DUMPSBOSS.

Securing Windows Server 2016

Microsoft 70-744

Version Demo

Total Demo Questions: 15

Total Premium Questions: 208

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 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 sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You network contains an Active Directory forest named contoso.com. All domain controllers run Windows Server 2016. Member servers run either Windows Server 2012 R2 or Windows Server 2016. Client computers run either Windows 8.1 or Windows 10.

You need to ensure that when users access files in shared folders on the network, the files are encrypted when they are transferred over the network.

Solution: You disable SMB 1.0 on all the computers in the domain, and then you enable the Encrypt data access option on each file share.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

QUESTION NO: 2

You have a virtual machine named FS1 that runs Windows Server 2016.

FS1 has the shared folders shown in the following table.

Share name	Folder path
Users	D:\Users
CorpData	D:\Data
UserArchives	D:\Archives

You need to ensure that each user can store 10 GB of files in \\FS1\Users.

What should you do?

A. From File Explorer, open the properties of volume D, and then modify the Quota settings.

B. Install the File Server Resource Manager role service, and then create a file screen.

C. From File Explorer, open the properties of D:\Users, and then modify the Advanced sharing settings.

D. Install the File Server Resource Manager role service, and then create a quota.

ANSWER: D

Explanation:

References: https://docs.microsoft.com/en-us/windows-server/storage/fsrm/create-quota

QUESTION NO: 3 - (HOTSPOT)

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.

Your company has a marketing department.

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

Server name	Domain or workgroup	Configuration
Server1	Domain	Windows Server Update Services (WSUS) server
Server2	Domain	Server that has a Trusted Platform Module (TPM)
Server3	Domain	Member server that will be configured for Just Enough Administration (JEA)
Server4	Domain	Application server
Server5	Workgroup	Web server
VM1	Domain	Generation 2 virtual machine
VM2	Domain	DHCP server

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members. All laptops are protected by using BitLocker Drive Encryption (BitLocker).

You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers. An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1. A GPO named GP2 is linked to OU2.

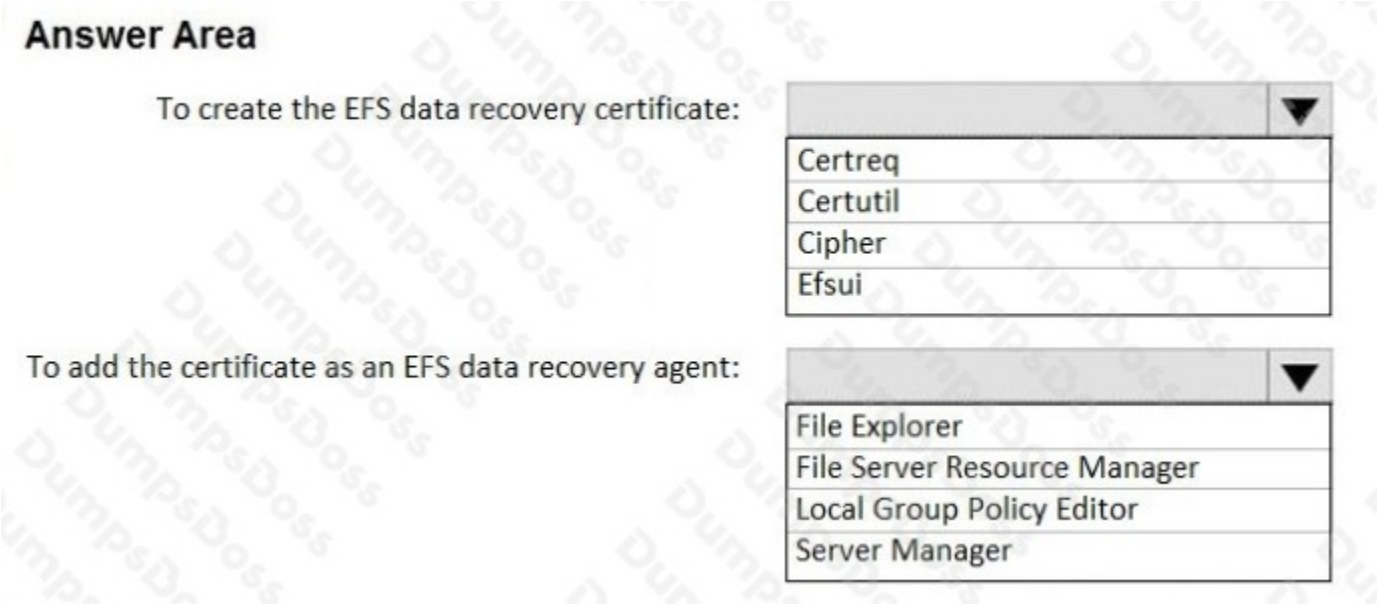
All computers receive updates from Server1. You create an update rule named Update1.

