MCSA / MCSE for Windows Server 2016

Exam 70-744
Securing with Windows Server 2016

Version 13.25 (155 Questions)

Microsoft CERTIFIED
Solutions Associate
Windows Server 2016

Microsoft CERTIFIED
Solutions Expert
Cloud Platform and Infrastructure

(70-744) Securing Windows Server 2016

Microsoft CERTIFIED Solutions Expert Cloud Platform and Infrastructure

QUESTION 1
Note: This question is part of a series of question 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 file server named Server1 that runs Windows Server 2016.
Server1 has a volume named Volume1.
Dynamic Access Control is configured. A resource property named Property1 was created in the domain.
You need to ensure that Property1 is set to a value of Big for all of the files in Volume1 that are larger than 10 MB.
Which tool should you use?

A. File Explorer
B. Shared Folders
C. Server Manager
D. Disk Management
E. Storage Explorer
F. Computer Management
G. System Configuration
H. File Server Resource Manager (FSRM)

Answer: H
Explanation:
In FSRM, "Large Files" creates a list of files conforming to a specified file spec that are a specified size or larger.

QUESTION 2
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.
All servers run Windows Server 2016. The forest contains 2,000 client computers that run Windows 10.
All client computers are deployed (rom a customized Windows image.
You need to deploy 10 Privileged Access Workstations (PAWs).

The solution must ensure that administrators can access several client applications used by all users.
Solution: You deploy 10 physical computers and configure each wie as a virtualization host.
You deploy the operating system on each host by using the customized Windows image.
On each host you create a guest virtual machine and configure the virtual machine as a PAW.
Does this meet the goal?

A. Yes
B. No

Answer: B

QUESTION 3
Your network contains an Active Directory forest named contoso.com.
The forest functional level is Windows Server 2012.
All servers run Windows Server 2016. You create a new bastion forest named admin.contoso.com.
The forest functional level of admin.contoso.com is Windows Server 2012 R2.
You need to implement a Privileged Access Management (PAM) solution.
Which two actions should you perform? Each correct answer presents part of the solution.

A. Raise the forest functional level of admm.contoso.com.
B. Deploy Microsoft Identify Management (MIM) 2016 to admin.contoso.com.
C. Configure contoso.com to trust admin.contoso.com.
D. Deploy Microsoft Identity Management (MIM) 2016 to contoso.com.
E. Raise the forest functional level of contoso.com.
F. Configure admin.contoso.com to trust contoso.com.

Answer: B, C

QUESTION 4
Your network contains an Active Directory domain named conioso.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 tor 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 m 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.
E. From the Update Services console, run the WSUS Server Configuration Wizard.

Answer: A, B

QUESTION 5
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 server named Server1 that runs Windows Server 2016.
Server1 has a shared folder named Share1.
You need to encrypt the contents of Share1. Which tool should you use?

A. File Explorer
B. Shared Folders
C. Server Manager
D. Disk Management
E. Storage Explorer
F. Computer Management
G. System Configuration
H. File Server Resource Manager (FSRM)

Answer: H

QUESTION 6
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 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 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.

End of repeated scenario

You need to ensure that you can deploy a shielded virtual machine to Server4.
Which server role should you deploy?

A. Hyper-V
B. Device Health Attestation
C. Network Controller
D. Host Guardian Service

Answer: D
Explanation:
A guarded fabric consists of: 1 host guardian service (hgs)
1 or more guarded hosts (in this case Server4) A set of shielded VMs .
https://technet.microsoft.com/en-us/windows-server-docs/security/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vms

QUESTION 7
Your network contains an Active Directory domain named contoso.com.
The domain contains four servers.
The servers are configured as shown in the following table.

Server name	Configuration	Operating system
DC1	Domain controller	Windows Server 2012 R2
DC2	Domain controller	Windows Server 2012
FS1	File server	Windows Server 2016
FS2	File server	Windows Server 2012 R2

You need to manage FS1 and FS2 by using Just Enough Administration (JEA).
What should you do before you can implement JEA?

