



Reference Solution for 70- 742.examcollection.premium.exam.254q 70-742

70-742

Identity with Windows Server 2016

Version 14.0

Score: 800/1000

Version:

Time Limit: 120 Minutes

Exam A (254 questions)

Question 1

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory forest named contoso.com. The forest contains an Active Directory Rights Management Services (AD RMS) deployment.

Your company establishes a partnership with another company named Fabrikam, Inc. The network of Fabrikam contains an Active Directory forest named fabrikam.com and an AD RMS deployment.

You need to ensure that the users in contoso.com can access rights protected documents sent by the users in fabrikam.com.

Solution: From AD RMS in contoso.com, you configure fabrikam.com as a trusted publisher domain.

Does this meet the goal?

- ☒ Yes
☐ No

Explanation:

Explanation:

By default, an AD RMS Licensing Server can issue use licenses for only content where it originally issued the publishing license. In some situations, this may not be acceptable. In order to specify a cluster that is allowed to issue use licenses for content protected by a different cluster, the first cluster must be defined as a trusted publishing domain. If content was published by another certification cluster either in your organization, for example, a subsidiary organization in another forest, or in a separate organization, your AD RMS cluster can grant use licenses to users for this content by configuring a Trusted Publishing Domain on your AD RMS cluster. By adding a Trusted Publishing Domain, you set up a trust relationship between your AD RMS cluster and the other certification cluster by importing the Trusted Publishing Certificate of the other cluster.

References:

<https://books.google.co.za/books?id=gjR-BAAQBAJ&pg=PA397&lpg=PA397&dq=configure+a+partners+forest+as+a+trusted+publishing+domain+-+AD+RMS&source=bl&ots=mohQXTyW9s&sig=NJ7oFHuLYOs72o9EM-yQilscUW8&hl=en&sa=X&ved=0ahUKEwjuiW24sPbAhWGRMAKHQcEB6EQ6AEIOzAD#v=onepage&q=configure%20a%20partners%20forest%20as%20a%20trusted%20publishing%20domain%20-%20AD%20RMS&f=false>

Question 2

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

You discover that users can use passwords that contain only numbers.

You need to ensure that all the user passwords in the domain contain at least three of the following types of characters:

Numbers

Uppercase letters

Lowercase letters

Special characters

What should you edit?

- ☐ The Default Domain Controllers Policy
- ☐ The local policy on each client computer
- ☒ The Default Domain Policy
- ☐ The local policy on each domain controller

Question 3

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

The user account for a user named User1 is in an organizational unit (OU) named OU1.

You need to enable User1 to sign in as user1@adatum.com.

Solution: From Active Directory Users and Computers, you set the E-mail property of User1 to user1@adatum.com.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 4

Your network contains an enterprise root certification authority (CA) named CA1.

Multiple computers on the network successfully enroll for certificates that will expire in one year. The certificates are based on a template named Secure_Computer. The template uses schema version 2.

You need to ensure that new certificates based on Secure_Computer are valid for three years.

What should you do?

- ☒ Modify the Validity period for the certificate template.
- ☐ Instruct users to request certificates by running the certreq.exe command.
- ☐ Instruct users to request certificates by using the Certificates console.
- ☐ Modify the Validity period for the root CA certificate.

Explanation:

Explanation:

Question 5**HOTSPOT**

Your network contains an Active Directory domain named adatum.com. The domain contains the objects shown in the following table.

Name	Type
User1	User
User01	User
User10	User
Group11	User
Group1	Security Group – Global
Group2	Security Group – Global
GroupA	Security Group – Domain Local
GroupB	Security Group – Domain Local

GroupA has Full Control permissions to a folder named Folder1. GroupB has Full Control permissions to a folder named Folder2.

You run the following PowerShell script:

```
$m2 = Get-ADUser - Filter {Name -eq 'User1' }
Add-ADGroupMember - Identity Group1 -Members $m1
Add-ADGroupMember - Identity Group2 -Members $m2
Add-ADGroupMember - Identity GroupA -Members User01
Add-ADGroupMember - Identity GroupA -Members Group02
Add-ADGroupMember - Identity GroupB -Members User10
Add-ADGroupMember - Identity GroupB -Members Group1
```

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area**Statements****Yes No**

User1 has Full Control permissions to Folder1	☐	☐
User11 has Full Control permissions to Folder2	☐	☐
User01 has Full Control permissions to Folder2	☐	☐

Solution:

Answer Area

Statements

Yes No

User1 has Full Control permissions to Folder1

☐
☐

User11 has Full Control permissions to Folder2

☐
☐

User01 has Full Control permissions to Folder2

☐
☐

Question 6

Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. The domain contains a server named Server1.

An administrator named Admin01 plans to configure Server1 as a standalone certification authority (CA).

You need to identify to which group Admin01 must be a member to configure Server1 as a standalone CA. The solution must use the principle of least privilege.

To which group should you add Admin01?

- ☒ Administrators on Server1.
- ☐ Domain Admins in contoso.com
- ☐ Cert Publishers on Server1
- ☐ Key Admins in contoso.com

Explanation:

Explanation:

When installing a Standalone CA, you must use an account that is a member of the local Administrators group.

References: <http://juventusitprofessional.blogspot.com/2015/06/active-directory-certificate-services.html>

Question 7

Your network contains an Active Directory forest named contoso.com. The forest contains 10 domains. The root domain contains a global catalog server named DC1.

You remove the global catalog server role from DC1.

You need to decrease the size of the Active Directory database on DC1.

Solution: You restart DC1 in Directory Services Repair Mode. You run compact.exe, and then restart DC1.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Explanation:

You need to run ntdsutil.exe with the 'compact to' option.

References:

<https://theitbros.com/active-directory-database-compact-defrag/>

Question 8

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. The computer account for Server1 is in organizational unit (OU) named OU1.

You create a Group Policy object (GPO) named GPO1 and link GPO1 to OU1.

You need to add a domain user named User1 to the local Administrators group on Server1.

Solution: From the Computer Configuration node of GPO1, you configure the Local Users and Groups preference.

Does this meet the goal?

- ☒ Yes
☐ No

Explanation:

Explanation:

to add users to the Local Administrator built In group on all the computers using Group Policy, open group policy editor and create or edit existing GPO. Go to User Configuration -> Preferences -> Control Panel Settings -> Local users and groups.

References: <https://www.ntweekly.com/2015/01/10/how-to-add-users-to-local-admin-group-using-group-policy-windows-server-2012/>

Question 9

You network contains an active Directory domain. The domain contains 20 domain controllers. You discover that some Group Policy objects (PROs) are not being applied by all the domain controllers.

You need to verify whether GPOs replicate successfully to all the domain controllers. What should you do?

- ☐ Set BurFlags in the registry, and then restart the File Replication Service (FRS). Run dcdiag.exe for each domain controller.
- ☐ Set BurFlags in the registry, and then restart the File Replication Service (FRS). View the Directory Service event log.
- ☒ From Group Policy Management, view the Status tab for the domain.
- ☐ Run repadmin.exe for each GPO.

Question 10

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You deploy a new Active Directory forest.

You need to ensure that you can create a group Managed Service Account (gMSA) for multiple member servers.

Solution: From Windows PowerShell on a domain controller, you run the Add-KdsRootKey cmdlet.

Does this meet the goal?

- ☒ Yes
- ☐ No

Explanation:

References:

<https://blogs.technet.microsoft.com/askpfeplat/2012/12/16/windows-server-2012-group-managed-service-accounts/>

Question 11

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

Domain users use smart cards to sign in to their client computer.

Some users report that it takes a long time to sign in to their computer and that the logon attempt times out, so they must restart the sign in process.

You discover that the issues to checking the certificate revocation list (CRL) of the smart card certificates.

You need to resolve the issue without diminishing the security of the smart card logons.

What should you do?

- ☐ From the properties of the smart card's certificate template, modify the Request Handling settings.
- ☐ From the properties of the smart card's certificate template, modify the Issuance Requirements settings.
- ☐ Deactivate certificate revocation checks on the computers.
- ☒ Implement an Online Certification Status Protocol (OCSP) responder.

Question 12

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You deploy a new Active Directory forest.

You need to ensure that you can create a group Managed Service Account (gMSA) for multiple member servers.

Solution: You configure Kerberos constrained delegation on the computer account of each member server.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 13

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. You have an organizational unit (OU) named LondonUsers that contains 10,000 users. You need to modify the office attribute of all the users in the LondonUsers OU.

Solution: You create a CSV file. You run csvde.exe and specify the `-i` and `-f` parameters.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

References:

<https://webactivedirectory.com/2011/07/18/simple-powershell-script-to-bulk-update-or-modify-active-directory-user-attributes/>

Question 14

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains two domain controllers named DC1 and DC2.

DC1 holds the RID master operations role. DC1 fails and cannot be repaired. You need to move the RID role to DC2.

Solution: On DC2, you open Active Directory Users and Computers, click Operations Masters..., verify that dc2.contoso.com is listed on the RID tab, and click Change.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Explanation:

This would work if DC1 was still online. In that case we would be “transferring” the role. However, as DC1 is offline, we need to “seize” the role which can only be done by using the ntdsutil command or the Move-AddirectoryServerOperationMasterRole PowerShell cmdlet with the -Force parameter.

Question 15

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains the Active Directory forests and domains shown in the following table:

Forest name	Domain name	Domain type
ForestA	DomainARoot	Root
ForestA	DomainAChild1	Child
ForestB	DomainBRoot	Root
ForestB	DomainBChild1	Child
ForestB	DomainBChild2	Child

A two-way forest trust exists between ForestA and ForestB.

Each domain in ForestB contains user accounts that are used to manage servers.

You need to ensure that the user accounts used to manage the servers in ForestB are members of the Server Operators in ForestA.

Solution: In each domain in ForestB, you create a global group that contains the user accounts of the respective domain. You create a universal group in DomainBRoot. You add the new global groups to the new universal group. You modify the membership of the Server Operators in ForestA.

Does this meet the goal?

- ☒ Yes
☐ No

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups#bkmk-serveroperators>

Question 16

Your network contains an Active Directory forest named contoso.com. The domain contains an Active Directory Federation Services (AD FS) server named Server1.

On a standalone server named Server2, you install and configure the Web Application Proxy.

You have an internal web application named WebApp1. AD FS has a relying party trust for WebApp1.

You need to provide external users with access to WebApp1. Authentication to WebApp1 must use AD FS preauthentication.

Which tool should you use to publish WebApp1?

- ☒ Remote Access Management on Server2
- ☐ Remote Access Management on Server1
- ☐ AD FS Management on Server2
- ☐ AD FS Management on Server1
- ☐ Routing and Remote Access on Server1

Explanation:

References:

<https://docs.microsoft.com/en-us/windows-server/remote/remote-access/web-application-proxy/publishing-applications-using-ad-fs-preauthentication>

Question 17

You have an enterprise certification authority (CA) named CA1.

You have a certificate template named UserAutoEnroll that is based on the User certificate template. Domain users are configured to autoenroll for UserAutoEnroll.

A user named User1 has an email address defined in Active Directory. A user named User2 does not have an email address defined in Active Directory.

You discover that User1 was issued a certificate based on UserAutoEnroll template automatically.

A request by user2 for a certificate based on the UserAutoEnroll template fails.

You need to ensure that all users can autoenroll for certificated based on the UserAutoEnroll template.

Which setting should you configure from the properties on the UserAutoEnroll certificate template?

- ☐ Issuance Requirements
- ☐ Request Handling
- ☐ Cryptography
- ☒ Subject Name

Question 18

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains two domain controllers named DC1 and DC2.

DC1 holds the RID master operations role. DC1 fails and cannot be repaired. You need to move the RID role to DC2.

Solution: On DC2, you open Windows PowerShell and run
`Move-AddirectoryServerOperationMasterRole -OperationMasterRidMaster -Identity DC2.Adatum.com`

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Explanation:

You would need to use the -Force parameter because the server that held the role (DC1) is offline.

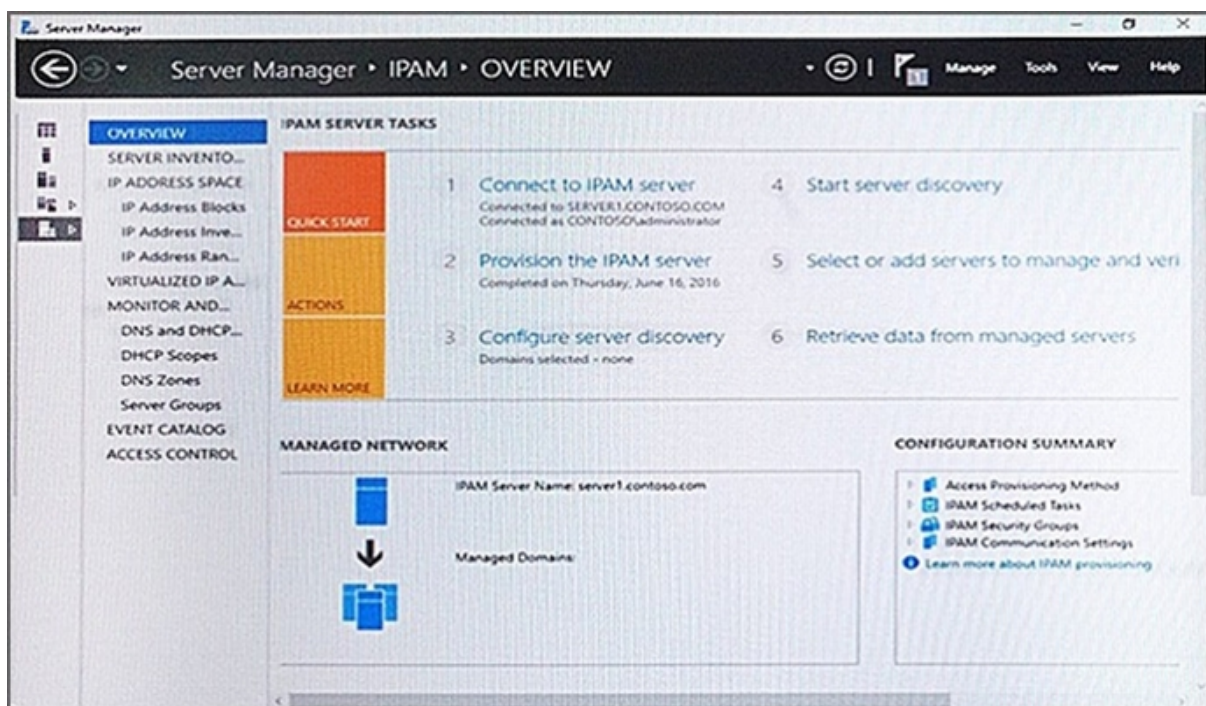
Question 19

HOTSPOT

Your company has a testing environment that contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. Server1 has IP Address Management (IPAM) installed. IPAM has the following configuration.

```
Version           : 6.3.0.1
Port              : 48885
ProvisioningMethod : Automatic
GpoPrefix         : IPAM
HMACKey           : System.Security.SecureString
```

The IPAM Overview page from Server Manager is shown in the IPAM Overview exhibit. (Click the Exhibit button.)



The group policy configurations are shown in the GPO exhibit. (Click the Exhibit button.)
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
If a DNS server is added to contoso.com, the server will be discovered by IPAM automatically.	☐	☐
If you manually add a DHCP server named Server3 to IPAM and set the Manageability status to Managed , the IPAM_DHCP Group Policy will apply to Server3.	☐	☐
If you click Start server discovery , the domain controllers in contoso.com will be discovered by IPAM.	☐	☐

Solution:

Answer Area

Statements	Yes	No
If a DNS server is added to contoso.com, the server will be discovered by IPAM automatically.	☐	☒
If you manually add a DHCP server named Server3 to IPAM and set the Manageability status to Managed , the IPAM_DHCP Group Policy will apply to Server3.	☐	☒
If you click Start server discovery , the domain controllers in contoso.com will be discovered by IPAM.	☐	☒

Explanation:

Explanation:

No domains have been selected in the "Configure Server Discovery" option. Therefore, no automatic discovery will take place. Manual addition of a server will also fail because IPAM needs a domain configured for server verification.

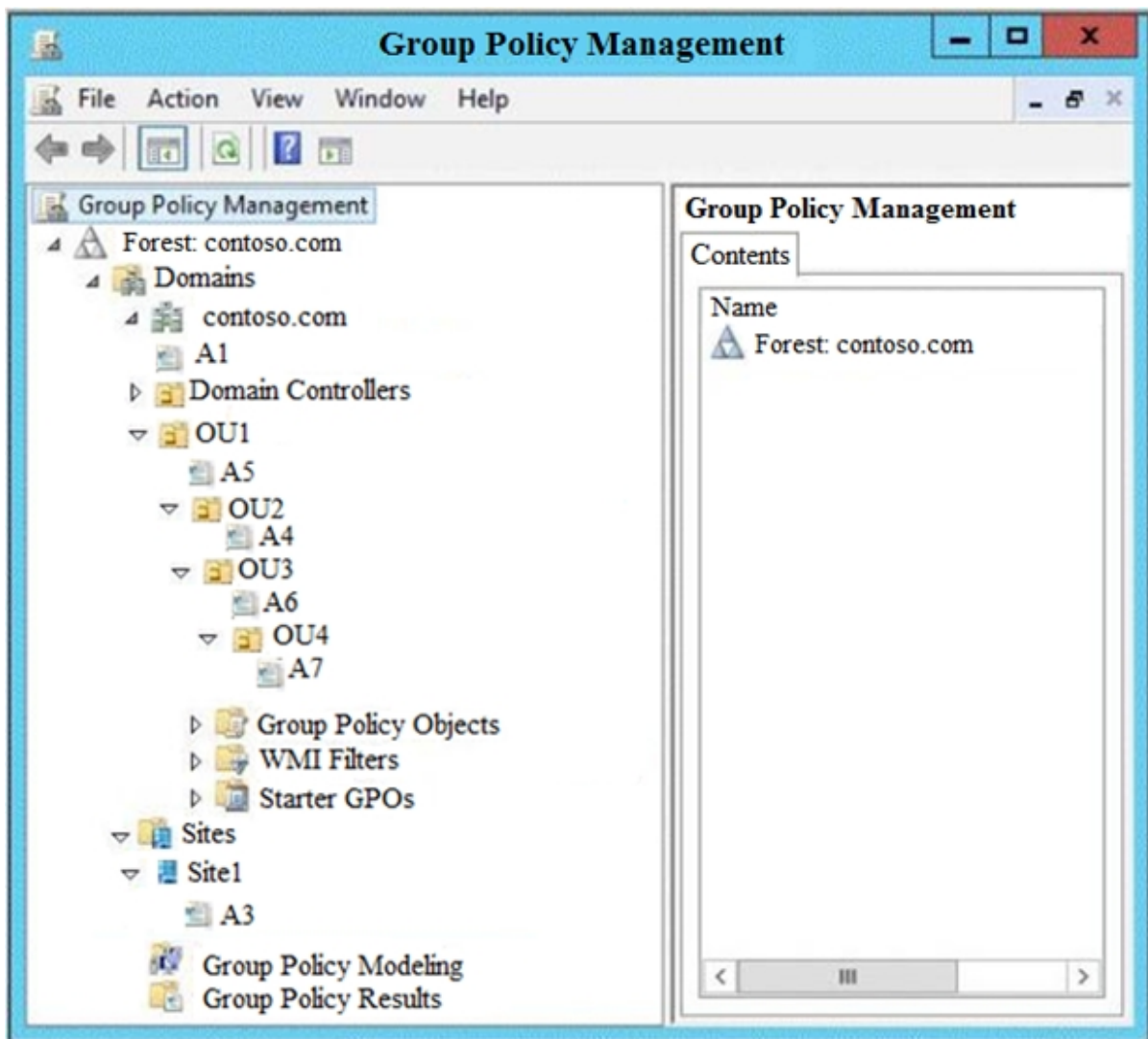
Question 20

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario

Your network contains an Active Directory domain named contoso.com. The domain contains a single site named Site1. All computers are in Site1.

The Group Policy objects (GPOs) for the domain are configured as shown in the exhibit. (Click the Exhibit button.)



The relevant users and client computer in the domain are configured as shown in the following table.

Object name	Object type	Object location
Computer1	Computer	OU4
User1	User	OU4
User2	User	OU2

End of repeated scenario

You are evaluating what will occur when you remove the Authenticated Users group from the Security Filtering settings of A5.

Which GPO or GPOs will apply to User1 when the user signs in to Computer1 after Security Filtering is configured?

- ☒ A1 and A7 only
- ☐ A3 and A1 only.
- ☐ A3, A1, A6 and A7
- ☐ A7 only

Question 21

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?

- ☐ Run `dnscmd` and specify the `CacheLockingPercent` parameter.
- ☐ Run `Set-DnsServerGlobalQueryBlockList`.
- ☐ Run `ipconfig` and specify the `Renew` parameter.
- ☒ Run `Set-DnsServerCache`.

Question 22

DRAG DROP

You network contains an Active Directory forest. The forest contains an Active Directory Federation Services (AD FS) deployment.

The AD FS deployment contains the following:

An AD FS server named server1.contoso.com that runs Windows Server 2016

A WEB Application Proxy used to publish AD FS

A UPN that uses the contoso.com suffix

A namespace named adfs.contoso.com

You create a Microsoft Office 365 tenant named contoso.onmicrosoft.com. You use Microsoft Azure Active Directory Connect (AD Connect) to synchronize all of the users and the UPNs from the contoso.com forest to Office 365.

You need to configure federation between Office 365 and the on-premises deployment of Active Directory.

Which three commands should you run in sequence from Server1? To answer, move the appropriate commands from the list of commands to the answer area and arrange them in the correct order.

Commands

Convert-MsolDomainToFederated -DomainName adfs.contoso.com

Connect-MsolService

Set-MsolADFSContext -Computer contoso.com

Convert-MsolDomainToFederated -DomainName contoso.com

Set-MsolADFSContext -Computer server1.contoso.com

Enter-PSSession -Name Office365

Answer Area

Solution:

Commands

Convert-MsolDomainToFederated -DomainName adfs.contoso.com

Connect-MsolService

Set-MsolADFSContext -Computer contoso.com

Convert-MsolDomainToFederated -DomainName contoso.com

Set-MsolADFSContext -Computer server1.contoso.com

Enter-PSSession -Name Office365

Answer Area

Connect-MsolService

Set-MsolADFSContext -Computer server1.contoso.com

Convert-MsolDomainToFederated -DomainName contoso.com

Question 23

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

You need to ensure that the Administrators group on each computer in the domain always contains Contoso\Domain Admins.

What should you do?

- ☐ Modify the Default Domain Policy and enable the Accounts: Administrator Account status setting.
- ☒ Modify the Default Domain Policy and configure the Restricted Groups setting.
- ☐ Modify the Default Domain Controllers Policy and enable the Accounts: Administrator account status setting.
- ☐ Modify the Default Domain Controllers Policy and configure the Restricted Groups setting.

Explanation:

References:

<https://www.grouppolicy.biz/2010/01/how-to-use-group-policy-preferences-to-secure-local-administrator-groups/>

Question 24

HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2016.

Server1 has IP Address Management (IPAM) installed. Server2 has the DHCP Server role installed. The IPAM server retrieves data from Server2.

You create a domain user account named User1.

You need to ensure that User1 can use IPAM to manage DHCP.

Which command should you run on Server1? To answer, select the appropriate options in the answer area.

Answer Area

▼ net localgroup Set-AdGroup	▼ "Server1\IPAM IP Audit Administrators" "Server1\IPAM IP Users" "Server1\IPAM MSM Administrators" "Server2\Administrators" "Server2\DHCP Administrtrators"	User1 /add
---	---	------------

Solution:

Answer Area

▼	▼	User1 /add
net localgroup	"Server1\IPAM IP Audit Administrators"	
Set-AdGroup	"Server1\IPAM IP Users"	
	"Server1\IPAM MSM Administrators"	
	"Server2\Administrators"	
	"Server2\DHCP Administrators"	

Question 25

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

You create a domain security group named Group1 and add several users to it.

You need to force all of the users in Group1 to change their password every 35 days. The solution must affect the Group1 users only.

What should you do?

- ☐ Create a forms authentication provider, and then set the forms authentication credentials.
- ☒ From Active Directory Administrative Center, create a Password Setting object (PSO).
- ☐ Modify the Password Policy settings in a Group Policy object (GPO) that is linked to the domain, and then filter the GPO to Group1 only.
- ☐ From Windows PowerShell, run the Set-ADDomain cmdlet, and then run the Set-ADAccountPassword cmdlet.

Question 26**HOTSPOT**

Your network contains an Active Directory domain named contoso.com. You plan to automate user account management.

You need to find user accounts that meet specific criteria by using the find command in Active Directory Users and Computers. The solution must minimize administrative effort.

Which Find option should you use for each section? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

To find all the disabled user accounts in the domain:

Common Queries
Custom Search
Users, Contacts, and Groups

To find all users who have not signed in during the last 60 days:

Common Queries
Custom Search
Users, Contacts, and Groups

Solution:**Answer Area**

To find all the disabled user accounts in the domain:

Common Queries
Custom Search
Users, Contacts, and Groups

To find all users who have not signed in during the last 60 days:

Common Queries
Custom Search
Users, Contacts, and Groups

Explanation:

References:

<https://activedirectorypro.com/find-disabled-active-directory-user-accounts/>

<https://www.oreilly.com/library/view/active-directory-cookbook/0596004648/ch06s29.html>

Question 27

You have an enterprise certification authority (CA) named ContosoCA. Recovery agents are configured for ContosoCA.

You duplicate the User certificate template and name it Cont_User. You plan to issue the certificates based on Cont_User to provide users with the ability to encrypt email messages and files.

You need to ensure that the recovery agents can access any user-encrypted files and email messages if the users lose their certificate.

What should you do?

- ☐ Modify the Recovery Agents settings for ContosoCA.
- ☐ Issue a certificate based on a key recovery agent certificate.
- ☒ Modify the Request Handling settings for Cont_User.
- ☐ On ContosoCA, configure the Key Recovery Agent template as a certificate template to issue.

Question 28

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

Your company plans to hire 500 temporary employees for a project that will last 90 days.

You create a new user account for each employee. An organizational unit (OU) named Temp contains the user accounts for the employees.

You need to prevent the new users from accessing any of the resources in the domain after 90 days.

What should you do?

- ☐ Run the Get-ADOrganizationalUnit cmdlet and pipe the output to the Set-Date cmdlet.
- ☐ Run the Get-ADOrganizationalUnit cmdlet and pipe the output to the Set-ADAccountPassword cmdlet.
- ☒ Run the Get-ADUser cmdlet and pipe the output to the Set-ADAccountExpiration cmdlet.
- ☐ Create a Group Policy object (GPO) and link the GPO to the Temp OU. Modify the Account Lockout Policy of the GPO.

Explanation:

References:

<https://docs.microsoft.com/en-us/powershell/module/addsadministration/set-adaccountexpiration?view=win10-ps>

Question 29

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario.

You work for a company named Contoso, Ltd.

The network contains an Active Directory forest named contoso.com. A forest trust exists between contoso.com and an Active Directory forest named adatum.com.

The contoso.com forest contains the objects configured as shown in the following table.

Object name	Object type	Group scope	Group type
User1	User	<i>Not applicable</i>	<i>Not applicable</i>
User2	User	<i>Not applicable</i>	<i>Not applicable</i>
Computer1	Computer	<i>Not applicable</i>	<i>Not applicable</i>
Group1	Group	Domain local	Security
Group2	Group	Domain local	Security
Group3	Group	Universal	Security
Group4	Group	Global	Security
Group5	Group	Universal	Security

Group1 and Group2 contain only user accounts.

Contoso hires a new remote user named User3. User3 will work from home and will use a computer named Computer3 that runs Windows 10. Computer3 is currently in a workgroup.

An administrator named Admin1 is a member of the Domain Admins group in the contoso.com domain.

From Active Directory Users and Computers, you create an organizational unit (OU) named OU1 in the contoso.com domain, and then you create a contact named Contact1 in OU1.

An administrator of the adatum.com domain runs the Set-ADUser cmdlet to configure a user named User1 to have a user logon name of User1@litwareinc.com.

End of repeated scenario.

You need to ensure that User2 can add Group4 as a member of Group5.

What should you modify?

- ☐ the group scope of Group5
- ☐ the Managed By settings of Group4
- ☐ the group scope of Group4
- ☒ the Managed By settings of Group5

Explanation:

Explanation:

Question 30

HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	Type	Group	In organizational unit (OU)
User1	User	Group1	OU1
User2	User	Group1	OU2

The domain has the Password Settings Objects (PSOs) shown in the following table:

Name	Precedence	Minimum password length	Directly applies to
PSO2	20	9	User1
PSO3	10	10	Group1

The domain has the Group Policy objects (GPOs) shown in the following table:

Name	Minimum password length	Linked to
GPO1	6	OU1
GPO2	7	OU2
GPO3	8	Contoso.com

What is the minimum password length for each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User 1:

6 characters
7 characters
8 characters
9 characters
10 characters

User 2:

6 characters
7 characters
8 characters
9 characters
10 characters

Answer Area

User 1:

6 characters
7 characters
8 characters
9 characters
10 characters

User 2:

6 characters
7 characters
8 characters
9 characters
10 characters

Solution:

Explanation:

References:

<https://www.tech-coffee.net/fine-grained-password-policy-active-directory/>

Question 31

You have an offline root certification authority (CA) named CA1. CA1 is hosted on a virtual machine.

You only turn on CA1 when the CA must be patched or you must generate a key for subordinate CAs.

You start CA1, and you discover that the filesystem is corrupted.

You resolve the filesystem corruption and discover that you must reload the CA root from a backup.

When you attempt to run the Restore-CARoleService cmdlet, you receive the following error message: "The process cannot access the file because it is being used by another process."

You need to ensure that you can restore the CA.

What should you do first?

- ☒ Stop the Active Directory Certificate Services (AD CS) service.
- ☐ Run the Restore-CARoleService cmdlet and specify the –Force parameter.
- ☐ Stop the Active Directory Domain Services (AD DS) service.
- ☐ Run the Restore-CARoleService cmdlet and specify the path to a valid CA key.

Question 32

Your network contains an Active Directory forest named contoso.com. The forest contains three domains named contoso.com, corp.contoso.com, and ext.contoso.com. The forest contains three Active Directory sites named Site1, Site2, and Site3.

You have the three administrators as described in the following table.

Administrator name	Group membership	Domain
Admin1	Domain Admins	Contoso.com
Admin2	Domain Admins	Corp.contoso.com
Admin3	Enterprise Admins	Contoso.com

You create a Group Policy object (GPO) named GPO1.

Which administrator or administrators can link GPO1 to Site2?

- ☐ Admin1 and Admin2 only
- ☐ Admin1, Admin2, and Admin3
- ☐ Admin3 only
- ☒ Admin1 and Admin3 only

Explanation:

Explanation:

To link an existing GPO to a site, domain, or OU, you must have Link GPOs permission on that site, domain, or OU. By default, only domain administrators and enterprise administrators have this privilege for domains and OUs. Enterprise administrators and domain administrators of the forest root domain have this privilege for sites.

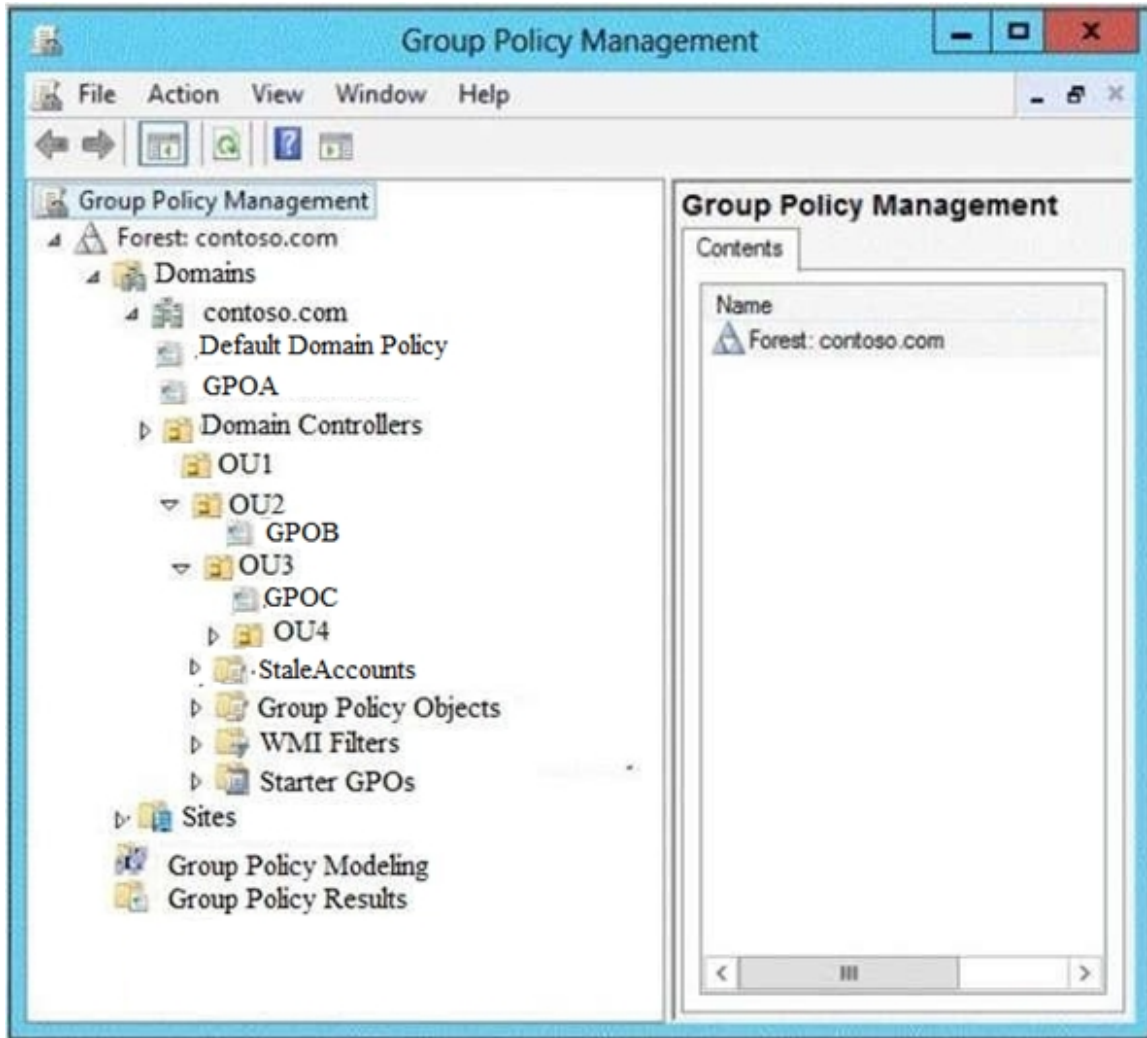
References:

[https://technet.microsoft.com/en-us/library/cc732979\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc732979(v=ws.11).aspx)

Question 33

HOTSPOT

Your Active Directory domain has the Group Policy objects (GPOs) shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

Answer Area

The computers in OU2 will receive settings from **[answer choice]**.

	▼
GPOA only	
GPOB only	
GPOA and GPOB only	
Default Domain Policy, GPOA, and GPOB	

The user accounts in OU3 will receive settings from **[answer choice]**.

	▼
GPOA only	
GPOC only	
GPOA and GPOC only	
Default Domain Policy, GPOA, and GPOC	

Solution:**Answer Area**

The computers in OU2 will receive settings from **[answer choice]**.

	▼
GPOA only	
GPOB only	
GPOA and GPOB only	
Default Domain Policy, GPOA, and GPOB	

The user accounts in OU3 will receive settings from **[answer choice]**.

	▼
GPOA only	
GPOC only	
GPOA and GPOC only	
Default Domain Policy, GPOA, and GPOC	

Explanation:

References:

<https://emeneye.wordpress.com/2016/02/16/group-policy-order-of-precedence-faq/>

Question 34

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.
Start of repeated scenario.

You work for a company named Contoso, Ltd.

The network contains an Active Directory forest named contoso.com. A forest trust exists between contoso.com and an Active Directory forest named adatum.com.

The contoso.com forest contains the objects configured as shown in the following table.

Object name	Object type	Group scope	Group type
User1	User	<i>Not applicable</i>	<i>Not applicable</i>
User2	User	<i>Not applicable</i>	<i>Not applicable</i>
Computer1	Computer	<i>Not applicable</i>	<i>Not applicable</i>
Group1	Group	Domain local	Security
Group2	Group	Domain local	Security
Group3	Group	Universal	Security
Group4	Group	Global	Security
Group5	Group	Universal	Security

Group1 and Group2 contain only user accounts.

Contoso hires a new remote user named User3. User3 will work from home and will use a computer named Computer3 that runs Windows 10. Computer3 is currently in a workgroup.

An administrator named Admin1 is a member of the Domain Admins group in the contoso.com domain.

From Active Directory Users and Computers, you create an organizational unit (OU) named OU1 in the contoso.com domain, and then you create a contact named Contact1 in OU1.

An administrator of the adatum.com domain runs the Set-ADUser cmdlet to configure a user named User1 to have a user logon name of User1@litwareinc.com.
End of repeated scenario.

You need to ensure that User1 can back up the data stored on Computer1. The solution must prevent the user from restoring the data on Computer1.

What should you do?

- ☐ Add User1 to the Backup Operators group of the domain
- ☒ Modify the Security Settings of the local Group Policy on Computer1

- ☐ Add User1 to the Power Users group on Computer1
- ☐ Add User1 to the Backup Operators group on Computer1

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/backup-files-and-directories>

Question 35

You have a server named Server1 that runs Windows Server 2016.
You need to configure Server1 as a Web Application Proxy.

Which server role or role service should you install on Server1?

- ☒ Remote Access
- ☐ Active Directory Federation Services
- ☐ Web Server (IIS)
- ☐ DirectAccess and VPN (RAS)
- ☐ Network Policy and Access Services

Explanation:

Explanation:

Question 36

Your network contains an Active Directory forest. The forest contains two domains named contoso.com and fabrikam.com. The functional level of the forest and the domains is Windows Server 2008 R2.