End of repeated scenario.

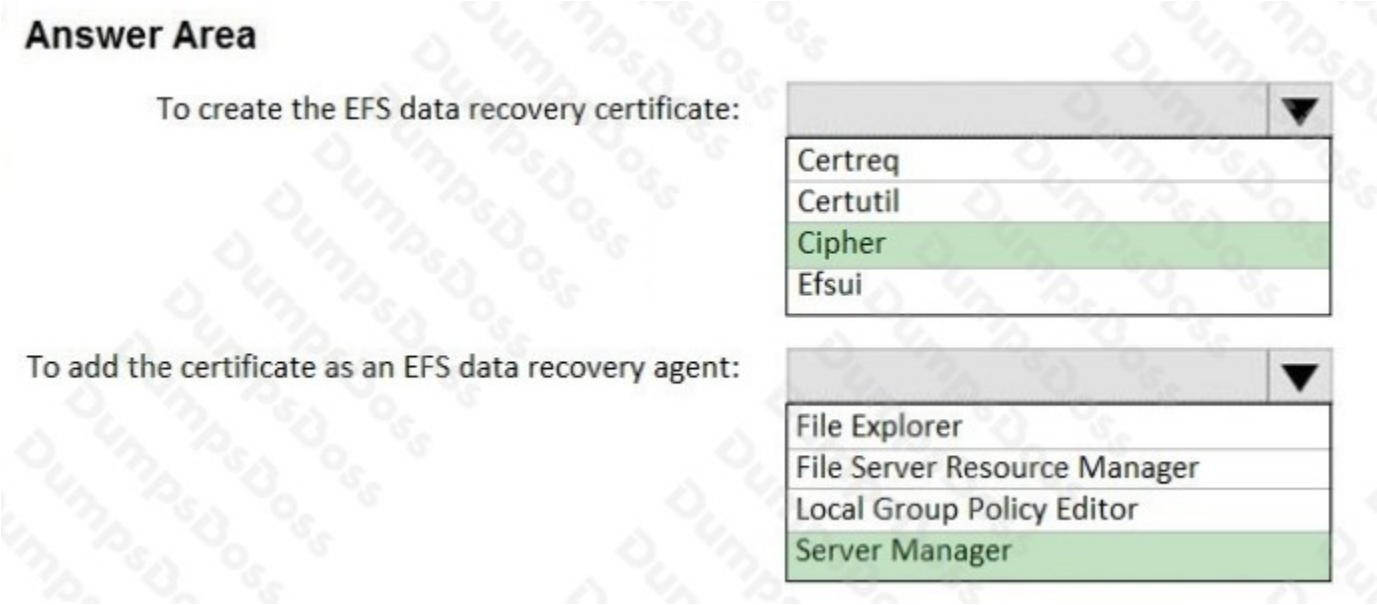
You need to create an Encrypting File System (EFS) data recovery certificate and then add the certificate as an EFS data recovery agent on Server5.

What should you use on Server5? To answer, select the appropriate options in the answer area.

Hot Area:



ANSWER:



Explanation:

References:

https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-and-verify-an-efs-dra-certificate https://www.rootusers.com/configure-efs-recovery-agent/

QUESTION NO: 4

Your network contains an Active Directory forest named contoso.com. The functional level of the forest and the domain is Windows Server 2012 R2.

You plan to use Local Administrator Password Solution (LAPS) for all member servers. You need to prepare the forest for LAPS.

