

**70-417.403q**

Number: 70-417  
Passing Score: 800  
Time Limit: 120 min  
File Version: 1

**Microsoft 70-417**

**Upgrading Your Skills to MCSA Windows Server 2012**

**Exam A**

**QUESTION 1**

**HOTSPOT**

Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2012 R2. The servers have the Hyper-V server role installed.

A certification authority (CA) is available on the network.

A virtual machine named vm1.contoso.com is replicated from Server1 to Server2. A virtual machine named vm2.contoso.com is replicated from Server2 to Server1.

You need to configure Hyper-V to encrypt the replication of the virtual machines.

Which common name should you use for the certificates on each server?

To answer, configure the appropriate common name for the certificate on each server in the answer area.

**Hot Area:**

Server name	Common name
Server1	<input type="text"/> server1.contoso.com server2.contoso.com vm1.contoso.com vm2.contoso.com
Server2	<input type="text"/> server1.contoso.com server2.contoso.com vm1.contoso.com vm2.contoso.com

**Correct Answer:**

Server name	Common name
Server1	<input type="text"/> server1.contoso.com server2.contoso.com vm1.contoso.com vm2.contoso.com
Server2	<input type="text"/> server1.contoso.com server2.contoso.com vm1.contoso.com vm2.contoso.com

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 2**

You have five servers that run Windows Server 2012 R2. The servers have the Failover Clustering feature installed.

You deploy a new cluster named Cluster1. Cluster1 is configured as shown in the following table.

Site name	Server name
Site1	Server1 Server2 Server3
Site2	Server4 Server5

Server1, Server2/ and Server3 are configured as the preferred owners of the cluster roles. Dynamic quorum management is disabled.

You plan to perform hardware maintenance on Server3.

You need to ensure that if the WAN link between Site1 and Site2 fails while you are performing maintenance on Server3, the cluster resource will remain available in Site1.

What should you do?

- A. Remove the node vote for Server3.
- B. Enable DrainOnShutdown on Cluster1.
- C. Add a file share witness in Site1.
- D. Remove the node vote for Server4 and Server5.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Exclude secondary site nodes.

In general, do not give votes to WSFC (Windows Server Failover Clustering) nodes that reside at a secondary disaster recovery site. You do not want nodes in the secondary site to contribute to a decision to take the cluster offline when there is nothing wrong with the primary site.

### QUESTION 3

You have 30 servers that run Windows Server 2012 R2.

All of the servers are backed up daily by using Windows Azure Backup.

You need to perform an immediate backup of all the servers to Windows Azure Backup.

Which Windows PowerShell cmdlets should you run on each server?

- A. Get-OBPolicy | Start-OBBBackup
- B. Get-WBPolicy | Start-WBBackup
- C. Start-OBRegistration | Start-OBBBackup
- D. Get-WBBackupTarget | Start-WBBackup

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

A: starts a backup job using a policy

Incorrect Answers:

B: Registers the current computer to Windows Azure Backup.

C, D: Not using Azure

References:

[http://technet.microsoft.com/en-us/library/hh770406\(v=wps.620\).aspx](http://technet.microsoft.com/en-us/library/hh770406(v=wps.620).aspx)

<http://technet.microsoft.com/en-us/library/hh770426.aspx>

<http://technet.microsoft.com/en-us/library/hh770398.aspx>

#### QUESTION 4

HOTSPOT

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.