You have a global group named Group1 in the contoso.com domain. Group1 contains the user accounts in contoso.com.

You need to ensure that you can add the user accounts in the fabrikam.com domain to Group1.

What should you do?

- ☐ Raise the domain functional level of fabrikam.com to Windows Server 2016
- ☒ Modify the scope of Group1 to Domain local
- ☐ Assign the Domain Controllers group in fabrikam.com permissions to Group1
- ☐ Run the Set-LocalGroup cmdlet
- ☐ Change Group1 to a distribution group
- ☐ Raise the domain functional level of contoso.com to Windows Server 2016
- ☐ In both domains, run the adprep.exe command and specify the /domainprep parameter

Explanation:

Explanation:

A domain local group can have a universal group as a member. A universal group can have users or global groups from any domain in the forest as a member.

To adhere to Microsoft best practice, we should add the Fabrikam.com users to a global group in the Fabrikam.com domain. Add the global group to a universal group. Convert Group1 to a domain local group and add the universal group to Group1.

Reference:

https://www.netwrix.com/active_directory_group_management.html

Question 37

Your company has a marketing department.

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

The domain contains two top-level organizational units (OUs) named MKT_Comps and MKT_Users. MKT_Comps contains the computer accounts for the computers in the marketing department. MKT_Users contains the user accounts for the users in the marketing department.

You link a new Group Policy object (GPO) named GPO1 to MKT_Comps.

You need to deploy a VPN connection to all of the users who sign in to the marketing department computers. The users must be able to modify the VPN connection settings.

Where in GPO1 should you create the settings for the VPN connection?

- ☐ Computer Configuration/Policies/Administrative Templates/Network/network Connections
- ☐ User Configuration/Policies/Administrative Templates/Network/Network Connections
- ☐ User Configuration/Preferences/Control Panel Settings/Network Options
- ☒ Computer Configuration/Preferences/Control Panel Settings/Network Options

Question 38

You need to ensure that clients will check at least every 30 minutes as to whether a certificate has been revoked.

Which of the following should you configure to accomplish this goal?

- ☐ Key recovery agent
- ☐ CRL publication interval
- ☒ Delta CRL publication interval
- ☐ Certificate templates.

Question 39

Your network contains an Active Directory domain.

You have a user account that is a member of the Domain Admins group.

You have 100 laptops that have a standard corporate image installed. The laptops are in workgroups and have random names.

A technician named Tech1 is assigned the task of joining the laptops to the domain. The computer accounts of each laptop must be in an organizational unit (OU) that is associated to the department of the user who will use the laptop. The laptop names must start with four characters indicating the department, followed by a four-digit number.

Tech1 is a member of the Domain Users group only. Tech1 has the administrator logon credentials for all the laptops.

You need Tech1 to join the laptops to the domain. The solution must ensure that the laptops are named correctly, and the computer accounts of the laptops are in the correct OUs.

Solution: You script the creation of files domain join, and then you give the files to Tech1.

You instruct Tech1 to sign in to each laptop, and then to run djoin.exe.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 40

HOTSPOT

Your network contains a single-domain Active Directory forest named contoso.com. The forest functional level is Windows Server 2016.

You plan to create and link a Group Policy object (GPO) named GPO1 to the domain. GPO1 will contain user settings only.

You plan to apply GPO1 only to users who are members of a group named Group1.

You need to ensure that GPO1 only applies to the members of Group1. The solution must use the principle of least privilege.

What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Assign both Read and Apply group policy permissions to:

	▼
Authenticated Users	
Domain Computers	
Domain Controllers	
Domain Users	
Group1	

Assign only Read permissions to:

	▼
Authenticated Users	
Domain Computers	
Domain Controllers	
Domain Users	
Group1	

Group to remove from the GPO permissions:

	▼
Authenticated Users	
Domain Computers	
Domain Controllers	
Domain Users	
Group1	

Solution:

Answer Area

Assign both Read and Apply group policy permissions to:

	▼
Authenticated Users	
Domain Computers	
Domain Controllers	
Domain Users	
Group1	

Assign only Read permissions to:

	▼
Authenticated Users	
Domain Computers	
Domain Controllers	
Domain Users	
Group1	

Group to remove from the GPO permissions:

	▼
Authenticated Users	
Domain Computers	
Domain Controllers	
Domain Users	
Group1	

Explanation:

Reference:

<https://blogs.technet.microsoft.com/askpfeplat/2016/07/05/who-broke-my-user-gpos/>

Question 41

You use Application Request Routing (ARR) to make internal web applications available to the Internet by using NTLM authentication.

You need to replace ARR by using the Web Application Proxy.

Which server role should you deploy first?

- ☐ Active Directory Certificate Services
- ☒ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services

Question 42

You have a certification authority (CA) named CA1. You create a certificate template named Template1 that has the following configurations:

Minimum key size: 2048

Cryptographic provider: Microsoft Strong Cryptographic Provider

Compatibility Settings-Certification Authority: Windows server 2012 R2

Compatibility Settings-Certificate recipient: Windows 8.1 /Windows Server 2012 R2

You plan to configure Template1 to require that computers requesting certificates based on Template1 must have a TPM-protected private key.

You need to modify Template1 to ensure that you can configure the Key Attestation settings.

What should you change?

- ☐ Compatibility Settings – Certification Authority to Windows Server 2016
- ☐ Compatibility Settings – Certificate recipient to Windows 10/Windows Server 2016
- ☒ Cryptographic provider to Microsoft Platform Crypto Provider
- ☐ Minimum key size to 4096

Explanation:

References:

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/tpm-key-attestation>

Question 43

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

The domain contains an Active Directory Federation Services (AD FS) server named ADFS1, a Web Application Proxy server named WAP1, and a web server named Web1.

You need to publish a website on Web1 by using the Web Application Proxy.

Users will authenticate by using OAuth2 preauthentication.

What should you do first?

- ☐ On Web1, add site bindings.
- ☐ On Web1, add handler mappings.
- ☒ On ADFS1, enable an endpoint.
- ☐ On ADFS1, add a claims provider trust.

Question 44

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

You have three top-level organizational units (OUs) named OU1, OU2 and OU3. OU1 contains user accounts. OU2 contains the computer accounts for shared public computers. OU3 contains the computer accounts for laptops.

You have two Group Policy objects (GPOs) named GPO1 and GPO2. GPO1 is linked to OU1. GPO2 is linked to OU2.

You need to prevent the user settings in GPO1 from being applied when a user signs in to a shared public computer. If a user signs in to a laptop, the user settings in GPO1 must be applied.

- ☒ Loopback processing
- ☐ GPO link enforcement
- ☐ Security Filtering
- ☐ Inheritance blocking

Question 45

DRAG DROP

Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2016. Server1 has IP Address Management (IPAM) installed. Server2 has Microsoft System Center 2016 Virtual Machine Manager (VMM) installed.

You need to integrate IPAM and VMM.

Which types of objects should you create on each server? To answer, drag the appropriate object types to the correct servers. Each object 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.

Objects

Access Policy	Network Service
Run As Account	Service Template
User Role	

Answer Area

Server1: Object

Server2: Object Object

Solution:

Objects

Access Policy	Network Service
Run As Account	Service Template
User Role	

Answer Area

Server1: Access Policy

Server2: Network Service Run As Account

Explanation:

Explanation:

Server 1 (IPAM): Access Policy

VMM must be granted permission to view and modify IP address space in IPAM, and to perform remote management of the IPAM server. VMM uses a "Run As" account to provide these permissions to the IPAM network service plugin. The "Run As" account must be configured with appropriate permission on the IPAM server.

To assign permissions to the VMM user account

In the IPAM server console, in the upper navigation pane, click ACCESS CONTROL, right- click Access Policies in the lower navigation pane, and then click Add AccessPolicy.

Etc.

Server 2 (VMM) #1: Network Service

Server 2 (VMM) #2: Run As Account

Perform the following procedure using the System Center VMM console.

To configure VMM (see step 1-3, step 6-7)

The screenshot shows the 'Create Run As Account' dialog box. The title bar is blue with a close button (X) on the right. The main area is white with a light blue header that says 'Provide the details for this Run As account'. Below this, there are several input fields: 'Name' with the value 'VMM User', 'Description' with the text 'This domain account is used exclusively by this instance of VMM to integrate with the IPAM server IPAM1.contoso.com', 'User name' with the value 'contoso\vmuser' and a hint 'Example: contoso\domainuser or localuser', 'Password' and 'Confirm password' both masked with dots, and a checkbox labeled 'Validate domain credentials' which is checked. At the bottom, there are three buttons: 'View Script', 'OK', and 'Cancel'.

References:

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn783349\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn783349(v=ws.11))

Question 46

Your network contains an Active Directory forest named contoso.com. The forest contains 10 domains. The root domain contains a global catalog server named DC1.

You remove the global catalog server role from DC1.

You need to decrease the size of the Active Directory database on DC1.

Solution: You stop the NTDS service on DC1. You run ntdsutil.exe, use the metadata cleanup option, and then start the NTDS server.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Explanation:

You need to run ntdsutil.exe with the 'compact to' option.

References:

<https://theitbros.com/active-directory-database-compact-defrag/>

Question 47

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

You deploy a new server named Server1 that runs Windows Server 2016.

A server administrator named ServerAdmin01 is a member of the Domain users group. You add ServerAdmin01 to the Administrators group on Server1.

ServerAdmin01 signs in to Server1 and successfully configures a new Active Directory Rights Management Services (AD RMS) cluster.

You need to ensure that clients discover the AD RMS cluster by querying Active Directory.

What should you do?

- ☐ Update the Active Directory schema.
- ☒ Register a Service Connection Point (SCP).
- ☐ Modify the Security settings of the computer account of Server1.
- ☐ Upgrade one domain controller to Windows Server 2016.

Question 48

Your company has a main office and three branch offices. The network contains an Active Directory domain named contoso.com.

The main office contains three domain controllers. Each branch office contains one domain controller.

You discover the new settings in the Default Domain Policy are not applied in one of the branch offices, but all other Group Policy objects (GPOs) are applied.

You need to check the replication of the Default Domain Policy for the branch office.

What should you do from a domain controller in the main office?

- ☐ From Group Policy Management, click Default Domain Policy under Contoso.com, and then open the Scope tab.
- ☐ From a command prompt, run dcdiag.exe.
- ☒ From a command prompt, run repadmin.exe.
- ☐ From Windows PowerShell, run the Get-GPOReport cmdlet.
- ☐ From Group Policy Management, click Default Domain Policy under Contoso.com, and then open the Details tab.
- ☐ From a command prompt, run gpresult.exe.

Question 49

Your network contains an Active Directory domain. The domain contains an organizational unit (OU) named FileServersOU. A Group Policy object (GPO) named GPO1 is linked to FileServersOU. FileServersOU contains all the file servers in the domain.

You make an urgent security edit to GPO1.

You need to ensure that all the file servers receive the updated setting as soon as possible.

What should you do?

- ☒ Right-click FileServersOU and click Group Policy Update...
- ☐ Right-click the GPO link for GPO1 and click Enforced.
- ☐ Right-click Group Policy Results and click Group Policy Results Wizard...
- ☐ Right-click FileServersOU and click Refresh.

Question 50

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains the Active Directory forests and domains shown in the following table.

Forest name	Domain name	Domain type
Forest A	DomainARoot	Root
Forest A	DomainAChild1	Child
Forest B	DomainBRoot	Root
Forest B	DomainBChild1	Child
Forest B	DomainBChild2	Child

A two-way forest trust exists between ForestA and ForestB. Each domain in ForestB contains user accounts that are used to manage servers. You need to ensure that the user accounts used to manage the servers in ForestB are members of the server Operators groups in ForestA.

Solution: In each domain in ForestB, you add the users to the Server Operators group. You modify the membership of the Server Operations in ForestA.

Does this meet the goal?

- ☐ Yes
- ☒ No

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups#bkmk-serveroperators>

Question 51

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs a Server Core installation of Windows Server 2016. Server1 is configured as an Active Directory Rights Management Services (AD RMS) server for the domain.

You need to install the Identity Federation Support role service on Server1.

What should you do first?

- ☐ Run the Install-WindowsFeature NET-Framework-45-ASPNET cmdlet.
- ☐ Install a Server with Desktop Experience installation of Windows Server 2016.
- ☒ Run the Add-AdfsClient cmdlet.
- ☐ Run the Install-WindowsFeature Desktop-Experience cmdlet.

Question 52

Your network contains an Active Directory domain. All client computers run Windows 10. A client computer named Computer1 was in storage for five months and was unused during that time.

You attempt to sign in to the domain from Computer1 and receive an error message.

You need to ensure that you can sign in to the domain from Computer1.

What should you do?

- ☒ Unjoin Computer1 from the domain, and then join the computer to the domain.
- ☐ From Active Directory Administrative Center, reset the computer account of Computer1.
- ☐ From Active Directory Administrative Center, disable Computer1, and then enable the computer account of Computer1.
- ☐ From Active Directory Users and Computers, run the Delegation of Control Wizard.
- ☐ From Windows PowerShell on Computer1, run the Restore-Computer cmdlet
- ☐ From a command prompt, run the Systemreset.exe command
- ☐ From Windows PowerShell on Computer1, run the Set-ADComputer cmdlet

Explanation:

Reference:

<https://mcpmag.com/articles/2015/03/05/rejoin-a-computer-from-a-domain.aspx>

Question 53

You network contains an Active Directory domain named contoso.com. The domain contains an enterprise certification authority (CA) named CA1.

You have a test environment that is isolated physically from the corporate network and the Internet.

You deploy a web server to the test environment. On CA1, you duplicate the Web Server template, and you name the template Web_Cert_Test.

For the web server, you need to request a certificate that does not contain the revocation information of CA1.

What should you do first?

- ☐ From the properties of CA1, allow certificates to be published to the file system.
- ☐ From the properties of CA1, select Restrict enrollment agents, and then add Web_Cert_Test to the restricted enrollment agent.
- ☐ From the properties of Web_Cert_Test, assign the Enroll permission to the guest account.
- ☒ From the properties of Web_Cert_Test, set the Compatibility setting of CA1 to Windows Server 2016.

Explanation:

Explanation:

The option “Do not include revocation information in issued certificates checkbox” is only available with the compatibility mode set to Windows Server 2008 R2 or later.

References: <http://techgenix.com/certificate-revocation-checking-test-labs/>

Question 54

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain.

You have a user account that is a member of the Domain Admins group.

You have 100 laptops that have a standard corporate image installed. The laptops are in workgroups and have random names.

A technician named Tech1 is assigned the task of joining the laptops to the domain. The computer accounts of each laptop must be in an organizational unit (OU) that is associated to the department of the user who will use the laptop. The laptop names must start with four characters indicating the department, followed by a four-digit number.

Tech1 is a member of the Domain Users group only. Tech1 has the administrator logon credentials for all the laptops.

You need Tech1 to join the laptops to the domain. The solution must ensure that the laptops are named correctly, and the computer accounts of the laptops are in the correct OUs.

Solution: You pre-create the computer account of each laptop in Active Directory Users and Computers.

You instruct Tech1 to sign in to each laptop, to rename each laptop, and then to join each laptop to the domain by using System in Control Panel.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 55

HOTSPOT

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

The domain contains four servers named Server1, Server2, Server3, and Server4 that run Windows Server 2016.

Server1 has IP Address Management (IPAM) installed. Server2, Server3, and Server 4 have the DHCP Server role installed. IPAM manages Server2, Server3, and Server4.

A domain user named User1 is a member of the groups shown in the following table.

Server name	Group
Server1	IPAM Users
Server2	DHCP Administrators
Server3	DHCP Users
Server4	Users

Which actions can User1 perform? To answer, select the appropriate options in the answer area.

Answer Area

Actions	Can be performed by User1	Cannot be performed by User1
Use the DHCP console on Server1 to create a DHCP scope on Server2.	☐	☐
Use the DHCP console on Server1 to create a DHCP scope on Server3.	☐	☐
Use the IPAM node of Server Manager on Server1 to create a DHCP scope on Server4.	☐	☐

Solution:

Answer Area

Actions	Can be performed by User1	Cannot be performed by User1
Use the DHCP console on Server1 to create a DHCP scope on Server2.	☐	☐
Use the DHCP console on Server1 to create a DHCP scope on Server3.	☐	☐
Use the IPAM node of Server Manager on Server1 to create a DHCP scope on Server4.	☐	☐

Explanation:

Explanation:

Box 1: Can be performed by User1

DHCP Administrators can create DHCP scopes.

Box 2: Cannot be performed by User1

DHCP Users cannot create scopes.

Box 3: Cannot be performed by User1

IPAM users cannot create scopes.

References: [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn741281\(v=ws.11\)#create_access_scope](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn741281(v=ws.11)#create_access_scope)

Question 56

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

The domain contains a server named Server1 that runs Windows Server 2016.

The Computer account for Server1 is in organizational unit (OU) named OU1.

You create a Group Policy object (GPO) named GPO1 and link GPO1 to OU1.

You need to add a domain user named User1 to the local Administrators group on Server1.

Solution: From the Computer Configuration node of GPO1, you configure the Restricted Groups settings.

Does this meet the goal?

- ☒ Yes
☐ No

Question 57

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. You have an organizational unit (OU) named LondonUsers that contains 10,000 users. You need to modify the office attribute of all the users in the LondonUsers OU.

Solution: From PowerShell, you run the Get-ADUser cmdlet and specify the –SearchBase parameter. You pipe the results to the Set-Aduser cmdlet.

Does this meet the goal?

- ☒ Yes
☐ No

Explanation:

References:

<https://webactivedirectory.com/2011/07/18/simple-powershell-script-to-bulk-update-or-modify-active-directory-user-attributes/>

Question 58**HOTSPOT**

Your network contains an Active Directory domain named adatum.com. The domain contains the servers configured as shown in the following table:

Server name	Configuration
Server1	Domain controller
Server2	Network controller
Server3	Network Policy Server (NPS) server
Server4	Active Directory Federation Services (AD FS) server
Server5	Host Guardian Service (HSG) server

You have a server named Server6 in the perimeter network.

Each server has the local users show in the following table.

User Name	Member of
User1	Administrators
User2	Power Users
User3	Network Configuration Operators
User4	Cryptographic Operators

The domain contains the users shown in the following table.

User Name	Member of
User1	Domain Admins
User2	Server Operators
User3	Network Configuration Operators
User4	Cryptographic Operators

You install a Web Application Proxy on Server6.

You need to configure the Web Application proxy on Server6. The solution must use the principle of least privilege.

Which account should you specify in the Web Application Proxy Configuration Wizard? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

	▼
Adatum\	
Server1\	
Server2\	
Server3\	
Server4\	
Server5\	

	▼
User1	
User2	
User3	
User4	

Solution:

Answer Area

	▼
Adatum\	
Server1\	
Server2\	
Server3\	
Server4\	
Server5\	

	▼
User1	
User2	
User3	
User4	

Explanation:

Explanation:

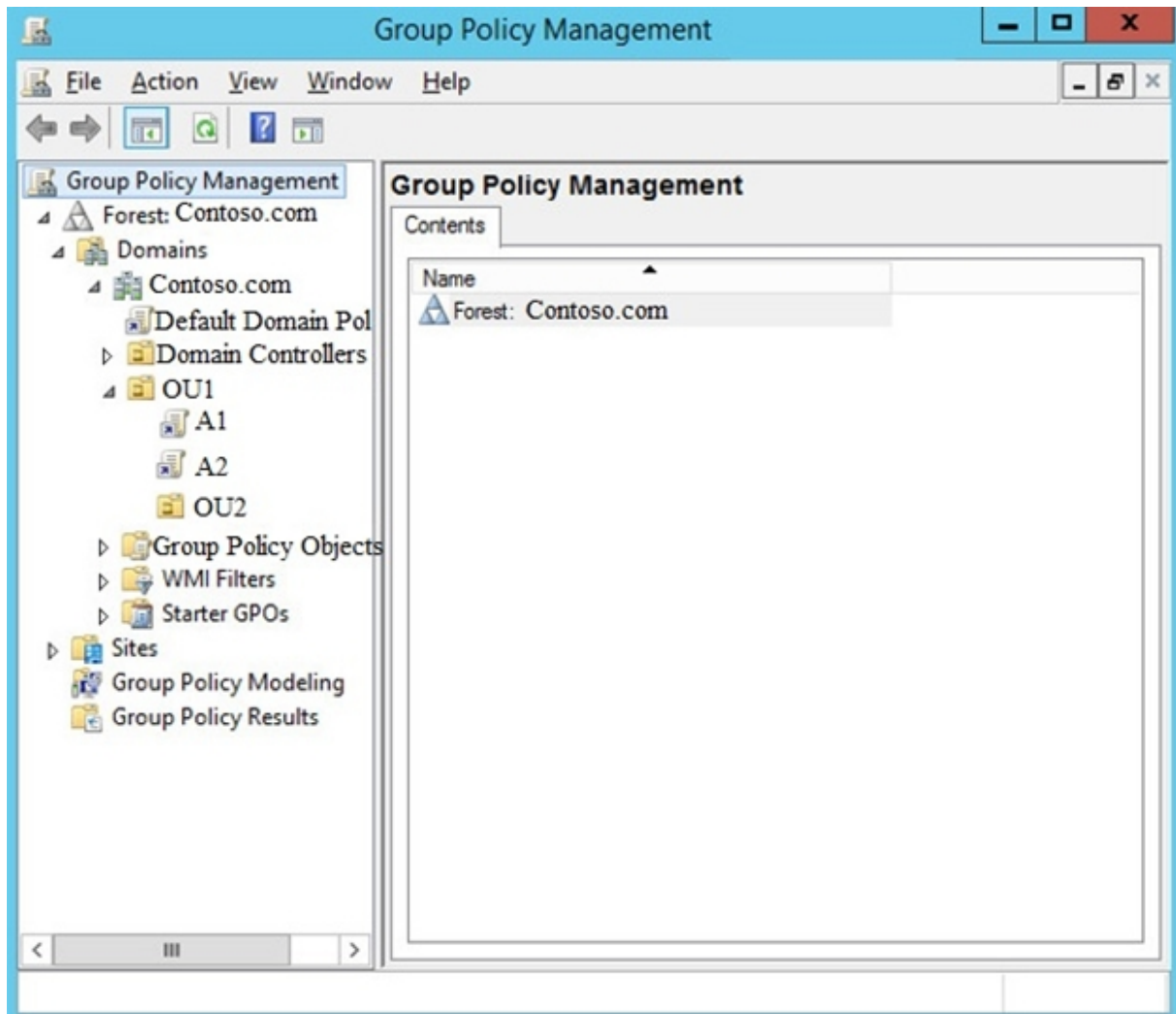
The user account used to configure the web application proxy must have local Administrator permission on the WAP server(s), and have access to an account that have local Administrator permissions on the AD FS servers.

References: <http://www.mistercloudtech.com/2015/11/25/how-to-install-and-configure-web-application-proxy-for-adfs/>

Question 59

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

You open Group Policy Management as shown in the exhibit. (Click the Exhibit button.)



You discover that some of the settings configured in the A1 Group Policy object (GPO) fail to apply to the users in the OU1 organizational unit (OU).

You need to ensure that all of the settings in A1 apply to the users in OU1.

What should you do?

- ☐ Enable loopback policy processing in A1.
- ☐ Block inheritance on OU1.
- ☒ Modify the policy processing order for OU1.
- ☐ Modify the GPO Status of A1.
- ☐ Modify Security Settings for A1
- ☐ Link the A2 GPO to the domain

Explanation:

Reference:

https://blogs.technet.microsoft.com/musings_of_a_technical_tam/2012/02/15/group-policy-basics-part-2-understanding-which-gpos-to-apply/

Question 60

You create a user account that will be used as a template for new user accounts.

Which setting will be copied when you copy the user account from Active Directory Users and Computers?

- ☐ Published Certificates
- ☒ the Member of attribute
- ☐ the Office attribute
- ☐ the Description attribute
- ☐ Permissions
- ☐ Remote Desktop Services Profile

Explanation:

References:

<http://www.rebeladmin.com/2014/07/create-users-with-user-templates-in-ad/>

Question 61

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

The domain contains five domain controllers.

You have a branch office that has a local support technician named Tech1.

Tech1 installs Windows Server 2016 on a server named RODC1 in a workgroup.

You need Tech1 to deploy RODC1 as a read-only domain controller (RODC) in the contoso.com domain.

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

- ☒ Instruct Tech1 to run the Active Directory Domain Services Configuration Wizard.
- ☒ Create an RODC computer account by using Active Administrative Center.
- ☐ Instruct Tech1 to run dcpromo.exe on RODC1.
- ☒ Instruct Tech1 to install the Active Directory Domain Services server role on RODC1.
- ☐ Modify the permissions of the Domain Controllers organizational unit (OU).

Question 62

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory forest named contoso.com. The forest contains a member server named Server1 that runs Windows Server 2016. All domain controllers run Windows Server 2012 R2.

Contoso.com has the following configuration.

```
PS C:\> (Get-ADForest).ForestMode
Windows2008R2Forest
```

```
PS C:\> (Get-ADDomain).DomainMode
Windows2008R2Domain
PS C:\>
```

You plan to deploy an Active Directory Federation Services (AD FS) farm on Server1 and to configure device registration.

You need to configure Active Directory to support the planned deployment.

Solution: You upgrade a domain controller to Windows Server 2016.

Does this meet the goal?

- ☒ Yes
☐ No

Explanation:

Explanation:

Device Registration requires Windows Server 2012 R2 forest schema. Upgrading a domain controller will run adprep.exe to upgrade the schema as part of the upgrade process.

References:

<https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/configure-a-federation-server-with-device-registration-service>

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/upgrade-domain-controllers-to-windows-server-2012-r2-and-windows-server-2012>

Question 63

Your network contains a single-domain Active Directory forest named contoso.com. The forest functional level is Windows Server 2016. The forest has Dynamic Access Control enabled. The domain contains two domain controllers named DC1 and DC2. Privileged user accounts used to manage Active Directory reside in a group named Contoso\AD_Admns.

You create an authentication policy named Policy1 and an authentication policy silo named Silo1.

You need to ensure that the accounts in the Contoso\AD_Admns group can sign in to the domain controllers only.

Which three configurations should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- ☒ Create an access control condition in Policy1.
- ☐ Create a managed service account and add the account to Permitted Accounts in Silo1.
- ☐ Add the domain controllers to the Contoso\AD_Admns group.
- ☒ Add the privileged user accounts and the domain controllers to Permitted Accounts in Silo1.
- ☒ Assign Silo1 to the privileged user accounts and the domain controllers.

Question 64

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

The user account for a user named User1 is in an organizational unit (OU) named OU1.

You need to enable User1 to sign in as user1@adatum.com.

Solution: From Active Directory Domains and Trusts, you configure an alternative UPN suffix. From Active Directory Administrative Center, you configure the User UPN logon property of User1.

Does this meet the goal?

- ☒ Yes
- ☐ No

Question 65

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory forest named contoso.com. The forest contains an Active Directory Rights Management Services (AD RMS) deployment.

Your company establishes a partnership with another company named Fabrikam, Inc. The network of Fabrikam contains an Active Directory forest named fabrikam.com and an AD RMS deployment.

You need to ensure that the users in contoso.com can access rights protected documents sent by the users in fabrikam.com.

Solution: From AD RMS in fabrikam.com, you configure contoso.com as a trusted publisher domain.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Explanation:

Contoso needs to trust Fabrikam.

References:

<https://books.google.co.za/books?id=gjR-BAAAQBAJ&pg=PA397&lpg=PA397&dq=configure+a+partners+forest+as+a+trusted+publishing+domain+-+AD+RMS&source=bl&ots=mohQXTyW9s&sig=NJ7oFHuLYOs72o9EM-yQilscUW8&hl=en&sa=X&ved=0ahUKEwjuiW24sPbAhWGRMAKHQcEB6EQ6AEIOzAD#v=onepage&q=configure%20a%20partners%20forest%20as%20a%20trusted%20publishing%20domain%20-%20AD%20RMS&f=false>

Question 66

Your network contains an Active Directory forest named contoso.com. The forest contains 10 domains. The root domain contains a global catalog server named DC1.

You remove the global catalog server role from DC1.

You need to decrease the size of the Active Directory database on DC1.

Solution: You stop the NTDS service on DC1. You run defrag.exe, and then start the NTDS service.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Explanation:

You need to run ntdsutil.exe with the 'compact to' option.

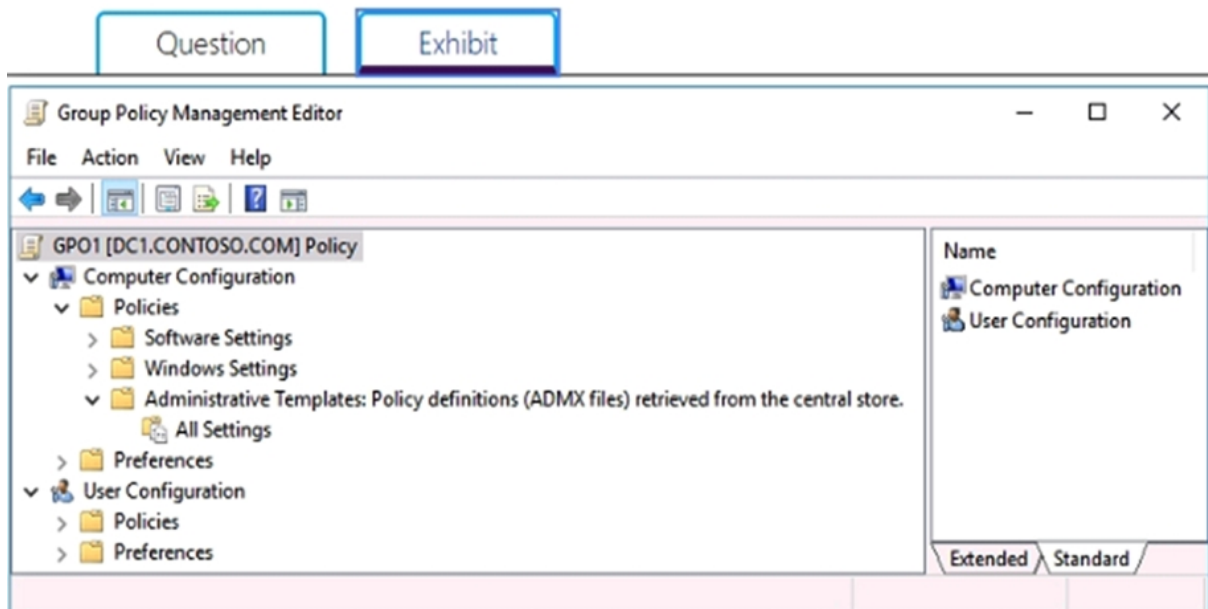
References:

<https://theitbros.com/active-directory-database-compact-defrag/>

Question 67

You network contains an Active Directory Domain named contoso.com.

You modify a Group Policy object (GPO) as shown in the exhibit.



You need to ensure that the Administrative Templates and their settings appear in Group Policy Management Editor.

What should you do?

- ☐ Modify the members of the Group Policy Creator Owners group.
- ☒ Configure the Group Policy filtering options.
- ☐ On DC1, delete the PolicyDefinitions folder from the C:\Windows\SYSVOL\sysvol\Contoso.com\Policies folder.
- ☐ On DC1, delete the PolicyDefinitions folder from C:\Windows.

Question 68

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series.

Information and details provided in a question apply only to that question.

Your network contains an Active Directory domain named contoso.com. The domain contains 5,000 user accounts.

You have a Group Policy object (GPO) named DomainPolicy that is linked to the domain and a GPO named DCPolicy that is linked to the Domain Controllers organizational unit (OU).

You need to configure the Documents folder of every user to be stored on a server named FileServer1.

What should you do?

- ☐ From the Computer Configuration node of DCPolicy, modify Security Settings.
- ☐ From the Computer Configuration node of DomainPolicy, modify Security Settings.
- ☐ From the Computer Configuration node of DomainPolicy, modify Administrative Templates.
- ☐ From the User Configuration node of DCPolicy, modify Security Settings.
- ☒ From the User Configuration node of DomainPolicy, modify Folder Redirection.
- ☐ From user Configuration node of DomainPolicy, modify Administrative Templates.
- ☐ From Preferences in the User Configuration node of DomainPolicy, modify Windows Settings.
- ☐ From Preferences in the Computer Configuration node of DomainPolicy, modify Windows Settings.

Explanation:

Explanation:

Question 69

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You need to identify which server is the schema master.

Solution: From Windows PowerShell, you run `Get-ADDomainController -Discover -Service 2`.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Explanation:

This command gets a global catalog in the current forest using Discovery.

References:

<https://docs.microsoft.com/en-us/powershell/module/addsadministration/get-addomaincontroller?view=win10-ps>

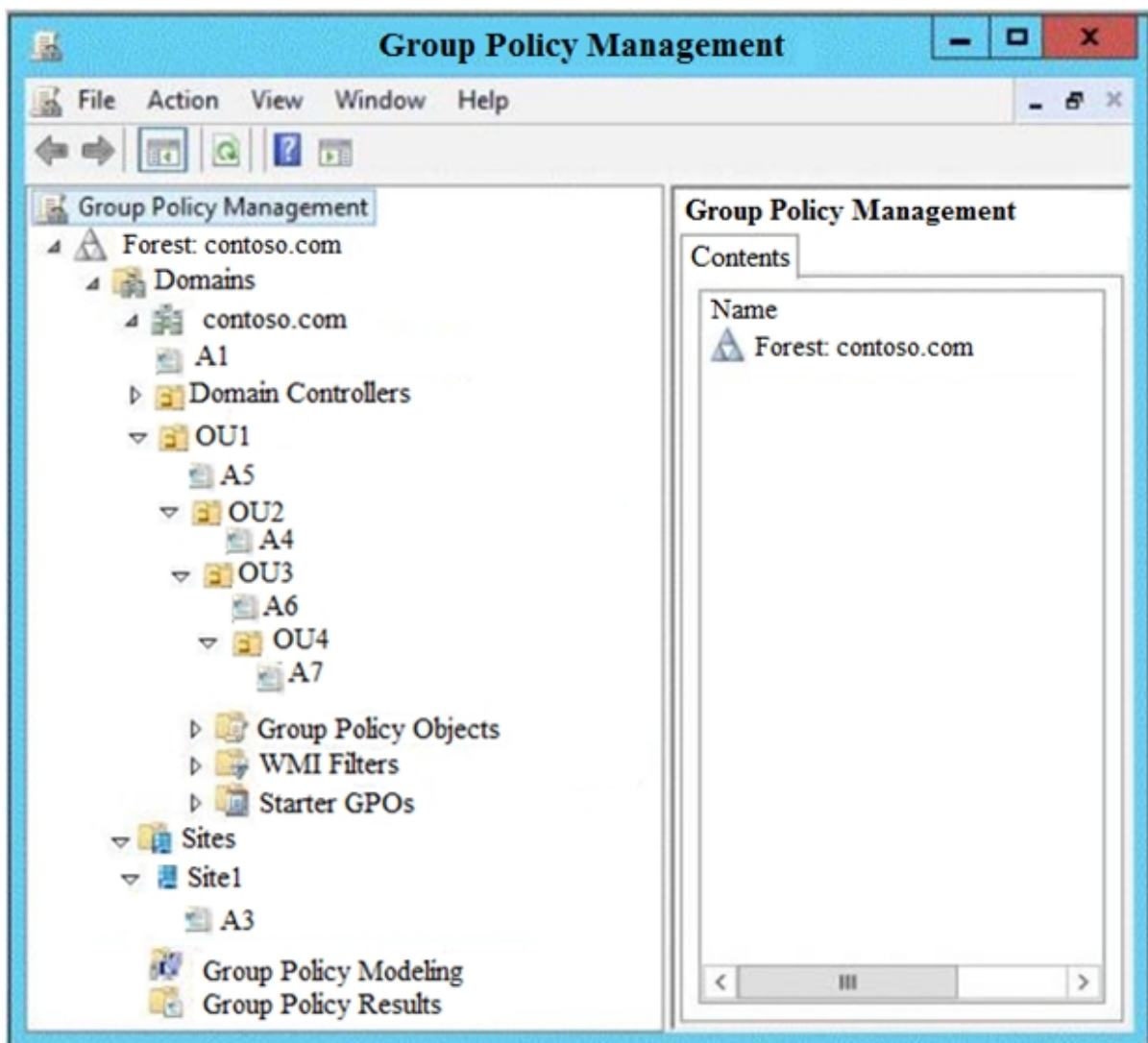
Question 70

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario.

Your network contains an Active Directory domain named contoso.com. The domain contains a single site named Site1. All computers are in Site1.

The Group Policy objects (GPOs) for the domain are configured as shown in the exhibit. (Click the Exhibit button.)



The relevant users and client computer in the domain are configured as shown in the following table.

Object name	Object type	Object location
Computer	Computer	OU4
User1	User	OU4
User2	User	OU2

End of repeated scenario.

You are evaluating what will occur when you block inheritance on OU4.

Which GPO or GPOs will apply to User1 when the user signs in to Computer1 after block inheritance is configured?

- ☐ A1, A5, and A6
- ☐ A3, A1, A5, and A7
- ☐ A3 and A7 only
- ☒ A7 only

Explanation:

Explanation:

Question 71

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

A Group Policy object (GPO) named GPO1 is linked to contoso.com.

GPO1 has computer configuration policies, user configuration policies, and user preferences configured.

You need to ensure that the user preferences in GPO1 apply only to users who sign in to computers that runs Windows 10. All the other settings in GPO1 must be applied, regardless of the computer to which the users sign in.

What should you configure?

- ☐ WMI Filtering
- ☒ Item-level targeting
- ☐ Security Settings
- ☐ Security Filtering

Question 72

Your company has an office in Montreal. The network contains an Active Directory domain named contoso.com.

You have an organizational unit (OU) named Montreal that contains all of the users accounts for the users in the Montreal office. An office manager in the Montreal office knows each user personally.

