

**2016 NEW 70-417 Questions and
Answers & NEW 70-417 Study Guide
612q RELEASED Today!**

【Exam Code】 [70-417](#)

【Exam Name】 Upgrading Your Skills to MCSA Windows
Server 2012

【Certification Provider】 Microsoft

【Corresponding Certifications】 MCSE, MCSE: Server
Infrastructure

2016 NEW 70-417 Study Guides:

MCSA, MCSA: Windows Server 2012, MCSE, MCSE: Communication,
MCSE: Desktop Infrastructure, MCSE: Messaging, MCSE: Private Cloud,
MCSE: Server Infrastructure, MCSE: SharePoint

**Braindump2go 2016 NEW 70-417 Questions and
Answers [612Q](#) Free Share: [61-80](#)**

QUESTION 61

Hotspot Question

You have a file server named Server1 that runs Windows Server 2012 R2.

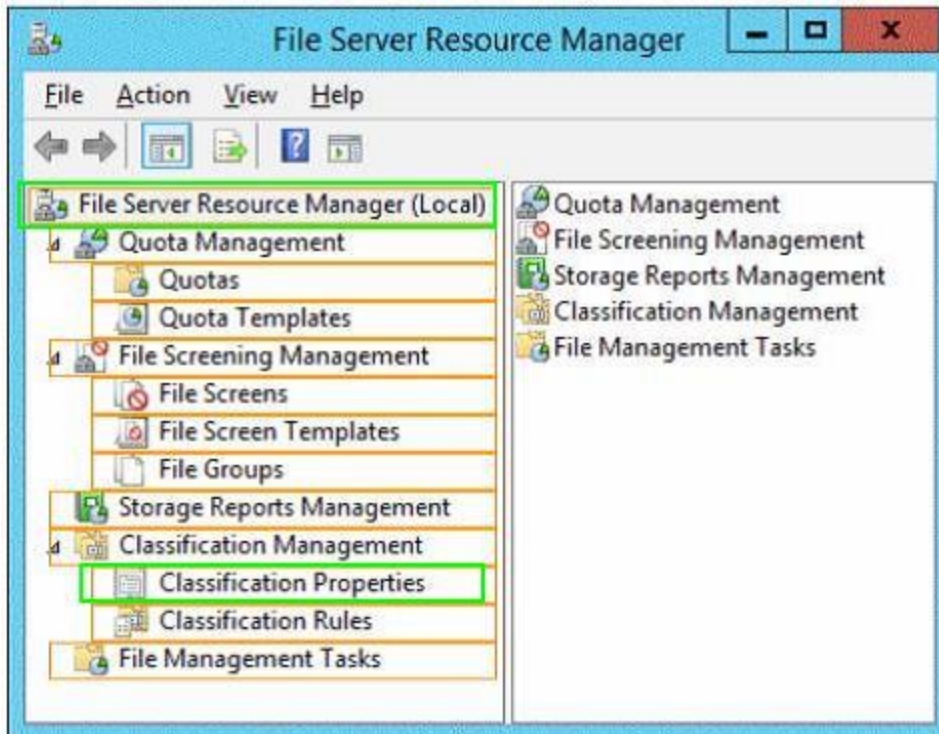
Server1 contains a file share that must be accessed by only a limited number of users.

You need to ensure that if an unauthorized user attempts to access the file share, a custom access-denied message appears, which contains a link to request access to the share. The message must not appear when the unauthorized user attempts to access other shares.

Which two nodes should you configure in File Server Resource Manager? To answer, select the appropriate two nodes in the answer area.

