70-744.84q

Number: 70-744
Passing Score: 800
Time Limit: 120 min

70-744

Securing Windows Server 2016

Exam A

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 sections, 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/cc771990(v=ws.11).aspx

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 sections, 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 create a Group Policy object (GPO), link it to the Operations Users OU, and modify the Users Rights Assignment in the GPO.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/cc771990(v=ws.11).aspx

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 sections, 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 a separate Windows container for each application.

https://vceplus.com/ Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/virtualization/windowscontainers/about/

QUESTION 4
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.

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 a separate Hyper-V container for each application.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/virtualization/windowscontainers/about/

QUESTION 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 sections, 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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

References:

https://docs.microsoft.com/en-us/virtualization/windowscontainers/about/

QUESTION 6
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References:
https://en.wikipedia.org/wiki/Pass_the_hash#Mitigations

QUESTION 7
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 admin.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 trustcontoso.com.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/hardware-software-requirements https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/planning-bastion-environment

QUESTION 8
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 is configured as a domain controller.

You configure Server1 as a Just Enough Administration (JEA) endpoint. You configure the required JEA rights for a user named User1.

You need to tell User1 how to manage Active Directory objects from Server2.

What should you tell User1 to do first on Server2?

A. From a command prompt, runntdsutil.exe.
B. From Windows PowerShell, run the Import-Module cmdlet.
C. From Windows PowerShell, run the Enter-PSSession cmdlet.

D. Install the management consoles for Active Directory, and then launch Active Directory Users and Computers.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://blogs.technet.microsoft.com/privatecloud/2014/05/14/just-enough-administration-step-by-step/

QUESTION 9
Your network contains an Active Directory domain named contoso.com. The domain contains 100 servers.

You deploy the Local Administrator Password Solution (LAPS) to the network.

You deploy a new server named FinanceServer5, and join FinanceServer5 to the domain.

You need to ensure that the passwords of the local administrators of FinanceServer5 are available to the LAPS administrators.

What should you do?

A. On FinanceServer5, register AdmPwd.dll.
B. On FinanceServer5, install the LAPS Windows PowerShell module.
C. In the domain, modify the permissions for the computer account of FinanceServer5.
D. In the domain, modify the permissions of the Domain Controllers organizational unit (OU).

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://gallery.technet.microsoft.com/Step-by-Step-Deploy-Local-7c9ef772

QUESTION 10

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 DC1 to Windows Server 2016.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://blogs.technet.microsoft.com/privatecloud/2014/05/14/just-enough-administration-step-by-step/

QUESTION 11
Your network contains an Active Directory domain named contoso.com. The domain contains five servers. All servers run Windows Server 2016.

A new security policy states that you must modify the infrastructure to meet the following requirements: ▪
Limit the rights of administrators.
▪ Minimize the attack surface of the forest.
▪ Support Multi-Factor authentication for administrators.

You need to recommend a solution that meets the new security policy requirements.

What should you recommend deploying?

A. an administrative forest
B. domain isolation
C. an administrative domain in contoso.com
D. the Local Administrator Password Solution (LAPS)

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material#ESAE_BM

QUESTION 12
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.

Correct Answer: D
Section: (none)
Explanation

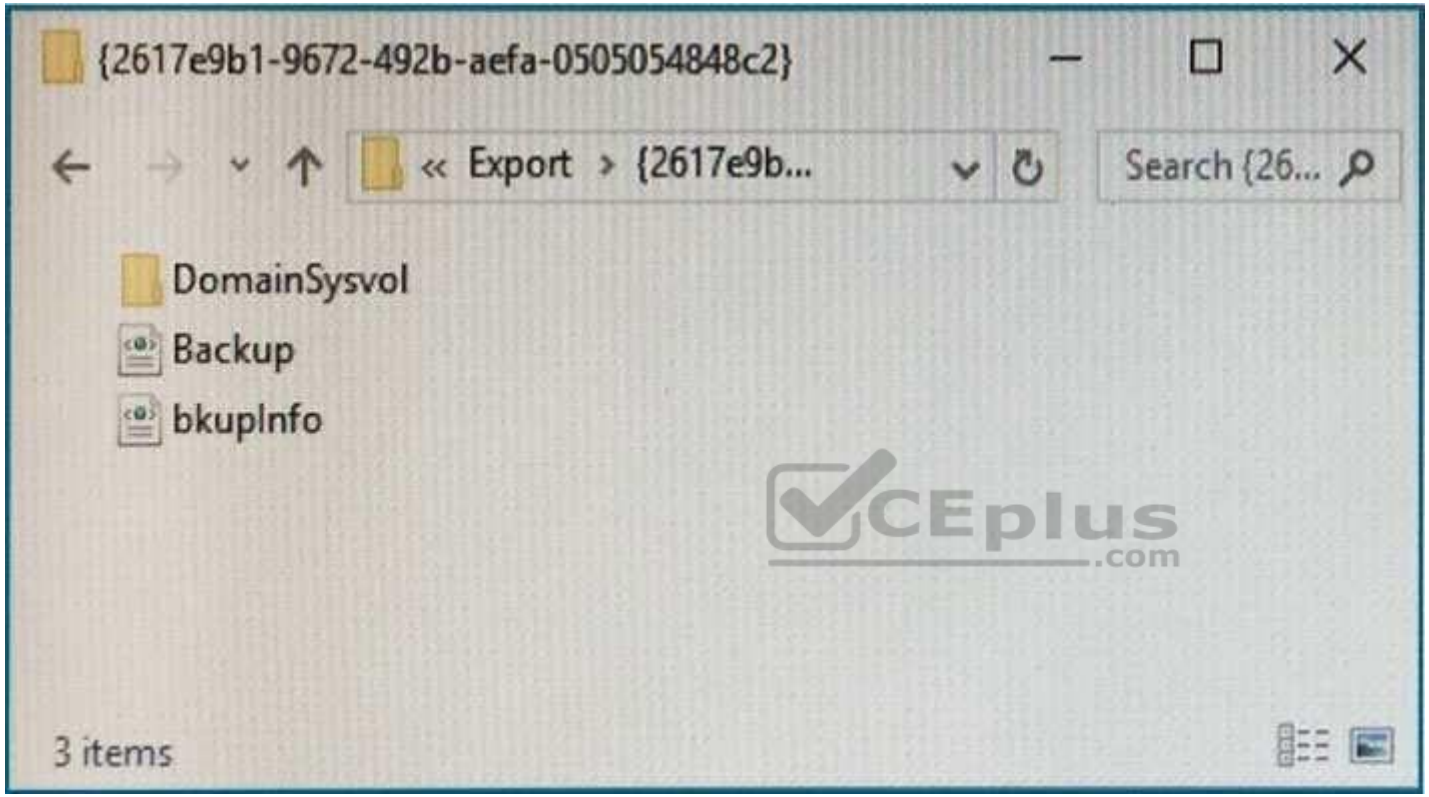
Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations

QUESTION 13
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 run 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://anytecho.wordpress.com/2015/05/22/importing-group-policies-using-powershell-almost/

QUESTION 14
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

A technician is testing the deployment of Credential Guard on Server1.