You need to ensure that the office manager can provide the users with a new password if the users forget their password.

What should you do?

- ☐ Create a Group Policy object (GPO) and link the GPO to the Montreal OU. Assign the office manager the Apply Group Policy permission on the GPO. Configure the Password Policy settings of the GPO.
- ☐ From the Security settings of each user account in the Montreal OU, assign the office manager the Change Password permission.
- ☒ From the Security settings of the Montreal OU, assign the office manager the Reset Password permission.
- ☐ Create a Group Policy object (GPO) and link the GPO to the OU of the domain. Filter the GPO to the Montreal users. Assign the office manager the Apply Group Policy permission on the GPO. Configure the Password Policy settings of the GPO.

Question 73

HOTSPOT

You have a server named Server1 that runs Windows Server 2016. Server1 has the Web Application Proxy role service installed.

You are publishing an application named App1 that will use Integrated Windows authentication as shown in the following graphic.

Publish New Application Wizard CONNECTED TO AD FS

Publishing Settings

Welcome
Preauthentication
Supported Clients
Relying Party
Publishing Settings
Confirmation
Results

Specify the publishing settings for this web application.

Name:

This name will appear in the list of published web applications.

External URL:

External certificate:

☐ Enable HTTP to HTTPS redirection

Backend server URL:

Backend server SPN:

< Previous Next > Publish Cancel

Use the drop-down menus to select the answer area choice that completes each statement based on the information presented in the graphic.

Answer Area

Before you can complete the wizard, you must
[answer choice]

▽
change the external certificate
configure the Backend server SPN
select Enable HTTP to HTTPS redirection

To ensure that users can access App1 externally,
you must change the External URL to [answer choice]

▽
https://app1.contoso.com/app1
http://server02.contoso.com/app1
https://server02.contoso.com/publish/app1

Solution:

Answer Area

Before you can complete the wizard, you must
[answer choice]

▽
change the external certificate
configure the Backend server SPN
select Enable HTTP to HTTPS redirection

To ensure that users can access App1 externally,
you must change the External URL to [answer choice]

▽
https://app1.contoso.com/app1
http://server02.contoso.com/app1
https://server02.contoso.com/publish/app1

Question 74

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

The domain contains an enterprise root certification authority (CA) on a server that runs Windows Server 2016.

You need to configure the CA to support Online Certificate Status Protocol (OCSP) responders.

Which two actions should you perform? Each correct selection presents part of the solution.

NOTE: Each correct selection is worth one point.

- ☒ Add a new certificate template to issue.
- ☒ Modify the Authority Information Access (AIA) of the CA.
- ☐ Configure an enrollment agent.
- ☐ Install a standalone subordinate CA.
- ☐ Modify the CRL distribution point (CDP) of the CA.

Explanation:

Explanation:

Once the OCSP service is configured, we need to configure the OCSP Response Signing template. This process includes adding an Authority Information Access (AIA) extension and then issuing a new certificate template.

References: <https://www.poweradmin.com/blog/deploying-active-directory-certificate-services-and-online-responder/>

Question 75

You have users that access web applications by using HTTPS. The web applications are located on the servers in your perimeter network. The servers use certificates obtained from an enterprise root certification authority (CA). The certificates are generated by using a custom template named WebApps. The certificate revocation list (CRL) is published to Active Directory.

When users attempt to access the web applications from the Internet, the users report that they receive a revocation warning message in their web browser. The users do not receive the message when they access the web applications from the intranet.

You need to ensure that the warning message is not generated when the users attempt to access the web applications from the Internet.

What should you do?

- ☐ Install the Certificate Enrollment Web Service role service on a server in the perimeter network.
- ☐ Modify the WebApps certificate template, and then issue the certificates used by the web application servers.
- ☐ Install the Web Application Proxy role service on a server in the perimeter network. Create a publishing point for the CA.
- ☒ Modify the CRL distribution point, and then reissue the certificates used by the web application servers.

Explanation:

Explanation:

Question 76

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

The user account for a user named User1 is in an organizational unit (OU) named OU1.

You need to enable User1 to sign in as user1@adatum.com.

Solution: From Windows PowerShell, you run
Set-ADUser User1 –UserPrincipalName User1@Adatum.com.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 77

DRAG DROP

Your network contains an Active Directory domain. The domain contains a domain controller named DC1 that runs Windows Server 2016.

You start DC1 in Directory Services Restore Mode (DRSM).

You need to compact the Active Directory database on DC1.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Run ntdsutil.exe.	1.
From the Metadata Cleanup context, select an operation target.	2.
Run dsamain.exe.	3.
From the Semantic Database Analysis context, run go fixup.	
Run activate instance ntds.	
From the Files context, run compact.	

Solution:

Actions	Answer Area
Run ntdsutil.exe.	1. Run ntdsutil.exe.
From the Metadata Cleanup context, select an operation target.	2. Run activate instance ntds.
Run dsamain.exe.	3. From the Files context, run compact.
From the Semantic Database Analysis context, run go fixup.	
Run activate instance ntds.	
From the Files context, run compact.	

Question 78

You have a server named Server1 that has the Active Directory Federation Services server role installed.

You need to configure Server1 as the authorization server. Server1 will be used to authorize access to a web API from a web application. The web application will use OAuth 2.0 and OpenID Connect to access the web API as the authenticated user. The solution must minimize administrative effort.

What should you do first?

- ☐ Run New-AdfsApplicationGroup
- ☐ Add a web API application
- ☐ Run Add-AdfsNativeClientApplication
- ☒ Run Add-AdfsWebApiApplication

Explanation:

References:

<https://docs.microsoft.com/en-us/powershell/module/adfs/add-adfswebapiapplication?view=win10-ps>

Question 79

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

The domain contains an enterprise certification authority (CA) named CA1.

You duplicate the Computer certificate template, and you name the template Cont_Computers.

You need to ensure that all of the certificates issued based on Cont_Computers have a key size of 4,096 bits.

What should you do?

- ☐ From the properties of CA1, modify the Security settings.
- ☐ From the properties of CA1, modify the Request Handling settings.
- ☐ From the properties of the Computer template, modify the Key Attestation settings.
- ☒ From the properties of Cont_Computers, modify the Cryptography settings.

Question 80

HOTSPOT

You have a server named Server1 that runs Windows Server 2016.

Server1 has the Web Application Proxy role service installed.

You publish an application named App1 by using the Web Application Proxy.

You need to change the URL that users use to connect to App1 when they work remotely.

Which command should you run? To answer, select the appropriate options in the answer area.

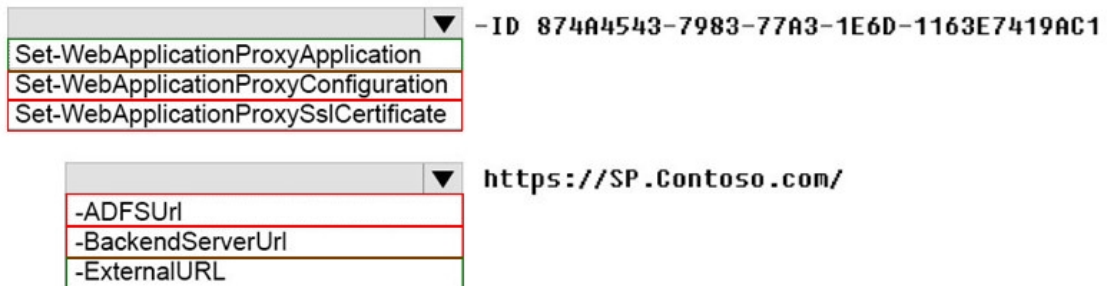
Answer Area

	▼	- ID 874A4543-7983-77A3-1E6D-1163E7419AC1
Set-WebApplicationProxyApplication		
Set-WebApplicationProxyConfiguration		
Set-WebApplicationProxySslCertificate		

	▼	https://SP.Contoso.com/
-ADFSUrl		
-BackendServerUrl		
-ExternalURL		

Solution:

Answer Area



Explanation:

Explanation:

The Set-WebApplicationProxyApplication cmdlet modifies settings of a web application published through Web Application Proxy. Specify the web application to modify by using its ID. Note that the method of preauthentication cannot be changed. The cmdlet ensures that no other applications are already configured to use any specified ExternalURL or BackendServerURL.

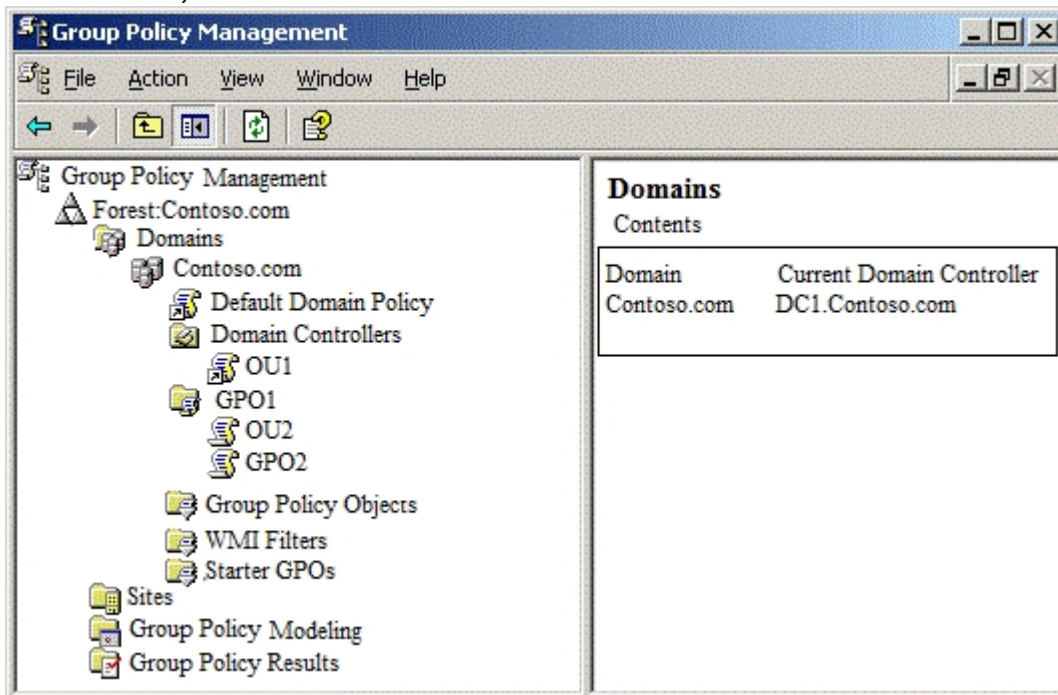
References: <https://docs.microsoft.com/en-us/powershell/module/webapplicationproxy/set-webapplicationproxyapplication?view=win10-ps>

Question 81

HOTSPOT

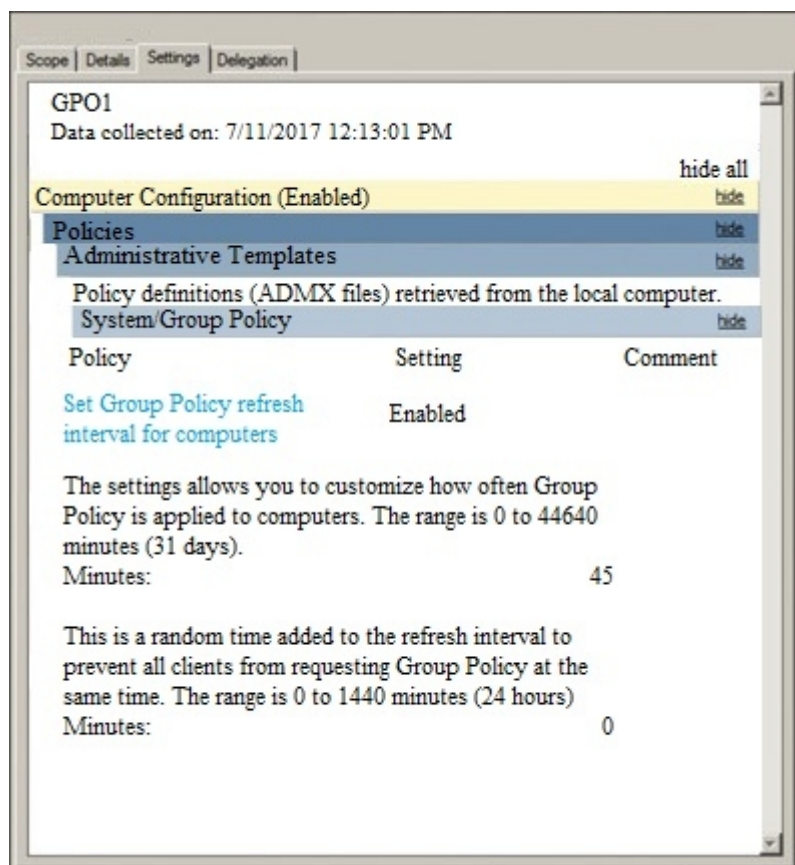
Your network contains an Active Directory domain named contoso.com.

You open Group Policy Management as shown in the Group Policy Management exhibit. (Click the Exhibit button.)

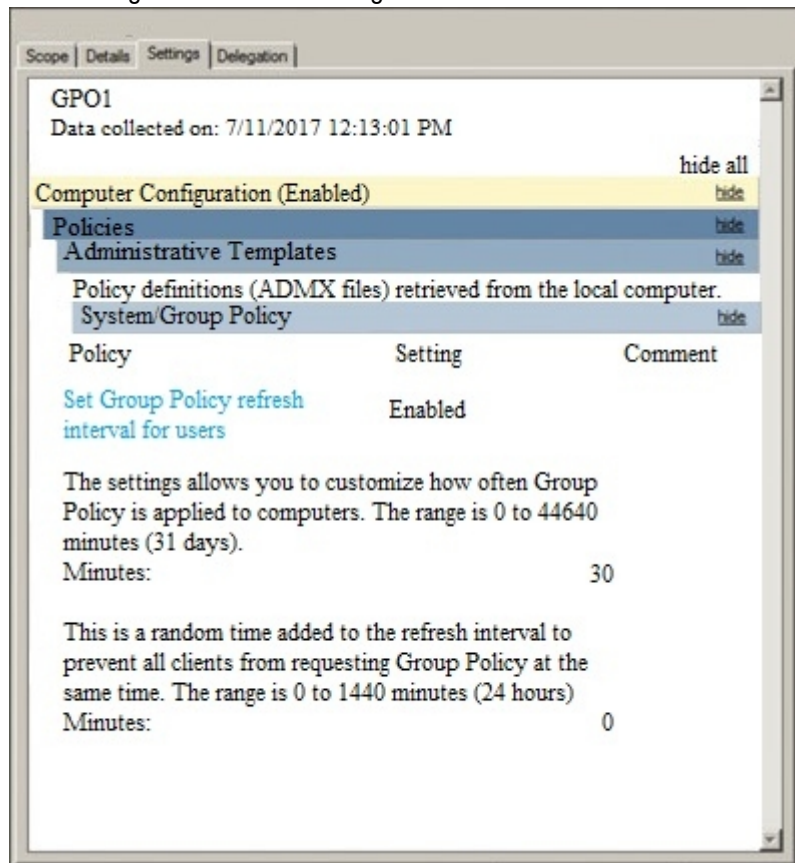


A user named User1 is in OU1. A computer named Computer2 is in OU2.

The settings of GPO1 are configured as shown in the GPO1 exhibit. (Click the Exhibit button.)



The settings of GPO2 are configured as shown in the GPO2 exhibit. (Click the Exhibit button.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 signs in to Computer2. The user Group Policy settings will refresh every 45 minutes.	☐	☐
User1 signs in to Computer2. The computer Group Policy will refresh every 30 minutes.	☐	☐
Contoso/Administrator signs in to Computer2. The user group Policy settings will refresh every 45 minutes.	☐	☐

Solution:

Answer Area

Statements	Yes	No
User1 signs in to Computer2. The user Group Policy settings will refresh every 45 minutes.	☐	☐
User1 signs in to Computer2. The computer Group Policy will refresh every 30 minutes.	☐	☐
Contoso/Administrator signs in to Computer2. The user group Policy settings will refresh every 45 minutes.	☐	☐

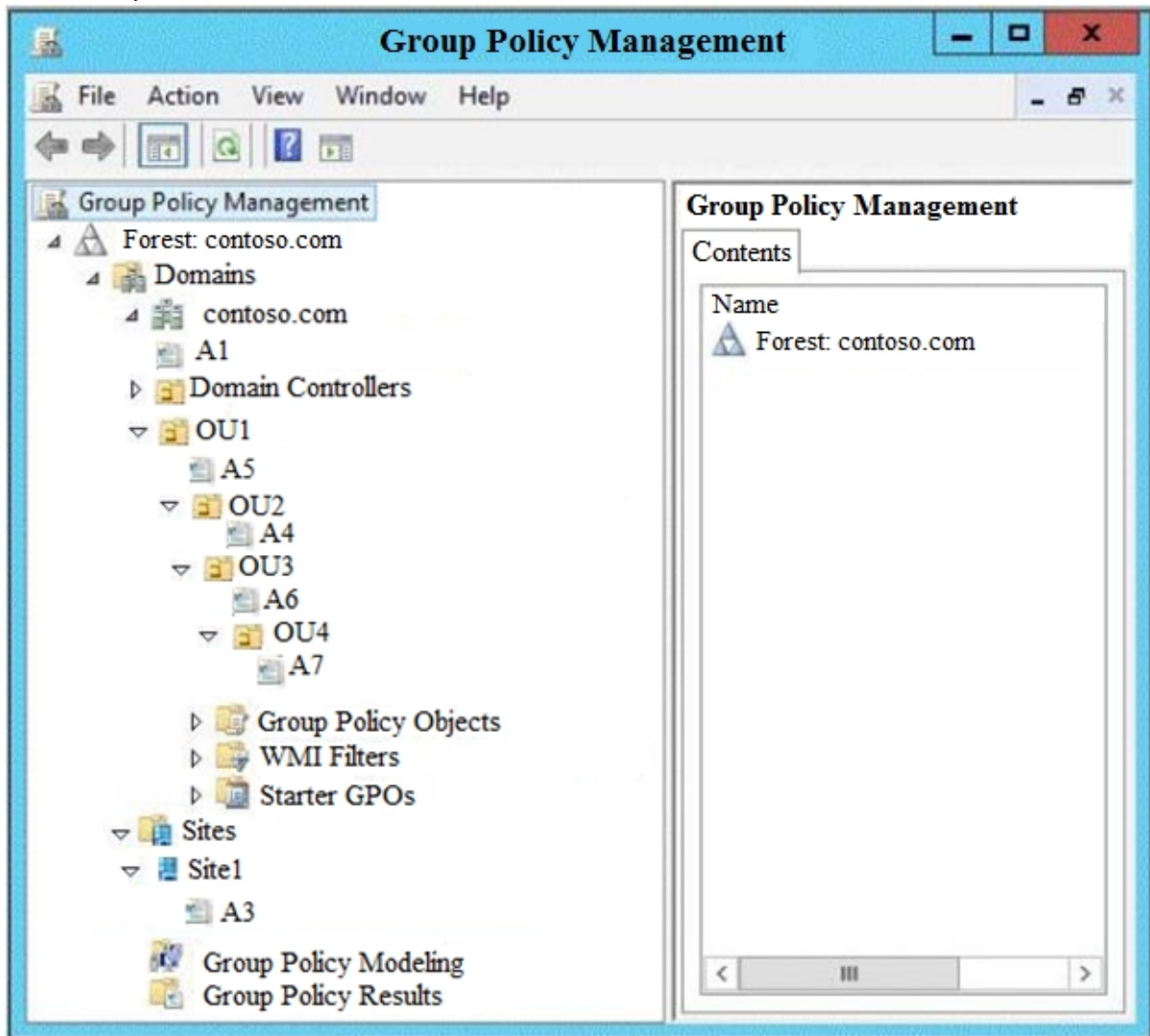
Question 82

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario

Your network contains an Active Directory domain named contoso.com. The domain contains a single site named Site1. All computers are in Site1.

The Group Policy objects (GPOs) for the domain are configured as shown in the exhibit. (Click the Exhibit tab.)



The relevant users and client computer in the domain are configured as shown in the following table.

Object name	Object type	Object location
Computer1	Computer	OU4
User1	User	OU4
User2	User	OU2

End of repeated scenario

You are evaluating what will occur when you set user Group Policy loopback processing mode to Replace in A4.

Which GPO or GPOs will apply to User2 when the user signs in to Computer1 after loopback processing is configured?

- ☐ A1, A5, A6 and A4
- ☐ A3, A1, A4, and A7
- ☐ A3, A1, A5 and A4
- ☒ A4 only

Question 83

Your company has a main office and three branch offices. The network contains an Active Directory domain named contoso.com.

The main office contains three domain controllers. Each branch office contains one domain controller.

You discover the new settings in the Default Domain Policy are not applied in one of the branch offices, but all other Group Policy objects (GPOs) are applied.

You need to check the replication of the Default Domain Policy for the branch office.

What should you do from a domain controller in the main office?

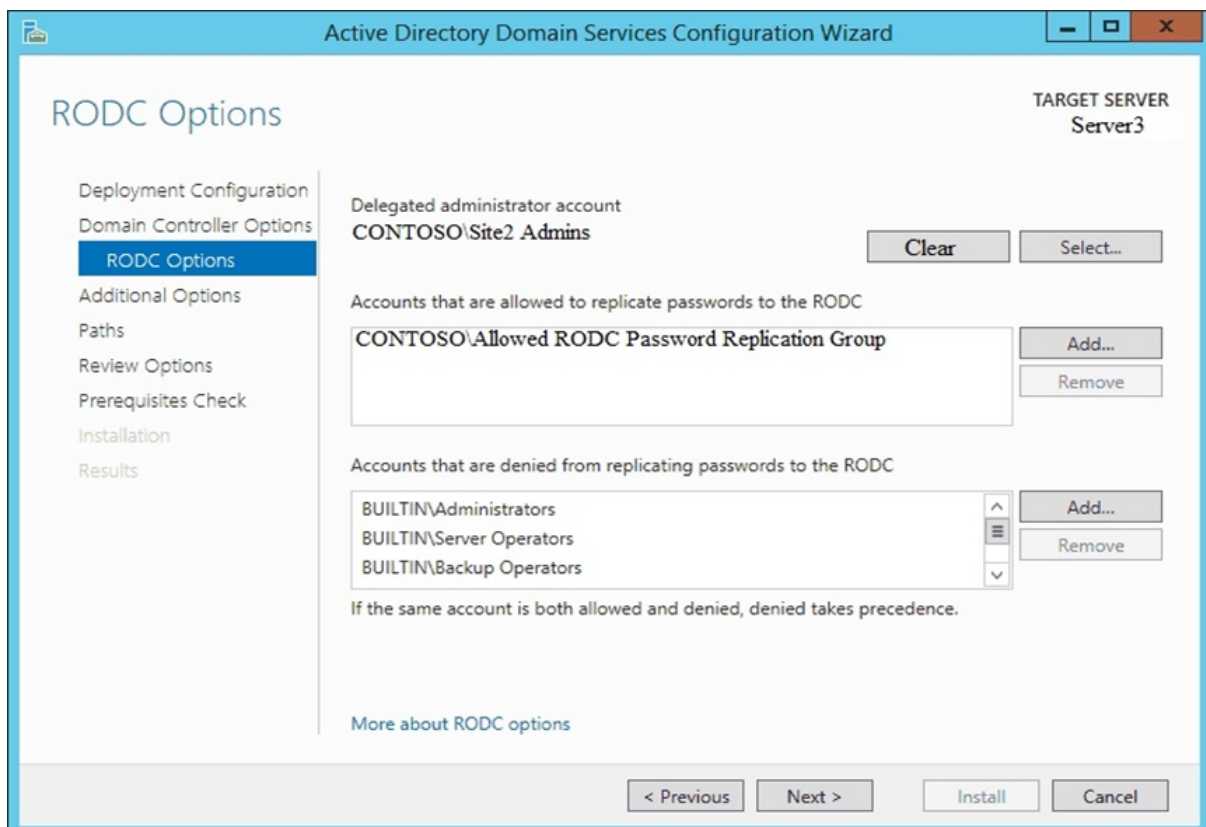
- ☐ From Group Policy Management, click Default Domain Policy under Contoso.com, and then open the Scope tab.
- ☐ From a command prompt, run dcdiag.exe.
- ☒ From Group Policy Management, click Default Domain Policy under the Group Policy Objects container, and then open the Status tab.
- ☐ From Windows PowerShell, run the Get-ADReplicationConnection cmdlet.
- ☐ From Group Policy Management, click Default Domain Policy under Contoso.com, and then open the Details tab.

Question 84

HOTSPOT

Your network contains an Active Directory forest. The forest contains two sites named Site1 and Site2. Site1 contains 10 domain controllers. Site1 and Site2 connect to each other by using a WAN link.

You run the Active Directory Domain Services Configuration Wizard as shown in the following graphic.



Server3 is the only server in Site2.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

Answer Area

Members of the Site2 Admins group will be able to [answer choice] on Server3.

	▼
make updates to SYSVOL content	
manage the password replication policy	
stop and start Active Directory Domain Services (AD DS)	

If the WAN link fails, users who are members of the Allowed RODC Password Replication Group [answer choice] in Site2.

	▼
will be prevented from logging on	
will log on with reduced security rights	
can log on if they have previously logged on	

Solution:

Answer Area

Members of the Site2 Admins group will be able to [answer choice] on Server3.

	▼
make updates to SYSVOL content	
manage the password replication policy	
stop and start Active Directory Domain Services (AD DS)	

If the WAN link fails, users who are members of the Allowed RODC Password Replication Group [answer choice] in Site2.

	▼
will be prevented from logging on	
will log on with reduced security rights	
can log on if they have previously logged on	

Explanation:

Explanation:

By selectively caching credentials, RODCs address some of the challenges that enterprises can encounter in branch offices and perimeter networks (also known as DMZs) that may lack the physical security that is commonly found in datacenters and hub sites.

Question 85

HOTSPOT

Your network contains an Active Directory forest named contoso.com. They connect to the forest by using ldp.exe and receive the output as shown in the following exhibit.

```
ldp://DC1.Contoso.com/DC=Contoso,DC=com
Connection  Browse  View  Options  Utilities  Help

ld = ldp_open("",389);
Established connection to.
Retrieving base DSA information...
Getting 1 entries:
Dn: (RootDSE)
configurationNamingContext: CN=Configuration, DC=Contoso, DC=com;
currentTime: 2/18/2017 9:35:27 PM Central Europe Standard Time;
defaultNamingContext: DC=Contoso,DC=com;
dnsHostName: DC1.Contoso.com;
domainControllerFunctionality: 7 = (WIN2016);
domainFunctionality: 5 = (WIN2012);
dsServiceName: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sities, CN=Configuration, DC=Contoso, DC=com;
forestFunctionality: 4 = (WIN2008R2);
highestCommittedUSN: 107202;
isGlobalCatalogReady: TRUE;
isSynchronized: TRUE;
ldapServiceName: Contoso.com:dc1$@CONTOSO.COM;
namingContexts (5): DC=Contoso,DC=com; CN=Configuration, DC=Contoso,DC=com; CN=Schema, CN=Configuration, DC=Contoso,DC=com;
rootDomainNamingContext: DC=Contoso,DC=com;
schemaNamingContext: CN=Schema, CN=Configuration, DC=Contoso,DC=com;
serverName: CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sities, CN=Configuration, DC=Contoso,DC=com;
subschemaSubentry: CN=Aggregate, CN=Schema, CN=Configuration, DC=Contoso,DC=com;
supportedCapabilities (6): 1.2.840.113556.1.4.800 = (ACTIVE_DIRECTORY); 1.2.840.113556.1.4.1670 = (ACTIVE_DIRECTORY_V51); 1.2.840.113556.1.4.1791 = (ACTIVE_DIRECTORY_LDAP_INTEG); 1.2.840.113556.1.4.1935 = (ACTIVE_DIRECTORY_V61); 1.2.840.113556.1.4.2080 = (ACTIVE_DIRECTORY_V61_R2); 1.2.840.113556.1.4.2237 = (ACTIVE_DIRECTORY_WB);
supportedControl (38): 1.2.840.113556.1.4.319 = (PAGED_RESULT); 1.2.840.113556.1.4.801 = (SD_FLAGS); 1.2.840.113556.1.4.473 = (SORT); 1.2.840.113556.1.4.528 = (NOTIFICATION); 1.2.840.113556.1.4.417 = (SHOW_DELETED); 1.2.840.113556.1.4.619 = (LAZY_COMMIT); 1.2.840.113556.1.4.841 = (DIRSYNC); 1.2.840.113556.1.4.529 = (EXTENDED_DN); 1.2.840.113556.1.4.805 = (TREE_DELETE); 1.2.840.113556.1.4.521 = (CROSSDOM_MOVE_TARGET); 1.2.840.113556.1.4.970 = (GET_STATS); 1.2.840.113556.1.4.1338 = (VERIFY_NAME); 1.2.840.113556.1.4.474 = (RESP_SORT); 1.2.840.113556.1.4.1339 = (DOMAIN_SCOPE); 1.2.840.113556.1.4.1340 = (SEARCH_OPTIONS); 1.2.840.113556.1.4.1413 = (PERMISSIVE_MODIFY); 2.16.840.1.113730.3.4.9 = (VLVREQUEST); 2.16.840.1.113730.3.4.10 = (VLVRESPONSE); 1.2.840.113556.1.4.1504 = (ASQ); 1.2.840.113556.1.4.1852 = (QUOTA_CONTROL); 1.2.840.113556.1.4.802 = (RANGE_OPTION); 1.2.840.113556.1.4.1907 = (SHUTDOWN_NOTIFY); 1.2.840.113556.1.4.1948 = (RANGE_RETRIEVAL_NOERR); 1.2.840.113556.1.4.1974 = (FORCE_UPDATE); 1.2.840.113556.1.4.1341 = (RODC_DCPROMO); 1.2.840.113556.1.4.2026 = (DN_INPUT); 1.2.840.113556.1.4.2064 = (SHOW_RECYCLED); 1.2.840.113556.1.4.2065 = (SHOW_DEACTIVATED_LINK); 1.2.840.113556.1.4.2068 = (POLICY_HINTS_DEPRECATED); 1.2.840.113556.1.4.2090 = (DIRSYNC_EX); 1.2.840.113556.1.4.2205 = (UPDATE_STATS); 1.2.840.113556.1.4.2204 = (TREE_DELETE_EX); 1.2.840.113556.1.4.2206 = (SEARCH_HINTS); 1.2.840.113556.1.4.2211 = (EXPECTED_ENTRY_COUNT); 1.2.840.113556.1.4.2239 = (POLICY_HINTS); 1.2.840.113556.1.4.2255; 1.2.840.113556.1.4.2256; 1.2.840.113556.1.4.2309.
supportedLDAPPolicies (20): MaxPoolThreads; MaxPercentDrSyncrequests; MaxDatagramRecv; MaxReceiveBuffer; InitRecvTimeout; MaxConnections; MaxConnIdleTime; MaxPageSize; MaxBatchReturnMessages; MaxQueryDuration; MaxDirSyncDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent;
supportedLDAPVersion (2); 3;2;
supportedSASLMechanism (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;
```

Use drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

The forest has **[answer choice]** Active Directory partitions.

	▼
one	
two	
three	
four	
five	
six	
seven	

The minimum requirement for domain controllers in Contoso.com is **[answer choice]**.

	▼
Windows Server 2008 R2	
Windows Server 2012	
Windows Server 2012 R2	
Windows Server 2016	

Solution:

Answer Area

The forest has [answer choice] Active Directory partitions.

	▼
one	
two	
three	
four	
five	
six	
seven	

The minimum requirement for domain controllers in Contoso.com is [answer choice].

	▼
Windows Server 2008 R2	
Windows Server 2012	
Windows Server 2012 R2	
Windows Server 2016	

Question 86

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series.

Information and details provided in a question apply only to that question.

Your network contains an Active Directory domain named contoso.com. The domain contains 5,000 user accounts.

You have a Group Policy object (GPO) named DomainPolicy that is linked to the domain and a GPO named DCPolicy that is linked to the Domain Controllers organizational unit (OU).

You need to force users to change their account password at least every 30 days.

What should you do?

- ☐ From the Computer Configuration node of DCPolicy, modify Security Settings.
- ☒ From the Computer Configuration node of DomainPolicy, modify Security Settings.
- ☐ From the Computer Configuration node of DomainPolicy, modify Administrative Templates.
- ☐ From the User Configuration node of DCPolicy, modify Security Settings.
- ☐ From the User Configuration node of DomainPolicy, modify Folder Redirection.
- ☐ From user Configuration node of DomainPolicy, modify Administrative Templates.
- ☐ From Preferences in the User Configuration node of DomainPolicy, modify Windows Settings.
- ☐ From Preferences in the Computer Configuration node of DomainPolicy, modify Windows Settings.

Explanation:

Explanation:

Question 87

You have an internal web server that hosts websites. The websites use HTTP and HTTPS.

You deploy a Web Application Proxy to your perimeter network.

You need to ensure that users from the Internet can access the websites by using HTTPS only. Internet access to the websites must use the Web Application Proxy.

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

NOTE: Each correct selection is worth one point.

- ☐ From the web server, enable HTTP Redirect on the Web Application Proxy server.
- ☐ Configure the Web Application Proxy to perform preauthentication by using OAuth2.
- ☒ From the Remote Access Management Console, publish the websites. Configure pass-through authentication and select Enable HTTP to HTTPS redirection.
- ☐ On external DNS name servers, create DNS entries that point to the private IP address of the web server.
- ☒ On external DNS name servers, create DNS entries that point to the public IP address of the Web Application Proxy.

Question 88

Your company uses Active Directory Rights Management Services (AD RMS).

You need to ensure that only users who use AD RMS client version 2.1 or newer can obtain a rights account certificate from the AD RMS cluster.

What should you enable first?

- ☐ decommissioning
- ☐ user exclusion
- ☒ lockbox exclusion
- ☐ Application Exclusion

Explanation:

References:

https://forsenergy.com/en-us/rms_help/html/9a944ab7-f0d9-4224-97c6-b2543f537827.htm

Question 89

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. All the accounts of the users in the sales department are in an organizational unit (OU) named SalesOU.

An application named App1 is deployed to the user accounts in SalesOU by using a Group Policy object (GPO) named Sales GPO.

You need to set the registry value of `\HKEY_CURRENT_USER\Software\App1\Collaboration` to 0.

Solution: You add a computer preference that has a Create action.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 90

HOTSPOT

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario

You work for a company named Contoso, Ltd.

The network contains an Active Directory forest named contoso.com. A forest trust exists between contoso.com and an Active Directory forest named adatum.com.

The contoso.com forest contains the objects configured as shown in the following table.

Object name	Object type	Group scope	Group type
User1	User	<i>Not applicable</i>	<i>Not applicable</i>
User2	User	<i>Not applicable</i>	<i>Not applicable</i>
Computer1	Computer	<i>Not applicable</i>	<i>Not applicable</i>
Group1	Group	Domain local	Security
Group2	Group	Domain local	Security
Group3	Group	Universal	Security
Group4	Group	Global	Security
Group5	Group	Universal	Security

Group1 and Group2 contain only user accounts.

Contoso hires a new remote user named User3. User3 will work from home and will use a computer named Computer3 that runs Windows 10. Computer3 is currently in a workgroup.

An administrator named Admin1 is a member of the Domain Admins group in the contoso.com domain.

From Active Directory Users and Computers, you create an organizational unit (OU) named OU1 in the contoso.com domain, and then you create a contact named Contact1 in OU1.

An administrator of the adatum.com domain runs the Set-ADUser cmdlet to configure a user named User1 to have a user logon name of User1@litwareinc.com.

End of repeated scenario

You need to join Computer3 to the contoso.com domain by using offline domain join.

Which commands should you use in the contoso.com domain and on Computer3? To answer, select the appropriate options in the answer area.

Answer Area

The contoso.com domain:

	▼
Add-Computer with the-DomainName parameter	
Djoin.exe with the /provision parameter	
Djoin.exe with the /requestodj parameter	
Net computer with the /add parameter	
Netdom.exe with the join parameter	

Computer3:

	▼
Add-Computer with the-DomainName parameter	
Djoin.exe with the /provision parameter	
Djoin.exe with the /requestodj parameter	
Net computer with the /add parameter	
Netdom.exe with the join parameter	

Solution:

Answer Area

The contoso.com domain:

	▼
Add-Computer with the-DomainName parameter	
Djoin.exe with the /provision parameter	
Djoin.exe with the /requestodj parameter	
Net computer with the /add parameter	
Netdom.exe with the join parameter	

Computer3:

	▼
Add-Computer with the-DomainName parameter	
Djoin.exe with the /provision parameter	
Djoin.exe with the /requestodj parameter	
Net computer with the /add parameter	
Netdom.exe with the join parameter	

Question 91

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory forest. The forest contains a domain named contoso.com. The domain contains three domain controllers.

A domain controller named lon-dc1 fails. You are unable to repair lon-dc1.

You need to prevent the other domain controllers from attempting to replicate to lon-dc1.

Solution: From Active Directory Sites and Trusts, you transfer the operations master roles from lon-dc1.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 92

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

The domain contains a server named Server1 that runs Windows Server 2016.

Server1 has IP Address Management (IPAM) installed. IPAM is configured to use the Group Policy based provisioning method.

The prefix for the IPAM Group Policy objects (GPOs) is IP.

From Group Policy Management, you manually rename the IPAM GPOs to have a prefix of IPAM.

You need to modify the GPO prefix used by IPAM.

What should you do?

- ☐ Click Configure server discovery in Server Manager.
- ☒ Run the Set-IpamConfiguration cmdlet.
- ☐ Run the Invoke-IpamGpoProvisioning cmdlet.
- ☐ Click Provision the IPAM server in Server Manager.

Explanation:

Explanation:

The Set-IpamConfiguration cmdlet modifies the configuration for the computer that runs the IPAM server.

The `-GpoPrefix<String>` parameter specifies the unique Group Policy object (GPO) prefix name that IPAM uses to create the group policy objects. Use this parameter only when the value of the `ProvisioningMethod` parameter is set to `Automatic`.

