Microsoft

Exam 70-412

Configuring Advanced Windows Server 2012 R2 Services

Version: 31.0

[Total Questions: 424]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	60
Topic 2: Volume B	60
Topic 3: Volume C	156
Topic 4: Volume D	148

Topic 1, Volume A

Question No : 1 - (Topic 1)

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

Users frequently access the website of an external partner company. The URL of the website is http://partners.adatum.com.

The partner company informs you that it will perform maintenance on its Web server and that the IP addresses of the Web server will change.

After the change is complete, the users on your internal network report that they fail to access the website. However, some users who work from home report that they can access the website.

You need to ensure that your DNS servers can resolve partners.adatum.com to the correct IP address immediately.

What should you do?

A. Run dnscmd and specify the CacheLockingPercent parameter.
B. Run Set-DnsServerGlobalQueryBlockList.
C. Run ipconfig and specify the Renew parameter.
D. Run Set-DnsServerCache.

Answer: D
Explanation:

The Set-DnsServerCache cmdlet modifies cache settings for a Domain Name System (DNS) server.

Run Set-DnsServerCache with the -LockingPercent switch.

/ -LockingPercent<UInt32>
Specifies a percentage of the original Time to Live (TTL) value that caching can consume. Cache locking is configured as a percent value. For example, if the cache locking value is set to 50, the DNS server does not overwrite a cached entry for half of the duration of the TTL. By default, the cache locking percent value is 100. This value means that the DNS server will not overwrite cached entries for the entire duration of the TTL.

Note. A better way would be clear the DNS cache on the DNS server with either Dnscmd /ClearCache (from command prompt), or Clear-DnsServerCache (from Windows PowerShell).

Reference: Set-DnsServerCache

http://technet.microsoft.com/en-us/library/jj649852.aspx

Incorrect:

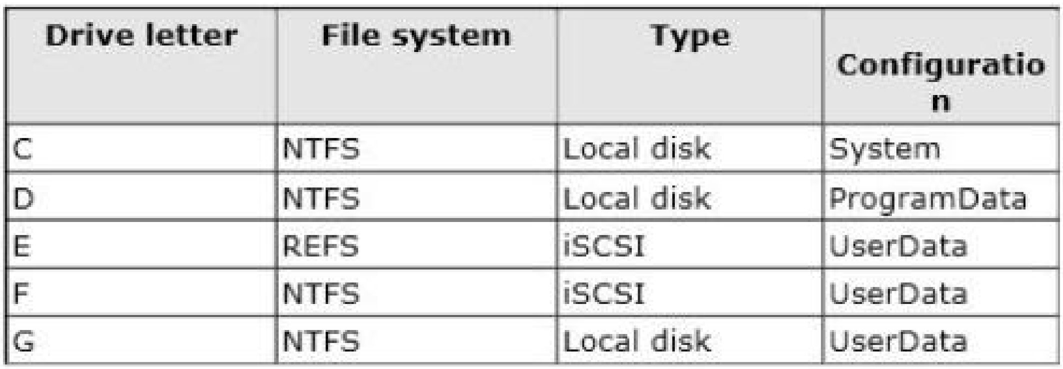
Not A. You need to use the /config parameter as well:

You can change this value if you like by using the dnscmd command:

dnscmd /Config /CacheLockingPercent<percent>

Question No : 2 - (Topic 1)

You have a server named Server1 that runs Windows Server 2012 R2. The storage on Server1 is configured as shown in the following table.



Drive letter	File system	Type	Configuration
C	NTFS	Local disk	System
D	NTFS	Local disk	ProgramData
E	REFS	iSCSI	UserData
F	NTFS	iSCSI	UserData
G	NTFS	Local disk	UserData

You plan to implement Data Deduplication on Server1.

You need to identify on which drives you can enable Data Deduplication.

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

A. C
B. D
C. E
D. F
E. G

Answer: B,D,E

Explanation:

Volumes that are candidates for deduplication must conform to the following requirements:
* Must not be a system or boot volume. (not A)
* Can be partitioned as a master boot record (MBR) or a GUID Partition Table (GPT), and must be formatted using the NTFS file system. (not C)
* Can reside on shared storage, such as storage that uses a Fibre Channel or an SAS array, or when an iSCSI SAN and Windows Failover Clustering is fully supported.
* Do not rely on Cluster Shared Volumes (CSVs). You can access data if a deduplication-enabled volume is converted to a CSV, but you cannot continue to process files for deduplication.
* Do not rely on the Microsoft Resilient File System (ReFS).
* Must be exposed to the operating system as non-removable drives. Remotely-mapped drives are not supported.

