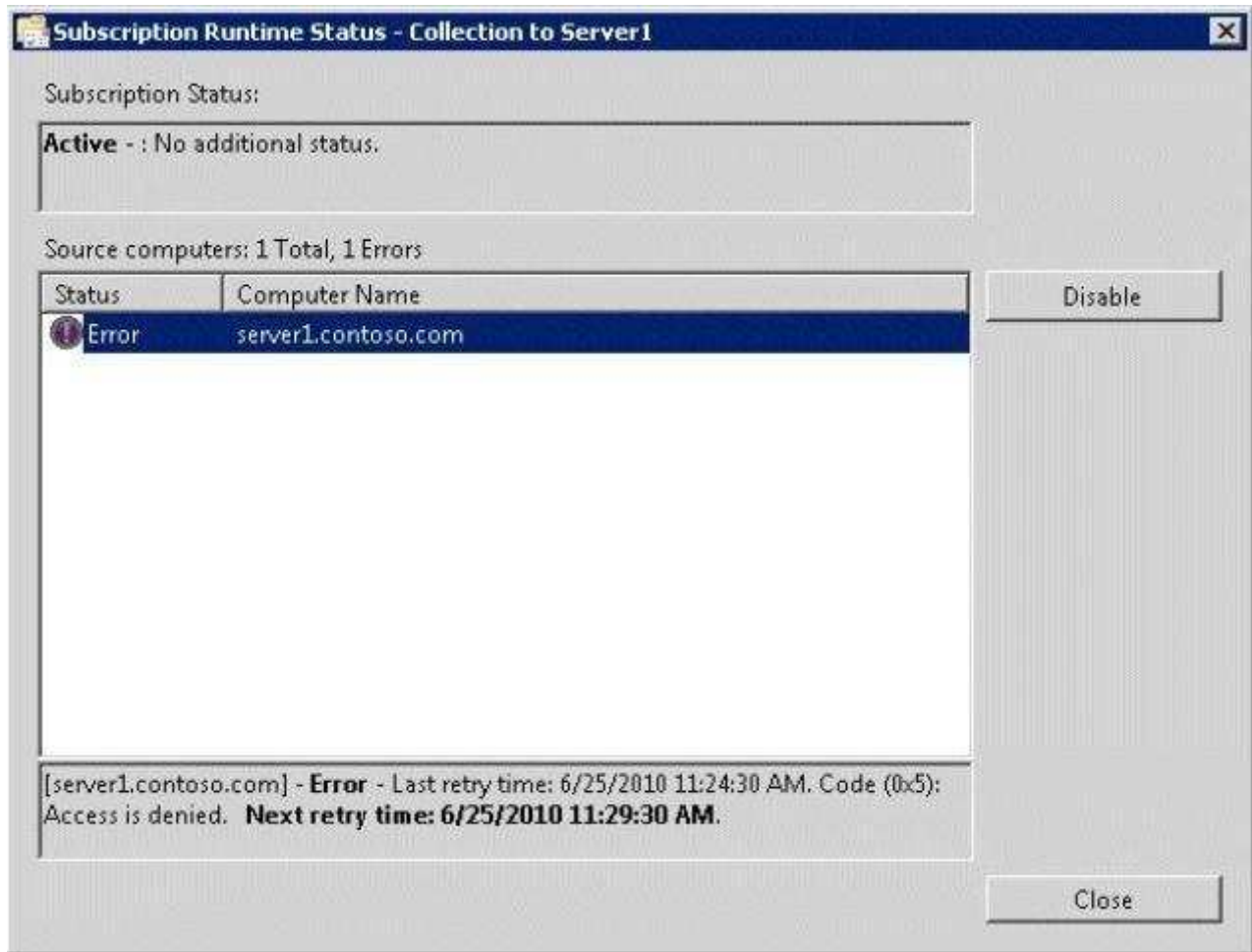
From Server1, you create a collector-initiated subscription that uses Server2 as a source computer.

You verify the event subscription and discover the error message shown in the exhibit. (Click the Exhibit button.)

You need to ensure that the subscription collection runs successfully.

What should you do?

**Exhibit:**



- A. From the properties of the subscription, modify the user Account options.
- B. On Server2, run winrmquickconfig.
- C. From the properties of the subscription, modify the Protocol and Port options.
- D. On Server1, run winrmquickconfig.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 31

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. wecutil cs
- D. winrm quickconfig



**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

### QUESTION 32

Your network contains a server named Server1 that runs Windows Server 2008 R2.

You need to identify which processes perform the most disk writes and disk reads per second.

Which tool should you use?

- A. Reliability Monitor
- B. Disk Management
- C. Resource Monitor
- D. Storage Explorer

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 33

Your network contains a windows Server update Services (WSUS) server named Server1.

You discover that certain updates listed in the WSUS administrative console are unavailable on Server1.

You need to ensure that all of the updates listed in the WSUS administrative console are available on Server1.

What should you do on Server1?

- A. Run wsusutil.exe and specify the reset parameter.
- B. Restart the Update Services service.
- C. Run wsusutil.exe and specify the deteteunneededrevisions parameter.
- D. Run vvuauct.exe and specify the /detectnow parameter.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Reset: Checks that every update metadata row in the database has corresponding update files stored in the file system. If update files are missing or have been corrupted, WSUS downloads the update files again use it:

After restoring the WSUS database.

When troubleshooting

<http://technet.microsoft.com/en-us/library/cc720466%28WS.10%29.aspx>

### QUESTION 34

Your network contains a Windows Server Update Services (WSUS) server. All computers on the network are configured to download and install updates once a week.

You need to deploy a critical update to a WSUS client as soon as possible.

Which command should you run?

- A. `dism.exe /online /check-apppatch`
- B. `secedit.exe /refreshpolicy`
- C. `wuauclt.exe /detectnow`
- D. `gpupdate.exe /force`

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Manipulate Automatic Updates Behavior Using Command-line Options There are two documented command-line options used for manipulating Automatic Updates behavior. These options are meant to be run from a command prompt. They are helpful for testing and troubleshooting client computers. For comprehensive troubleshooting information for problems with both the WSUS server and client computers, see "Microsoft Windows Server Update Services Operations Guide."

Detectnow Option Because waiting for detection to start can be a time-consuming process, an option has been added to allow you to initiate detection right away. On one of the computers with the new Automatic Update client installed, run the following command at the command prompt:  
`wuauclt.exe /detectnow`

### **QUESTION 35**

Your network contains a server that runs Windows Server 2008 R2.

You create a User Defined Data Collector Set (DCS) named Set1.

You need to ensure that the reports generated for Set1 are stored for at least one year.

What should you do?

- A. From Data Manager for Set1, modify the Data Manager settings.
- B. From Data Manager for Set1, modify the Actions settings.
- C. From the properties of Set1, modify the Task settings.
- D. From the properties of Set1, modify the Schedule settings.

**Correct Answer: B**

**Section: (none)**

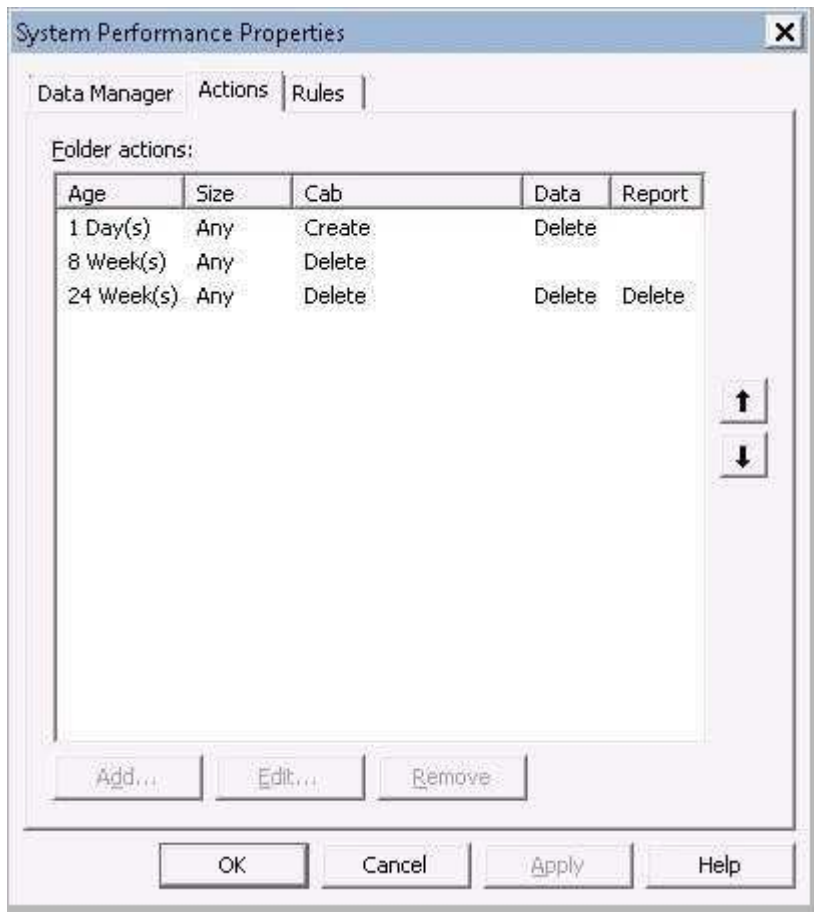
**Explanation**

**Explanation/Reference:**

Explanation:

**The old answer was: From the properties of Set1, modify the Task settings.**

The time before a log shall be deleted settings are in the Data Manager's "Actions Tab" of the custom/user defined DSC.



### QUESTION 36

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 (CMAC)
- 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**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 37**

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 to provide central authentication of dial-up, VPN, and wireless connections to the network.

Which server role, role service or feature should you install?

- A. Windows System Resource Manager (WSRM)
- B. Health Registration Authority (HRA)
- C. Services for Network File System (NFS)
- D. Simple TCP/IP Services
- E. Network Load Balancing (NLB)
- F. Windows Internal Database
- G. Connection Manager Administration Kit (CMAK)
- H. File Server Resource Manager (FSRM)
- I. Windows Server Update Services (WSUS)
- J. Group Policy Management
- K. Network Policy Server (NPS)
- L. Wireless LAN Service
- M. Routing and Remote Access service (RRAS)

**Correct Answer:** K

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**With NPS Installed Roles**

Create Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.

For NAP VPN or 802.1X, you must configure PEAP authentication in connection request policy.

**QUESTION 38**

Your network contains an Active Directory domain. The domain contains several VPN servers that have the Routing and Remote Access service (RRAS) role service installed.

You need to configure all of the VPN servers to use the same network policies.

The solution must ensure that any changes to the network policies automatically apply to all of the VPN servers.

What should you configure on the VPN servers?

- A. health policies
- B. remediation server groups
- C. system health validators (SHVs)
- D. the Windows Authentication authentication provider
- E. Group Policy preferences
- F. the Windows Accounting accounting provider
- G. IKEv2 client connections

- H. the RADIUS Accounting accounting provider
- I. the RADIUS Authentication authentication provider
- J. connection request policies

**Correct Answer: I**

**Section: (none)**

**Explanation**

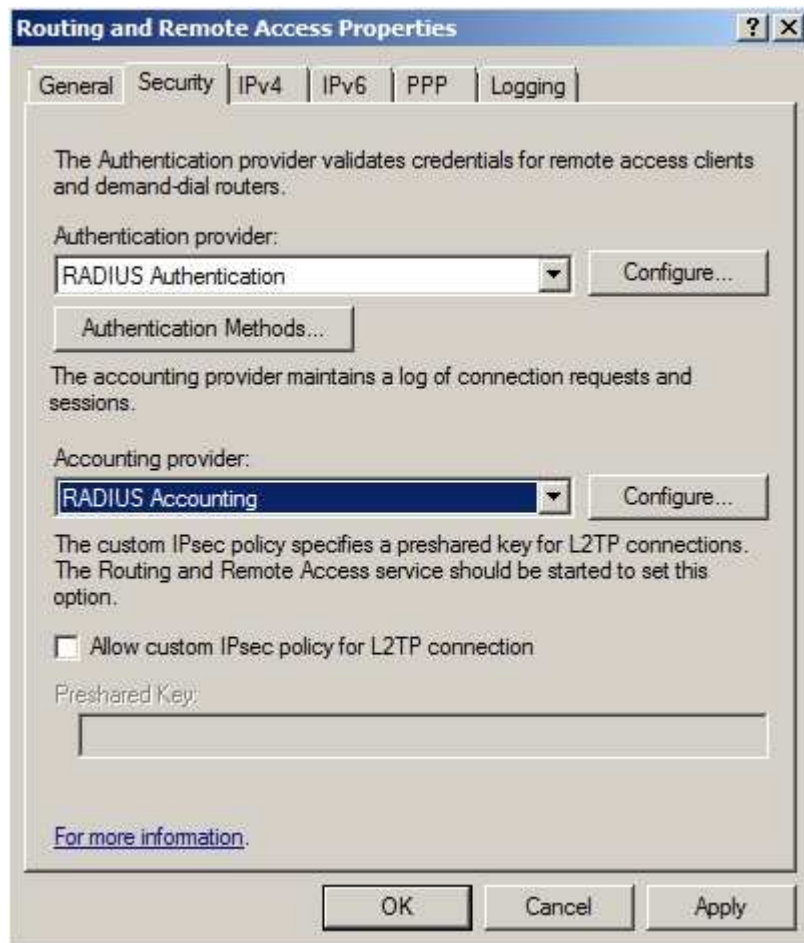
**Explanation/Reference:**

Explanation:

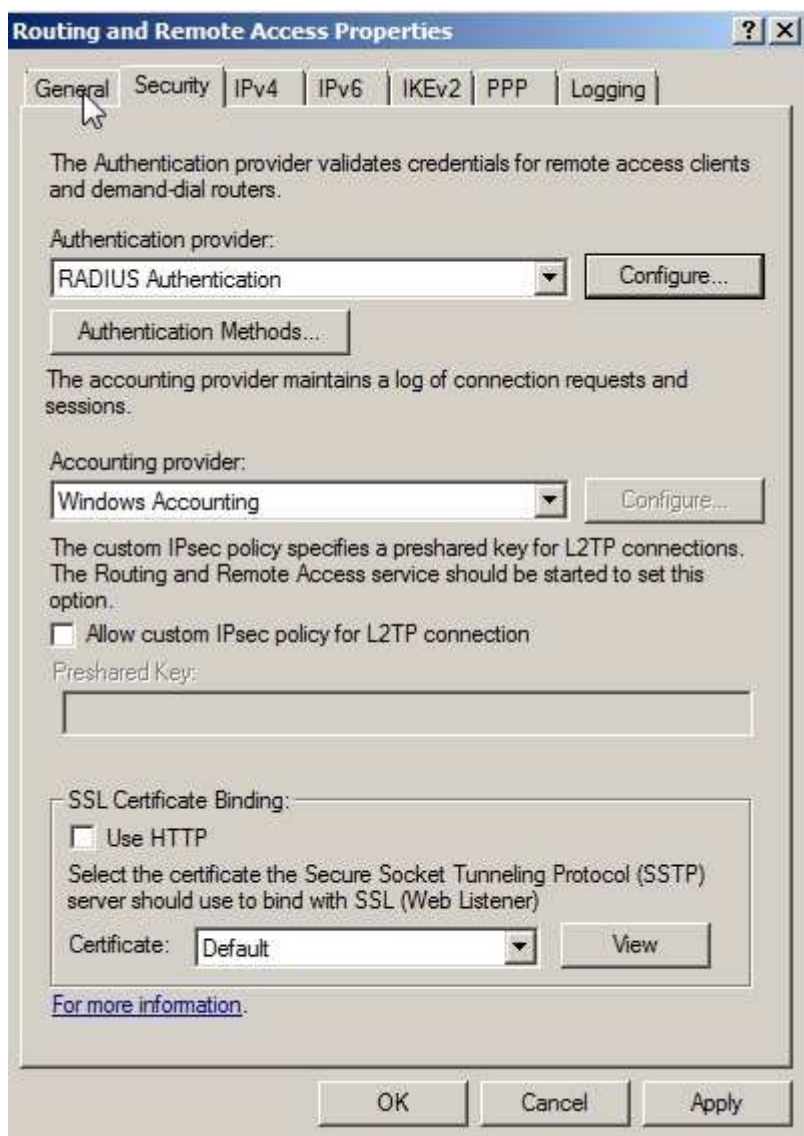
This example is from an Server08 RRAS role without NPS services role activated used as VPN Server.