You need to verify whether Credential Guard is enabled on Server1.

What should you do?

A. From a command prompt, run the credwiz.exe command.
B. From Task Manager, review the processes listed on the Details tab.
C. From Server Manager, click Local Server, and review the properties of Server1.
D. From Windows PowerShell, run the Get-WsManCredSSP cmdlet.
E. From a command prompt, run the tsecimp.exe command.
F. From Control Panel, open **Credential Manager**, and review the list of Windows Credentials.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://yungchou.wordpress.com/2016/10/10/credential-guard-made-easy-in-windows-10-version-1607/

QUESTION 15
HOTSPOT

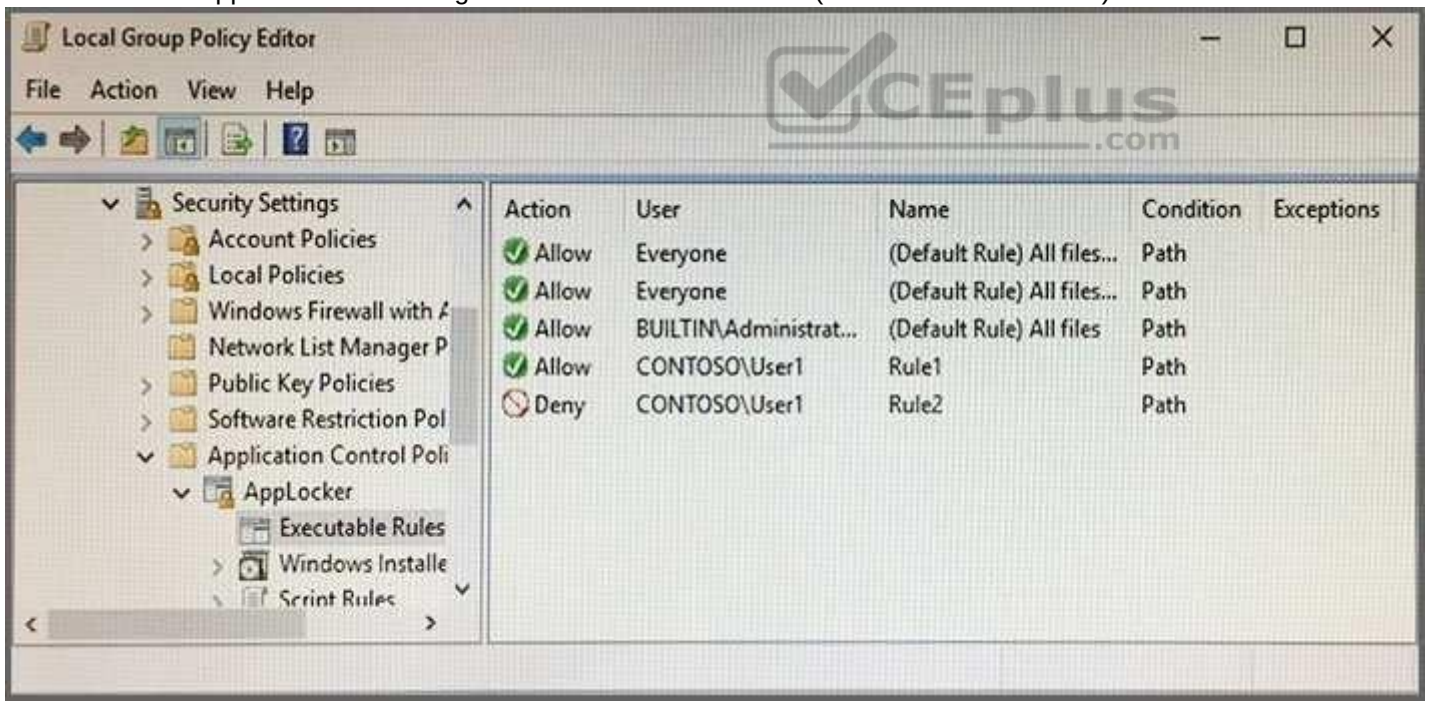
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

The services on Server1 are shown in the following output.

```
PS C:\> get-service *ap*

Status     Name               DisplayName
------     ----               -----------
Running    AppHostSvc         Application Host Helper Service
Stopped    AppIDSvc           Application Identity
Running    Appinfo            Application Information
Running    AppMgmt            Application Management
Running    AppReadiness       App Readiness
```

Server1 has the AppLocker rules configured as shown in the exhibit. (Click the Exhibit button.)

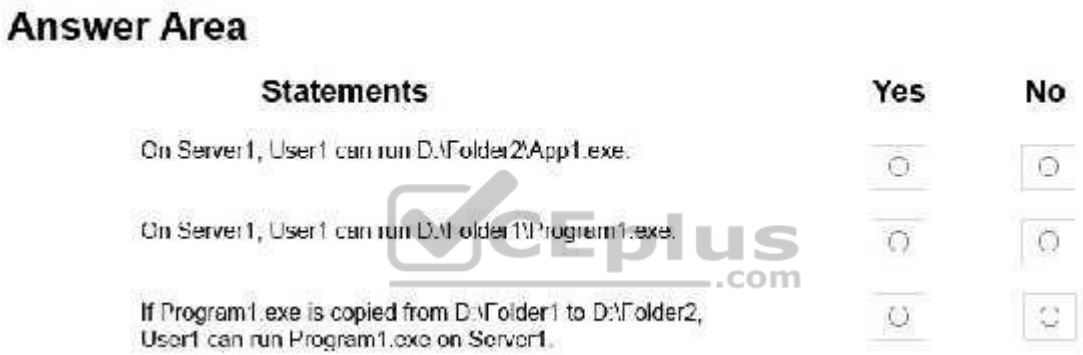


Rule1 and Rule2 are configured as shown in the following table.

