Microsoft

Exam Questions 70-744

Securing Windows Server 2016

NEW QUESTION 1
Note: The question is part of a series of questions th« 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 from 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 them as PAWs. You deploy 10 additional computers and configure them by using the customized Windows image.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
References:
https://technet.microsoft.com/en-us/windows-server-docs/security/securing-privilegedaccess/privileged-access-workstations

NEW 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#W 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 will 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

Explanation:
References:
https://technet.microsoft.com/en-us/windows-server-docs/security/securing-privilegedaccess/privileged-access-workstations

NEW QUESTION 3
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question In this section, you will NOT be able to return to It. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The 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 in the Control Panel, you add an application and allow the application to communicate through the firewall on a Private network.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
References:
http://www.online-tech-tips.com/windows-10/adjust-windows-10-firewall-settings/

NEW 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 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 create a Group Policy object (GPO), you link the GPO to the Servers OU, and then you modify the Users Rights Assignment in the GPO.

Does this meet the goat?

A. Yes
B. No

Answer: B

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

NEW 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. 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

Explanation:
References:
https://technet.microsoft.com/en-us/library/cc771990(v=ws.11).aspx users.
The solution would let User1 to backup files and folders on domain controllers for contoso.com instead.

NEW QUESTION 6
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 multiple Hyper-V hosts.
You need to deploy several critical line-to-business applications to the network to meet the following requirements:
*The resources of the applications must be isolated (rom 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

Answer: A

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

NEW QUESTION 7
Note: Thb 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 willNOTbeabletorrturntoit.Asa 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:
References:
https://docs.microsoft.com/en-us/virtualization/windowscontainers/about/

NEW QUESTION 8
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: C

Explanation:
https://docs.microsoft.com/en-us/windows/access-protection/remote-credential-guard

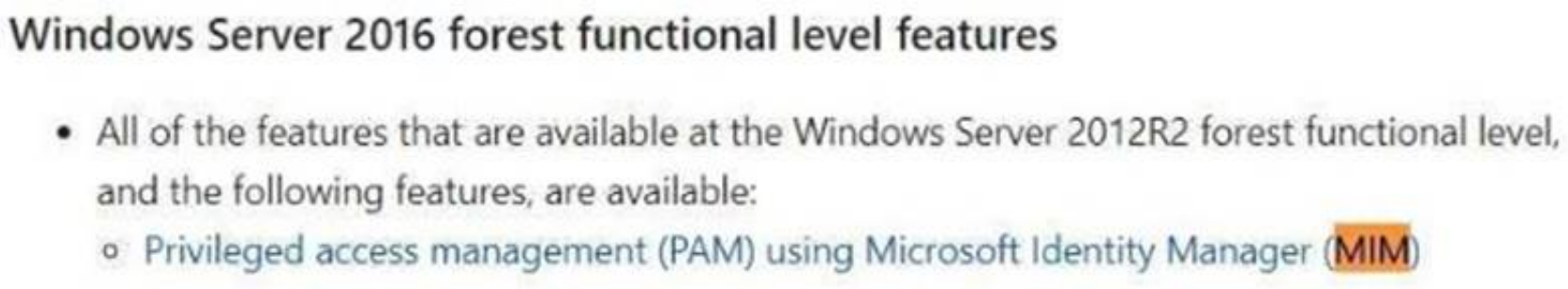
Feature	Remote Desktop	Windows Defender Remote Credential Guard	Restricted Admin mode
Protection benefits	Credentials on the server are not protected from Pass-the-Hash attacks.	User credentials remain on the client. An attacker can act on behalf of the user *only* when the session is ongoing	User logs on to the server as local administrator, so an attacker cannot act on behalf of the "domain user". Any attack is local to the server
Version support	The remote computer can run any Windows operating system	Both the client and the remote computer must be running **at least Windows 10, version 1607, or Windows Server 2016**.	The remote computer must be running **at least patched Windows 7 or patched Windows Server 2008 R2**. For more information about patches (software updates) related to Restricted Admin mode, see Microsoft Security Advisory 2871997.
Helps prevent	N/A	• Pass-the-Hash • Use of a credential after disconnection	• Pass-the-Hash • Use of domain identity during connection
Credentials supported from the remote desktop client device	• **Signed on** credentials • **Supplied** credentials • **Saved** credentials	• **Signed on** credentials only	• **Signed on** credentials • **Supplied** credentials • **Saved** credentials

NEW QUESTION 9
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.co

Answer: DE

Explanation:
https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/deploy-pam-with-windowsserver- 2016
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/windows-server-2016-functionallevels



For the bastion forest which deploys MIM, you should raise the Forest Functional Level to “Windows Server 2016?

NEW QUESTION 10
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 FinanceServerS 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 FinanceServerS, register AdmPwd.dll.
B. On FmanceServerS, install the LAPS Windows PowerShell module.
C. In the domain, modify the permissions for the computer account of FmanceServer5.
D. In the domain, modify the permissions of the Domain Controllers organizational unit (OU).

Answer: A

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

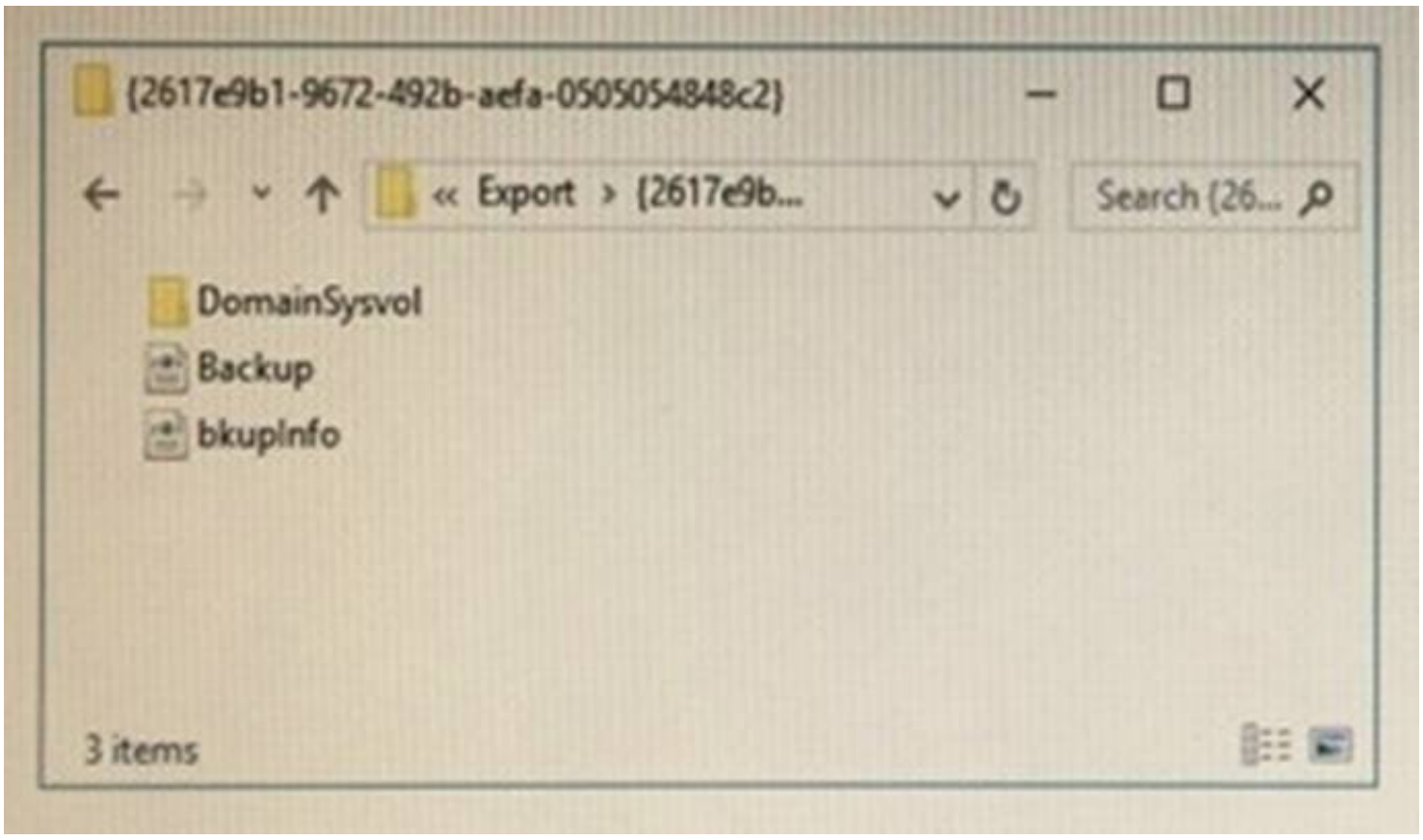
NEW QUESTION 10
Your network contains an Active Directory domain named contoso.com. The domain contains five servers. All servers run Windows Server 2016.
A new secunty policy states that you must modify the infrastructure to meet the following requirements:
*Limit the nghts of administrators.
*Minimize the attack surface of the forest
*Support Multi-Factor authentication for administrators.
You need to recommend a solution that meets the new secunty 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)

Answer: A

Explanation:
You have to “-Minimize the attack surface of the forest”, then you must create another forest for administrators.
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securingprivilegedaccess- reference-material#ESAE_BM
This section contains an approach for an administrative forest based on the Enhanced Security Administrative
Environment (ESAE) reference architecture deployed
by Microsoft’s cybersecurity professional services teams to protect customers against cybersecurity attacks.
Dedicated administrative forests allow organizations to host administrative accounts, workstations, and groups in an environment that has stronger security controls than the production environment.

NEW QUESTION 14
Vout network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2016.
The domain contains a server named Serverl 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 paramete

Answer: D

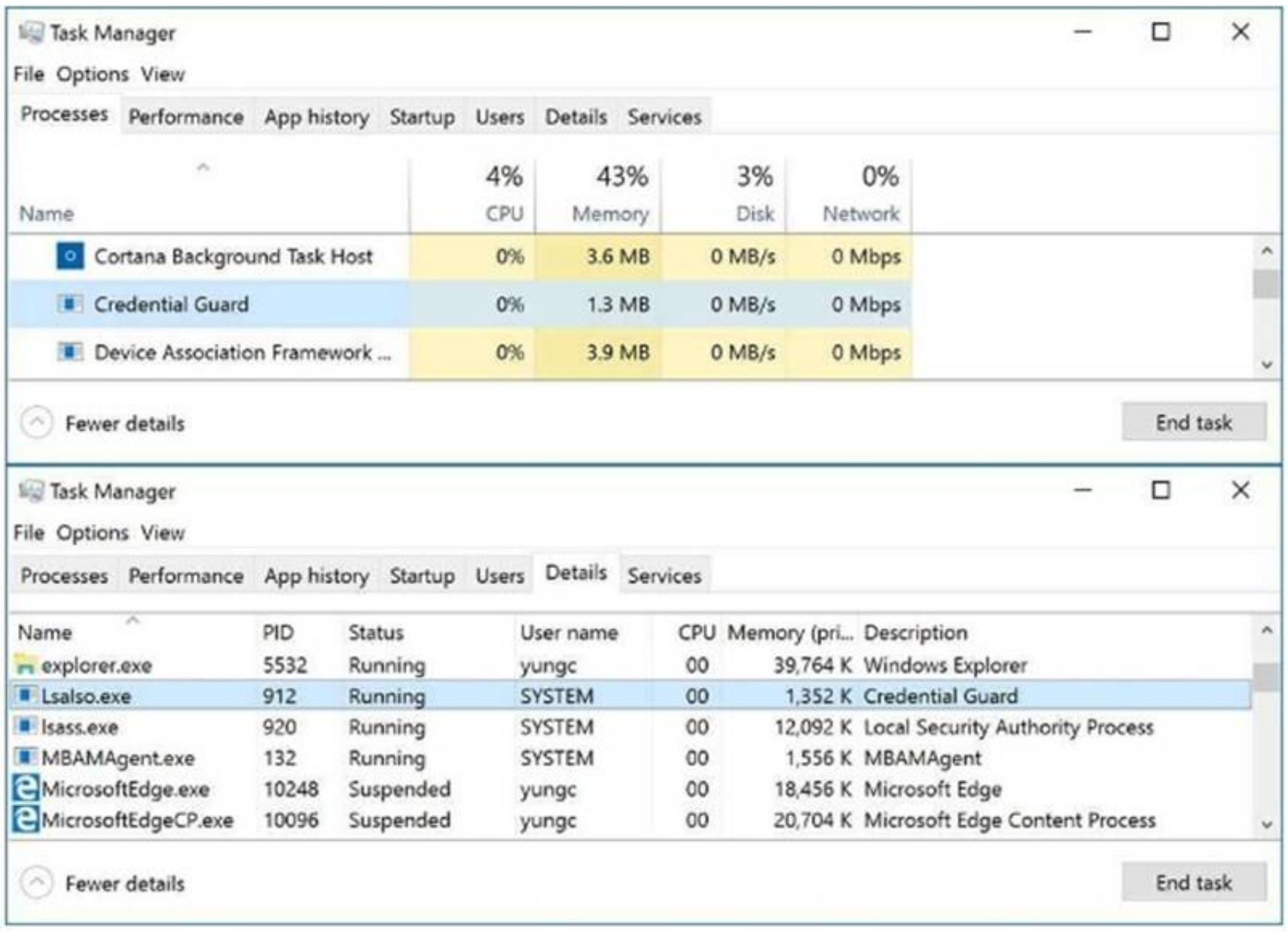
Explanation:
References:
https://anytecho.wordpress.com/2015/05/22/importing-group-policies-using-powershell-almost/

NEW QUESTION 18
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Serve1, 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?

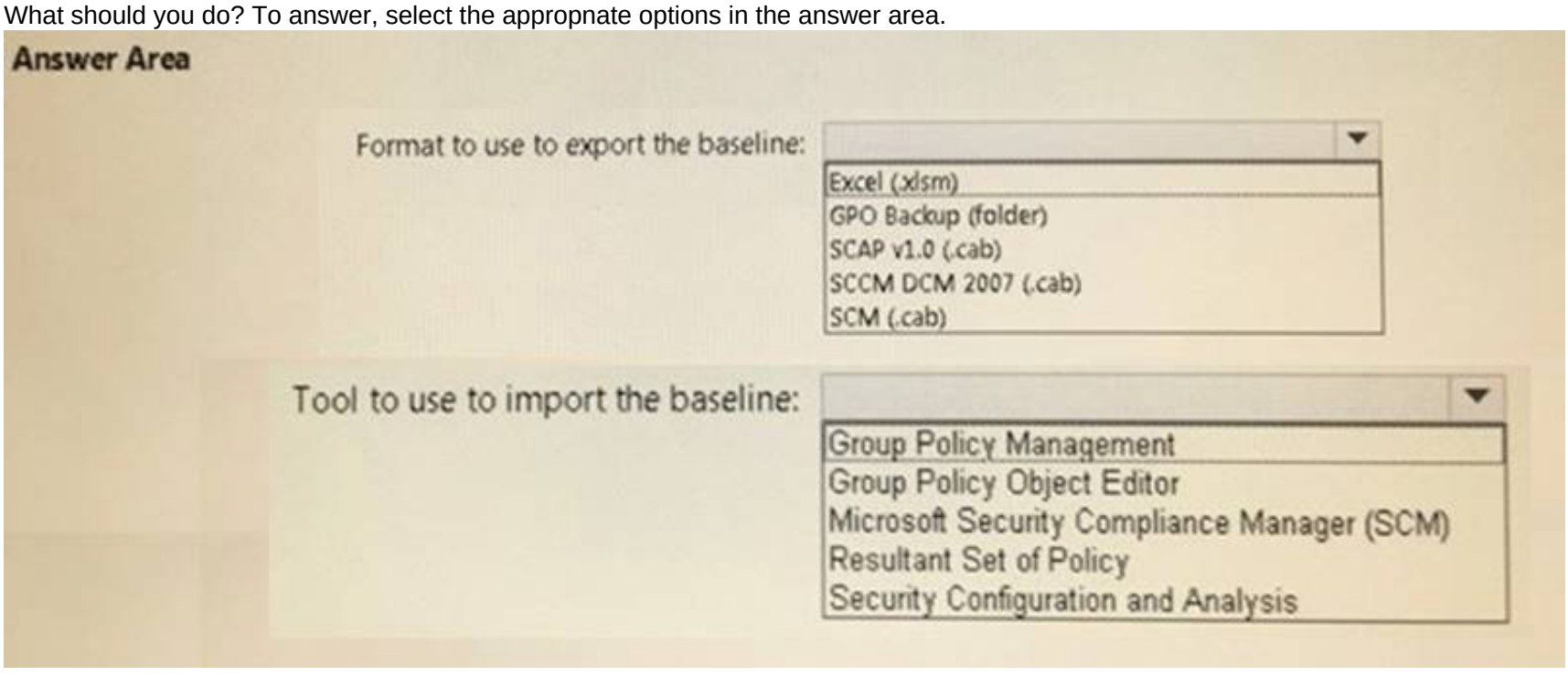
A. From a command prompt fun the credwiz.exe command.
B. From Task Manager, review the processes listed on the Details tab.
C. From Server Manager, click Local Server, and review the properties of Server!
D. From Windows PowerShell, run the Get-WsManCredSSP cmdle

Answer: B

Explanation:
https://yungchou.wordpress.com/2016/10/10/credential-guard-made-easy-in-windows-10-version- 1607/
The same as before, once Credential Guard is properly configured, up and running.
You should find in Task Manager the ‘Credential Guard’ process and ‘lsaiso.exe’ listed in the Details page as below.



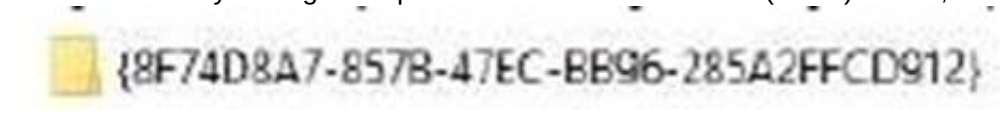
NEW QUESTION 22
HOTSPOT
Your network contains an Active Directory domain named contoso.com. You have an organizational unit (OU) named Secure that contains all servers.
You install Microsoft Security Compliance Manager (SCM) 4.0 on a server named Server1. You need to export the SCM Pnnt Server Secunty baseline and to deploy the baseline to a server named Server2.
What should you do? To answer, select the appropnate options in the answer area.