Show here screenshots from RRAS Properties:

From Server 2008:



From Server 2008 R2:



<http://blogs.technet.com/b/rrasblog/archive/2009/03/25/remote-access-deployment-part-2-configuring-rras-as-a-vpn-server.aspx>

<http://technet.microsoft.com/en-us/library/cc754107.aspx> ==> NPS Used

### QUESTION 39

Your network contains an Active Directory domain.

Your company is implementing Network Access Protection (NAP).

You need to define which network resources non-compliant client computers can access.

What should you configure?

- A. system health validators (SHVs)
- B. the Windows Accounting accounting provider
- C. remediation server groups
- D. Group Policy preferences

- E. the Windows Authentication authentication provider
- F. health policies
- G. connection request policies
- H. the RADIUS Accounting accounting provider
- I. IKEv2 client connections
- J. the RADIUS Authentication authentication provider

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation: Remediation Server Groups allow you to specify the remediation servers that provide services and updates to noncompliant NAP client computers

#### **QUESTION 40**

Your network contains an Active Directory domain. The domain contains several VPN servers that have the Routing and Remote Access service (RRAS) role service installed.

You need to collect information about the duration of the VPN connections. The information must be stored in a central location.

What should you configure on the VPN servers?

- A. the RADIUS Authentication authentication provider
- B. system health validators (SHVs)
- C. IKEv2 client connections
- D. remediation server groups
- E. the Windows Accounting accounting provider
- F. the Windows Authentication authentication provider
- G. health policies
- H. Group Policy preferences
- I. connection request policies
- J. the RADIUS Accounting accounting provider

**Correct Answer: J**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

To use RADIUS accounting:

- 1.Open Routing and Remote Access.
- 2.Right-click the server name for which you want to configure RADIUS accounting, and then click Properties.
- 3.On the Security tab, in Accounting provider, click RADIUS accounting, and then click Configure.
- 4.In the RADIUS Accounting dialog box, click Add.
- 5.In the Add RADIUS Server dialog box, configure the settings for your RADIUS accounting server, and then click OK.

**Note**

To perform this procedure, you must be a member of the Administrators group. As a security best practice, consider using the Run As command rather than logging on with administrative credentials. If you have logged on with administrative credentials, you can also open Routing and Remote Access by clicking Start, clicking Control Panel, double-clicking Administrative Tools, and then double-clicking Routing and Remote Access. For

more information, see Default local groups, Default groups, and Using Run as.

**QUESTION 41**

Your network contains a server named Server1 that has the Remote Desktop Connection Broker (RD Connection Broker) role service installed.

You deploy two new servers named Server2 and Server3. On Server2 and Server3, you install the Remote Desktop Session Host (RD Session Host) role service.

From the Remote Desktop Session Host Configuration snap-in, you configure Server2 and Server3 as server farm members.

You need to ensure that all Remote Desktop sessions are distributed between Server2 and Server3.

What should you do?

- A. On Server1, install the Remote Desktop Gateway (RD Gateway) role service. Add Server2 and Server3 as RD Gateway server farm members.
- B. On Server1, add the Server2 computer account and the Server3 computer account to the Session Broker Computers group.
- C. On Server1, install the Remote Desktop Gateway (RD Gateway) role service. Add Server1 as an RD Gateway server farm member.
- D. On Server2 and Server3, add the Server1 computer account to the Remote Desktop Users group.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:





#### QUESTION 42

Your network contains a server named Server1 that runs windows Server 2008 R2. Server1 has the Remote Desktop Session Host (RD Session Host) role service installed.

You need to ensure that Remote Desktop users can use the user interface elements of Windows Aero.

What should you do on Server1?

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

#### **Explanation/Reference:**

Explanation:

When a user uses Remote Desktop Connection to connect to a Remote Desktop Session Host (RD Session Host) server, the desktop that exists on the RD Session Host server is reproduced, by default, in the remote session. To make the remote session look and feel more like the user's local Windows 7 desktop experience, install the Desktop Experience feature on an RD Session Host server that is running Windows Server 2008 R2.

Desktop Experience installs components and features of Windows 7, such as Windows Media

Player, Windows Defender, and Windows Calendar

Source:<http://technet.microsoft.com/en-us/library/cc772567.aspx>

#### QUESTION 43

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

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

You need to ensure that Server1 only issues Remote Desktop Services client access licenses (RDS CALs) to Server2.

Which two tasks should you perform? (Each correct answer presents part of the solution. Choose two.)

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

**Correct Answer:** BD

**Section:** (none)

**Explanation**

#### Explanation/Reference:

Explanation:

When the Remote Desktop Licensing role service is installed on the server, the Terminal Server Computers local group is created. The license server will respond only to requests for RDS CALs from Remote Desktop Session Host servers whose computer accounts are members of this group if the Computer Configuration \Administrative Templates\Windows Components\Remote Desktop Services\RD Licensing\License server security group Group Policy setting has been enabled and applied to the license server. By default, the Terminal Server Computers local group is empty.

When the Remote Desktop Licensing role service is removed from the server, the Terminal Server Computers local group is deleted.

Source:[http://technet.microsoft.com/en-us/library/ee891291\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ee891291(WS.10).aspx)

#### QUESTION 44

Your network contains a server named Server1 that runs windows Server 2008 R2. Server1 has the Remote Desktop Session Host (RD Session Host) role service and the Windows System Resource Manager (WSRM) feature installed.

Users from two Active Directory groups named Group1 and Group2 connect to Server1 and run the same RemoteApp program.

You need to ensure that when Server1 experiences high CPU usage. Group1 users have priority over Group2 users regarding the use of CPU resources. You want to achieve this goal by using the minimum amount of administrative effort.

What should you do from the WSRM console?

- A. Add a new Conditional Policy.
- B. Create a new Process Matching criteria.
- C. Implement Weighted\_Remote\_Sessions.
- D. Create a new Calendar Schedule.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

When the Weighted\_Remote\_Sessions resource allocation policy is managing the system, the processes are grouped according to the priority assigned with the user account. For example, if three users are remotely connected, the user assigned Premium priority will receive highest priority access to the CPU, the user assigned Standard priority will receive second priority to the CPU, and the user assigned Basic priority will receive lowest priority to the CPU. This policy is for use with RD Session Host servers.

Source:<http://technet.microsoft.com/en-us/library/cc732553.aspx>

#### **QUESTION 45**

Your network contains a server named Server1 that runs windows Server 2008 R2. Server1 has the Remote Desktop Session Host (RD Session Host) role service installed. Server1 hosts RemoteApp programs.

Two hundred users connect to Server1 to run the RemoteApp programs.

You need to use Performance Monitor to view the CPU usage of each RemoteApp program.

Which Performance Monitor object should you monitor?

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

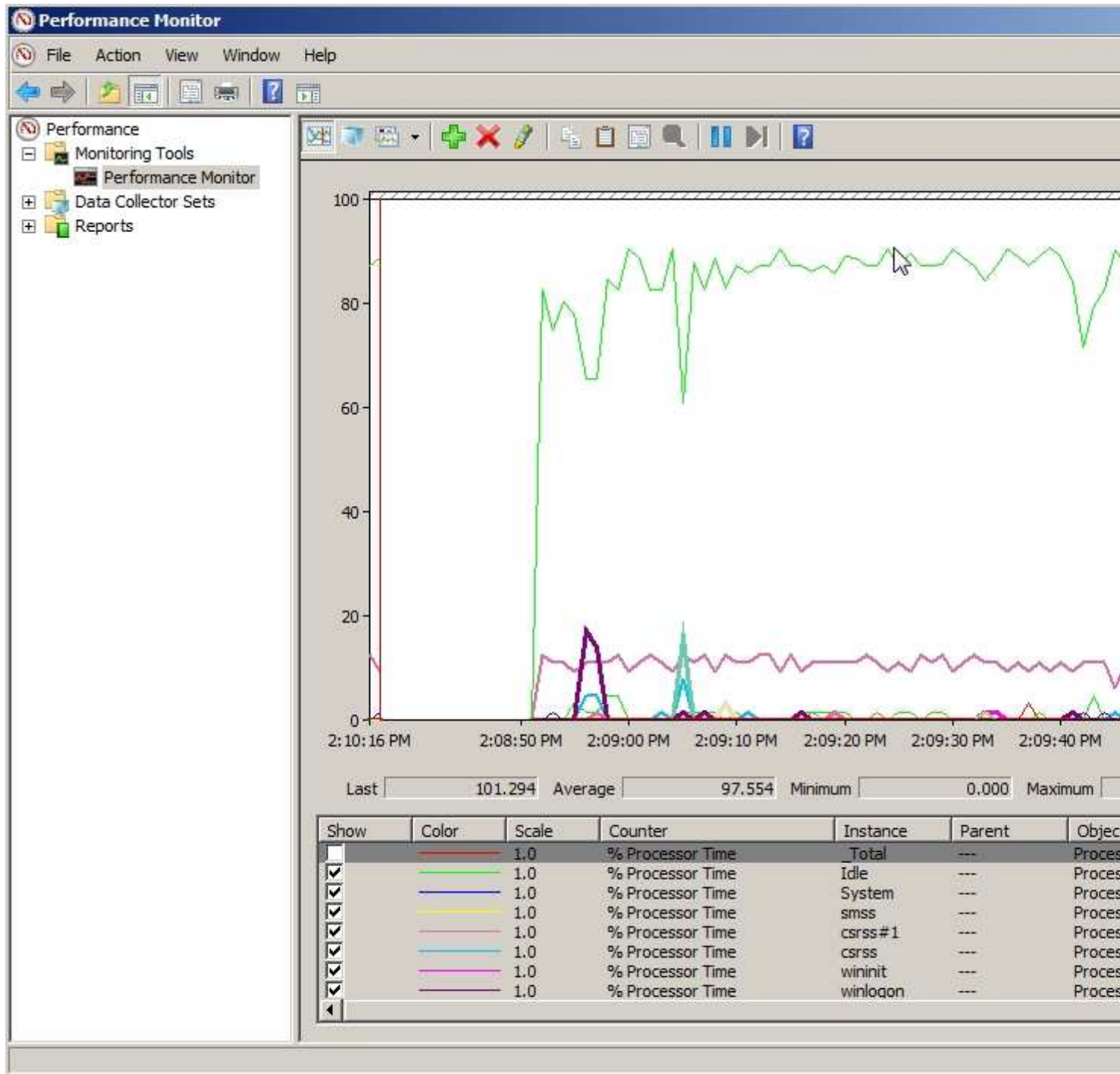
**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:



#### QUESTION 46

Your network consists of a single Active Directory domain. The network contains a Remote Desktop Session Host Server that runs Windows Server 2008 R2, and client computers that run Windows 7. All computers are members of the domain.

You deploy an application by using the RemoteApp Manager. The Remote Desktop Session Host Server's security layer is set to Negotiate.

You need to ensure that domain users are not prompted for credentials when they access the application.

What should you do?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Configuration

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

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

#### **QUESTION 47**

Your network contains an FTP server that runs Windows Server 2008 R2. You need to prevent FTP users from viewing all folders named \_private. What should you configure?

- A. FTP Request Filtering
- B. FTP Directory Browsing
- C. FTP IPv4 Address and Domain Restrictions
- D. FTP Authorization Rules

**Correct Answer:** A

**Section:** (none)

**Explanation**

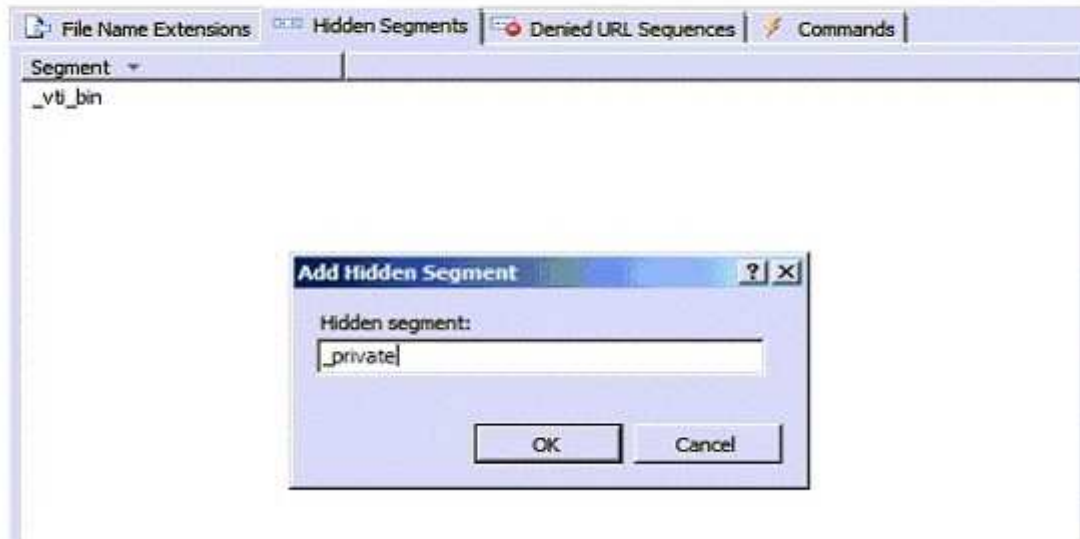
**Explanation/Reference:**

Explanation:



## FTP Request Filtering

Use this feature to configure filtering rules for the FTP service.



### QUESTION 48

Your network contains a server named Server1. Server1 has three disk volumes. Two volumes drives named C and E are configured as simple volumes. The third disk volume 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**

**Section: (none)**

**Explanation**

#### Explanation/Reference:

Explanation:

Extend a Simple or Spanned Volume

A spanned volume is a dynamic volume that consists of disk space on more than one physical disk. If a simple volume is not a system volume or boot volume, you can extend across additional disks. If you extend a simple volume across multiple disks, it becomes a spanned volume. You can extend a volume only if it does not have a file system or if it is formatted using the NTFS file system.

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

Extending a simple or spanned volume

1. In Disk Management, right-click the simple or spanned volume you want to extend.
  2. Click Extend Volume.
  3. Follow the instructions on your screen.
- Source:<http://technet.microsoft.com/en-us/library/cc753058.aspx>

#### QUESTION 49

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Windows Deployment Services (WDS) server role installed.

You need to create a multicast session to deploy a virtual hard disk (VHD).

Which tool should you use?

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

#### Explanation/Reference:

Explanation:

Creating a multicast transmission for a virtual hard disk image

You can create multicast transmissions for your .vhd images in the same way that you can for .wim images (except you can only create the transmissions from the command line).

To create a multicast transmission

1. Click Start, right-click Command Prompt, and then click Run as administrator.
2. Do one of the following:

To create an Auto-Cast transmission, use the following syntax: WDSUTIL /New- MulticastTransmission /

Image:<image name> /FriendlyName:<friendly name> /ImageType:Install /ImageGroup:<Image group name> [/FileName:<file name>] /TransmissionType:AutoCast.