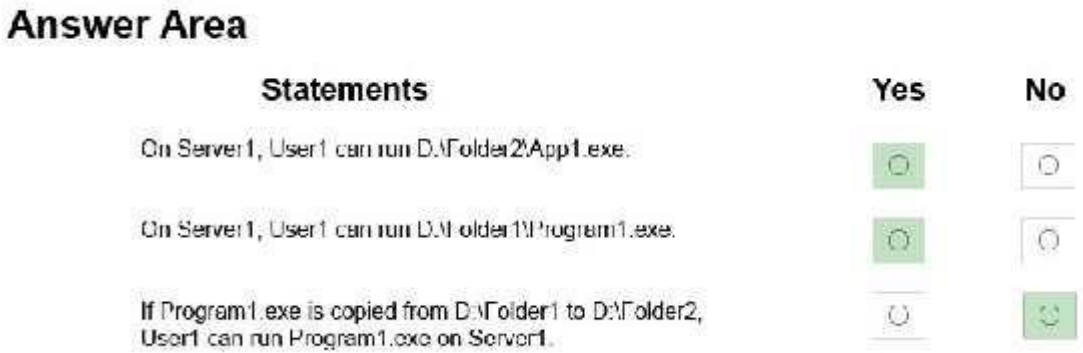
Rule name	Path
Rule1	D:\Folder1*.exe
Rule2	Pr*.*

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

Hot Area:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Your network contains an Active Directory domain named contoso.com.

You install the Windows Server Update Services server role on a member server named Server1. Server1 runs Windows Server 2016.

You need to ensure that a user named User1 can perform the following tasks:
▪ View the Windows Server Update Services (WSUS) configuration. ▪
Generate WSUS update reports.

The solution must use the principle of least privilege.

What should you do on Server1?

A. Modify the permissions of the ReportWebService virtual folder from the WSUS Administration website.
B. Add User1 to the WSUS Reporters local group.
C. Add User1 to the WSUS Administrators local group.
D. Run wsusutil.exe and specify the postinstall parameter.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/hh852346(v=ws.11).aspx#BKMK_ConfigComputerGroups

QUESTION 17
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server5 that has the Windows Server Update Services server role installed.

You need to configure Windows Server Update Services (WSUS) on Server5 to use SSL.

You install a certificate in the local Computer store.

Which two tools should you use? Each correct answer presents part of the solution.

A. Wsusutil
B. Netsh
C. Internet Information Services (IIS) Manager
D. Server Manager
E. Update Services

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/hh852346(v=ws.11).aspx#bkmk_3.5.ConfigSSL

QUESTION 18
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.

Correct Answer: AB
Section: (none)
Explanation
Explanation/Reference:
Explanation:

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

QUESTION 19
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 volume named Volume1.

A central access policy named Policy1 is deployed to the domain.

You need to apply Policy1 to Volume1.

https://vceplus.com/ 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)

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/deploy-a-central-access-policy--demonstration-steps-#BKMK_1.4

QUESTION 20
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 to 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)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://msdn.microsoft.com/en-us/library/dd163562.aspx

QUESTION 21
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 ensure that all access to Share1 uses SMB Encryption.

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)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://support.microsoft.com/en-za/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,windows-server-2008-r2,-windows-8,-and-windows-server-2012 https://blogs.technet.microsoft.com/filecab/2012/05/03/smb-3-security-enhancements-in-windows-server-2012/

QUESTION 22
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 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)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/hh831434(v=ws.11).aspx

QUESTION 23
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 file server named Server1 that runs Windows Server 2016.

You need to create Work Folders on Server1.

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)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References:
https://blogs.technet.microsoft.com/canitpro/2015/01/19/step-by-step-creating-a-work-folders-test-lab-deployment-in-windows-server-2012-r2/
https://technet.microsoft.com/en-us/library/dn265974(v=ws.11).aspx

QUESTION 24
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 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)

Correct Answer: H
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/cc732431(v=ws.11).aspx

QUESTION 25
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 26
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 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/ee649182(v=ws.10).aspx

QUESTION 27

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 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://blogs.technet.microsoft.com/datacentersecurity/2016/03/16/windows-server-2016-and-host-guardian-service-for-shielded-vms/

QUESTION 28
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 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://support.microsoft.com/en-za/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,windows-server-2008-r2,-windows-8,-and-windows-server-2012

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.

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 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 for 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.

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/jj679890(v=ws.11).aspx#BKMK_rec3

QUESTION 30
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/working-with-detection-settings

QUESTION 31
Your network contains an Active Directory domain named contoso.com.

You create a Microsoft Operations Management Suite (OMS) workspace.

You need to connect several computers directly to the workspace.

Which two pieces of information do you require? Each correct answer presents part of the solution.

A. the ID of the workspace
B. the name of the workspace
C. the URL of the workspace
D. the key of the workspace

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-windows-agents

QUESTION 32
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1.

Server1 is configured as shown in the following table.

Setting	Value
Domain	Contoso.com
IPv4 address	192.168.1.10
IPv6 link-local address	fe80::19a9:9e4c:87cd:12%13

You plan to create a pilot deployment of Microsoft Advanced Threat Analytics (ATA).

You need to install the ATA Center on Server1.

What should you do first?

A. Install Microsoft Security Compliance Manager (SCM).
B. Obtain an SSL certificate.
C. Assign an additional IPv4 address.D. Remove Server1 from the domain.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/install-ata-step1

QUESTION 33
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 Logon Events
D. Audit File System in Object Access

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/cc976403.aspx

QUESTION 34
Your network contains an Active Directory domain named contoso.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 Serve1.

You import the Active Directory module to Server1.

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 Server1.

What should you do?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://www.petri.com/enable-powershell-logging

QUESTION 35
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 Center on server named Server1 and the ATA Gateway on a server named Server2.

You need to ensure that Server2 can collect NTLM authentication events.

What should you configure?

A. the domain controllers to forward Event ID 4776 to Server2
B. the domain controllers to forward Event ID 1000 to Server1
C. Server2 to forward Event ID 1026 to Server1
D. Server1 to forward Event ID 1000 to Server 2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: http://winrook.blogspot.co.za/2015/12/configuring-windows-event-forwarding.html

QUESTION 36
Your network contains an Active Directory forest named contoso.com.