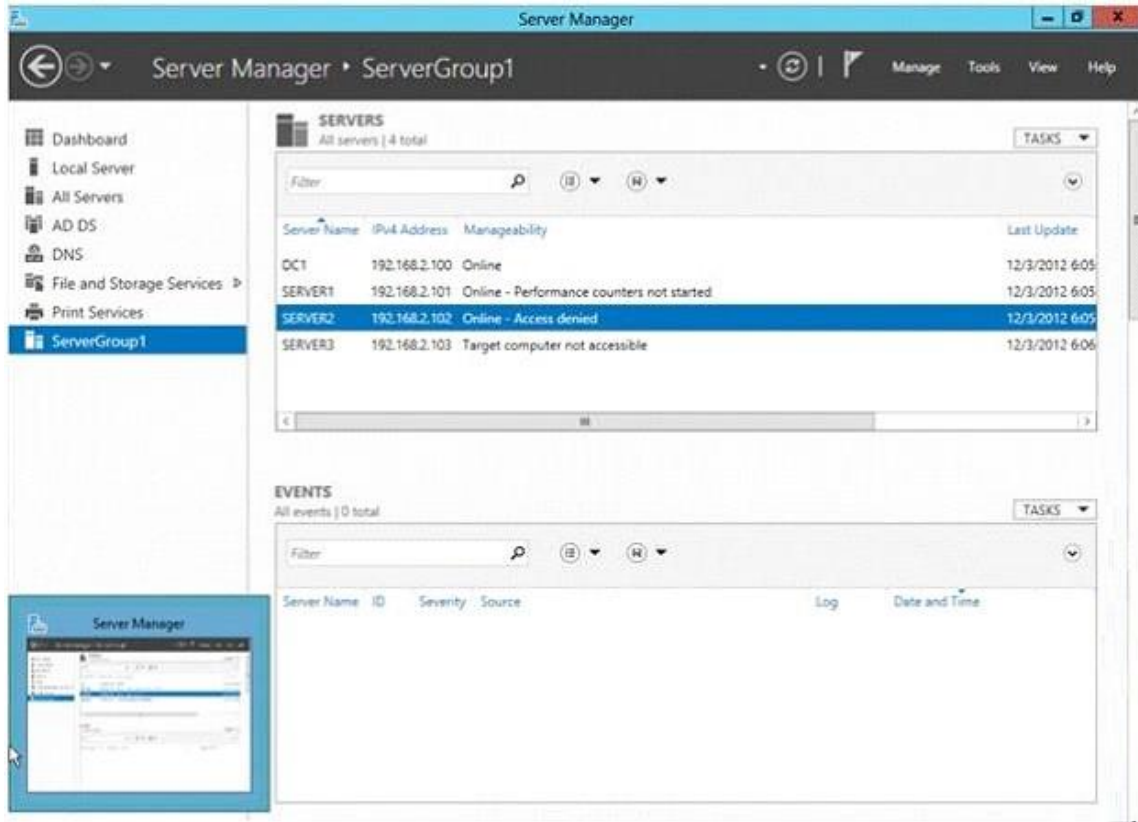


Answer:



QUESTION 62

Your network contains an Active Directory domain named contoso.com. The domain contains three servers named Server1, Server2, and Server3. You create a server group named ServerGroup1. You discover the error message shown in the following exhibit. (Click the Exhibit button.)



You need to ensure that Server2 can be managed remotely by using Server Manager. What should you do?

- A. On Server2, run the netdom.exe command.
- B. On Server2, run the net stop netlogon command, and then run the net start netlogon command.
- C. On DC1, run the Enable-PSSessionConfigurationcmdlet.
- D. On Server2, modify the membership of the Remote Management Users group.

Answer: D

Explanation:

This is a security issue. To be able to access Server2 remotely through Server Manager the user need to be a member of the Remote Management Users group.

QUESTION 63

You have a server named Server1 that runs Windows Server 2012 R2. Server1 has six network adapters. Two of the network adapters are connected to a network named LAN1, two of the network adapters are connected to a network named LAN2, and two of the network adapters are connected to a network named LAN3.

You create a network adapter team named Team1 from the two adapters connected to LAN1.

You create a network adapter team named Team2 from the two adapters connected to LAN2.

A company policy states that all server IP addresses must be assigned by using a reserved address in DHCP.

You need to identify how many DHCP reservations you must create for Server1.

How many reservations should you identify?

- A. 3
- B. 4

- C. 6
- D. 8

Answer: B

Explanation:

2 Adapters = LAN1 = Team1 = 1 IP
2 Adapters = LAN2 = Team2 = 1 IP
2 Adapters = LAN3 = No Team = 2 IP
1 + 1 + 2 = 4

QUESTION 64

Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC5. DC5 has a Server Core Installation of Windows Server 2012 R2. You need to uninstall Active Directory from DC5 manually. Which tool should you use?

- A. The Remove-ADComputercmdlet
- B. The ntdsutil.exe command
- C. The dsamain.exe command
- D. The Remove-WindowsFeaturecmdlet

Answer: D

Explanation:

<http://technet.microsoft.com/en-us/library/jj205471.aspx>

QUESTION 65

You have a server named Server1. You install the IP Address Management (IPAM) Server feature on Server1. You need to provide a user named User1 with the ability to set the access scope of all the DHCP servers that are managed by IPAM. The solution must use the principle of least privilege. Which user role should you assign to User1?

- A. IP Address Record Administrator Role
- B. IPAM Administrator Role
- C. IPAM MSM Administrator Role
- D. IPAM DHCP Scope Administrator Role

Answer: B

Explanation:

IPAM Administrator Role This built-in role provides all permissions that are provided by the IPAM ASM Administrator Role and IPAM MSM Administrator Role in addition to permissions to manage access scopes, access policies, and logical groups.

QUESTION 66

Your network contains two servers that run Windows Server 2012 R2 named Server1 and Server2. Both servers have the File Server role service installed. On Server2, you create a share named Backups. From Windows Server Backup on Server1, you schedule a full backup to run every night. You set the backup destination to \\Server2 \Backups. After several weeks, you discover that \\Server2\Backups only contains the last backup that completed on Server1. You need to ensure that multiple backups of Server1 are maintained. What should you do?

- A. Modify the properties of the Windows Store Service (WSService) service.
- B. Change the backup destination.
- C. Modify the Volume Shadow Copy Service (VSS) settings.
- D. Configure the permission of the Backups share.

Answer: B

QUESTION 67

Your network contains an Active Directory domain named contoso.com. The domain contains a main office and a branch office. An Active Directory site exists for each office. The domain contains two servers named Server1 and Server2 that run Windows Server 2012 R2. Both servers have the DHCP Server server role installed. Server1 is located in the main office site. Server2 is located in the branch office site. Server1 provides IPv4 addresses to the client computers in the main office site. Server2 provides IPv4 addresses to the client computers in the branch office site.