Example: WDSUTIL /New-MulticastTransmission /Image:WindowsServer2008R2 / ImageType:Install / ImageGroup:"VHD Image Group" /FileName:install.vhd / TransmissionType:AutoCast

To create a Scheduled-Cast transmission, use the following syntax: WDSUTIL /New- MulticastTransmission /

Image:<image name> /FriendlyName:<friendly name> /ImageType:Install /ImageGroup:<Image group name> / TransmissionType:ScheduledCast [/Time:<yyyy/mm/dd:hh:mm>][/Clients:<no of clients>].

Example: WDSUTIL /New-MulticastTransmission /Image:WindowsServer2008R2 / ImageType:Install / ImageGroup:"VHD Image Group" /TransmissionType:ScheduledCast /Time:"2008/01/20:17:00" /Clients:10

Source:[http://technet.microsoft.com/en-us/library/dd363560\(WS.10\).aspx#BKMK5](http://technet.microsoft.com/en-us/library/dd363560(WS.10).aspx#BKMK5)

#### QUESTION 50

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

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

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



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

#### QUESTION 51

Your network contains a two-node Hyper-V cluster that hosts 10 virtual machines (VMs). You discover that when a failover occurs, all of the VMs fail over simultaneously. You need to modify the cluster so that you can fail over each VM individually. What should you do first?

- A. Add a third node to the cluster.
- B. Modify the properties of the cluster failover.
- C. Create a Clustered Shared volume.
- D. Add a new disk to the failover cluster.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 52

Your network contains a server named Server1 that runs Windows Server 2008 R2. You need to configure



Server1 as a Key Management Service (KMS) host. What should you do first?

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

To install a KMS host on a Windows Vista or Windows Server 2008 computer

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

slui.exe 4

5. After activation is complete, restart the Software Licensing Service using the Service application.

Source:[http://technet.microsoft.com/en-us/library/cc303280.aspx#\\_Install\\_KMS\\_Hosts](http://technet.microsoft.com/en-us/library/cc303280.aspx#_Install_KMS_Hosts)

**QUESTION 53**

You manage a Web server named Server1 that runs Windows Server 2008 R2. Server1 has the SMTP Server feature installed.

You need to manage the SMTP server settings.

Which tool should you use?

- A. Telnet
- B. windows Firewall
- C. System Configuration
- D. Iisreset
- E. Local Security Policy
- F. Performance Monitor
- G. Internet Information Services (IIS) Manager
- H. Ftp
- I. Component Services
- J. Services
- K. Security Configuration Wizard (SCW)
- L. Internet Information Services (IIS) 6.0 Manager

**Correct Answer: L**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Ref: <http://technet.microsoft.com/en-us/library/dd364124%28WS.10%29.aspx>

**QUESTION 54**

You manage a Web server named Server1 that runs Windows Server 2008 R2. Server1 has the SMTP Server feature installed.

You need to verify whether you can connect to Server1 over TCP port 25.

Which tool should you use?

- A. Internet Information Services (IIS) Manager
- B. Ftp
- C. Performance Monitor
- D. Windows Firewall
- E. Local Security Policy
- F. Telnet
- G. Iisreset
- H. System Configuration
- I. Services
- J. Component Services
- K. Internet Information Services (IIS) 6.0 Manager
- L. Security Configuration Wizard (SCW)

**Correct Answer: F**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 55**

Your network contains a Web server named Server1 that runs Windows Server 2008 R2. Server1 has four application pools.

You need to view a list of the CPU and memory resources used by each application pool.

Which feature should you configure from Internet Information Services (IIS) Manager?

- A. IP Address and Domain Restrictions
- B. Request Filtering
- C. HTTP Response Headers
- D. HTTP Redirect
- E. SSL Settings
- F. Feature Delegation
- G. Error Pages
- H. Worker Processes
- I. Default Document
- J. Authentication
- K. Connection Strings
- L. ISAPI Filters
- M. Authorization Rules

- N. US Manager Permissions
- O. ISAPI and CGI Restrictions
- P. Management Service

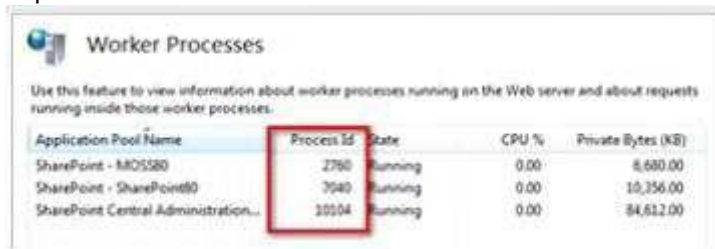
**Correct Answer: H**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:



Application Pool Name	Process ID	State	CPU %	Private Bytes (KB)
SharePoint - MOSS80	2760	Running	0.00	8,600.00
SharePoint - SharePoint80	7040	Running	0.00	10,356.00
SharePoint Central Administration...	10104	Running	0.00	84,612.00

#### QUESTION 56

Your network contains a Web server named Server1 that runs windows Server 2008 R2.

You need to ensure that when a user attempts to connect to a page on Server1 that does not exist, Server1 displays a custom page that contains a site map.

Which feature should you configure from Internet Information Services (IIS) Manager?

- A. HTTP Response Headers
- B. Worker Processes
- C. Default Document
- D. Error Pages
- E. ISAPI and CGI Restrictions
- F. Authentication
- G. Management Service
- H. Feature Delegation
- I. IIS Manager Permissions
- J. SSL Settings
- K. Connection Strings
- L. Request Filtering
- M. Authorization Rules
- N. ISAPI Filters
- O. HTTP Redirect
- P. IP Address and Domain Restrictions

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 57

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

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

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

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

What should you do?

- A. From RemoteApp Deployment Settings, configure the Common RDP Settings.
- B. From RemoteApp 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**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 58**

Your network contains a Web server that runs Windows Server 2008 R2.

Remote management is configured for Internet Information Services (IIS).

From IIS Manager Permissions, you add a user to a Web site.

You need to prevent the user from using Internet Information Services (IIS) Manager to modify the authorization rules of the Web site.

Which settings should you configure?

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 59**

Your network contains a Web server named Web1 that runs Windows Server 2008 R2.

Web1 has a wildcard certificate installed. Web1 has two Web sites:

**Shown in Exhibit**

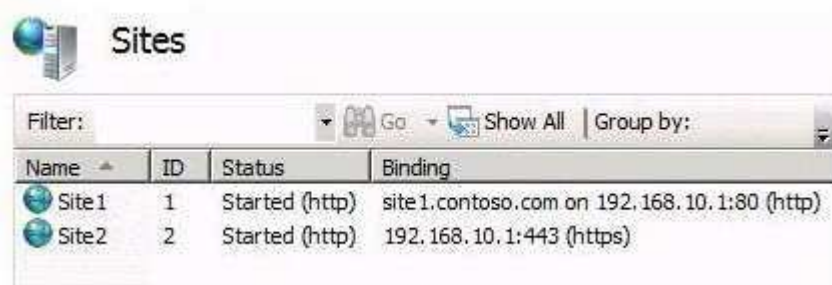
You discover that when you go to the URL <https://site1.contoso.com> in Internet Explorer, you connect to Site2.

You need to ensure that when users go to <https://site1.contoso.com> in Internet Explorer, they connect to Site1.

The solution must ensure that all connections to Site1 are secure.

Which two settings should you modify? (Each correct answer presents part of the solution. Choose two.)

**Exhibit:**



Name	ID	Status	Binding
Site1	1	Started (http)	site1.contoso.com on 192.168.10.1:80 (http)
Site2	2	Started (http)	192.168.10.1:443 (https)

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

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 60

Your network contains a client computer named Computer1 that runs Windows 7. Computer1 is configured to use DirectAccess.

You need to identify the URL of the network location server that Computer1 is configured to use.

What should you do?

- A. From a command prompt, run `ipconfig.exe /displaydns`.
- B. From a command prompt, run `netsh.exe namespace show policy`.
- C. From Control Panel, run the network adapter troubleshooter.
- D. From the Network Connection Status window, view the Network Connection Details.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

"use the netsh namespace show policy command to display the NRPT rules configured through Group Policy. There should be NRPT rules for the intranet namespace and an exemption rule for the fully qualified domain name (FQDN) of the network location server"

#### QUESTION 61

Your network contains three servers named Server1, Server2, and Server3 that have the Network Policy Server (NPS) role service installed.

On Server1, you configure a Remote RADIUS Server Group that contains Server2 and Server3. On Server2 and Server3, you configure Server1 as a RADIUS client.

You configure Server2 and Server3 to authenticate remote users.

You need to configure Server1 to forward RADIUS authentication requests to Server2 and Server3.

What should you create on Server1?

- A. a connection request policy
- B. a health policy
- C. a network policy
- D. a remediation server group

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.

For NAP VPN or 802.1X, you must configure PEAP authentication in connection request policy.

<http://technet.microsoft.com/en-us/library/cc754518.aspx>

### QUESTION 62

Your network contains an Active Directory domain named Contoso.com. Contoso.com contains an enterprise certification authority (CA) named CA1.

You enable Secure Socket Tunneling Protocol (SSTP) on a server named Server1.

A user named User1 attempts to establish an SSTP connection to Server1 and receives the following error message: "Error 0x80092013: The revocation function was unable to check revocation because the revocation server was offline."

You verify that all certificates services are online.

You need to ensure that User1 can connect to Server1 by using SSTP.

What should you do first?

- A. Configure User1 for certificate auto enrollment.
- B. Configure a pre-shared key for IPsec on User1's computer.
- C. Add a certificate to Server1 that contains Server1.contoso.com as a Subject Alternative Name (SAN).
- D. Publish the certificate revocation list distribution point (CDP) to a location that is accessible from the Internet.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation: Ref : <http://blogs.technet.com/b/rasblog/archive/2007/09/26/how-to-debug-sstp-specific-connection-failures.aspx>

Client tries to connect to SSTP VPN server and it fails to connect giving error message 0x80092013

Trouble-shooting steps: This will happen if client is failing the certificate revocation check of the SSL certificate obtained from server side.

This can happen because of two reasons:

a) Ensure the CRL check servers on the server side are exposed on the Internet (i.e. are available on the Internet). This is because CRL check is done on the client side during SSL connection establishment phase and the CRL check query will be directly going on the Internet (and not on top of VPN connection because it is

not up yet).

b) CRL URL that is set inside the machine certificate on RRAS server is pointing to the internal DNS name (e.g. myvpn.contoso.local) and not the external name (special thanks to one of our esteemed customers, Bill Voltmer, in pointing this out). To validate this, open the certificate snap-in on your RRAS server, go to details tab and look at "CRL distribution point" field. To fix this:

1. Open Server Manager and navigate to Roles, Active Directory Certificate Services
2. Right click on CA name (e.g. mycompany-vpn1-CA) and choose Properties.
3. Click Extensions tab.
4. Select the pre-existing http: URL and click Remove.
5. Click Add...
6. Type http://
7. Type external URL of VPN server
8. Type CertEnroll/
9. Insert variable <CaName>
10. Insert variable <CRLNameSuffix>
11. Insert variable <DeltaCRLAllowed>
12. Type .crl
13. Check boxes Include in CRLs... and Include in the CDP...

The above should be done before SSTP VPN is configured on RRAS. Or if it is already configured, change the machine certificate by following this blog.

### **QUESTION 63**

You deploy Network Access Protection (NAP) on your network.

An administrator configures a network policy as shown in the exhibit. (Click the Exhibit button.)

You discover that noncompliant client computers cannot access the remediation network.

You need to configure the network policy to ensure that noncompliant client computers can access the remediation network.

What should you do?

**Exhibit:**

**NonCompliant-Restricted Access Properties**

Overview | Conditions | Constraints | Settings

Policy name: NonCompliant-Restricted Access

**Policy State**  
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

☒ Policy enabled

**Access Permission**  
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. [What is access permission?](#)

☐ Grant access. Grant access if the connection request matches this policy.

☒ Deny access. Deny access if the connection request matches this policy.

☐ Ignore user account dial-in properties.  
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts.

**Network connection method**  
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

☐ Type of network access server:  
Unspecified

☒ Vendor specific:  
10

OK Cancel Apply

- A. In the Type of network access server list, click HCAP Server.
- B. In the Type of network access server list, click Health Registration Authority.
- C. In Access Permission, select the Ignore user account dial-in properties check box.
- D. In Access Permission, select the Grant access. Grant access if the connection request matches this policy option button.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 64

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

You publish a RemoteApp named WebApp5. The Remote Desktop Connection (.rdp) file for WebAppS is unsigned.

When a user named Users runs WebApp5 from the Remote Desktop Web Access (RD Web Access) website, User5 is prompted for credentials.



You need to prevent users from being prompted for credentials when they run WebApp5.

What should you do?

- A. Enable Forms-based authentication for the Remote Desktop Web Access website.
- B. Enable the Assign a default domain for logon Group Policy setting.
- C. Add a Managed Module for the RDWeb virtual directory.
- D. Enable the Allow Delegating Default Credentials Group Policy setting.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

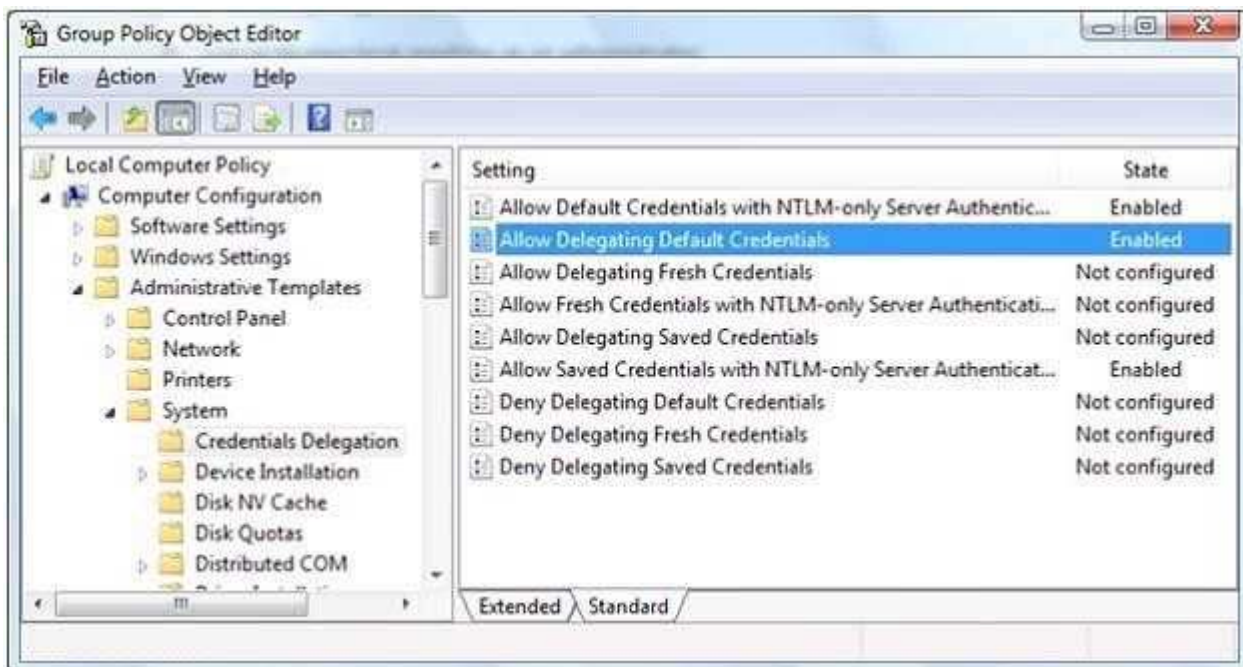
Explanation:

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.