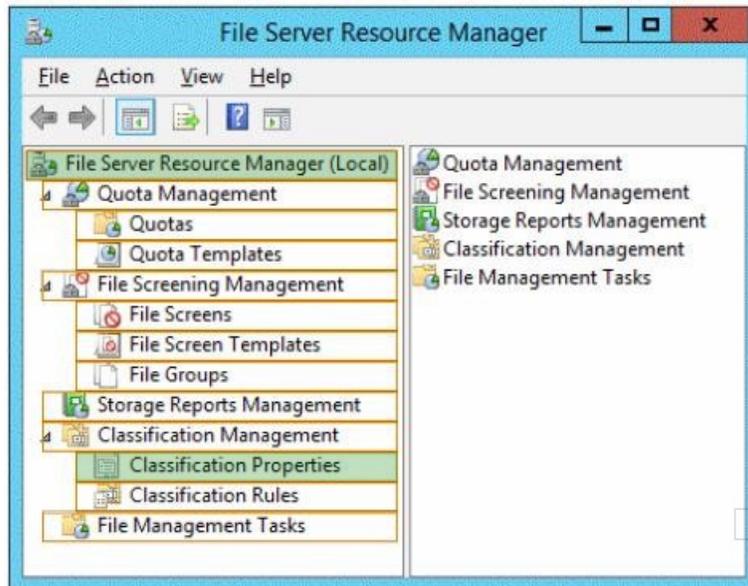
You need to ensure that if an unauthorized user attempts to access the file share, a custom access-denied message appears, which contains a link to request access to the share. The message must not appear when the unauthorized user attempts to access other shares.

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

Hot Area:



Correct Answer:



**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 5**

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

You install the File and Storage Services server role on Server1.

From Windows Explorer, you view the properties of a folder named Folder1 and you discover that the Classification tab is missing.

You need to ensure that you can assign classifications to Folder1 from Windows Explorer manually.

What should you do?

- A. Install the File Server Resource Manager role service.
- B. From Folder Options, clear Hide protected operating system files (Recommended).
- C. Install the Share and Storage Management Tools.
- D. From Folder Options, select the Always show menus.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Classification Management is a feature of FSRM

References:

<http://technet.microsoft.com/en-us/library/dd759252.aspx>

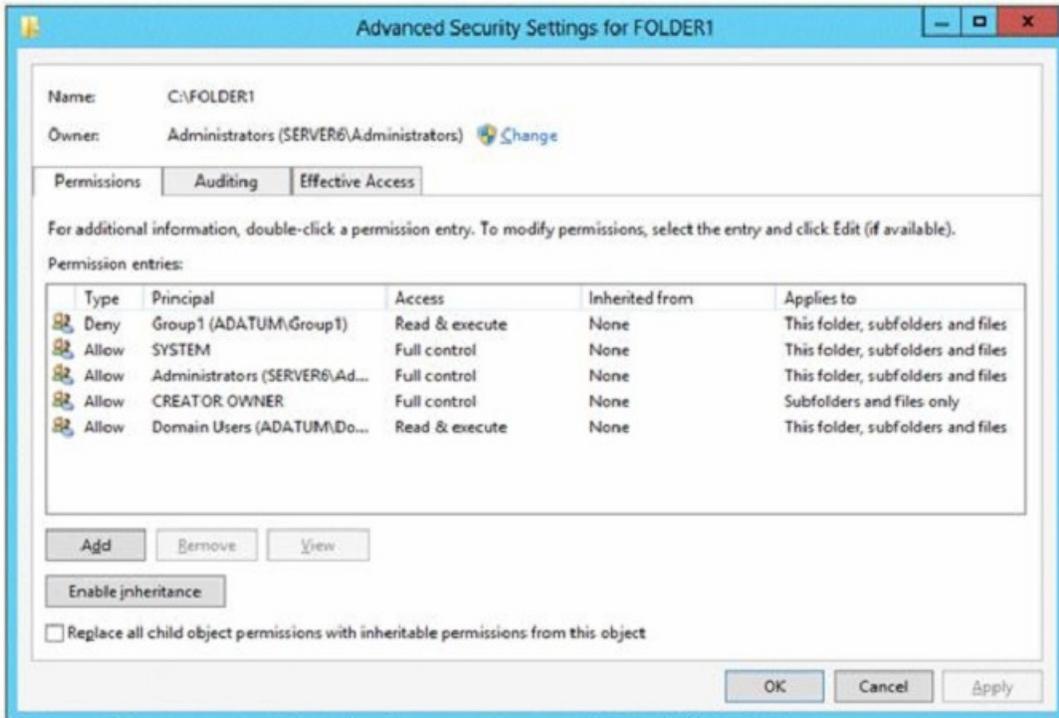
[http://technet.microsoft.com/en-us/library/dd758759\(v=WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd758759(v=WS.10).aspx)

#### **QUESTION 6**

Your network contains an Active Directory domain named adatum.com. All domain controllers run Windows

Server 2008 R2.