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

NOTE: Each correct selection is worth one point.

A. Run the Set-AdmPwdComputerSelfPermission cmdlet.

B. Install the LAPS client-side extension on all domain controllers.

C. Run the Update-AdmPwdADSchema cmdlet.

D. Run the Set-AdmPwdAuditing cmdlet.

E. Deploy an enterprise certification authority (CA).

ANSWER: A C

Explanation:

References:

https://blog.thesysadmins.co.uk/deploying-microsoft-laps-part-1.html

QUESTION NO: 5

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 manage a file server that runs Windows Server 2016. The file server contains the volumes configured as shown in the following table.

Volume label	Volume letter	Size(TB)	Format
System	C	4	NTFS
HRFiles	H	8	NTFS
SalesFiles	J	8	ReFS
DevFiles	K	10	NTFS
BackUp	L	6	ReFS

You need to encrypt DevFiles by using BitLocker Drive Encryption (BitLocker).

Solution: You run the manage-bde.exe command and specify the –lock parameter.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

References:

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/manage-bde-lock

QUESTION NO: 6

Your network contains an Active Directory domain.

Microsoft Advanced Threat Analytics (ATA) is deployed to the domain.

A database administrator named DBA1 suspects that her user account was compromised.

Which three events can you identify by using ATA? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Domain computers into which DBA1 recently signed.

B. Phishing attempts that targeted DBA1.

C. The last time DBA1 experienced a failed logon attempt.

D. Spam messages received by DBA1.

E. Servers that DBA1 recently accessed.

ANSWER: A C E

Explanation:

References: https://github.com/MicrosoftDocs/ATADocs/blob/master/ATADocs/suspicious-activity-guide.md

QUESTION NO: 7

Your network contains an Active Directory Domain named contoso.com. The domain contains 10 servers that run Windows Server 2016 and 800 client computers that run Windows 10.

You need to configure the domain to meet the following requirements:

- Users must be locked out from their computer if they enter an incorrect password twice.
- Users must only be able to unlock a locked account by using a one-time password that is sent to their mobile phone.

You deploy all the components of Microsoft Identity Manager (MIM) 2016.

Which three actions should you perform before you deploy the MIM add-ins and extensions? Each correct answer presents part of the solution.

A. Deploy a Multi-Factor Authentication provider and copy the required certificates to the MIM server.

B. From a Group Policy object (GPO), configure Public Key Policies.

C. From the MIM Portal, configure the Owner Approval Workflow.

D. Deploy a Multi-Factor Authentication provider and copy the required certificates to the client computers.

E. From the MIM Portal, configure the Password Reset AuthN Workflow.

F. From a Group Policy object (GPO), configure Security Settings.

ANSWER: A E F

Explanation:

References: https://docs.microsoft.com/en-us/microsoft-identity-manager/working-with-self-service-password-reset

QUESTION NO: 8

Your network contains an Active Directory forest named contoso.com. The forest contains three domains. All domain controllers run Windows Server 2016.

You deploy a second Active Directory forest named admin.contoso.com. The forest contains a domain member server named Server1. Server1 has Microsoft Identity Manager (MIM) 2016 deployed.

You need to implement Privileged Access Management (PAM) and to use admin.contoso.com as an administrative forest.

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

A. From Server1, run the New-PAMTrust cmdlet.

B. From a domain controller in contoso.com, run the New-PAMDomainConfiguration cmdlet.

C. From a domain controller in admin.contoso.com, run the New-PAMTrust cmdlet.

D. From a domain controller in contoso.com, run the New-PAMTrust cmdlet.

E. From a domain controller in admin.contoso.com, run the New-PAMDomainConfiguration cmdlet.

F. From Server1, run the New- PAMDomainConfiguration cmdlet.

ANSWER: A F

Explanation:

References: https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/configuring-mim-environment-for-pam
https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/step-5-establish-trust-between-priv-corp-forests

QUESTION NO: 9

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 sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You network contains an Active Directory forest named contoso.com. All domain controllers run Windows Server 2016. Member servers run either Windows Server 2012 R2 or Windows Server 2016. Client computers run either Windows 8.1 or Windows 10.