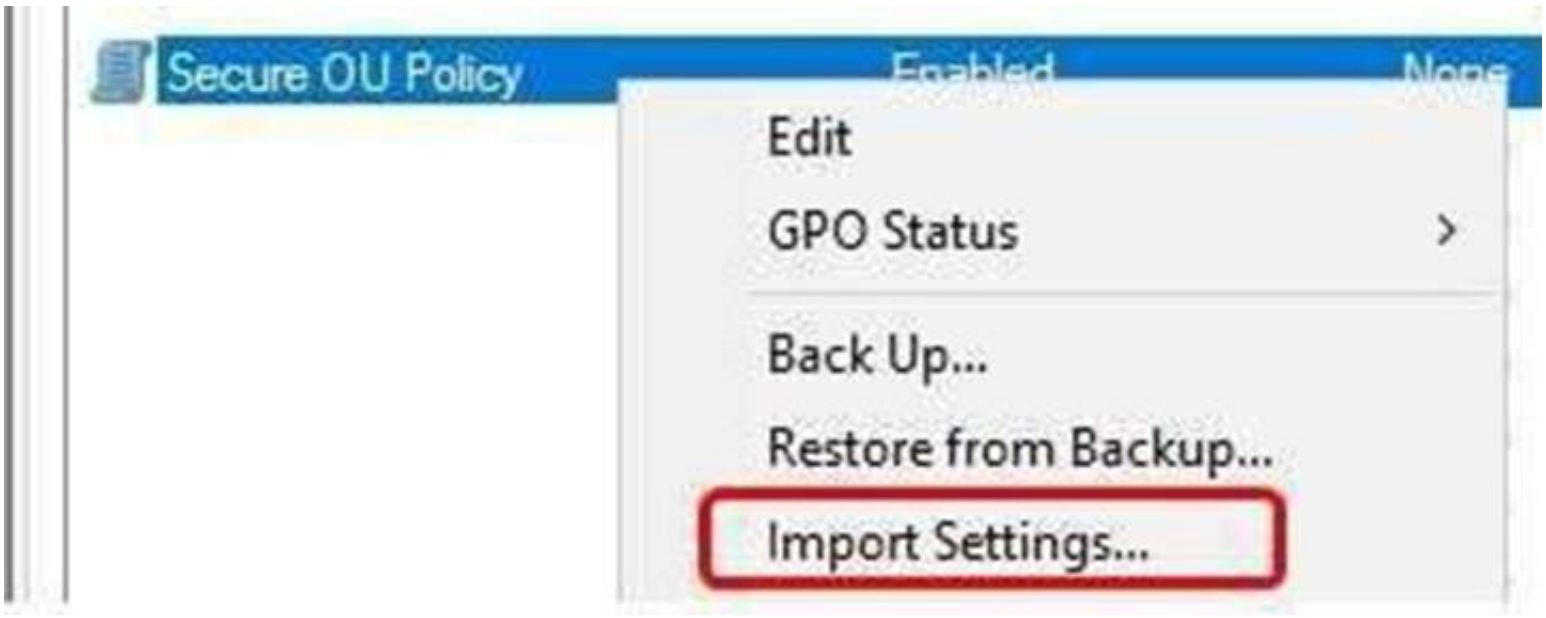
A. Mastered
B. Not Mastered

Answer: A

Explanation:
When the security settings is exported from SCM 4 in a GPO (folder) format, with a long GUID name



You have to import it to GPO by using “Group Policy Management”, right-click the GPO and use “Import Settings” button



Do not confuse with security template .inf files. Only security template .INF file (which is a single file, not a folder) could be imported to a GPO by Group Policy Object Editor

NEW QUESTION 26
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: A

NEW QUESTION 31
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:
Either use PowerShell Remoting to Nano1 and use “Enable-DedupVolume” cmdlet, however ,there is no such choice for this question; or
From Server1, connect it’s server manager to remotely manage Nano1 and enable Data Deduplication for
volumes on Nano1
https://channel9.msdn.com/Series/Nano-Server-Team/Server-Manager-managing-Nano-Server

To assign a central access policy to a file server

1. In Hyper-V Manager, connect to server FILE1. Log on to the server by using contoso\administrator with the password: **pass@word1**.
2. Open an elevated command prompt and type: **gpupdate /force**. This ensures that your Group Policy changes take effect on your server.
3. You also need to refresh the Global Resource Properties from Active Directory. Open an elevated Windows PowerShell window and type `Update-FSRMClassificationpropertyDefinition`. Click ENTER, and then close Windows PowerShell.

> **Tip**
>
> You can also refresh the Global Resource Properties by logging on to the file server. To refresh the Global Resource Properties from the file server, do the following
>
> a. Logon to File Server FILE1 as contoso\administrator, using the password **pass@word1**.
>
> b. Open File Server Resource Manager. To open File Server Resource Manager, click **Start**, type **file server resource manager**, and then click **File Server Resource Manager**.
>
> c. In the File Server Resource Manager, click **File Classification Management**, right-click **Classification Properties** and then click **Refresh**.

4. Open Windows Explorer, and in the left pane, click drive D. Right-click the **Finance Documents** folder, and click **Properties**.
5. Click the **Classification** tab, click **Country**, and then select **US** in the **Value** field.
6. Click **Department**, then select **Finance** in the **Value** field and then click **Apply**.

NEW QUESTION 34
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)

Answer: C

NEW QUESTION 38
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 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.
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-StorageSetting
B. Set-FsrmFileScreenException
C. Set-MpPreference
D. Set-DtcAdvancedSetting

Answer: C

Explanation:
https://technet.microsoft.com/en-us/itpro/powershell/windows/defender/set-mppreference

NEW QUESTION 40
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 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.
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:
https://blogs.technet.microsoft.com/datacentersecurity/2016/06/06/step-by-step-creating-shieldedvms- withoutvmm/
Shielding an existing VM
Let’s start with the simpler approach. This requires you to have a running VM on a host which is not the guarded host.
This is important to distinguish, because you are simulating the scenario where a tenant wants to take an existing, unprotected VM and shield it before moving it to a guarded host.
For clarity, the host machine which is not the guarded host will be referred as the tenant host below. A shielded VM can only run on a trusted guarded host.
The trust is established by the adding the Host Guardian Service server role (retrieved from the HGS server) to the Key Protector which is used to shield the VM.
That way, the shielded VM can only be started after the guarded host successfully attest against the HGS server.
In this example, the running VM is named SVM. This VM must be generation 2 and have a supported OS installed with remote desktop enabled.
You should verify the VM can be connected through RDP first, as it will almost certainly be the primary way to access the VM once it is shielded (unless you have installed other remoting capabilities).

NEW QUESTION 42
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 a DNSSEC-signed zone named adatum.com
Server4	Hyper-V host
Server1	Application server

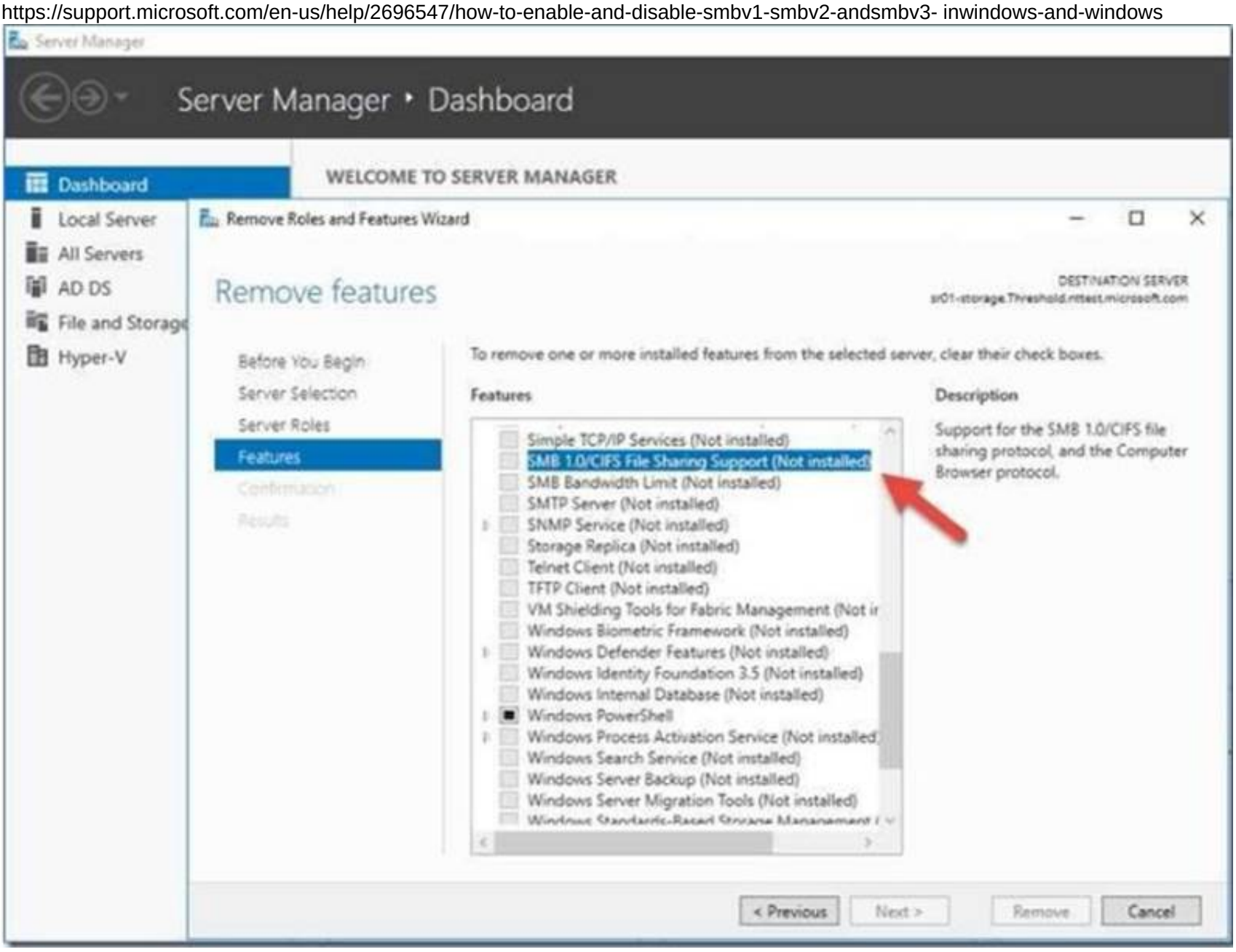
All servers run Windows Server 2016. All client computers run Windows 10.
You have an organizational unit (OU) named Marketing that contains the computers in the marketing department You have an OU named Finance that contains the computers in the finance department You have an OU named AppServers that 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.
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://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-andsmbv3- inwindows-and-windows



NEW QUESTION 47
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 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.
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 Bittocker 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: D

Explanation:
https://technet.microsoft.com/en-us/library/jj679890%28v=ws.11%29.aspx?f=255&MSPPError=- 2147217396#BKMK_rec1

Choose how BitLocker-protected operating system drives can be recovered

This policy setting is used to configure recovery methods for operating system drives.

Policy description	With this policy setting, you can control how BitLocker-protected operating system drives are recovered in the absence of the required startup key information.
Introduced	Windows Server 2008 R2 and Windows 7
Drive type	Operating system drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
Conflicts	You must disallow the use of recovery keys if the **Deny write access to removable drives not protected by BitLocker** policy setting is enabled. When using data recovery agents, you must enable the **Provide the unique identifiers for your organization** policy setting.
When enabled	You can control the methods that are available to users to recover data from BitLocker-protected operating system drives.
When disabled or not configured	The default recovery options are supported for BitLocker recovery. By default, a data recovery agent is allowed, the recovery options can be specified by the user (including the recovery password and recovery key), and recovery information is not backed up to AD DS.

Reference

This policy setting is applied when you turn on BitLocker.

The **Allow data recovery agent** check box is used to specify whether a data recovery agent can be used with BitLocker-protected operating system drives. Before a data recovery agent can be used, it must be added from **Public Key Policies**, which is located in the Group Policy Management Console (GPMC) or in the Local Group Policy Editor.

For more information about adding data recovery agents, see BitLocker Basic Deployment.

In **Configure user storage of BitLocker recovery information**, select whether users are allowed, required, or not allowed to generate a 48-digit recovery password.

Select **Omit recovery options from the BitLocker setup wizard** to prevent users from specifying recovery options when they enable BitLocker on a drive. This means that you will not be able to specify which recovery option to use when you enable BitLocker. Instead, BitLocker recovery options for the drive are determined by the policy setting.

In **Save BitLocker recovery information to Active Directory Domain Services**, choose which BitLocker recovery information to store in Active Directory Domain Services (AD DS) for operating system drives. If you select **Store recovery password and key packages**, the BitLocker recovery password and the key package are stored in AD DS. Storing the key package supports recovering data from a drive that is physically corrupted. If you select **Store recovery password only**, only the recovery password is stored in AD DS.

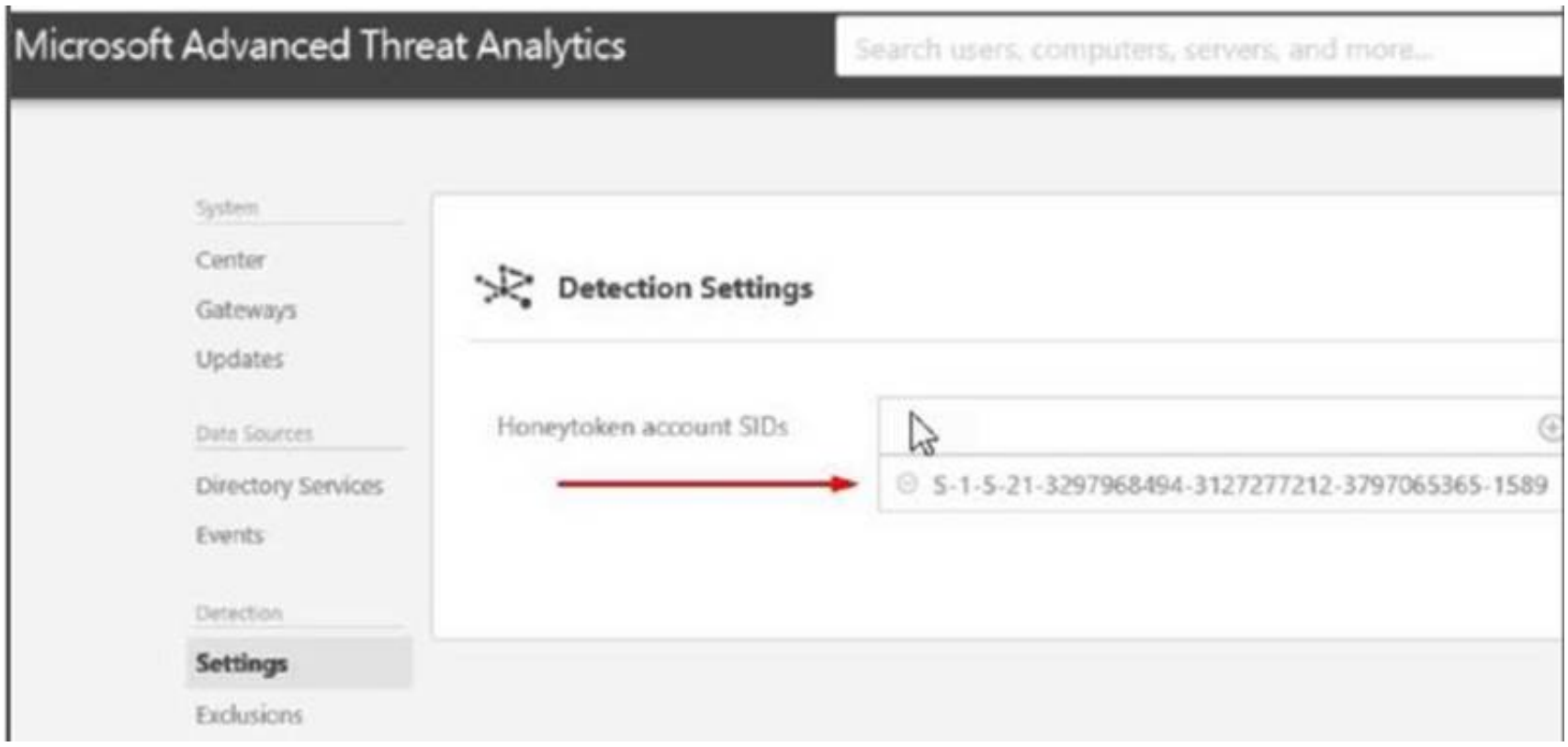
Select the **Do not enable BitLocker until recovery information is stored in AD DS for operating system drives** check box if you want to prevent users from enabling BitLocker unless the computer is connected to the domain and the backup of BitLocker recovery information to AD DS succeeds.

NEW QUESTION 51
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:
https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-prerequisites A user account of a user who has no network activities.
This account is configured as the ATA Honeytoken user.
To configure the Honeytoken user you need the SID of the user account, not the username.



https://docs.microsoft.com/en-us/advanced-threat-analytics/install-ata-step7
ATA also enables the configuration of a Honeytoken user, which is used as a trap for malicious actors – any authentication associated with this (normally dormant) account will trigger an alert.

NEW QUESTION 55
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 domai

Answer: B

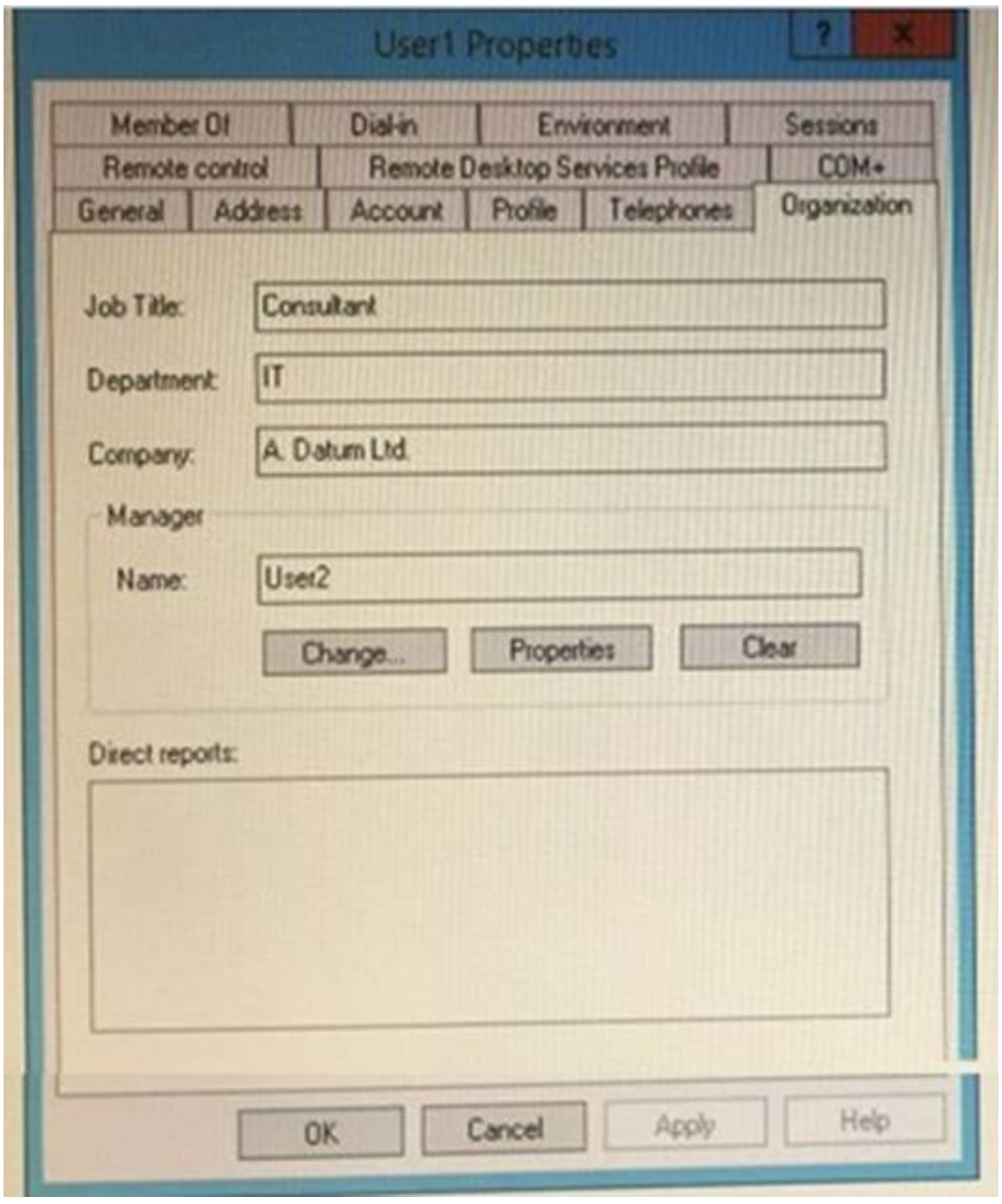
Explanation:
https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-prerequisites
ATA Center which is the first component to be deployed on Server1, requires the use of SSL protocol to communicate with ATA Gateway
To ease the installation of ATA, you can install self-signed certificates during installation.
Post deployment you should replace the self-signed with a certificate from an internal Certification Authority tobe used by the ATA Center.
Make sure the ATA Center and ATA Gateways have access to your CRL distribution point.
If the they don't have Internet access, follow the procedure to manually import a CRL, taking care to install the all the CRL distribution points for the whole chain.