A. Install Microsoft .NET Framework 4.6.2 on FS2.
B. Install Microsoft .NET Framework 4.6.2 on FS1.
C. Install Windows Management Framework 5.0 on FS2.
D. Upgrade FS2 to Windows Server 2016.

Answer: C
Explanation:
JEA is incorporated into Windows Server 2016 and Windows 10, and is also incorporated into Windows Management Framework 5.0, which you can download and install on computers running Windows Server 2012 R2.

QUESTION 8
Your network contains an Active Directory domain named contoso.com.
You are deploying Microsoft Advanced Threat Analytics (ATA).
You create a user named User1.
You need to configure the user account of User1 as a Honeytoken account.
Which information must you use to configure the Honeytoken account?

A. the SAM account name of User1
B. the Globally Unique Identifier (GUID) of User1
C. the SID of User1
D. the UPN of User1

Answer: C
Explanation:
To configure a Honeytoken user you will need the SID of the user account, not the user name.
https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/working-with-detection-settings

QUESTION 9
Your network contains two single-domain Active Directory forests named contoso.com and contosoadmin.com. Contosoadmin.com contains all of the user accounts used to manage the servers in contoso.com. You need to recommend a workstation solution that provides the highest level of protection from vulnerabilities and attacks.

What should you include in the recommendation?

A. Provide a Privileged Access Workstation (PAW) for each user account in both forests.
Join each PAW to the contoso.com domain.
B. Provide a Privileged Access Workstation (PAW) for each user in the contoso.com forest.
Join each PAW to the contoso.com domain.
C. Provide a Privileged Access Workstation (PAW) for each administrator.
Join each PAW to the contoso.com domain.
D. Provide a Privileged Access Workstation (PAW) for each administrator.
Join each PAW to the contosoadmin.com domain.

Answer: D
Explanation:
Dedicated administrative forests allow organizations to host administrative accounts, workstations, and groups in an environment that has stronger security controls than the production environment.
https://technet.microsoft.com/windows-server-docs/security/securing-privileged-access/securing-privileged-access-reference-material#ESAE_BM

QUESTION 10
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario b 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 functional level of the forest and the domain is Windows Server 2008 R2.
The domain contains the servers configured as shown m 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 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.

End of repeated scenario

You need to disable SMB 1.0 on Server2. What should you do?

A. From File Server Resource Manager, create a classification rule.
B. From the properties of each network adapter on Server2. modify the bindings.
C. From Windows PowerShell, run the Set -SmbClientConfiguration cmdlet.
D. From Server Manager, remove a Windows feature.

Answer: D
Explanation:
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

QUESTION 11
Your network contains an Active Directory domain named contoso.com.
The domain contains 1,000 client computers that run Windows 10.
A security audit reveals that the network recently experienced a Pass-the-Hash attack.
The attack was initiated from a client computer and accessed Active Directory objects restricted to the members of the Domain Admins group.
You need to minimize the impact of another successful Pass-the-Hash attack on the domain.
What should you recommend?

A. Instruct all users to sign in to a client computer by using a Microsoft account.
B. Move the computer accounts of all the client computers to a new organizational unit (OU).
   Remove the permissions to the new OU from the Domain Admins group.
C. Instruct all administrators to use a local Administrators account when they sign in to a client computer.
D. Move the computer accounts of the domain controllers to a new organizational unit (OU).
   Remove the permissions to the new OU from the Domain Admins group.

Answer: B
Explanation:
Minimize the membership of privileged groups:
Minimize the number and type of computer that members of privileged groups are allowed to log on to.
For example:
1. Prevent members of the Domain Admins group form logging on to non-domain controllers
2. Prevent Local Administrators (and other local accounts with elevated permissions) from performing network log on

3. Prevent elevated accounts from logging on to any computers except the ones they need.
https://www.microsoft.com/security/sir/strategy/default.aspx#!pass_the_hash_defenses

QUESTION 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.

Start of repeated scenario

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 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.

End of repeated scenario

You need to exclude D:\Folder1 on Nano1 from being scanned by Windows Defender.
Which cmdlet should you run?