The network is connected to the Internet.

You have 100 point-of-sale (POS) devices that run Windows 10. The devices cannot access the Internet.

You deploy Microsoft Operations Management Suite (OMS).

You need to use OMS to collect and analyze data from the POS devices.

What should you do first?

A. Deploy Windows Server Gateway to the network.
B. Install the OMS Log Analytics Forwarder on the network.
C. Install Microsoft Data Management Gateway on the network.
D. Install the Simple Network Management Protocol (SNMP) feature on the devices.
E. Add the Microsoft NDIS Capture service to the network adapter of the devices.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://blogs.technet.microsoft.com/msoms/2016/03/17/oms-log-analytics-forwarder/

QUESTION 37
Your network contains an Active Directory forest named contoso.com. The forest functional level is Windows Server 2012. The forest contains a single domain. The domain contains multiple Hyper-V hosts.

You plan to deploy guarded hosts.

You deploy a new server named Server22 to a workgroup.

You need to configure Server22 as a Host Guardian Service server.

What should you do before you initialize the Host Guardian Service on Server22?

A. Install the Active Directory Domain Services server role on Server22.
B. Obtain a certificate.
C. Raise the forest functional level.
D. Join Server22 to the domain.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabric-prepare-for-hgs#prerequisites-for-the-host-guardianservice

QUESTION 38
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
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 deploy Windows Server 2016 to a server named Server1.

You need to ensure that you can run Windows Containers on Server1.

Solution: On Server1, you enable the Containers feature, and then you install the PowerShell for Docker module. You restart the server.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/virtualization/windowscontainers/deploy-containers/deploy-containers-on-server

QUESTION 41

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 deploy Windows Server 2016 to a server named Server1.

You need to ensure that you can run Windows Containers on Server1.

Solution: On Server1, you enable the Containers feature, and then you install the Hyper-V server role. You restart the server.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/virtualization/windowscontainers/deploy-containers/deploy-containers-on-server

QUESTION 42
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 deploy Windows Server 2016 to a server named Server1.

You need to ensure that you can run Windows Containers on Server1.

Solution: On Server1, you enable the Containers feature, and then you restart the server.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/virtualization/windowscontainers/deploy-containers/deploy-containers-on-server

QUESTION 43
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.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

You need to prevent NTLM authentication on Server1.

Solution: From a Group Policy, you configure the Security Options.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://www.rootusers.com/implement-ntlm-blocking-in-windows-server-2016/

QUESTION 44
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.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

You need to prevent NTLM authentication on Server1.

Solution: From Windows PowerShell, you run the **Disable-WindowsOptionalFeature** cmdlet.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://www.rootusers.com/implement-ntlm-blocking-in-windows-server-2016/

QUESTION 45
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.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

You need to prevent NTLM authentication on Server1.

Solution: From Windows PowerShell, you run the **New-ADAuthenticationPolicy** cmdlet.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://www.rootusers.com/implement-ntlm-blocking-in-windows-server-2016/

QUESTION 46

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 file server named Server1 that runs Windows Server 2016.

Server1 has a shared folder named Share1.

You plan to create a subfolder in Share1 for each domain user.

You need to limit each user to using 100 MB of data in their respective subfolder. The solution must enable the users to be notified when they use 80 percent of the available space in the subfolder.

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)

Correct Answer: H
Section: (none)
Explanation

Explanation/Reference:
References: https://4sysops.com/archives/file-server-resource-manager-fsrm-part-3-quota-management/

QUESTION 47
DRAG DROP

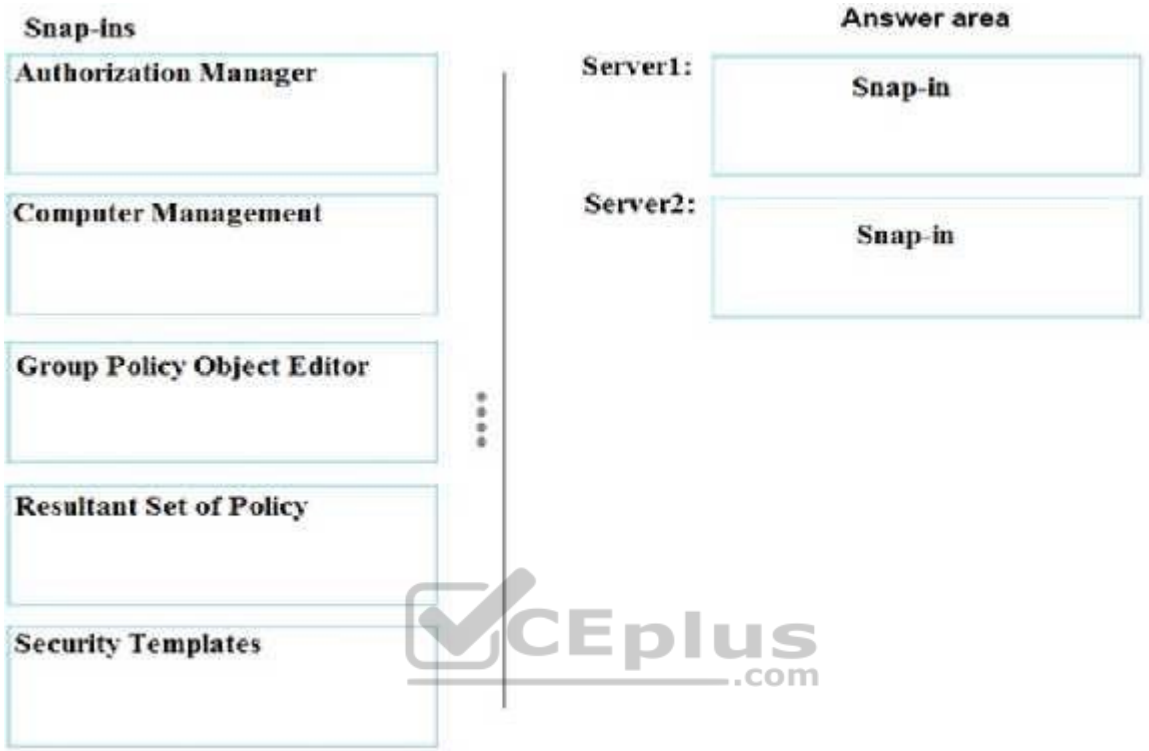
You have two servers named Server1 and Server2 that run Windows Server 2016. The servers are in a workgroup.