The domain contains a file server named Server6 that runs Windows Server 2012 R2. Server6 contains a folder named Folder1. Folder1 is shared as Share1. The NTFS permissions on Folder1 are shown in the exhibit. (Click the Exhibit button.)



The domain contains two global groups named Group1 and Group2.

You need to ensure that only users who are members of both Group1 and Group2 are denied access to Folder1.

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

- A. Remove the Deny permission for Group1 from Folder1.
- B. Deny Group2 permission to Folder1.
- C. Install a domain controller that runs Windows Server 2012 R2.
- D. Create a conditional expression.
- E. Deny Group2 permission to Share1.
- F. Deny Group1 permission to Share1.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Conditional Expressions for Permission Entries Windows Server 2008 R2 and Windows 7 enhanced Windows security descriptors by introducing a conditional access permission entry. Windows Server 2012 R2 takes advantage of conditional access permission entries by inserting user claims, device claims, and resource properties, into conditional expressions. Windows Server 2012 R2 security evaluates these expressions and allows or denies access based on results of the evaluation. Securing access to resources through claims is known as claims-based access control. Claims-based access control works with traditional access control to provide an additional layer of authorization that is flexible to the varying needs of the enterprise environment.

References:

<http://social.technet.microsoft.com/wiki/contents/articles/14269.introducing-dynamicaccesscontrol-en-us.aspx>

### QUESTION 7

Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1 and a domain controller named DC1. All servers run Windows Server 2012 R2.

A Group Policy object (GPO) named GPO1 is linked to the domain.

Server1 contains a folder named Folder1. Folder1 is shared as Share1.

You need to ensure that authenticated users can request assistance when they are denied access to the resources on Server1.

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

- A. Enable the Enable access-denied assistance on client for all file types policy setting for GPO1.
- B. Configure the Customize message for Access Denied errors policy setting of GPO1.
- C. Install the File Server Resource Manager role service on DC1.
- D. Install the File Server Resource Manager role service on Server1.
- E. Assign the Read Attributes NTFS permission on Folder1 to the Authenticated Users group.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

#### Explanation/Reference:

Explanation:

To configure access-denied assistance by using Group Policy

- Open Group Policy Management. In Server Manager, click Tools, and then click Group Policy Management.
- Right-click the appropriate Group Policy, and then click Edit.
- Click Computer Configuration, click Policies, click Administrative Templates, click System, and then click Access-Denied Assistance.
- Right-click Customize message for Access Denied errors, and then click Edit.
- Select the Enabled option.

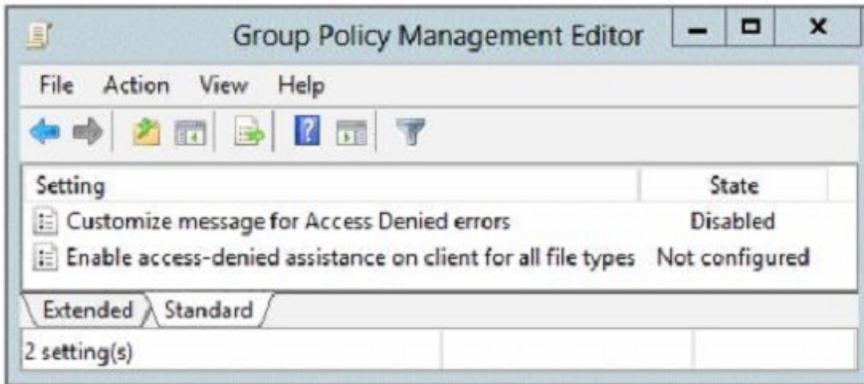
You can configure access-denied assistance within a domain by using Group Policy, or you can configure the assistance individually on each file server by using the File Server Resource Manager console.

References: <https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/deploy-access-denied-assistance--demonstration-steps->

### QUESTION 8

Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1. The File Server Resource Manager role service is installed on Server1. All servers run Windows Server 2012 R2.

A Group Policy object (GPO) named GPO1 is linked to the organizational unit (OU) that contains Server1. The following graphic shows the configured settings in GPO1.



Server1 contains a folder named Folder1. Folder1 is shared as Share1.