NEW QUESTION 56
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

Answer: C

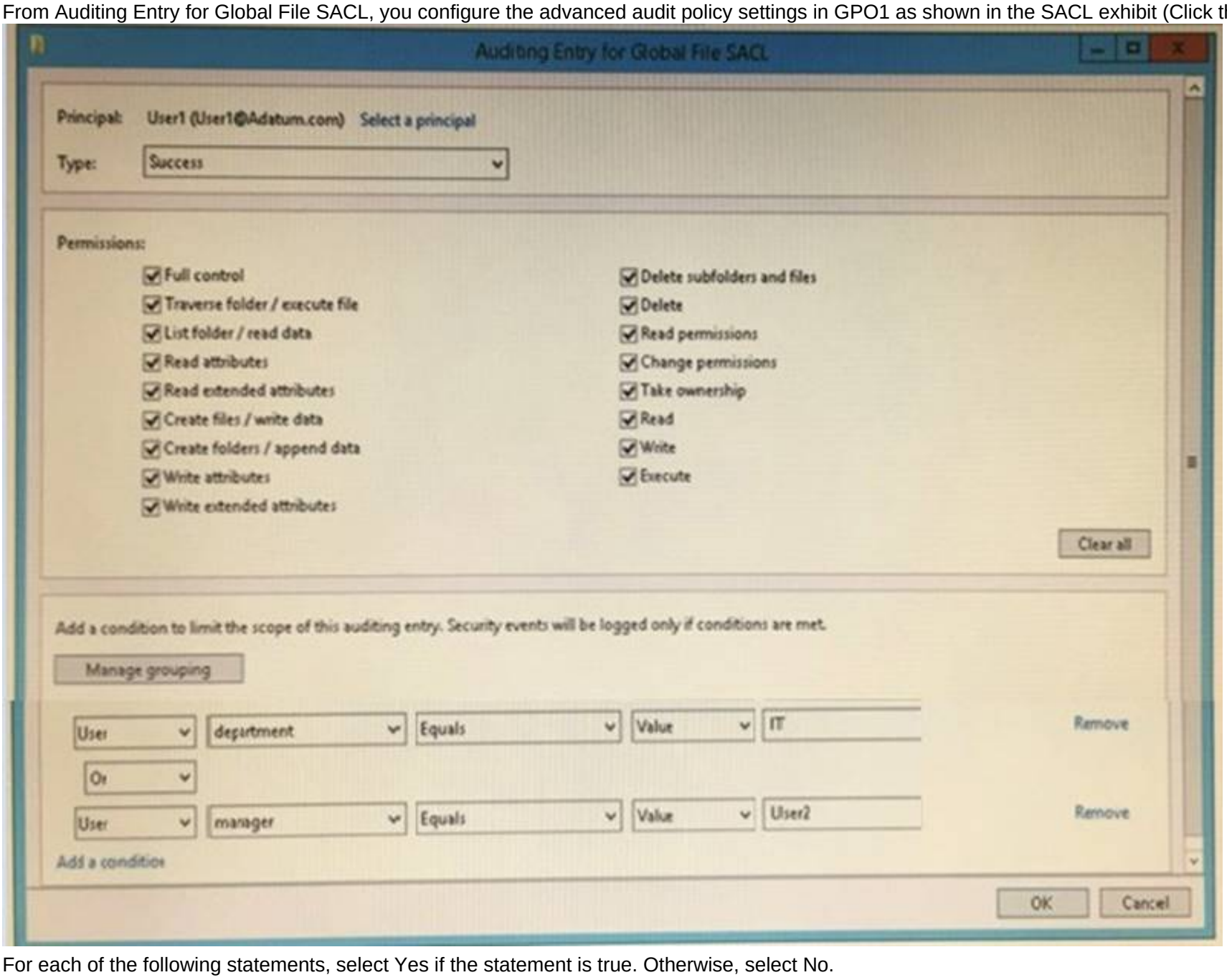
NEW QUESTION 61
HOTSPOT
Your network contains an Active Directory domain named adatum.com. The domain contains a file server named Server1 that runs Windows Server 2016.
You have an organizational unit (OU) named OU1 that contains Server1. You create a Group Policy object (GPO) named GPO1 and link GPO1 to OU1.
A user named User1 is a member of group named Group1. The properties of User1 are shown in the User1 exhibit (Click the Exhibit button.)



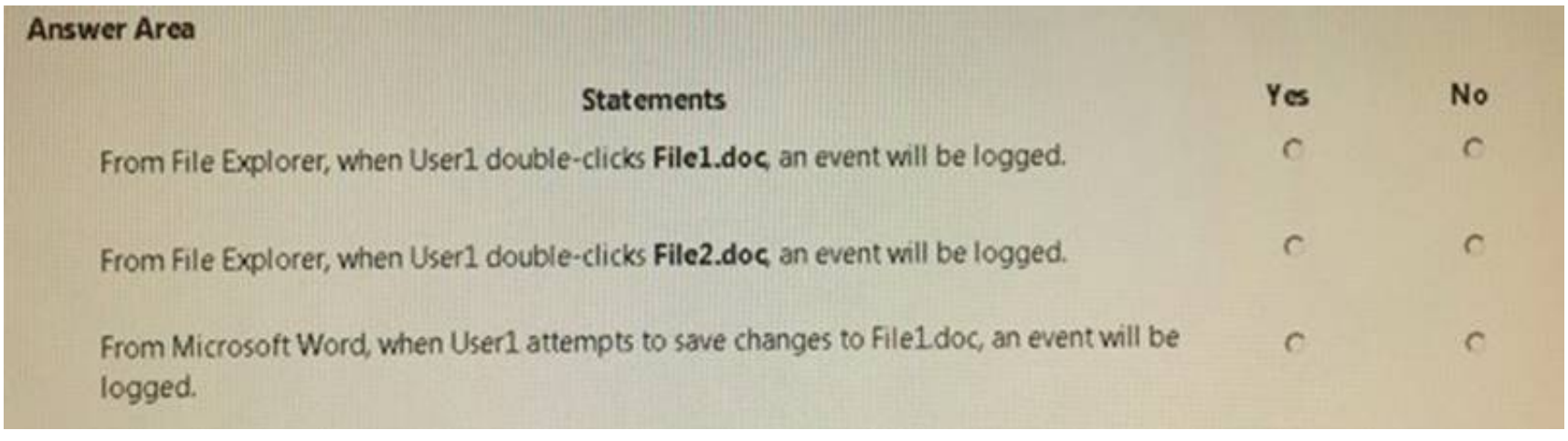
User1 has permissions to two files on Server1 configured as shown in the following table.

File name	Permission
File1.doc	Allow Read
File2.doc	Deny Modify

From Auditing Entry for Global File SACL, you configure the advanced audit policy settings in GPO1 as shown in the SACL exhibit (Click the Exhibit button.)



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


Answer Area

Statements	Yes	No
From File Explorer, when User1 double-clicks **File1.doc**, an event will be logged.	○	○
From File Explorer, when User1 double-clicks **File2.doc**, an event will be logged.	○	○
From Microsoft Word, when User1 attempts to save changes to File1.doc, an event will be logged.	○	○

A. Mastered
B. Not Mastered

Answer: A

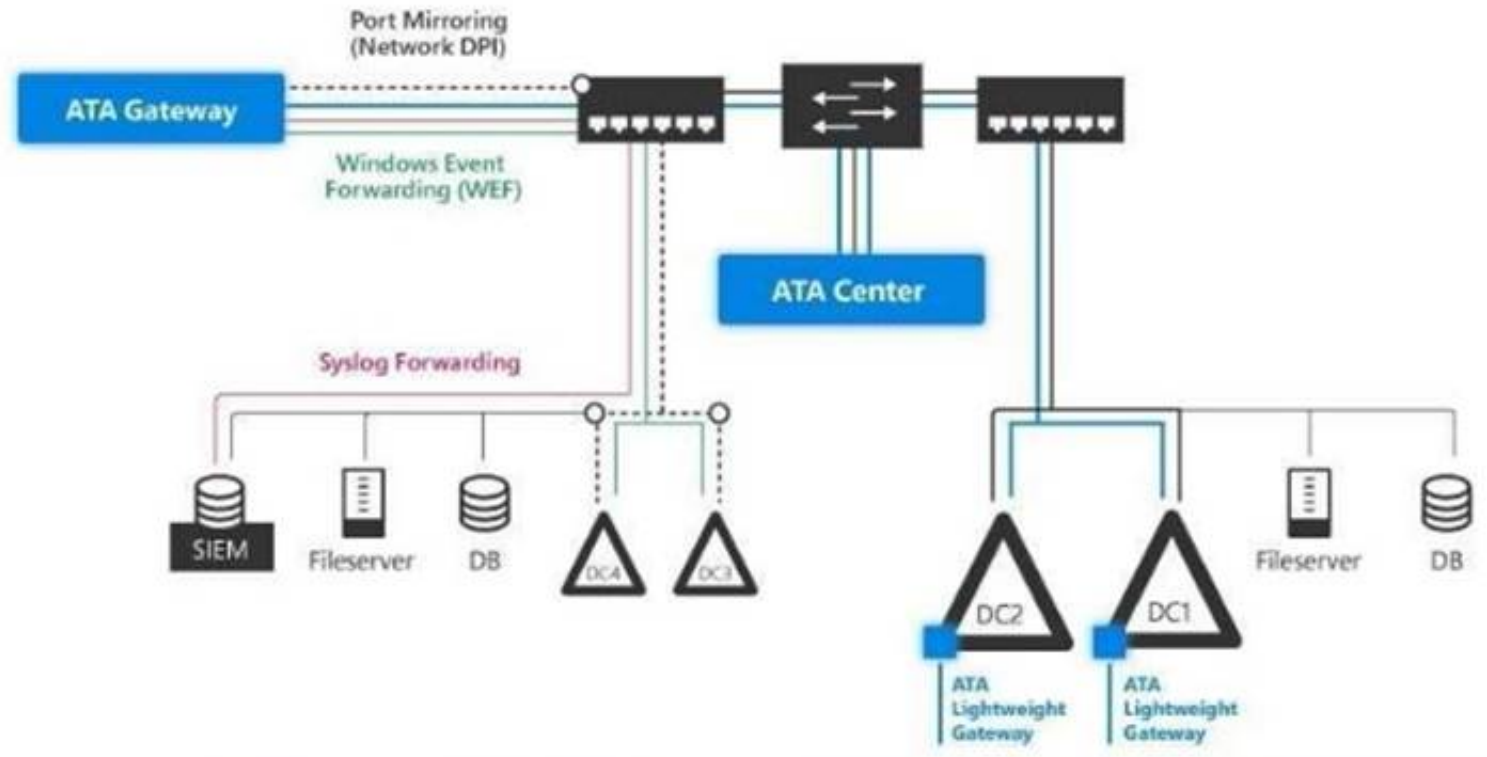
Explanation:
From File Explorer, when User1 double-clicks File1.doc. an event will be logged: Yes From File Explorer, when User1 double-clicks File2.doc. an event will be logged: No
From Microsoft Word, when User1 attempts to save changes to File1.doc, an event will be logged: No
From the SACL, only Successful operations by User1 will be logged “Type: Success”.

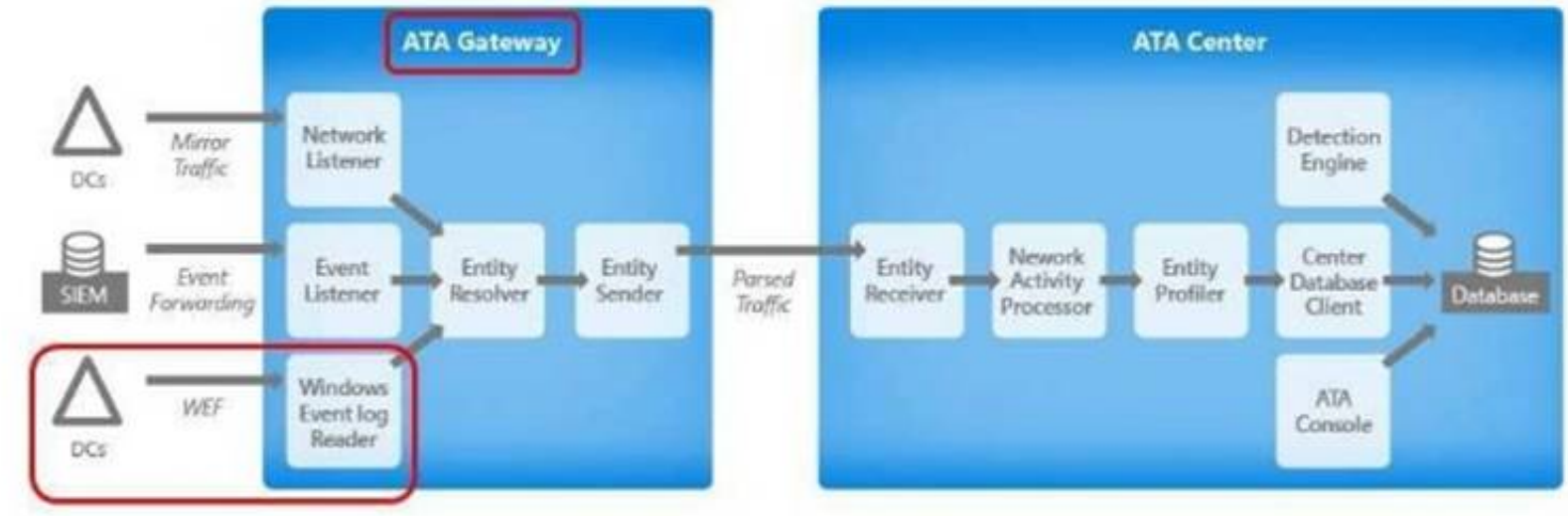
NEW QUESTION 63
Your network contains an Active Directory domain named contoso.com.
You are deploying Microsoft Advanced Threat Analytics (ATA) to the domain.
You install the ATA Center on server named Server1 and the ATA Gateway on a server named Served. You need to ensure that Server2 can collect NTLM 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 Server2

Answer: A

Explanation:
https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-architecture
ATA monitors your domain controller network traffic by utilizing port mirroring to an ATA Gateway using physical or virtual switches.
If you deploy the ATA Lightweight Gateway directly on your domain controllers, it removes the requirement for port mirroring.
In addition, ATA can leverage Windows events (forwarded directly from your domain controllers or from a SIEM server) and analyze the data for attacks and threats.
See the GREEN line in the following figure, forward event ID 4776 which indicates NTLM authentication is being used to ATA Gateway Server2.





NEW QUESTION 65
Your network contains an Active Directory forest named conloso.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 NDJS Capture service to the network adapter of the devices.

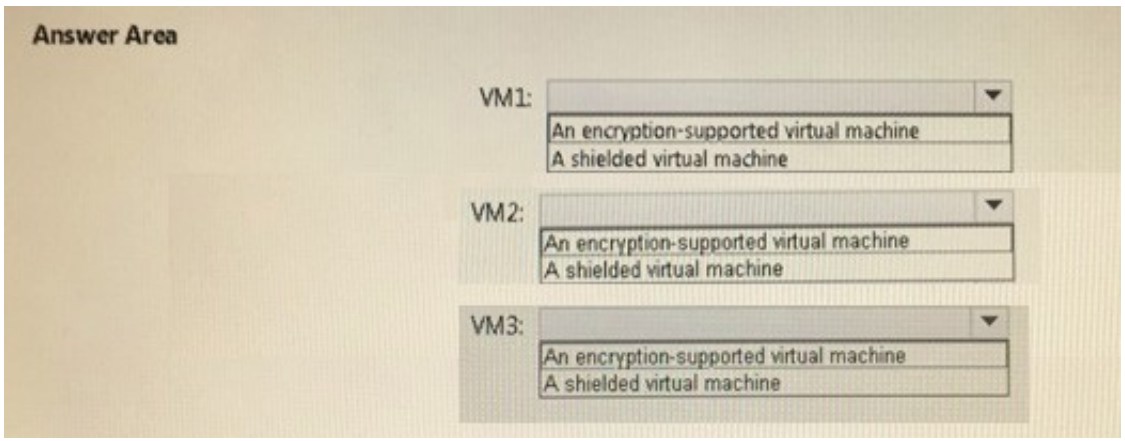
Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-oms-gateway OMS Log Analytics Forwarder = OMS Gateway
If your IT security policies do not allow computers on your network to connect to the Internet, such as point of sale (POS) devices, or servers supporting IT services, but you need to connect them to OMS to manage and monitor them, they can be configured to communicate directly with the OMS Gateway (previous called “OMS Log Analytics Fowarder”) to receive configuration and forward data on their behalf.

NEW QUESTION 67
HOTSPOT
You plan to deploy three encrypted virtual machines that use Secure Boot. The virtual machines will be configured as shown in the following table.

Virtual machine name	Operating system	Requirement
VM1	Windows Server 2016	Prevent console connections that use Virtual Machine Connection.
VM2	Windows Server 2012 R2	Support administration by using PowerShell Direct.
VM3	Windows Server 2016	Support file transfers by using the Data Exchange integration service.

How should you protect each virtual machine? To answer, select the appropriate options in the answer area.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Shielded VM Prevents Virtual Machine connection and PowerShell Direct, it prevent the Hyper-V host to interact in any means with the Shielded VM.
https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shieldedvm/guarded-fabric-andshielded-vms

The following table summarizes the differences between encryption-supported and shielded VMs.