You need to create a security template that contains the security settings of Server1 and to apply the template to Server2. The solution must minimize administrative effort.

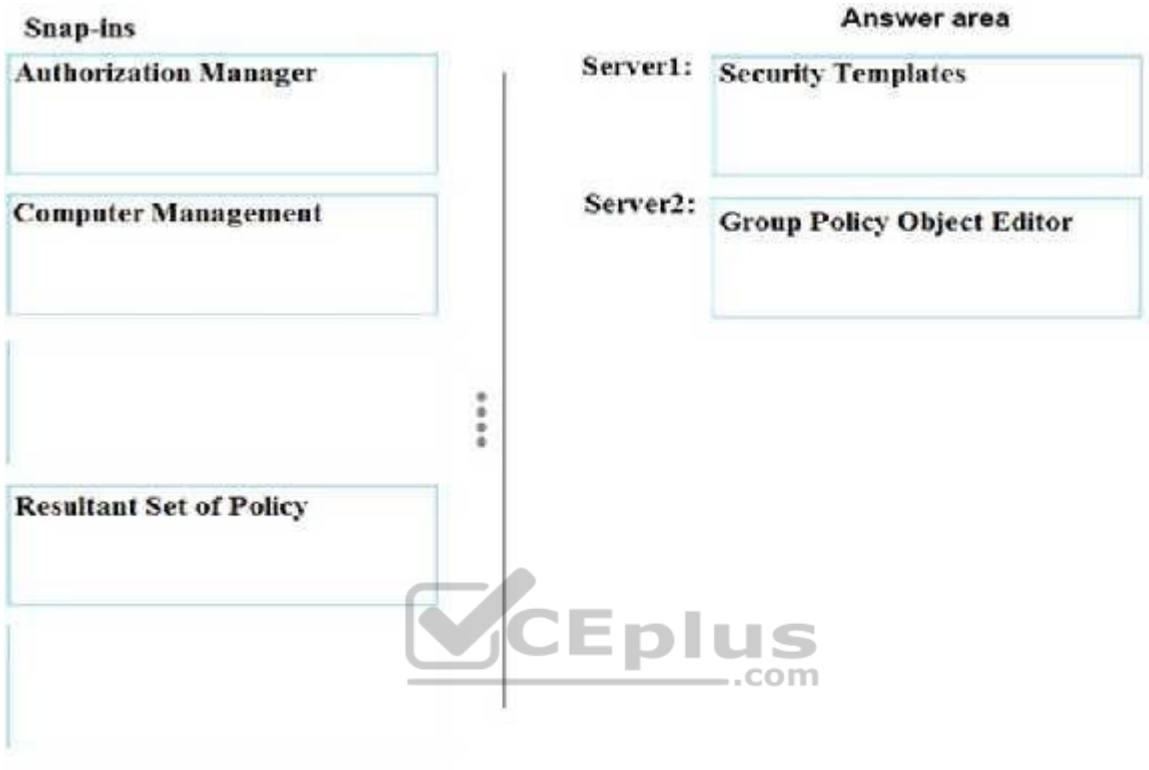
Which snap-in should you use for each server? To answer, drag the appropriate snap-ins to the correct servers. Each snap-in may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
References: https://www.windows-server-2012-r2.com/security-templates.html

QUESTION 48
You are creating a Nano Server image for the deployment of 10 servers.

You need to configure the servers as guarded hosts that use Trusted Platform Module (TPM) attestation.

Which three packages should you include in the Nano Server image? Each correct answer presents part of the solution.

A. Microsoft-NanoServer-SCVMM-Compute-Package

B. Microsoft-NanoServer-SecureStartup-Package
C. Microsoft-NanoServer-Compute-Package
D. Microsoft-NanoServer-ShieldedVM-Package
E. Microsoft-NanoServer-Storage-Package
F. Microsoft-NanoServer-SCVMM- Package

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/system-center/vmm/guarded-deploy-host?toc=/windows-server/virtualization/ https://docs.microsoft.com/en-us/windows-server/get-started/deploy-nano-server

QUESTION 49
Your network contains an Active Directory domain named contoso.com. The domain contains several shielded virtual machines.

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

You install the Hyper-V server role on Server1.

You need to ensure that you can host shielded virtual machines on Server1.

What should you install on Server1?

A. Host Guardian Hyper-V Support
B. the Windows Biometric Framework (WBF)
C. VM Shielding Tools for Fabric Management
D. BitLocker Network Unlock

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabricguarded-host-prerequisites

QUESTION 50
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 constoso.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 updated from Server1. You create an update rule named Update1.

End of repeated scenario.

You enable deep script block logging for Windows PowerShell.

In which event log will PowerShell code that is generated dynamically appear?

A. Applications and Services Logs/Windows PowerShell
B. Windows Logs/Security
C. Applications and Services Logs/Microsoft/Windows/PowerShell/Operational
D. Windows Logs/Application

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit_script

QUESTION 51
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 constoso.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 updated from Server1. You create an update rule named Update1.

End of repeated scenario.

You need to create a Role Capability file on Server3. Which file should you create?

A. File1.ini
B. File1.ps1
C. File1.xml
D. File1.psrc

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/jea/role-capabilities#create-a-role-capability-file

QUESTION 52
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 constoso.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 updated from Server1. You create an update rule named Update1.

End of repeated scenario.

You need to ensure that AppLocker rules will apply to the marketing department computers. What should you do?

A. From the properties of OU2, modify the COM+ partition Set.
B. In GP2, configure the Startup type for the Application Identity service.
C. In GP2, configure the Startup type for the Application Management service.
D. From the properties of OU2, modify the Security settings.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows/device-security/applocker/configure-the-application-identity-service

QUESTION 53
Your network contains an Active Directory domain named contoso.com. The domain contains a certification authority (CA).

You need to implement code integrity policies and sign them by using certificates issued by the CA.

You plan to use the same certificate to sign policies on multiple computers.

You duplicate the Code Signing certificate template and name the new template CodeIntegrity.

How should you configure the CodeIntegrity template?