You attempt to configure access-denied assistance on Server1, but the Enable access-denied assistance option cannot be selected from File Server Resource Manager.

You need to ensure that you can configure access-denied assistance on Server1 manually by using File Server Resource Manager.

What should you do?

- A. Set the Customize message for Access Denied errors policy setting to Enabled for GPO1.
- B. Set the Enable access-denied assistance on client for all file types policy setting to Disabled for GPO1.
- C. Set the Enable access-denied assistance on client for all file types policy setting to Enabled for GPO1.
- D. Set the Customize message for Access Denied errors policy setting to Not Configured for GPO1.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Ensure that you can configure access-denied assistance

References:

[http://technet.microsoft.com/en-us/library/hh831402.aspx#BKMK\\_1](http://technet.microsoft.com/en-us/library/hh831402.aspx#BKMK_1)

### QUESTION 9

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2.

You are creating a central access rule named Test Finance that will be used to audit members of the Authenticated users group for access failure to shared folders in the finance department.

You need to ensure that access requests are unaffected when the rule is published.

What should you do?

- A. Set the Permissions to Use the following permissions as proposed permissions.
- B. Add a Resource condition to the current permissions entry for the Authenticated Users principal.
- C. Set the Permissions to Use following permissions as current permissions.
- D. Add a User condition to the current permissions entry for the Authenticated Users principal.

**Correct Answer: A**

**Section: (none)**  
**Explanation**

**Explanation/Reference:**  
Explanation:

Proposed permissions

Proposed permissions enable an administrator to more accurately model the impact of potential changes to access control settings without actually changing them.

What value does this change add?

Predicting the effective access to a resource helps you plan and configure permissions for those resources before actually implementing those changes.

What works differently?

Proposed permissions were not available in earlier versions of Windows.

References:

<http://technet.microsoft.com/en-us/library/jj134043.aspx>

**QUESTION 10**

**DRAG DROP**

Your network contains two Active Directory forests named contoso.com and adatum.com. All domain controllers run Windows Server 2012 R2.

A federated trust exists between adatum.com and contoso.com. The trust provides adatum.com users with access to contoso.com resources.

You need to configure Active Directory Federation Services (AD FS) claim rules for the federated trust.

The solution must meet the following requirements:

- In contoso.com, replace an incoming claim type named Group with an outgoing claim type named Role.
- In adatum.com, allow users to receive their tokens for the relying party by using their Active Directory group membership as the claim type.

The AD FS claim rules must use predefined templates.

Which rule types should you configure on each side of the federated trust?

To answer, drag the appropriate rule types to the correct location or locations. Each rule 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.

**Select and Place:**

Rule Types	Answer Area
An acceptance transform rule	Claims Provider trust: Rule type
A delegation authorization rule	Relaying Party trust: Rule type
An issuance authorization rule	
An issuance transform rule	

**Correct Answer:**



**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

\* Acceptance transform rule set

A set of claim rules that you use on a particular claims provider trust to specify the incoming claims that will be accepted from the claims provider organization and the outgoing claims that will be sent to the relying party trust.

Used on: Claims provider trusts

\* Issuance Authorization Rule Set

A set of claim rules that you use on a relying party trust to specify the claims that will be issued to the relying party.

Used on: Relying party trusts

References:

[http://docs.nimsoft.com/prodhelp/en\\_US/NSD/6.2.2/SSOConfigGuide/index.htm?toc.htm?2010473.html](http://docs.nimsoft.com/prodhelp/en_US/NSD/6.2.2/SSOConfigGuide/index.htm?toc.htm?2010473.html)

**QUESTION 11**

**DRAG DROP**

Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server3. The network contains a standalone server named Server2. All servers run Windows Server 2012 R2. The servers are configured as shown in the following table.

Server name	Role
Server1	Active Directory Federation Services
Server2	Web Application Proxy
Server3	Web Server (IIS)

Server3 hosts an application named App1. App1 is accessible internally by using the URL https://app1.contoso.com. App1 only supports Integrated Windows authentication.

You need to ensure that all users from the Internet are pre-authenticated before they can access App1.

What should you do? To answer, drag the appropriate servers to the correct actions. Each server 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.

**Select and Place:**