You need to ensure that if either Server1 or Server2 are offline, the client computers can still obtain IPv4 addresses. The solution must meet the following requirements:

The storage location of the DHCP databases must not be a single point of failure. Server1 must provide IPv4 addresses to the client computers in the branch office site only if Server2 is offline. Server2 must provide IPv4 addresses to the client computers in the main office site only if Server1 is offline.

Which configuration should you use?

- A. Load sharing mode failover partners
- B. Hot standby mode failover partners
- C. A Network Load Balancing (NLB) cluster
- D. A failover cluster

Answer: B

Explanation:

<http://blogs.technet.com/b/teamdhcp/archive/2012/06/28/ensuring-high-availability-of-dhcpusing-windowsserver-2012-dhcp-failover.aspx>

Ensuring

High Availability of DHCP using Windows Server 2012 R2 DHCP Failover The Hot Standby mode results in an Active-Passive configuration. You will be required to designate one of the two DHCP servers as the active server and the other as standby. The standby server is dormant with regard to serving client requests as long as the active server is up.

However,

the standby server receives all the inbound lease updates from the active DHCP server and keeps its database up to date.

<http://blogs.technet.com/b/teamdhcp/archive/2012/09/03/dhcp-fail-over-hot-standbymode.aspx>

DHCP Failover Hot-Standby Mode In the previous blog on DHCP Failover, we discussed the DHCP failover load balance mode where both DHCP servers respond to client requests and load balance the requests between them based on an admin specified load distribution ratio. In the other mode of a failover relationship, known as the Hot-Standby mode (ActivePassive), only one of the servers actively leases IP addresses and option configuration to clients in given subnet(s)/scope(s) while the other server (standby) is passive. The standby server services the clients, only in event of active server being down. The clients fallback to the active server once the active server becomes available again post the outage. The Load balance mode is more suited for single site deployment where the 2 DHCP servers in a failover relationship are co-located with the subnets/scopes being served by them. As the servers are in network proximity with the clients, the clients do not experience any latency while acquiring or renewing an IP address. Hot-Standby mode is more suited for multi-site deployment topologies. Each site would have a local DHCP server which is configured to provide the DHCP service to the clients on the local network and DHCP server at a remote site would be standby server. In a normal state of

operation, computers and devices on a given site receive IP addresses and other network configuration from the DHCP server located at the same site as the clients. However, in the event of the local DHCP server being down, the DHCP server from the remote site would provide the service to the clients.

You could choose to deploy hot standby mode in a single-site deployment also if you need to.

QUESTION 68

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

The domain contains two servers named Server1 and Server2. Both servers have the IP Address Management (IPAM) Server feature installed.

You have a support technician named Tech1.

Tech1 is a member of the IPAM Administrators group on Server1 and Server2.

You need to ensure that Tech1 can use Server Manager on Server1 to manage IPAM on Server2.

To which group on Server2 should you add Tech1.

- A. IPAM MSM Administrators
- B. IPAM Administrators
- C. WinRMRemoteWMIUsers_
- D. Remote Management Users

Answer: C

Explanation:

Since the user is already a member of IPAM administrators group (and the IPAM MSM Administrators Administrators group provides access that is already available to the IPAM Administrators group), Then, about the debate on winRMRemoteWMIUsers VS Remote Management Users, i know they're told to have exactly the same permissions, but in the IPAM Microsoft documentation, they don't talk about Remote Management Users, not even once on 97 pages, whereas this is said about winRMRemoteWMIUsers_:

Understand and Troubleshoot IP Address Management (IPAM) in Windows Server 8 Beta If you are accessing the IPAM server remotely using ServerManager IPAM client RSAT, then you must be a member of the WinRMRemoteWMIUsers group on the IPAM server, in addition to being a member of the appropriate IPAM security group (or local Administrators group).



Note:

A domain user connecting to the IPAM server from a remote IPAM client must be a member of the 'WinRMRemoteWMIUsers_' group on the IPAM server in addition to being a member of the appropriate IPAM security group. IPAM client is available with the Server Manager RSAT. Server Manager RSAT is also available with the installation on a Windows 8 Consumer Preview client machine. The Server Manager navigation tree by default on the Windows 8 RSAT.

<http://social.technet.microsoft.com/wiki/contents/articles/13444.windows-server-2012server-managertroubleshooting-guide-part-ii-troubleshoot-manageability-status-errors-inserver-manager.aspx>

Windows

Server 2012 - Server Manager Troubleshooting Guide, Part II: Troubleshoot Manageability Status Errors in Server Manager Error

<computer name>: Configuration refresh failed with the following error: The metadata failed to be retrieved from the server, due to the following error: Access is denied. The user is attempting to manage the remote server with a credential that has only standard user (not a member of the Administrators group) access rights on the target server, and the user has not enabled standard user remote management of the target server. By default, an account with

[70-417 Dumps](#) [70-417 Exam Questions](#) [70-417 PDF](#) [70-417 VCE](#)

<http://www.braindump2go.com/70-417.html>

standard user access rights is not a part of the WinRM remote WMI user's group, and can perform limited management tasks on a remote server in Server Manager. To allow standard users more management access rights on a target server, run the Enable-ServerManagerStandardUserRemotingcmdlet on the target server, in a Windows PowerShell session that has been opened with elevated user rights (Run as Administrator). For more information about how to use this cmdlet (and disable standard user management access when it is no longer needed), see the cmdlet Help topic for Enable-ServerManagerStandardUserRemoting [This link is external to TechNet Wiki. It will open in a new window.]