References: <https://docs.microsoft.com/en-us/powershell/module/ipamserver/set-ipamconfiguration?view=win10-ps>

Question 93

HOTSPOT

Your network contains an Active Directory forest. The forest contains two domain controllers named DC1 and DC2 that run Windows Server 2016. DC1 holds all of the operations master roles.

DC1 experiences a hardware failure.

You plan to use an automated process that will create 1,000 user accounts.

You need to ensure that the automated process can complete successfully.

Which command should you run? To answer, select the appropriate options in the answer area.

Answer Area

▼	-identity "DC2" - OperationMasterRole
Move-ADDirectoryServerOperationMasterRole	
ntdsutil	

▼	▼
InfrastructureMaster	-Force
PCDEmulator	Seize pdc
RIDMaster	
SchemaMaster	

Solution:

Answer Area

▼	-identity "DC2" - OperationMasterRole
Move-ADDirectoryServerOperationMasterRole	
ntdsutil	

▼	▼
InfrastructureMaster	-Force
PCDEmulator	Seize pdc
RIDMaster	
SchemaMaster	

Question 94

Your network contains an Active Directory domain named contoso.com. The domain contains a user named User1, a group named Group1, and an organizational unit (OU) named OU1.

You need to enable User1 to link Group Policies to OU1.

Solution: From Active Directory Users and Computers, you add User1 to the Group Policy Creator owners group.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

References:

<http://www.itprotoday.com/management-mobility/what-group-policy-creator-owners-group>

Question 95

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a server named Web1 that runs Windows Server 2016.

You need to list all the SSL certificates on Web1 that will expire during the next 60 days.

Solution: You run the following command.

```
Get-ChildItem Cert:\CurrentUser\Trust | ? { $_.NotAfter -lt (Get-Date).AddDays( 60 ) }
```

Does this meet the goal?

- ☐ Yes
☒ No

Question 96

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

The user account for a user named User1 is in an organizational unit (OU) named OU1.

You need to enable User1 to sign in as user1@adatum.com.

Solution: From Windows PowerShell, you run

```
Set-ADObject 'CN=User1,OU=OU1,DC=Contoso,DC=com'  
-Add @{UserPrincipalName='User1@Adatum.com'}  
-Remove @ {UserPrincipalName='User1@Contoso.com'}.
```

Does this meet the goal?

- ☐ Yes
☒ No

Question 97

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. All the accounts of the users in the sales department are in an organizational unit (OU) named SalesOU.

An application named App1 is deployed to the user accounts in SalesOU by using a Group Policy object (GPO) named Sales GPO.

You need to set the registry value of \HKEY_CURRENT_USER\Software\App1\Collaboration to 0.

Solution: You add a user preference that has an Update action.

Does this meet the goal?

- ☒ Yes
☐ No

Question 98

Your network contains an Active Directory domain named contoso.com. All the accounts of the users in the sales department are in an organizational unit (OU) named SalesOU.

An application named App1 is deployed to the user accounts in SalesOU by using a Group Policy object (GPO) named Sales GPO.

You need to set the registry value of `\HKEY_CURRENT_USER\Software\App1\Collaboration` to 0.

Solution: You add a user preference that has a Replace action.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 99

HOTSPOT

You deploy a Remote Desktop server named RDP1. RDP1 has two volumes named C and D.

You plan to allow users to connect to RDP1 to run multiple applications.

You need to ensure that when the users establish a Remote Desktop connection to RDP1, volume D is hidden.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Type of Group Policy
preference to create:

	▼
Devices	
Drive Maps	
Folder Options	
Folders	

Action to configure for the
Group Policy preference:

	▼
Create	
Delete	
Replace	
Update	

Answer Area

Type of Group Policy preference to create:

	▼
Devices	
Drive Maps	
Folder Options	
Folders	

Action to configure for the Group Policy preference:

	▼
Create	
Delete	
Replace	
Update	

Solution:

Explanation:

References:

<https://support.citrix.com/article/CTX220108>

Question 100

HOTSPOT

You have a server named Server1 that runs Windows Server 2016. Server1 has the Web Application Proxy role service installed.

You plan to deploy Remote Desktop Gateway (RD Gateway) services.

Clients will connect to the RD Gateway services by using various types of devices including Windows, iOS and Android devices.

You need to publish the RD Gateway services through the Web Application Proxy.

Which command should you run? To answer, select the appropriate options in the answer area.

Answer Area

	▼	-BackendServerURL 'https://rdg.contoso.com/rdg1/'
Add-WebApplicationProxyApplication		-ExternalCertificateThumbprint
Set-WebApplicationProxyApplication		
Set-WebApplicationProxyConfiguration		
'1a2b3c4d5e6f1a2b3c4d5e6f1a2b3c4d5e6f1a2b' -ExternalURL 'https://rdg.contoso.com/rdg1' -Name 'RDG1'		
-ExternalPreAuthentication		▼ -ADFSRelyingPartyName 'Default provider'
	ADFS	
	ADFSforOAuth	
	ClientCertificate	
	PassThrough	
-BackendServerAuthenticationSPN 'HTTP/RDG1'		

Solution:

Answer Area

	▼	-BackendServerURL 'https://rdg.contoso.com/rdg1/'
Add-WebApplicationProxyApplication		-ExternalCertificateThumbprint
Set-WebApplicationProxyApplication		
Set-WebApplicationProxyConfiguration		
'1a2b3c4d5e6f1a2b3c4d5e6f1a2b3c4d5e6f1a2b' -ExternalURL 'https://rdg.contoso.com/rdg1' -Name 'RDG1'		
-ExternalPreAuthentication		▼ -ADFSRelyingPartyName 'Default provider'
	ADFS	
	ADFSforOAuth	
	ClientCertificate	
	PassThrough	
-BackendServerAuthenticationSPN 'HTTP/RDG1'		

Explanation:

References:

<https://docs.microsoft.com/en-us/powershell/module/webapplicationproxy/add-webapplicationproxyapplication?view=win10-ps>

Question 101

DRAG DROP

You are the network administrator for a company named Contoso, Ltd.

Contoso has a partner company named Fabrikam, Inc.

The networks of both companies contain Active Directory forests. The functional level of both forests is Windows Server 2016. Both forests have Active Directory Rights Management Services (AD RMS) and Microsoft Exchange Server 2016 installed. The users in both forests can access AD RMS and Exchange servers.

You need to ensure that the Contoso users can access rights-protected content of the Fabrikam users. The solution must minimize changes to the AD RMS clients and must eliminate the need to exchange AD RMS private keys.

Which three actions should you perform in the Contoso forest? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Enable anonymous access on the AD RMS licensing pipeline.

Import the trusted publishing domain file to Contoso.

Import a trusted user domain file to Contoso.

Extend the Active Directory schema of Contoso.

Export the trusted publishing domain file from Fabrikam.

Export the trusted user domain file from Fabrikam.

Answer Area

Solution:

Actions

Enable anonymous access on the AD RMS licensing pipeline.

Import the trusted publishing domain file to Contoso.

Import a trusted user domain file to Contoso.

Extend the Active Directory schema of Contoso.

Export the trusted publishing domain file from Fabrikam.

Export the trusted user domain file from Fabrikam.

Answer Area

Import a trusted user domain file to Contoso.

Enable anonymous access on the AD RMS licensing pipeline.

Extend the Active Directory schema of Contoso.

Explanation:

References:

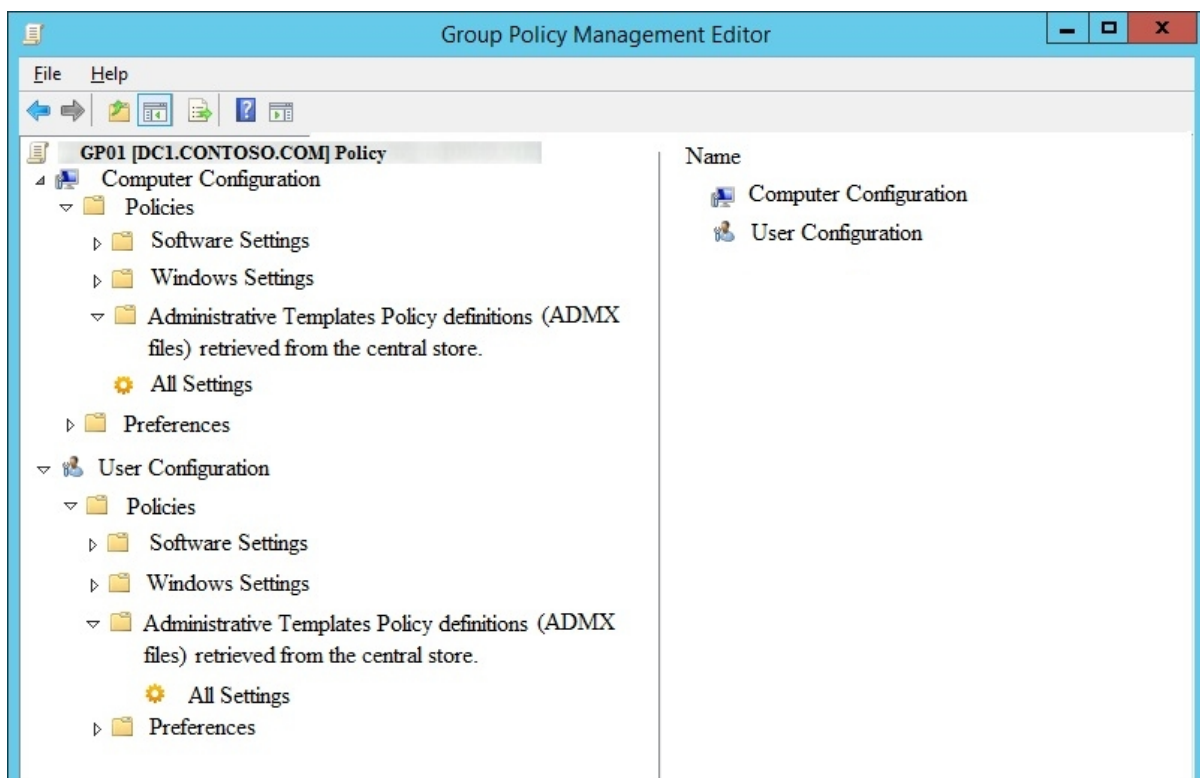
[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc755110\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc755110(v=ws.10))

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels>

Question 102

Your network contains an Active Directory domain named contoso.com. The domain contains a member server named Server1 and a domain controller named DC1. Both servers run Windows Server 2016. Server1 is used to perform administrative tasks, including managing Group Policies.

After maintenance is performed on DC1, you open a Group Policy object (GPO) from Server1 as shown in the exhibit.



You need to be able to view all of the Administrative Templates settings in GPO1. What should you do?

- ☐ From File Explorer, copy the administrative templates from \\contoso.com\SYSVOL\contoso.com\Policies to the PolicyDefinitions folder on Server1.
- ☒ From File Explorer, delete \\contoso.com\SYSVOL\contoso.com\Policies\PolicyDefinitions.
- ☐ From File Explorer, delete the PolicyDefinitions folder from Server1.
- ☐ From Group Policy Management, configure WMI Filtering for GPO1.

Question 103

You have a server named Server1 in a workgroup.

You need to configure a Group Policy setting on Server1 that will apply to only non-administrative users.

What should you do?

- ☐ Open Local Group Policy Editor. From the View menu, modify the Customize settings.
- ☐ Open Local Group Policy Editor. From the File menu, modify the Options settings.
- ☐ Open Local Users and Groups. Create a new group. Run New-GPO.
- ☒ Run mmc.exe. Add the Group Policy Object Editor snap-in and change the Group Policy object (GPO).

Explanation:

References:

<https://www.windowcentral.com/how-apply-local-group-policy-settings-specific-users-windows-10>

Question 104

Which of the following CA types would you deploy if you wanted to deploy a CA at the top of a hierarchy that could issue signing certificates to other CAs and which would be taken offline if not issuing, renewing, or revoking signing certificates?

- ☐ Enterprise root
- ☐ Enterprise subordinate
- ☒ Standalone root
- ☐ Standalone subordinate

Question 105

HOTSPOT

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

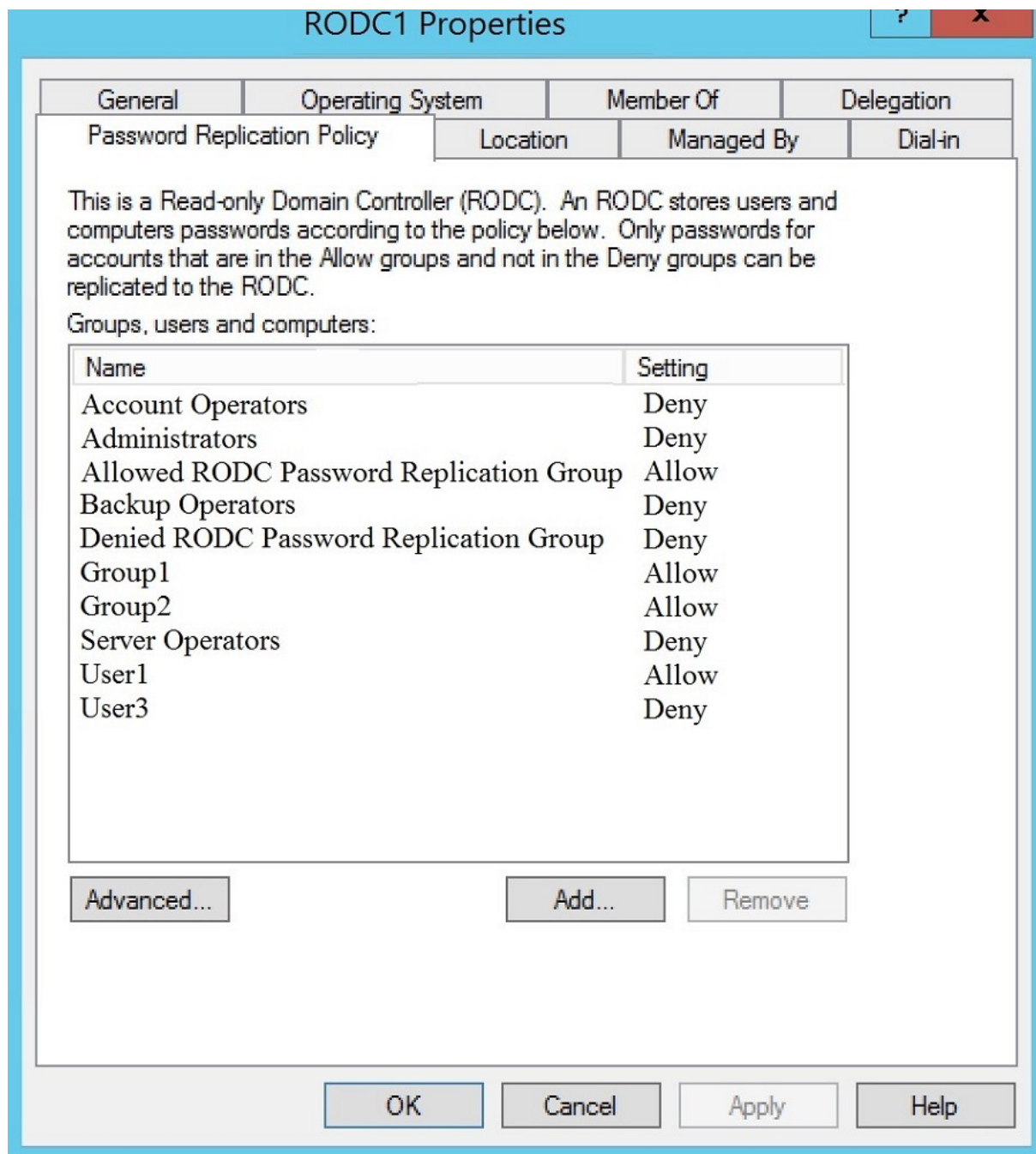
The domain contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1 and Group2

Group1 is a member of the Backup Operators group.

RODC1 has a Password Replication Policy configured as shown in the exhibit. (Click the Exhibit button.)

Exhibit:



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
After User1 is authenticated by RODC1, the password will be cached on RODC1	☐	☐
After User2 is authenticated by RODC1, the password will be cached on RODC1	☐	☐
After User3 is authenticated by RODC1, the password will be cached on RODC1	☐	☐

Solution:

Answer Area

Statements	Yes	No
After User1 is authenticated by RODC1, the password will be cached on RODC1	☐	☐
After User2 is authenticated by RODC1, the password will be cached on RODC1	☐	☐
After User3 is authenticated by RODC1, the password will be cached on RODC1	☐	☐

Question 106

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

The domain contains a web application that uses Kerberos authentication.

You change the domain name of the web application.

You need to ensure that the service principal name (SPN) for the application is registered.

Which tool should you use?

- ☐ Internet Information Services (IIS) Manager
- ☐ Rdsperf
- ☐ Repladmin
- ☒ Setspn
- ☐ Netsh
- ☐ Active Directory Users and Computers

Question 107

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory forest. The forest contains a domain named contoso.com. The domain contains three domain controllers.

A domain controller named lon-dc1 fails. You are unable to repair lon-dc1.

You need to prevent the other domain controllers from attempting to replicate to lon-dc1.

Solution: From Active Directory Domains and Trusts, you transfer the operations master roles from lon-dc1.

Does this meet the goal?

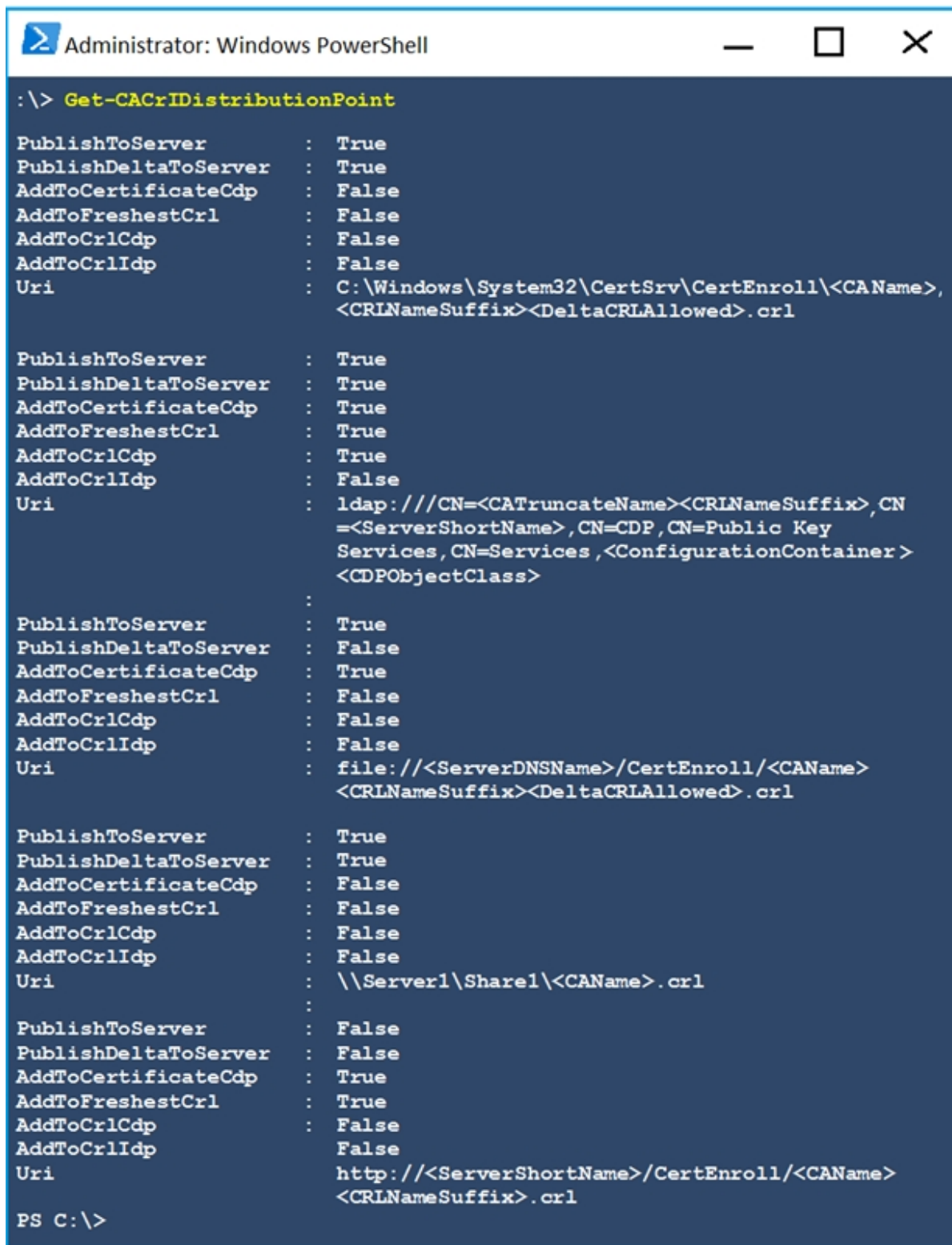
- ☒ Yes
☐ No

Question 108

HOTSPOT

Your network is isolated from the Internet. The network contains computers that are members of a domain and computers that are members of a workgroup. All the computers are configured to use internal DNS servers and WINS servers for name resolution.

The domain has a certification authority (CA). You run the `Get-CACrIDistributionPoint` cmdlet and receive the output as shown in the following exhibit.



```

Administrator: Windows PowerShell

:\> Get-CACrIDistributionPoint

PublishToServer      : True
PublishDeltaToServer : True
AddToCertificateCdp  : False
AddToFreshestCrl     : False
AddToCrlCdp          : False
AddToCrlIdp          : False
Uri                  : C:\Windows\System32\CertSrv\CertEnroll\<CAName>,
                     <CRLNameSuffix><DeltaCRLAllowed>.crl

PublishToServer      : True
PublishDeltaToServer : True
AddToCertificateCdp  : True
AddToFreshestCrl     : True
AddToCrlCdp          : True
AddToCrlIdp          : False
Uri                  : ldap:///CN=<CATruncateName><CRLNameSuffix>,CN
                     =<ServerShortName>,CN=CDP,CN=Public Key
                     Services,CN=Services,<ConfigurationContainer>
                     <CDPObjecClass>

PublishToServer      : True
PublishDeltaToServer : False
AddToCertificateCdp  : True
AddToFreshestCrl     : False
AddToCrlCdp          : False
AddToCrlIdp          : False
Uri                  : file://<ServerDNSName>/CertEnroll/<CAName>
                     <CRLNameSuffix><DeltaCRLAllowed>.crl

PublishToServer      : True
PublishDeltaToServer : True
AddToCertificateCdp  : False
AddToFreshestCrl     : False
AddToCrlCdp          : False
AddToCrlIdp          : False
Uri                  : \\Server1\Share1\<CAName>.crl

PublishToServer      : False
PublishDeltaToServer : False
AddToCertificateCdp  : True
AddToFreshestCrl     : True
AddToCrlCdp          : False
AddToCrlIdp          : False
Uri                  : http://<ServerShortName>/CertEnroll/<CAName>
                     <CRLNameSuffix>.crl

PS C:\>

```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

The certificate revocation list (CRL) can be accessed by using **[answer choice]**.

- ▼
- All the computers connected to the internal network
 - All computers from the Internet and the internal network
 - Only domain-joined computers connected to the internal network

The Delta certificate revocation list (CRL) can be accessed by using **[answer choice]**.

- ▼
- All the computers connected to the internal network
 - All computers from the Internet and the internal network
 - Only domain-joined computers connected to the internal network

Solution:

Answer Area

The certificate revocation list (CRL) can be accessed by using **[answer choice]**.

- ▼
- All the computers connected to the internal network
 - All computers from the Internet and the internal network
 - Only domain-joined computers connected to the internal network

The Delta certificate revocation list (CRL) can be accessed by using **[answer choice]**.

- ▼
- All the computers connected to the internal network
 - All computers from the Internet and the internal network
 - Only domain-joined computers connected to the internal network

Question 109

HOTSPOT

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

The domain contains three servers named Server1, Server2, and Server3 that run Windows Server 2016.

Server1 has IP Address Management (IPAM) installed. Server2 and Server3 have the DHCP Server role installed and have several DHCP scopes configured.

The IPAM server retrieves data from Server2 and Server3.

A domain user named User1 is a member of the groups shown in the following table.

Server name	Group
Server2	DHCP Administrators
Server3	DHCP Users

On Server1, you create a security policy for User1. The policy grants the IPAM DHCP Scope Administrator Role with the \Global access scope to the user.

Which actions can User1 perform? To answer, select the appropriate options in the answer area.

Answer Area

From Server Manager on Server1, User1 can modify the description of the DHCP scopes:

	▼
On Server2 only	
On Server3 only	
On both Server2 and Server3	

From Server Manager on Server1, User1 can create a new DHCP scope:

	▼
On Server2 only	
On Server3 only	
On both Server2 and Server3	

Solution:

Answer Area

From Server Manager on Server1, User1 can modify the description of the DHCP scopes:

	▼
On Server2 only	
On Server3 only	
On both Server2 and Server3	

From Server Manager on Server1, User1 can create a new DHCP scope:

	▼
On Server2 only	
On Server3 only	
On both Server2 and Server3	

Explanation:

Explanation:

User1 is using Server Manager, not IPAM to perform the administration. Therefore, only the "DHCP Administrators" permission on Server2 and the "DHCP Users" permissions on Server3 are applied.

The permissions granted through membership of the "IPAM DHCP Scope Administrator Role" are not applied when the user is not using the IPAM console.

Question 110

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

You need to create a central store for Group Policy administrative templates.

What should you use?

- ☐ Group Policy Management Console (GPMC)
- ☒ Copy-item
- ☐ Group Policy Management Editor
- ☐ Copy-GPO
- ☐ Server Manager
- ☐ Gpfixup.exe
- ☐ Dcgpofix.exe

Explanation:

References: <https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/copy-item?view=powershell-6>

Question 111

Your network contains an Active Directory domain. The domain contains a server named Server1 that runs Windows Server 2016. Server1 runs a service named Service1 in the security context of the Network Service account.

The domain contains an enterprise certification authority (CA).

You plan to create template that will be used to issue certificates for Service1. Server1 will enroll for the certificates on behalf of Service1.

Which template settings must you configure to allow Service1 to access the private keys of the certificates installed on Server1?

- ☐ Issuance requirements
- ☐ Request Handling
- ☐ Extensions
- ☒ Security

Explanation:

References:

<https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/configure-server-certificate-autoenrollment>

Question 112

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains the Active Directory forests and domains shown in the following table:

Forest name	Domain name	Domain type
ForestA	DomainARoot	Root
ForestA	DomainAChild1	Child
ForestB	DomainBRoot	Root
ForestB	DomainBChild1	Child
ForestB	DomainBChild2	Child

A two-way forest trust exists between ForestA and ForestB.

Each domain in ForestB contains user accounts that are used to manage servers.

You need to ensure that the user accounts used to manage the servers in ForestB are members of the Server Operators in ForestA.

Solution: You create a universal group in DomainBRoot. You add users to the new group. You modify the membership of the Server Operators in ForestA.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups#bkmk-serveroperators>

Question 113

Your network contains an Active Directory forest. The forest functional level is Windows Server 2016.

The network contains Linux servers that use MIT Kerberos V5 to provide an authentication, authorization, and access service.

You need to ensure that users can use their Active Directory credentials to access the resources on the Linux servers. The solution must minimize administrative effort.

What should you implement?

- ☐ an external trust
- ☒ a realm trust
- ☐ Active Directory Federation Services (AD FS)
- ☐ a Web Application Proxy

Explanation:

References:

<http://techgenix.com/active-directory-trusts/>

<https://www.rootusers.com/how-to-join-centos-linux-to-an-active-directory-domain/>

Question 114

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series.

Information and details provided in a question apply only to that question.

Your network contains an Active Directory domain named contoso.com. The domain contains 5,000 user accounts.

You have a Group Policy object (GPO) named DomainPolicy that is linked to the domain and a GPO named DCPolicy that is linked to the Domain Controllers organizational unit (OU).

You need to ensure that the members of the Backup Operators group can back up domain controllers.

What should you do?

- ☐ From the Computer Configuration node of DCPolicy, modify Security Settings.
- ☐ From the Computer Configuration node of DomainPolicy, modify Security Settings.
- ☐ From the Computer Configuration node of DomainPolicy, modify Administrative Templates.
- ☒ From the User Configuration node of DCPolicy, modify Security Settings.
- ☐ From the User Configuration node of DomainPolicy, modify Folder Redirection.
- ☐ From user Configuration node of DomainPolicy, modify Administrative Templates.
- ☐ From Preferences in the User Configuration node of DomainPolicy, modify Windows Settings.
- ☐ From Preferences in the Computer Configuration node of DomainPolicy, modify Windows Settings.

Question 115

HOTSPOT

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

You need to add a new domain named fabrikam.com to the forest.

What command should you run? To answer, select the appropriate options in the answer area.

Answer Area

	-DomainType
Install-ADDSDomain	TreeDomain
Install-ADDSDomainController	ChildDomain
Install-ADDSEForest	


```
-InstallDns:$true -NewDomainName fabrikam.com -ParentDomainName contoso.com
```

Solution:

Answer Area

	-DomainType
Install-ADDSDomain	TreeDomain
Install-ADDSDomainController	ChildDomain
Install-ADDSEForest	


```
-InstallDns:$true -NewDomainName fabrikam.com -ParentDomainName contoso.com
```

Explanation:

Reference:

<https://docs.microsoft.com/en-us/powershell/module/addsdeployment/install-addsdomain?view=winserver2012r2-ps>

Question 116

Your network contains two Active Directory forests named fabrikam.com and contoso.com. Each forest contains two sites. Each site contains two domain controllers.

You need to configure all the domain controllers in both the forests as global catalog servers.

Which snap-in should you use?

- ☐ Active Directory Users and Computers
- ☒ Active Directory Sites and Services
- ☐ Active Directory Domains and Trusts
- ☐ Active Directory Federation Services

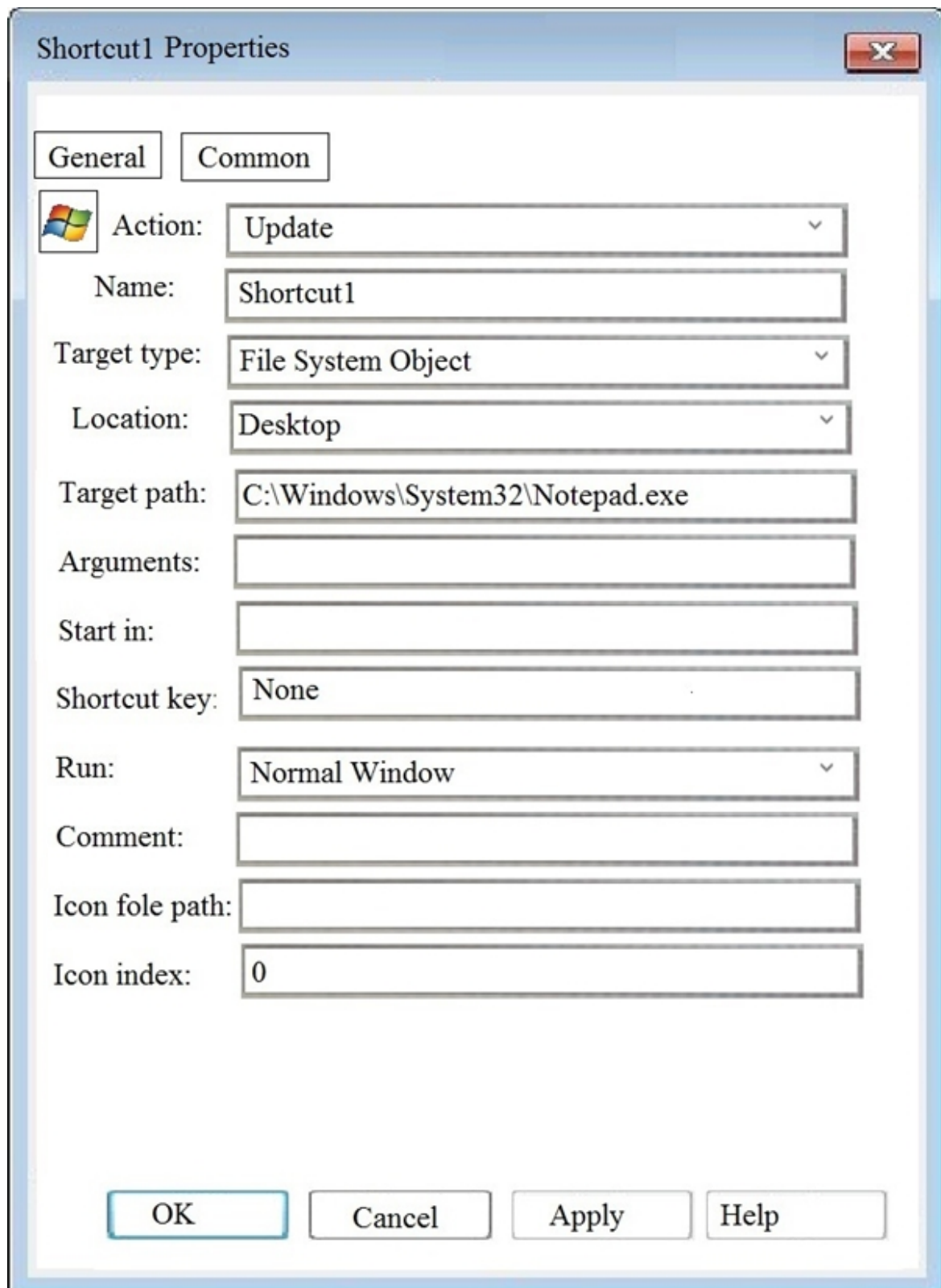
Question 117

HOTSPOT

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

A user named User1 and a computer named Computer1 are in an organizational unit OU1. A user named User2 and a computer named Computer 2 are in an OU named OU2.

A Group Policy object (GPO) named GPO1 is linked to the domain. GPO1 contains a user preference that is configured as shown in the Shortcut1 Properties exhibit. (Click the Exhibit button.)



Item-level targeting for the user preference is configured as shown in the Targeting exhibit. (Click the Exhibit button.)

Targeting Editor

New Item ▾ Add Collection Item Options ▾ [undo] [redo] [cut] [copy] [paste] [delete] [help]

The DNS computer name is contoso.com

Computer name

☐ NetBIOS
☒ DNS

A Computer Name targeting item allows a preference item to be applied to computers or users only if the computer's name matches the specified computer name in the targeting item. [Additional information...](#)

OK Cancel

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If User1 signs in to Computer1, Shortcut1 will appear on the desktop.	☐	☐
If User1 signs in to Computer2, Shortcut1 will appear on the desktop.	☐	☐
If User2 signs in to Computer1, Shortcut1 will appear on the desktop.	☐	☐

Solution:

Answer Area

Statements	Yes	No
If User1 signs in to Computer1, Shortcut1 will appear on the desktop.	☐	☐
If User1 signs in to Computer2, Shortcut1 will appear on the desktop.	☐	☐
If User2 signs in to Computer1, Shortcut1 will appear on the desktop.	☐	☐

Explanation:

References: <https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc730752%28v%3dws.10%29>

Question 118

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

A partner company has a forest named fabrikam.com. Each forest contains one domain.

You need to provide access for a group named Research in fabrikam.com to resources in contoso.com. The solution must use the principle of least privilege.

What should you do?

- ☐ Create an external trust from fabrikam.com to contoso.com. Enable Active Directory split permissions in fabrikam.com.
- ☐ Create an external trust from contoso.com to fabrikam.com. Enable Active Directory split permissions in contoso.com.
- ☒ Create a one-way forest trust from contoso.com to fabrikam.com that uses selective authentication.
- ☐ Create a one-way forest trust from fabrikam.com to contoso.com that uses selective authentication.

Explanation:

Explanation:

Question 119

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

A user named User1 is in an organizational unit (OU) named OU1.

You are troubleshooting a folder access issue for User1.

You need a list of groups to which User1 is either a direct member or an indirect member.

Solution: You run `dsget user cn=User1, ou=OU1, dc=contoso, dc=com -memberof -expand`.

Does this meet the goal?

- ☒ Yes
☐ No

Explanation:

Explanation:

DSGET displays the properties of a user in the directory. There are two variations of this command. The first variation displays the properties of multiple users. The second variation displays the group membership information of a single user.

To show the list of groups, recursively expanded, to which the user Mike Danseglio belongs, type:

`dsget user "CN=Mike Danseglio,CN=users,dc=ms,dc=tld" -memberof -expand`

References: <https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732535%28v%3dws.10%29>

Question 120

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

A partner organization has an Active Directory forest named contoso.com.

Adatum.com contains an Active Directory Rights Management (AD RMS) cluster installed on a server named adat1.adatum.com.

Contoso.com contains an Active Directory Rights Management Services (AD RMS) cluster installed on a server named cont1.contoso.com.

You need to allow the AD RMS cluster in adatum.com to accept rights account certificates (RACs) from contoso.com.

What should you do?

- ☐ In contoso.com, import the trusted user domain file from adat1.adatum.com
- ☐ In adatum.com, import the trusted publishing domain file from adat1.adatum.com
- ☐ In contoso.com, import the trusted publishing domain file from cont1.contoso.com
- ☒ In adatum.com, import the trusted user domain file from cont1.contoso.com

Explanation:

References:

https://winintro.ru/rms_help.en/html/59c802d0-3982-432c-b06f-3e148dca0166.htm

Question 121

You deploy a new enterprise certification authority (CA) named CA1.

You plan to issue certificates based on the User certificate template.

You need to ensure that the issued certificates are valid for two years and support autoenrollment.

What should you do first?

- ☐ Run the certutil.exe command and specify the resubmit parameter.
- ☒ Duplicate the User certificate template.
- ☐ Add a new certificate template for CA1 to issue.
- ☐ Modify the Request Handling settings for the CA.

Explanation:

Explanation:

The built-in templates do not support auto-enrollment. You need to duplicate the template then modify the permissions on the new template.