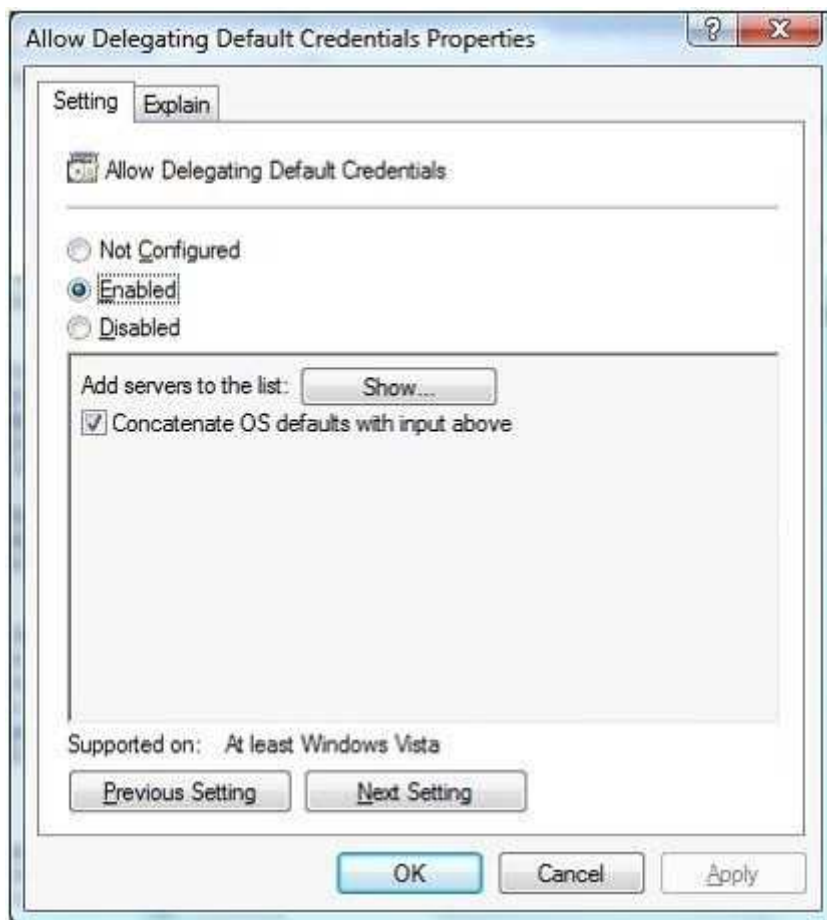
How to enable Single Sign-On?

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

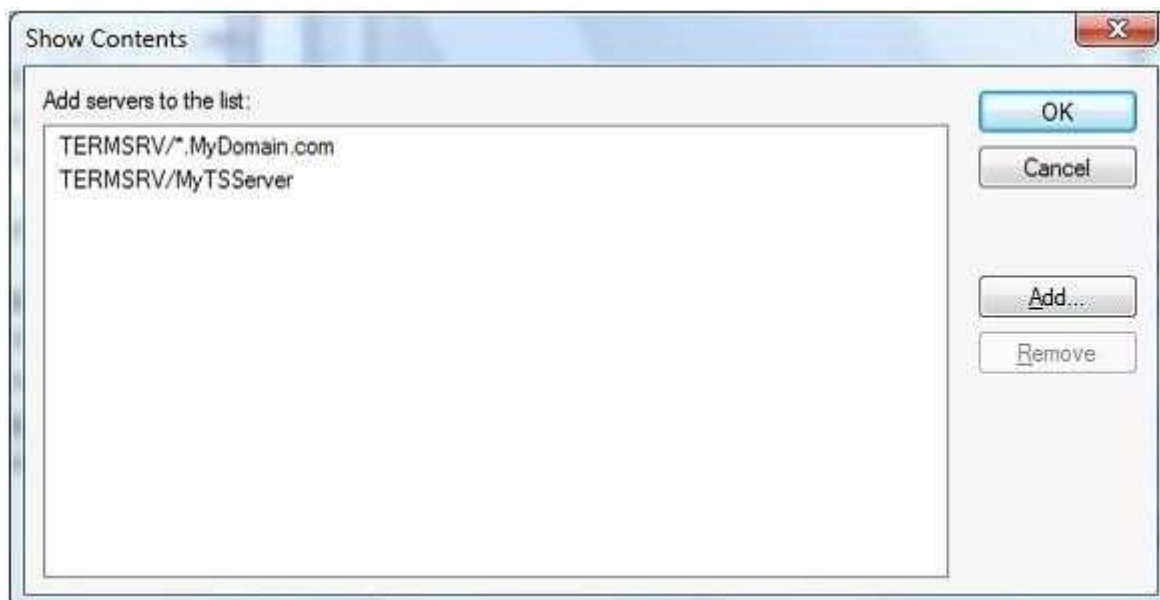
1. Log on to your local machine as an administrator.
2. Start Group Policy Editor - "gpedit.msc".
3. Navigate to "Computer Configuration\Administrative Templates\System\Credentials Delegation".



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/<Your server name>" 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>

#### **QUESTION 65**

Your company has an Active Directory domain. A server named Server1 runs Windows Server 2008 R2. The Remote Desktop Services server role and the RD Web Access role service are installed on Server1.

You install the RD Gateway role service on Server1. You create the Remote Desktop connection authorization policy. Users report that they cannot connect to Server1.

You need to ensure that users can connect to Server1.

What should you do?

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

#### **Explanation/Reference:**

Explanation:

Remote Desktop resource authorization policies (RD RAPs) allow you to specify the internal network resources (computers) that remote users can connect to through an RD Gateway server. Remote users connecting to the network through an RD Gateway server are granted access to computers on the internal network if they meet the conditions specified in at least one RD CAP and one RD RAP.

When you associate an RD Gateway-managed computer group with an RD RAP, you can support both fully qualified domain names (FQDNs) and NetBIOS names by adding both names to the RD Gateway-managed computer group separately.

When you associate an Active Directory security group or an RD Session Host server farm with an RD RAP, both FQDNs and NetBIOS names are supported automatically if the internal network computer that the client is connecting to belongs to the same domain as the RD Gateway server.

If the internal network computer belongs to a different domain than the RD Gateway server, users must specify the FQDN of the internal network computer.

Source:<http://technet.microsoft.com/en-us/library/cc772397.aspx>

#### **QUESTION 66**

Your network contains an Active Directory domain named fabrikam.com. The domain contains a Web server named Web1 that runs Windows Server 2008 R2.

You create a new site named Site1.

You need to prevent Web1 from accepting HTTP URLs that are longer than 1,024 bytes.

Which feature should you configure?

- A. Authorization Rules
- B. Connection Strings
- C. HTTP Response Headers
- D. Request Filtering

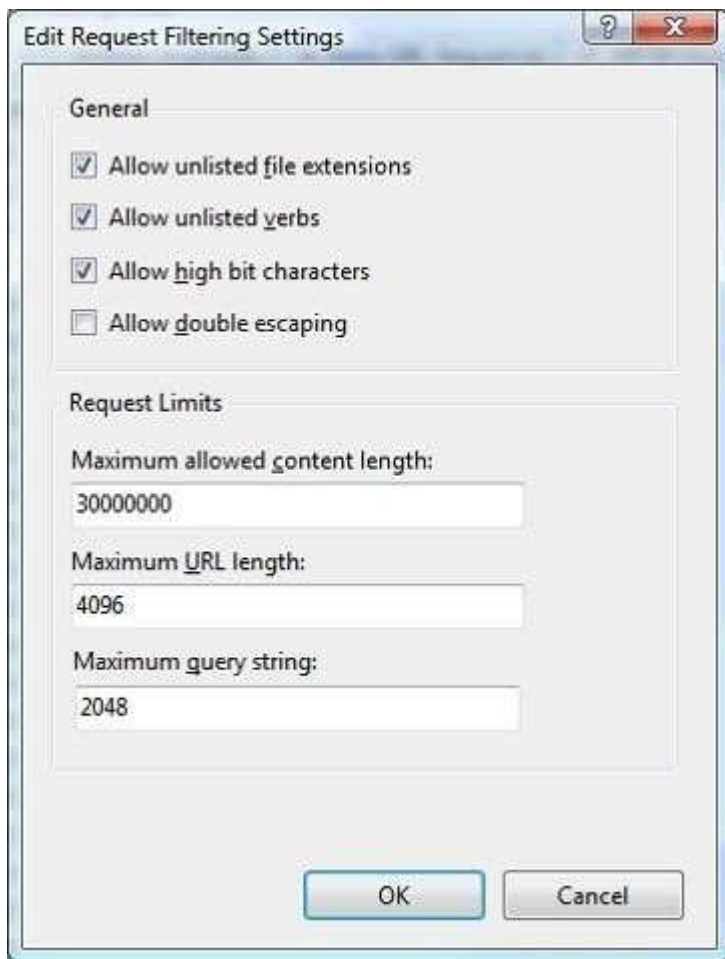
**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:



**QUESTION 67**

Your network contains an Active Directory domain. The network has DirectAccess deployed.

You deploy the DirectAccess Connectivity Assistant (DCA) to all client computers.

You need to ensure that users can view their DirectAccess status by using the DCA.

Which two group policy settings should you configure? (Each correct answer presents part of the solution. Choose two.)

- A. PortalName
- B. Corporate Portal Site

- C. CorporateResources
- D. Dynamic Tunnel Endpoints (DTEs)

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

You must configure the DTE and CorporateResources settings to have DCA functionality. The others settings are optional, but recommended.

<http://technet.microsoft.com/en-us/library/gg502552.aspx>

#### **QUESTION 68**

Your network contains a server named Server1 that runs Windows Server 2008 R2 Service Pack (SP1).

All users have laptops that run Windows 7. The users frequently work from network locations that only allow outbound communication to the Internet by using HTTP and HTTPS.

You plan to configure Server1 as a VPN server.

You need to identify which VPN protocol you should use to ensure that all of the users can establish VPN connections to Server1.

Which VPN protocol should you identify?

- A. SSTP
- B. PPTP
- C. IKEv2
- D. L2TP

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation: [http://technet.microsoft.com/en-us/library/cc731352\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc731352(v=ws.10).aspx)

Secure Socket Tunneling Protocol (SSTP) is a new form of VPN tunnel with features that allow traffic to pass through firewalls that block PPTP and L2TP/IPsec traffic.

SSTP provides a mechanism to encapsulate PPP traffic over the SSL channel of the HTTPS protocol.

The use of PPP allows support for strong authentication methods such as EAP-TLS.

The use of HTTPS means traffic will flow through TCP port 443, a port commonly used for Web access.

Secure Sockets Layer (SSL) provides transport-level security with enhanced key negotiation, encryption, and integrity checking.

#### **QUESTION 69**

.

Your network consists of an Active Directory forest that contains one domain. All domain controllers run Windows Server 2008 R2 and are configured as DNS servers. You have an Active Directory- integrated zone.

You have two Active Directory sites. Each site contains five domain controllers.

You add a new NS record to the zone.

You need to ensure that all domain controllers immediately receive the new NS record.

What should you do?

- A. From the DNS Manager console, reload the zone.
- B. From the Services snap-in, restart the DNS Server service.
- C. From the command prompt, run repadmin /syncall.
- D. From the DNS Manager console, increase the version number of the SOA record.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 70**

.

You have a domain controller named DC1 that runs Windows Server 2008 R2. DC1 is configured as a DNS server for contoso.com.

You install the DNS Server server role on a member server named Server1 and then you create a standard secondary zone for contoso.com. You configure DC1 as the master server for the zone.

You need to ensure that Server1 receives zone updates from DC1.

What should you do?

- A. On Server1, add a conditional forwarder.
- B. On DC1, modify the permissions of contoso.com zone.
- C. On DC1, modify the zone transfer settings for the contoso.com zone.
- D. Add the Server1 computer account to the DNSUpdateProxy group.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 71**

Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2008 R2 and are configured as DNS servers.

A domain controller named DC1 has a standard primary zone for contoso.com. A domain controller named DC2 has a standard secondary zone for contoso.com.

You need to ensure that the replication of the contoso.com zone is encrypted. You must not lose any zone data.

What should you do?

- A. On both servers, modify the interface that the DNS server listens on.
- B. Convert the primary zone into an Active Directory-integrated zone. Delete the secondary zone.
- C. Convert the primary zone into an Active Directory-integrated stub zone. Delete the secondary zone.

- D. Configure the zone transfer settings of the standard primary zone. Modify the Master Servers lists on the secondary zone.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

## QUESTION 72

Your network consists of a single Active Directory domain. The domain contains 10 domain controllers. The domain controllers run Windows Server 2008 R2 and are configured as DNS servers.

You plan to create a new Active Directory-integrated zone.

You need to ensure that the new zone is only replicated to four of your domain controllers.

What should you do first?

- A. Create a new delegation in the ForestDnsZones application directory partition.
- B. Create a new delegation in the DomainDnsZones application directory partition.
- C. From the command prompt, run dnscmd and specify the /enlistdirectorypartition parameter.
- D. From the command prompt, run dnscmd and specify the /createdirectorypartition parameter.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

## QUESTION 73

Your network contains a server named Server1. Server1 has the Volume Activation Management Tool (VAMT) installed.

You need to activate Windows on a server named Server2 by using VAMT.

Which firewall rule should you enable on Server2?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Section: Key Management Services (KMS)

Product key management with VAMT enables:

Single local console to manage keys for Windows client, Windows Server and Office 2010 Installation of the

keys on remote managed systems through WMI Tracking remaining activations on MAKs3  
Source: <http://technet.microsoft.com/en-us/library/ff686876.aspx>

#### **QUESTION 74**

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Windows Deployment Services (WDS) server role installed.

You need to ensure that WDS only responds to computers that are prestaged in Active Directory.

Which WDS properties should you modify?

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 75**

Your network contains a server that has the Hyper-V server role installed. The server hosts a virtual machine (VM) named VM1. VM1 runs Windows Server 2008 R2 and has the file server role installed.

You need to add more disk space to VM1. The solution must minimize the amount of downtime for VM1.

What should you do first on VM1?

- A. Add a virtual disk to IDE controller 0.
- B. Add a virtual disk to IDE controller 1.
- C. Add a virtual disk to the SCSI controller.
- D. Add a pass-through disk to IDE controller 0.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 76**

Your network contains a server named Server1 that runs Windows Server 2008 R2. You plan to deploy DirectAccess on Server1.

You need to configure Windows Firewall on Server1 to support DirectAccess connections. What should you allow from Windows Firewall on Server1?

- A. ICMPv6 Echo Requests
- B. IPv6-Route
- C. ICMPv6 Redirect
- D. IGMP

**Correct Answer: A**



**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 77**

Your network contains two servers named Server1 and Server2 that run Windows Server 2008 R2.

Network Access Protection (NAP) is deployed on Server1. Server2 has the Routing and Remote Access service (RRAS) role service installed.

You need to configure Server2 to use NAP VPN enforcement.

Which authentication method should you enable on Server2?

- A. Encrypted authentication (CHAP)
- B. Allow machine certificate authentication for IKEv2
- C. Extensible authentication protocol (EAP)
- D. Microsoft encrypted authentication version 2 (MS-CHAP v2)

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

To deploy NAP with VPN, you must configure the following:

Install and configure Routing and Remote Access as a VPN server. Configure your server running Network Policy Server (NPS) as the primary RADIUS server in Routing and Remote Access.

In NPS, configure VPN servers as RADIUS clients. Also configure connection request policy, network policy, and NAP health policy. You can configure these policies individually using the NPS console, or you can use the New Network Access Protection wizard.

Enable the NAP Remote Access and EAP enforcement clients on NAP-capable client computers.

Enable the NAP service on NAP-capable client computers.

Configure the Windows Security Health Validator (WSHV) or install and configure other system health agents (SHAs) and system health validators (SHVs), depending on your NAP deployment.

If you are using PEAP-TLS or EAP-TLS with smart cards or certificates, deploy a public key infrastructure (PKI) with Active Directory® Certificate Services (AD CS).

If you are using PEAP-MS-CHAP v2, issue server certificates with either AD CS or purchase server certificates from a trusted root certification authority (CA).