You need to ensure that when users access files in shared folders on the network, the files are encrypted when they are transferred over the network.

Solution: You enable access-based enumeration on all the file shares.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

QUESTION NO: 10

Your network contains an Active Directory domain named contoso.com. The domain contains domain controllers that run Windows Server 2016.

The Job Title attribute for a domain user named User1 has a value of Sales Manager.

User1 runs whoami/claims and receives the following output.

USER CLAIMS INFORMATION				
Claim Name	Claim ID	Flags	Type	Values
"Country"	ad://ext/Country:88d469316297e518		String	"US"
Kerberos support for Dynamic Access Control on this device has been disabled.				

You need to ensure that the security token of User1 has a claim for Job Title.

What should you do?

A. From Active Directory Users and Computers, modify the properties of the User1 account.

B. From a Group Policy object(GPO), configure KDC support for claims, compound authentication, and Kerberos armoring.

C. From Active Directory Administrative Center, add a claim type.

D. From Windows PowerShell, run the New-ADClaimTransformPolicy cmdlet and specify the –Name parameter.

ANSWER: C

Explanation:

References: https://www.nyazit.com/how-to-configure-dynamic-access-control-in-windows-server-2012-r2-2/

QUESTION NO: 11 - (HOTSPOT)

HOTSPOT

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

You are deploying Microsoft Advanced Threat Analytics (ATA) to the domain. You install the ATA Gateway on a server named Server1.

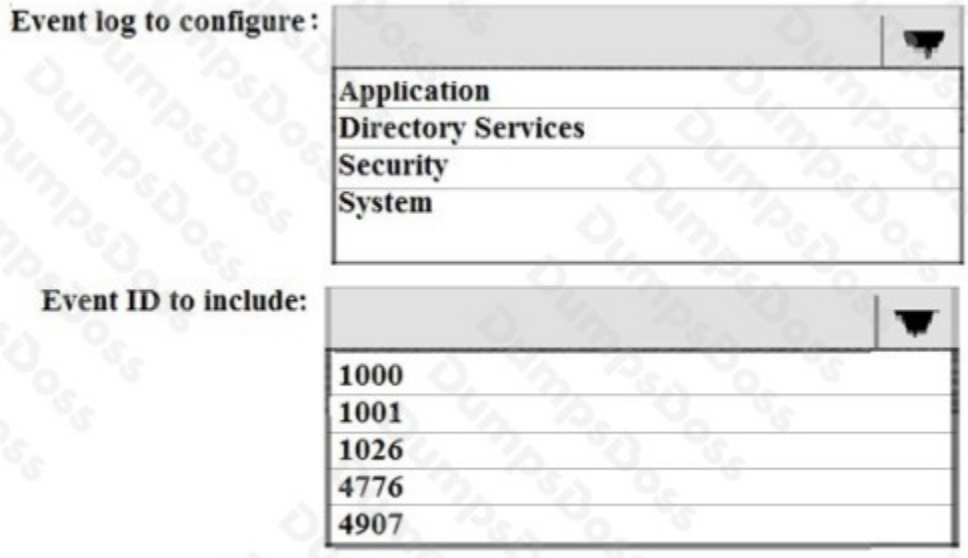
To assist in detecting Pass-the-Hash attacks, you plan to configure ATA Gateway to collect events.

You need to configure the query filter for event subscriptions on Server1.

How should you configure the query filter? To answer, select the appropriate options in the answer are.