References: <https://docs.centrixy.com/en/centrixy/adminref/index.html#page/cloudhelp/cloud-admin-install-create-cert-templates.html>

Question 122

HOTSPOT

You have a server named Server1 that runs Windows Server 2016. Server1 has the Web Application Proxy role service installed.

You need to publish Microsoft Exchange Server 2013 services through the Web Application Proxy. The solution must use preauthentication whenever possible.

How should you configure the preauthentication method for each service? To answer, select the appropriate options in the answer area.

Answer Area

Exchange ActiveSync:	Active Directory Federation Services (AD FS) Pass-through
Outlook Web App:	Active Directory Federation Services (AD FS) Pass-through
Outlook Anywhere:	Active Directory Federation Services (AD FS) Pass-through

Solution:

Answer Area

Exchange ActiveSync:	 ▼ Active Directory Federation Services (AD FS) Pass-through
Outlook Web App:	 ▼ Active Directory Federation Services (AD FS) Pass-through
Outlook Anywhere:	 ▼ Active Directory Federation Services (AD FS) Pass-through

Explanation:

Explanation:

Box 1: Pass-through

Box 2: Active Directory Federation Services (ADFS)

Box 3: Pass-through

The following table describes the Exchange services that you can publish through Web Application Proxy and the supported preauthentication for these services:

Exchange service	Preauthentication
Outlook Web App	• AD FS using non-claims-based authentication • Pass-through • AD FS using claims-based authentication for on-premises Exchange 2013 Service Pak 1 (SP1)
Exchange Control Panel	Pass-through
Outlook Anywhere	Pass-through
Exchange ActiveSync	Pass-through

References: <https://docs.microsoft.com/en-us/windows-server/remote/remote-access/web-application-proxy/publishing-applications-with-sharepoint%2C-exchange-and-rdg>

Question 123

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You deploy a new Active Directory forest.

You need to ensure that you can create a group Managed Service Account (gMSA) for multiple member servers.

Solution: You configure Kerberos constrained delegation on the computer account of each domain controller.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 124

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario.

You work for a company named Contoso, Ltd.

The network contains an Active Directory forest named contoso.com. A forest trust exists between contoso.com and an Active Directory forest named adatum.com.

The contoso.com forest contains the objects configured as shown in the following table.

Object name	Object type	Group scope	Group type
User1	User	<i>Not applicable</i>	<i>Not applicable</i>
User2	User	<i>Not applicable</i>	<i>Not applicable</i>
Computer1	Computer	<i>Not applicable</i>	<i>Not applicable</i>
Group1	Group	Domain local	Security
Group2	Group	Domain local	Security
Group3	Group	Universal	Security
Group4	Group	Global	Security
Group5	Group	Universal	Security

Group1 and Group2 contain only user accounts.

Contoso hires a new remote user named User3. User3 will work from home and will use a computer named Computer3 that runs Windows 10. Computer3 is currently in a workgroup.

An administrator named Admin1 is a member of the Domain Admins group in the contoso.com domain.

From Active Directory Users and Computers, you create an organizational unit (OU) named OU1 in the contoso.com domain, and then you create a contact named Contact1 in OU1.

An administrator of the adatum.com domain runs the Set-ADUser cmdlet to configure a user named User1 to have a user logon name of User1@litwareinc.com.

End of repeated scenario.

You need to ensure that Admin1 can add Group2 as a member of Group3.

What should you modify?

- ☐ Modify the Security settings of Group3.
- ☒ Modify the group scope of Group3.
- ☐ Modify the group type of Group3.
- ☐ Set Admin1 as the manager of Group3.
- ☐ Add Admin1 to the Enterprise Admins group

Explanation:

Explanation:

A domain local group (group2) can only be a member of another domain local group. Therefore, we need to change the scope of Group3 from Universal to Domain Local.

Question 125

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

You plan to deploy a new Active Directory Rights Management Services (AD RMS) cluster on a server named Server1.

You need to create the AD RMS service account. The solution must use the principle of least privilege.

What should you do?

- ☐ Create a local user account on Server1 and add the account to the Administrators group on Server1.
- ☐ Create a domain user account and add the account to the Administrators group on Server1.
- ☒ Create a domain user account and add the account to the Domain Users group in the domain.
- ☐ Create a domain user account and add the account to the Account Operators group in the domain.

Question 126

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

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

The domain functional level is Windows Server 2012 R2.

Your company hires a new security administrator to manage sensitive user data.

You create a user account named Security1 for the security administrator.

You need to ensure that the password for Security1 has at least 12 characters and is modified every 10 days. The solution must apply to Security1 only.

Which tool should you use?

- ☐ Dsadd quota
- ☐ Dsmmod
- ☒ Active Directory Administrative Center
- ☐ Dsacls
- ☐ Dsamain
- ☐ Active Directory Users and Computers
- ☐ Ntdsutil
- ☐ Group Policy Management Console

Question 127

Your network contains an Active Directory forest named contoso.com. The forest contains several domains.

An administrator named Admin01 installs Windows Server 2016 on a server named Server1 and then joins Server1 to the contoso.com domain.

Admin01 plans to configure Server1 as an enterprise root certification authority (CA).

You need to ensure that Admin01 can configure Server1 as an enterprise CA. The solution must use the principle of least privilege.

To which group should you add Admin01?

- ☐ Server Operators in the contoso.com domain
- ☐ Cert Publishers on Server1
- ☐ Enterprise Key Admins in the contoso.com domain
- ☒ Enterprise Admins in the contoso.com domain.

Explanation:

Explanation:

To install Active Directory Certificate Services, log on as a member of both the Enterprise Admins group and the root domain's Domain Admins group.

References: <https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/install-the-certification-authority>

Question 128

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain.

You have a user account that is a member of the Domain Admins group.

You have 100 laptops that have a standard corporate image installed. The laptops are in workgroups and have random names.

A technician named Tech1 is assigned the task of joining the laptops to the domain. The computer accounts of each laptop must be in an organizational unit (OU) that is associated to the department of the user who will use the laptop. The laptop names must start with four characters indicating the department, followed by a four-digit number.

Tech1 is a member of the Domain Users group only. Tech1 has the administrator logon credentials for all the laptops.

You need Tech1 to join the laptops to the domain. The solution must ensure that the laptops are named correctly, and the computer accounts of the laptops are in the correct OUs.

Solution: You instruct Tech1 to sign in to each laptop, to rename each laptop by using System in Control Panel, and then to join each laptop to the domain by using the Netdom join command.

Does this meet the goal?

- ☒ Yes
☐ No

Question 129

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory forest. The forest contains a domain named contoso.com. The domain contains three domain controllers.

A domain controller named lon-dc1 fails. You are unable to repair lon-dc1.

You need to prevent the other domain controllers from attempting to replicate to lon-dc1.

Solution: From ntdsutil.exe, you perform a metadata cleanup.

Does this meet the goal?

- ☒ Yes
- ☐ No

Question 130

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

You need to create a central store for Group Policy administrative templates.

What should you use?

- ☐ Server Manager
- ☒ File Explorer
- ☐ Copy-GPO
- ☐ Group Policy Management Console (GPMC)
- ☐ Group Policy Management Editor
- ☐ Gpfixup.exe
- ☐ Dcgpofix.exe

Explanation:

References:

<http://www.redbass.net/create-central-store-group-policy-administrative-templates/>

Question 131

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

You have an Active Directory Federation Services (AD FS) farm. The farm contains a server named Server1 that runs Windows Server 2012 R2.

You add a server named Server2 to the farm. Server2 runs Windows Server 2016.

You remove Server1 from the farm.

You need to ensure that you can use role separation to manage the farm.

Which cmdlet should you run?

- ☐ Set-AdfsFarmInformation
- ☐ Update-AdfsRelyingPartyTrust
- ☐ Set-AdfsProperties
- ☒ Invoke-AdfsFarmBehaviorLevelRaise

Explanation:

Explanation:

Question 132

You are deploying a web application named WebApp1 to your internal network. WebApp1 is hosted on a server named Web1 that runs Windows Server 2016.

You deploy an Active Directory Federation Services (AD FS) infrastructure and a Web Application Proxy to provide access to WebApp1 for remote users.

You need to ensure that Web1 can authenticate the remote users.

What should you do?

- ☐ Publish WebApp1 by using AD FS preauthentication.
- ☐ Publish WebApp1 as a Remote Desktop Gateway (RD Gateway) application in the Web Application Proxy.
- ☒ Publish WebApp1 by using pass-through preauthentication.
- ☐ Publish WebApp1 by using client certificate preauthentication.

Question 133

Your network contains an Active Directory forest named contoso.com. The forest contains a member server named Server1 that runs Windows Server 2016. Server1 is located in the perimeter network.

You install the Active Directory Federation Services server role on Server1. You create an Active Directory Federation Services (AD FS) farm by using a certificate that has a subject name of sts.contoso.com.

You need to enable certificate authentication from the Internet on Server1.

Which two inbound TCP ports should you open on the firewall? Each correct answer presents part of the solution.

- ☐ 389
- ☒ 443
- ☐ 3389
- ☐ 8531
- ☒ 49443

Explanation:

Explanation:

Question 134

Your network contains an Active Directory domain named contoso.com. The relevant objects in the domain are configured as shown in the following table.

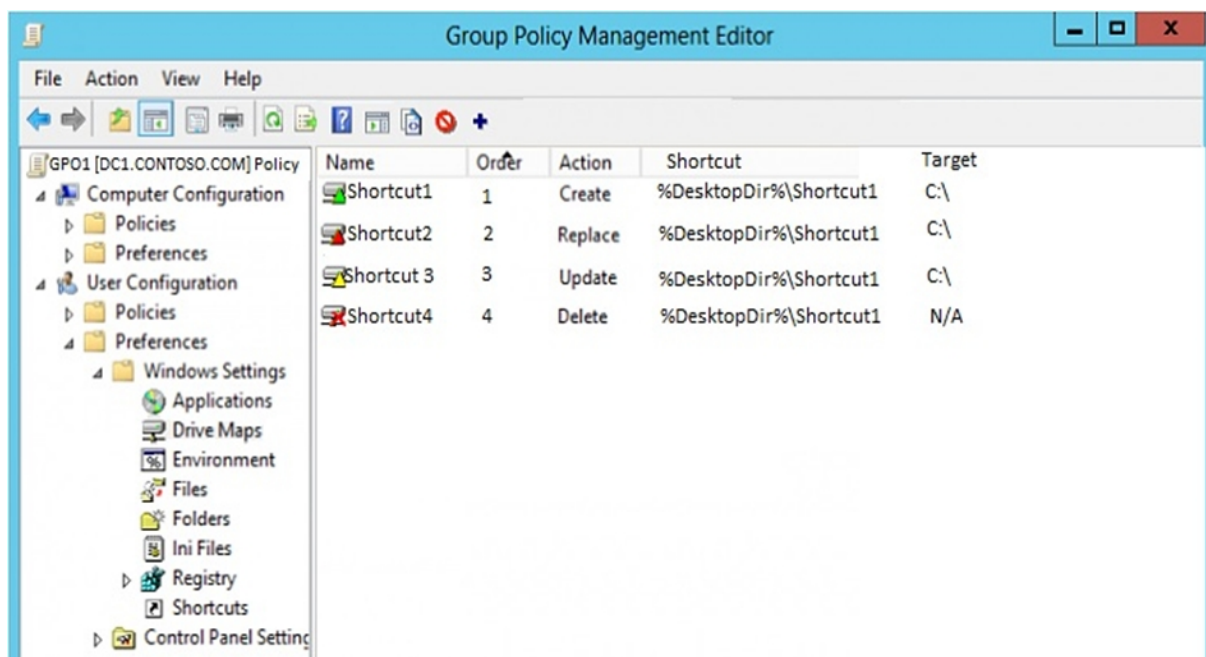
Object name	Type
Computer1	Domain computer
OU1	Organizational unit (OU)
GPO1	Group Policy object (GPO)
User1	User account

User1 is in OU1. GPO1 is linked to OU1.

The settings in GPO1 are configured as shown in the exhibit. (Click the Exhibit tab.)

Computer1 does not have any shortcuts on the desktop.

How many shortcuts appear on the desktop after User1 signs in to Computer1?



- ☒ 1
- ☐ 2
- ☐ 3
- ☐ 4

Question 135

HOTSPOT

You have a server named Server1 that runs Windows Server 2016. Server1 has the Web Application Proxy role service installed.

You need to publish Microsoft Exchange ActiveSync services by using the Publish New Application Wizard. The ActiveSync services must use preauthentication.

How should you configure Server1? To answer, select the appropriate options in the answer area.

Answer Area

Preauthentication method:

	▼
Active Directory Federation Services (AD FS)	
Pass-through	

Preauthentication type:

	▼
HTTP Basic	
OAuth2	
Web and MS-OFBA	

Solution:**Answer Area**

Preauthentication method:

	▼
Active Directory Federation Services (AD FS)	
Pass-through	

Preauthentication type:

	▼
HTTP Basic	
OAuth2	
Web and MS-OFBA	

Question 136

Your network contains an Active Directory domain named contoso.com. The network contains several IP subnets. One of the subnets uses a network ID of 192.168.10.0/24.

You link a Group Policy object (GPO) named GPO1 to the domain.

You need to map a drive to a specific file share on the computers in the 192.168.10.0/24 network only.

What should you do?

- ☐ From the User Configuration node of GPO1, configure the Folder Redirection settings. Link a WMI filter to GPO1.
- ☐ From the Computer Configuration node of GPO1, configure the Network Connections settings. Link a WMI filter to GPO1.
- ☒ From the User Configuration node of GPO1, create a Group Policy preference that uses item-level targeting.
- ☐ From the Computer Configuration node of GPO1, create a Group Policy preference that uses item-level targeting.

Question 137

Your network contains an Active Directory domain named contoso.com. The domain contains servers that run Windows Server 2016 and client computers that run Windows 10. The naming conventions for the computers and the servers is inconsistent.

You plan to create a Group Policy object (GPO) named GPO1 and to link GPO1 to the domain. GPO1 will contain custom Group Policy preference settings.

You need to ensure that the preference settings in GPO1 will apply only to member servers. GPO1 must NOT apply to domain controllers or client computers.

Which type of item level targeting should you use?

- ☐ Security Group
- ☐ Processing Mode
- ☒ Operating System
- ☐ Environment Variable
- ☐ Domain

Explanation:

References:

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc733022\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc733022(v=ws.11))

<https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753566%28v%3dws.10%29>

Question 138

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

You have an organizational unit (OU) named OU1. A Group Policy object (GPO) named GPO1 is linked to OU1.

You create a user named User1, and you assign User1 the Full control permission to OU1.

Which administrative action for GPOs can User1 perform?

- ☒ Link an existing GPO from the domain to OU1
- ☐ Create a new GPO and link the GPO to OU1
- ☐ Add an administrative template to GPO1
- ☐ Edit the User Rights Assignment in GPO1

Question 139

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory forest named contoso.com. The forest contains a member server named Server1 that runs Windows Server 2016. All domain controllers run Windows Server 2012 R2.

Contoso.com has the following configuration.

```
PS C:\> (Get-ADForest).ForestMode
Windows2008R2Forest
```

```
PS C:\> (Get-ADDomain).DomainMode
Windows2008R2Domain
PS C:\>
```

You plan to deploy an Active Directory Federation Services (AD FS) farm on Server1 and to configure device registration.

You need to configure Active Directory to support the planned deployment.

Solution: You raise the domain functional level to Windows Server 2012 R2.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Explanation:

Device Registration requires Windows Server 2012 R2 forest schema (not just domain schema).

References: <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/configure-a-federation-server-with-device-registration-service>

Question 140

You are configuring AD FS. Which server should you deploy on your organization's perimeter network?

- ☒ Web application proxy
- ☐ Relying-party server
- ☐ Federation server
- ☐ Claims-provider server

Question 141

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You need to identify which server is the schema master.

Solution: You open Active Directory Domains and Trusts, right-click Active Directory Domains and Trust in the console tree, and then click Operations Master.

Does this meet the goal?

- ☐ Yes
- ☒ No

Explanation:

Explanation:

You need to use the Schema snap-in to find the schema master. The Schema snap-in is not installed by default but can be installed by using Schmmgmt.dll.

References:

https://www.petri.com/determining_fsmo_role_holders

Question 142

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory forest named contoso.com. The forest contains a member server named Server1 that runs Windows Server 2016. All domain controllers run Windows Server 2012 R2.

Contoso.com has the following configuration.

```
PS C:\> (Get-ADForest).ForestMode
Windows2008R2Forest
```

```
PS C:\> (Get-ADDomain).DomainMode
Windows2008R2Domain
PS C:\>
```

You plan to deploy an Active Directory Federation Services (AD FS) farm on Server1 and to configure device registration.

You need to configure Active Directory to support the planned deployment.

Solution: You run adprep.exe from the Windows Server 2016 installation media.

Does this meet the goal?

- ☒ Yes
☐ No

Explanation:

Explanation:

Device Registration requires Windows Server 2012 R2 forest schema. We can run adprep.exe to upgrade the schema.

References:

<https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/configure-a-federation-server-with-device-registration-service>

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/upgrade-domain-controllers-to-windows-server-2012-r2-and-windows-server-2012>

Question 143

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You need to identify which server is the schema master.

Solution: You open Active Directory Users and Computers, right-click contoso.com in the console tree, and then click Operations Master.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Explanation:

You need to use the Schema snap-in to find the schema master. The Schema snap-in is not installed by default but can be installed by using Schmmgmt.dll.

References:

https://www.petri.com/determining_fsmo_role_holders

Question 144

You create a user account that will be used as a template for new user accounts.

Which setting will be copied when you copy the user account from Active Directory Users and Computers?

- ☒ the Department attribute
☐ the Description attribute
☐ Permission
☐ Remote Desktop Services Profile
☐ the User logon name attribute
☐ Published Certificates
☐ the Office attribute

Explanation:

Explanation:

A user template in Active Directory can be used if you are creating users for a specific department, with exactly the same properties, and membership to the same user groups. A user template is nothing more than a disabled user account that has all these settings already in place.

References: <http://www.rebeladmin.com/2014/07/create-users-with-user-templates-in-ad/>

Question 145

Your network contains an Active Directory forest. The forest contains two domains named contoso.com and fabrikam.com. The functional level of the forest and the domains is Windows Server 2008 R2.

You have a global group named Group1 in the contoso.com domain. Group1 contains the user accounts in the contoso.com.

You need to ensure that you can add the user accounts in the fabrikam.com domain to Group1.

What should you do?

- ☐ Assign the Domain Controllers group in fabrikam.com permissions to Group1.
- ☒ Modify the scope of Group1 to Universal.
- ☐ Raise the domain functional level contoso.com to Windows Server 2016.
- ☐ Raise the domain functional level of fabriakm.com Windows Server 2016.
- ☐ Change Group1 to a distribution group

Question 146

Your network contains an Active Directory domain. The domain contains a computer named Computer1 and an organizational unit (OU) named TestOU. TestOU contains 10 computer accounts that are used for testing. A Group Policy object (GPO) named GPO1 is linked to TestOU.

On Computer1, you modify the User Right Assignment by using the local policy.

You need to apply the User Right Assignment from Computer1 to the 10 test computers.

What should you do?

- ☒ On Computer1 run the secedit.exe command and specify the /export parameter. Edit GPO1, and then import a security template.
- ☐ On Computer1, run the gpresult.exe command and specify the /x parameter. Edit GPO1, and then import a security template.
- ☐ On Computer1, run the secedit.exe command and specify the /export parameter. From Group Policy Management, run the Import Settings Wizard.
- ☐ On Computer1, run the gpresult.exe command and specify the /x parameter. From Group Policy Management, run the Restore Group Policy Object Wizard.

Question 147

DRAG DROP

You network contains an Active Directory domain named contoso.com.
The domain contains an enterprise certification authority (CA).
A user named Admin1 is a member of the Domain Admins group.

You need to ensure that you can archive keys on the CA. The solution must use Admin1 as a key recovery agent.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
From the Certificate Templates console, modify the extensions of a certificate template.	
From Server Manager, install the Online Responder role service.	
From the Certificates Console, request a certificate.	
From the Certification Authority console, add a certificate template to issue.	
From the Certification Authority console, add a Key Recovery Agent certificate.	
From the Certification Authority console, issue a pending request.	
From the Certificate Templates console, modify the security of a certificate template.	

Solution:

Actions	Answer Area
From the Certificate Templates console, modify the extensions of a certificate template.	From the Certification Authority console, add a certificate template to issue.
From Server Manager, install the Online Responder role service.	From the Certificates Console, request a certificate.
From the Certificates Console, request a certificate.	From the Certification Authority console, issue a pending request.
From the Certification Authority console, add a certificate template to issue.	From the Certification Authority console, add a Key Recovery Agent certificate.
From the Certification Authority console, add a Key Recovery Agent certificate.	
From the Certification Authority console, issue a pending request.	
From the Certificate Templates console, modify the security of a certificate template.	

Question 148**HOTSPOT**

Your network contains a single-domain Active Directory forest named contoso.com. The forest functional level is Windows Server 2016. The Active Directory Recycle Bin feature is enabled.

You need to design a procedure to restore the values of user object attributes if the values are changed accidentally.

Which cmdlets should you include in the procedure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Cmdlet to capture the attribute value changes:	▼ Add-History Enable-ADOptionalFeature New-AdIStore New-ADSnapshot New-VirtualDiskSnapshot
Cmdlets to restore the attribute values:	▼ Enable-ADOptionalFeature and Repair-ADAttribute Enable-ADOptionalFeature and Restore-ADObject Mount-ADDatabase and Repair-ADAttribute Move-ADObject and Restore-ADObject

Solution:

Answer Area

Cmdlet to capture the attribute value changes:	▼
	Add-History
	Enable-ADOptionalFeature
	New-AdIStore
	New-ADSnapshot
Cmdlets to restore the attribute values:	▼
	Enable-ADOptionalFeature and Repair-ADAttribute
	Enable-ADOptionalFeature and Restore-ADObject
	Mount-ADDatabase and Repair-ADAttribute
	Move-ADObject and Restore-ADObject

Explanation:

References:

<https://blogs.technet.microsoft.com/ashleymcglone/2014/04/24/oh-snap-active-directory-attribute-recovery-with-powershell/>

Question 149

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You need to identify which server is the schema master.

Solution: From a command prompt, you run netdom query fsmo.

Does this meet the goal?

- ☒ Yes
☐ No

Explanation:

References:

<https://blogs.technet.microsoft.com/canitpro/2017/05/24/step-by-step-migrating-active-directory-fsmo-roles-from-windows-server-2012-r2-to-2016/>

Question 150

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory forest named contoso.com. The forest contains 10 domains.

The root domain contains a global catalog server named DC1.

You remove the global catalog server role from DC1.

You need to decrease the size of the Active Directory database on DC1.

Solution: You restart DC1 in Safe Mode. You run ntdsutil.exe, use the files option, and then restart DC1.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

References:

<https://theitbros.com/active-directory-database-compact-defrag/>

Question 151

Your company has a marketing department and a security department.
The network contains an Active Directory domain named contoso.com.
The domain contains an enterprise certification authority (CA).

You have two organizational units (OUs) named MKT_UsersOU and MKT_ComputersOU.
MKT_UsersOU contains the user accounts for the users in the marketing department.
MKT_ComputersOU contains the computer accounts for the computers in the marketing department.

A Group policy object (GPO) named GPO1 is linked to MKT_UsersOU.
A GPO named GPO2 linked to MKT_ComputersOU.
You plan to deploy a web application for the marketing department users.
The application will require certificates for authentication.
The security department configures the CA to support the planned deployment.

You need to ensure that the web application can authenticate the marketing department users.
What should you do?

- ☐ From the User Configuration node of GPO1, create an Internet Setting preference.
- ☒ From the User Configuration node of GPO1, configure the Certificate Services Client - Auto-enrollment settings.
- ☐ From the Computer Configuration node of GPO2, configure the Certificate Services Client - Certificate Enrollment Policy settings.
- ☐ From the Computer Configuration node of GPO2, create the Automatic Certificate Request Settings.

Question 152

Your network contains two Active Directory forests named fabrikam.com and contoso.com. Each forest contains a single domain.

Contoso.com has a Group Policy object (GPO) named Cont_GPO1.

You need to apply the settings from Cont_GPO1 to the computers in fabrikam.com.

Which two actions should you perform? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- ☒ Back up Cont_GPO1. In fabrikam.com, create and link a new GPO by using the Group Policy Management Console (GPMC), and then run the Import Settings Wizard.
- ☐ Back up Cont_GPO1. In fabrikam.com, run the Restore-GPO cmdlet, and then run the New-GPLink cmdlet.
- ☒ Back up Cont_GPO1. In fabrikam.com run the Import-GPO cmdlet, and then run the New-GPLink cmdlet.
- ☐ Copy\\contoso.com\SysVol\contoso.com\Policies to \\fabrikam.com\SysVol\fabrikam.com\Policies. In fabrikam.com, run the New-GPLink cmdlet.
- ☐ Back up Cont_GPO1. In fabrikam.com, create and link a new GPO by using the Group Policy Management Console (GPMC), and then run the Restore Group Policy Object Wizard.

Question 153

HOTSPOT

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

Some user accounts in the domain have the P.O. Box attribute set.

You plan to remove the value of the P.O. Box attribute for all of the users by using Ldifde.

You have a user named User1 who is located in the Users container.

How should you configure the LDIF file to remove the value of the P.O. Box attribute for User1? To answer, select the appropriate options in the answer area.

Answer Area

dn:

	▼
CN=User1, CN=Users, DC=contoso, DC=com	
CN=User1, OU=Users, DC=contoso, DC=com Contoso.com/Users/User1	
User1	

changetype:

	▼
add	
delete	
modify	

delete: postOfficeBox

Solution:

Answer Area

dn:

	▼
CN=User1, CN=Users, DC=contoso, DC=com	
CN=User1, OU=Users, DC=contoso, DC=com Contoso.com/Users/User1	
User1	

changetype:

	▼
add	
delete	
modify	

delete: postOfficeBox

Question 154

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains the Active Directory forests and domains shown in the following table:

Forest name	Domain name	Domain type
ForestA	DomainARoot	Root
ForestA	DomainAChild1	Child
ForestB	DomainBRoot	Root
ForestB	DomainBChild1	Child
ForestB	DomainBChild2	Child

A two-way forest trust exists between ForestA and ForestB.

Each domain in ForestB contains user accounts that are used to manage servers.

You need to ensure that the user accounts used to manage the servers in ForestB are members of the Server Operators in ForestA.

Solution: In DomainBRoot, you add the users to the Server Operators group. You modify the membership of the Server Operators in ForestA.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups#bkmk-serveroperators>

Question 155

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory forest. The forest contains a domain named contoso.com. The domain contains three domain controllers.

A domain controller named lon-dc1 fails. You are unable to repair lon-dc1.

You need to prevent the other domain controllers from attempting to replicate to lon-dc1.

Solution: From Active Directory Users and Computers, you remove the computer account of lon-dc1.

Does this meet the goal?

- ☒ Yes
☐ No

Explanation:

Explanation:

To remove the failed server object from the domain controllers container, access Active Directory Users and Computers, expand the domain controllers container, and delete the computer object associated with the failed domain controller

References: https://www.petri.com/delete_failed_dcs_from_ad

Question 156

Your network contains an Active Directory forest. The forest contains two domains named litwarenc.com and contoso.com. The contoso.com domain contains two domain controllers named LON-DC01 and LON-DC02. The domain controllers are located in a site named London that is associated to a subnet of 192.168.10.0/24

You discover that LON-DC02 is not a global catalog server.

You need to configure LON-DC02 as a global catalog server.

What should you do?

- ☐ From Active Directory Sites and Services, modify the properties of the 192.168.10.0/24 IP subnet.
- ☐ From Windows PowerShell, run the Set-NetNatGlobal cmdlet.
- ☒ From Active Directory Sites and Services, modify the NTDS Settings object of LON-DC02.
- ☐ From Windows PowerShell, run the Enable-ADOptionalFeature cmdlet.
- ☐ From the properties of the LON-DC02 computer account in Active Directory Users and Computers, modify the NTDS settings.
- ☐ From the properties of the LON-DC02 computer account in Active Directory Users and Computers, modify the City attribute.
- ☐ From the properties of the Domain Controllers organizational unit (OU) in Active Directory Users and Computers, modify the Security settings.

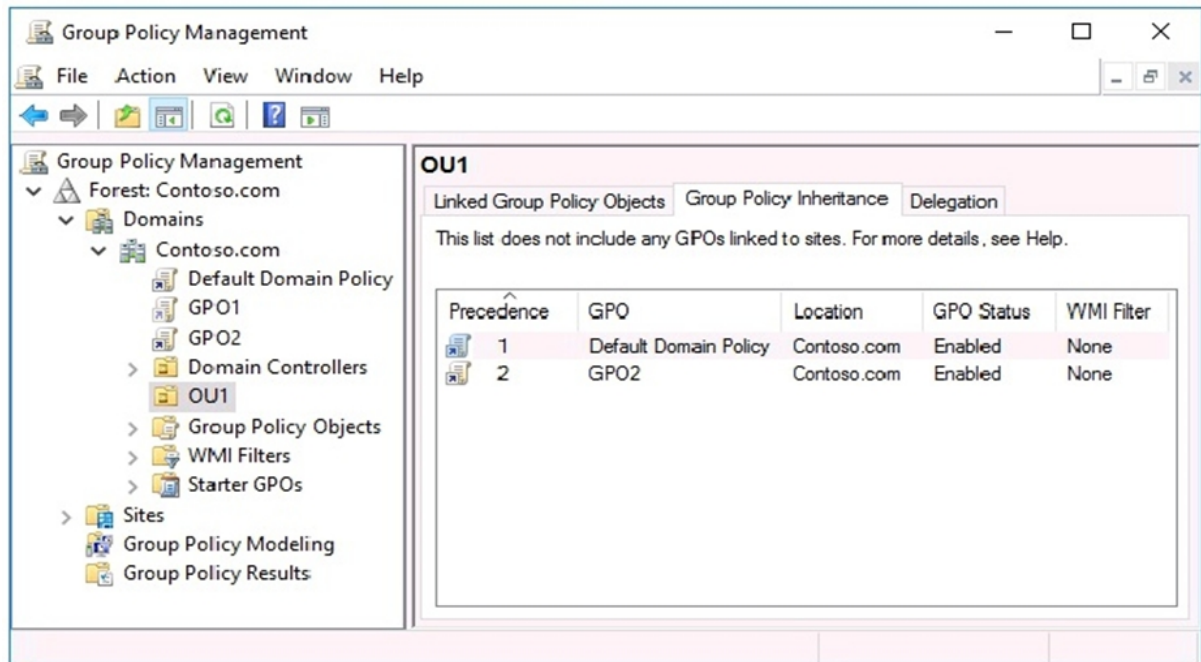
Explanation:

Explanation:

Question 157

Your network contains an Active Directory forest named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. The computer account of Server1 is an organizational unit (OU) named OU1.

You open Group Policy Management as shown in the exhibit. (Click the Exhibit button.)



An administrator reports that the settings from GPO1 are not applied to Server1.

You need to ensure that the settings from GPO1 are applied to Server1.

What should you do?

- ☒ Enable the link of GPO1
- ☐ Enforce GPO1
- ☐ Disable Block inheritance
- ☐ Remove the security filtering

Explanation:

Explanation:

If the GPO link is enabled, the settings of the GPO are applied when Group Policy is processed for the site, domain or OU.

References:

<https://docs.microsoft.com/en-us/powershell/module/grouppolicy/set-gplink?view=win10-ps>

Question 158

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You deploy a new Active Directory forest.

You need to ensure that you can create a group Managed Service Account (gMSA) for multiple member servers.

Solution: From Windows PowerShell on a domain controller, you run the Set-KdsConfiguration cmdlet.

Does this meet the goal?

- ☐ Yes
☒ No

Question 159**HOTSPOT**

Your company has a main office and a branch office. The two offices connect to each other by using a WAN link.

Your network contains an Active Directory forest named contoso.com. The forest contains a domain controller named DC1. All of the domain controllers are located in the main office.

You install a read-only domain controller (RODC) named RODC1 in the branch office.

You create a user account for a new user named User1. You add User1 to the Allowed RODC Password Replication Group. User1 starts work on Monday.

You are notified that the WAN link will be down for maintenance on Monday.

You need to ensure that User1 can log on in the branch office site on Monday.

Which command should you run? To answer, select the appropriate options in the answer area.

Answer Area

▼
clonepr
ldifde
repadmin
replmon

▼
/prp
/replicate
/rodcpwdrepl
/syncall

rodc1.fabrikam.com dc1.fabrikam.com "cn=user1,ou=users,dc=fabrikam,DC=com"

Solution:

Answer Area

▼
clonepr
ldifde
repadmin
replmon

▼
/prp
/replicate
/rodcpwdrepl
/syncall

rodc1.fabrikam.com dc1.fabrikam.com "cn=user1,ou=users,dc=fabrikam,DC=com"

Explanation:

Explanation:

The following example triggers replication of the passwords for the user account named JaneOh from the source domain controller named source-dc01 to all RODCs that have the name prefix dest-rodc:

```
repadmin /rodcpwdrepl dest-rodc* source-dc01 cn=JaneOh,ou=execs,dc=contoso,dc=com
```

References:

[https://technet.microsoft.com/en-us/library/cc742095\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc742095(v=ws.11).aspx)

Question 160

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory forest named contoso.com. The forest contains an Active Directory Rights Management Services (AD RMS) deployment.

Your company establishes a partnership with another company named Fabrikam, Inc. The network of Fabrikam contains an Active Directory forest named fabrikam.com and an AD RMS deployment.

You need to ensure that the users in contoso.com can access rights protected documents sent by the users in fabrikam.com.

Solution: From AD RMS in contoso.com, you configure fabrikam.com as a trusted user domain.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Contoso would need to be the Trusted User Domain.

References:

<https://books.google.co.za/books?id=gjR-BAAAQBAJ&pg=PA397&lpg=PA397&dq=configure+a+partners+forest+as+a+trusted+publishing+domain+-+AD+RMS&source=bl&ots=mohQXTyW9s&sig=NJ7oFHuLYOs72o9EM-yQilscUW8&hl=en&sa=X&ved=0ahUKEwjuiW24sPbAhWGRMAKHQcEB6EQ6AEIOzAD#v=onepage&q=configure%20a%20partners%20forest%20as%20a%20trusted%20publishing%20domain%20-%20AD%20RMS&f=false>

Question 161

HOTSPOT

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

You have a Central Store for Group Policy. You have a custom administrative template that contains the settings for an application named App1.

Administrators who use computers in French report that the App1 settings always appear in French for users who have French computers.

What should you do? To answer, select the appropriate option in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

File type to create:

ADM
ADML
ADMX

Copy file to:

\\adatum.com\netlogon\fr-fr\
\\adatum.com\sysvol\adatum.com\policies\PolicyDefinitions\fr-fr\
\\adatum.com\sysvol\adatum.com\staging\domain\fr-fr
C:\Windows\PolicyDefinitions\fr-fr\

Solution:

Answer Area

File type to create:

ADM
ADML
ADMX

Copy file to:

\\adatum.com\netlogon\fr-fr\
\\adatum.com\sysvol\adatum.com\policies\PolicyDefinitions\fr-fr\
\\adatum.com\sysvol\adatum.com\staging\domain\fr-fr
C:\Windows\PolicyDefinitions\fr-fr\

Explanation:

References:

<https://fileinfo.com/extension/adml>

<https://sourcedaddy.com/windows-7/local-storage-of-admx-template-files.html>

Question 162**HOTSPOT**

You network contains an Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

Name	Type	In organizational unit (OU)
Server1	Computer	OU1
User1	User	OU2
User2	User	OU3

The domain has the Group Policy objects (GPOs) shown in the following table.

Name	Linked to	Configuration
GPO1	OU1	- Startup script: Script1A - Shutdown script: Script1B - Logon script: Script1C - Logoff script: Script1D
GPO2	OU2	- Startup script: Script2A - Shutdown script: Script2B - Logon script: Script2C - Logoff script: Script2D
GPO3	OU3	- Startup script: Script3A - Shutdown script: Script3B - Logon script: Script3C - Logoff script: Script3D

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer area	Statements	Yes	No
	If User1 signs in to Server1, Script1C runs.	☐	☐
	If User2 signs in to Server1, Script4C runs.	☐	☐
	If User2 restarts Server1, Script1D runs.	☐	☐

Solution:

Answer area	Statements	Yes	No
	If User1 signs in to Server1, Script1C runs.	☐	☐
	If User2 signs in to Server1, Script4C runs.	☐	☐
	If User2 restarts Server1, Script1D runs.	☐	☐

Question 163

Your network contains an Active Directory forest. The forest functional level is Windows Server 2016. You have a failover cluster named Cluster1. Cluster1 has two nodes named Server1 and Server2. All the optional features in Active Directory are enabled.

A junior administrator accidentally deletes the computer object named Cluster1. You discover that Cluster1 is offline.

You need to restore the operation of Cluster1 in the least amount of time possible. What should you do?

- ☐ Run the Enable-ADAccount cmdlet from Windows PowerShell.
- ☐ Perform an authoritative restore by running ntdutil.exe.
- ☐ Perform a tombstone reanimation by running ldp.exe.
- ☒ Recover a deleted object from the Active Directory Recycle Bin.

Question 164

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a user named User1, a group named Group1, and an organizational unit (OU) named OU1.

You need to enable User1 to link Group Policies to OU1.

Solution: From Active Directory Administrative Center, you add User1 to Group1 and grant Group1 Full Control permissions to OU1.

Does this meet the goal?

- ☒ Yes
☐ No

Question 165

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

On Server1, you create a local user named User1. User1 is a member of the local Administrators group.

Server1 has the following local Group Policies:

Local Computer Policy

Local Computer\User1 Policy

Local Computer\Administrators Policy

You need to force User1 to change his password every 14 days.

Solution: You configure the Password Policy settings in a Group Policy object (GPO) that is linked to the Domain Controllers organizational unit (OU).