Capability	Generation 2 Encryption Supported	Generation 2 Shielded
Secure Boot	Yes, required but configurable	Yes, required and enforced
Vtpm	Yes, required but configurable	Yes, required and enforced
Encrypt VM state and live migration traffic	Yes, required but configurable	Yes, required and enforced
Integration components	Configurable by fabric admin	Certain integration components blocked (e.g. data exchange, PowerShell Direct)
Virtual Machine Connection (Console), HID devices (e.g. keyboard, mouse)	On, cannot be disabled	Disabled (cannot be enabled)
COM/Serial ports	Supported	Disabled (cannot be enabled)
Attach a debugger (to the VM process)[1]	Supported	Disabled (cannot be enabled)

NEW QUESTION 68
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 domai

Answer: D

Explanation:
https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shieldedvm/guarded-fabricchoose-where-to-install-hgs
The only technical requirement for installing HGS in an existing forest is that it be added to the root domain;
non-root domains are not supported.

NEW QUESTION 72
Read the following statement carefully and answer YES or NO.
You create a rule “Allow Everyone to run Windows except Registry Editor” that allows everyone in the organization to run Windows but does not allow anyone to run Registry Editor.
The effect of this rule would prevent users such as help desk personnel from running a program that is necessary for their support tasks.
To resolve this problem, you create a second rule that applies to the Helpdesk user group: “Allow Helpdesk to run Registry Editor.”
However, if you created a deny rule that did not allow any users to run Registry Editor, would the deny rule override the second rule that allows the Helpdesk user group to run Registry Editor?

A. NO

B. YES

Answer: B

NEW QUESTION 76
Windows PowerShell is a task-based command-line shell and scripting language designed especially for system administration.
Windows Defender comes with a number of different Defender-specific cmdlets that you can run through PowerShell to automate common tasks.
Which Cmdlet would you run first if you wanted to perform an offline scan?

A. Start-MpWDOScan
B. Start-MpScan
C. Set-MpPreference -DisableRestorePoint $true
D. Set-MpPreference -DisablePrivacyMode $true

Answer: A

Explanation:
Some malicious software can be particularly difficult to remove from your PC. Windows Defender Offline (Start-MpWDOScan) can help to find and remove this using up-to-date threat definitions.

NEW QUESTION 80
____ enables easier management for BitLocker enabled desktops and servers in a domain environment by providing automatic unlock of operating system volumes at system reboot when connected to a wired corporate network. This feature requires the client hardware to have a DHCP driver implemented in its UEFI firmware.

A. Network Unlock
B. EFS recovery agent
C. JEA
D. Credential Guard

Answer: A

Explanation:
https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-how-to-enablenetwork- unlock

NEW QUESTION 81
This question relates to Windows Firewall and related technologies. These rules use IPsec to secure traffic while it crosses the network.
You use these rules to specify that connections between two computers must be authenticated or encrypted.
What is the name for these rules?

A. Connection Security Rules
B. Firewall Rules
C. TCP Rules
D. DHP Rules

Answer: A

NEW QUESTION 84
Windows Firewall rules can be configured using PowerShell.
The “Set-NetFirewallProfile” cmdlet configures settings that apply to the per-profile configurations of the Windows Firewall with Advanced Security.
What is the default setting for the AllowInboundRules parameter when managing a GPO?

A. FALSE
B. NotConfigured

Answer: B

Explanation:
The default setting when managing a computer is True. When managing a GPO, the default setting is NotConfigured. The NotConfigured value is only valid when configuring a Group Policy Object (GPO). This parameter removes the setting from the GPO, which results in the policy not changing the value on the computer when the policy is applied.

NEW QUESTION 86
Encryption-supported VMs are intended for use where the fabric administrators are fully trusted. For example, an enterprise might deploy a guarded fabric in order to ensure VM disks are encrypted at-rest for compliance purposes.
Shielded VMs are intended for use in fabrics where the data and state of the VM must be protected from both fabric administrators and untrusted software that might be running on the Hyper-V hosts. Is the Virtual Machine Connection (Console), HID devices (e.g. keyboard, mouse) ON or OFF for Encryption Supported VM’s?

A. Off
B. On

Answer: B

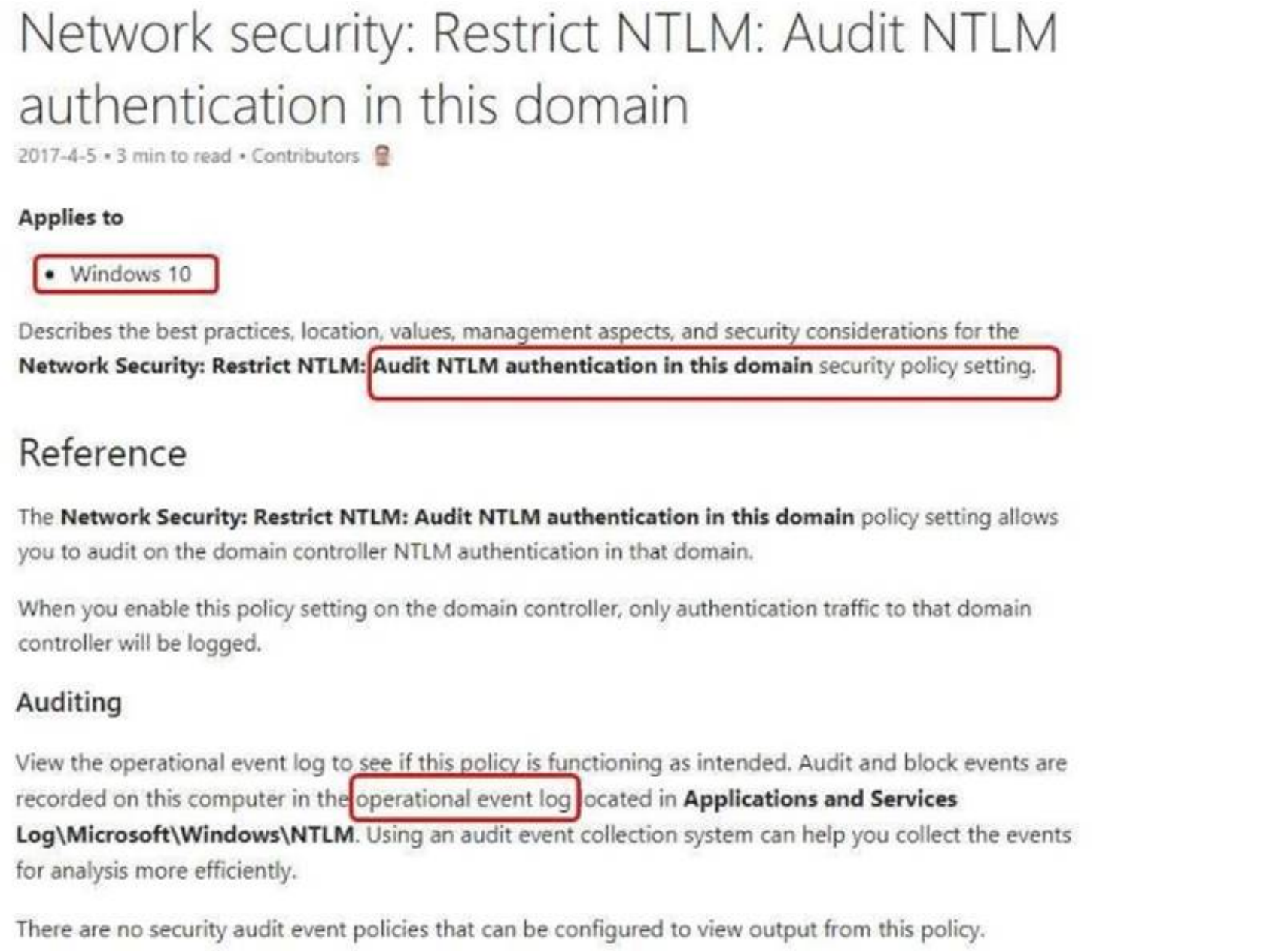
NEW QUESTION 88
Your network contains an Active Directory domain named contoso.com. The domain contains multiple servers that run multiple applications.

Domain user accounts are used to authenticate access requests to the servers. You plan to prevent NTLM from being used to authenticate to the servers. You start to audit NTLM authentication events for the domain.
You need to view all of the NTLM authentication events and to identify which applications authenticate by using NTLM.
On which computers should you review the event logs and which logs should you review?

A. Computers on which to review the event logs: Only client computers
B. Computers on which to review the event logs: Only domain controllers
C. Computers on which to review the event logs: Only member servers
D. Event logs to review: Applications and Services Logs\\Microsoft\\Windows\\Diagnostics- Networking\\Operational
E. Event logs to review: Applications and Services Logs\\Microsoft\\Windows\\NTLM\\Operational
F. Event logs to review: Applications and Services Logs\\Microsoft\\Windows\\SMBClient\\Security
G. Event logs to review: Windows Logs\\Security
H. Event logs to review: Windows Logs\\System

Answer: AE

Explanation:
Do not confuse this with event ID 4776 recorded on domain controller's security event log!!!
This question asks for implementing NTLM auditing when domain clients is connecting to member servers! See below for further information.
https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/networksecurity- restrict-ntlmaudit-ntlm-authentication-in-this-domain
Via lab testing, most of the NTLM audit logs are created on Windows 10 clients, except that you use Windows
Server 2016 OS as clients (but this is unusual)


Network security: Restrict NTLM: Audit NTLM authentication in this domain

2017-4-5 • 3 min to read • Contributors

Applies to

- Windows 10

Describes the best practices, location, values, management aspects, and security considerations for the **Network Security: Restrict NTLM: Audit NTLM authentication in this domain** security policy setting.

Reference

The **Network Security: Restrict NTLM: Audit NTLM authentication in this domain** policy setting allows you to audit on the domain controller NTLM authentication in that domain.

When you enable this policy setting on the domain controller, only authentication traffic to that domain controller will be logged.

Auditing

View the operational event log to see if this policy is functioning as intended. Audit and block events are recorded on this computer in the operational event log located in **Applications and Services Log\Microsoft\Windows\NTLM**. Using an audit event collection system can help you collect the events for analysis more efficiently.

There are no security audit event policies that can be configured to view output from this policy.

NEW QUESTION 93
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. A user named User1 is a member of the local Administrators group. Server1 has the AppLocker rules
configured as shown in follow:

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

Rule name	Path	File hash
Rule1	D:\Folder1*.*	*Not applicable*
Rule2	*Not applicable*	App2.exe

You verify that User1 is unable to run App2.exe on Server1.
Which changes will allow User1 to run D:\\Folder1\\Program.exe and D:\\Folder2\\App2.exe? Choose Two.

A. User1 can run D:\\Folder1\\Program.exe if Program.exe is moved to another folder
B. User1 can run D:\\Folder1\\Program.exe if Program.exe is renamed
C. User1 can run D:\\Folder1\\Program.exe if Program.exe is updated
D. User1 can run D:\\Folder2\\App2.exe if App2.exe is moved to another folder
E. User1 can run D:\\Folder2\\App2.exe if App2.exe is renamed
F. User1 can run D:\\Folder2\\App2.exe if App2.exe is upgraded

Answer: AF

Explanation:
https://technet.microsoft.com/en-us/library/ee449492(v=ws.11).aspx

Important

When determining whether a file is permitted to run, AppLocker processes rules in the following order:

1. **Explicit deny.** An administrator created a rule to deny a file.
2. **Explicit allow.** An administrator created a rule to allow a file.
3. **Implicit deny.** This is also called the default deny because all files that are not affected by an allow rule are automatically blocked.

For “D:\\Folder1\\Program.exe”, it is originally explicitly denied due to Rule1, when moving the “Program,exe” out of “D:\\Folder1\\”, it does not match Rule1.
Assume that “Program.exe” is moved to “D:\\Folder2”, it matches an Explicit Allow rule for group “BUILTIN
\\Administrators” which User1 is a member of, therefore A is correct.
For “App2”,exe, it matches a Explicit Deny rule using its File Hash (created File content), no matter where you move it to, or how you rename it, it would still match Rule2.
Only changing the file content of App2.exe would let it no longer match the explicit deny hash-based rule
“Rule2”.
By upgrading its version and content, it will generate a new hash. so F is correct.

NEW QUESTION 95
HOTSPOT
Your network contains an Active Directory domain named contoso.com. You plan to deploy an application named App1.exe.
You need to verify whether Control Flow Guard is enabled for App1.exe.
Which command should you run? To answer, select the appropriate options in the answer area.

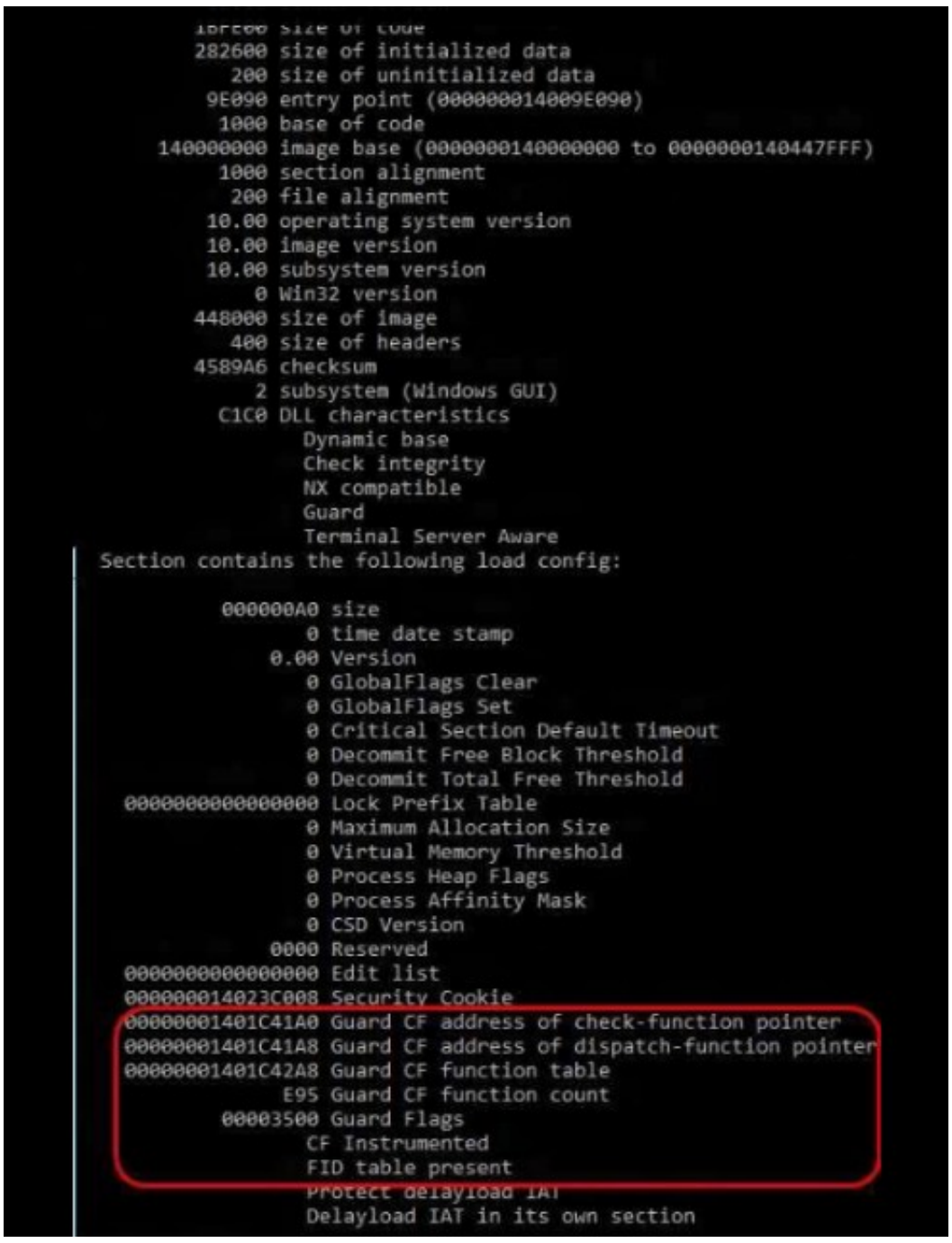
Answer Area

Dumpbin.exe Sfc.exe Sigverif.exe Verifier.exe	/dependents /headers /relocations /symbols	/loadconfig App1.exe

A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://msdn.microsoft.com/en-us/library/windows/desktop/mt637065(v=vs.85).aspx
Control Flow Guard (CFG) is a highly-optimized platform security feature that was created to combat memory corruption vulnerabilities.
By placing tight restrictions on where an application can execute code from, it makes it much harder for explogts to execute arbitrary code through vulnerabilities such as buffer overflows.To verify if Control Flow Guard is enable for a certain application executable:-
Run the dumpbin.exe tool (included in the Visual Studio 2015 installation) from the Visual Studio command
prompt with the /headers and /loadconfig options: dumpbin.exe /headers /loadconfig test.exe.
The output for a binary under CFG should show that the header values include “Guard”, and that the load
config values include “CF Instrumented” and “FID table present”.1



NEW QUESTION 99
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.

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

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.
All laptops are protected by using BitLocker Drive Encryption (BitLocker).
You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.
An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1.
A GPO named GP2 is linked to OU2.
All computers receive updates from Server1. You create an update rule named Update1.
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/Microsoft/Windows/PowerShell/Operational
B. Windows Logs/Security
C. Applications and Services Logs/Windows PowerShell
D. Windows Logs/Application

Answer: A

Explanation:
https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit_script
While Windows PowerShell already has the LogPipelineExecutionDetails Group Policy setting to log the
invocation of cmdlets, PowerShell's scripting language has plenty of features that you might want to log and/or audit.
The new Detailed Script Tracing feature lets you enable detailed tracking and analysis of Windows PowerShell scripting use on a system.
After you enable detailed script tracing, Windows PowerShell logs all script blocks to the ETW (event tracing for windows) event log – Microsoft-WindowsPowerShell/Operational.
If a script block creates another script block (for example, a script that calls the Invoke-Expression cmdlet on a string), that resulting script block is logged as well.
Logging of these events can be enabled through the Turn on PowerShell Script Block Logging Group Policy
setting (in Administrative Templates -> Windows Components -> Windows PowerShell).

NEW QUESTION 101

Your network contains an Active Directory domain named contoso.com. The domain contains a DNS server named Server1 that runs Windows Server 2016.
A domain-based Group Policy object (GPO) is used to configure the security policy of Server1.
You plan to use Security Compliance Manager (SCM) 4.0 to compare the security policy of Server1 to the WS2012 DNS Server Security 1.0 baseline.
You need to import the security policy into SCM. What should you do first?

A. From Security Configuration and Analysis, use the Export Template option.
B. Run the Copy-GPO cmdlet and specify the -TargetName parameter.
C. Run the Backup-GPO cmdlet and specify the -Path parameter.
D. Run the secedit.exe command and specify the/export paramete

Answer: C

Explanation:
https://technet.microsoft.com/en-us/library/ee461052.aspx
Backup-GPO cmdlet and specify the -Path parameter creates a GPO backup folder with GUID name and is suitable to import to SCM 4.0

NEW QUESTION 105
You have the servers configured as shown in the following table.