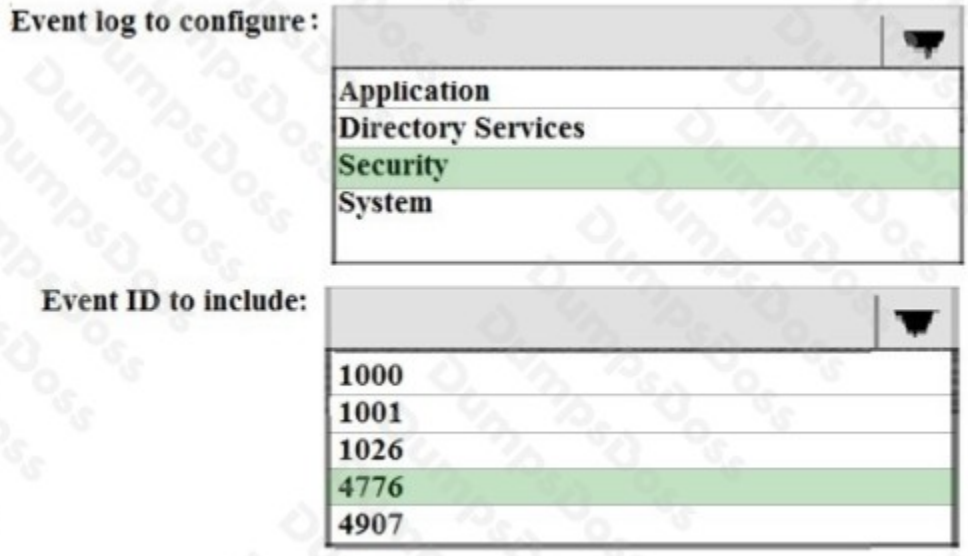
Hot Area:

Answer Area



ANSWER:

Answer Area



Explanation:

References: https://docs.microsoft.com/en-us/advanced-threat-analytics/configure-event-collection

QUESTION NO: 12

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.

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

The domain contains the servers configured as shown in the following table.

Server name	Configuration
Nano1	Nano Server
Nano2	Nano Server
Server2	File server that has a shared folder named DATA
Server3	DNS server that has a DNSSEC-signed zone named adatum.com
Server4	Hyper-V host
Server1	Application server

All servers run Windows Server 2016. All client computers run Windows 10.

You have an organizational unit (OU) named Marketing that contains the computers in the marketing department. You have an OU named Finance that contains the computers in the finance department. You have an OU named AppServers that contains application servers. A Group Policy object (GPO) named GP1 is linked to the Marketing OU. A GPO named GP2 is linked to the AppServers OU.

You install Windows Defender on Nano1.

You need to execute D:\Folder1 on Nano1 from being scanned by Windows Defender.

Which cmdlet should you run?

A. Set-StorageSetting

B. Set-FsrmFileScreenException

C. Set-MpPreference

D. Set-DtcAdvancedSetting

ANSWER: C

Explanation:

References: http://www.thomasmaurer.ch/2016/07/how-to-disable-and-configure-windows-defender-on-windows-server-2016-using-powershell/

QUESTION NO: 13

Your network contains an Active Directory domain named contoso.com. The domain contains 1,000 client computers that run Windows 8.1 and 1,000 client computers that run Windows 10.

You deploy a Windows Server Update Services (WSUS) server. You create a computer group for each organizational unit (OU) that contains client computers. You configure all of the client computers to receive updates from WSUS.

You discover that all of the client computers appear in the Unassigned Computers computer group in the Update Services console.

You need to ensure that the client computers are added automatically to the computer group that corresponds to the location of the computer account in Active Directory.

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

A. From Group Policy objects (GPOs), configure the Enable client-side targeting setting.

B. From the Update Services console, configure the Computers option.

C. From Active Directory Users and Computers, create a domain local distribution group for each WSUS computer group.

D. From Active Directory Users and Computers, modify the flags attribute of each OU.

ANSWER: A B

Explanation:

References:

https://technet.microsoft.com/en-us/library/dd252762.aspx https://technet.microsoft.com/en-us/library/cc720433(v=ws.10).aspx

QUESTION NO: 14

Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. The domain has Dynamic Access Control enabled.

Server1 contains a folder named C:\Folder1. Folder1 is shared as Share1.

You need to audit all access to the contents of Folder1 from Server2. The solution must minimize the number of event log entries.