**QUESTION 78**

Your network contains a server named Server1. Server1 has DirectAccess deployed. A group named Group1 is enabled for DirectAccess.

Users report that when they log on to their computers, the computers are not configured to use DirectAccess.

You need to ensure that the users' computers are configured to use DirectAccess.

What should you do first?

- A. From Active Directory Users and Computers, add the users' user accounts to Group1.
- B. On each client computer, add Group1 to the Network Configuration Operators group.
- C. From Active Directory Users and Computers, add the users' computer accounts to Group1.
- D. On each client computer, add Group1 to the Distributed COM Users group.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 79

.

Your network consists of a single Active Directory domain. You have a domain controller and a member server that run Windows Server 2008 R2. Both servers are configured as DNS servers. Client computers run either Windows XP Service Pack 3 or Windows 7. You have a standard primary zone on the domain controller. The member server hosts a secondary copy of the zone.

You need to ensure that only authenticated users are allowed to update host (A) records in the DNS zone.

What should you do first?

- A. On the member server, add a conditional forwarder.
- B. On the member server, install Active Directory Domain Services.
- C. Add all computer accounts to the DNSUpdateProxy group.
- D. Convert the standard primary zone to an Active Directory-integrated zone.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 80

.

Your company has an Active Directory domain. The main office has a DNS server named DNS1 that is configured with Active Directory-integrated DNS. The branch office has a DNS server named DNS2 that contains a secondary copy of the zone from DNS1. The two offices are connected with an unreliable WAN link.

You add a new server to the main office. Five minutes after adding the server, a user from the branch office reports that he is unable to connect to the new server. You need to ensure that the user is able to connect to the new server.

What should you do?

- A. Clear the cache on DNS2.
- B. Reload the zone on DNS1.
- C. Refresh the zone on DNS2.
- D. Export the zone from DNS1 and import the zone to DNS2.

**Correct Answer:** C

**Section:** (none)

## **Explanation**

### **Explanation/Reference:**

#### **QUESTION 81**

You need to deploy a read-only domain controller (RODC) that runs Windows Server 2008 R2.

What is the minimal forest functional level that you should use?

- A. Windows Server 2008 R2
- B. Windows Server 2008
- C. Windows Server 2003
- D. Windows 2000

**Correct Answer: C**

**Section: (none)**

## **Explanation**

### **Explanation/Reference:**

#### **QUESTION 82**

Your company has a single Active Directory domain named intranet.contoso.com. All domain controllers run Windows Server 2008 R2. The domain functional level is Windows 2000 native and the forest functional level is Windows 2000.

You need to ensure the UPN suffix for contoso.com is available for user accounts.

What should you do first?

- A. Raise the intranet.contoso.com forest functional level to Windows Server 2003 or higher.
- B. Raise the intranet.contoso.com domain functional level to Windows Server 2003 or higher.
- C. Add the new UPN suffix to the forest.
- D. Change the Primary DNS Suffix option in the Default Domain Controllers Group Policy Object (GPO) to contoso.com.

**Correct Answer: C**

**Section: (none)**

## **Explanation**

### **Explanation/Reference:**

#### **QUESTION 83**

Your company, A. Datum Corporation, has a single Active Directory domain named intranet.adatum.com. The domain has two domain controllers that run Windows Server 2008 R2 operating system. The domain controllers also run DNS servers.

The intranet.adatum.com DNS zone is configured as an Active Directoryintegrated zone with the Dynamic updates setting configured to Secure only. A new corporate security policy requires that the intranet.adatum.com DNS zone must be updated only by domain controllers or member servers.

You need to configure the intranet.adatum.com zone to meet the new security policy requirement.

Which two actions should you perform?

(Each correct answer presents part of the solution. Choose two.)

- A. Remove the Authenticated Users account from the Security tab of the intranet.adatum.com DNS zone properties.
- B. Assign the SELF Account Deny on Write permission on the Security tab of the intranet.adatum.com DNS zone properties.
- C. Assign the server computer accounts the Allow on Write All Properties permission on the Security tab of the intranet.adatum.com DNS zone properties.
- D. Assign the server computer accounts the Allow on Create All Child Objects permission on the Security tab of the intranet.adatum.com DNS zone properties.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 84

<http://www.lead2pass.com/70-649.html>

Your company has an Active Directory forest that contains only Windows Server 2008 domain controllers.

You need to prepare the Active Directory domain to install Windows Server 2008 R2 domain controllers.

Which two tasks should you perform?

<http://www.lead2pass.com/70-649.html>

(Each correct answer presents part of the solution. Choose two.)

- A. Run the adprep /forestprep command.
- B. Run the adprep /domainprep command.
- C. Raise the forest functional level to Windows Server 2008.
- D. Raise the domain functional level to Windows Server 2008.

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 85

You have a test lab that contains 20 client computers and a server named Server1. The client computers run Windows 7. Server1 runs Windows Server 2008 Service Pack 2 (SP2).

You install the Key Management Service (KMS) on Server1.

You need to ensure that the client computers can successfully activate by using Server1.

What should you do?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Minimum Computer Requirements

When planning for KMS activation, the network must meet or exceed the activation threshold, or the minimum number of qualifying computers that KMS requires. You must also understand how the KMS host tracks the number of computers on the network.

KMS Activation Thresholds

KMS can activate both physical computers and virtual machines. To qualify for KMS activation, a network must meet the activation threshold: KMS hosts activate client computers only after meeting this threshold. To ensure that the activation threshold is met, a KMS host counts the number of computers that are requesting activation on the network. For computers running Windows Server 2008 or Windows Server 2008 R2, the activation threshold is five. For computers running Windows Vista or Windows 7, the activation threshold is 25. The thresholds include client

computers and servers that are running on physical computers or virtual machines. Source:<http://technet.microsoft.com/en-us/library/ff793434.aspx>

## Exam

### QUESTION 1

Your network contains a server named Server1 that has the Web Server (IIS) server role installed. The network contains a computer named computer1 that runs Windows 7. Computer has the the Remote Server Administrator Tools (RSAT) installed.

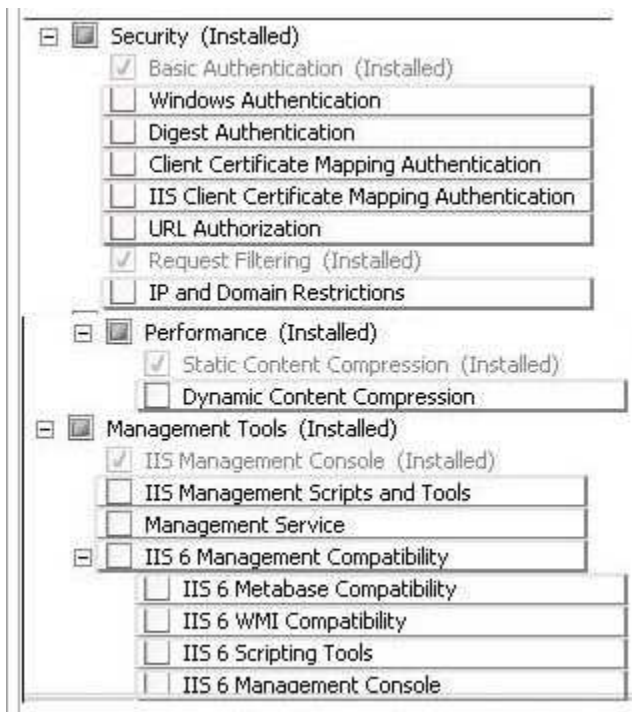
**You need to ensure that you can administer Server1 from Computer1 by using IIS Manager.**

**The solution must minimize the number of roles services installed on Server1.**

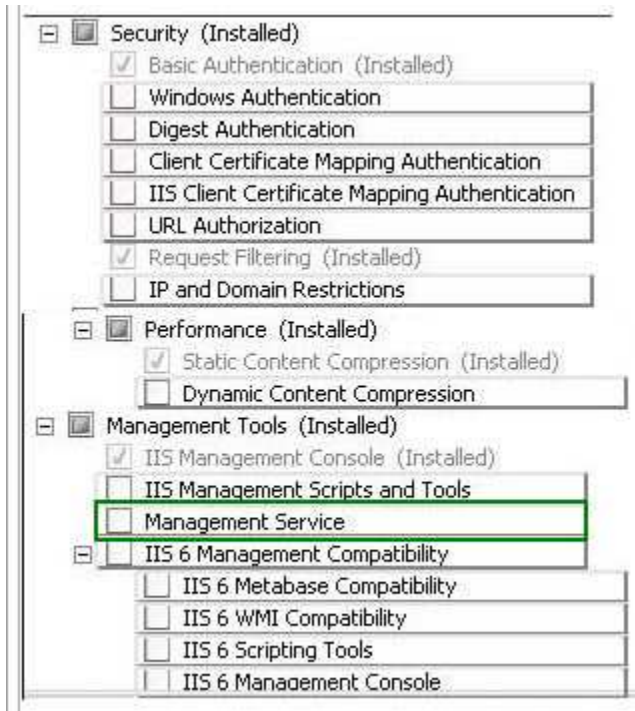
**What should you install on Server1?**

To answer, select the appropriate role service from the Add Role Service dialog box in the answer area.

**Point and Shoot:**



**Correct Answer:**



**Section: (none)**

**Explanation**

**Explanation/Reference:**

## **QUESTION 2**

Your network contains a web server named Server1.

You need to ensure that Server1 authenticates users by using a custom Web page.

**Which authentication method should you enable from IIS Manager?**

To answer, select the appropriate authentication method in the answer area.

**Point and Shoot:**



**Correct Answer:**



**Section: (none)**

**Explanation**

**Explanation/Reference:**

### QUESTION 3

Your network contains a Windows Server Update Services (WSUS) server named Server1. All client computers are configured to download updates from Server1. Server1 is configured only to synchronize manually to Microsoft Update.

Your company deploys a new Microsoft application.

You discover that the new application is not listed on the Products and Classifications list.

You synchronize the WSUS server.



You need to ensure that updates for the new application are available to all of the client computers.

What should you do?

To answer, move the appropriate actions from the Possible Actions list to the Necessary Actions area and arrange them in the correct order.

**Select and Place:**

Possible Actions		Necessary Actions
Add a computer group.		
Approve the updates.		
Move computers to a group.	➡	
Synchronize the WSUS server.	⬅	
Run the Server Cleanup Wizard.		
Modify the Products and Classifications settings.		

**Correct Answer:**

Possible Actions		Necessary Actions
Add a computer group.		Synchronize the WSUS server.
		Modify the Products and Classifications settings.
Move computers to a group.	➡	Approve the updates.
	⬅	
Run the Server Cleanup Wizard.		

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Correct answer(s):

1. Synchronize the WSUS server
2. Modify the Products and Classifications settings
3. Approve the updates

#### QUESTION 4

Your network contains three servers.

The servers are configured as shown in the following table:

Server name	Role service
Server1	Remote Desktop Gateway (RD Gateway)
Server2	Remote Desktop Session Host (RD Sessions Host)
Server3	Network Policy Server (NPS)

You need to configure Server1 to use Network Access Protection (NAP) for all client connections.

Which node from RD Gateway Manager should you use to make this configuration?

To answer, select the appropriate node in the answer area.

Point and Shoot:



Correct Answer:



**Section: (none)**

**Explanation**

**Explanation/Reference:**

### QUESTION 5

Your network contains a Web server named Server1.

You install a server certificate on Server1.

**You need to ensure that users can access the default Web site over HTTPS.**

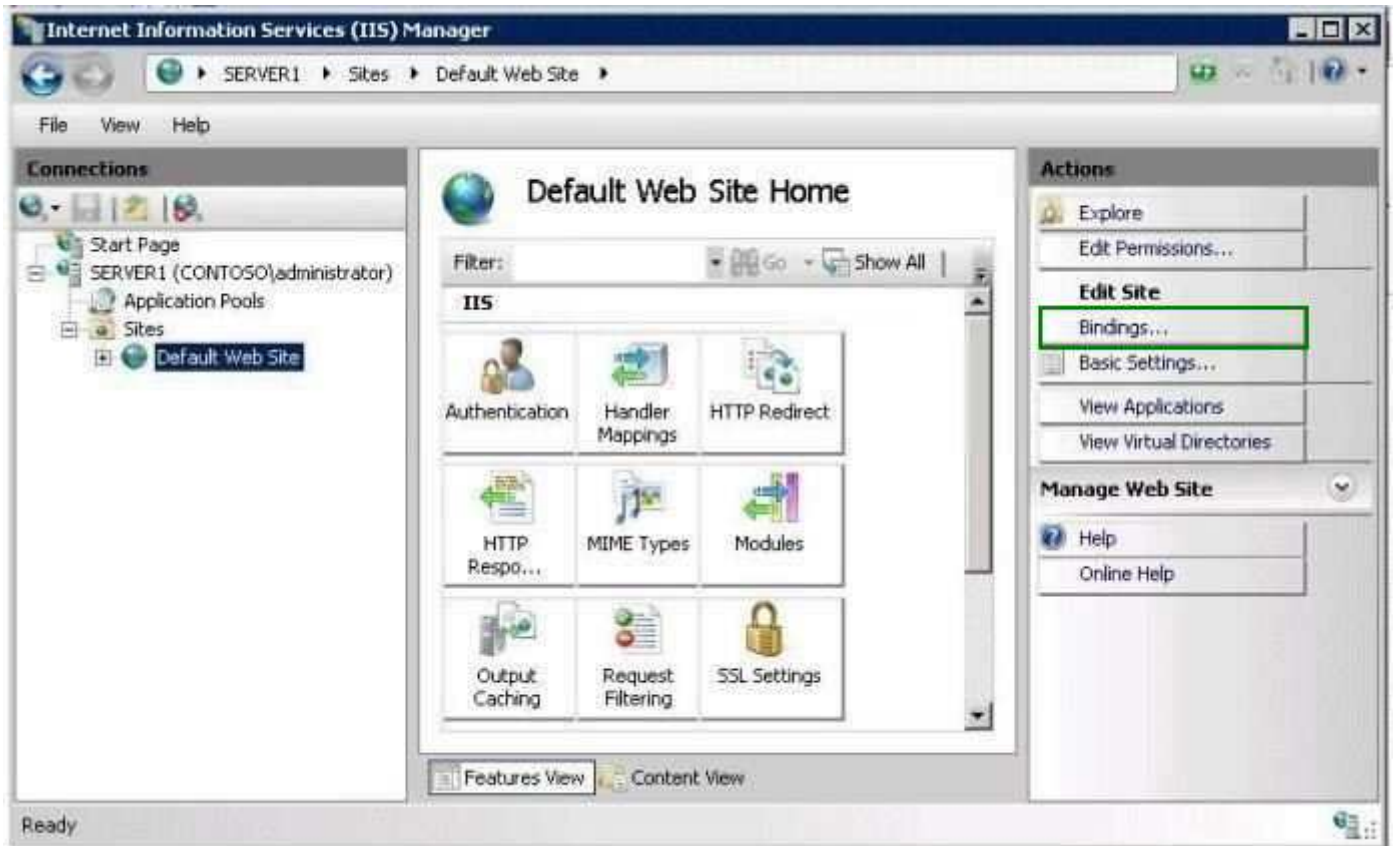
What should you configure from Internet Information Services (IIS) Manager?

To answer, select the appropriate component or action in the answer area.

**Point and Shoot:**



**Correct Answer:**



**Section: (none)**

**Explanation**

**Explanation/Reference:**

Select the Bindings

#### QUESTION 6

Your network contains two servers named Server1 and Server2.

Server1 and Server2 run Windows Server 2008 R2 Enterprise and have the Hyper-V server role installed.

**You need to deploy a Hyper-V host cluster.**

**The solution must ensure that if one of the hosts is disconnected from the shared storage device, all of the virtual machines (VMs) running on the host will continue to run**

What should you do?