Ref: Plan to Deploy Data Deduplication
http://technet.microsoft.com/en-us/library/hh831700.aspx

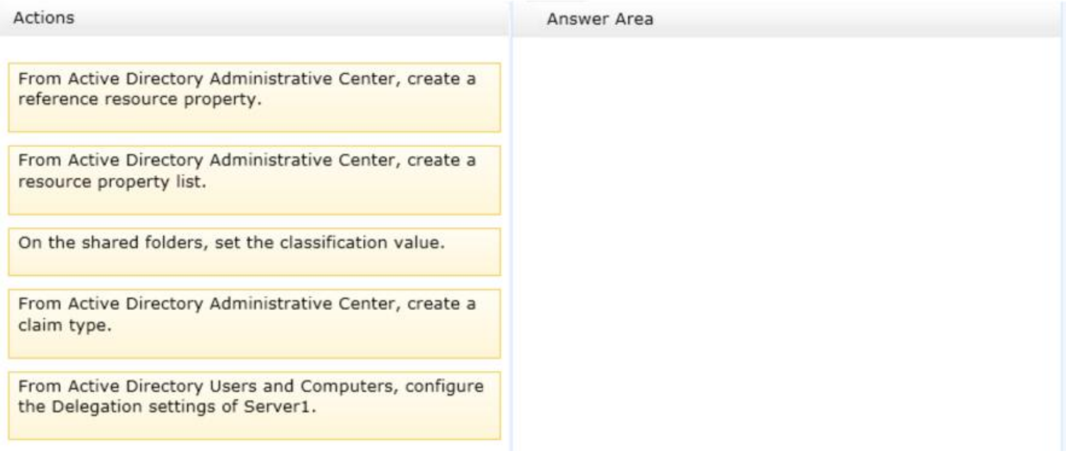
Question No : 3 DRAG DROP - (Topic 1)

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

All domain user accounts have the Division attribute automatically populated as part of the user provisioning process. The Support for Dynamic Access Control and Kerberos armoring policy is enabled for the domain.

You need to control access to the file shares on Server1 based on the values in the Division attribute and the Division resource property.

Which three actions should you perform in sequence?



Actions

From Active Directory Administrative Center, create a reference resource property.

From Active Directory Administrative Center, create a resource property list.

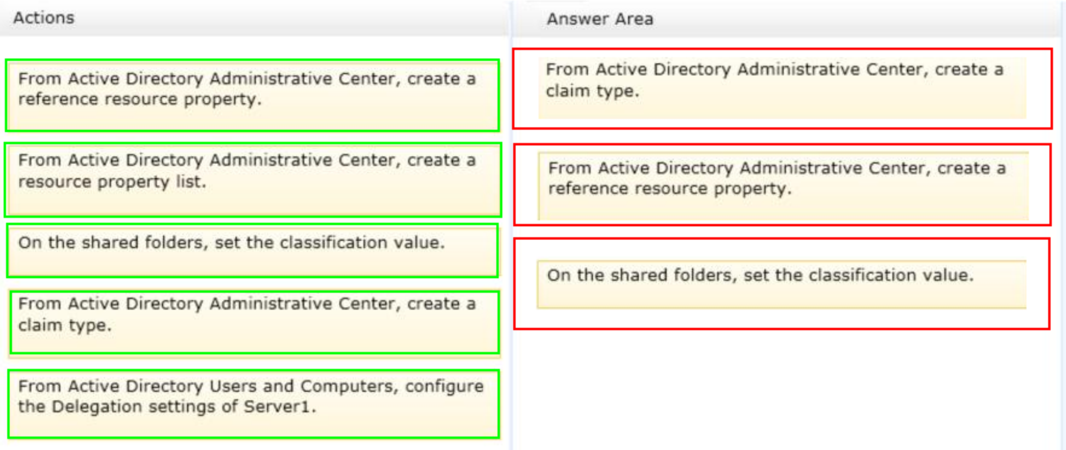
On the shared folders, set the classification value.

From Active Directory Administrative Center, create a claim type.

From Active Directory Users and Computers, configure the Delegation settings of Server1.

Answer Area

Answer:



Actions

From Active Directory Administrative Center, create a reference resource property.

From Active Directory Administrative Center, create a resource property list.

On the shared folders, set the classification value.

From Active Directory Administrative Center, create a claim type.

From Active Directory Users and Computers, configure the Delegation settings of Server1.