Which two audit policies should you enable on Server1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Global Object Access- File System

B. Object Access – Audit Detailed File Share

C. Object Access – Audit Other Object Access Events

D. Object Access – Audit File System

E. Object Access – Audit File Share

ANSWER: B E

Explanation:

References:

https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-detailed-file-share
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-file-share

QUESTION NO: 15 - (DRAG DROP)

DRAG DROP

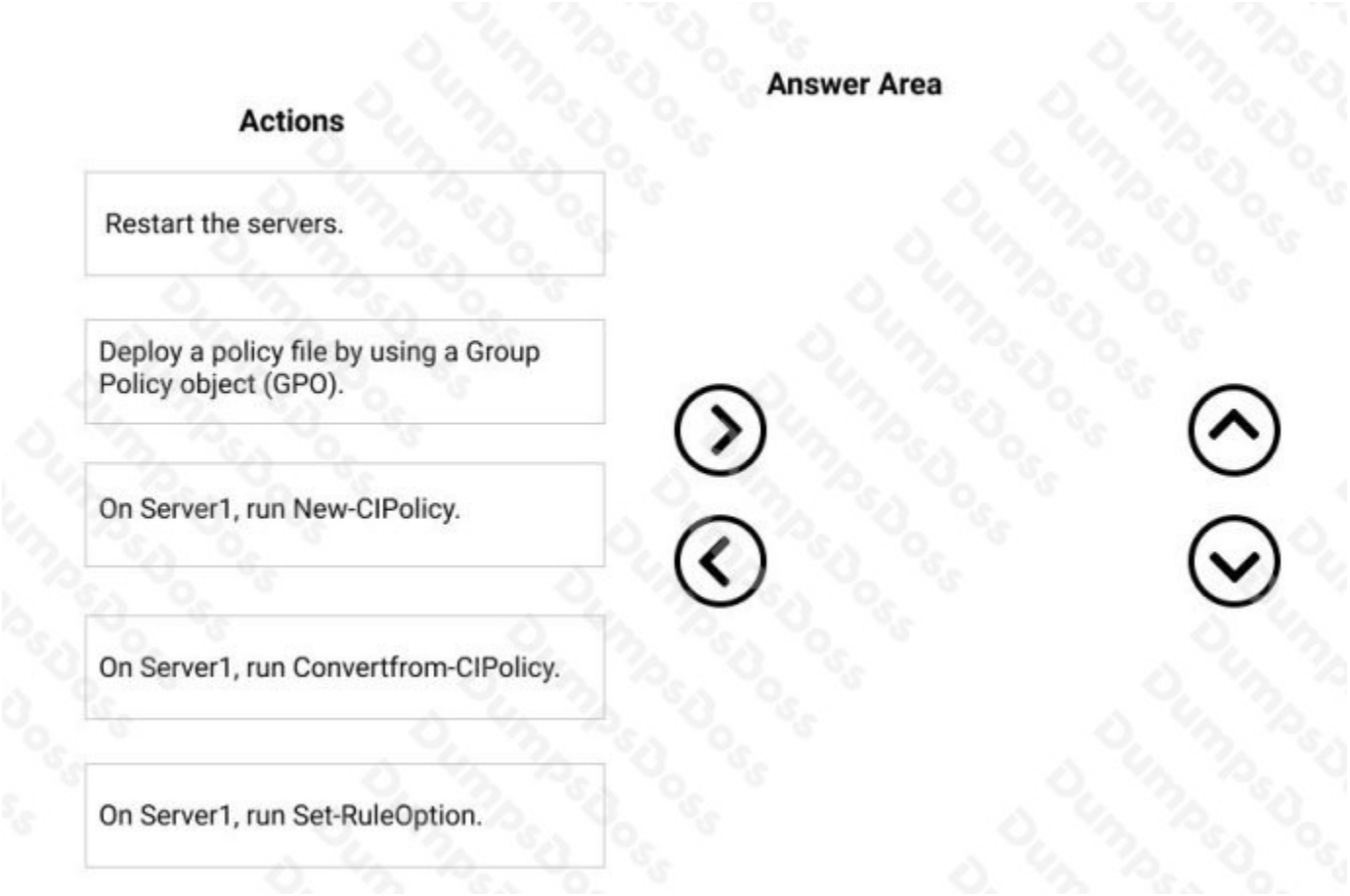
Your network contains an Active Directory domain named contoso.com. The domain functional level is Windows Server 2016. The domain contains a member server named Server1.

You test Code Integrity on Server1 in audit mode.