To answer, move the appropriate actions from the Possible Actions list to the Necessary Actions area and arrange them in the correct order.

**Build List and Reorder:**

Ordered List Title	Answer Choices Title
<div> <div>▲</div> <div>▼</div> <div></div> </div>	<div> <div>Create Failover Cluster</div> <div>Create a Network Load Balancing (NLB) Cluster</div> <div>Enable Failover Clustering on both servers</div> <div>Enable Storage Manager For SANs on both servers</div> <div>Enable Cluster Share Volumes (CSV) on the cluster</div> <div>Enable Network Load Balancing (NLB) on both servers</div> </div>
	<div> <div>&lt;&lt; Move</div> <div>Remove &gt;&gt;</div> </div>

**Correct Answer:**

Enable Failover Clustering on both servers

Create Failover Cluster

Enable Cluster Share Volumes (CSV) on the cluster

**Section: (none)**

**Explanation**

**Explanation/Reference:**

### QUESTION 7

Your company has a server named VS1 that runs Windows Server 2008 R2 and Hyper-V. The VS1 server hosts 10 virtual servers.

A virtual server named VS-DB has one 64-GB fixed-size virtual hard disk (VHD). The VHD file name is disk1.vhd.

You discover that VS-DB utilizes only 5 GB of the VHD.

You turn off the VS-DB virtual server and want to regain the unused disk space on the VS1 physical server.

**You need to configure VS-DB to make the disk1.vhd file as small as possible.**

What should you do? (To answer, move the appropriate tasks from the list of tasks to the answer area and arrange them in the correct order.)

**Select and Place:**

### Steps, Select from these

Create a new differencing VHD file named disk2.vhd that had disk1.vhd as a parent disk.

Compact the disk2.vhd file

Delete the disk1.vhd file. Rename the disk2.vhd to disk1.vhd

Convert the disk1.vhd file to a new dynamically expanding VHD file named disk2.vhd

Convert the disk2.vhd file to a new fixed-size VHD file named disk1.vhd

### Steps, place here

*Place first step here*

*Place second step, if any, here*

*Place third step, if any, here*

*Place fourth step, if any, here*

*Place fifth step, if any, here*

**Correct Answer:**

### Steps, Select from these

Create a new differencing VHD file named disk2.vhd that had disk1.vhd as a parent disk.

Convert the disk2.vhd file to a new fixed-size VHD file named disk1.vhd

### Steps, place here

Convert the disk1.vhd file to a new dynamically expanding VHD file named disk2.vhd

Compact the disk2.vhd file

Delete the disk1.vhd file. Rename the disk2.vhd to disk1.vhd

*Place fourth step, if any, here*

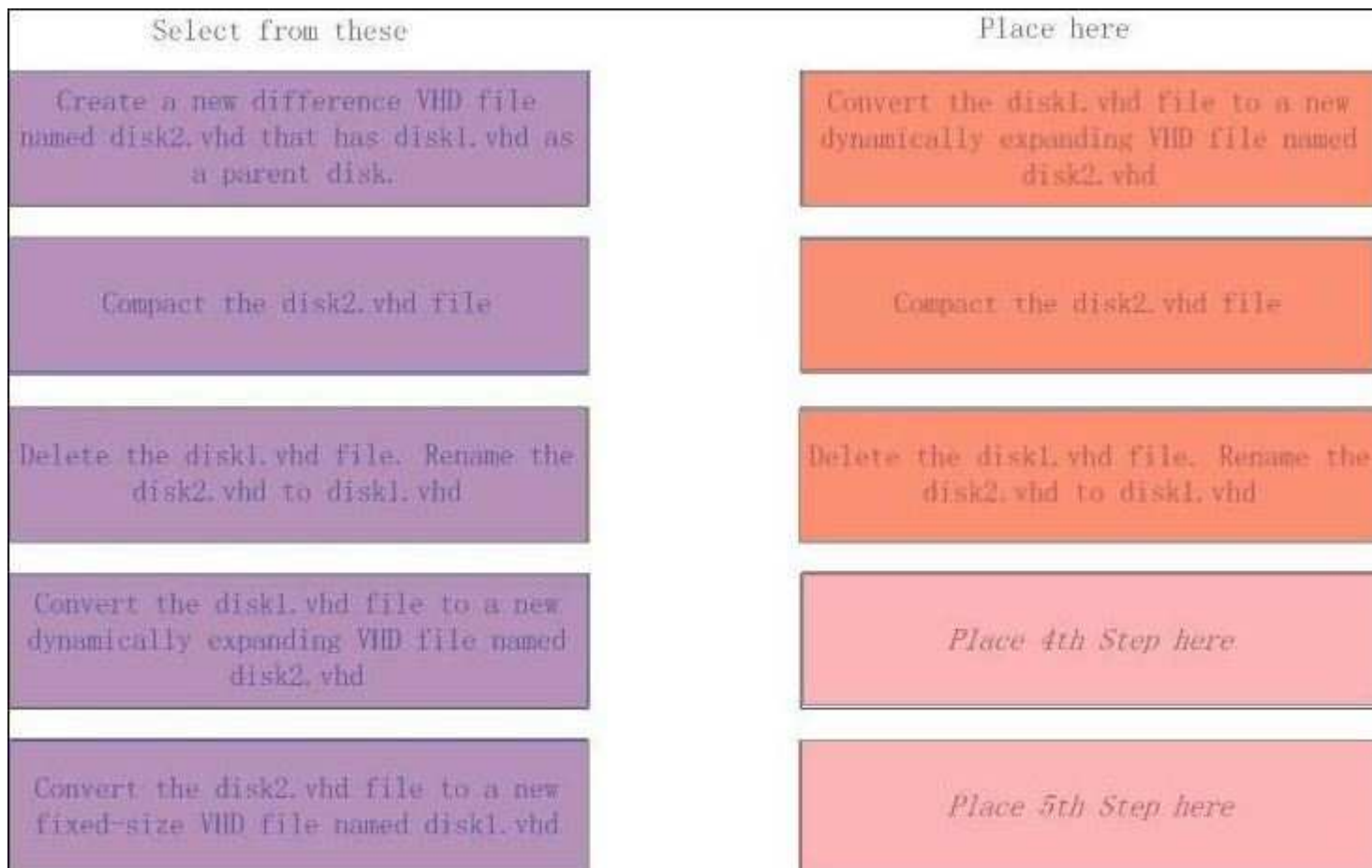
*Place fifth step, if any, here*

Section: (none)

Explanation

Explanation/Reference:





### QUESTION 8

Your network contains a server named Server1 that runs Windows Server 2008 R2. You enable IPSec on Server1. You need to identify which client computers have active IPSec associations to Server1.

Which administrative tool should you use to achieve this task?

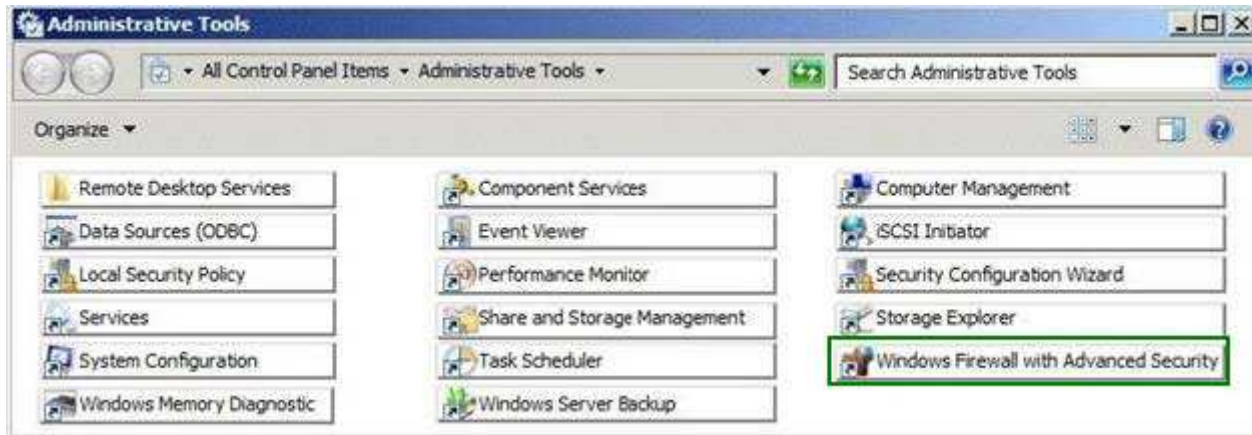
To answer, select the appropriate tool from the answer area.

**Point and Shoot:**



**Correct Answer:**





**Section: (none)**

**Explanation**

**Explanation/Reference:**

Correct answer(s):  
Windows firewall

#### QUESTION 9

You need to modify the Password Replication Policy on a read-only domain controller (RODC).

Which tool should you use?

To answer, select the appropriate tool in the answer area.

**Point and Shoot:**



**Correct Answer:**



**Section: (none)**

**Explanation**

**Explanation/Reference:**

Practically the same as H/Q5.

Reference:

<http://technet.microsoft.com/en-us/library/rodc-guidance-for-administering-the-password-replication-policy.aspx>

### **Administering the Password Replication Policy**

This topic describes the steps for viewing, configuring, and monitoring the Password Replication Policy (PRP) and password caching for read-only domain controllers (RODCs).

#### **To configure the PRP using Active Directory Users and Computers**

1. Open **Active Directory Users and Computers** as a member of the Domain Admins group.
2. Ensure that you are connected to a writeable domain controller running Windows Server 2008 in the correct domain.
3. Click Domain Controllers, and in the details pane, right-click the RODC computer account, and then click Properties.
4. Click the Password Replication Policy tab.
5. The Password Replication Policy tab lists the accounts that, by default, are defined in the Allowed list and the Deny list on the RODC. To add other groups that should be included in either the Allowed list or the Deny list, click Add.
  - To add other accounts that will have credentials cached on the RODC, click Allow passwords for the account to replicate to this RODC.
  - To add other accounts that are not allowed to have credentials cached on the RODC, click Deny passwords for the account from replicating to this RODC.

#### **QUESTION 10**

A server named DC1 has the Active Directory Domain Services (AD DS) role and the Active Directory Lightweight Directory Services (AD LDS) role installed. An AD LDS instance named LDS1 stores its data on the C: drive.

You need to relocate the LDS1 instance to the D: drive.

Which three actions should you perform in sequence?

(To answer, move the three appropriate actions from the list of actions to the answer area and arrange them in

the correct order.)

**Build List and Reorder:**

Ordered List Title	Answer Choices Title
<div><div>▲▼</div><div></div></div>	<div>run the net stop "active directory domain services" command</div> <div>run the net stop LDS1 command</div> <div>use the ntdsutil tool to move the database files.</div> <div>run the xcopy command to move the database files.</div> <div>run the net start LDS1 command.</div> <div>run the net start "active Directory Domain Services" command</div> <div>use the windows backup tool and restore the LDS1 instance to the D: drive</div>
	<div>&lt;&lt; Move</div> <div>Remove &gt;&gt;</div>

**Correct Answer:**

run the net stop LDS1 command

use the ntdsutil tool to move the database files.

run the net start LDS1 command.

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference:

<http://www.ucertify.com/blog/windows-server-2008-tools-used-for-configuring-and-maintaining-active-directory.html>

**NTDSUTIL**

NTDSUTIL.EXE is a command-line tool that is used to manage Active Directory.

**Important Usage**

**To relocate AD LDS directory partition, use the NTDSUTIL tool. Take the following steps:**

- Stop the LDS by using the **net stop** command.
- Move the Database file through **NTDSUTIL** tool.
- Start the directory service using the **net start** command.

**QUESTION 11**

Your network contains two Hyper-V hosts named Server1 and Server2. Server1 and Server2 belong to a failover cluster. Server1 and Server2 are connected to the same 2-terabyte logical unit number (LUN).

You open Failover Cluster Manager as shown in the exhibit. (Click the **Exhibit** button.)

The cluster will host 20 highly available virtual machines (VMs).

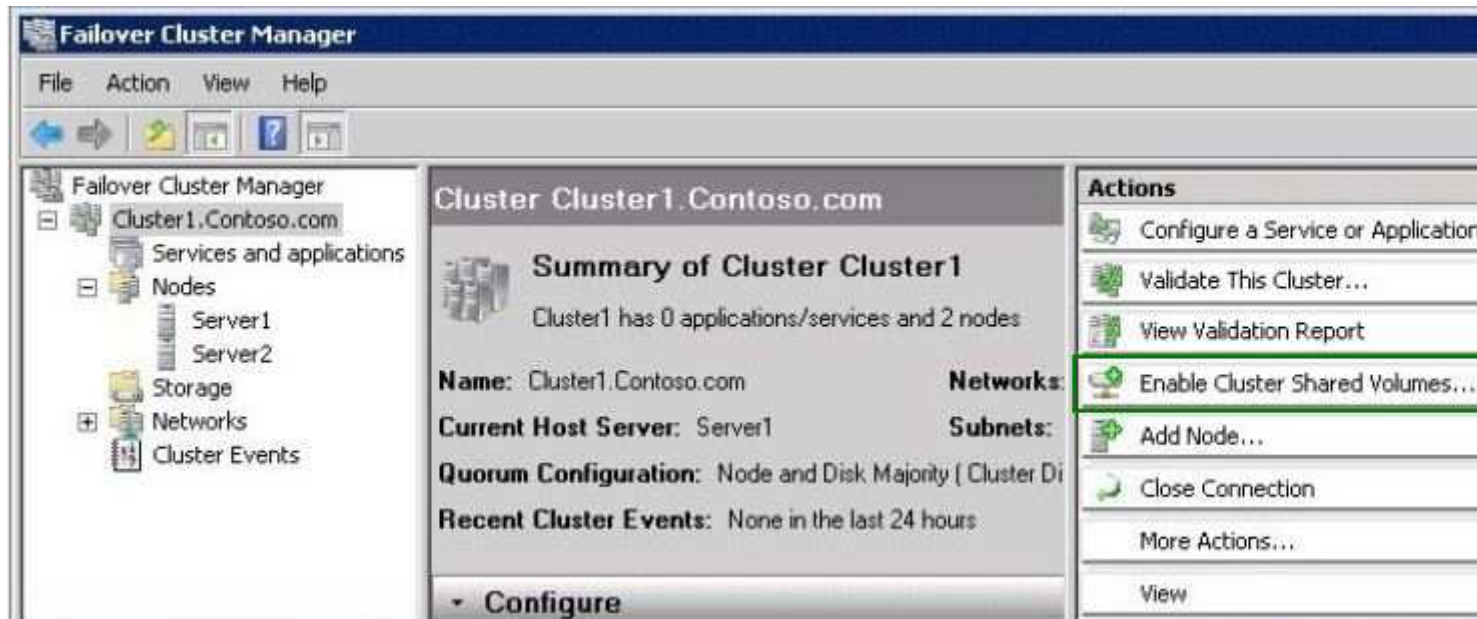
**You need to ensure that the VMs can fail over independently.**

Which action should you select from Failover Cluster Manager?

**Point and Shoot:**



**Correct Answer:**



**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 12

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.