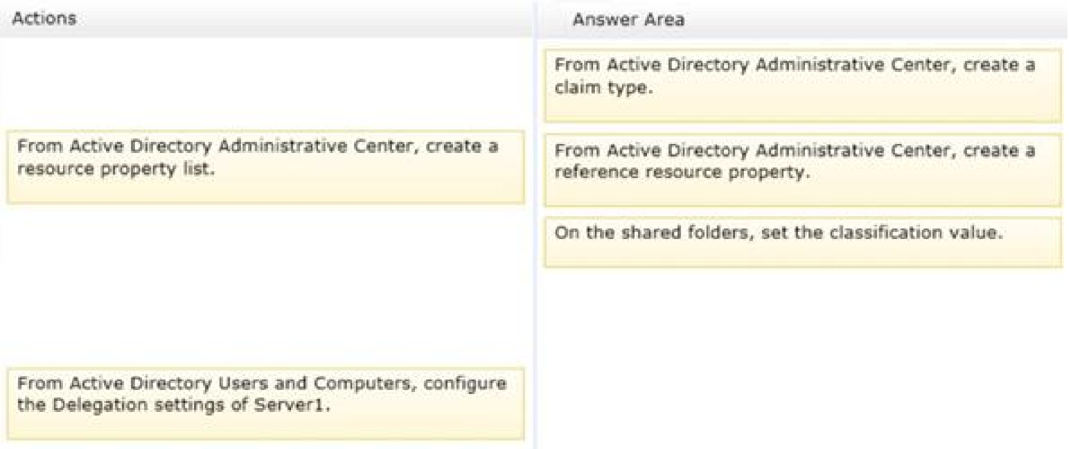
Answer Area

From Active Directory Administrative Center, create a claim type.

From Active Directory Administrative Center, create a reference resource property.

On the shared folders, set the classification value.

Explanation:



Actions

From Active Directory Administrative Center, create a resource property list.

From Active Directory Users and Computers, configure the Delegation settings of Server1.

Answer Area

From Active Directory Administrative Center, create a claim type.

From Active Directory Administrative Center, create a reference resource property.

On the shared folders, set the classification value.

* First create a claim type for the property, then create a reference resource property that

points back to the claim. Finally set the classification value on the folder.

* Configure the components and policy

1. Create claim types
2. Create resource properties

Deploy the central access policy

3. Assign the CAP to the appropriate shared folders on the file server.

Question No : 4 - (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains a member server named Server1 that has the Active Directory Federation Services server role installed. All servers run Windows Server 2012.

You complete the Active Directory Federation Services Configuration Wizard on Server1.

You need to ensure that client devices on the internal network can use Workplace Join.

Which two actions should you perform on Server1? (Each correct answer presents part of the solution. Choose two.)

A. Run Enable-AdfsDeviceRegistration -PrepareActiveDirectory.
B. Edit the multi-factor authentication global authentication policy settings.
C. Run Enable-AdfsDeviceRegistration.
D. Run Set-AdfsProxyProperties HttpPort 80.
E. Edit the primary authentication global authentication policy settings.

Answer: C,E

Explanation:

C. To enable Device Registration Service

On your federation server, open a Windows PowerShell command window and type:

Enable-AdfsDeviceRegistration

Repeat this step on each federation farm node in your AD FS farm.

E. Enable seamless second factor authentication

Seamless second factor authentication is an enhancement in AD FS that provides an added level of access protection to corporate resources and applications from external devices that are trying to access them. When a personal device is Workplace Joined, it becomes a ‘known’ device and administrators can use this information to drive conditional access and gate access to resources.

To enable seamless second factor authentication, persistent single sign-on (SSO) and conditional access for Workplace Joined devices.

In the AD FS Management console, navigate to Authentication Policies. Select Edit Global Primary Authentication. Select the check box next to Enable Device Authentication, and then click OK.

Reference: Configure a federation server with Device Registration Service.

