Microsoft

Exam Questions 70-744

Securing Windows Server 2016

NEW QUESTION 1
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this 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 one physical computer and configure it as a Hyper-V host that runs Windows Server 2016. You create 10 virtual machines and configure each one 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 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 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 Group Policy Management, You create an Applocker rule.

A. Yes
B. No

Answer: B

Explanation:
AppLocker does not filter incoming network traffic, what you actually need is Windows Firewall Inbound Rule on the Private profile.
https://technet.microsoft.com/en-us/library/dd759068(v=ws.11).aspx

NEW QUESTION 3
Note: This question b 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 contow.com. All servers run Windows Server 2016. All client computers run Windows 10.
The relevant objects in the domain are configured as shown in the following table.

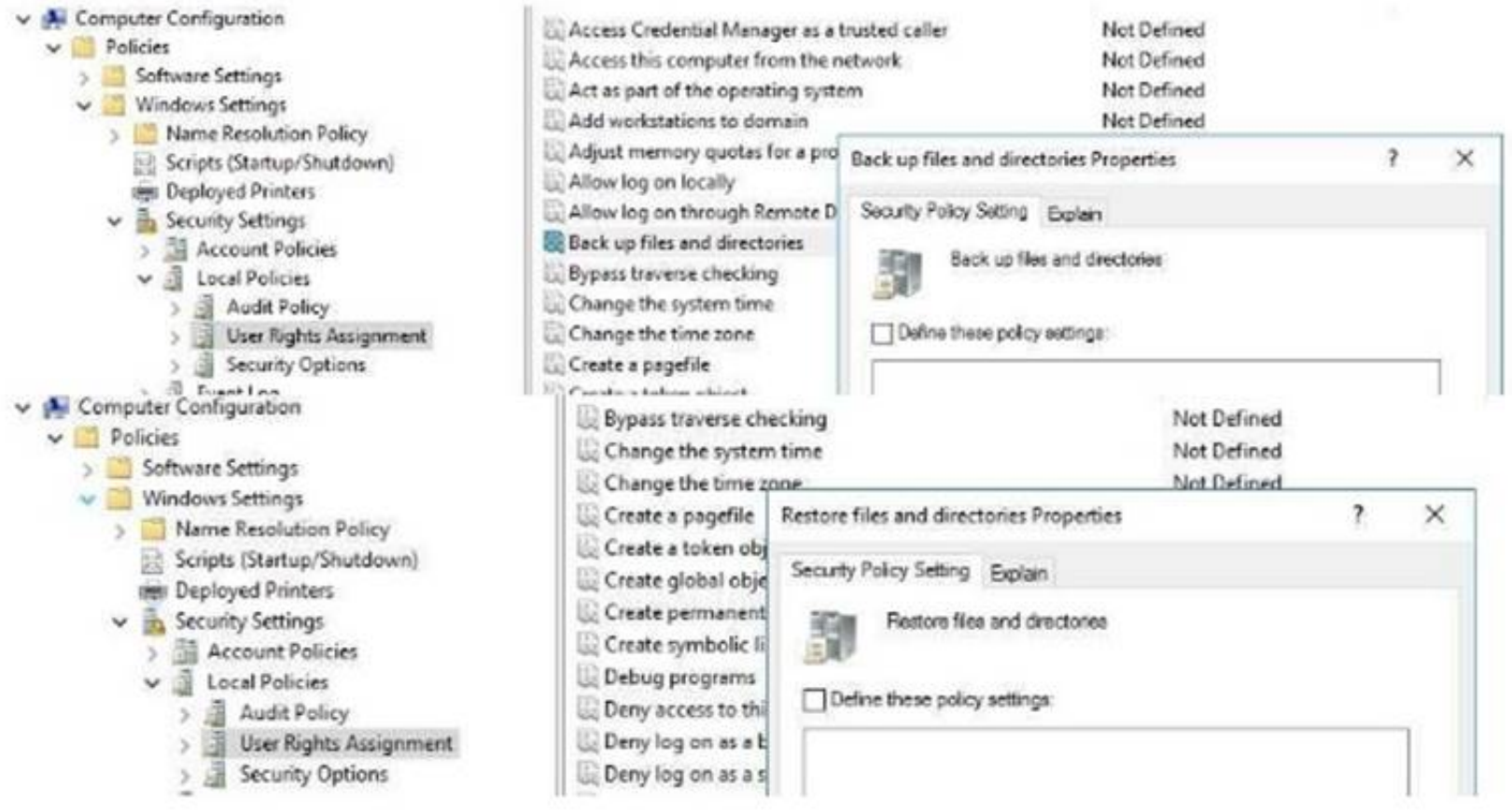
Server name	Object	Organizational unit (OU) name
Server1	Computer account	Servers
Server2	Computer account	Servers
User1	User account	Operations Users

You need to assign User1 the right to restore files and folders on Server1 and Server2.
Solution: You create a Group Policy object (GPO), link it to the Operations Users OU, and modify the Users Rights Assignment in the GPO.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Yes, in “User Rights Assignment” section of a GPO, two settings for assigning backup and restore user rights are available as follow:



NEW QUESTION 4
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 5
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2016. Server1 is configured as a domain controller.
You configure Server1 as a Just Enough Administration (JEA) endpoint You configure the required JEA rights for a user named User1.
You need to tell User1 how to manage Active Directory objects from Server2. What should you tell User1 to do first on Server2?