<http://www.lead2pass.com/70-649.html>

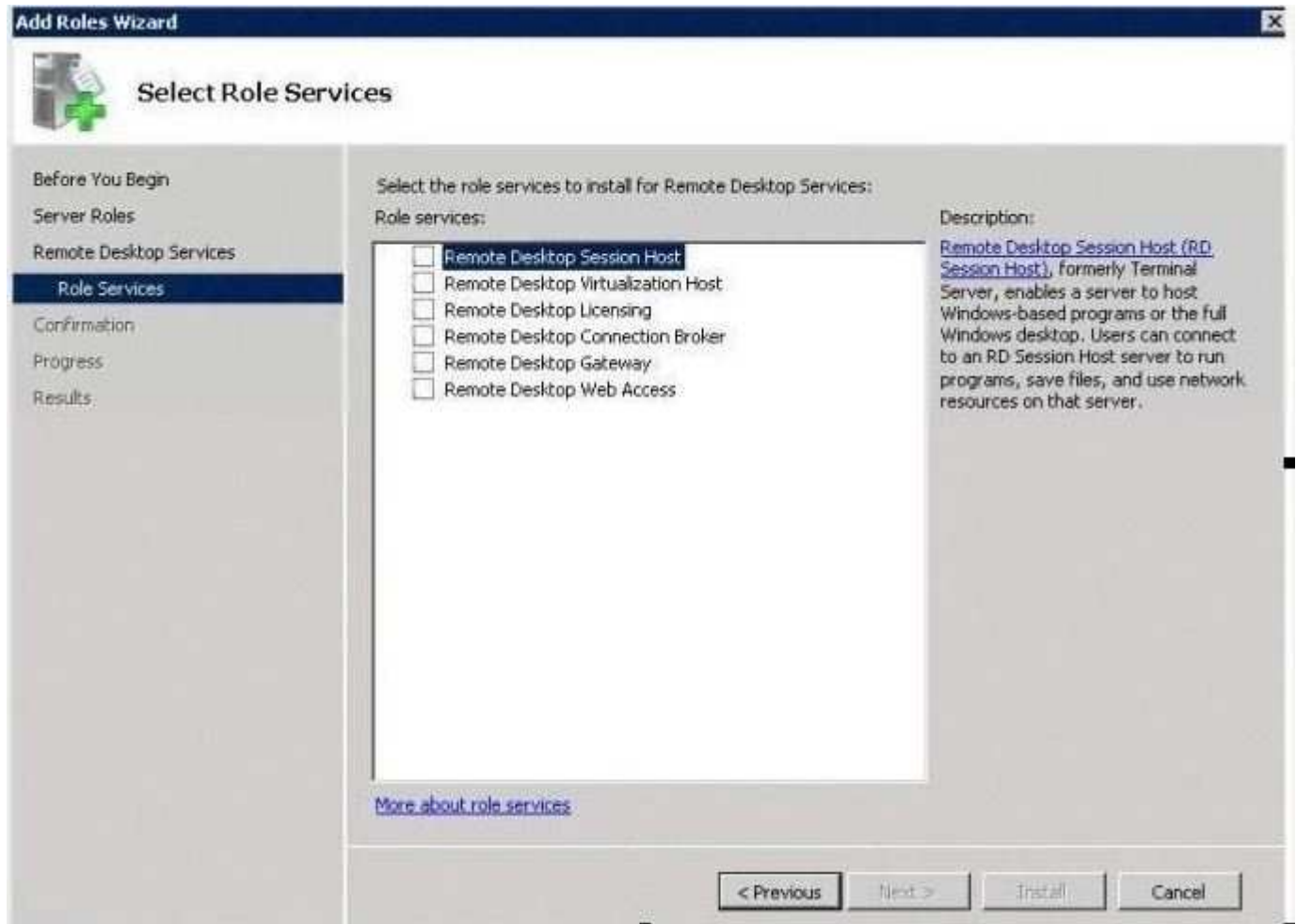
Users connect to Server2 and Server3 to run RemoteApp programs.

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 or role services from the Add Roles Wizard should you install on Server3?

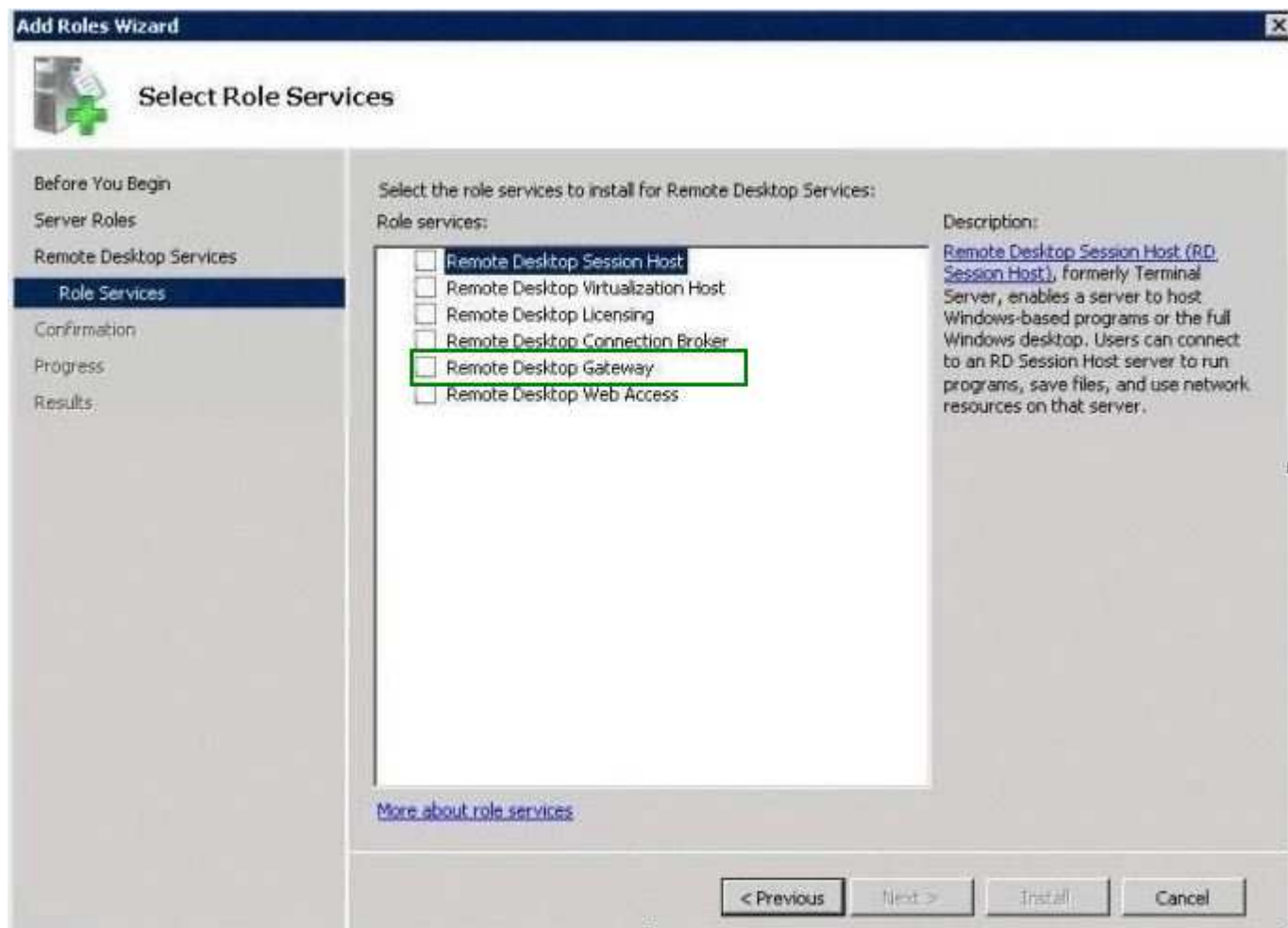
To answer, select the appropriate role service or role services in the answer area. Select only the required role service or role services.

**Point and Shoot:**



**Correct Answer:**





**Section: (none)**

**Explanation**

**Explanation/Reference:**

Original MS exam have an typing error in this question. You must read "Server1" instead of "Server3".  
select RD Gateway Role

### QUESTION 13

You need to perform an offline defragmentation of an Active Directory database. Which four actions should you perform in sequence? (To answer, move the appropriate four actions from the list of actions to the answer area and arrange them in the correct order.)

**Build List and Reorder:**

Ordered List Title	Answer Choices Title
<div> <div>▲</div> <div>▼</div> <div></div> </div>	<div>stop the active directory domain services service.</div> <div>compact the ntds.dit</div> <div>move the ntds.dit file to %windir%\ntds</div> <div>start the active directory domain services service.</div> <div>restart the domain controller in safe mode</div> <div>copy the ntds.dit file to %winder%\sysvol</div>
	<div>&lt;&lt; Move</div> <div>Remove &gt;&gt;</div>

**Correct Answer:**

stop the active directory domain services service.

compact the ntds.dit

move the ntds.dit file to %windir%\ntds

start the active directory domain services service.

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**Correct Answer**

List of Actions	Answer Area
Compact ntds.dit.	Stop the Active Directory Domain Services service.
Move the ntds.dit file to %WINDIR%\NTDS.	Compact ntds.dit.
Restart the domain controller in Safe Mode.	Move the ntds.dit file to %WINDIR%\NTDS.
Start the Active Directory Domain Services service.	Restart the domain controller in Safe Mode.
Copy the ntds.dit file to %WINDIR%\SYSVOL.	Start the Active Directory Domain Services service.
Stop the Active Directory Domain Services service.	

#### QUESTION 14

##### DRAG DROP

Your company has a main office and a branch office. All servers are located in the main office.

The network contains an Active Directory forest named adatum.com. The forest contains a domain controller

named MainDC that runs Windows Server 2008 R2 Enterprise and a member server named FileServer that runs Windows Server 2008 R2 Standard.

You have a kiosk computer named Public\_Computer that runs Windows 7. Public\_Computer is not connected to the network.

You need to join Public\_Computer to the adatum.com domain.

What should you do?

To answer, move the appropriate actions from the Possible Actions list to the Necessary Actions area and arrange them in the correct order.

**Select and Place:**

Possible Actions	Necessary Actions
Restart Public_Computer.	
Copy the BLOB file to MainDC.	
Copy the BLOB file to Public_Computer.	
Run <b>netdom.exe /add</b> on MainDC.	
Run <b>djoin.exe /requestODJ</b> on MainDC.	
Run <b>djoin.exe /provision</b> on FileServer.	
Run <b>netdom.exe /join</b> on Public_Computer.	
Run <b>djoin.exe /provision</b> on Public_Computer.	
Run <b>djoin.exe /requestODJ</b> on Public_Computer.	

**Correct Answer:**



Possible Actions	Necessary Actions
	Run <b>djoin.exe /provision</b> on FileServer.
Copy the BLOB file to MainDC.	Copy the BLOB file to Public_Computer.
	Run <b>djoin.exe /requestODJ</b> on Public_Computer.
Run <b>netdom.exe /add</b> on MainDC.	Restart Public_Computer.
Run <b>djoin.exe /requestODJ</b> on MainDC.	
Run <b>netdom.exe /join</b> on Public_Computer.	
Run <b>djoin.exe /provision</b> on Public_Computer.	

**Section: (none)**  
**Explanation**

**Explanation/Reference:**

#### QUESTION 15

DRAG DROP

Your network contains an Active Directory forest named adatum.com. The forest contains four child domains named europe.adatum.com, northamerica.adatum.com, asia.adatum.com, and africa.adatum.com.





You need to create four new groups in the forest root domain. The groups must be configured as shown in the following table.

Group name	Group members	Group requirement
Group1	A domain local group from adatum.com A universal group from africa.adatum.com	Visible in all domains
Group2	A universal group from europe.adatum.com	Only visible in the adatum.com
Group3	A global group from asia.adatum.com A universal group from northamerica.adatum.com	Only visible in the adatum.com domain
Group4	User accounts from adatum.com	Visible in all domains





What should you do?

To answer, drag the appropriate group type to the correct group name in the answer area.

**Select and Place:**

Group Type	Answer Area	
<input type="text" value="Domain Local"/>	 Group1 <input type="text" value="Group Type"/>	 Group3 <input type="text" value="Group Type"/>
<input type="text" value="Global"/>	 Group2 <input type="text" value="Group Type"/>	 Group4 <input type="text" value="Group Type"/>
<input type="text" value="Universal"/>		

**Correct Answer:**

Group Type	Answer Area	
<input type="text" value="Domain Local"/>	 Group1 <input type="text" value="Universal"/>	 Group3 <input type="text" value="Domain Local"/>
<input type="text" value="Global"/>	 Group2 <input type="text" value="Domain Local"/>	 Group4 <input type="text" value="Global"/>
<input type="text" value="Universal"/>		

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 16**

##### **HOTSPOT**

Your network contains an Active Directory forest.

The DNS infrastructure fails.

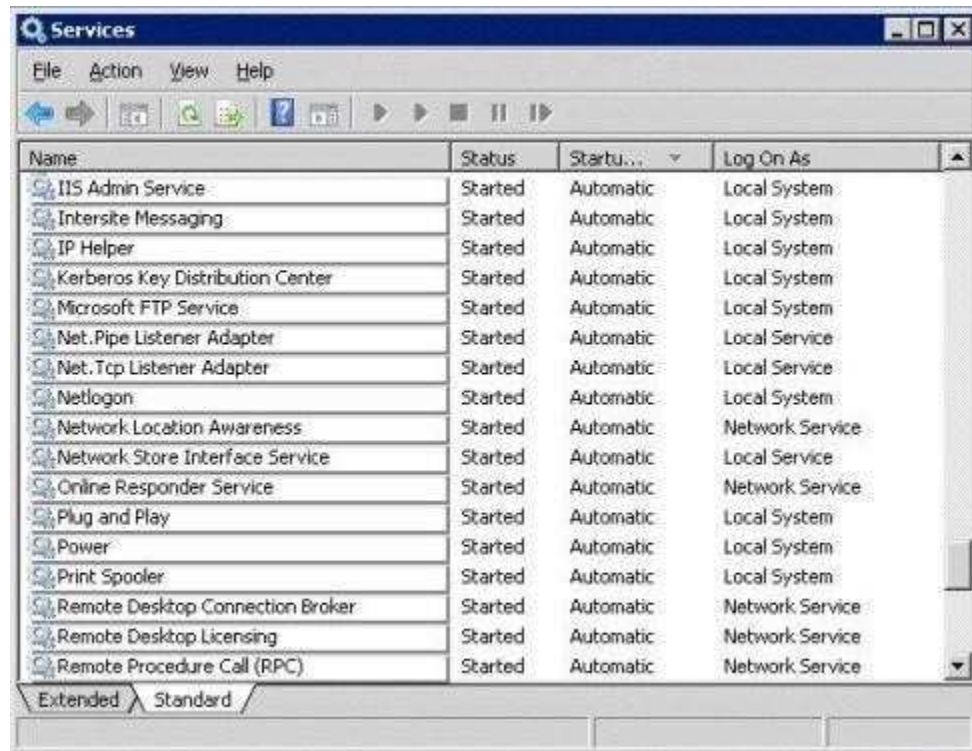
You rebuild the DNS infrastructure.

You need to force the registration of the Active Directory Service Locator (SRV) records in DNS.

