

DUMPSBOSS.

Identity with Windows Server 2016

Microsoft 70-742

Version Demo

Total Demo Questions: 15

Total Premium Questions: 267

Buy Premium PDF

<https://dumpsboss.co>

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Install and Configure Active Directory Domain Services (AD DS)	77
Topic 2, Manage and Maintain AD DS	49
Topic 3, Create and Manage Group Policy	71
Topic 4, Implement Active Directory Certificate Services	27
Topic 5, Implement Identity Federation and Access Solutions	43
Total	267

QUESTION NO: 1 - (HOTSPOT)**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:
App1
This name will appear in the list of published web applications.

External URL:
https://server02.contoso.com/app1

External certificate:
server02.contoso.com View...

Enable HTTP to HTTPS redirection

Backend server URL:
http://server02.contoso.com/publish/app1

Backend server SPN:

< Previous Next > Publish Cancel

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

Hot Area:

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

ANSWER:

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

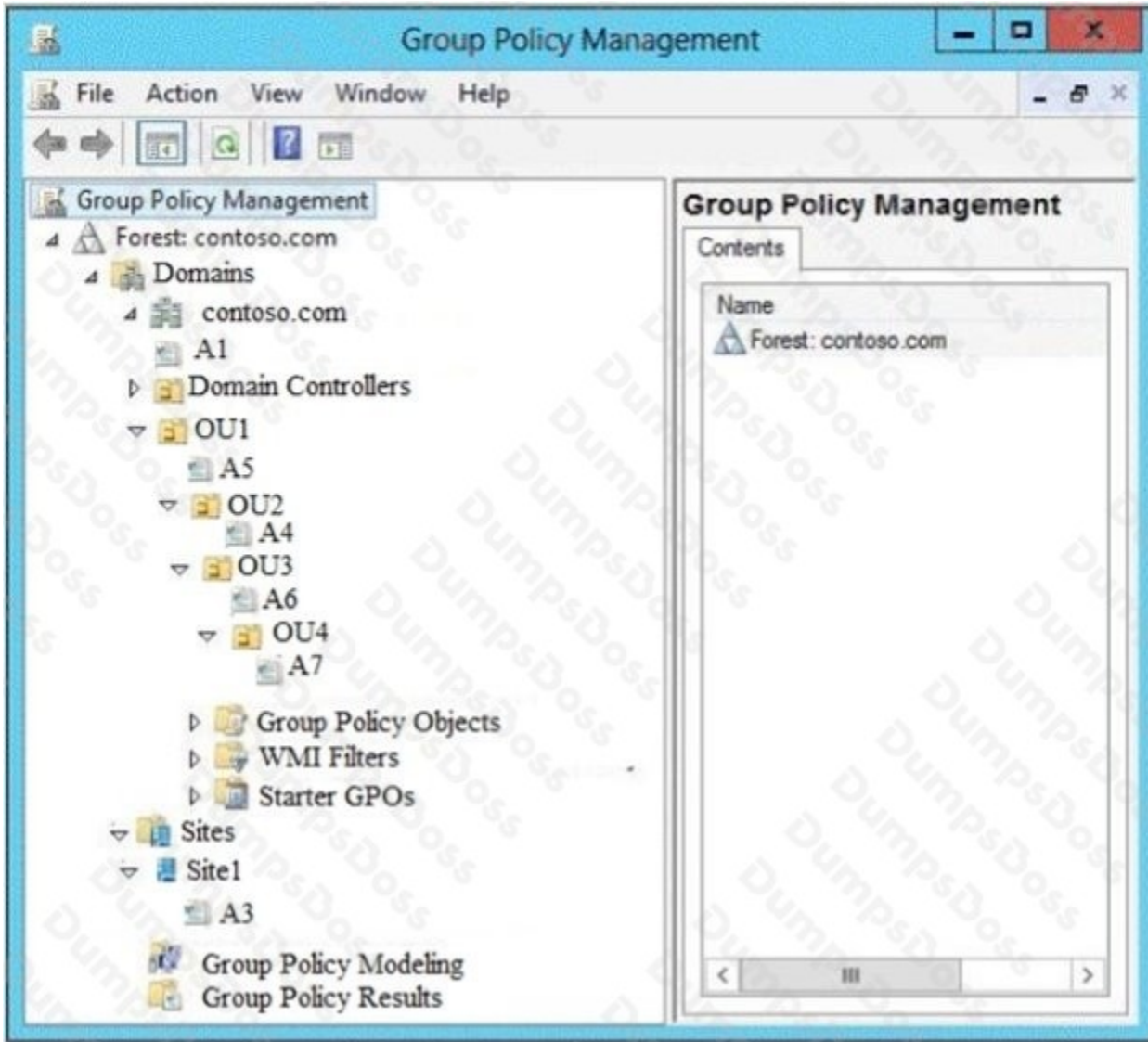
QUESTION NO: 2

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?

- A. A1 and A7 only
- B. A3, A1, A5, A6 and A7
- C. A3, A5, A1, and A7 only
- D. A7 only

ANSWER: D

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 NO: 3

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?

- A. secdit with the /configure switch
- B. Invoke-Gpupdate with the –Boot switch
- C. gpupdate with the /force switch
- D. Invoke-Gpupdate with the –Sync switch

ANSWER: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/powershell/module/grouppolicy/invoke-gpupdate?view=win10-ps>

QUESTION NO: 4

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.