QUESTION 69

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the Active Directory Certificate Services server role installed and is configured as an enterprise certification authority (CA).

You need to ensure that all of the users in the domain are issued a certificate that can be used for the following purposes:

- Email security
- Client authentication
- Encrypting File System (EFS)

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

- A. Modify the properties of the User certificate template, and then publish the template.
- B. From a Group Policy, configure the Certificate Services Client - Certificate Enrollment Policy settings.
- C. From a Group Policy, configure the Automatic Certificate Request Settings settings.
- D. Duplicate the User certificate template, and then publish the template.
- E. From a Group Policy, configure the Certificate Services Client - Auto-Enrollment settings.

Answer: DE

Explanation:

The default user template supports all of the requirements EXCEPT autoenroll as shown below:

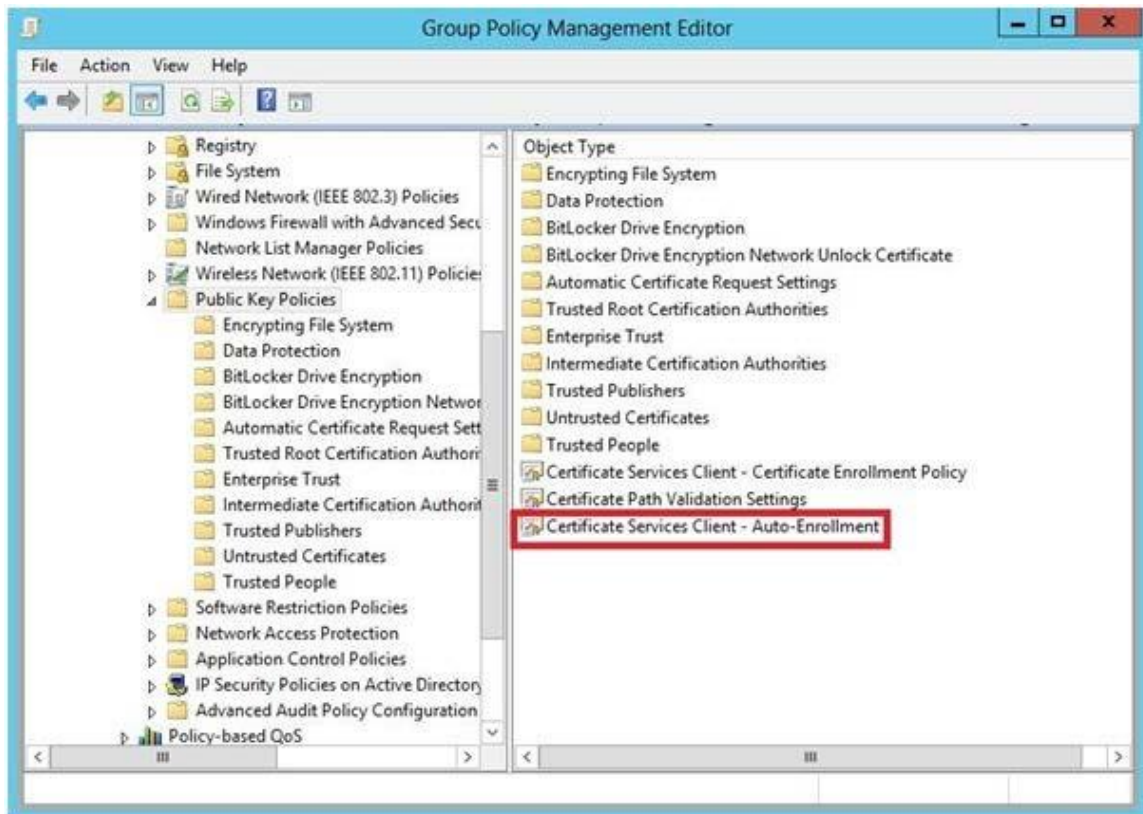
Permissions for Authenticated Users	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Enroll	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click **Advanced**.

However a duplicated template from users has the ability to autoenroll:

Permissions for Authenticated Users	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Enroll	<input type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The Automatic Certificate Request Settings GPO setting is only available to Computer, not user.



QUESTION 70

You manage an environment that has many servers. The servers run Windows Server 2012 R2 and use iSCSI storage. Administrators report that it is difficult to locate available iSCSI resources on the network.

You need to ensure that the administrators can locate iSCSI resources on the network by using a central repository.

Which feature should you deploy?