Role	Type	Number of servers
Domain controller	Physical	5
Member server	Physical	15
Virtualization host	Physical	8
Member server	Virtual	40
Server in a workgroup	Physical	5

You purchase a Microsoft Azure subscription, and you create three Microsoft Operations Management Suite (OMS) workspaces named Workspace1, Workspace2, and Workspace3
You need to deploy Microsoft Monitoring Agent to the servers to meet the following requirements:
-Antimalware data from all the servers must be visible in Workspace1.
-Security and audit data from the domain controllers and the virtualization hosts must be visible in Workspace2.
-System update data from all the servers in all the workgroups must be visible in Workspace& How many OMS agents should you deploy?

A. 10
B. 33
C. 73
D. 45

Answer: C

Explanation:
-Antimalware data from all the servers must be visible in Workspace1.
-Security and audit data from the domain controllers and the virtualization hosts must be visible in Workspace2.
-System update data from all the servers in all the workgroups must be visible in Workspace& “All the servers” mean all 5 domain controllers, plus all member servers (physical and virtual, domain and
workgroup) and virtualization hosts, so there are no exemptions.
All servers in the above table mentioned must install OMS Microsoft Monitoring agents

NEW QUESTION 106
Your network contains an Active Directory domain named contoso.com. The domain contains multiple servers that run either Windows Server 2012 or Windows Server 2012 R2.
You plan to implement Just Enough Administration (JEA) to manage all of the servers.
What should you install on each server to ensure that the servers can be managed by using JEA?

A. Remote Server Administration Tools (RSAT)
B. Microsoft .NET Framework 3.5 Service Pack 1 (SP1)
C. Management Odata Internet Information Services (IIS) Extension
D. Windows Management Framework 5.0

Answer: D

Explanation:
https://msdn.microsoft.com/en-us/library/dn896648.aspx Get JEA
The current release of JEA is available on the following platforms: Windows Server
Windows Server 2016 Technical Preview 5 and higher
Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2* with Windows Management Framework 5.0 installed

NEW QUESTION 108
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-SecureStartup-Package
B. Microsoft-NanoServer-ShieldedVM-Package
C. Microsoft-NanoServer-Storage-Package
D. Microsoft-NanoServer-SCVMM-Compute-Package
E. Microsoft-NanoServer-SCVMM-Package
F. Microsoft-NanoServer-Compute-Package

Answer: ABF

Explanation:
https://docs.microsoft.com/en-us/system-center/vmm/guarded-deploy-host?toc=/windowsserver/virtualization/toc.json
For an SCVMM Managed Nano Server Hyper-V case:
If your host is running Nano Server Hyper-V host, it should have the Compute, SCVMM-Package, SCVMMCompute, SecureStartup, and ShieldedVM packages installed.
https://docs.microsoft.com/en-us/windows-server/get-started/deploy-nano-server
For an standalone Nano Server Hyper-V host, no SCVMM related packages are required, only Compute, SecureStartup, and ShieldedVM packages are required.
This table shows the roles and features that are available in this release of Nano Server, along with the Windows PowerShell options that will install the packages for them.
Some packages are installed directly with their own Windows PowerShell switches (such as -Compute); others you install by passing package names to the –
Package parameter, which you can combine in a comma-separated list. You can dynamically list available packages using the Get-NanoServerPackage cmdlet.

Role or feature	Option
Hyper-V role (including NetQoS)	-Compute
Failover Clustering and other components, detailed after this table	-Clustering
Basic drivers for a variety of network adapters and storage controllers. This is the same set of drivers included in a Server Core installation of Windows Server 2016.	-OEMDrivers
File Server role and other storage components, detailed after this table	-Storage
Windows Defender, including a default signature file	-Defender
Reverse forwarders for application compatibility, for example common application frameworks such as Ruby, Node.js, etc.	Now included by default
DNS Server role	-Package Microsoft-NanoServer-DNS-Package
PowerShell Desired State Configuration (DSC)	-Package Microsoft-NanoServer-DSC-Package **Note:** For full details, see Using DSC on Nano Server.
Internet Information Server (IIS)	-Package Microsoft-NanoServer-IIS-Package **Note:** See IIS on Nano Server for details about working with IIS.
Host support for Windows Containers	-Containers
System Center Virtual Machine Manager agent	-Package Microsoft-NanoServer-SCVMM-Package -Package Microsoft-NanoServer-SCVMM-Compute-Package **Note:** Use the SCVMM Compute package only if you are monitoring Hyper-V. For hyper-converged deployments in VMM, you should also specify the -Storage parameter. For more details, see the VMM documentation.
System Center Operations Manager agent	Installed separately. See the System Center Operations Manager documentation for more details at https://technet.microsoft.com/en-us/system-center-docs/om/manage/install-agent-on-nano-server.

NEW QUESTION 111
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 on Server1 and Server2. Does this meet the goal?

A. Yes
B. No

Answer: A

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

Members of this group can back up and restore files on a computer, regardless of any permissions that protect those files.
This is because the right to perform a backup takes precedence over all file permissions. Members of this group cannot change security settings.

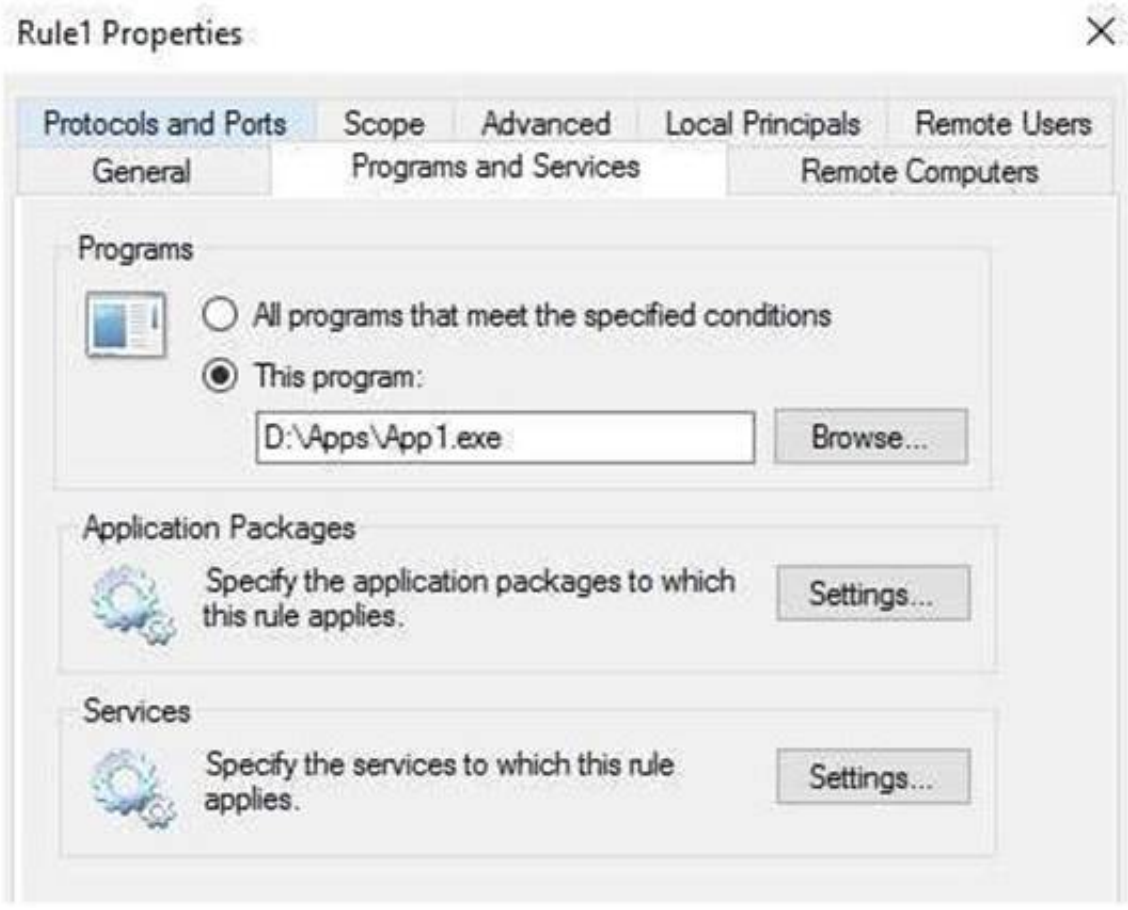
NEW QUESTION 113
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. Computer1 connects to a home network and a corporate network.
The corporate network uses the 172.16.0.0/24 address space internally. Computer1 runs an application named App1 that listens to 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 command New-NetFirewallRule -DisplayName “Rule1” -Direction Inbound - Program “D:\\Apps\\App1.exe” –Action Allow -Profile Domain
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Tested correct cmdlet, worked, and the profile “Domain” for corporate network is also correct.

```
PS C:\> New-NetFirewallRule -DisplayName "Rule1" -Direction Inbound -Program "D:\Apps\App1.exe" -Action Allow -Profile D
omain


Name                  : {27cb5030-bd59-41df-b4d8-d37e97941dad}
DisplayName           : Rule1
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Domain
Platform              : {}
Direction             : Inbound
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local
```



NEW QUESTION 115
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 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.
End of repeated scenario
You need to ensure that when a configuration change is made on Nano2, Nano2 will revert back to the original configuration automatically.
What should you do first?

A. Enable File History for all volumes.
B. Install the Microsoft-NanoServer-DSC-Package optional package
C. Install the Microsoft-NanoServer-DCB-Package optional package
D. Enable System Protection on all volumes
E. Deploy Microsoft System Center 2016 – Data Protection Manager (DPM)

Answer: B

Explanation:
Using PowerShell DSC (Desire State Configuration) to mitigate configuration drift on Nano Server requires
additional steps, like installing the support package “Microsoft-NanoServer-DSC-Package” https://docs.microsoft.com/en-us/powershell/dsc/nanodsc
DSC on Nano Server is an optional package in the NanoServer\\Packages folder of the Windows Server 2016 media.
The package can be installed when you create a VHD for a Nano Server by specifying Microsoft-
NanoServerDSC-Package as the value of the Packages
parameter of the New-NanoServerImage function, or the following PowerShell cmdlets on a live Nano server
“Nano2”.
Import-PackageProvider NanoServerPackage
Install-package Microsoft-NanoServer-DSC-Package -ProviderName NanoServerPackage -Force

NEW QUESTION 120
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 We accounting department to connect to Server11 What should you recommend implementing?

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

Answer: C

Explanation:
In IPsec connection security rule, the IPsec protocol verifies the sending host IP address by utilize integrity
functions like Digitally signing all packets.
If unsigned packets arrives Server11, those are possible source address spoofed packets, when using connection security rule in-conjunction with inbound firewall rules, you can kill those un-signed packets with the action “Allow connection if it is secure” to prevent spoofing and session hijacking attacks.

NEW QUESTION 121
You have a server named Server1 that runs Windows Server 2016.
You need to identify whether IPsec tunnel authorization is 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

Answer: A

Explanation:
https://technet.microsoft.com/en-us/itpro/powershell/windows/netsecurity/get-netipsecrule

```
PS C:\> Get-NetIPsecRule

IPsecRuleName           : {1D65FF82-CBDF-402E-BC92-3489C196602E}
DisplayName             : Site-to-Site_IPSecTunnel
Description             :
DisplayGroup            :
Group                   :
Enabled                 : True
Profile                 : Domain
Platform                : {}
Mode                    : Tunnel
InboundSecurity         : Require
OutboundSecurity        : Require
QuickModeCryptoSet      : Default
Phase1AuthSet           : {E0926672-59CD-45B9-A36D-857B1C00EC6B}
Phase2AuthSet           :
KeyModule               : Default
AllowWatchKey           : False
AllowSetKey             : False
LocalTunnelEndpoint     : {197.6.8.9}
RemoteTunnelEndpoint    : {203.4.5.6}
RemoteTunnelHostname    :
ForwardPathLifetime     : 0
EncryptedTunnelBypass   : False
RequireAuthorization    : True
User                    : Any
Machine                 : Any
PrimaryStatus           : OK
Status                  : The rule was parsed successfully from the store. (65536)
EnforcementStatus       : NotApplicable
PolicyStoreSource       : PersistentStore
PolicyStoreSourceType   : Local
```

NEW QUESTION 123
You have a server named Server1 that runs Windows Server 2016. You need to view all of the inbound rules 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

Answer: B

Explanation:
Get-NetFirewallRule -Direction Inbound <— view inbound rules for all profiles The following examples shows inbound rule for specific firewall profile.
Get-NetFirewallRule -Direction Inbound | where {$_.Profile -eq “Domain”} Get-NetFirewallRule -Direction Inbound | where {$_.Profile -eq “Public”} Get-NetFirewallRule -Direction Inbound | where {$_.Profile -eq “Private”}

NEW QUESTION 127
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 machin

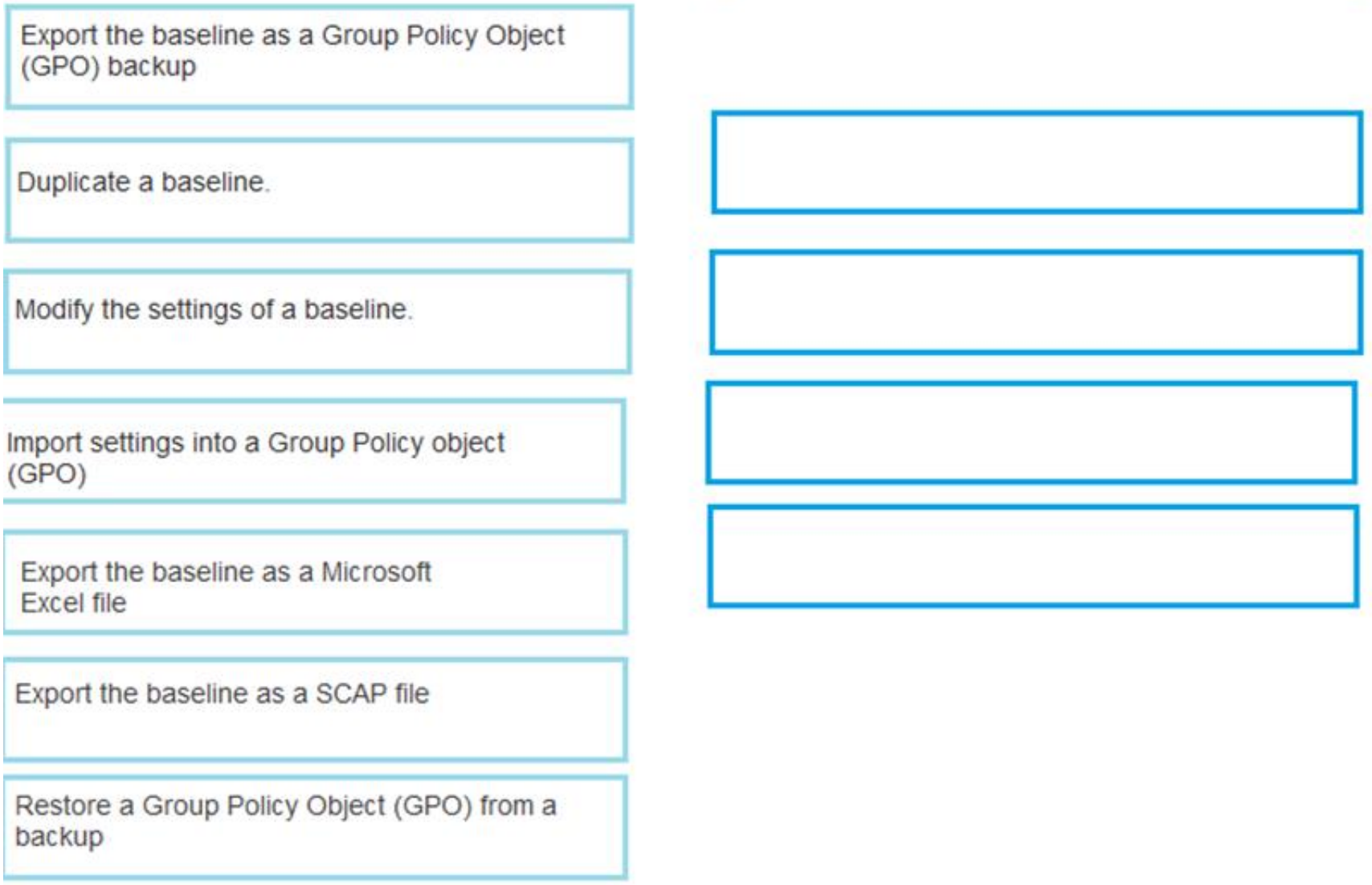
Which of the above server you could enable Credential Guard?

A. Server1
B. Server2
C. Server3
D. Server4

Answer: D

Explanation:
https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guardrequirements Hardware and software requirements
To provide basic protections against OS level attempts to read Credential Manager domain credentials, NTLM
and Kerberos derived credentials, Windows Defender Credential Guard uses:
-Support for Virtualization-based security (required)
-Secure boot (required)
-TPM 2.0 either discrete or firmware (preferred – provides binding to hardware)-UEFI lock (preferred
– prevents attacker from disabling with a simple registry key change)

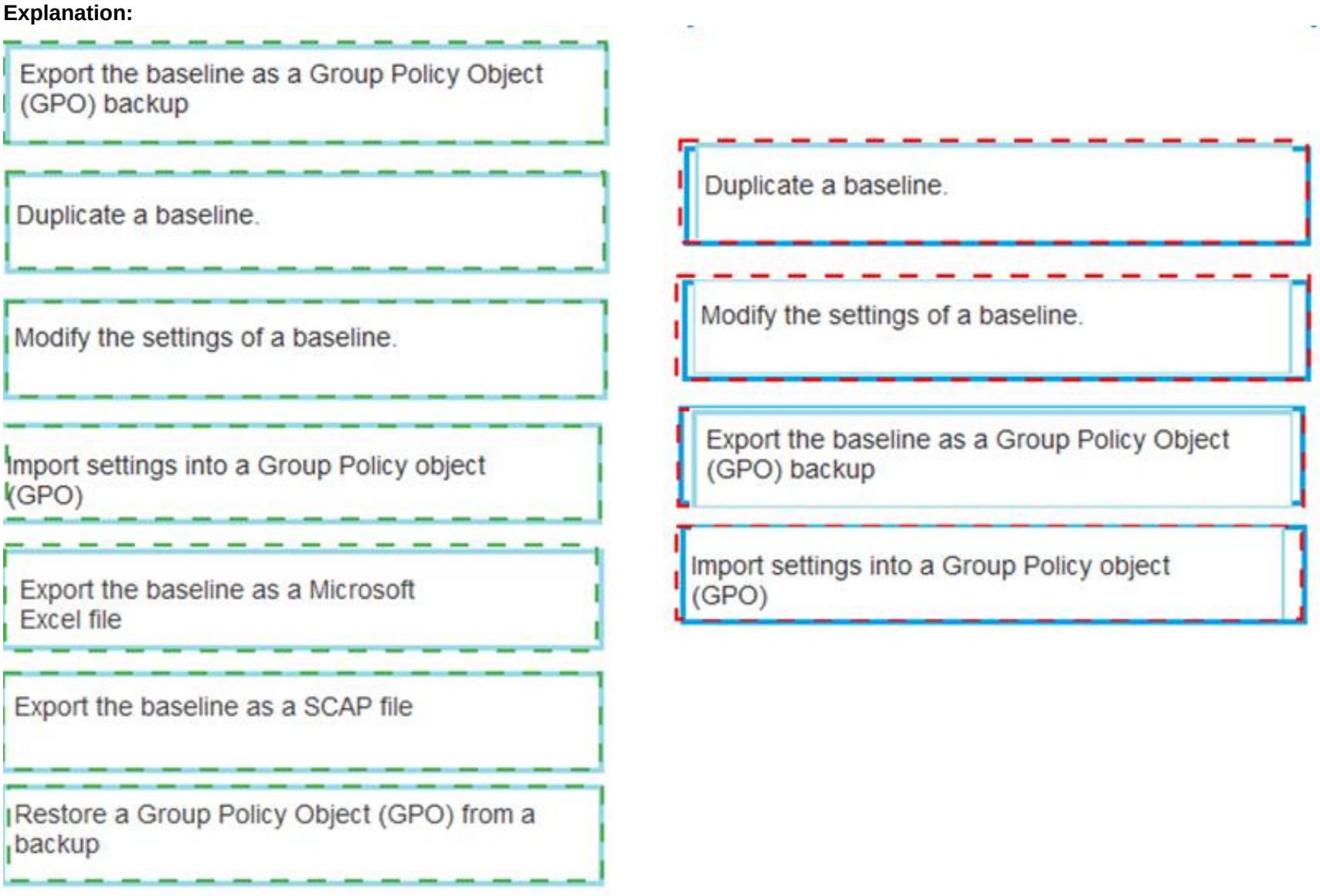
NEW QUESTION 131
DRAG DROP
Your network contains an Active Directory domain.
You install Security Compliance Manager (SCM) 4.0 on a server that runs Windows Server 2016. You need to modify a baseline, and then make the baseline available as a domain policy.
Which four actions should you perform in sequence?