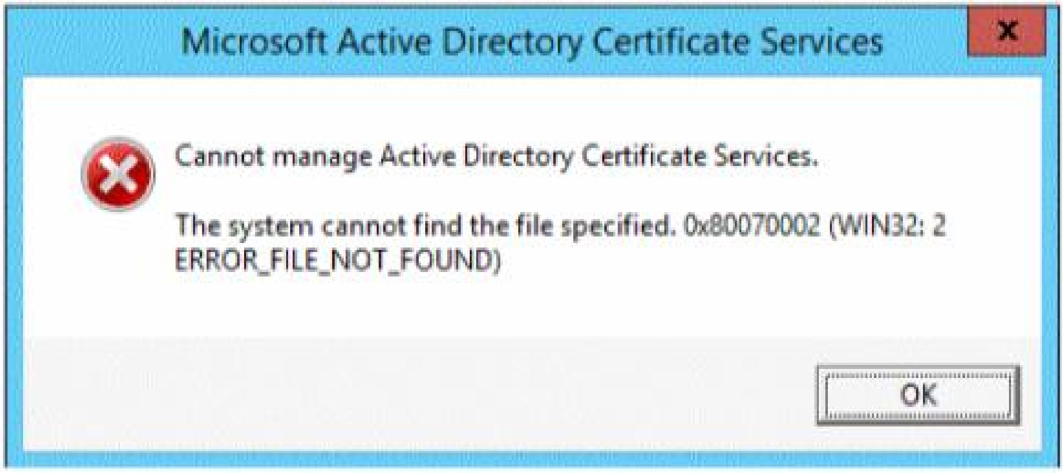
Question No : 5 - (Topic 1)

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

From Server Manager, you install the Active Directory Certificate Services server role on Server1.

A domain administrator named Admin1 logs on to Server1.

When Admin1 runs the Certification Authority console, Admin1 receives the following error message.



Microsoft Active Directory Certificate Services

Cannot manage Active Directory Certificate Services.

The system cannot find the file specified. 0x80070002 (WIN32: 2 ERROR_FILE_NOT_FOUND)

You need to ensure that when Admin1 opens the Certification Authority console on Server1, the error message does not appear.

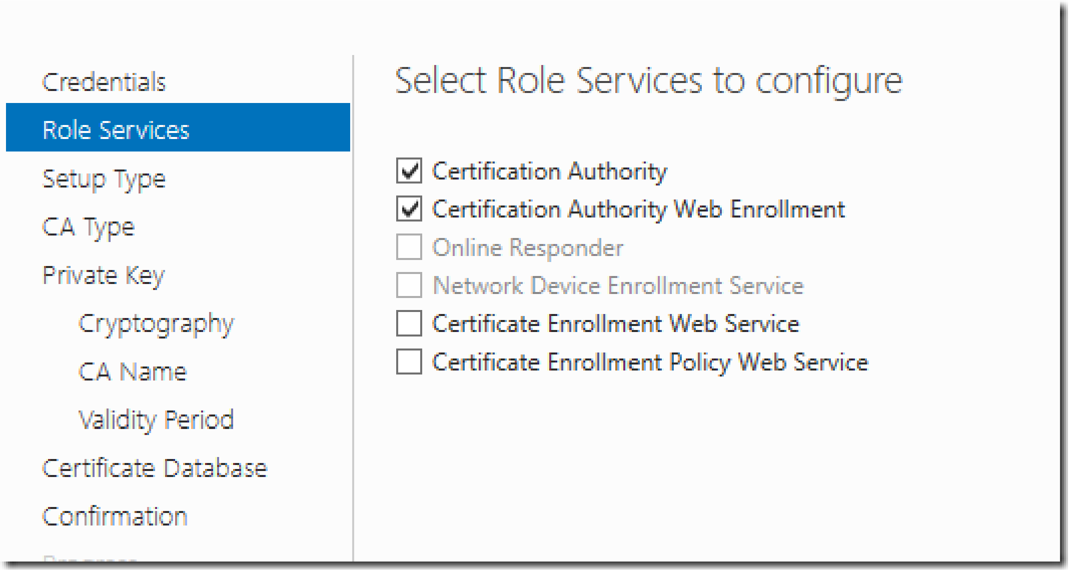
What should you do?

A. Install the Active Directory Certificate Services (AD CS) tools.
B. Run the regsvr32.exe command.
C. Modify the PATH system variable.
D. Configure the Active Directory Certificate Services server role from Server Manager.

Answer: D
Explanation:

The error message is related to missing role configuration.

* Cannot Manage Active Directory Certificate Services
Resolution: configure the two Certification Authority and Certification Authority Web Enrollment Roles:



Select Role Services to configure

☑ Certification Authority
☑ Certification Authority Web Enrollment
☐ Online Responder
☐ Network Device Enrollment Service
☐ Certificate Enrollment Web Service
☐ Certificate Enrollment Policy Web Service

image

Reference: Cannot manage Active Directory Certificate Services in Server 2012 Error 0x800070002

Question No : 6 - (Topic 1)

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

Answer: B

Explanation:

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

Reference: Access Control and Authorization Overview

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

Question No : 7 - (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains two member servers named Server1 and Server2. All servers run Windows Server 2012 R2.

Server1 and Server2 have the Failover Clustering feature installed. The servers are configured as nodes in a failover cluster named Cluster1. Cluster1 contains a cluster disk resource.