- A. The iSNS Server service feature
- B. The iSCSI Target Storage Provider feature
- C. The Windows Standards-Based Storage Management feature
- D. The iSCSI Target Server role service

Answer: A

Explanation:

<http://technet.microsoft.com/en-us/library/cc772568.aspx>

iSNS Server Overview

Internet iStorage Name Service Server

The Internet Storage Name Service (iSNS) protocol is used for interaction between iSNS servers and iSNS clients. iSNS clients are computers, also known as initiators, that are attempting to discover storage devices, also known as targets, on an Ethernet network. iSNS facilitates automated discovery, management, and configuration of iSCSI and Fibre Channel devices (using iFCP gateways) on a TCP/IP network. Note The Microsoft iSNS Server only supports the discovery of iSCSI devices, and not Fibre Channel devices. iSNS Server provides intelligent storage discovery and management services comparable to those found in Fibre Channel networks, allowing a commodity IP network to function in a similar capacity as a storage area network. iSNS facilitates a seamless integration of IP networks and manages iSCSI devices. iSNS thereby provides value in any storage network comprised of iSCSI devices.

Features of iSNS Server iSNS Server is a repository of currently active iSCSI nodes, as well as their associated portals, entities, etc.

Nodes can be initiators, targets, or management nodes. Typically, initiators and targets register with the iSNS server, and the initiators query the iSNS server for the list of available targets.

A dynamic database of the iSCSI devices and related information that are currently available on the network:

The database helps provide iSCSI target discovery functionality for the iSCSI initiators on the network. The database is kept dynamic by using the Registration Period and Entity Status Inquiry features of iSNS.

Registration Period allows the server to automatically deregister stale entries. Entity Status Inquiry provides the server a functionality similar to ping to determine whether registered clients are still present on the network, and allows the server to automatically deregister those clients which are no longer present. State Change Notification Service: This allows registered clients to be made aware of changes to the database in the iSNS server. It allows the clients to maintain a dynamic picture of the iSCSI devices available on the network.

Discovery Domain Service: This allows an administrator to assign iSCSI nodes and portals into one or more groups called discovery domains. Discovery domains provide a zoning functionality by which an iSCSI initiator can only discover those iSCSI targets who have at least one discovery domain in common with it.

Benefits of iSNS Server in iSCSI Storage Area Networks Centralized management

Easily scalable to large IP storage networks

Extensible

Asynchronous notification of changes in the iSCSI storage network Ability to monitor the status and availability of clients Microsoft-preferred discovery method for iSCSI

Designed for Windows Logo Program requirement for iSCSI HBAs

QUESTION 71

You have a server named Server1 that runs Windows Server 2012 R2.

You download and install the Microsoft Online Backup Service Agent on Server1.

You need to ensure that you can configure an online backup from Windows Server Backup.

What should you do first?

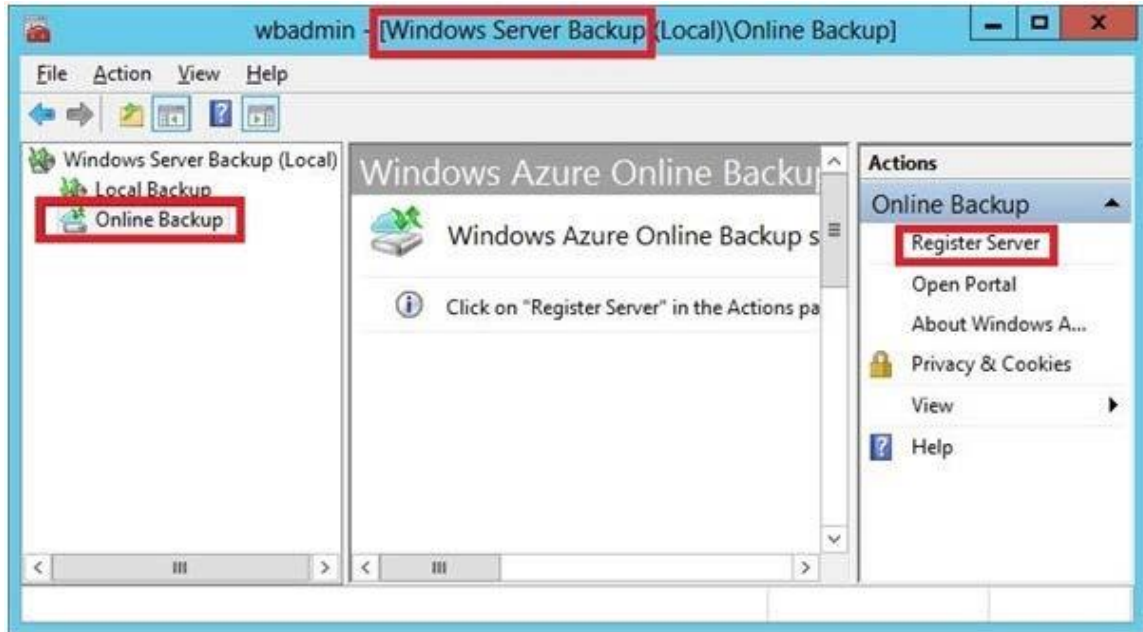
- A. From a command prompt, run `wbadmin.exe enable backup`.
- B. From Windows Server Backup, run the Register Server Wizard.
- C. From the Services console, modify the Log On settings of the Microsoft Online Backup Service Agent.
- D. From Computer Management, add the Server1 computer account to the Backup Operators group.