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 135

Your network contains an Active Directory domain named contoso.com. The domain contains servers that run
Windows Server 2016.
You enable Remote Credential Guard on a server named Server1.
You have an administrative computer named Computer1 that runs Windows 10. Computer1 is configured to require Remote Credential Guard.
You sign in to Computer1 as Contoso\\User1.
You need to establish a Remote Desktop session to Server1 as Contoso\\ServerAdmin1. What should you do first?

A. Install the Universal Windows Platform (UWP) Remote Desktop application
B. Turn on virtualization based security
C. Run the mstsc.exe /remoteGuard
D. Sign in to Computer1 as Contoso\\ServerAdmin1

Answer: D

Explanation:
When Computer1 is configured to require Remote Credential Guard, you cannot use NTLM authentication to specify (or impersonate) another user account when connecting to Server1.
Therefore, you have to sign in to Computer1 as “ServerAdmin1” and use Kerberos for authenticating to RDP server “Server1” when Remote Credential Guard is required.

NEW QUESTION 139
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.

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

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 configure Nano1 as a Hyper-V Host. Which command should you run?

A. Add-WindowsFeature Microsoft-NanoServer-Compute-Package
B. Add-WindowsFeature Microsoft-NanoServer-Guest-Package
C. Add-WindowsFeature Microsoft-NanoServer-Host-Package
D. Add-WindowsFeature Microsoft-NanoServer-ShieldedVM-Package
E. Install-Package Microsoft-NanoServer-Compute-Package
F. Install-Package Microsoft-NanoServer-Guest-Package
G. Install-Package Microsoft-NanoServer-Host-Package
H. Install-Package Microsoft-NanoServer-ShieldedVM-Package
I. Install-WindowsFeature Microsoft-NanoServer-Compute-Package
J. Install-WindowsFeatureMicrosoft-NanoServer-Guest-Package
K. Install-WindowsFeatureMicrosoft-NanoServer-Host-Package
L. Install-WindowsFeature Microsoft-NanoServer-ShieldedVM-Package

Answer: E

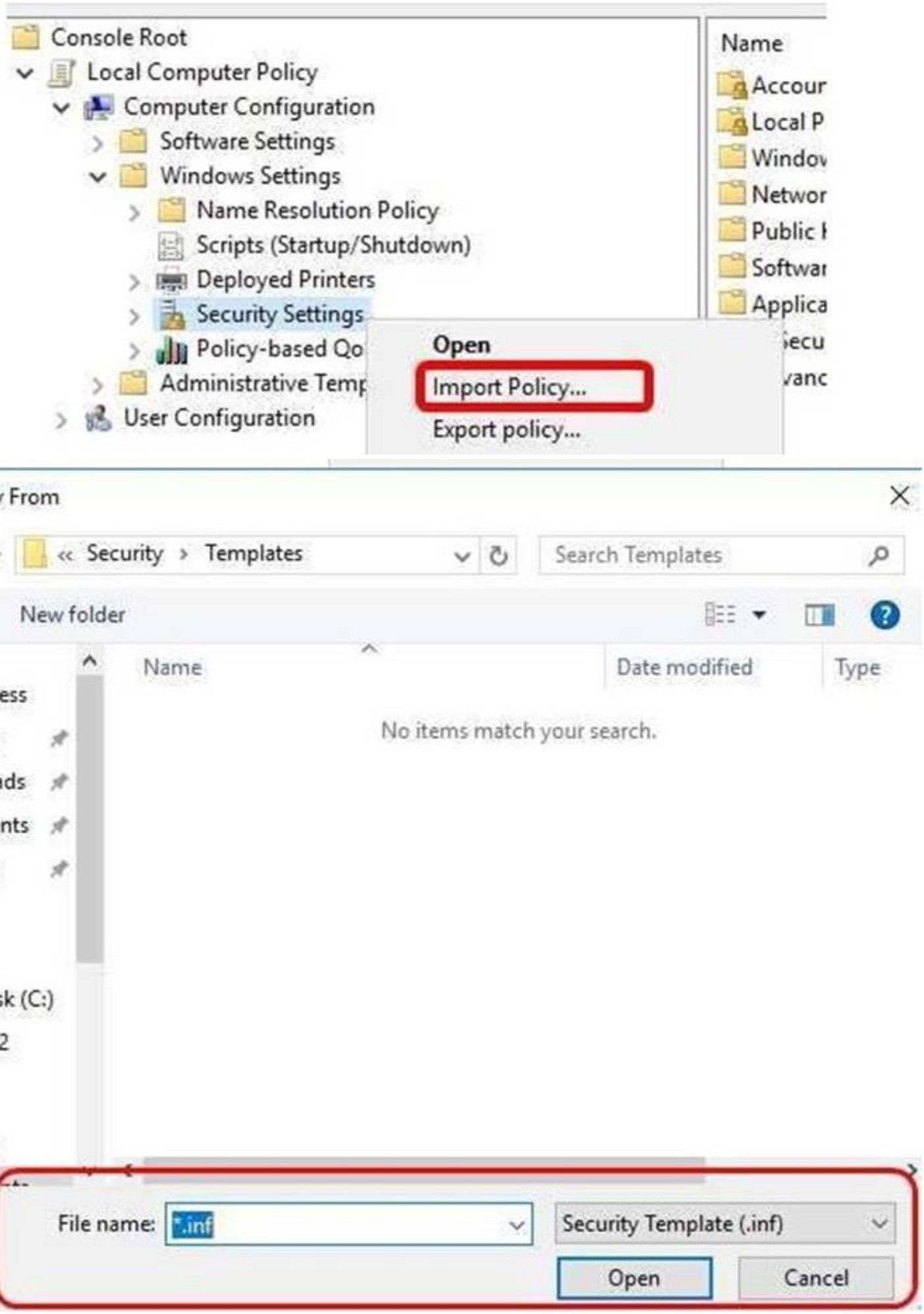
Explanation:
https://docs.microsoft.com/en-us/windows-server/get-started/deploy-nano-server#BKMK_online The Nano Server package “Microsoft-NanoServer-Compute-Package” includes the Hyper-V role for a Nano
Server host.
Moreover, the Install-WindowsFeature or Add-WindowsFeature cmdlet are NOT available on a Nano Server.

NEW QUESTION 141
Your network contains an internal network and a perimeter network. The internal network contains an Active Directory forest named contoso.com.
You deploy five servers to the perimeter network.
All of the servers run Windows Server 2016 and are the members of a workgroup.
You need to apply a security baseline named Perimeter.inf to the servers in the perimeter network. What should you use to apply Perimeter.inf?

A. Local Computer Policy
B. Security Configuration Wizard (SCW)
C. Group Policy Management
D. Server Manager

Answer: A

Explanation:
https://docs.microsoft.com/en-us/windows-server/get-started/deprecated-features https://blogs.technet.microsoft.com/secguide/2016/01/21/lgpo-exe-local-group-policy-objectutility- v1-0/
https://msdn.microsoft.com/en-us/library/bb742512.aspx

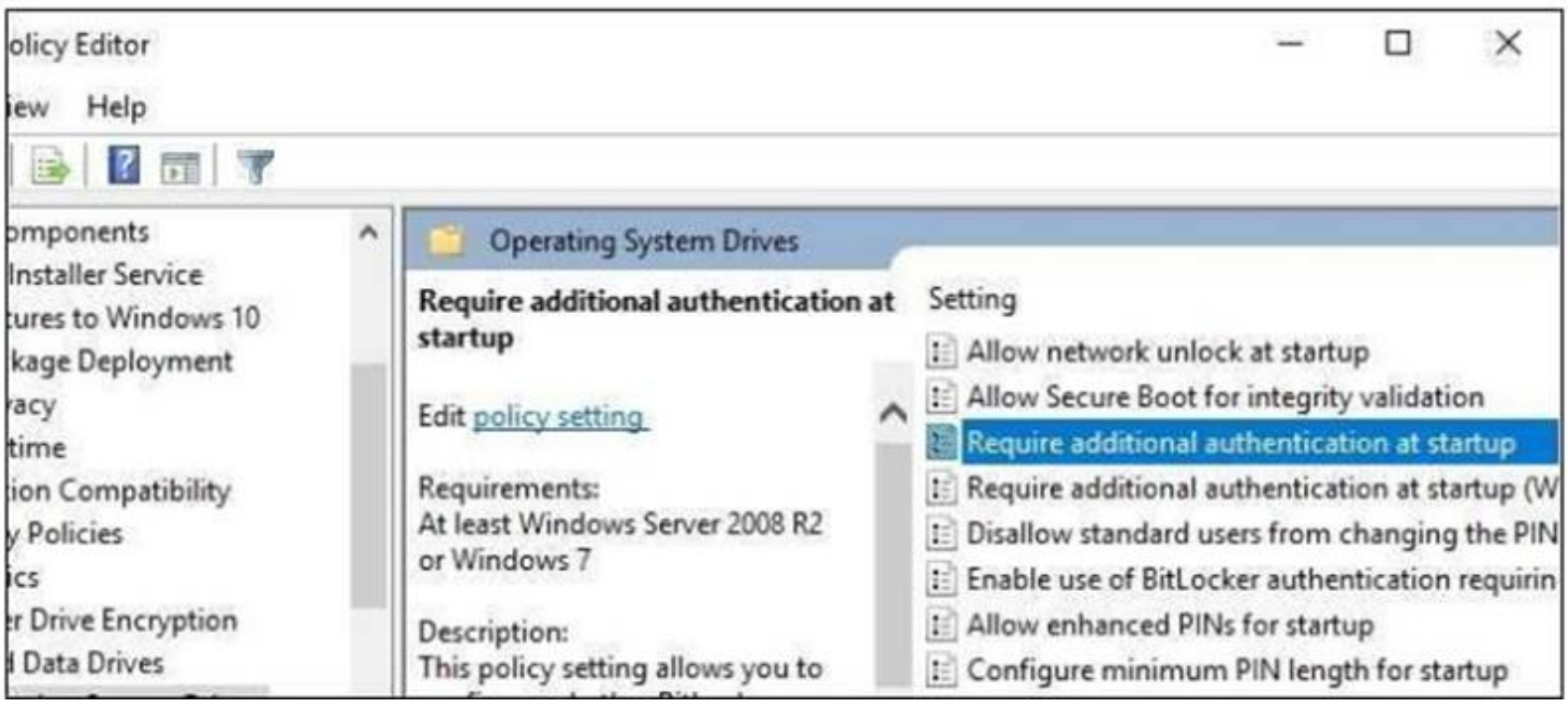


NEW QUESTION 142
You have a Hyper-V host named Server1 that runs Windows Server 2016. Server1 has a generation 2 virtual machine named VM1 that runs Windows 10.
You need to ensure that you can turn on BitLocker Drive Encryption (BitLocker) for drive C: on VM1. What should you do?

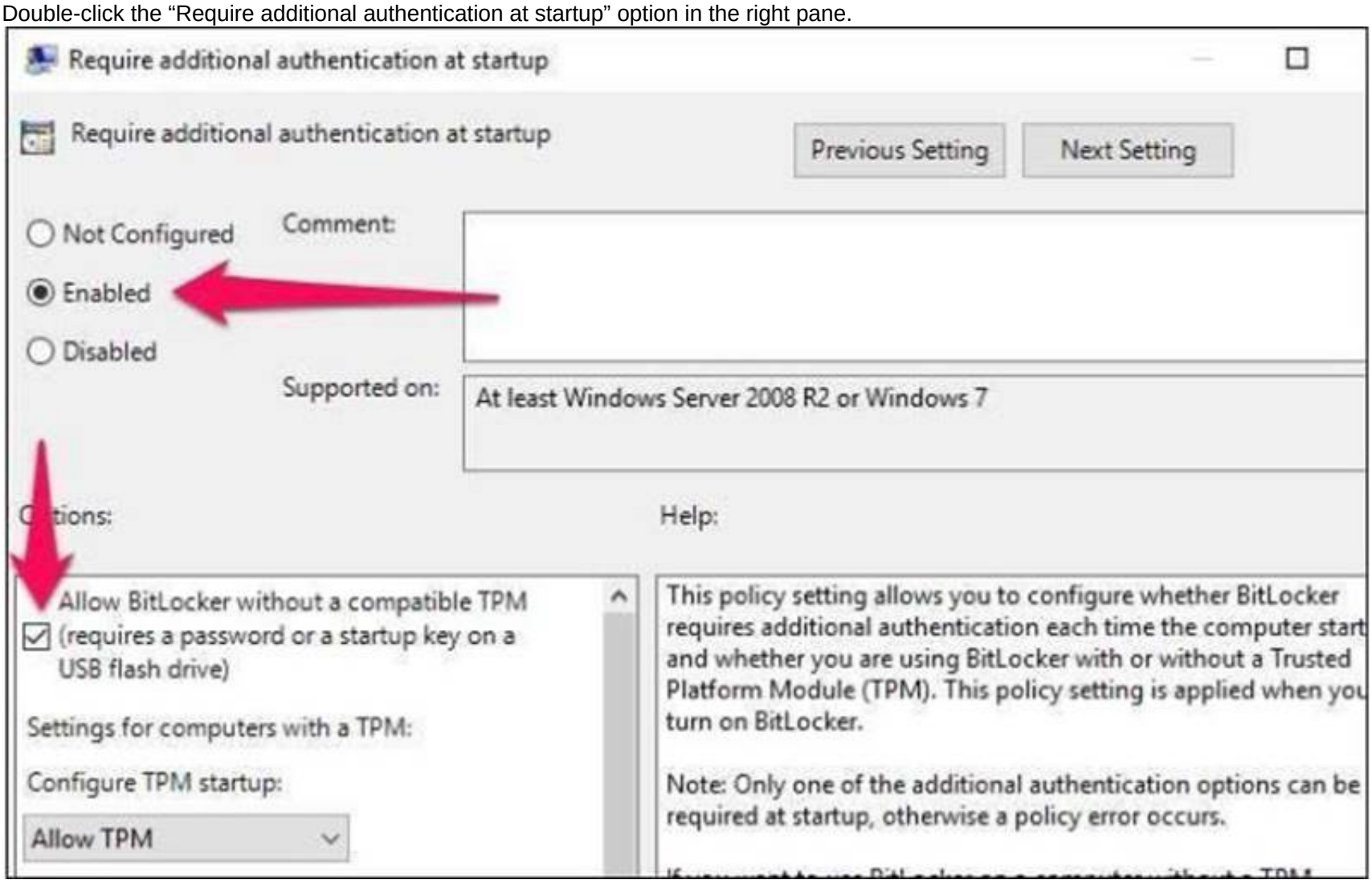
A. From Server1, install the BitLocker feature.
B. From Server1, enable nested virtualization for VM1.
C. From VM1, configure the Require additional authentication at startup Group Policy setting.
D. From VM1, configure the Enforce drive encryption type on fixed data drives Group Policy settin

Answer: C

Explanation:
https://www.howtogeek.com/howto/6229/how-to-use-bitlocker-on-drives-without-tpm/
If you don’t use TPM for protecting a drive, there is no such Virtual TPM or VM Generation, or VM Configuration
version requirement, you can even use Bitlocker without TPM Protector with earlier versions of Windows. How to Use BitLocker Without a TPM
You can bypass this limitation through a Group Policy change. If your PC is joined to a business or school
domain, you can’t change the Group Policy setting
yourself. Group policy is configured centrally by your network administrator.
To open the Local Group Policy Editor, press Windows+R on your keyboard, type “gpedit.msc” into the Run
dialog box, and press Enter.
Navigate to Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives in the left pane.



Double-click the “Require additional authentication at startup” option in the right pane.



Select “Enabled” at the top of the window, and ensure the “Allow BitLocker without a compatible TPM
(requires a password or a startup key on a USB flash drive)” checkbox is enabled here.
Click “OK” to save your changes. You can now close the Group Policy Editor window. Your change takes effect immediately—you don’t even need to reboot.