A. Enable the Allow private key to be exported setting and modify the Key Usage extension.
B. Disable the Allow private key to be exported setting and modify the Application Policies extension.
C. Disable the Allow private key to be exported setting and disable the Basic Constraints extension.
D. Enable the Allow private key to be exported setting and enable the Basic Constraints extension

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References: https://blogs.technet.microsoft.com/ukplatforms/2017/05/04/create-code-integrity-signing-certificate/

QUESTION 54
Your network contains an Active Directory domain named contoso.com. The domain contains 100 servers.

You deploy the Local Administrator Password Solution (LAPS) to the network.

You discover that the members of a group named FinanceAdministartors can view the password of the local Administrator accounts on the servers in an organizational unit (OU) named FinanceServers.

You need to prevent the FinanceAdministartors members from viewing the local administrators 'passwords on the servers in FinanceServers. Which permission should you remove from FinanceAdministartors?

A. all extended rights
B. read all properties

C. read permissions
D. list contents

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://4sysops.com/archives/set-up-microsoft-laps-local-administrator-password-solution-in-active-directory/

QUESTION 55
Your network contains an Active Directory Domain named contoso.com. The domain contains 10 servers hat 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.

Correct Answer: AEF
Section: (none)
Explanation

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

QUESTION 56
You have a file server named FS1 that runs Windows Server 2016.

You plan to disable SMB 1.0 on the server.

You need to verify which computers access FS1 by using SMB 1.0.

 What should you run first?

A. **Debug-FileShare**
B. **Set-FileShare**
C. **Set-SmbShare**
D. **Set-SmbServerConfiguration**
E. **Set-SmbClientConfiguration**

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Your network contains an Active Directory domain named contoso.com. The domain contains domain controllers that run Windows Server 2016.

A Group Policy object (GPO) named GPO1 is applied to all of the domain controllers. GPO1 has a Globally Unique Identifier (GUID) of 6AC1786C-016F-11D2945F-00C04fB984F9.

You need to create a new baseline that contains the settings from GPO1.

What should you do first?

A. Copy the \\contoso.com\sysvol\contoso.com\Policies\{6AC1786C-016F-11D2-945F-00CO4fB984F9} folder to Server1.
B. From Group Policy Management, create a backup of GPO1.
C. From Microsoft Security Compliance Manager, associate a baseline.
D. From a command prompt, run the **secedit.exe** command and specify the */export* parameter.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://technet.microsoft.com/en-us/library/hh489604.aspx

QUESTION 58
You plan to enable Credential Guard on four servers. Credential Guard secrets will be bound to the TPM.

The servers run Windows Server 2016 and are configured as shown in the following table.

Server name	Trusted Platform Module (TPM) version	UEFI firmware version	Hypervisor installed	Platform
Server1	1.2	2.3.2	Hyper-V	Physical
Server2	2.0	2.3.1	Hyper-V	Physical
Server3	2.0	2.3.2	*None*	Physical
Server4	2.0	2.3.2	Hyper-V	Generation 2 virtual machine

You need to identify which server you must modify to support the planned implementation.

Which server should you identify?

A. Server1

B. Server2
C. Server3
D. Server4

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard-requirements **QUESTION 59** HOTSPOT

You manage a guarded fabric in TPM-trusted attestation mode.

You plan to create a virtual machine template disk for shielded virtual machines.

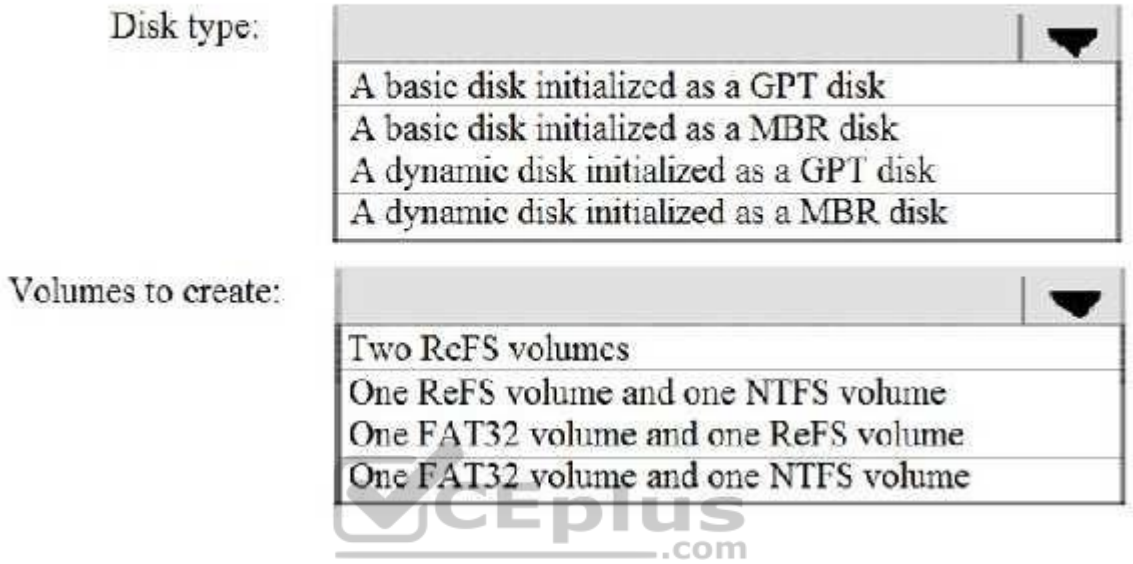
You need to create the virtual machine disk that you will use to generate the template.

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

NOTE: Each correct selection is worth one point.