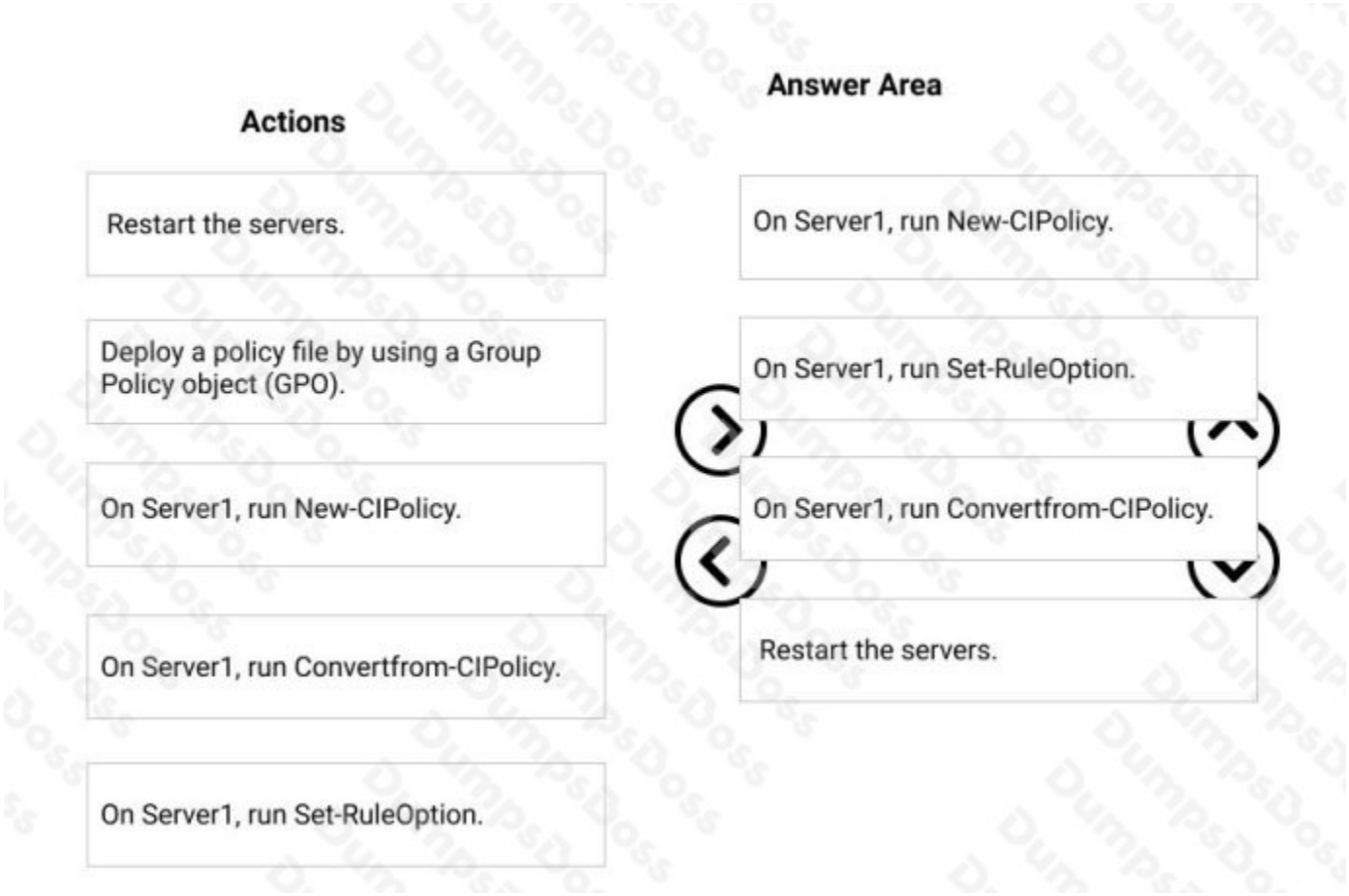
You need to enforce the Code Integrity levels on all the Windows Server 2016 servers in the domain.

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.

Select and Place:



ANSWER:



Explanation:

References: https://blogs.technet.microsoft.com/datacentersecurity/2018/03/10/default-code-integrity-policy-for-windows-server/