NEW QUESTION 144
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 Hyper1, run the Invoke-WebRequest cmdlet, and then run the Import-HgsGuardian cmdlet.
B. On HGS1, run the Invoke-WebRequest cmdlet, and then run the Import-HgsGuardian cmdlet.
C. On Hyper1, run the Export-HgsKeyProtectionState cmdlet, and then run the Import-HgsGuardian cmdlet.
D. On HGS1, run the Export-HgsKeyProtectionState cmdlet, and then run the Import-HgsGuardian cmdlet

Answer: A

Explanation:
https://blogs.technet.microsoft.com/datacentersecurity/2016/06/06/step-by-step-creating-shieldedvms- withoutvmm/
The first step is to get the HGS guardian metadata from the HGS server, and use it to create the Key protector.
To do this, run the following PowerShell command
on a guarded host or any machine that can reach the HGS server:
Invoke-WebRequest http://<HGSServer”>FQDN>/KeyProtection/service/metadata/2014- 07/metadata.xml –
OutFile C:\\HGSGuardian.xml Shield the VM
Each shielded VM has a Key Protector which contains one owner guardian, and one or more HGS guardians.
The steps below illustrate the process of getting the guardians, create the Key Protector in order to shield the VM.
Run the following cmdlets on a tenant host “Hyper1”:
SVM is the VM name which to be shielded

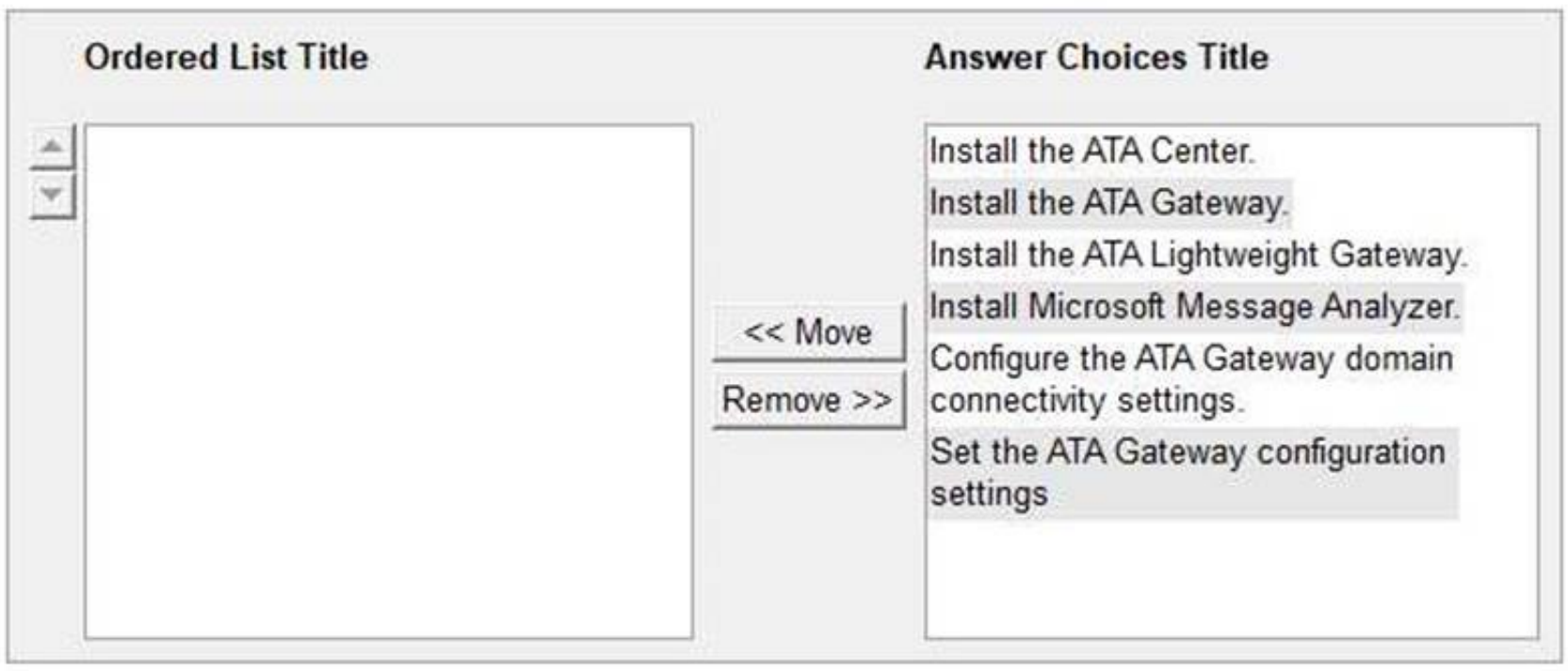
```
$VMName = 'SVM'
# Turn off the VM first. You can only shield a VM when it is powered off Stop-VM –VMName $VMName
# Create an owner self-signed certificate
$Owner = New-HgsGuardian –Name 'Owner' –GenerateCertificates
# Import the HGS guardian
$Guardian = Import-HgsGuardian -Path 'C:\\HGSGuardian.xml' -Name 'TestFabric' – AllowUntrustedRoot
# Create a Key Protector, which defines which fabric is allowed to run this shielded VM
$KP = New-HgsKeyProtector -Owner $Owner -Guardian $Guardian -AllowUntrustedRoot
# Enable shielding on the VM
Set-VMKeyProtector –VMName $VMName –KeyProtector $KP.RawData
# Set the security policy of the VM to be shielded
Set-VMSecurityPolicy -VMName $VMName -Shielded $true
# Enable vTPM on the VM
Enable-VMTPM -VMName $VMName
```

NEW QUESTION 149
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.

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

Answer: BE

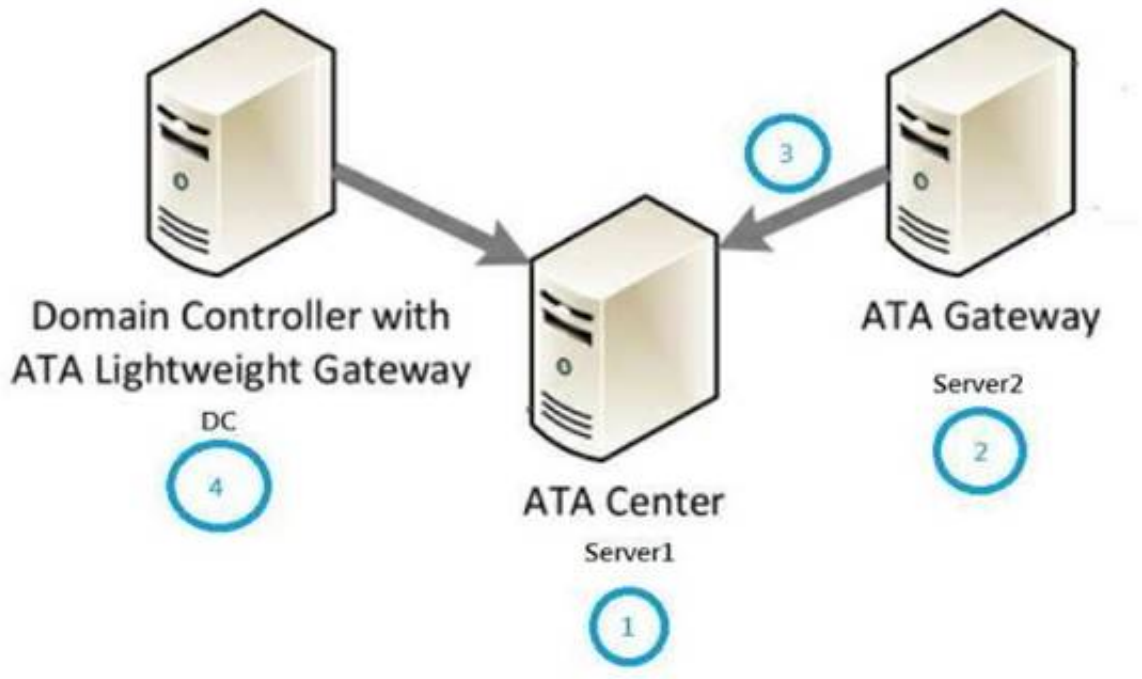
NEW QUESTION 153
DRAG DROP
Your network contains an Active Directory domain named contoso.com.
The domain contains two servers named Server1 and Server2 that run Windows Server 2016. You need to install Microsoft Advanced Threat Analytics (ATA) on Server1 and Server2. Which four actions should you perform in sequence?



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Correct Order of Actions:-
1. Install ATA Center (on Server1 for example)
2. Install ATA Gateway (on Server2 for example, if Server2 has internet connectivity)
3. Set the ATA Gateway configuration settings. (Register Server2 ATA Gateway to Server1's ATA Center)
4. Install the ATA Lightweight Gateway.
Since there are not switch-based port mirroring choice used to capture domain controller's inbound and outbound traffic,
installing ATA Lightweight Gateway on DCs to forward security related events to ATA Center is necessary.



NEW QUESTION 157
You have a server named Server1 that runs Windows Server 2016.
You need to install Security Compliance Manager (SCM) 4.0 on Server1. What should you install on Server1 first?

A. the .NET Framework 3.5 Features feature
B. the Active Directory Rights Management Services server role
C. the Remote Server Administration Tools feature
D. the Group Policy Management feature

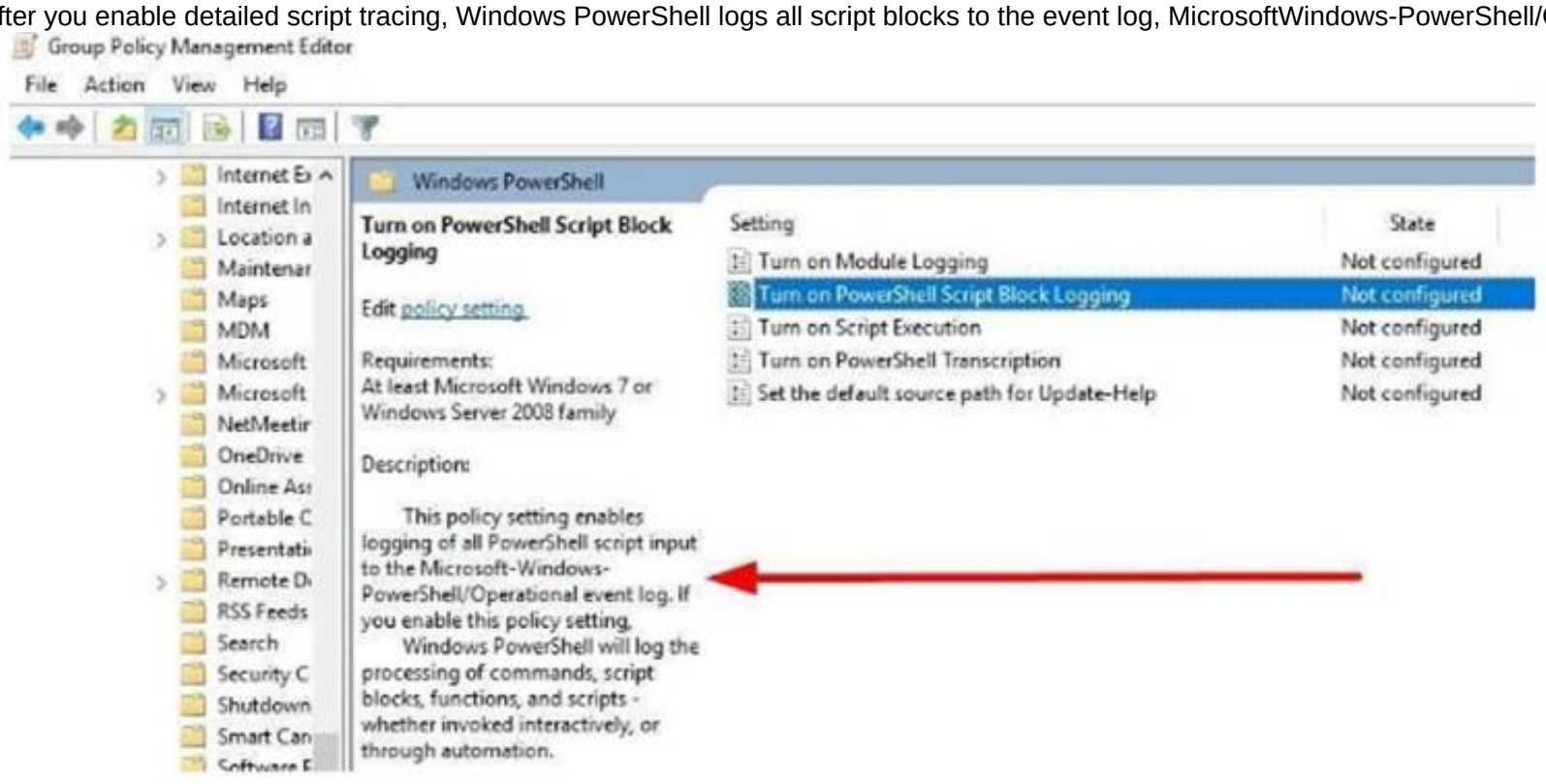
Answer: A

NEW QUESTION 161
You enable and configure PowerShell Script Block Logging.
You need to view which script blocks were executed by using Windows PowerShell scripts. What should you do?

A. View the Microsoft-Windows-PowerShell/Operational event log.
B. Open the log files in %LocalAppData%\\Microsoft\\Windows\\PowerShell.
C. View the Windows PowerShell event log.
D. Open the log files in %SYSTEMROOT%\\Log

Answer: A

Explanation:
https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit_script
After you enable detailed script tracing, Windows PowerShell logs all script blocks to the event log, MicrosoftWindows-PowerShell/Operational.



NEW QUESTION 163
Your network contains an Active Directory domain named contoso.com. All client computers run Windows 10.
You plan to deploy a Remote Desktop connection solution for the client computers.
You have four available servers in the domain that can be configured as Remote Desktop servers. The servers are configured as shown in the following table.

Server name	Operating system	Location
Server1	Windows Server 2012 R2	on-premises
Server2	Windows Server 2016	Microsoft Azure
Server3	Windows Server 2016	on-premises
Server4	Windows Server 2012 R2	Microsoft Azure

You need to ensure that all Remote Desktop connections can be protected by using Remote Credential Guard.
Solution: You deploy the Remote Desktop connection solution by using Server4. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
No, as Server4 is a Windows Server 2012R2 which does not meet the requirements of Remote Credential Guard.
https://docs.microsoft.com/en-us/windows/access-protection/remote-credential-guard Remote Credential Guard requirements
To use Windows Defender Remote Credential Guard, the Remote Desktop client and remote host must meet the following requirements:
The Remote Desktop client device:
Must be running at least Windows 10, version 1703 to be able to supply credentials.
Must be running at least Windows 10, version 1607 or Windows Server 2016 to use the user's signed-in credentials. This requires the user's account be able to sign in to both the client device and the remote host.
Must be running the Remote Desktop Classic Windows application. The Remote Desktop Universal Windows Platform application doesn't support Windows Defender Remote Credential Guard.
Must use Kerberos authentication to connect to the remote host. If the client cannot connect to a domain controller, then RDP attempts to fall back to NTLM.
Windows Defender Remote Credential Guard does not allow NTLM fallback because this would expose credentials to risk.
The Remote Desktop remote host:
Must be running at least Windows 10, version 1607 or Windows Server 2016. Must allow Restricted Admin connections.
Must allow the client's domain user to access Remote Desktop connections. Must allow delegation of non-exportable credentials.

NEW QUESTION 165
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. 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

Answer: B

Explanation:
You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network."
Therefore, you should not create firewall rule for all three profiles.

NEW QUESTION 167
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. 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

Answer: B

Explanation:
"You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.", you should create the firewall rule for "Domain" profile instead, not the "Private" profile.
https://technet.microsoft.com/en-us/library/getting-started-wfas-firewall-profilesipsec(v=ws.10).aspx

A firewall profile is a way of grouping settings, such as firewall rules and connection security rules, which are applied to the computer depending on where the computer is connected. On computers running this version of Windows, there are three profiles for Windows Firewall with Advanced Security:

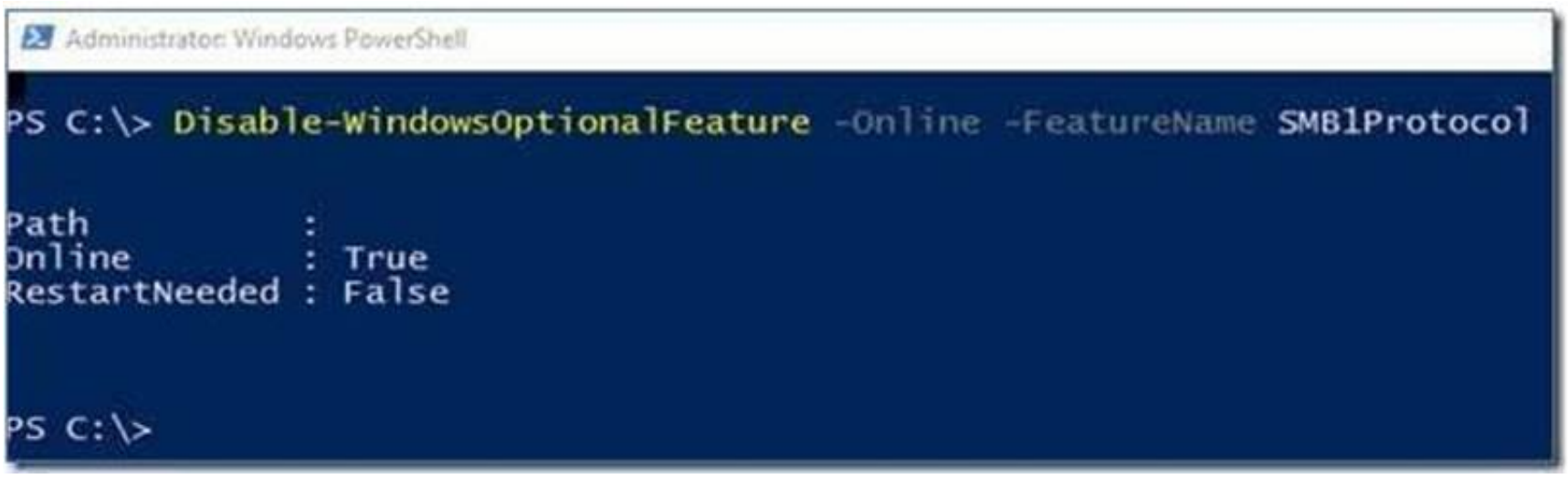
Profile	Description
Domain	Applied to a network adapter when it is connected to a network on which it can detect a domain controller of the domain to which the computer is joined.
Private	Applied to a network adapter when it is connected to a network that is identified by the user or administrator as a private network. A private network is one that is not connected directly to the Internet, but is behind some kind of security device, such as a network address translation (NAT) router or hardware firewall. For example, this could be a home network, or a business network that does not include a domain controller. The Private profile settings should be more restrictive than the Domain profile settings.
Public	Applied to a network adapter when it is connected to a public network such as those available in airports and coffee shops. When the profile is not set to Domain or Private, the default profile is Public. The Public profile settings should be the most restrictive because the computer is connected to a public network where the security cannot be controlled. For example, a program that accepts inbound connections from the Internet (like a file sharing program) may not work in the Public profile because the Windows Firewall default setting will block all inbound connections to programs that are not on the list of allowed programs.

NEW QUESTION 172
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?

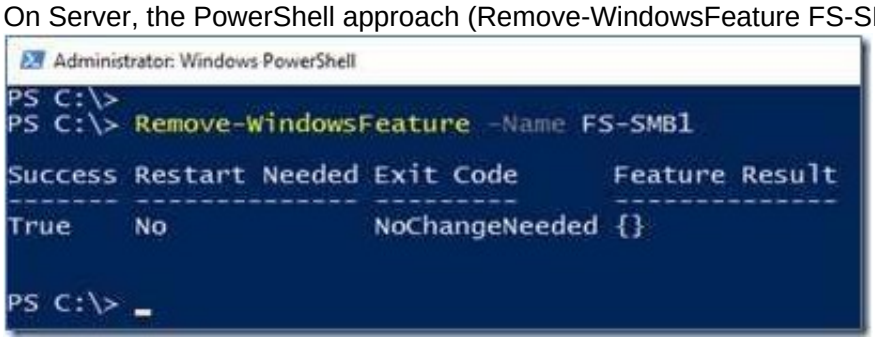
A. Yes
B. No

Answer: B

Explanation:
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
On Client, the PowerShell approach (Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol)
Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol



However, the question asks about Server!
On Server, the PowerShell approach (Remove-WindowsFeature FS-SMB1): Remove-WindowsFeature FS-SMB1



Even if SMB1 is removed, SMB2 and SMB3 could still run NTLM authentication! Therefore, answer is a“NO”.