A. Set-StorageSett ing
B. Set-FsrmFileScreenException
C. Set-MpPreference
D. Set-DtcAdvancedSetting

Answer: C

Explanation:
-ExclusionPath: Specifies an array of file paths to exclude from scheduled and real-time scanning.
You can specify a folder to exclude all the files under the folder.
https://technet.microsoft.com/en-us/itpro/powershell/windows/defender/set-mppreference

QUESTION 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

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 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.

End of repeated scenario

You need to ensure that the marketing department computers validate DNS responses from adatum.com.
Which setting should you configure in the Computer Configuration node of GP1?

A. TCPIP Settings from Administrative Templates
B. Connection Security Rule from Windows Settings
C. DNS Client from Administrative Templates
D. Name Resolution Policy from Windows Settings

Answer: D

QUESTION 14
Note: This question is port 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 server named Server1 that runs Windows Server 2016 and a Nano Server named Nano1.
Nano1 has two volumes named C and D.
You are signed in to Server1.
You need to configure Data Deduplication on Nano1.
Which tool should you use?

A. File Explorer
B. Shared Folders
C. Server Manager
D. Disk Management
E. Storage Explorer
F. Computer Management
G. System Configuration
H. File Server Resource Manager (FSRM)

Answer: C
Explanation:
Enable Data Deduplication by using Server Manager
https://technet.microsoft.com/en-us/windows-server-docs/storage/data-deduplication/install-enable

QUESTION 15
Note: This question It 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 goats. 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 computer named Computer1 that runs Windows 10.
Computer1 connects to a home network and a corporate network.
The corporate network uses the 17216.0.0/24 address space internally.
Computer runs an application named App1 that listens to port 8080.
You need to prevent connections to App1 when Computer1 is connected to the home network.

Solution: From Group Policy Management you create a software restriction policy.
Does this meet the goal?

A. Yes
B. No

Answer: A

QUESTION 16
Your network contains an Active Directory domain named contoso.com.
The domain contains five file servers that run Windows Server 2016.
You have an organizational unit (OU) named Finance that contains all of the servers.
You create a Group Policy object (GPO) and link the GPO to the Finance OU.
You need to ensure that when a user in the finance department deletes a file from a file server, the event is logged.
The solution must log only users who have a manager attribute of Ben Smith.
Which audit policy setting should you configure in the GPO?

A. File system in Global Object Access Auditing
B. Audit Detailed File Share
C. Audit Other Account Logan Events
D. Audit File System in Object Access

Answer: B
Explanation:
This is why answer C is incorrect:
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/audit-other-account-logon-events
Correct Answer is B. Audit Detailed File Share generates this Event Log ID: 5145.
Source: https://technet.microsoft.com/en-us/itpro/windows/keep-secure/event-5145

QUESTION 17
Note: The 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 multiple Hyper-V hosts.
You need to deploy several critical line-of-business applications to the network to meet the following requirements:

- The resources of the applications must be isolated from the physical host
- Each application must be prevented from accessing the resources of the other applications.
- The configurations of the applications must be accessible only from the operating system that hosts the application.

Solution: You deploy one Windows container to host all of the applications.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
Isolation occurs at the container level. Multiple applications in the same container would share the same resources.
http://windowsitpro.com/windows-server-2016/differences-between-windows-containers-and-hyper-v-containers-windows-server-201

QUESTION 18
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 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 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.

End of repeated scenario

You plan to implement BitLocker Drive Encryption (BitLocker) on the operating system volumes of the application servers.
You need to ensure that the BitLocker recovery keys are stored in Active Directory.
Which Group Policy setting should you configure?

A. System cryptography; Force strong key protection (or user keys stored on the computer
B. Store BitLocker recovery information in Active Directory Domain Services (Windows Server 2008 and Windows Vista)
C. System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing
D. Choose how BitLocker-protected operating system drives can be recovered

Answer: B
Explanation:
Among the available answers, B is the only possible one. Though all servers are Windows 2016, the forest and domain are still in 2008 R2 mode.
https://technet.microsoft.com/en-us/library/dd875529(v=ws.10).aspx

QUESTION 19
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 servers run Windows Server 2016.
All client computers run Windows 10.
The relevant objects in the domain are configured as shown in the following table.