Answer: B

Explanation:

Download and install the Windows Azure Online Backup Agent After you create an account on the Windows Azure Online Backup website, you can download the Windows Azure Online

Backup Agent and install it locally. An Online Backup node then appears in the navigation pane of the Windows Server Backup console, as shown in Figure 12-



If you prefer, you can also configure online backups from the Windows Azure Online Backup console, which becomes available after you install the agent. The Windows Azure Online Backup console provides exactly the same set of options as the Online Backup node in the Windows Server Backup console.

Register server The next step is to register your server. Registering a server enables you to perform backups from that same server only. (Remember this point for the exam.)

To register the server, from the Actions menu, select Register Server.

The Register Server Wizard includes two configuration steps. First, you are given an opportunity to specify a proxy server if desired. Second, you are asked to provide a passphrase that will be used to encrypt your backup data and a location to save this passphrase in a file.

You need to provide this passphrase when you perform a restore operation, so it's essential that you don't lose it. (Microsoft doesn't maintain a copy of your passphrase.) A Generate Passphrase option creates the passphrase for you automatically.

After you register a server, new options for Online Backup appear in the Actions pane, including Schedule Backup, Recover Data, Change Properties, and Unregister Server.

QUESTION 72

Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. Both servers have the Hyper-V server role installed. You plan to replicate virtual machines between Server1 and Server2. The replication will be encrypted by using Secure Sockets Layer (SSL).

You need to request a certificate on Server1 to ensure that the virtual machine replication is encrypted.

Which two intended purposes should the certificate for Server1 contain? (Each correct answer presents part of the solution. Choose two.)

- A. Server Authentication
- B. KDC Authentication
- C. Kernel Mode Code Signing
- D. IP Security end system
- E. Client Authentication

Answer: AE

Explanation:

<http://blogs.technet.com/b/virtualization/archive/2012/03/13/hyper-v-replica-certificaterequirements.aspx>

Replica Server Certificate Requirements

To enable a server to receive replication traffic, the certificate in the replica server must meet the following conditions

- **Enhanced Key Usage** must support both **Client and Server authentication**
- Set the Subject field or the Subject Alternative Name using **one** of the following methods:
 - For a SAN certificate, set the Subject Alternative Name's DNS Name to the replica server name (e.g.: *replica1.contoso.com*). If the replica server is part of cluster, the Subject Alternative Name of the certificate must contain the replica server name ***and*** FQDN of the HVR Broker (install this certificate on all the nodes of the cluster.)

QUESTION 73

Drag and Drop Question

You have a file server named Server1 that runs Windows Server 2012 R2.

The folders on Server1 are configured as shown in the following table.

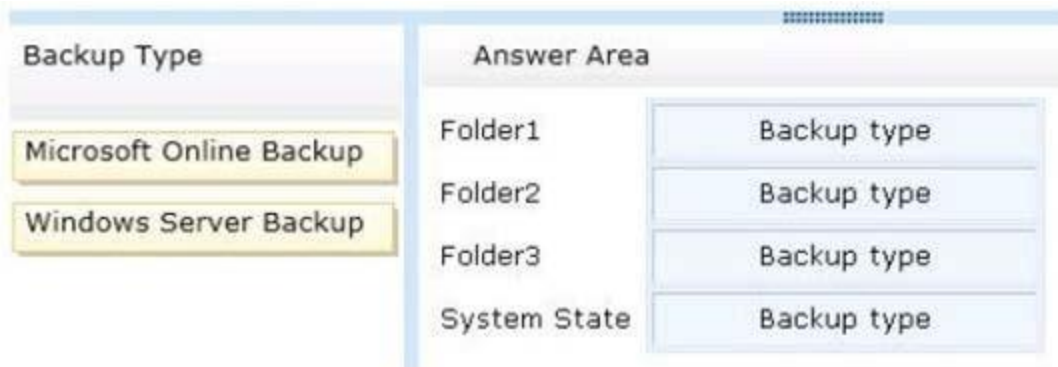
Folder name	NTFS encryption	NTFS compression
Folder1	No	No
Folder2	Yes	No
Folder3	No	Yes

A new corporate policy states that backups must use Microsoft Online Backup whenever possible.

You need to identify which technology you must use to back up Server1.

The solution must use Microsoft Online Backup whenever possible.

What should you identify? To answer, drag the appropriate backup type to the correct location or locations. Each backup type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:

Backup Type	Answer Area
Microsoft Online Backup	Folder1 Microsoft Online Backup
Windows Server Backup	Folder2 Microsoft Online Backup
	Folder3 Microsoft Online Backup
	System State Windows Server Backup

QUESTION 74

Your network contains an Active Directory domain named contoso.com. The domain contains two member servers named Server1 and Server2 that run Windows Server 2012 R2. Both servers have the Hyper-V server role installed. The network contains an enterprise certification authority (CA). All servers are enrolled automatically for a certificate-based on the Computer certificate template. On Server1, you have a virtual machine named VM1. VM1 is replicated to Server2. You need to encrypt the replication of VM1.