NEW QUESTION 173
You have a server named Server1 that runs Windows Server 2016.
You need to identify whether any inbound rules on Server1 require that users be authenticated before they can connect to the server. 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-NetFirewallApplicationFilter

Answer: B

Explanation:
The complete cmdlet to perform the required action:-

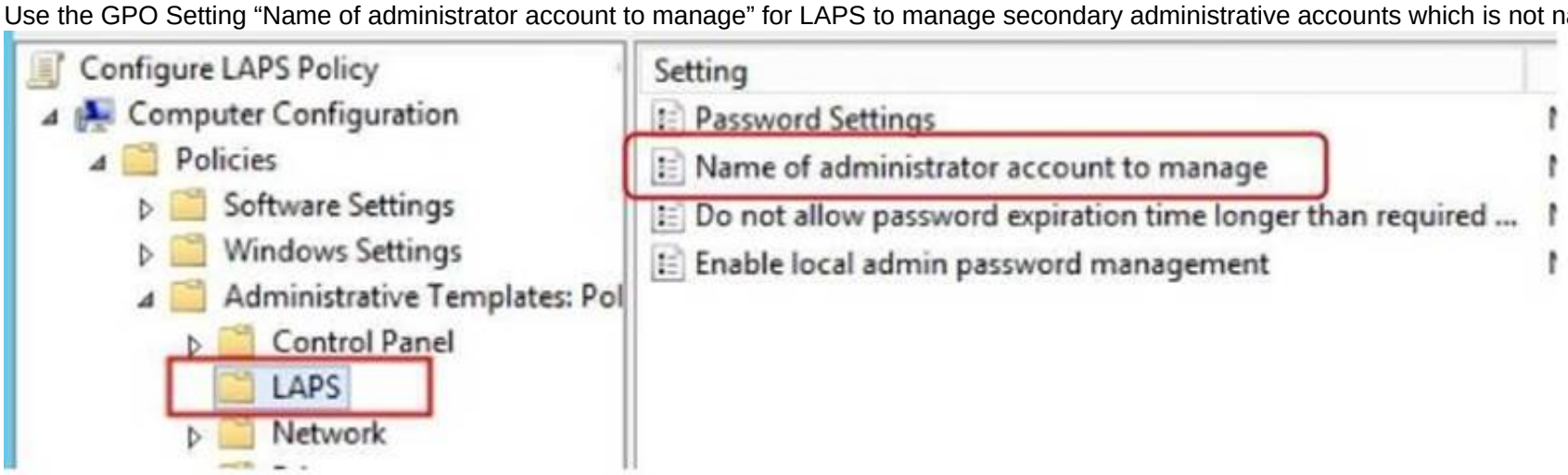
```
PS C:\> Get-NetFirewallRule -DisplayName TEST | Get-NetFirewallSecurityFilter


Authentication      : Required
Encryption          : NotRequired
OverrideBlockRules  : False
LocalUser           : Any
RemoteUser          : Any
RemoteMachine       : Any


PS C:\>
```

NEW QUESTION 175
Your network contains an Active Directory domain named contoso.com. All servers in the domain run Windows Server 2016.All client computers run Windows 10.
Your company has deployed the Local Administrator Password Solution (LAPS).
Client computers in the finance department are located in an organizational unit (OU) named Finance.
Each finance computer has a custom administrative account named FinAdmin. You discover that the FinAdmin accounts are not managed by LAPS.
You need to ensure that the FinAdmin accounts are managed by LAPS. What should you do?

A. On the finance computers, register the AdmPwd.ps Windows PowerShell module and then run the ResetAdmPwdPassword cmdlet
B. Modify the Password Policy in a Group Policy object (GPO).
C. Modify the LAPS settings in a Group Policy object (GPO).
D. On the finance computer
E. rename the FinAdmin accounts to Administrato

Answer: C

Explanation:
Use the GPO Setting “Name of administrator account to manage” for LAPS to manage secondary administrative accounts which is not named as “Administrator”



NEW QUESTION 179
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. Create a new file share.
B. Modify the properties of any share.
C. Stop any process.
D. View the NTFS permissions of any folder.

Answer: B

Explanation:
https://docs.microsoft.com/en-us/powershell/jea/role-capabilities Focus on the 3rd Visible Cmdlets in this question ‘SmbShare\\Set-*’
The PowerShell “SmbShare” module has the following “Set-*” cmdlets, as reported by “Get- Command -Module SmbShare” command:-

```
Set-SmbBandwidthLimit
Set-SmbClientConfiguration
Set-SmbPathAcl
Set-SmbServerConfiguration
Set-SmbShare
```

The “Set-SmbShare” cmdlet is then visible on Server5’s JEA endpoint, and allows JEA users to modify the properties of any file share.
https://technet.microsoft.com/en-us/itpro/powershell/windows/smbshare/set-smbshare

NEW QUESTION 183
Your network contains an Active Directory forest named contoso.com. The forest functional level is Windows Server 2012.
The forest contains 20 member servers that are configured as file servers. All domain controllers run Windows Server 2016.
You create a new forest named contosoadmin.com.
You need to use the Enhanced Security Administrative Environment (ESAE) approach for the administration of the resources in contoso.com.
Which two actions should you perform? Each correct answer presents part of the solution.

A. From the properties of the trust, enable selective authentication.
B. Configure contosoadmin.com to trust contoso.com.
C. Configure contoso.com to trust contosoadmin.com.
D. From the properties of the trust, enable forest-wide authentication.
E. Configure a two-way trust between both forest

Answer: AC

Explanation:
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securingprivilegedaccess- reference-material#ESAE_BM
Trust configurations – Configure trust from managed forests(s) or domain(s) to the administrative forest
A one-way trust is required from production environment to the admin forest. This can be a domain trust or a forest trust.
The admin forest/domain (contosoadmin.com) does not need to trust the managed domains/forests (contoso.com) to manage Active Directory, though additional applications may require a two-way trust relationship, security validation, and testing.
Selective authentication should be used to restrict accounts in the admin forest to only logging on to the appropriate production hosts.

NEW QUESTION 184
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.

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

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.
All laptops are protected by using BitLocker Drive Encryption (BitLocker).You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.
An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1.
A GPO named GP2 is linked to OU2.
All computers receive updates from Server1. You create an update rule named Update1.
You need to create a Role Capability file on Server3. Which file should you create?

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

Answer: D

NEW QUESTION 189
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.

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

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.
All laptops are protected by using BitLocker Drive Encryption (BitLocker).You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.
An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1.
A GPO named GP2 is linked to OU2.

All computers receive updates from Server1. You create an update rule named Update1.
You need to implement BitLocker Network Unlock for all of the laptops. Which server role should you deploy to the network?

A. Network Controller
B. Windows Deployment Services
C. Host Guardian Service
D. Device Heath Attestation

Answer: B

Explanation:
https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-how-to-enablenetwork- unlock Network Unlock core requirements
Network Unlock must meet mandatory hardware and software requirements before the feature can automatically unlock domain joined systems. These requirements include:
You must be running at least Windows 8 or Windows Server 2012.
Any supported operating system with UEFI DHCP drivers can be Network Unlock clients.
A server running the Windows Deployment Services (WDS) role on any supported server operating system.
BitLocker Network Unlock optional feature installed on any supported server operating system. A DHCP server, separate from the WDS server.
Properly configured public/private key pairing. Network Unlock Group Policy settings configured.

NEW QUESTION 194
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 Server1.
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 executed successfully from Server1. What should you do?

A. From Advanced Audit Policy in GPO1. configure auditing for other privilege use events.
B. Run the Add-NetEventProvider -Name “Microsoft-Active-Directory” -MatchAnyKeyword PowerShell command.
C. From Advanced Audit Policy in GPO1, configure auditing for directory service changes.
D. From Administrative Templates in GPO1, configure a Windows PowerShell polic

Answer: D

Explanation:
In the following GPO location, you can enable the setting “Turn on Module Logging” to record an event each
time the PowerShell executes a cmdlet of a specific PowerShell module, for example “ActiveDirectory”.
“Computer Configuration\\Administrative Templates\\Windows Components\\Windows PowerShell”

NEW QUESTION 195
Your network contains several secured subnets that are disconnected from the Internet.
One of the secured subnets contains a server named Server1 that runs Windows Server 2016.
You implement Log Analytics in Microsoft Operations Management Suite (OMS) for the servers that connect to the Internet.
You need to ensure that Log Analytics can collect logs from Server1.
Which two actions should you perform? Each correct answer presents part of the solution.

A. Install the OMS Log Analytics Forwarder on a server that has Internet connectivity.
B. Create an event subscription on a server that has Internet connectivity.
C. Create a scheduled task on Server1.
D. Install the OMS Log Analytics Forwarder on Server1.
E. Install Microsoft Monitoring Agent on Server1.

Answer: AE

Explanation:
https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-oms-gateway OMS Log Analytics Forwarder = OMS Gateway
If your IT security policies do not allow computers on your network to connect to the Internet, such as point of sale (POS) devices, or servers supporting IT services, but you need to connect them to OMS to manage and monitor them, they can be configured to communicate directly with the OMS Gateway (previous called “OMS Log Analytics Fowarder”) to receive configuration and forward data on their behalf.
You have to also install Microsoft Monitoring Agent on Server1 to generate and send events to the OMS Gateway,since Server1 does not have direct Internet connectivity.

NEW QUESTION 196
You have the Windows Server 2016 operating system images as following table.

Image name	Description
Image1	A Nano Server that runs the Standard edition of Windows Server
Image2	A Server Core installation that runs the Datacenter edition of Windows Server
Image3	A Full installation that runs the Standard edition of Windows Server
Image4	A Nano Server that runs the Datacenter edition of Windows Server

Your company's security policy states that you must minimize the attack surface when provisioning new servers.
You need to deploy a Host Guardian Service cluster. Which image should you use for the deployment?

A. image1
B. image2
C. image3
D. image4

Answer: C

Explanation:
https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shieldedvm/ guarded-fabricprepare-for-hgs
Prerequisites
Hardware: HGS can be run on physical or virtual machines, but physical machines are recommended. If you want to run HGS as a three-node physical cluster (for availability), you must have three physical servers.
(As a best practice for clustering, the three servers should have very similar hardware.)
Operating system: Windows Server 2016, Standard or Datacenter edition. <—- so you cannot use Server Core or Nano Server for running Host Guardian Service.
Server Roles: Host Guardian Service and supporting server roles.
Configuration permissions/privileges for the fabric (host) domain: You will need to configure DNS forwarding between the fabric (host) domain and the HGS domain.
If you are using Admin-trusted attestation (AD mode), you will need to configure an Active Directory trust between the fabric domain and the HGS domain.

NEW QUESTION 200
You network contains an Active Directory forest named contoso.com.
All domain controllers run Windows Server 2016 Member servers run either Windows Server 2012 R2 or Windows Server 2016.
Client computers run either Windows 8.1 or Windows 10.
You need to ensure that when users access files in shared folders on the network, the files are encrypted when they are transferred over the network.
Solution: You enable access-based enumeration on all the file shares. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Access-Based Enumeration does not help encrypting network file transfer.

NEW QUESTION 201
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. 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

Answer: B

NEW QUESTION 205
You have a virtual machine named FS1 that runs Windows Server 2016. FS1 has the shared folders shown in the following table.

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

You need to ensure that each user can store 10 GB of files in \\FS1\Users. What should you do?

A. From File Explorer, open the properties of volume D, and then modify the Quota settings.
B. Install the File Server Resource Manager role service, and then create a file screen.
C. From File Explorer, open the properties of D:\Users, and then modify the Advanced sharing settings.
D. Install the File Server Resource Manager role service, and then create a quota.

Answer: D

Explanation:

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

NEW QUESTION 206
Your network contains an Active Directory domain named contoso.com.

You download Microsoft Security Compliance Toolkit 1.0 and all the security baselines.
You need to deploy one of the security baselines to all the computers in an organizational unit (OU) named OU1.
What should you do?

A. Run 1gpo.exe and specify the /g paramete
B. From Policy Analyzer, click Add.
C. From Group Policy Management, create and link a Group Policy object (GPO). Select the GPO and run the Import Settings Wizard.
D. From Group Policy Management, click Group Policy Objects, and then click Manage Backups…
E. From Group Policy Management, create and link a Group Policy object (GPO). Run 1gpo.exe and specify the /g parameter.

Answer: B

Explanation:

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/distributecertificates- to-client-computers-by-using-group-policy

NEW QUESTION 209
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 allow network administrators to use Just Enough Administration (JEA) to change the
TCP/IP settings on Server1. The solution must use the principle of least privilege. How should you configure the session configuration file?

A. Set RunAsVirtualAccount to $false and set RunAsVirtualAccountGroups to Contoso\Network Configuration Operators.
B. Set RunAsVirtualAccount to $true and set RunAsVirtualAccountGroups to Contoso\Network Configuration Operators.
C. Set RunAsVirtualAccount to $false and set RunAsVirtualAccountGroups to Network Configuration Operators.
D. Set RunAsVirtualAccount to $true and set RunAsVirtualAccountGroups to Network Configuration Operators.

Answer: D

Explanation:

References:
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/newpssessionconfigurationfile? view=powershell-6

NEW QUESTION 214
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. The domain has Dynamic Access Control enabled.
Server1 contains a folder named C:\Folder1. Folder1 is shared as Share1.
You need to audit all access to the contents of Folder1 from Server2. The solution must minimize the number of event log entries.
Which two audit policies should you enable on Server1? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Global Object Access- File System
B. Object Access – Audit Detailed File Share
C. Object Access – Audit Other Object Access Events
D. Object Access – Audit File System
E. Object Access – Audit File Share

Answer: BE

Explanation:

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

NEW QUESTION 215
Your network contains an Active Directory domain named contoso.com.
The domain contains four global groups named Group1, Group2, Group3, and Group4. A user named User1 is a member of Group3.
You have an organizational unit (OU) named OU1 that contains computer accounts. A Group Policy object (GPO) named GPO1 is linked to OU1. OU1 contains a computer account named Computer1. GPO1 has the User Rights Assignment configured as shown in the following table.

A. Modify the membership of Group3.
B. Modify the membership of Group2.
C. Modify the membership of Group1.
D. Modify the membership of Group4.

Answer: B

NEW QUESTION 218
DRAG DROP
Your network contains an Active Directory domain named contoso.com. The domain contains a user named User1 and a computer named Computer1. Remote Server Administration Tools (RSAT) is installed on Computer1.
You need to add User1 as a data recovery agent in the domain.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

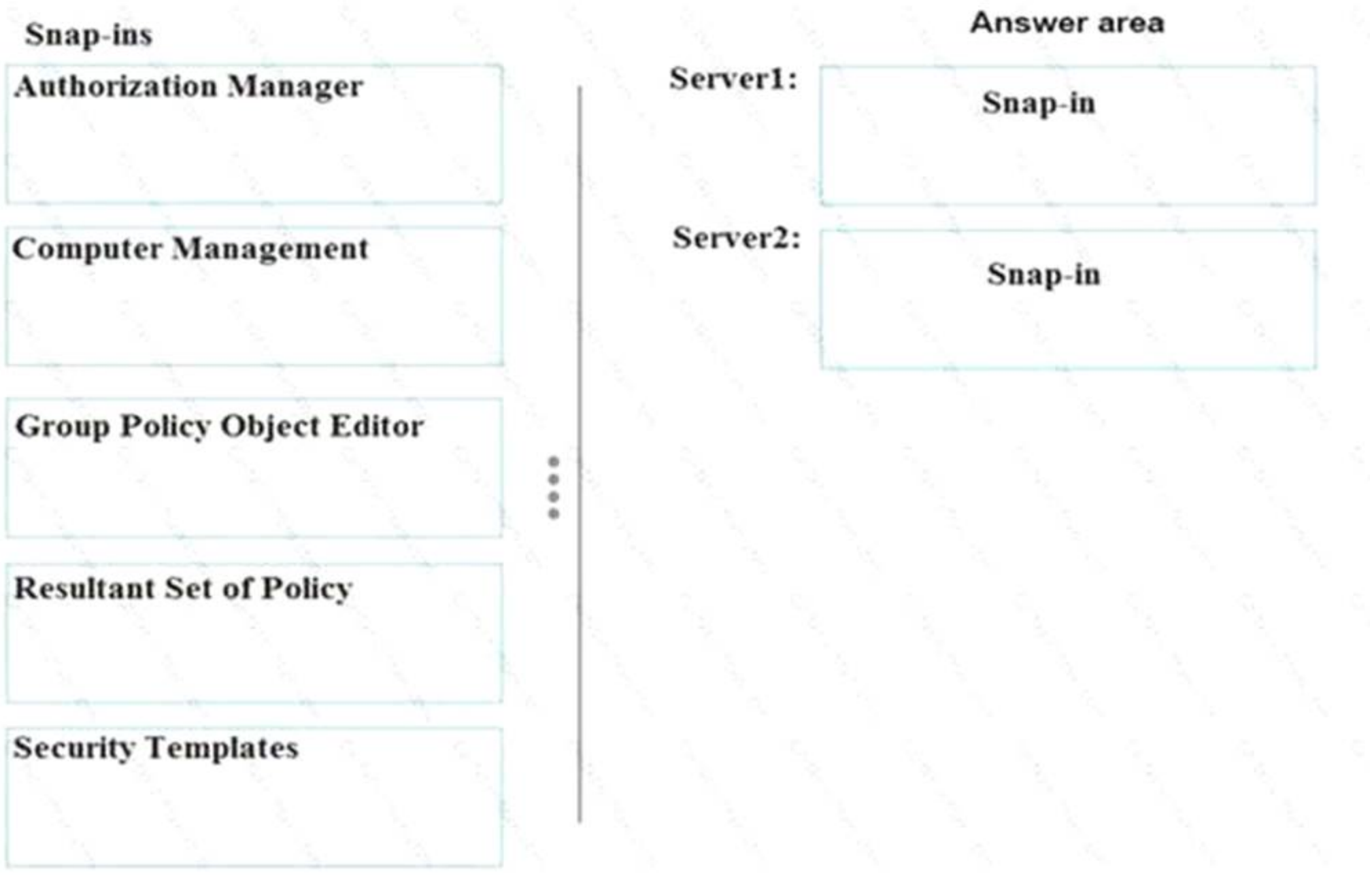
A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:
https://msdn.microsoft.com/library/cc875821.aspx#EJAA
https://www.serverbrain.org/managing-security-2003/using-the-cipher-command-to-add-datarecovery- agent.html

NEW QUESTION 220
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.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 223
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

70-744 Practice Exam Features:

* 70-744 Questions and Answers Updated Frequently

* 70-744 Practice Questions Verified by Expert Senior Certified Staff

* 70-744 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 70-744 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year