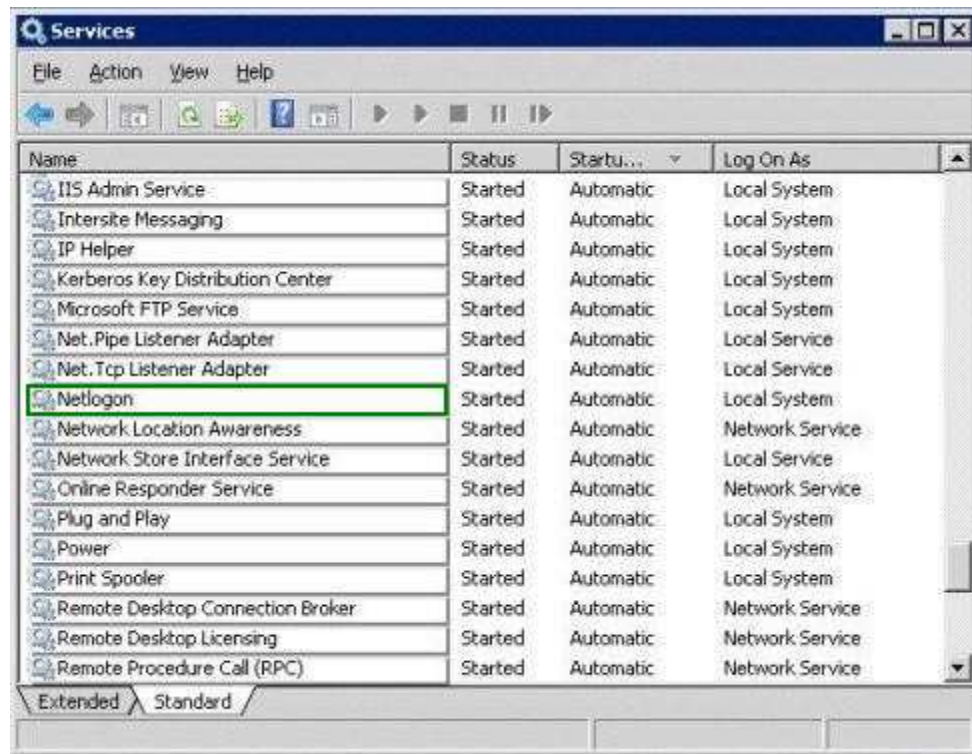
Which service should you restart on the domain controllers?

To answer, select the appropriate service in the answer area.

**Point and Shoot:**



**Correct Answer:**



**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 17

**DRAG DROP**

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

You need to use Group Policies to deploy the line-of-business applications shown in the following table.

Application name	Application requirement
Business_App1	<ul style="list-style-type: none"> <li>The application must be installed the first time the user clicks on the shortcut.</li> <li>An application shortcut must appear on the Start menu of each user's client computer.</li> </ul>
Business_App2	<ul style="list-style-type: none"> <li>Users must be able to install the application from Control Panel on their client computer.</li> <li>An application shortcut must NOT appear on the desktop or the Start menu of the user's client computer until the application is installed.</li> </ul>
Business_App3	<ul style="list-style-type: none"> <li>The application must be installed on the client computer of each user.</li> <li>Only the local Administrators group must be able to uninstall the application.</li> </ul>

What should you do?

To answer, drag the appropriate deployment method to the correct application in the answer area.

**Select and Place:**

Deployment Method	Answer Area
<div>Assign to user</div> <div>Assign to computer</div> <div>Publish to user</div>	<div>Business_</div> <div>Deployment method</div> <div>Business_</div> <div>Deployment method</div> <div>Business_</div> <div>Deployment method</div>

**Correct Answer:**

Deployment Method	Answer Area
<div></div> <div></div> <div></div>	<div>Business_</div> <div>Assign to user</div> <div>Business_</div> <div>Publish to user</div> <div>Business_</div> <div>Assign to computer</div>

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 18**

**HOTSPOT**

Your network contains an Active Directory forest named contoso.com. All client computers run Windows 7 Enterprise.

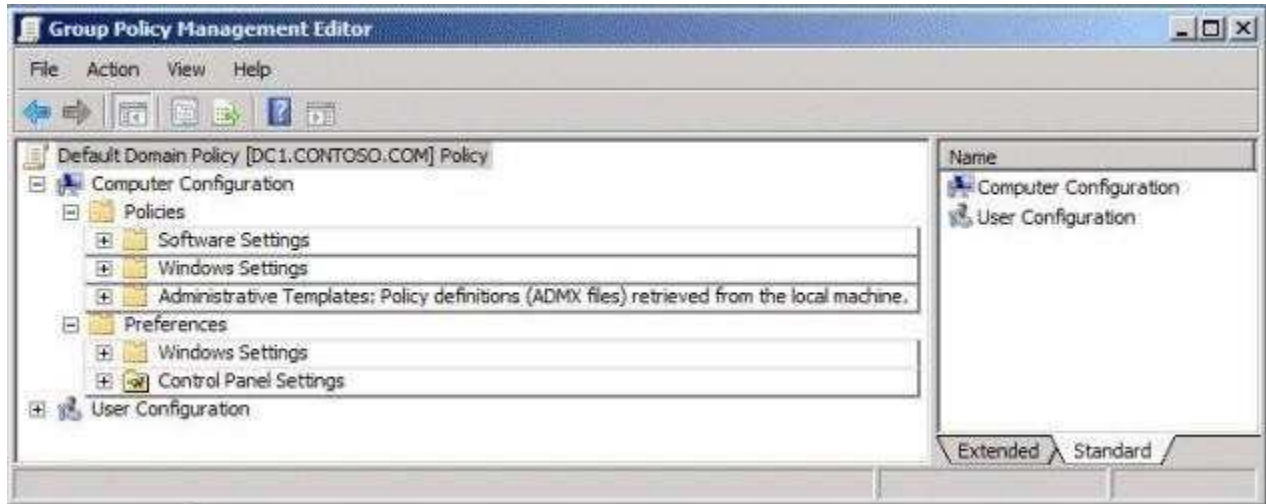


You need to automatically create a local group named PowerManagers on each client computer that contains a battery. The solution must minimize the amount of administrative effort.

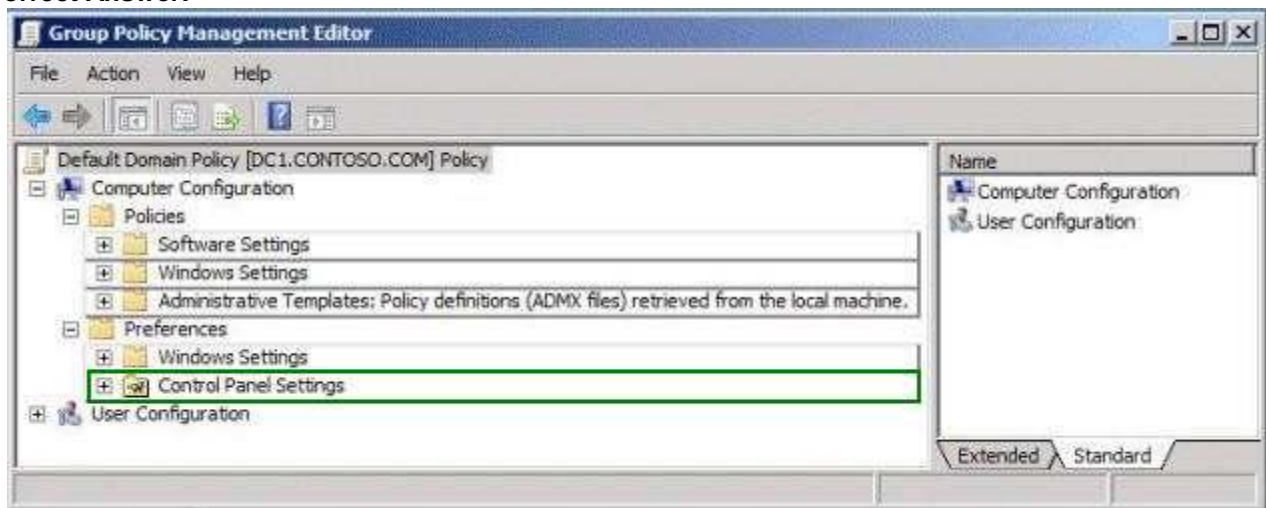
Which node in Group Policy Management Editor should you use?

To answer, select the appropriate node in the answer area.

**Point and Shoot:**



**Correct Answer:**



**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 19

**DRAW DROP**

Your network contains two forests named contoso.com and fabrikam.com. The functional level of all the domains is Windows Server 2003. The functional level of both forests is Windows 2000.

You need to create a trust between contoso.com and fabrikam.com. The solution must ensure that users from contoso.com can only access the servers in fabrikam.com that have the Allowed to Authenticate permission set.

What should you do?

To answer, move the appropriate actions from the Possible Actions list to the Necessary Actions area and arrange them in the correct order.

**Select and Place:**

Possible Actions		Necessary Actions
Create a forest trust.		
Create a shortcut trust.		
Create an external trust.		
Configure SID filtering.	➡	
Configure selective authentication.	⬅	
Configure forest-wide authentication.		
Raise the functional level of all domains.		
Raise the functional level of both forests.		

**Correct Answer:**

Possible Actions		Necessary Actions
Create a forest trust.		Raise the functional level of both forests.
Create a shortcut trust.		Create an external trust.
Configure SID filtering.	➡	Configure selective authentication.
	⬅	
Configure forest-wide authentication.		
Raise the functional level of all domains.		

Section: (none)

## Explanation

### Explanation/Reference:

## QUESTION 20

### DRAG DROP

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

You need to create an Active Directory Rights Management Services (AD RMS) licensing-only cluster.

What should you do?

To answer, move the appropriate actions from the Possible Actions list to the Necessary Actions area and arrange them in the correct order.

### Select and Place:

Possible Actions		Necessary Actions
Deploy AD RMS policy templates.		
Create an AD RMS root cluster.		
Create an AD RMS licensing-only cluster.		
Install Microsoft SQL Server 2008.	➡	
Install the Failover Clustering feature.	⬅	
Install the Active Directory Certificate Services (AD CS) role.		

### Correct Answer:



Possible Actions	Necessary Actions
	Install Microsoft SQL Server 2008.
	Create an AD RMS root cluster.
	Create an AD RMS licensing-only cluster.
	Deploy AD RMS policy templates.
Install the Failover Clustering feature.	
Install the Active Directory Certificate Services (AD CS) role.	

**Section: (none)**

**Explanation**

**Explanation/Reference:**

### QUESTION 21

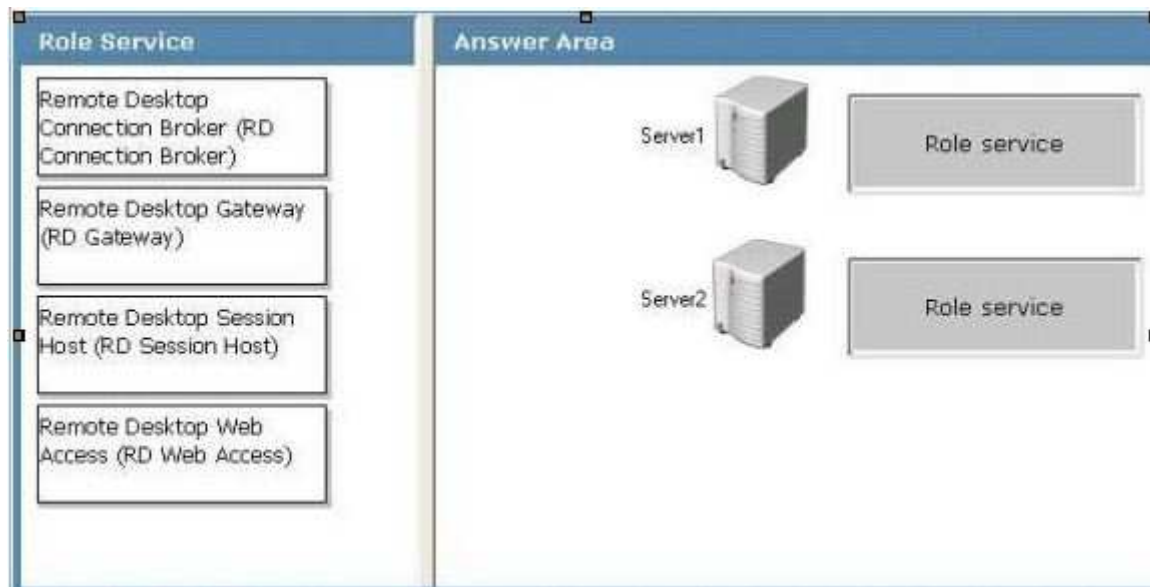
Your network contains two servers named Server1 and Server2 that run Windows Server 2008 R2. You plan to publish a RemoteApp program named App1 to Server2.

You need to ensure that App1 appears as a RemoteApp program when you connect to <https://server1/rdweb>.

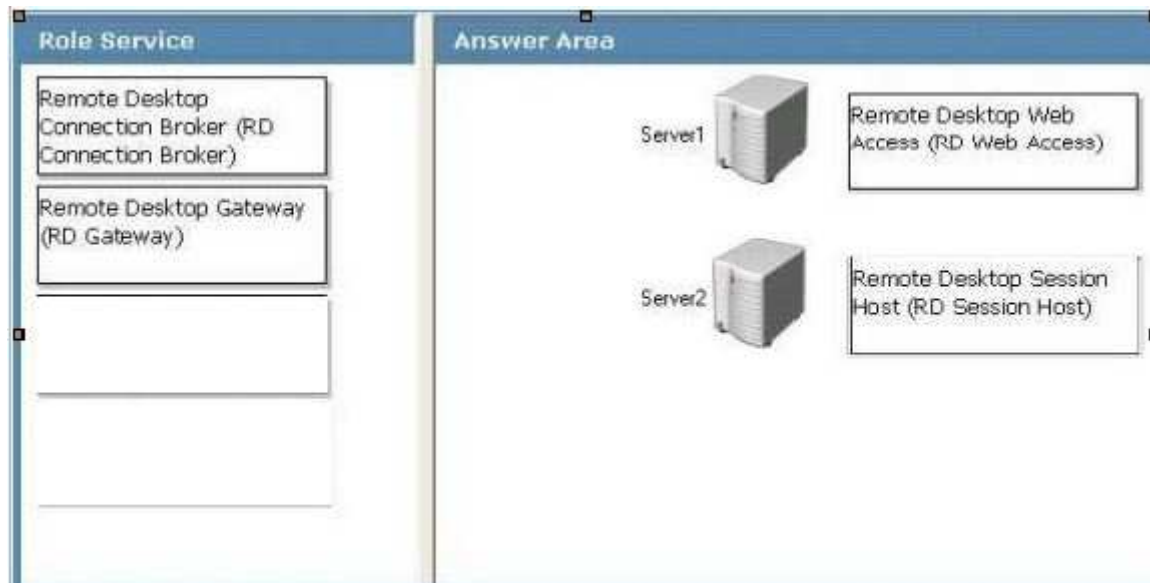
**Which role services should you install on Server1 and Server2?**

To answer, drag the appropriate role service to the correct server in the answer area.

**Select and Place:**



**Correct Answer:**



**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 22

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

Server name	Server configuration
Server1	Windows Server 2008 R2 Enterprise (64-bit) Remote Desktop Session Host (RD Session Host)
Server2	Windows Server 2008 R2 Enterprise (64-bit) Remote Desktop Web Access (RD Web Access)

All client computers run the 32-bit version of Windows Vista.

Your company purchases a new sales application named SalesApp1.  
SalesApp1 is a 64-bit application.  
SalesApp1 is associated with the .abc file extension.

**You need to ensure that when users in the sales department open files that have the .abc file extension, SalesApp1 automatically opens.**

What should you do?

To answer, move the appropriate actions from the Possible Actions list to the Necessary Actions area and arrange them in the correct order.

**Build List and Reorder:**

Ordered List Title	Answer Choices Title
<div><div>▲▼</div><div></div></div>	<div>Install SalesApp1 on Server2</div> <div>Create a RemoteApp program on Server2</div> <div>Create a Remote Desktop Connection (.rdp) file</div> <div>Create a Windows Installer package for SalesApp1</div> <div>Deploy the Windows Installer package by using a Group Policy object (GPO)</div> <div>Deploy the Remote Desktop Connection (.rdp) file by using a Group Policy object (GPO)</div>
	<div>&lt;&lt; Move</div> <div>Remove &gt;&gt;</div>

**Correct Answer:**

Install SalesApp1 on Server2

Create a RemoteApp program on Server2

Create a Windows Installer package for SalesApp1

Deploy the Windows Installer package by using a Group Policy object (GPO)

**Section: (none)**

**Explanation**

**Explanation/Reference:**



<http://www.gratisexam.com/>