- A. `dnscmd /DirectoryPartitionInfo`
- B. `dcdiag.exe /test:DNS`
- C. `dcdiag.exe /test:connectivity`
- D. `dnscmd /IpValidate`
- E. `dcdiag.exe /test:DnsRecordRegistration`
- F. `dnscmd /info`

ANSWER: C E

QUESTION NO: 5 - (DRAG DROP)

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.

Select and Place:

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

Empty answer boxes for the first question.

ANSWER:

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

Selected answers for the first question:

- 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 NO: 6

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?

- A. Create a forms authentication provider, and then set the forms authentication credentials.

- B. From Active Directory Administrative Center, create a Password Setting object (PSO).
- C. 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.
- D. From Windows PowerShell, run the Set-ADDomain cmdlet, and then run the Set-ADAccountPassword cmdlet.

ANSWER: B

QUESTION NO: 7

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.

- A. Certificate Enrollment Policy Web Service
- B. Certificate Authority Web Enrollment
- C. Online Responder
- D. Certificate Enrollment Web Service
- E. Network Device Enrollment Service

ANSWER: A B

Explanation:

References:

https://www.ejbca.org/docs/Part_2_Microsoft_Certification_Authority_and_Group_Policies.html

QUESTION NO: 8

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.

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

ANSWER: A B D

QUESTION NO: 9

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?

- A. Remote Access Management on Server2
- B. Remote Access Management on Server1
- C. AD FS Management on Server2
- D. AD FS Management on Server1
- E. Routing and Remote Access on Server1

ANSWER: A

Explanation:

To publish a claims-based application

1. On the Web Application Proxy server, in the Remote Access Management console, in the Navigation pane, click Web Application Proxy, and then in the Tasks pane, click Publish.
2. On the Publish New Application Wizard, on the Welcome page, click Next.
3. On the Preauthentication page, click Active Directory Federation Services (AD FS), and then click Next.
4. On the Supported Clients page, select Web and MSOFBA, and then click Next.
5. On the Relying Party page, in the list of relying parties select the relying party for the application that you want to publish, and then click Next.
6. On the Publishing Settings page, do the following, and then click Next:
 - In the Name box, enter a friendly name for the application.
 - This name is used only in the list of published applications in the Remote Access Management console.
 - In the External URL box, enter the external URL for this application; for example, <https://sp.contoso.com/app1/>.
 - In the External certificate list, select a certificate whose subject covers the external URL.
 - In the Backend server URL box, enter the URL of the backend server. Note that this value is automatically entered when you enter the external URL and you should change it only if the backend server URL is different; for example, <http://sp/app1/>.
7. On the Confirmation page, review the settings, and then click Publish. You can copy the PowerShell command to set up additional published applications.
8. On the Results page, make sure that the application published successfully, and then click Close.

References:

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

QUESTION NO: 10

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?

- A. Run the Delegation of Control Wizard on the Computers container.
- B. Run the redircmp.exe command.
- C. Modify the Security settings of the technician's user account.
- D. Add the technician to the Windows Authorization Access group.

E. Configure the technician's user account as a manager service account.

F. Run the Set-ADComputer cmdlet.

G. Add the technician to the Domain Computers group.

ANSWER: A

Explanation:

References: <https://www.itprotoday.com/active-directory/delegating-privileges-active-directory>

QUESTION NO: 11 - (HOTSPOT)

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.

Hot Area:

Answer Area

First cmdlet to run:

	▼
Add-AdfsRelyingPartyTrust	
New-AdfsLdapServerConnection	
Set-AdfsEndpoint	

Second cmdlet to run:

	▼
Add-AdfsLocalClaimsProviderTrust	
Enable-AdfsRelyingPartyTrust	
Set-AdfsEndpoint	

ANSWER:

Answer Area

First cmdlet to run:

Add-AdfsRelyingPartyTrust
New-AdfsLdapServerConnection
Set-AdfsEndpoint

Second cmdlet to run:

Add-AdfsLocalClaimsProviderTrust
Enable-AdfsRelyingPartyTrust
Set-AdfsEndpoint

Explanation:

To configure your AD FSfarm 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 50000SslMode 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 L

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 NO: 12

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.

- A. Add Tech1 to the Group Policy Creator Owners group.
- B. From Group Policy Management, modify the Delegation settings of the TestOU OU.
- C. Add Tech1 to the Protected Users group.
- D. From Group Policy Management, modify the Delegation settings of the contoso.com container.
- E. Create a new universal security group and add Tech1 to the group.

ANSWER: A B

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 NO: 13

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 or repeated scenario.

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

What should you modify?

- A. Modify the Security settings of Group3.
- B. Modify the group scope of Group3.
- C. Modify the group type of Group3.
- D. Set Admin1 as the manager of Group3.
- E. Add Admin1 to the Enterprise Admins group

ANSWER: B

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 NO: 14

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.

- A. 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.
- B. Back up Cont_GPO1. In fabrikam.com, run the Restore-GPO cmdlet, and then run the New-GPLink cmdlet.
- C. Back up Cont_GPO1. In fabrikam.com run the Import-GPO cmdlet, and then run the New-GPLink cmdlet.
- D. Copy \\contoso.com\SysVol\contoso.com\Policies to \\fabrikam.com\SysVol\ fabrikam.com\Policies. In fabrikam.com, run the New-GPLink cmdlet.
- E. 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.

ANSWER: A C

QUESTION NO: 15 - (DRAG DROP)

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 DEFAULTSITELINK.

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.

Select and Place:

Actions

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.

Answer Area

ANSWER:

Actions

Create a new connection object.

Move the server object of the domain controller.

Answer Area

Create a new site object.

Create a new subnet object.

Promote the member server to a domain controller.