Does this meet the goal?

- ☐ Yes
☒ No

Question 166**HOTSPOT**

Your network contains an Active Directory forest. The forest contains one domain named contoso.com. The domain contains two domain controllers named DC1 and DC2. DC1 holds all of the operations master roles.

During normal network operations, you run the following commands on DC2:

```
Move-ADDirectoryServerOperationMasterRole -Identity "DC2" -OperationMasterRole PDCEmulator
Move- ADDirectoryServerOperationMasterRole –Identity "DC2" -OperationMasterRole RIDMaster
```

DC1 fails.

You remove DC1 from the network, and then you run the following command:

```
Move-ADDirectoryServerOperationMasterRole –Identity "DC2" -OperationMasterRole
SchemaMaster
```

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
DC2 holds the schema master operations role.	☐	☐
DC2 holds the PDC emulator master operations role.	☐	☐
Currently, you can add additional domains to the forest.	☐	☐

Solution:

Answer Area

Statements	Yes	No
DC2 holds the schema master operations role.	☐	☐
DC2 holds the PDC emulator master operations role.	☐	☐
Currently, you can add additional domains to the forest.	☐	☐

Question 167

HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2016.

Server1 has Microsoft System Center 2016 Virtual Machine Manager (VMM) installed. Server2 has IP Address Management (IPAM) installed.

You create a domain user named User1.

You need to integrate IPAM and VMM. VMM must use the account of User1 to manage IPAM. The solution must use the principle of least privilege.

What should you do on each server? To answer, select the appropriate options in the answer area.

Answer Area

On Server1:

	▼
Create a Run as Account that uses User1	
Add User1 to the Fabric Administrator user role	
Add User1 to the Remote Management Users group	

On Server2:

	▼
Add User1 to IPAM Administrator Role	
Add User1 to IPAM ASM Administrator Role	
Add User1 to IPAM MSM Administrator Role	

Solution:

Answer Area

On Server1:

	▼
Create a Run as Account that uses User1	
Add User1 to the Fabric Administrator user role	
Add User1 to the Remote Management Users group	

On Server2:

	▼
Add User1 to IPAM Administrator Role	
Add User1 to IPAM ASM Administrator Role	
Add User1 to IPAM MSM Administrator Role	

Explanation:

Explanation:

To enable IPAM and Virtual Machine Manager (VMM) integration, you must first configure a user account for VMM on the IPAM server and then configure the IPAM network service plugin in VMM.

VMM must be granted permission to view and modify IP address space in IPAM, and to perform remote management of the IPAM server. VMM uses a “Run As” account to provide these permissions to the IPAM network service plugin. The “Run As” account must be configured with appropriate permission on the IPAM server.

Any local or domain account can be used by VMM to access the IPAM server, but it is recommended to use a unique domain account that will only be used by VMM to connect to the IPAM server.

The minimum required permissions for this scenario is supplied by the IPAM ASM Administrator Role.

References:

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn783349\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn783349(v=ws.11))

Question 168

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

The domain contains a read-only domain controller (RODC) named RODC1.

You need to retrieve a list of accounts that have their password cached on RODC1.

Which command should you run?

- ☒ repadmin.exe
- ☐ ntdsutil.exe
- ☐ dcdiag.exe
- ☐ netdom.exe

Explanation:

Explanation:

To list the user and computer accounts for the passwords that are cached on the RODC, run the following command:

```
repadmin /prp view <read-only domain controller> reveal
```

References <https://support.microsoft.com/en-za/help/2028962/the-active-directory-users-and-computers-mmc-snap-in-does-not-list-all>

Question 169

You have a server named Server1 that has the Active Directory Federation Services server role installed.

You need to configure Server1 as the authorization server. Server1 will be used to authorize access to a web API from a web application. The web application will use OAuth 2.0 and OpenID Connect to access the web API as the authenticated user.

The solution must minimize administrative effort.

What should you do first?

- ☒ Run Add-AdfsServerApplication
- ☐ Run New-AdfsapplicationGroup
- ☐ Enable the OAuth endpoint
- ☐ Run Add-AdfsNativeClientApplication

Explanation:

References:

<https://docs.microsoft.com/en-us/powershell/module/adfs/add-adfsserverapplication?view=win10-ps>

Question 170

Your network contains an Active Directory domain named contoso.com.
The domain contains a user named User1 and an organizational unit (OU) named OU1.
You create a Group Policy object (GPO) named GPO1.

You need to ensure that User1 can link GPO1 to OU1.
What should you do?

- ☐ Modify the security settings of User1.
- ☐ Add User1 to the Group Policy Creator Owner group.
- ☒ Modify the security settings of OU1.
- ☐ Modify the security settings of GPO1.

Question 171

Your company recently deployed a new child domain to an Active Directory forest.

You discover that a user modified the Default Domain Policy to configure several Windows components in the child domain.

A company policy states that the Default Domain Policy must be used only to configure domain-wide security settings.

You create a new Group Policy object (GPO) and configure the settings for the Windows components in the new GPO.

You need to restore the Default Domain Policy to the default settings from when the domain was first installed.

What should you do?

- ☐ From Group Policy Management, click Starter GPOs, and then click Manage Backups.
- ☒ From a command prompt, run the dcgpofix.exe command.
- ☐ From Windows PowerShell, run the Copy-GPO cmdlet.
- ☐ Run ntdsutil.exe to perform a metadata cleanup and a semantic database analysis.

Explanation:

Explanation:

Question 172

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

You have an organizational unit (OU) named OU1 that contains the computer accounts from two servers and the user account of a user named User1. A Group Policy object (GPO) named GPO1 is linked to OU1.

You have an application named App1 that installs by using an application installer named App1.exe.

You need to publish App1 to OU1 by using Group Policy.

What should you do?

- ☐ Create a Config.zap file and add a file to the File System node to the Computer Configuration node of GPO1.
- ☐ Create a Config.xml file and add a software installation package to the User Configuration node of GPO1.
- ☒ Create a Config.zap file and add a software installation package to the User Configuration node of GPO1.
- ☐ Create a Config.xml file and add a software installation package to the Computer Configuration node of GPO1.

Explanation:

Explanation:

Question 173

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. All domain-joined computers have Fast Logon Optimization enabled.

You need to ensure that the next time a user signs in to Server1, the user-targeted Group Policy objects (GPOs) are processed fully before the user gains access to the desktop.

What should you run on Server?

- ☐ Invoke-Gpupdate with the –Logoff switch
- ☐ Invoke-Gpupdate with the –Boot switch
- ☐ gpupdate with the /force switch
- ☒ Invoke-Gpupdate with the –Sync switch

Explanation:

References:

<https://docs.microsoft.com/en-us/powershell/module/grouppolicy/invoke-gpupdate?view=win10-ps>

Question 174

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario

You work for a company named Contoso, Ltd.

The network contains an Active Directory forest named contoso.com. A forest trust exists between contoso.com and an Active Directory forest named adatum.com.

The contoso.com forest contains the objects configured as shown in the following table.

Object name	Object type	Group scope	Group type
User1	User	<i>Not applicable</i>	<i>Not applicable</i>
User2	User	<i>Not applicable</i>	<i>Not applicable</i>
Computer1	Computer	<i>Not applicable</i>	<i>Not applicable</i>
Group1	Group	Domain local	Security
Group2	Group	Domain local	Security
Group3	Group	Universal	Security
Group4	Group	Global	Security
Group5	Group	Universal	Security

Group1 and Group2 contain only user accounts.

Contoso hires a new remote user named User3. User3 will work from home and will use a computer named Computer3 that runs Windows 10. Computer3 is currently in a workgroup.

An administrator named Admin1 is a member of the Domain Admins group in the contoso.com domain.

From Active Directory Users and Computers, you create an organizational unit (OU) named OU1 in the contoso.com domain, and then you create a contact named Contact1 in OU1.

An administrator of the adatum.com domain runs the Set-ADUser cmdlet to configure a user named User1 to have a user logon name of User1@litwareinc.com.

End of repeated scenario

Admin1 attempts to delete OU1 and receives an error message.

You need to ensure that Admin1 can delete OU1.

What should you do first?

- ☒ Modify the Object settings for OU1

- ☐ Add Admin1 to the Enterprise Admins group
- ☐ Delete Contact1
- ☐ Disable the Active Directory Recycle Bin

Explanation:

References:

<https://www.dtonias.com/access-denied-delete-move-ou-active-directory/>

Question 175

HOTSPOT

Your network contains an Active Directory forest named contoso.com. The forest contains an Active Directory Federation Services (AD FS) farm. You install Windows Server 2016 on a server named Server2.

You need to configure Server2 as a node in the federation server farm. Which cmdlets should you run? To answer, select the appropriate options in the answer area.

Answer Area

First cmdlet to run

	▼
Install-AdfsFarm	
Install-Package	
Install-WindowsFeature	

Second cmdlet to run

	▼
Install-AdfsFarm	
New-AdfsOrganization	
Set-AdfsFarmInformation	
Set-AdfsProperties	

Answer Area

First cmdlet to run

▼
Install-AdfsFarm
Install-Package
Install-WindowsFeature

Second cmdlet to run

▼
Install-AdfsFarm
New-AdfsOrganization
Set-AdfsFarmInformation
Set-AdfsProperties

Solution:**Question 176**

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains two domain controllers named DC1 and DC2.

DC1 holds the RID master operations role. DC1 fails and cannot be repaired. You need to move the RID role to DC2.

Solution: On DC2, you open the command prompt, run ntdsutil.exe, connect to DC2, and use the Transfer RID master option.

Does this meet the goal?

- ☒ Yes
☐ No

Explanation:

Explanation:

There are 2 ways of transferring FSMO roles. You can do that using graphical consoles available on a DC or any server/workstation with Administrative Tools / Remote Server Administration Tools installed or using command-line tool called ntdsutil.

First of all you need to connect to Domain Controller to which you want to transfer FSMO roles. To do that you have to type:

```
ntdsutil: roles (enter)
```

```
fsmo maintenance: connections (enter)
```

```
server connections: connect to server <DC-Name> (enter)
```

```
server connections: quit (enter)
```

```
fsmo maintenance:
```

Now you will be able to transfer FSMO roles to selected Domain Controller.

RID master

```
fsmo maintenance: transfer RID master (enter)
```

Click “Yes” button to move role.

References: <http://kpytko.pl/active-directory-domain-services/transferring-fsmo-roles-from-command-line/>

Question 177

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

You have an organizational unit (OU) named TestOU that contains test computers.

You need to enable a technician named Tech1 to create Group Policy objects (GPOs) and to link the GPOs to TestOU. The solution must use the principle of least privilege.

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

- ☒ Add Tech1 to the Group Policy Creator Owners group.
- ☒ From Group Policy Management, modify the Delegation settings of the TestOU OU.
- ☐ Add Tech1 to the Protected Users group.
- ☐ From Group Policy Management, modify the Delegation settings of the contoso.com container.
- ☐ Create a new universal security group and add Tech1 to the group.

Explanation:

Explanation:

The Group Policy Creator Owners group lets its members create new GPOs.

You can delegate the ability for users to be given the ability to link GPOs to an OU or domain via the Delegation tab of the OU/domain/site within the GPMC.

References:

<http://www.itprotoday.com/management-mobility/what-group-policy-creator-owners-group>
<http://www.itprotoday.com/management-mobility/how-do-i-delegate-permissions-someone-edit-gpo>

Question 178

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains two domain controllers named DC1 and DC2.

DC1 holds the RID master operations role. DC1 fails and cannot be repaired. You need to move the RID role to DC2.

Solution: On DC2, you open the command prompt, run dsmgmt.exe, connect to DC2, and use the Seize RID master opinion.

Does this meet the goal?

- ☐ Yes
☒ No

Question 179

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

A user named User1 is in an organizational unit (OU) named OU1.

You are troubleshooting a folder access issue for User1.

You need a list of groups to which User1 is either a direct member or an indirect member.

Solution: You run `Get-ADGroup -Identity User1 -Property MemberOf`.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Explanation:

The `Get-ADGroup` cmdlet does not include the `MemberOf` property. The command above is, therefore, not valid.

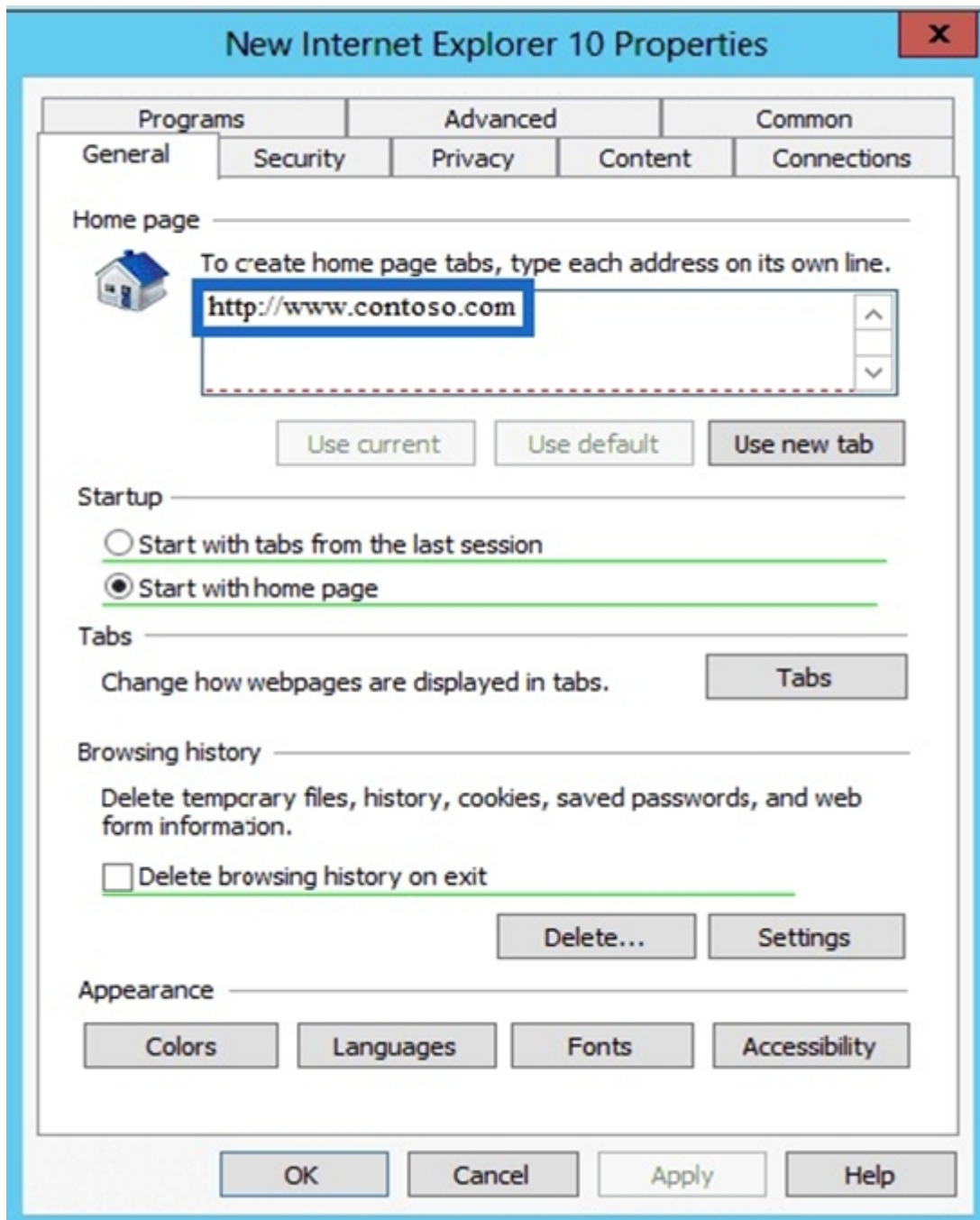
References: <https://docs.microsoft.com/en-us/powershell/module/addsadministration/get-adgroup?view=win10-ps>

Question 180

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

The domain contains a Group Policy object (GPO) named GPO1.

You configure the Internet Settings preference in GPO1 as shown in the exhibit. (Click the Exhibit button.)



A user reports that the homepage of Internet Explorer is not set to http://www.contoso.com.

You confirm that the other settings in GPO1 are applied.

You need to configure GPO1 to set the Internet Explorer homepage.

What should you do?

- ☒ Edit the GPO1 preference and press F5.
- ☐ Modify Security Settings for GPO1.
- ☐ Modify WMI Filtering for GPO1.
- ☐ Modify the GPO1 preference to use item-level targeting.

Explanation:

Explanation:

The red dotted line under the homepage URL means that setting is disabled. Pressing F5 enables all settings.

References: <https://community.spiceworks.com/topic/285312-add-default-website-in-group-policy>

Question 181

Your company has multiple branch offices.

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

In one of the branch offices, a new technician is hired to add computers to the domain.

After successfully joining multiple computers to the domain, the technician fails to join any more computers to the domain.

You need to ensure that the technician can join an unlimited number of computers to the domain.

What should you do?

- ☐ Configure the technician's user account as a manager service account.
- ☐ Run the Set-ADComputer cmdlet.
- ☒ Modify the Security settings of the Computers container.
- ☐ Add the technician to the Domain Computers group.
- ☐ Modify the Security settings of the technician's user account.
- ☐ Run the redircmp.exe command.
- ☐ Add the technician to the Windows Authorization Access Group group.

Explanation:

Explanation:

Users who have the Create Account Objects privilege for the Computers container can create an unlimited number of computer accounts in the domain. You can grant this privilege by accessing the

Advanced Security settings on the Security Tab of the Computer container via Active Directory Users And Computers or the Active Directory Administrative Center.

References:

https://books.google.co.za/books?id=LvNODQAAQBAJ&pg=PT268&lpg=PT268&dq=Modify+the+Security+settings+of+the+Computers+container+2016&source=bl&ots=1IRBQ21cL0&sig=1AUSon_6cJlqyN_927iOB7z3-Eg&hl=en&sa=X&ved=0ahUKEwjBi4OS-rnbAhXKD8AKHerKDcgQ6AEISjAC#v=onepage&q=Modify%20the%20Security%20settings%20of%20the%20Computers%20container%202016&f=false

Question 182

Your network contains an Active Directory domain named contoso.com. The domain contains servers that run Windows Server 2016. The servers are configured as shown in the following table:

Name	Configuration
DC1	Domain controller, DNS server
DC2	Domain controller, DNS server
CA1	Enterprise certification authority (CA)
CA2	<i>None</i>

You have a research department. The computers in the research department are not domain-joined.

You need to ensure that the research department computers can use automatic certificate enrollment to receive and renew certificates from the CA.

Which two role services should you install and configure on CA1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- ☒ Certificate Enrollment Policy Web Service
- ☒ Certificate Authority Web Enrollment
- ☐ Online Responder
- ☐ Certificate Enrollment Web Service
- ☐ Network Device Enrollment Service

Explanation:

References:

https://www.ejbca.org/docs/Part_2__Microsoft_Certification_Authority_and_Group_Policies.html

Question 183

Your network contains an Active Directory domain. The domain contains the servers shown in the following table.

Name	Configuration
DC1	Domain controller
DC2	Domain controller
ADFS1	Active Directory Federation Services (AD FS)
ADFS2	Active Directory Federation Services (AD FS), Internet Information Services (IIS)
Exch1	Microsoft Exchange Server 2016 Mailbox server
WebServer1	Internet Information Services (IIS)

You have a server named WebServer2 in a workgroup. WebServer2 has the Web Server (IIS) server role installed. You plan to deploy a Web Application Proxy to provide preauthentication for HTTP Basic application publishing to allow users to connect to mailboxes by using Exchange ActiveSync.

You need to install the Web Application Proxy role service. The solution must minimize the attack surface.

On which server should you install the role service?

- ☒ WebServer2
- ☐ WebServer1
- ☐ ADFS1
- ☐ ADFS2

Explanation:

References:

<https://www.techsupportpk.com/2016/12/deploy-web-application-proxy-windows-server-2016.html>

<https://docs.microsoft.com/en-us/sharepoint/hybrid/configure-web-application-proxy-for-a-hybrid-environment>

<https://docs.microsoft.com/en-us/windows-server/storage/work-folders/deploy-work-folders-adfs-step4>

Question 184

DRAG DROP

Your network contains an Active Directory domain named contoso.com.
 The domain contains a server named Server1 that runs Windows Server 2016.
 You install IP Address Management (IPAM) on Server1.

You need to manually start discovery of servers that IPAM can manage in contoso.com.
 Which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.

Actions		Answer Area
Start-ScheduledTask		
Invoke-IpamServerProvisioning	⬅	⬆
Update-IpamServer	➡	⬇
Add-IpamSubnet		
Add-IpamAddress		
Add-IpamDiscoveryDomain		

Solution:

Actions		Answer Area
Start-ScheduledTask		Invoke-IpamServerProvisioning
Invoke-IpamServerProvisioning	⬅	Add-IpamDiscoveryDomain
Update-IpamServer	➡	Start-ScheduledTask
Add-IpamSubnet		
Add-IpamAddress		
Add-IpamDiscoveryDomain		

Explanation:

Explanation:

Step 1: Invoke-IpamServerProvisioning

Choose a provisioning method

The Invoke-IpamGpoProvisioning cmdlet creates and links three group policies specified in the Domain parameter for provisioningrequired access settings on the server roles managed by the computer running the IP Address Management (IPAM) server.

Step 2: Add-IpamDiscoveryDomain

Configure the scope of discovery

The Add-IpamDiscoveryDomain cmdlet adds an Active Directory discovery domain for an IP AddressManagement (IPAM) server. A discovery domain is a domain that IPAM searches to find infrastructure servers. An IPAM server uses the list of discovery domains to determine what type of servers to add. By default, IPAM discovers all domain controllers, Dynamic Host Configuration Protocol (DHCP) servers, and Domain Name System (DNS) servers.

Step 3: Start-ScheduledTask

Start server discovery

To begin discovering servers on the network, click Start server discovery to launch the IPAM ServerDiscovery task or use the Start-ScheduledTask command.

Question 185

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

You have an application named App1 that is deployed to all the client computers in the domain. App1 writes a registry value named LocalStorage on all the client computers.

You need to delete the LocalStorage registry value from all the client computers in the domain that have less than 100 GB of free disk space on their system volume.

What should you do?

- ☐ Configure Software Settings in a Group Policy object (GPO) and enable a WMI filter.
- ☐ Configure a Group Policy setting to modify the security of the LocalStorage registry value.
- ☐ Create an administrative template file that contains the LocalStorage registry setting, and then add the administrative template to a Group Policy object (GPO).
- ☒ Configure a Group Policy preference that uses item-level targeting.

Explanation:

Explanation:

In Windows Server 2008 Microsoft introduced a Group Policy extension, named Group Policy Preferences (GPP). GPP that includes registry settings, allows you to add, remove or modify key values.

References: <https://theitbros.com/add-modify-and-delete-registry-keys-using-group-policy/>

Question 186

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a user named User1, a group named Group1, and an organizational unit (OU) named OU1.

You need to enable User1 to link Group Policies to OU1.

Solution: From Active Directory Administrative Center, you add User1 to Group1. From ADSI Edit, you grant Group1 Full Control permissions to the "CN=Policies, CN=System, DC=Contoso, DC=com" object.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 187

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

All users are in an organizational unit (OU) named Corp_Users.

You plan to modify the description of all the users who have a string of 514 in their mobile phone number.

You need to view a list of the users that will be modified.

What should you run?

- ☐ Get-ADOrganizationalUnit-Filter "mobilePhone-Like '*514*' "
- ☐ Get-ADUser-LDAPFilter "(mobilePhone= '*514*')"
- ☒ Get-ADUser-Filter "mobilePhone-Like '*514*' "
- ☐ Get-ADOrganizationalUnit-LDAPFilter "(mobilePhone= '*514*')"

Question 188

Your company has two offices. The offices are located in Montreal and Seattle. The network contains an Active Directory forest named contoso.com.

The forest contains three domain controllers configured as shown in the following table.

Server name	Active Directory site
Server1	Montreal
Server2	Montreal
Server3	Seattle

The company physically relocates Server2 from the Montreal office to the Seattle office.

You discover that both Server1 and Server2 authenticate users who sign in to the client computers in the Montreal office. Only Server3 authenticates users who sign in to the computers in the Seattle office.

You need to ensure that Server2 authenticates the users in the Seattle office during normal network operations.

What should you do?

- ☐ From Windows PowerShell, run the Set-ADReplicationSite cmdlet.
- ☐ From Active Directory Users and Computers, modify the Location Property of Server2.
- ☐ From Network Connections on Server2, modify the Internet Protocol Version 4 (TCP/IPv4) configuration.
- ☒ From Windows PowerShell, run the Move-ADDirectoryServer cmdlet.

Question 189

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario

You work for a company named Contoso, Ltd.

The network contains an Active Directory forest named contoso.com. A forest trust exists between contoso.com and an Active Directory forest named adatum.com.

The contoso.com forest contains the objects configured as shown in the following table.

Object name	Object type	Group scope	Group type
User1	User	<i>Not applicable</i>	<i>Not applicable</i>
User2	User	<i>Not applicable</i>	<i>Not applicable</i>
Computer1	Computer	<i>Not applicable</i>	<i>Not applicable</i>
Group1	Group	Domain local	Security
Group2	Group	Domain local	Security
Group3	Group	Universal	Security
Group4	Group	Global	Security
Group5	Group	Universal	Security

Group1 and Group2 contain only user accounts.

Contoso hires a new remote user named User3. User3 will work from home and will use a computer named Computer3 that runs Windows 10. Computer3 is currently in a workgroup.

An administrator named Admin1 is a member of the Domain Admins group in the contoso.com domain.

From Active Directory Users and Computers, you create an organizational unit (OU) named OU1 in the contoso.com domain, and then you create a contact named Contact1 in OU1.

An administrator of the adatum.com domain runs the Set-ADUser cmdlet to configure a user named User1 to have a user logon name of User1@litwareinc.com.

End of repeated scenario

You need to ensure that Admin1 can convert Group1 to a global group.

What should you do?

- ☐ Add Admin1 to the Enterprise Admins group.
- ☒ Remove all the members from Group1.
- ☐ Modify the Security settings of Group1.
- ☐ Convert Group1 to a universal security group.

Question 190

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains an Active Directory forest named contoso.com. The forest functional level is Windows Server 2012 R2.

You need to ensure that a domain administrator can recover a deleted Active Directory object quickly.

Which tool should you use?

- ☐ Dsadd quota
- ☐ Dsmmod
- ☒ Active Directory Administrative Center
- ☐ Dsacis
- ☐ Dsadmin
- ☐ Active Directory Users and Computers
- ☐ Ntdsutil
- ☐ Group Policy Management Console

Explanation:

Explanation:

You can restore objects from the Active Directory Recycle Bin by using Active Directory Administrative Center.

References: <https://blogs.technet.microsoft.com/canitpro/2014/07/28/step-by-step-restoring-a-deleted-object-via-active-directory-recycle-bin/>

Question 191**HOTSPOT**

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

The domain contains the computers configured as shown in the following table.

Name	IP address	Free space on volume C
Client1	172.16.0.5	150 GB
Client2	172.16.0.25	50 GB
Client3	172.16.0.95	200 GB

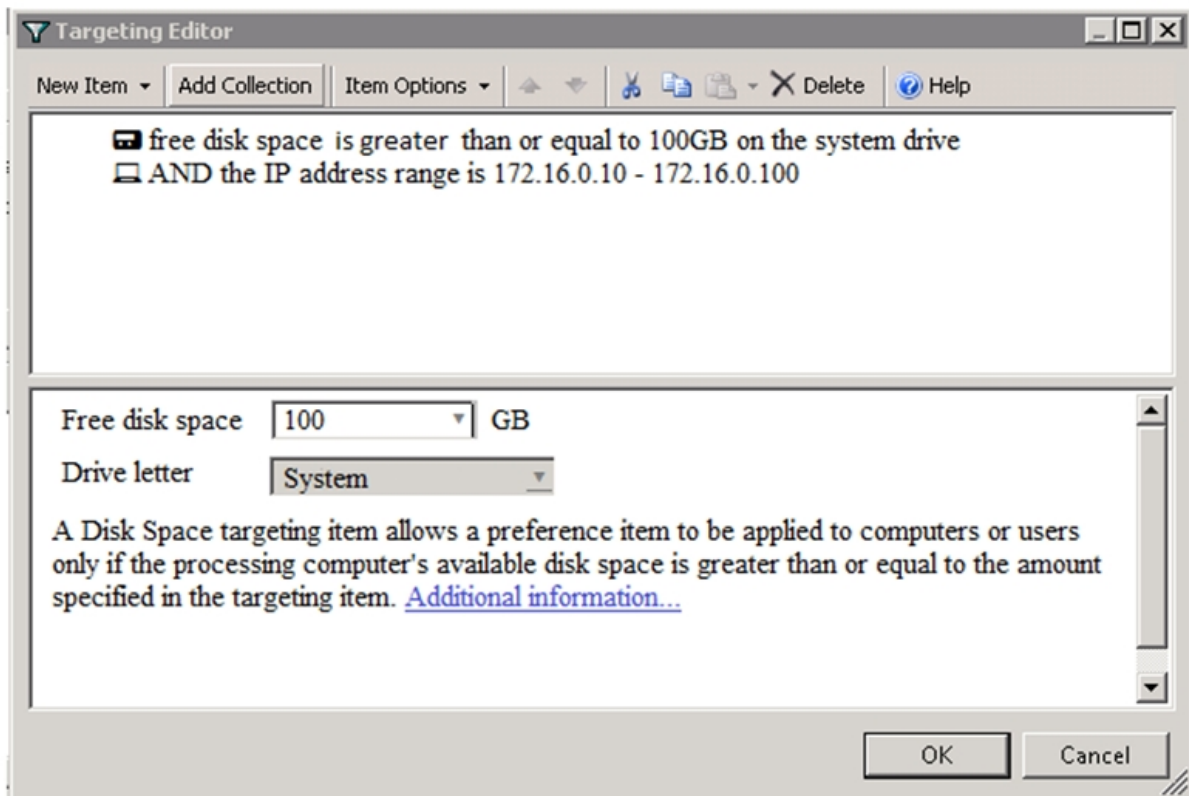
The domain contains a user named User1.

A Group Policy object (GPO) named GPO1 is linked to the domain. GPO1 contains a user preference that is configured as shown in the Shortcut1 Properties exhibit.

The screenshot shows the 'Shortcut1 Properties' dialog box with the 'General' tab selected. The 'Common' sub-tab is also visible. The 'Action' dropdown is set to 'Update'. The 'Name' field is 'Shortcut1'. The 'Target type' is 'File System Object'. The 'Location' is 'Desktop'. The 'Target path' is 'C:\Windows\System32\notepad.exe'. The 'Arguments' field is empty. The 'Start in' field is empty. The 'Shortcut key' is 'None'. The 'Run' dropdown is set to 'Formal Window'. The 'Comment' field is empty. The 'Icon file path' field is empty. The 'Icon index' is '0'. At the bottom are buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

Shortcut1 Properties	
General	
Common	
Action:	Update
Name:	Shortcut1
Target type:	File System Object
Location:	Desktop
Target path:	C:\Windows\System32\notepad.exe
Arguments:	
Start in:	
Shortcut key:	None
Run:	Formal Window
Comment:	
Icon file path:	
Icon index:	0
OK Cancel Apply Help	

Item-level targeting for the user preference is configured as shown in the Targeting exhibit. (Click the Exhibit button.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If User1 signs in to Client1, Shortcut1 will appear on the desktop.	☐	☐
If User1 signs in to Client2, Shortcut1 will appear on the desktop.	☐	☐
If User1 signs in to Client3, Shortcut1 will appear on the desktop.	☐	☐

Solution:

Answer Area

Statements	Yes	No
If User1 signs in to Client1, Shortcut1 will appear on the desktop.	☒	☐
If User1 signs in to Client2, Shortcut1 will appear on the desktop.	☐	☒
If User1 signs in to Client3, Shortcut1 will appear on the desktop.	☐	☒

Explanation:

References: <https://www.dell.com/support/article/za/en/zabsdt1/sln285439/windows-server-using-item-level-targeting-with-group-policy-preferences?lang=en>

Question 192

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains an Active Directory domain named contoso.com.
You recently deleted 5,000 objects from the Active Directory database.

You need to reduce the amount of disk space used to store the Active Directory database on a domain controller.

Which tool should you use?

- ☐ Dsadd quota
- ☐ Dsmmod
- ☐ Active Directory Administrative Center
- ☐ Dsacis
- ☐ Dsadmin
- ☐ Active Directory Users and Computers
- ☒ Ntdsutil
- ☐ Group Policy Management Console

Question 193

Your network contains an Active Directory forest named contoso.com. The forest contains an enterprise root certification authority (CA) on a server that runs Windows Server 2016.

You plan to create and issue a custom subordinate CA template.

You need to prevent subordinate CAs from issuing subordinate certificates.

What should you configure in the template?

- ☐ The Cryptography settings
- ☐ The Request Handling settings
- ☒ The Basic Constraints extension
- ☐ The Security settings

Question 194

Your network contains an Active Directory forest. The forest contains a forest root domain named contoso.com and a child domain named eu.contoso.com. Each domain contains two domain controllers that run Windows Server 2012 R2.

The forest functional level is Windows Server 2008 R2. The domain functional level of contoso.com is Windows Server 2012 R2. The domain functional level of eu.contoso.com is Windows Server 2008 R2.

You need to raise the domain functional level of contoso.com to Windows Server 2016. The solution must minimize administrative effort.

What should you do before you raise the domain functional level?

- ☐ Raise the forest functional level
- ☐ Upgrade all of the domain controllers in the forest
- ☒ Upgrade all of the domain controllers in contoso.com
- ☐ Raise the domain functional level of eu.contoso.com

Explanation:

References:

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels>

Question 195

HOTSPOT

Your network contains an Active Directory domain named contoso.com.
The domain contains a member server named Server1 that runs Windows Server 2016.
Server1 has IP Address Management (IPAM) installed. IPAM uses a Windows Internal Database.
You install Microsoft SQL Server on Server1.
You plan to move the IPAM database to SQL Server.

You need to create a SQL Server login for the IPAM service account.
For which user should you create the login? To answer, select the appropriate options in the answer area.

Answer Area

	▼
CONTOSO\	
NT AUTHORITY\	
NT SERVICE	
SERVER1\	

	▼
LOCAL SERVICE	
LOCAL SYSTEM	
NETWORK SERVICE	

Solution:**Answer Area**

	▼
CONTOSO\	
NT AUTHORITY\	
NT SERVICE	
SERVER1\	

	▼
LOCAL SERVICE	
LOCAL SYSTEM	
NETWORK SERVICE	

Question 196

HOTSPOT

Your network contains an Active Directory forest named contoso.com. The forest contains the root domain and two child domains named child1.contoso.com and child2.contoso.com. Child1 contains three domain controllers named DC1, DC2, and DC3. Child2 contains one domain controller named DC4.

You have two accounts named Child1\Admin1 and Child2\Admin2 that you use to perform administrative tasks. Currently, the accounts can manage only the member servers in their respective domain.

You plan to demote DC3 and to remove the Child2 domain.

You need to ensure that Admin1 can demote DC3 and that Admin2 can demote DC4. The solution must use the principle of least privilege.

To which groups should you add Admin1 and Admin2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Admin1:

	▼
Child1\Domain Admins	
Child1\Server Operators	
Contoso\Domain Admins	
Contoso\Enterprise Admins	
Contoso\Schema Admins	

Admin2:

	▼
Child2\Domain Admins	
Child2\Server Operators	
Contoso\Domain Admins	
Contoso\Enterprise Admins	
Contoso\Schema Admins	

Answer Area

Admin1:

	▼
Child1\Domain Admins	
Child1\Server Operators	
Contoso\Domain Admins	
Contoso\Enterprise Admins	
Contoso\Schema Admins	

Admin2:

	▼
Child2\Domain Admins	
Child2\Server Operators	
Contoso\Domain Admins	
Contoso\Enterprise Admins	
Contoso\Schema Admins	

Solution:

Explanation:

References:

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/demoting-domain-controllers-and-domains--level-200->

Question 197

Your network contains an Active Directory forest named contoso.com

Your company plans to hire 500 temporary employees for a project that will last 90 days.

You create a new user account for each employee. An organizational unit (OU) named Temp contains the user accounts for the employees.

You need to prevent the new users from accessing any of the resources in the domain after 90 days.

What should you do?

- ☒ Run the Get-ADUser cmdlet and pipe the output to the Set-ADUser cmdlet.
- ☐ Create a group that contains all of the users in the Temp OU. Create a Password Setting object (PSO) for the new group.
- ☐ Create a Group Policy object (GPO) and link the GPO to the Temp OU. Modify the Password Policy settings of the GPO.
- ☐ Run the GET-ADOrganizationalUnit cmdlet and pipe the output to the Set-Date cmdlet.

Explanation:

Explanation:

Question 198

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. All the accounts of the users in the sales department are in an organizational unit (OU) named SalesOU.

An application named App1 is deployed to the user accounts in SalesOU by using a Group Policy object (GPO) named Sales GPO.

You need to set the registry value of \HKEY_CURRENT_USER\Software\App1\Collaboration to 0.

Solution: You add a computer preference that has a Replace action.

Does this meet the goal?

- ☒ Yes
- ☐ No

Question 199

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series.

Information and details provided in a question apply only to that question.

Your network contains an Active Directory domain named contoso.com. The domain contains 5,000 user accounts.

You have a Group Policy object (GPO) named DomainPolicy that is linked to the domain and a GPO named DCPolicy that is linked to the Domain Controllers organizational unit (OU).

You need to use the application control policy settings to prevent several applications from running on the network.

What should you do?

- ☐ From the Computer Configuration node of DCPolicy, modify Security Settings.
- ☒ From the Computer Configuration node of DomainPolicy, modify Security Settings.
- ☐ From the Computer Configuration node of DomainPolicy, modify Administrative Templates.
- ☐ From the User Configuration node of DCPolicy, modify Security Settings.
- ☐ From the User Configuration node of DomainPolicy, modify Folder Redirection.
- ☐ From user Configuration node of DomainPolicy, modify Administrative Templates.
- ☐ From Preferences in the User Configuration node of DomainPolicy, modify Windows Settings.
- ☐ From Preferences in the Computer Configuration node of DomainPolicy, modify Windows Settings.