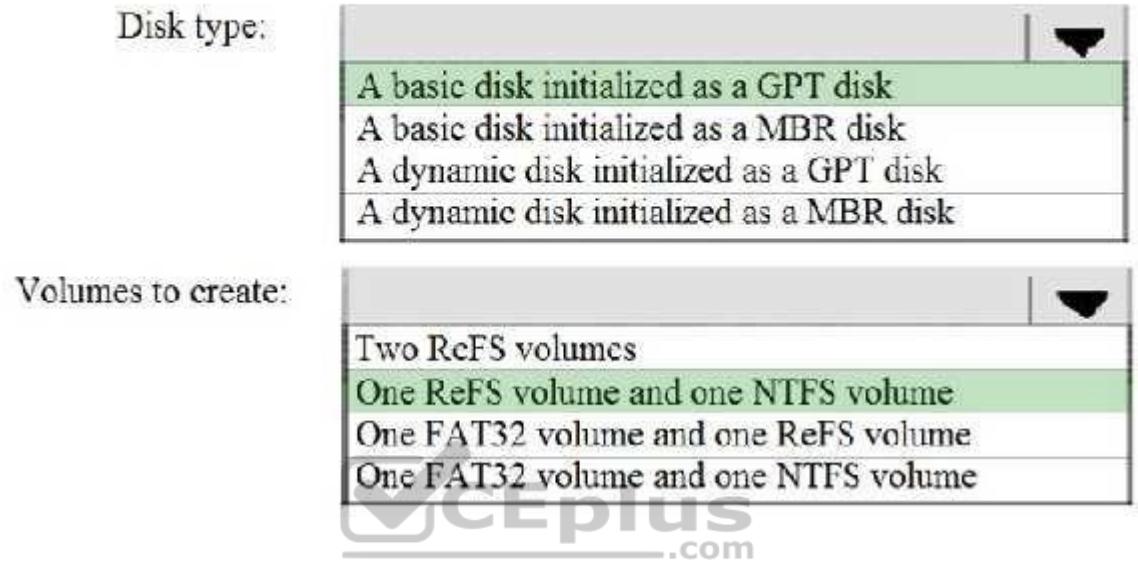
Hot Area:

Answer Area



Correct Answer:

Answer Area



Section: (none)
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabric-configuration-scenarios-for-shielded-vms-overview
https://docs.microsoft.com/en-us/system-center/dpm/what-s-new-in-dpm-2016?view=sc-dpm-1801

QUESTION 60
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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
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 61
You implement Just Enough Administration (JEA) on several file servers that run Windows Server 2016. The Role Capability file from a server named Server5 contains the following code.

```
VisibleCmdlets = 'Set-Acl',
@{
Name = 'Stop-Process"
Parameters = @{ Name = 'Name'; ValidateSet = 'proc' }
},
'SmbShare\Set-*'
'SmbShare\Get-*'
```

Which action can be performed by a user who connects to Server5?

A. View the NTFS permissions of any folder.
B. Stop any process.
C. Create a new file share.
D. Modify the properties of any share.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/jea/role-capabilities https://technet.microsoft.com/en-us/itpro/powershell/windows/smbshare/set-smbshare

QUESTION 62
Your network contains an Active Directory domain named contoso.com. The domain contains 10 computers that are in an organizational unit (OU) named OU1.

You deploy the Local Administrator Password Solution (LAPS) client to the computers. You link a Group Policy object (GPO) named GPO1 to OU1, and you configure the LAPS password policy settings in GPO1.

You need to ensure that the administrator passwords on the computers in OU1 are managed by using LAPS.

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

NOTE: Each correct selection is worth one point.

A. Enable LDAP encryption on the domain controllers.
B. Restart the computers.
C. Modify the permissions on OU1.
D. Restart the domain controller that hosts the PDC emulator role.
E. Update the Active Directory Schema.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
References: https://www.techrepublic.com/article/pro-tip-securing-windows-local-administrator-password-with-laps/

QUESTION 63
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.

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:
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-corpforests

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 sections, 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 Windows10.

The network uses the 172.16.0.0/16 address space.

Computer1 has an application named App1.exe that is located in D:\Apps\. App1.exe is configured to accept connections on TCP port 8080.

You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.

Solution: You run the **New-NetFirewallRule -DisplayName "Rule1" -Direction Inbound -LocalPort 8080 -Protocol TCP -Action Allow -Profile Domain** command.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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 sections, 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 Windows10.

The network uses the 172.16.0.0/16 address space.

Computer1 has an application named App1.exe that is located in D:\Apps\. App1.exe is configured to accept connections on TCP port 8080.

You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.

Solution: You configure an inbound rule that allows the TCP protocol on port 8080, uses a scope of 172.16.0.0/16 for local IP addresses, and applies to a private profile.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd448531(v=ws.10)

QUESTION 66
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.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

You need to prevent NTLM authentication on Server1.

Solution: From a Group Policy, you configure the Kerberos Policy.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://www.rootusers.com/implement-ntlm-blocking-in-windows-server-2016/

QUESTION 67
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 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 (ButLocker).

Solution: You run the **Lock-BitLocker** cmdlet.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/module/bitlocker/lock-bitlocker?view=win10-ps

QUESTION 68
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 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 (ButLocker).

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

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/manage-bde-on

QUESTION 69
You have a guarded fabric and a Host Guardian Service server named HGS1.

You deploy a Hyper-V host named Hyper1, and configure Hyper1 as part of the guarded fabric.

You plan to deploy the first shielded virtual machine.

You need to ensure that you can run the virtual machine on Hyper1.

What should you do?

A. On HGS1, run the **Export-HgsKeyProtectionState** cmdlet, and then run the **Import-HgsGuardian** cmdlet.

B. On Hyper1, run the **Invoke-WebRequest** cmdlet, and then run the **Import-HgsGuardian** cmdlet.
C. On the virtual machine, retrieve the metadata of the guarded fabric, and then import the metadata.
D. On Hyper1, run the **Export-HgsKeyProtectionState** cmdlet, and then run the **Import-HgsGuardian** cmdlet.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://blogs.technet.microsoft.com/datacentersecurity/2016/06/06/step-by-step-creating-shielded-vms-without-vmm/

QUESTION 70
You are building a guarded fabric.

You need to configure Admin-trusted attestation.

Which cmdlet should you use?

A. **Add-HgsAttestationHostGroup**
B. **Add-HgsAttestationTpmPolicy**
C. **Add-HgsAttestationTpmHost**
D. **Add-HgsAttestationCIPolicy**

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabric-add-host-information-for-admin-trustedattestation

QUESTION 71
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.

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows-server/storage/fsrm/create-quota

QUESTION 72
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.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 73
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.

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 74
Your network has an internal network and a perimeter network. Only the servers on the perimeter network can access the Internet. You create a Microsoft Operations Management Suite (OMS) instance in Microsoft Azure.

You deploy Microsoft Monitoring Agent to all the servers on both the networks.

You discover that only the servers on the perimeter network report to OMS.

You need to ensure that all the servers report to OMS.

What should you do?