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

- A. On Server1, modify the settings of VM1.
- B. On Server2, modify the settings of the virtual switch to which VM1 is connected.
- C. On Server1, modify the Hyper-V Settings.
- D. On Server1, modify the settings of the virtual switch to which VM1 is connected.
- E. On Server2, modify the settings of VM1.
- F. On Server2, modify the Hyper-V Settings.

Answer: AF

Explanation:

Once you change the Hyper-V Settings of Server 2 to encrypt replications with a certificate, you then need to change the replication information of VM1 to use the secure connection.

QUESTION 75

Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1 that runs Windows Server 2012 R2. You create a user account named User1 in the domain. You need to ensure that User1 can use Windows Server Backup to back up Server1. The solution must minimize the number of administrative rights assigned to User1. What should you do?

- A. Assign User1 the Back up files and directories user right.
- B. Add User1 to the Backup Operators group.
- C. Add User1 to the Power Users group.
- D. Assign User1 the Back up files and directories user right and the Restore files and directories user right.

Answer: A

Explanation:

Backup Operators have these permissions by default:

- 10 210 Back up files and directories
- 10 210 Restore files and directories
- 10 210 Shut down the system

- Administrators, Backup Operators
- Administrators, Backup Operators
- Administrators, Backup Operators

However the question explicitly says we need to minimize administrative rights. Since the requirement is for backing up the data only--no requirement to restore or shutdown--then assigning the "Back up files and directories user right" would be the correct. answer.

Back up files and directories

This user right determines which users can bypass file and directory, registry, and other persistent object permissions for the purposes of backing up the system.

Specifically, this user right is similar to granting the following permissions to the user or group in question on all files and folders on the system:

- Traverse Folder/Execute File
- List Folder/Read Data
- Read Attributes
- Read Extended Attributes
- Read Permissions

QUESTION 76

You have a datacenter that contains six servers. Each server has the Hyper-V server role installed and runs Windows Server 2012 R2. The servers are configured as shown in the following table.

Host name	Processor manufacturer	Storage type
Host1	Intel	Local disk
Host2	AMD	iSCSI disk
Host3	Intel	iSCSI disk
Host4	Intel	Cluster Shared Volume (CSV)
Host5	Intel	Cluster Shared Volume (CSV)
Host6	AMD	iSCSI disk

Host4 and Host5 are part of a cluster named Cluster1. Cluster1 hosts a virtual machine named VM1. You need to move VM1 to another Hyper-V host. The solution must minimize the downtime of VM1. To which server and by which method should you move VM1?

- A. To Host3 by using a storage migration
- B. To Host6 by using a storage migration
- C. To Host2 by using a live migration
- D. To Host1 by using a quick migration

Answer: A

Explanation:

The processor vendors should be the same so Host2 and Host6 are not possible answers Local disk cannot be used neither so Host1 is not a possible answer neither For more information about VM storage migration:

<http://technet.microsoft.com/en-us/library/hh831656.aspx>

Virtual Machine Storage Migration Overview Applies

To: Windows Server 2012 R2 In Windows Server 2008 R2, you can move a running instance of a virtual machine using live migration, but you are not able to move the virtual machine's storage while the virtual machine is running.

Hyper-V in Windows Server 2012 R2 introduces support for moving virtual machine storage without downtime by making it possible to move the storage while the virtual machine remains running. You can perform this task by using a new wizard in Hyper-V Manager or by using new Hyper-V cmdlets for Windows PowerShell.

You can add storage to either a stand-alone computer or to a Hyper-V cluster, and then move virtual machines to the new storage while the virtual machines continue to run. The most common reason for moving a virtual machine's storage is to update the physical storage that is available to Hyper-V. You can also move virtual machine storage between physical storage devices, at run time, to respond to reduced performance that results from bottlenecks in the storage throughput. Key benefits Hyper-V in Windows Server 2012 R2 makes it possible to move virtual machine storage while a virtual machine is running.

Requirements

You need the following to use the Hyper-V functionality of moving virtual machine storage:

One or more installations of Windows Server 2012 R2 with the Hyper-V role installed.

A server that is capable of running Hyper-V.

Specifically, it must have processor support for hardware virtualization.

Virtual machines that are configured to use only virtual hard disks for storage.

NOTE: You cannot move the storage of a virtual machine when any of its storage is directly attached to a physical disk.

Technical overview This new feature allows you to move the virtual hard disks of a virtual machine while those virtual hard disks remain available for use by the running virtual machine.

When you move a running virtual machine's virtual hard disks, Hyper-V performs the following steps, as shown in Figure 1:

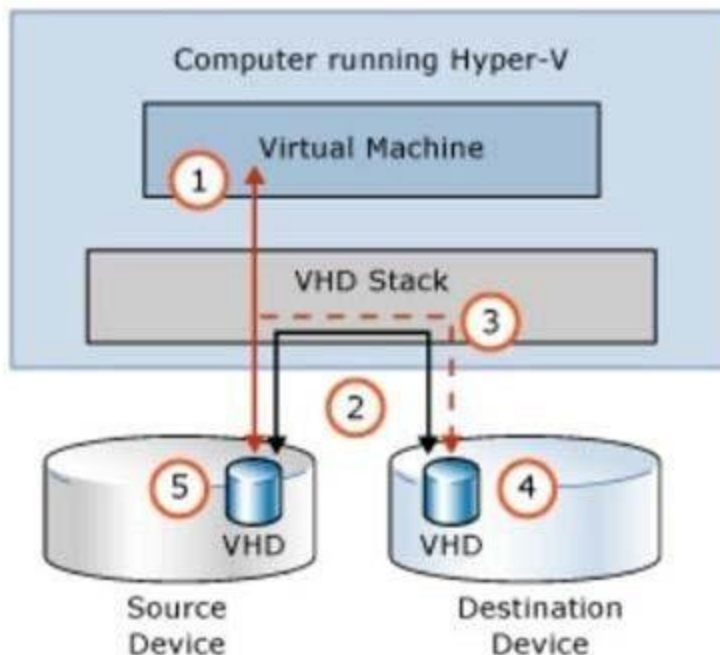


Figure 1 Moving virtual hard disks

Throughout most of the move operation, disk reads and writes go to the source virtual hard disk. While reads and writes occur on the source virtual hard disk, the disk contents are copied to the

new destination virtual hard disk. After the initial disk copy is complete, disk writes are mirrored to both the source and destination virtual hard disks while outstanding disk changes are replicated. After the source and destination virtual hard disks are completely synchronized, the virtual machine switches over to using the destination virtual hard disk. The source virtual hard disk is deleted.

QUESTION 77

Your network contains an active directory domain named Contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. You create a group Managed Service Account named gservice1. You need to configure a service named service1 to run as the gservice1 account. How should you configure service1?

- A. From Services Console configure the recovery settings
- B. From a command prompt ,run sc.exe and specify the config parameter
- C. From Windows PowerShell,run Set-Service and specify the -PassThrough parameter
- D. From a command prompt ,run sc.exe and specify the sdset parameter

Answer: B

Explanation:

Executing the sc.exe command with the config parameter will modify service configuration.

QUESTION 78

Your network contains an Active Directory domain named adatum.com. The domain contains a domain controller named Server1. On Server1, you create a new volume named E. You restart Server1 in Directory Service Restore Mode. You open ntdsutil.exe and you set NTDS as the active instance. You need to move the Active Directory logs to E:\NTDS\. Which Ntdsutil context should you use?

- A. IFM
- B. Files
- C. Configurable Settings
- D. Partition management

Answer: B

Explanation:

<http://support.microsoft.com/kb/816120#5>

How to Move Log Files

Use the **move logs to** command to move the directory service log files to another folder. For the new settings to take effect, restart the computer after you move the log files.

To move the log files, follow these steps:

1. Click **Start**, click **Run**, type **ntdsutil** in the **Open** box, and then press ENTER.
2. At the Ntdsutil command prompt, type **files**, and then press ENTER.
3. At the file maintenance command prompt, type **move logs to new location** (where *new location* is an existing folder that you have created for this purpose), and then press ENTER.
4. Type **quit**, and then press ENTER.
5. Restart the computer.

QUESTION 79

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2. The domain contains two servers. The servers are configured as shown in the

following table.

Server name	Configuration
DC1	DNS server Domain controller Enterprise certification authority (CA)
Server2	Network Policy Server (NPS) Health Registration Authority (HRA)

All client computers run Windows 8 Enterprise.

You plan to deploy Network Access Protection (NAP) by using IPsec enforcement. A Group Policy object (GPO) named GPO1 is configured to deploy a trusted server group to all of the client computers.

You need to ensure that the client computers can discover HRA servers automatically.

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

- A. On Server2, configure the EnableDiscovery registry key.
- B. On DC1, create an alias (CNAME) record.
- C. On DC1, create a service location (SRV) record.
- D. In a GPO, modify the Request Policy setting for the NAP Client Configuration.
- E. On all of the client computers, configure the EnableDiscovery registry key.

Answer: CDE

Explanation:

[http://technet.microsoft.com/en-us/library/dd296901\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd296901(v=ws.10).aspx)

▲ Requirements for HRA automatic discovery

The following requirements must be met in order to configure trusted server groups on NAP client computers using HRA automatic discovery:

- Client computers must be running Windows Vista® with Service Pack 1 (SP1) or Windows XP with Service Pack 3 (SP3).
- The HRA server must be configured with a Secure Sockets Layer (SSL) certificate.
- The **EnableDiscovery** registry key must be configured on NAP client computers.
- DNS SRV records must be configured.
- The trusted server group configuration in either local policy or Group Policy must be cleared.

QUESTION 80

Your network contains an Active Directory domain named adatum.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 is configured as a Network Policy Server (NPS) server and as a DHCP server.

You need to ensure that only computers that send a statement of health are checked for Network Access Protection (NAP) health requirements.

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

- A. The NAP-Capable Computers conditions
- B. The MS-Service Class conditions
- C. The NAS Port Type constraints
- D. The Called Station ID constraints
- E. The Health Policies conditions

Answer: AE

Explanation:

[70-417 Dumps](#) [70-417 Exam Questions](#) [70-417 PDF](#) [70-417 VCE](#)

<http://www.braindump2go.com/70-417.html>

The NAP-Capable ensures that the machine is able to send a statement of health, and the Health Policy tells it which policy to evaluate against.