Explanation:

Explanation:

Question 200

Your network contains an Active Directory domain.

Users do not have administrative privileges to their client computer.

You modify a computer setting in a Group Policy object (GPO).

You need to ensure that the setting is applied to five client computers as soon as possible.

What should you do?

- ☐ From each client computer, run the gpresult.exe command and specify the /r parameter.
- ☐ From a domain controller, run the gpupdate.exe command and specify the Force parameter.
- ☒ From a domain controller, run the Invoke-GPUUpdate cmdlet.
- ☐ From each client, run the Get-Gpo cmdlet and specify the –all parameter.

Question 201

Your network contains an Active Directory forest.

Some users report experiencing difficulties signing in to domain controllers. You suspect that the service location (SRV) records might be causing the issue.

What are two possible commands that you can run to verify the SRV records? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- ☐ dnscmd /DirectoryPartitionInfo
- ☐ dcdiag.exe /test:DNS
- ☒ dcdiag.exe /test:connectivity
- ☐ dnscmd /IpValidate
- ☒ dcdiag.exe /test:DnsRecordRegistration
- ☐ dnscmd /info

Question 202

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

You deploy a standalone root certification authority (CA) named CA1.

You need to autoenroll domain computers for certificates by using a custom certificate template.

What should you do first?

- ☐ Modify the Policy Module for CA1.
- ☐ Modify the Exit Module for CA1.
- ☐ Install a standalone subordinate CA.
- ☒ Install an enterprise subordinate CA.

Explanation:

Explanation:

You can't create templates or configure auto-enrollment on a standalone CA.

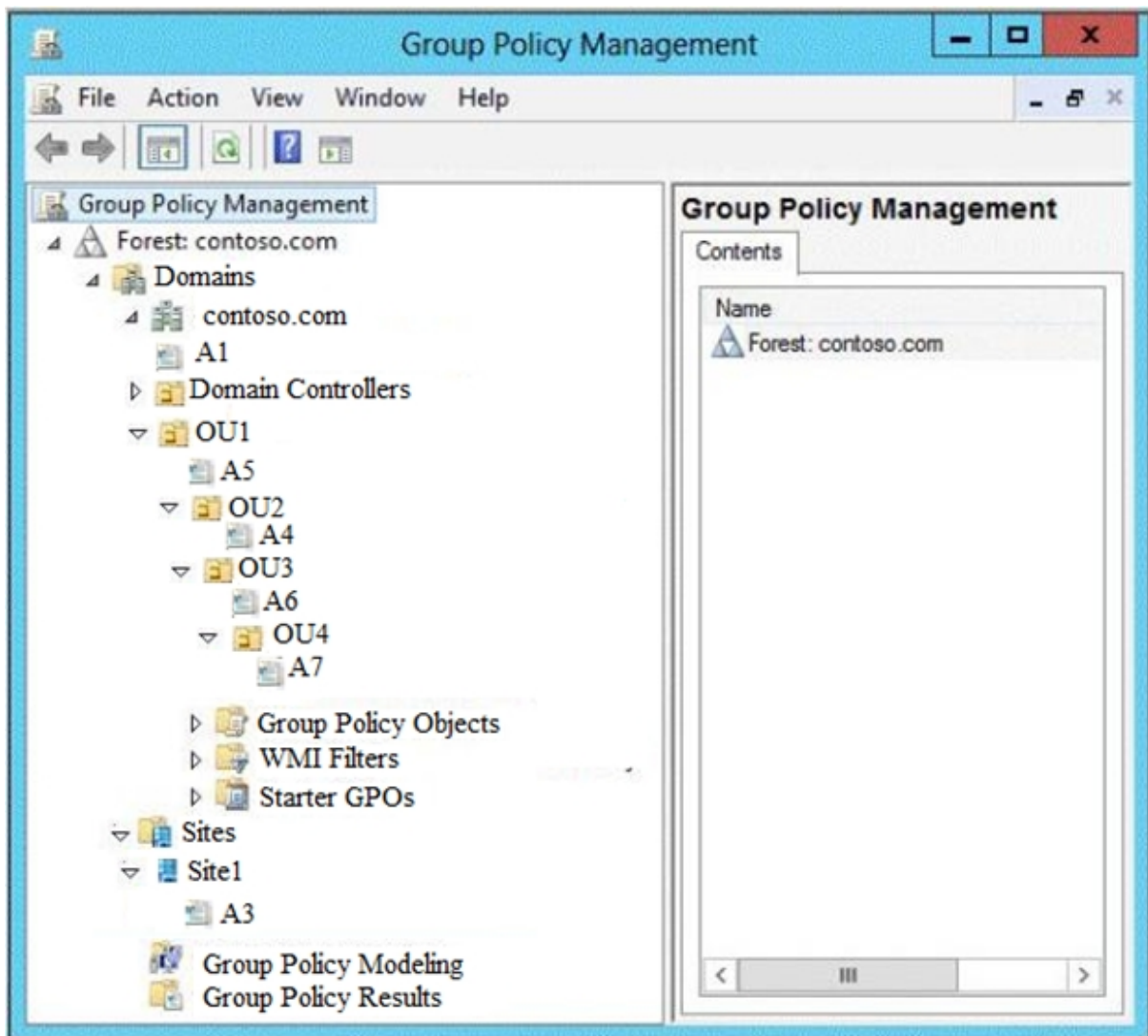
Question 203

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario.

Your network contains an Active Directory domain named contoso.com. The domain contains a single site named Site1. All computers are in Site1.

The Group Policy objects (GPOs) for the domain are configured as shown in the exhibit. (Click the Exhibit button.)



The relevant users and client computer in the domain are configured as shown in the following table.

Object name	Object type	Object location
Computer	Computer	OU4
User1	User	OU4
User2	User	OU2

End of repeated scenario.

You are evaluating what will occur when you set user Group Policy loopback processing mode to Replace in A7.

Which GPO or GPOs will apply to User2 when the user signs in to Computer1 after loopback processing is configured?

- ☐ A1 and A7 only
- ☐ A3, A1, A5, A6 and A7
- ☐ A3, A5, A1, and A7 only
- ☒ A7 only

Explanation:

Explanation:

In Replace Mode, the user's list of GPOs is not gathered. Only the list of GPOs based on the computer object is used.

References: <https://support.microsoft.com/en-us/help/231287/loopback-processing-of-group-policy>

Question 204

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

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

You need to limit the number of Active Directory Domain Services (AD DS) objects that a user can create in the domain.

Which tool should you use?

- ☒ Dsadd quota
- ☐ Dsmmod
- ☐ Active Directory Administrative Center
- ☐ Dsacis
- ☐ Dsamain
- ☐ Active Directory Users and Computers
- ☐ Ntdsutil
- ☐ Group Policy Management Console

Explanation:

Explanation:

Dsadd quota adds a quota specification to a directory partition. A quota specification determines the maximum number of directory objects that a given security principal can own in a specified directory partition.

References:

<https://blogs.technet.microsoft.com/activedirectoryua/2009/03/19/active-directory-quotas/>

Question 205

HOTSPOT

Your network contains an Active Directory domain named contoso.com. The relevant objects in the domain are configured as shown in the following table.

Object name	Type
Server1	Member server
OU1	Organizational unit (OU)
OU2	Organizational unit (OU)
GPO1	Group Policy object (GPO)
User1	User account
User2	User account
Group1	Global group
Group2	Global group
Group3	Global group

You have the following configurations:

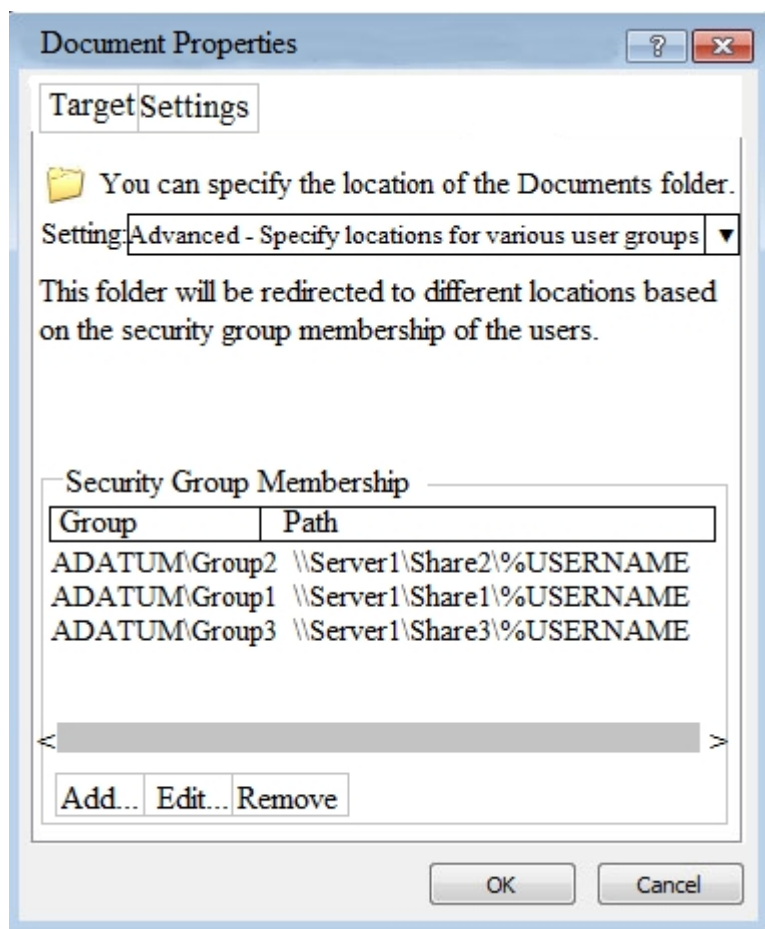
User1 is in OU1 and is a member of Group1 and Group2

User2 is in OU2 and is a member of Group1 and Group3

GPO1 is linked to OU1.

Server1 has three shares named Share1, Share2, and Share3. The Domain Users group permissions to all three shares.

GPO1 is configured as shown in the exhibit. (Click the Exhibit button.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
When User1 signs in to Server1, the user's Documents folder will be redirected to \\Server1\Share1.	☐	☐
If you add User1 to Group3, and then User1 signs in to Server1, the user's Documents folder will be redirected to \\Server1\Share3.	☐	☐
When User2 signs in to Server1, the user's Documents folder will be redirected to \\Server1\Share1	☐	☐

Solution:

Answer Area

Statements	Yes	No
When User1 signs in to Server1, the user's Documents folder will be redirected to \\Server1\Share1.	☒	☐
If you add User1 to Group3, and then User1 signs in to Server1, the user's Documents folder will be redirected to \\Server1\Share3.	☐	☐
When User2 signs in to Server1, the user's Documents folder will be redirected to \\Server1\Share1	☐	☐

Question 206

You deploy a new certification authority (CA) to a server that runs Windows Server 2016.

You need to configure the CA to support recovery of certificates.

What should you do first?

- ☐ Assign the Request Certificates permission to the user account that will be responsible for recovering certificates.
- ☒ Configure the Key Recovery Agent template as a certificate template to issue.
- ☐ Modify the Recovery Agents settings from the properties of the CA.
- ☐ Modify the extension of the OCSP Response Signing template.

Explanation:

References:

<http://markgossa.blogspot.co.uk/2017/03/enable-key-archival-in-server-2012-r2.html>

Question 207

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

On Server1, you create a local user named User1. User1 is a member of the local Administrators group.

Server1 has the following local Group Policies:

Local Computer Policy

Local Computer\User1 Policy

Local Computer\Administrators Policy

You need to force User1 to change his password every 14 days.

Solution: You create a Password Setting object (PSO) in the domain.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 208

You have a standalone root certification authority (CA).

You have a new security policy requirements specifying that any changes to the CA configuration must be logged.

You need to ensure that the CA meets the new security requirement.

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

- ☐ From the Certification Authority console, modify the Auditing settings for the CA.
- ☐ From the Certification Authority console, modify the Security settings for the CA.
- ☒ From Local Group Policy Editor, configure auditing for policy change.
- ☐ From the Certification Authority console, modify the Certificate Managers settings for the CA.
- ☒ From Local Group Policy Editor, configure auditing for object access.

Explanation:

Explanation:

Audit policy change defines whether every incident of a change to user rights assignment policies, audit policies, or trust policies is audited.

Audit object access defines whether the event of a user accessing an object--for example, a file, folder, registry key, printer, and so forth--that has its own system access control list (SACL) specified is audited.

References: <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-audit-policy-change>

<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-audit-object-access>

Question 209

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory forest. The forest contains a domain named contoso.com. The domain contains three domain controllers.

A domain controller named lon-dc1 fails. You are unable to repair lon-dc1.

You need to prevent the other domain controllers from attempting to replicate to lon-dc1.

Solution: From Active Directory Sites and Services, you remove the object of lon-dc1.

Does this meet the goal?

- ☒ Yes
☐ No

Question 210

HOTSPOT

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

You need to view a list of all the domain user accounts that are enabled. But whose users have not signed in during the last 30 days.

Which command should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Dsget.exe
Get-LocalUser
Ldp.exe
Net user
Search-ADAccount

AccountDisabled
AccountExpiring
AccountInactive
PasswordExpired

-TimeSpan 30 -UsersOnly | Format - Table Name, UserPrincipalName

Solution:

Answer Area

▼
Dsget.exe
Get-LocalUser
Ldp.exe
Net user
Search-ADAccount

▼
AccountDisabled
AccountExpiring
AccountInactive
PasswordExpired

-TimeSpan 30 -UsersOnly | Format - Table Name, UserPrincipalName

Question 211

Your network contains an Active Directory domain named contoso.com. The domain functional level is Windows Server 2012 R2.

You need to secure several high-privilege user accounts to meet the following requirements:

Prevent authentication by using NTLM.

Use Kerberos to verify authentication request to any resources.

Prevent the users from signing in to a client computer if the computer is disconnected from the domain.

What should you do?

- ☐ Create a universal security group for the user accounts and modify the Security settings of the group.
- ☐ Add the users to the Windows Authorization Access Group group.
- ☒ Add the user to the Protected Users group.
- ☐ Create a separate organizational unit (OU) for the user accounts and modify the Security settings of the OU.

Explanation:

Explanation:

Question 212

Your company has multiple branch offices.

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

In one of the branch offices, a new technician is hired to add computers to the domain.

After successfully joining multiple computers to the domain, the technician fails to join any more computers to the domain.

You need to ensure that the technician can join an unlimited number of computers to the domain.

What should you do?

- ☒ Run the Delegation of Control Wizard on the Computers container.
- ☐ Run the redircmp.exe command.
- ☐ Modify the Security settings of the technician's user account.
- ☐ Add the technician to the Windows Authorization Access group.
- ☐ Configure the technician's user account as a manager service account.
- ☐ Run the Set-ADComputer cmdlet.
- ☐ Add the technician to the Domain Computers group.

Explanation:

References:

<https://www.itprotoday.com/active-directory/delegating-privileges-active-directory>

Question 213

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

A user named User1 is in an organizational unit (OU) named OU1.

You are troubleshooting a folder access issue for User1.

You need a list of groups to which User1 is either a direct member or an indirect member.

Solution: You instruct User 1 to sign in and run whoami.exe/groups.

Does this meet the goal?

- ☒ Yes
☐ No

Explanation:

References: <https://www.thewindowsclub.com/whoami-windows>

Question 214

Your network contains an Active Directory domain. The domain contains an Active Directory Rights Management Services (AD RMS) cluster and a certification authority (CA).

You need to ensure that all the documents that are protected by using AD RMS can be decrypted if the account used to encrypt the documents is deleted.

What should you do?

- ☒ Configure super users in the AD RMS deployment.
☐ Manually configure the AD RMS cluster key password.
☐ Back up the AD-RMS-protected files by using Windows Server Backup.
☐ Configure key archival on the CA.

Question 215

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series.

Information and details provided in a question apply only to that question.

Your network contains an Active Directory domain named contoso.com. The domain contains 5,000 user accounts.

You have a Group Policy object (GPO) named DomainPolicy that is linked to the domain and a GPO named DCPolicy that is linked to the Domain Controllers organizational unit (OU).

You need to ensure that all of the client computers on the network automatically download and install Windows updates.

What should you do?

- ☐ From the Computer Configuration node of DCPolicy, modify Security Settings.
- ☐ From the Computer Configuration node of DomainPolicy, modify Security Settings.
- ☒ From the Computer Configuration node of DomainPolicy, modify Administrative Templates.
- ☐ From the User Configuration node of DCPolicy, modify Security Settings.
- ☐ From the User Configuration node of DomainPolicy, modify Folder Redirection.
- ☐ From user Configuration node of DomainPolicy, modify Administrative Templates.
- ☐ From Preferences in the User Configuration node of DomainPolicy, modify Windows Settings.
- ☐ From Preferences in the Computer Configuration node of DomainPolicy, modify Windows Settings.

Explanation:

Explanation:

To load policy settings by using Group Policy, you must use the Wuau.adm file that describes the new policy settings for the Automatic Updates client. Wuau.adm is automatically installed in the Windows\Inf folder when you install the new Automatic Updates feature.

You can load Windows\Inf\Wuau.adm as an administrative template in Group Policy Object Editor.

References: <https://support.microsoft.com/en-za/help/328010/how-to-configure-automatic-updates-by-using-group-policy-or-registry-s>

Question 216

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution. Determine whether the solution meets the stated goals.

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

The domain contains a DNS server named Server1. All client computers run Windows 10.

On Server1, you have the following zone configuration.

ZoneName	ZoneType	IsAutoCreated	IsDnsIntegrated	IsReverseLookupZone	IsSigned
_msdcs.contoso.com	Primary	False	True	False	False
0.in-addr.arpa	Primary	True	False	True	False
127.in-addr.arpa	Primary	True	False	True	False
255.in-addr.arpa	Primary	True	False	True	False
adatum.com	Forwarder	False	False	False	False
contoso.com	Primary	False	True	False	False
fabrikam.com	Primary	False	True	False	True
TrustAnchors	Primary	False	True	False	False

You need to ensure that all of the client computers in the domain perform DNSSEC validation for the fabrikam.com namespace.

Solution: From a Group Policy object (GPO) in the domain, you add a rule to the Name Resolution Policy Table (NRPT).

Does this meet the goal?

- ☒ Yes
☐ No

Explanation:

Explanation:

The NRPT stores configurations and settings that are used to deploy DNS Security Extensions (DNSSEC), and also stores information related to DirectAccess, a remote access technology.

Note: The Name Resolution Policy Table (NRPT) is a new feature available in Windows Server 2008 R2. The NRPT is a table that contains rules you can configure to specify DNS settings or special behavior for names or namespaces. When performing DNS name resolution, the DNS Client service checks the NRPT before sending a DNS query. If a DNS query or response matches an entry in the NRPT, it is handled according to settings in the policy. Queries and responses that do not match an NRPT entry are processed normally.

References: [https://technet.microsoft.com/en-us/library/ee649207\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/ee649207(v=ws.10).aspx)

Question 217

HOTSPOT

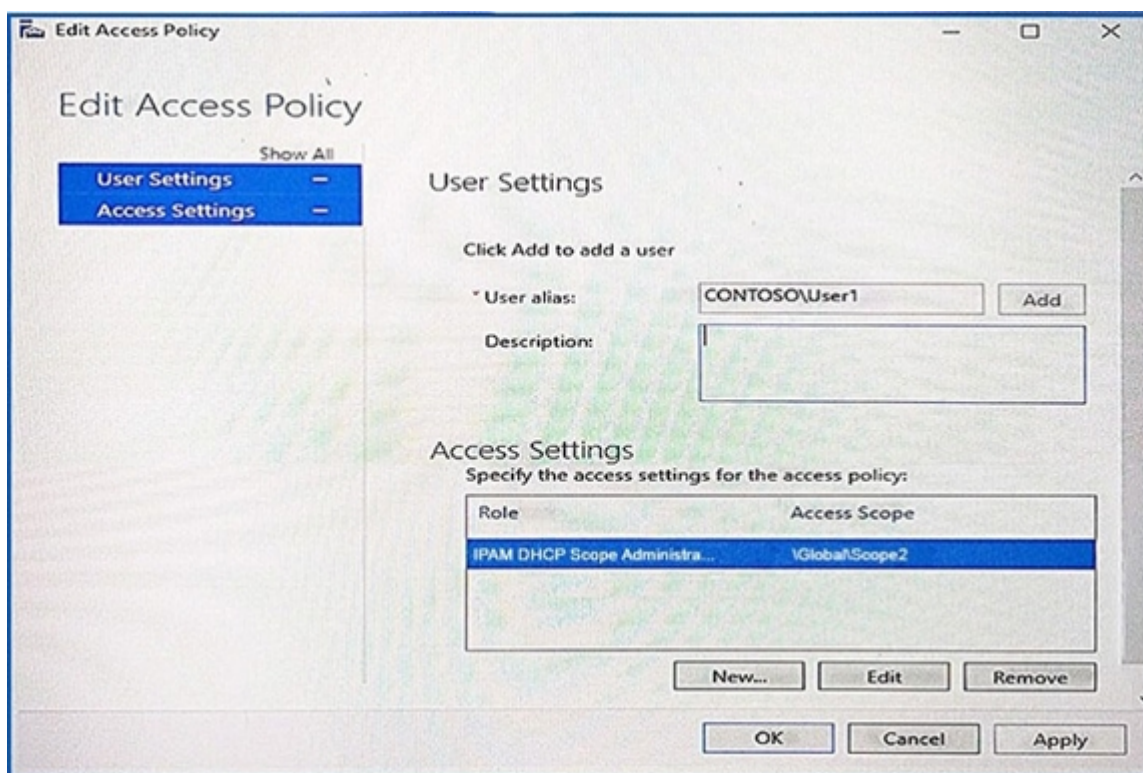
Your network contains an Active Directory domain named contoso.com.

The domain contains two servers named Server1 and Server2 that run Windows Server 2016.

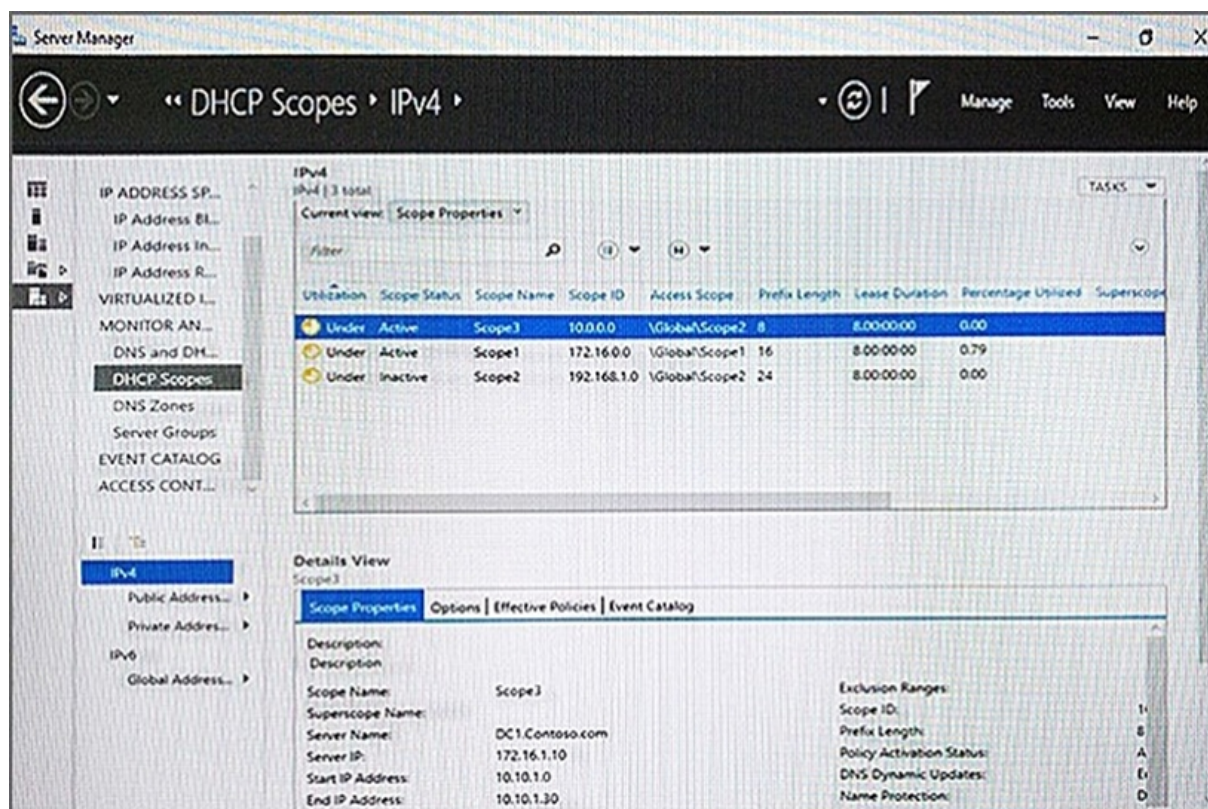
Server1 has IP Address Management (IPAM) installed. Server2 has the DHCP Server role installed. The IPAM server retrieves data from Server2.

The domain has two users named User1 and User2 and a group named Group1. User1 is the only member of Group1.

Server1 has one IPAM access policy. You edit the access policy as shown in the Policy exhibit. (Click the Exhibit button.)



The DHCP scopes are configured as shown in the Scopes exhibit. (Click the Exhibit button.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
User1 can modify the description of Scope1.	☐	☐
User2 can modify the description of Scope1.	☐	☐
User1 can modify the description of Scope2.	☐	☐

Solution:

Answer Area

Statements	Yes	No
User1 can modify the description of Scope1.	☐	☐
User2 can modify the description of Scope1.	☐	☐
User1 can modify the description of Scope2.	☐	☐

Question 218

DRAG DROP

Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1.

You create and link a Group Policy object (GPO) named SalesAppGPO to an organizational unit (OU) named SalesOU. All the computer accounts are in the Computers container. All the user accounts of the users in the sales department are in SalesOU.

You have a line-of-business application named SalesApp that is installed by using a Windows Installer package.

You need to make SalesApp available to only the sales department users.

Which three actions should you perform in sequence? To answer move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

In SalesAppGPO, create a software restriction policy in Computer Configuration\Policies\Windows Settings\Security Settings.

In SalesAppGPO, add a package to Computer Configuration\Policies\Software Settings\Software installation.

Copy the Windows Installer package to SalesApp.

On DC1, create a WebDAV folder named SalesApp.

On DC1, create a shared folder named SalesApp.

In SalesAppGPO, add a package to User Configuration\Policies\Software Settings\Software installation.

In SalesAppGPO, create a Software restriction policy in User Configuration\Policies\Windows Settings\Windows Settings.

Answer Area

Solution:

Actions

In SalesAppGPO, create a software restriction policy in Computer Configuration\Policies\Windows Settings\Security Settings.

In SalesAppGPO, add a package to Computer Configuration\Policies\Software Settings\Software installation.

Copy the Windows Installer package to SalesApp.

On DC1, create a WebDAV folder named SalesApp.

On DC1, create a shared folder named SalesApp.

In SalesAppGPO, add a package to User Configuration\Policies\Software Settings\Software installation.

In SalesAppGPO, create a Software restriction policy in User Configuration\Policies\Windows Settings\Windows Settings.

Answer Area

On DC1, create a WebDAV folder named SalesApp.

Copy the Windows Installer package to SalesApp.

In SalesAppGPO, add a package to Computer Configuration\Policies\Software Settings\Software installation.

Question 219

HOTSPOT

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

Your company has a custom application named ERP1. ERP1 uses an Active Directory Lightweight Directory Services (AD LDS) server named Server1 to authenticate users.

You have a member server named Server2 that runs Windows Server 2016. You install the Active Directory Federation Services (AD FS) server role on Server2 and create an AD FS farm.

You need to configure AD FS to authenticate users from the AD LDS server.

Which cmdlets should you run? To answer, select the appropriate options in the answer area.

Answer Area

First cmdlet to run:

	▼
Add-AdfsRelyingPartyTrust	
New-AdfsLdapServerConnection	
Set-AdfsEndpoint	

Second cmdlet to run:

	▼
Add-AdfsLocalClaimsProviderTrust	
Enable-AdfsRelyingPartyTrust	
Set-AdfsEndpoint	

Solution:

Answer Area

First cmdlet to run:

	▼
Add-AdfsRelyingPartyTrust	
New-AdfsLdapServerConnection	
Set-AdfsEndpoint	

Second cmdlet to run:

	▼
Add-AdfsLocalClaimsProviderTrust	
Enable-AdfsRelyingPartyTrust	
Set-AdfsEndpoint	

Explanation:

Explanation:

To configure your AD FS farm to authenticate users from an LDAP directory, you can complete the following steps:

Step 1: New-AdfsLdapServerConnection

First, configure a connection to your LDAP directory using the New-AdfsLdapServerConnection cmdlet:

```
$DirectoryCred = Get-Credential
```

```
$VendorDirectory = New-AdfsLdapServerConnection -HostName dirserver -Port 50000 -SslMode  
None -AuthenticationMethod Basic -Credential $DirectoryCred
```

Step 2 (optional):

Next, you can perform the optional step of mapping LDAP attributes to the existing AD FS claims using the New-AdfsLdapAttributeToClaimMapping cmdlet.

Step 3: Add-AdfsLocalClaimsProviderTrust

Finally, you must register the LDAP store with AD FS as a local claims provider trust using the Add-AdfsLocalClaimsProviderTrust cmdlet:

```
Add-AdfsLocalClaimsProviderTrust -Name "Vendors" -Identifier "urn:vendors" -Type I
```

References:

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn823754\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn823754(v=ws.11))

Question 220

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

The domain contains a web application that uses Kerberos authentication.

You change the domain name of the web application.

You need to ensure that the service principal name (SPN) for the application is registered.

Which tool should you use?

- ☐ Rdsfnf
- ☐ Active Directory Users and Computers
- ☐ Dnscmd
- ☒ Ldifde
- ☐ Netsh
- ☐ Internet Information Services (IIS) Manager
- ☐ Repladmin

Explanation:

Reference:

<https://blogs.technet.microsoft.com/tristank/2006/05/08/3-simple-rules-to-kerberos-authenticationdelegation-spns/>

Question 221

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a username User1, a group named Group1, and an organizational unit (OU) named OU1.

You need to enable User1 to link Group Policies to OU1.

Solution: From Active Directory Administrative Center, you add User1 to Group1. From Group Policy Management, you click the Group Policy Objects container. From the Delegation tab, you add Group1.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 222

Your network contains an Active Directory forest named contoso.com. The forest contains a member server named Server1.

Server1 has several line-of-business applications. Each application runs as a service that uses the Network Service account.

You need to configure the line-of-business applications to run by using a virtual account.

What should you do?

- ☐ From Windows PowerShell, run the Install-ADServiceAccount cmdlet.
- ☒ From the Services console, modify the Log On properties of the services.
- ☐ From the Microsoft Application Compatibility Toolkit (ACT), create a shim.
- ☐ From Windows PowerShell, run the New-ADServiceAccount cmdlet.

Question 223

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a server named Web1 that runs Windows Server 2016.

You need to list all the SSL certificates on Web1 that will expire during the next 60 days.

Solution: You run the following command.

```
Get-ChildItem Cert:\CurrentUser\My |? { $_.NotAfter -lt (Get-Date).AddDays( 60 ) }
```

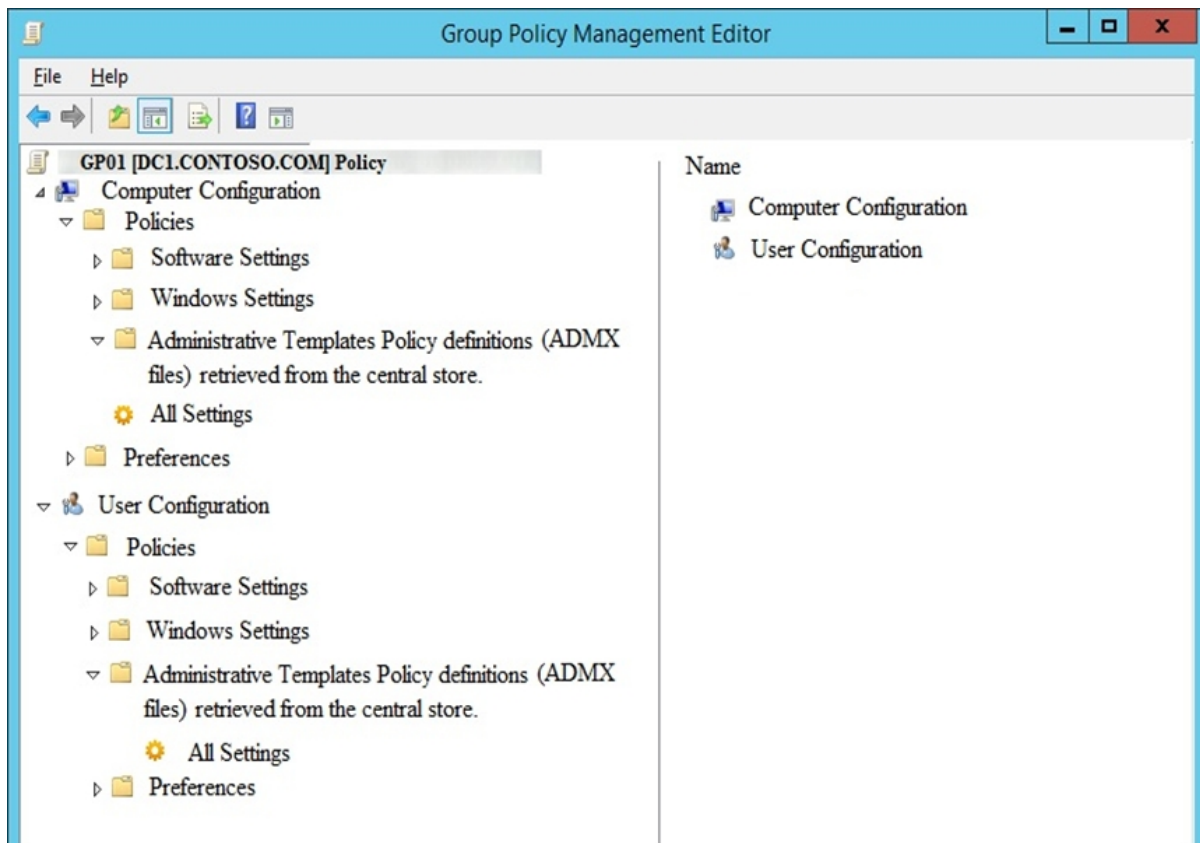
Does this meet the goal?

- ☐ Yes
☒ No

Question 224

Your network contains an Active Directory domain named contoso.com. The domain contains a member server named Server1 and a domain controller named DC1. Both servers run Windows Server 2016. Server1 is used to perform administrative tasks, including managing Group Policies.

After maintenance is performed on DC1, you open a Group Policy object (GPO) from Server1 as shown in the exhibit.



You need to be able to view all of the Administrative Templates settings in GPO1.

What should you do?

- ☐ From File Explorer, copy the administrative templates from \\contoso.com\SYSVOL\contoso.com\Policies to the PolicyDefinitions folder on Server1.
- ☒ From File Explorer, copy the administrative templates from Server1 to \\DC1\SYSVOL\contoso.com\Policies\PolicyDefinitions
- ☐ From Group Policy Management Editor, configure item-level targeting in GPO1.
- ☐ From Group Policy Management, configure WMI Filtering for GPO1.
- ☐ From Group Policy Management, configure Security Filtering for GPO1.
- ☐ From File Explorer, delete the PolicyDefinitions folder from Server1.

Explanation:

References:

<https://serverfault.com/questions/458144/where-did-my-group-policy-templates-go>

Question 225

You network contains an Active Directory domain named contoso.com. The domain contains 1,000 desktop computers and 500 laptops. An organizational unit (OU) named OU1 contains the computer accounts for the desktop computers and the laptops.

You create a Windows PowerShell script named Script1.ps1 that removes temporary files and cookies. You create a Group Policy object (GPO) named GPO1 and link GPO1 to OU1.

You need to run the script once weekly only on the laptops.

What should you do?

- ☐ In GPO1, create a File preference that uses item-level targeting.
- ☒ In GPO1, create a Scheduled Tasks preference that uses item-level targeting.
- ☐ In GPO1, configure the File System security policy. Attach a WMI filter to GPO1.
- ☐ In GPO1, add Script1.ps1 as a startup script. Attach a WMI filter to GPO1.

Explanation:

Explanation:

Question 226**HOTSPOT**

Your network contains an Active Directory forest named fabrikam.com. The forest contains three domains named fabrikam.com, sales.fabrikam.com, and contoso.com.

You recently added a site named Europe.

The forest contains four users who are members of the groups shown in the following table.

User name	Member of	Domain
User1	Domain Admins	Fabrikam.com
User2	Enterprise Admins	Fabrikam.com
User3	Domain Admins	Sales.fabrikam.com
User4	Domain Admins	Contoso.com

You need to create a Group Policy object (GPO) named GPO1 and to link GPO1 to the Europe site.

Which users can perform each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Users who can create GPO1:

▼

☐ User1 only
 ☐ User2 only
 ☐ User3 only
 ☐ User4 only
 ☐ User1 and User4 only
 ☐ User1 and User2 only
 ☐ User2 and User3 only
 ☐ User1, User2, User3, and User4

Users who can link GPO1 to Europe:

▼

☐ User1 only
 ☐ User2 only
 ☐ User3 only
 ☐ User4 only
 ☐ User1 and User4 only
 ☐ User1 and User2 only
 ☐ User2 and User3 only
 ☐ User1, User2, User3, and User4

Solution:

Answer Area

Users who can create GPO1:

	▼
User1 only	
User2 only	
User3 only	
User4 only	
User1 and User4 only	
User1 and User2 only	
User2 and User3 only	
User1, User2, User3, and User4	

Users who can link GPO1 to Europe:

	▼
User1 only	
User2 only	
User3 only	
User4 only	
User1 and User4 only	
User1 and User2 only	
User2 and User3 only	
User1, User2, User3, and User4	

Question 227

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a server named Web1 that runs Windows Server 2016.