A. Install a Web Application Proxy on the perimeter network and install an OMS Gateway on the internal network. Publish the OMS Gateway from the Web Application Proxy.
B. Install a Web Application Proxy and an OMS Gateway on the perimeter network. Publish the OMS Gateway from the Web Application Proxy.
C. Configure the network firewalls to allow the internal servers to access the IP addresses of the Azure OMS instance by using TCP port 443.
D. On the internal servers, run the **Add-AzureRmUsageConnect** cmdlet and specify the *–AdminUri* parameter.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-oms-gateway

QUESTION 75
You have a server named Server1 that runs Windows Server 2016.

You configure Just Enough Administration (JEA) on Server1.

You need to view a list of commands that will be available to a user named User1 when User1 establishes a JEA session to Server1.

Which cmdlet should you use?

A. **Get-PSSessionCapability**
B. **Trace-Command**
C. **Show-Command**

D. **Get-PSSessionConfiguration**

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/module/Microsoft.PowerShell.Core/get-pssessioncapability?view=powershell-6&viewFallbackFrom=powershell-5.0.

QUESTION 76
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.

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

You need to identify the default action for the inbound traffic when Server1 connects to the domain.

Which cmdlet should you use?

A. **Get-NetIPSecRule**
B. **Get-NetFirewallRule**
C. **Get-NetFirewallProfile**
D. **Get-NetFirewallSetting**
E. **Get-NetFirewallPortFilter**
F. **Get-NetFirewallAddressFilter**
G. **Get-NetFirewallSecurityFilter**
H. **Get-NetFirewallApplicationFilter**

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/module/netsecurity/get-netfirewallprofile?view=win10-ps

QUESTION 77
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.

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

You need to identify whether any connection security rules are configured on Server1.

Which cmdlet should you use?

A. **Get-NetIPSecRule**
B. **Get-NetFirewallRule**
C. **Get-NetFirewallProfile**
D. **Get-NetFirewallSetting**
E. **Get-NetFirewallPortFilter**
F. **Get-NetFirewallAddressFilter**
G. **Get-NetFirewallSecurityFilter**
H. **Get-NetFirewallApplicationFilter**

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/module/netsecurity/get-netipsecrule?view=win10-ps

QUESTION 78
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.

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

You need to identify whether ICMP traffic is exempt from IPsec on Server1.

Which cmdlet should you use?

A. **Get-NetIPSecRule**
B. **Get-NetFirewallRule**
C. **Get-NetFirewallProfile**
D. **Get-NetFirewallSetting**
E. **Get-NetFirewallPortFilter**
F. **Get-NetFirewallAddressFilter**
G. **Get-NetFirewallSecurityFilter**
H. **Get-NetFirewallApplicationFilter**

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/module/netsecurity/get-netfirewallsetting?view=win10-ps

QUESTION 79
Your company has an accounting department.

The network contains an Active Directory domain named contoso.com. the domain contains 10 servers.

You deploy a new server named Server11 that runs Windows Server 2016. Server11 will host several network applications and network shares used by the accounting department.

You need to recommend a solution for Server11 that meets the following requirements:

- Protects Server11 from address spoofing and session hijacking
- Allows only the computers in the accounting department to connect to Server11 What

should you recommend implementing?

A. Just Enough Administration (JEA)
B. AppLocker rules
C. Privileged Access Management (PAM)
D. connection security rules

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
References: https://support.microsoft.com/en-us/help/942957/security-rules-for-windows-firewall-and-for-ipsec-based-connections-in

QUESTION 80
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 computer named Computer1 that runs Windows10.

The network uses the 172.16.0.0/16 address space.

Computer1 has an application named App1.exe that is located in D:\Apps\. App1.exe is configured to accept connections on TCP port 8080.

You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.

Solution: You configure an inbound rule that allows the TCP protocol on port 8080 and applies to all profiles.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
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 contain 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 172.16.0.0/24 address space internally.

Computer1 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 Windows Firewall with Advanced Security, you create an inbound rule.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd421709(v=ws.10)#what-is-an-inbound-rule

QUESTION 82
You have a Hyper-V host named Hyper1 that has a virtual machine named FS1. FS1 is a file server that contains sensitive data.

You need to secure FS1 to meet the following requirements:

- Prevent console access to FS1.
- Prevent data from being extracted from the VHDX file of FS1.

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

NOTE: Each correct selection is worth one point.

A. Disable all the Hyper-V integration services for FS1.
B. On Hyper1, enable BitLocker Drive Encryption (BitLocker) for the drive that contains the VHDX file for FS1.
C. Disable the virtualization extensions for FS1.
D. Enable shielding for FS1.

E. Enable BitLocker Drive Encryption (BitLocker) for all the volumes on FS1.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vms

QUESTION 83
You deploy the Host Guardian Service (HGS).

You have several Hyper-V that have older hardware and Trusted Platform Modules (TPMs) version 1.2.

You discover that the Hyper-V hosts cannot start shielded virtual machines.

You need to configure HGS to ensure that the older Hyper-V hosts can host shielded virtual machines.

What should you do?

A. Run the **Set-HgsServer** cmdlet and specify the **–TrustActiveDirectory** parameter.
B. Run the **Clear-HgsServer** cmdlet and specify the **–Clustername** parameter.
C. Run the **Clear-HgsServer** cmdlet and specify the **–Force** parameter.
D. Run the **Set-HgsServer** cmdlet and specify the **–TrustTpm** parameter.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References:
https://blogs.technet.microsoft.com/datacentersecurity/2016/03/16/windows-server-2016-and-host-guardian-service-for-shielded-vms/
https://docs.microsoft.com/en-us/powershell/module/hgsserver/set-hgsserver?view=win10-ps

QUESTION 84
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 Microsoft Advanced Threat Analytics (ATA) Center service is installed on Server1.

The domain contains the users shown in the following table.

Name	Group membership
User1	Contoso\Server Operators
User2	Contoso\Key Admins
User3	Server1\Administrators
User4	Server1\Network Configuration Operators
User5	Server1\Power Users
User6	Server1\Microsoft Advanced Threat Analytics Administrators
User7	Server1\Microsoft Advanced Threat Analytics Users
User8	Server1\Microsoft Advanced Threat Analytics Viewers

You are installing ATA Gateway on Server2.

You need to specify a Gateway Registration account.

Which account should you use?

A. User8
B. User5
C. User7
D. User3

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/advanced-threat-analytics/install-ata-step1

https://vceplus.com/