Server name	object	Organizational unit (OU) name
Server1	Computer account	Servers
Server2	Computer account	Servers
User1	User account	Operations Users

You need to assign User1 the right to restore files and folders on Server1, and Server2.
Solution: You add User1 to the Backup Operators group in contoso.com.
Does this meet the goal?

A. Yes
B. No

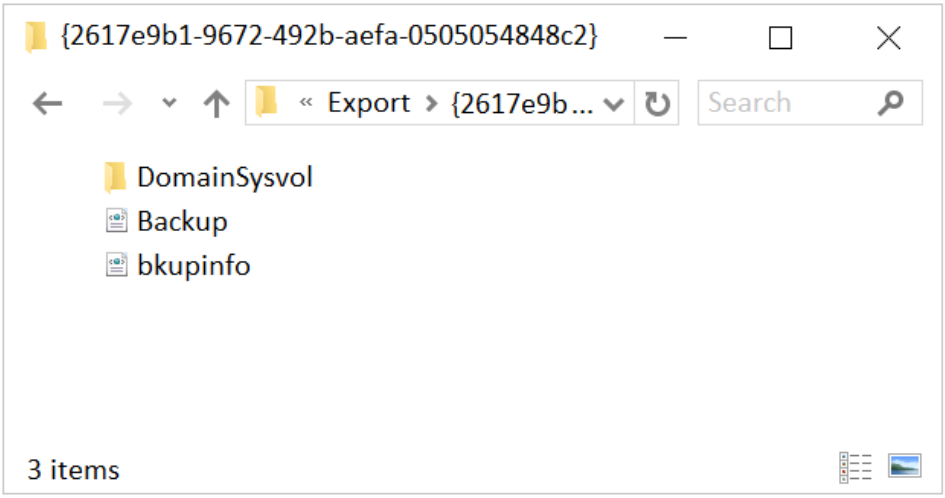
Answer: A

QUESTION 20
Your network contains an Active Directory domain named contoio.com.
The domain contains a server named Server1 that runs Windows Server 2016.
You have an organizational unit (OU) named Administration that contains the computer account of Server1.
You import the Active Directory module to Served1.
You create a Group Policy object (GPO) named GPO1. You link GPO1 to the Administration OU.
You need to log an event each time an Active Directory cmdlet is executed successfully from Server.
What should you do?

A. From Advanced Audit Policy in GPO1 configure auditing for directory service changes.
B. Run the (Get-Module ActiveDirectory).LogPipelineExecutionDetails - $false command.
C. Run the (Get-Module ArtivcDirectory).LogPipelineExecutionDetails = $true command.
D. From Advanced Audit Policy in GPO1 configure auditing for other privilege use events.

Answer: C

QUESTION 21
Your network contains an Active Directory domain named contoso.com.
All domain controllers run Windows Server 2016.
The domain contains a server named Server1 that has Microsoft Security Compliance Manager (SCM) 4.0 installed.
You export the baseline shown in the following exhibit.



You have a server named Server2 that is a member of a workgroup.
You copy the (2617e9b1-9672-492b-aefa-0505054848c2) folder to Server2.
You need to deploy the baseline settings to Server2.

What should you do?

A. Download, install, and then fun the Lgpo.exe command.
B. From Group Policy Management import a Group Policy object (GPO).
C. From Windows PowerShell, run the Restore-GPO cmdlet.
D. From Windows PowerShell, run the Import-GPO cmdlet.
E. From a command prompt run the secedit.exe command and specify the /import parameter.

Answer: A
Explanation:
Server2 is a non-domain joined computer using the GPO pack feature.
Source: https://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx
LGPO.exe replaces the no-longer-maintained Local GPO tool that shipped with the Security Compliance Manager (SCM).
https://biogs.technet.microsoft.com/secguide/2016/01/21/lgpo-exe-local-group-policy-object-utility-v1-0/