You need to list all the SSL certificates on Web1 that will expire during the next 60 days.

Solution: You run the following command.

```
Get-ChildItem Cert:\LocalMachine\Trust |? { $_.NotAfter -lt (Get-Date).AddDays( 60 ) }
```

Does this meet the goal?

- ☐ Yes
☒ No

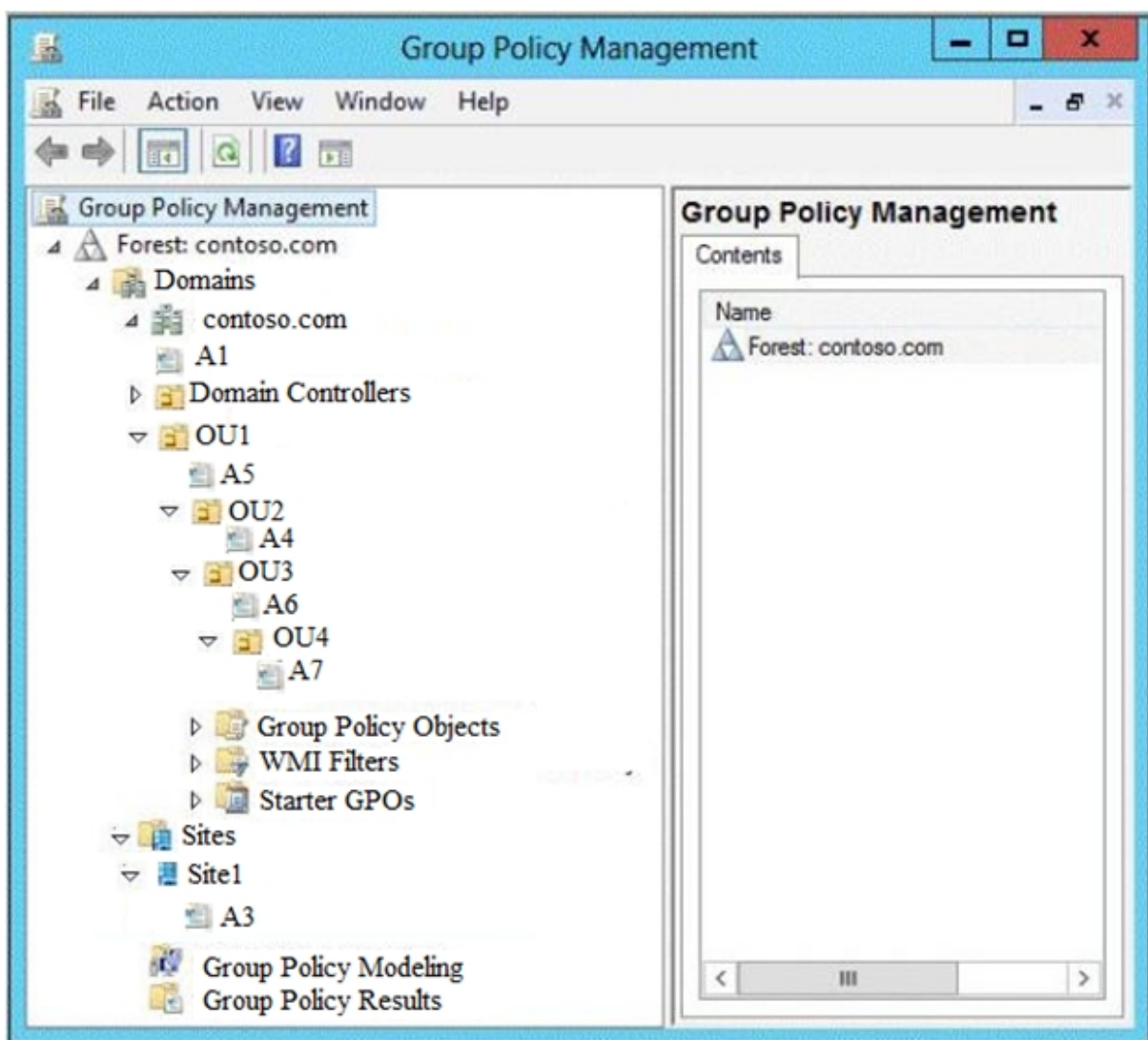
Question 228

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario.

Your network contains an Active Directory domain named contoso.com. The domain contains a single site named Site1. All computers are in Site1.

The Group Policy objects (GPOs) for the domain are configured as shown in the exhibit. (Click the Exhibit button.)



The relevant users and client computer in the domain are configured as shown in the following table.

Object name	Object type	Object location
Computer	Computer	OU4
User1	User	OU4
User2	User	OU2

End of repeated scenario.

You are evaluating what will occur when you disable the Group Policy link for A6.

Which GPOs will apply to User2 when the user signs in to Computer1 after the link for A6 is disabled?

- ☐ A1 and A5 only
- ☐ A3, A1, and A5 only
- ☒ A3, A1, A5, and A4 only
- ☐ A3, A1, A5, and A7

Explanation:

Explanation:

Question 229

HOTSPOT

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

The domain contains a server named Server1 that runs Windows Server 2016.

You install IP Address Management (IPAM) on Server1.

You select the automatic provisioning method, and then you specify a prefix of IPAM1.

You need to configure the environment for automatic IPAM provisioning.

Which cmdlet should you run? To answer, select the appropriate options in the answer area.

Answer Area

▼ Add-IpamDiscoveryDomain Enable-IpamCapability Invoke-IpamGpoProvisioning Set-IpamConfiguration	-Domain "Contoso.com"	▼ -AssetTag -DiscoverDns -GpoPrefixName -ProvisioningMethod
---	-----------------------	--

Solution:

Answer Area

▼ Add-IpamDiscoveryDomain Enable-IpamCapability Invoke-IpamGpoProvisioning Set-IpamConfiguration	-Domain "Contoso.com"	▼ -AssetTag -DiscoverDns -GpoPrefixName -ProvisioningMethod
---	-----------------------	--

Question 230

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. The computer account for Server1 is in organizational unit (OU) named OU1.

You create a Group Policy object (GPO) named GPO1 and link GPO1 to OU1.

You need to add a domain user named User1 to the local Administrators group on Server1.

Solution: From the Computer Configuration node of GPO1, you configure the Account Policies settings.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Explanation:

Account Lockout Policy settings encapsulates Password Policy, Account Lockout Policy, and Kerberos Policy. It will not allow you to add a domain user to a local Administrators group.

References: [https://technet.microsoft.com/pt-pt/library/cc757692\(v=ws.10\).aspx](https://technet.microsoft.com/pt-pt/library/cc757692(v=ws.10).aspx)

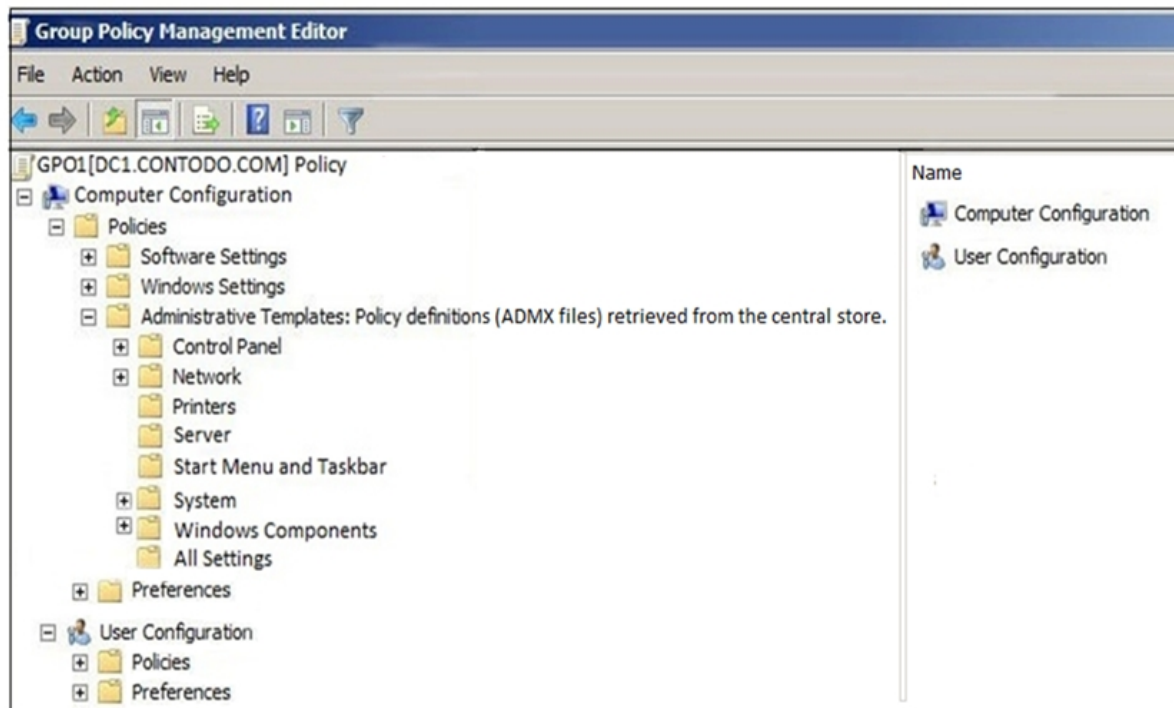
Question 231

HOTSPOT

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

You have an administrative computer named Computer1 that runs Windows Server 2016.

From Computer1, you edit a Group Policy object (GPO) named GPO1 as shown in the exhibit.



You receive a new administrative template named Template1. Template1 consists of Template1.admx and Template1.adml. Template1 is in English US.

You need to ensure that the settings of Template1 appear under the Administrative Templates node.

To where should you copy the Template1 files? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Copy Template1admx to:

▼
C:\Windows\en-US
C:\Windows\System32\GroupPolicy
C:\Windows\System32\PolicyDefinitions
C:\Windows\System32\PolicyDefinitions\en-US
\\Contoso.com\Sysvol\Contoso.com\Policies\PolicyDefinitions
\\Contoso.com\Sysvol\Contoso.com\Policies\PolicyDefinitions\en-US

Copy Template1adml to:

▼
C:\Windows\en-US
C:\Windows\System32\GroupPolicy
C:\Windows\System32\PolicyDefinitions
C:\Windows\System32\PolicyDefinitions\en-US
\\Contoso.com\Sysvol\Contoso.com\Policies\PolicyDefinitions
\\Contoso.com\Sysvol\Contoso.com\Policies\PolicyDefinitions\en-US

Solution:**Answer Area**

Copy Template1admx to:

▼
C:\Windows\en-US
C:\Windows\System32\GroupPolicy
C:\Windows\System32\PolicyDefinitions
C:\Windows\System32\PolicyDefinitions\en-US
\\Contoso.com\Sysvol\Contoso.com\Policies\PolicyDefinitions
\\Contoso.com\Sysvol\Contoso.com\Policies\PolicyDefinitions\en-US

Copy Template1adml to:

▼
C:\Windows\en-US
C:\Windows\System32\GroupPolicy
C:\Windows\System32\PolicyDefinitions
C:\Windows\System32\PolicyDefinitions\en-US
\\Contoso.com\Sysvol\Contoso.com\Policies\PolicyDefinitions
\\Contoso.com\Sysvol\Contoso.com\Policies\PolicyDefinitions\en-US

Explanation:

References:

[https://docs.microsoft.com/en-us/previous-versions/dotnet/articles/bb530196\(v=msdn.10\)](https://docs.microsoft.com/en-us/previous-versions/dotnet/articles/bb530196(v=msdn.10))

Question 232

You have an Active Directory Rights Management Services (AD RMS) server named RMS1.

Multiple documents are protected by using RMS1.

RMS1 fails and cannot be recovered.

You install the AD RMS server role on a new server named RMS2.

You restore the AD RMS database from RMS1 to RMS2.

Users report that they fail to open the protected documents and to protect new documents.

You need to ensure that the users can access the protected content.

What should you do?

- ☐ From Active Directory Rights Management, update the Service Connection Point (SCP) for RMS1.
- ☐ From DNS, create an alias (CNAME) record for RMS2.
- ☐ From DNS, modify the service location (SRV) record for RMS1.
- ☒ From RMS2, register a service principal name (SPN) in Active Directory.

Question 233

You have an enterprise certification authority (CA).

You create a global security group named Group1.

You need to provide members of Group1 with the ability to issue and manage certificates.

The solution must prevent the Group1 members from managing certificates requested by members of the Domain Admins group.

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

NOTE: Each correct selection is worth one point.

- ☐ From the CA properties, modify the Policy Module settings.
- ☐ From the Certificate Templates console, modify the Security settings of the Administrator certificate template.
- ☒ From the CA properties, modify the security settings.
- ☐ From the CA properties, modify the Enrollment Agents settings.
- ☒ From the CA properties, modify the Certificate Managers Settings.
- ☐ From the Certificate Templates console, modify the Security settings of the User certificate template.

Question 234

HOTSPOT

Your network contains an Active Directory domain named adatum.com. The domain uses Active Directory Federation Services (AD FS), AD FS has a relying party trust named RP1 to a claims-aware application named App1. The domain contains the users shown in the following table.

Name	Group
User1	Group1
User2	Group1, Group2
User3	Group2

The network contains the network segments shown in the following table.

Name	Address space
Network1	192.168.1.0/24
Network2	192.168.2.0/24

The following access control policy is assigned to RP1.

```
Name      : Policy1
Identifier : Policy 1
IsBuiltIn  : False
RpUsageCount : 1
LastUpdateTime : 1/21/2019 2:20:00 PM
Description :
PolicyMetadata : RequireFreshAuthentication:False
IssuanceAuthorizationRules:
{
  Permit users
  from IP range '192.168.1.0/24'
  and from 'ADATUM\Group2' group
  except
  from 'ADATUM\Group1' group;

  Permit users
  from IP range '192.168.2.0/24'
  and from 'ADATUM\Group1' group;

  Permit users
  from 'extranet' location
  and when authentication includes MFA
}
AssignedTo : {RP1}
```

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can access App1 from a device connected to Network2.	☐	☐
User2 can access App1 from a device connected to Network1.	☐	☐
User3 can access App1 from a device connected to Network1.	☐	☐

Solution:

Answer Area

Statements	Yes	No
User1 can access App1 from a device connected to Network2.	☒	☐
User2 can access App1 from a device connected to Network1.	☐	☒
User3 can access App1 from a device connected to Network1.	☒	☐

Explanation:

References:

<https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/access-control-policies-in-ad-fs>

Question 235

DRAG DROP

Your network contains an Active Directory domain. The domain contains two domain controllers named DC1 and DC2. DC2 is a virtual machine that is hosted on a Hyper-V host named HyperV1. DC1 holds the PDC emulator operations master role.

You need to create a new domain controller named DC3 by using domain controller cloning.

Which five actions should you perform in sequence before you can import the cloned virtual machine? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions	Answer Area
Run the Get-ADDCCloningExcludedApplicationList cmdlet	
Modify the group membership of DC2	
Export DC2	
Run the New-ADDCCloneConfigFile cmdlet	
Modify the group membership of DC3	
Stop DC2	

Solution:

Actions	Answer Area
Run the Get-ADDCCloningExcludedApplicationList cmdlet	Modify the group membership of DC2
Modify the group membership of DC2	Run the Get-ADDCCloningExcludedApplicationList cmdlet
Export DC2	Run the New-ADDCCloneConfigFile cmdlet
Run the New-ADDCCloneConfigFile cmdlet	Stop DC2
Modify the group membership of DC3	Export DC2
Stop DC2	

Explanation:

References:

<https://blogs.technet.microsoft.com/askpfeplat/2012/10/01/virtual-domain-controller-cloning-in-windows-server-2012/>

Question 236

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. You have an organizational unit (OU) named LondonUsers that contains 10,000 users. You need to modify the office attribute of all the users in the LondonUsers OU.

Solution: You create an LDIF file. You run `ldifde.exe` and specify the `-i` and `-f` parameters.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

References:

<https://webactivedirectory.com/2011/07/18/simple-powershell-script-to-bulk-update-or-modify-active-directory-user-attributes/>

Question 237

Your network contains an Active Directory domain named adatum.com. The domain contains a security group named G_Research and an organizational unit (OU) named OU_Research.

All the users in the research department are members of G_Research and their user accounts are in OU_Research.

You need to ensure that all the research department users change their password every 28 days and enforce a complex password that is 12 characters long.

What should you do?

- ☐ From a Group Policy Management, create and link a Group Policy object (GPO) to OU_Research. Modify the password policy in the GPO.
- ☐ From a Group Policy Management, create and link a Group Policy object (GPO) to the domain. Modify the password policy in the GPO. Filter the GPO to apply to G_Research only.
- ☐ From Active Directory Users and Computers, modify the properties of the Password Settings Container.
- ☒ From Active Directory Administrative Center, create a new Password Settings object (PSO).

Question 238

HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

Name	Object Type	In organizational unit (OU)
Server1	Computer	OU1
User1	User	OU2
User2	User	OU3

Server1 has a local user named Admin1 and a local Group Policy that sets the minimum password length to four characters. The domain has the Group Policy objects (GPOs) shown in the following table.

Name	Minimum password length	Linked to
GPO1	5	OU1
GPO2	6	OU2
GPO3	8	OU3
Default Domain Policy	7	Contoso.com

What is the minimum password length for each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area**User1:**

4
5
6
7
8

User2:

4
5
6
7
8

User3:

4
5
6
7
8

Answer Area

User1:

4
5
6
7
8

User2:

4
5
6
7
8

User3:

4
5
6
7
8

Solution:

Question 239

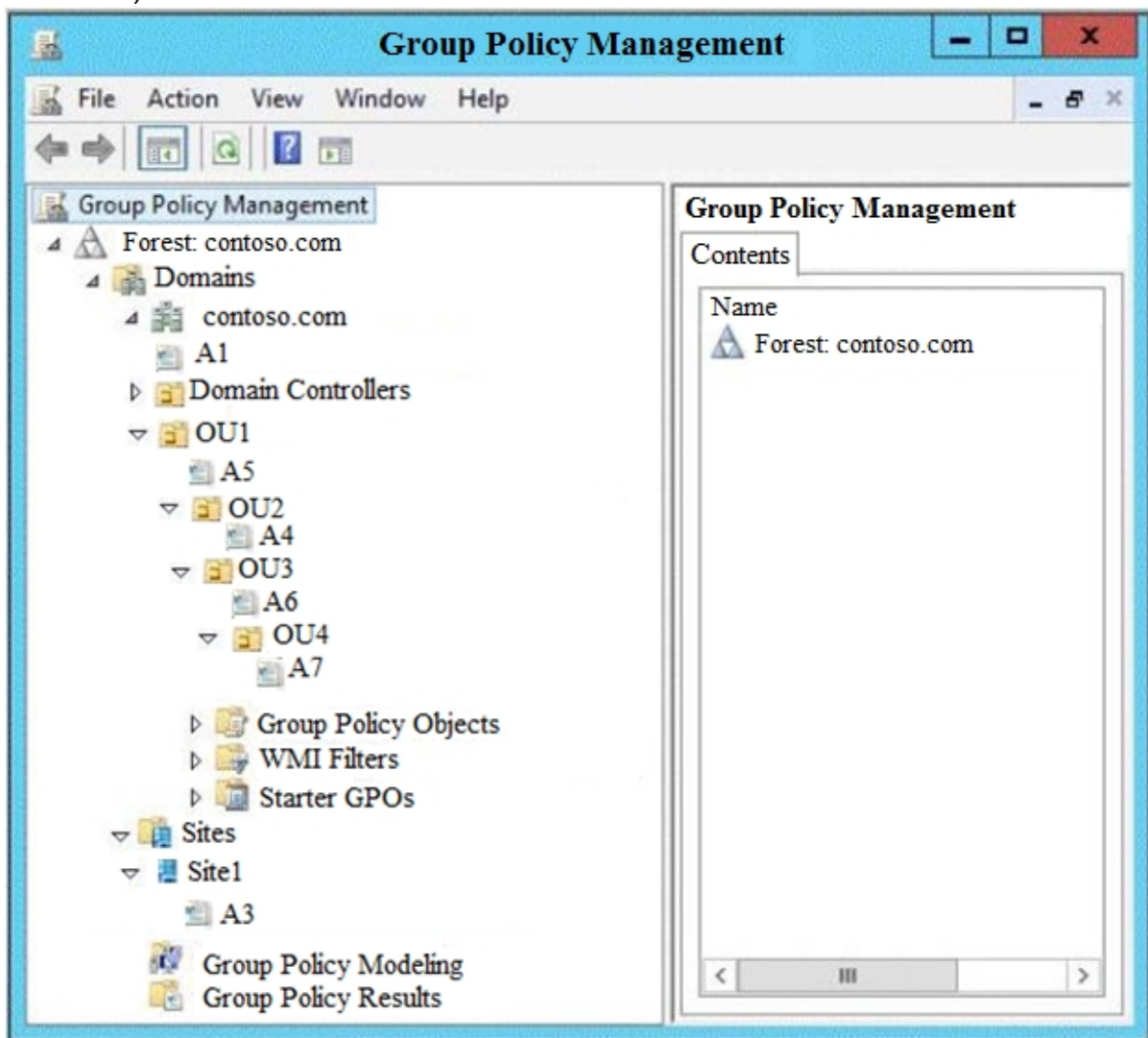
DRAG DROP

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario

Your network contains an Active Directory domain named contoso.com. The domain contains a single site named Site1. All computers are in Site1.

The Group Policy objects (GPOs) for the domain are configured as shown in the exhibit. (Click the Exhibit tab.)



The relevant users and client computer in the domain are configured as shown in the following table.

Object name	Object type	Object location
Computer1	Computer	OU4
User1	User	OU4
User2	User	OU2

End of repeated scenario

You plan to enforce the GPO link for A6.

Which five GPOs will apply to User1 in sequence when the user signs in to Computer1 after the link is enforced? To answer, move the appropriate GPOs from the list of GPOs to the answer area and arrange them in the correct order.

GPOs

A1
A3
A4
A5
A6
A7

Answer Area

GPOs

A1
A3
A4
A5
A6
A7

Answer Area

A3
A1
A5
A7
A6

Solution:

Question 240

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named Server1.

You recently restored a backup of the Active Directory database from Server1 to an alternate Location. The restore operation does not interrupt the Active Directory services on Server1.

You need to make the Active Directory data in the backup accessible by using Lightweight Directory Access Protocol (LDAP).

Which tool should you use?

- ☐ Dsadd quota
- ☐ Dsmmod
- ☐ Active Directory Administrative Center
- ☐ Dsacls
- ☒ Dsmain
- ☐ Active Directory Users and Computers
- ☐ Ntdsutil
- ☐ Group Policy Management Console

Explanation:

Explanation:

Dsmain.exe, allows an ntds.dit file to be mounted and exposed as an LDAP server, which means you can use such familiar tools as ADSIEdit, LDP.exe, and Active Directory Users and Computers to interact with a mounted database.

References:

<http://www.itprotoday.com/windows-8/using-active-directory-snapshots-and-dsmain-tool>

Question 241

You network contains one Active Directory domain named adatum.com.

The domain contains a DNS server named Server1 that runs Windows Server 2016.

All domain computers use Server1 for DNS.

You sign adatum.com by using DNSSEC.

You need to configure the domain computers to validate DNS responses for adatum.com records.

What should you configure in Group Policy?

- ☐ Network List Manager Policies
- ☐ Network Access Protection (NAP)
- ☒ Name Resolution Policy
- ☐ Public Key Policy

Question 242

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. The computer account for Server1 is in organizational unit (OU) named OU1.

You create a Group Policy object (GPO) named GPO1 and link GPO1 to OU1.

You need to add a domain user named User1 to the local Administrators group on Server1.

Solution: From a domain controller, you run the Set-AdComputer cmdlet.

Does this meet the goal?

- ☐ Yes
- ☒ No

Explanation:

Explanation:

The Set-AdComputer cmdlet modifies an Active Directory computer object. It will not allow you to add a domain user to a local Administrators group.

References: [https://technet.microsoft.com/es-es/library/hh852268\(v=wps.620\).aspx](https://technet.microsoft.com/es-es/library/hh852268(v=wps.620).aspx)

Question 243

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

You have a Group Policy object (GPO) named GPO1. GPO1 is linked to an organizational unit (OU) named OU1.

GPO1 contains several corporate desktop restrictions that apply to all computers.

You plan to deploy a printer to the computers in OU1.

You need to ensure that any user who signs in to a computer that runs Windows 10 in OU1 receives the new printer. All of the computers in OU1 must continue to apply the corporate desktop restrictions from GPO1.

What should you configure?

- ☐ a user preference and a WMI filter on GPO1.
- ☒ a computer preference that uses item-level targeting
- ☐ a computer preference and WMI filter on GPO1
- ☐ a user preference that uses item-level targeting

Explanation:

Explanation:

Question 244

HOTSPOT

You have a Nano Server named Nano1 that runs Windows Server 2016. Nano1 is deployed to a virtual machine and is a member of a workgroup.

You need to join Nano1 to a domain named contoso.com.

Which two commands should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

First command to run:

▼
Add-Computer with DomainName parameter
Djoin.exe with the Provision parameter
Netdom.exe with the JOIN parameter
New-nanoServerImage with the DomainName parameter
Nltest.exe with the SC_RESET parameter

Second command to run:

▼
Dism.exe with the Commit-Image parameter
Djoin.exe with the RequestODJ parameter
Restart-Computer with the Force parameter
Shutdown.exe with the r parameter

Solution:

Answer Area

First command to run:

▼
Add-Computer with DomainName parameter
Djoin.exe with the Provision parameter
Netdom.exe with the JOIN parameter
New-nanoServerImage with the DomainName parameter
Nltest.exe with the SC_RESET parameter

Second command to run:

▼
Dism.exe with the Commit-Image parameter
Djoin.exe with the RequestODJ parameter
Restart-Computer with the Force parameter
Shutdown.exe with the r parameter

Explanation:

References:

<https://charbelnemnom.com/2016/11/how-to-add-nano-server-to-a-domain-nanoserver-ws2016/>

Question 245

HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains an administrative workstation named WKS1 that runs Windows 10.

You have a Group Policy object (GPO) named GPO1.

You download a custom administrative template that contains the following files:

App1.admx

App1.adml

You need to ensure that you can configure GPO1 by using the settings in the new administrative template.

To where should you copy each file? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

App1.adml:

	▼
C:\Windows\PolicyDefinitions	
C:\Windows\PolicyDefinitions\en-US	
C:\Windows\System32\Configuration	
C:\Windows\System32\en-US	

App1.admx:

	▼
C:\Windows\PolicyDefinitions	
C:\Windows\PolicyDefinitions\en-US	
C:\Windows\System32\Configuration	
C:\Windows\System32\en-US	

Solution:

Answer Area

App1.adml:

	▼
C:\Windows\PolicyDefinitions	
C:\Windows\PolicyDefinitions\en-US	
C:\Windows\System32\Configuration	
C:\Windows\System32\en-US	

App1.admx:

	▼
C:\Windows\PolicyDefinitions	
C:\Windows\PolicyDefinitions\en-US	
C:\Windows\System32\Configuration	
C:\Windows\System32\en-US	

Explanation:

References: <https://msdn.microsoft.com/en-us/library/bb530196.aspx>

Question 246

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains an Active Directory domain named contoso.com.
The domain contains a domain controller named DC1 that runs Windows Server 2016.

You need to create a snapshot of the Active Directory database on DC1.
Which tool should you use?

- ☐ Dsadd quota
- ☐ Dsmmod
- ☐ Active Directory Administrative Center
- ☐ Dsacls
- ☐ Dsamain
- ☐ Active Directory Users and Computers
- ☒ Ntdsutil
- ☐ Group Policy Management Console

Question 247

Your network contains an Active directory domain named contoso.com. The domain has an enterprise certification authority (CA).

You duplicate the Basic EFS template, and you name the template Template1. You configure the CA to issue Template1.

Users are configured to obtain a new certificate automatically when they sign in to a computer in the domain.

You need to enable the users to automatically obtain a certificate based on Template1.

What should you modify?

- ☐ The Publication Settings for the CA.
- ☒ The Security Settings for Template1.
- ☐ The Request Handling properties for Template1.
- ☐ The Request Handling properties for the CA.

Question 248

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

A user named User1 is in an organizational unit (OU) named OU1.

You are troubleshooting a folder access issue for User1.

You need a list of groups to which User1 is either a direct member or an indirect member.

Solution: You run `Get-ADUser -Identity User1 -Property MemberOf`.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Explanation:

The `Get-ADUser` cmdlet does not include the `MemberOf` property. The command above is, therefore, not valid.

References: <https://docs.microsoft.com/en-us/powershell/module/addsadministration/get-aduser?view=win10-ps>

Question 249

DRAG DROP

Your company implements Active Directory Federation Services (AD FS).

You confirm that the company meets all the prerequisites for using Microsoft Azure Multi-Factor Authentication (MFA) and AD FS.

You need to ensure that you can select MFA as the primary authentication method for AD FS.

Which three actions should you perform in sequence? To answer move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Add a claims provider trust.	1.
Run the New-AdfsAzureMfatenant Certificate cmdlet.	2.
Run the New-MsolServicePrincipal Credential cmdlet.	3.
Edit the authentication methods.	
Run the Set-AdfsAzureMfaTenant cmdlet.	

Solution:

Actions	Answer Area
Add a claims provider trust.	1. Run the New-AdfsAzureMfatenant Certificate cmdlet.
Run the New-AdfsAzureMfatenant Certificate cmdlet.	2. Run the New-MsolServicePrincipal Credential cmdlet.
Run the New-MsolServicePrincipal Credential cmdlet.	3. Run the Set-AdfsAzureMfaTenant cmdlet.
Edit the authentication methods.	
Run the Set-AdfsAzureMfaTenant cmdlet.	

Explanation:

Explanation:

References:

<https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-and-azure-mfa>

Question 250

DRAG DROP

Your company has multiple offices.

The network contains an Active Directory domain named contoso.com. An Active Directory site exists for each office. All of the sites connect to each other by using DEFAULTIPSITELINK.

The company plans to open a new office. The new office will have a domain controller and 100 client computers.

You install Windows Server 2016 on a member server in the new office. The new server will become a domain controller.

You need to deploy the domain controller to the new office. The solution must ensure that the client computers in the new office will authenticate by using the local domain controller.

Which three actions should you perform next in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Create a new site object.	
Create a new connection object.	
Promote the member server to a domain controller.	
Create a new subnet object.	
Move the server object of the domain controller.	

Solution:

Actions	Answer Area
Create a new site object.	Create a new site object.
Create a new connection object.	Create a new subnet object.
Promote the member server to a domain controller.	Promote the member server to a domain controller.
Create a new subnet object.	
Move the server object of the domain controller.	

Question 251

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a server named Web1 that runs Windows Server 2016.

You need to list all the SSL certificates on Web1 that will expire during the next 60 days.

Solution: You run the following command.

```
Get-ChildItem Cert:\LocalMachine\My |? { $_.NotAfter -lt (Get-Date).AddDays( 60 ) }
```

Does this meet the goal?

- ☒ Yes
☐ No

Question 252

Your network contains an Active Directory domain named contoso.com. The domain contains a certification authority (CA).

The CA certificate was valid for five years and is about to expire.

You need to ensure that when you renew the CA certificate, the maximum Validity period for the certificate is 10 years.

What should you do before you renew the certificate?

- ☐ From Microsoft XML Notepad, create a file named CAPolicy.xml in the C:\Window\System32\ADC folder.
- ☐ From Windows System Image Manager, create a file named Unattend.xml. Store Unattend.xml in the C:\Windows\System32\Config folder.
- ☐ From Windows Imaging and Configuration Designer, create a file named Unattend.ini. Store Unattend.ini in the C:\Windows\Panther folder.
- ☒ From Microsoft Notepad, create a file named CAPolicy.inf. Store CAPolicy.inf in the C:\Windows folder.

Explanation:

References:

<https://www.sysadmins.lv/blog-en/how-to-change-ca-certificate-validity-period.aspx>

Question 253

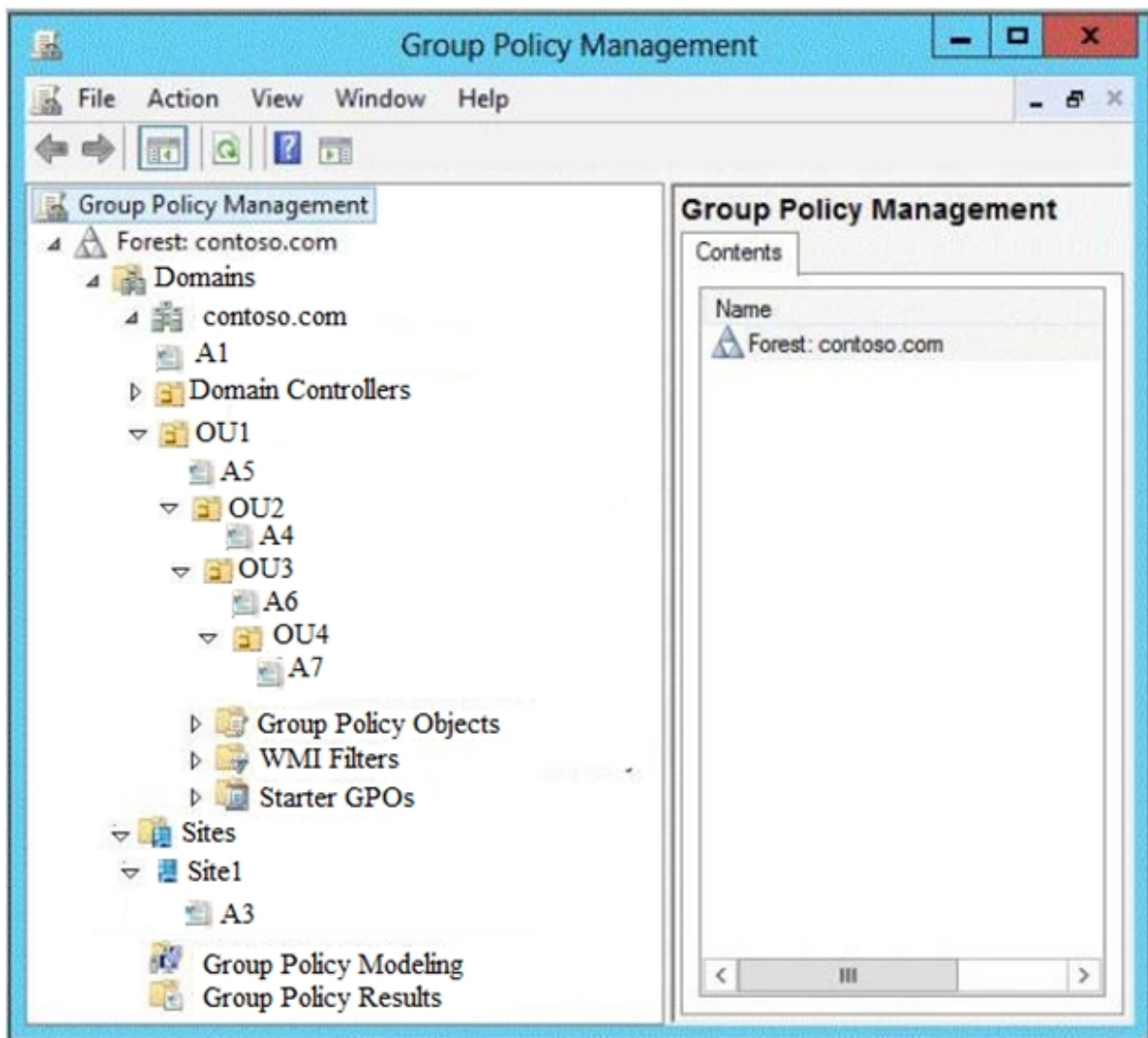
DRAG DROP

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario

Your network contains an Active Directory domain named contoso.com. The domain contains a single site named Site1. All computers are in Site1.

The Group Policy objects (GPOs) for the domain are configured as shown in the exhibit. (Click the Exhibit button.)



The relevant users and client computer in the domain are configured as shown in the following table.

Object name	Object type	Object location
Computer1	Computer	OU4
User1	User	OU4
User2	User	OU2

End of repeated scenario

Which five GPOs will apply to User1 in sequence when the user signs in to Computer1? To answer, move the appropriate GPOs from the list to the answer area and arrange them in the correct order.

GPOs

A1
A3
A4
A5
A6
A7

Answer Area

GPOs	Answer Area
A1	A3
A3	A1
A4	A5
A5	A6
A6	A7
A7	

Solution:

Question 254

Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2016. The computer accounts of Server1 and Server2 are in the Computers container.

A Group Policy object (GPO) named GPO1 is linked to the domain. GPO1 has multiple computer settings defined and has following configurations.

DisplayName:	GPO1
Domain Name:	Contoso.com
Owner:	CONTOSO\Domain Admins
Id:	bf3b4d96-59f6-4d0f-84c3-b9c37180b9ca
GpoStatus:	UserSettingsDisabled
Description:	
CreationTime:	2/18/2017 7:11:30 AM
ModificationTime:	2/18/2017 9:33:04 AM
UserVersion:	AD Version 18, SysVol Version: 18
ComputerVersion:	AD Version 6, SysVol Version: 6
WmiFilter:	WMI1

An administrator discovers that GPO1 is not applied to Server1. GPO1 is applied to Server2.

Which configuration possibly prevents GPO1 from being applied to Server1?

- ☐ The permissions on the domain object of contoso.com
- ☒ The WMI filter settings
- ☐ The Enforced setting of GPO1
- ☐ The GpoStatus property
- ☐ The loopback processing mode in GPO1
- ☐ The permissions on the domain object of contoso.com

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/create-wmi-filters-for-the-gpo>