A. From a command prompt, run ntdsutil.exe.
B. From Windows PowerShell, run the Import-Module cmdlet.
C. From Windows PowerShell run the Enter-PSSession cmdlet.
D. Install the management consoles for Active Directory, and then launch Active Directory Users and Computer.

Answer: C

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

NEW QUESTION 6
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 7
Your network contains an Active Directory domain named contoso.com. The domain contains four servers. The servers are configured as shown in the following table.

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

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

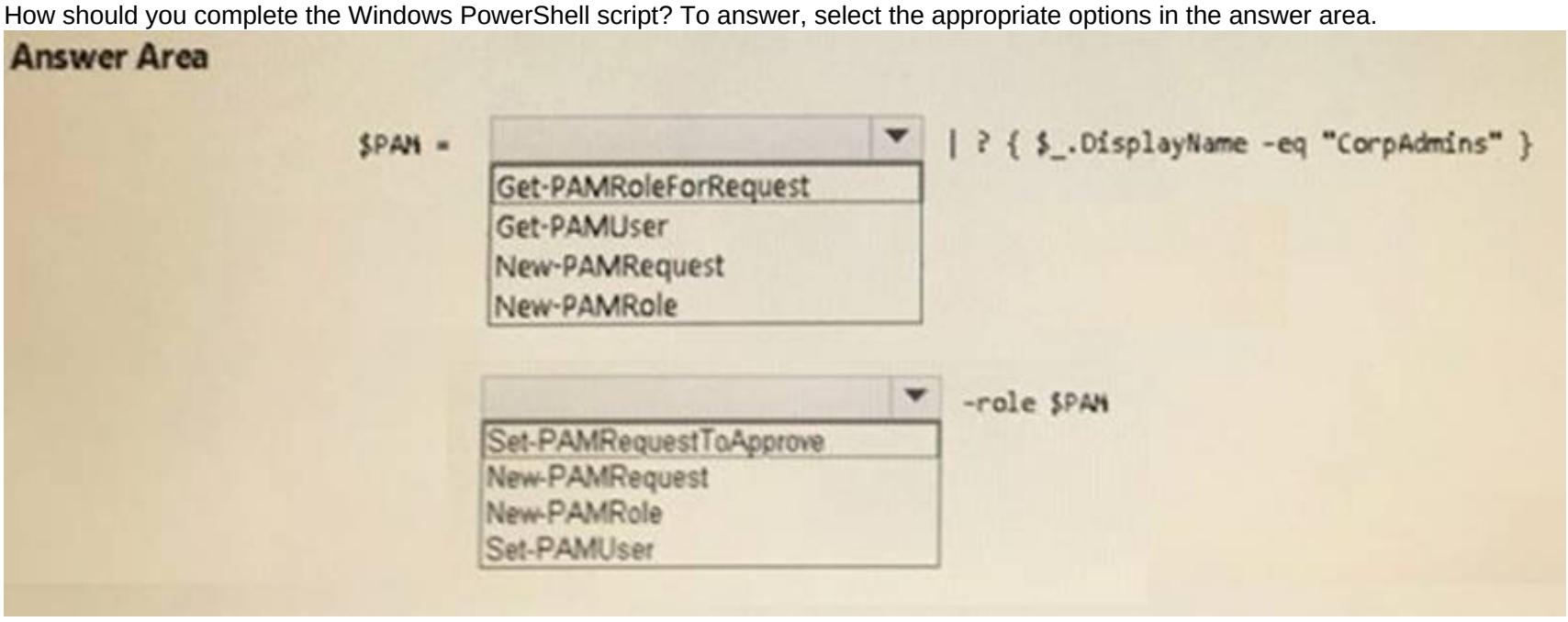
A. Install Microsoft .NET Framework 4.6.2 on FS1
B. Upgrade DC1 to Windows Server 2016
C. Install Windows Management Framework 5.0 on FS2.
D. Deploy Microsoft Identity Manager (MIM) 2016 to the domai

Answer: C

Explanation:
https://msdn.microsoft.com/en-us/library/dn896648.aspx
The current release of JEA is available on the following platforms:
-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 FS1 is ready to be managed by JEA, but FS2 need some extra work to do, either upgrade it to Windows Server 2016 or install Windows Management Framework 5.0 installed,

NEW QUESTION 8
HOTSPOT

Your network contains an Active Directory forest named contoso.com. The forest has Microsoft Identity Manager (MIM) 2016 deployed. You implement Privileged Access Management (PAM).
You need to request privileged access from a client computer in contoso.com by using PAM.
How should you complete the Windows PowerShell script? To answer, select the appropriate options in the answer area.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
$PAM = Get-PAMRoleForRequest | ? {$_,DisplayName -eq “CorpAdmins” } New-PAMRequest -role $PAM
References:
https://technet.microsoft.com/en-us/library/mt604089.aspx https://technet.microsoft.com/en-us/library/mt604084.aspx

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

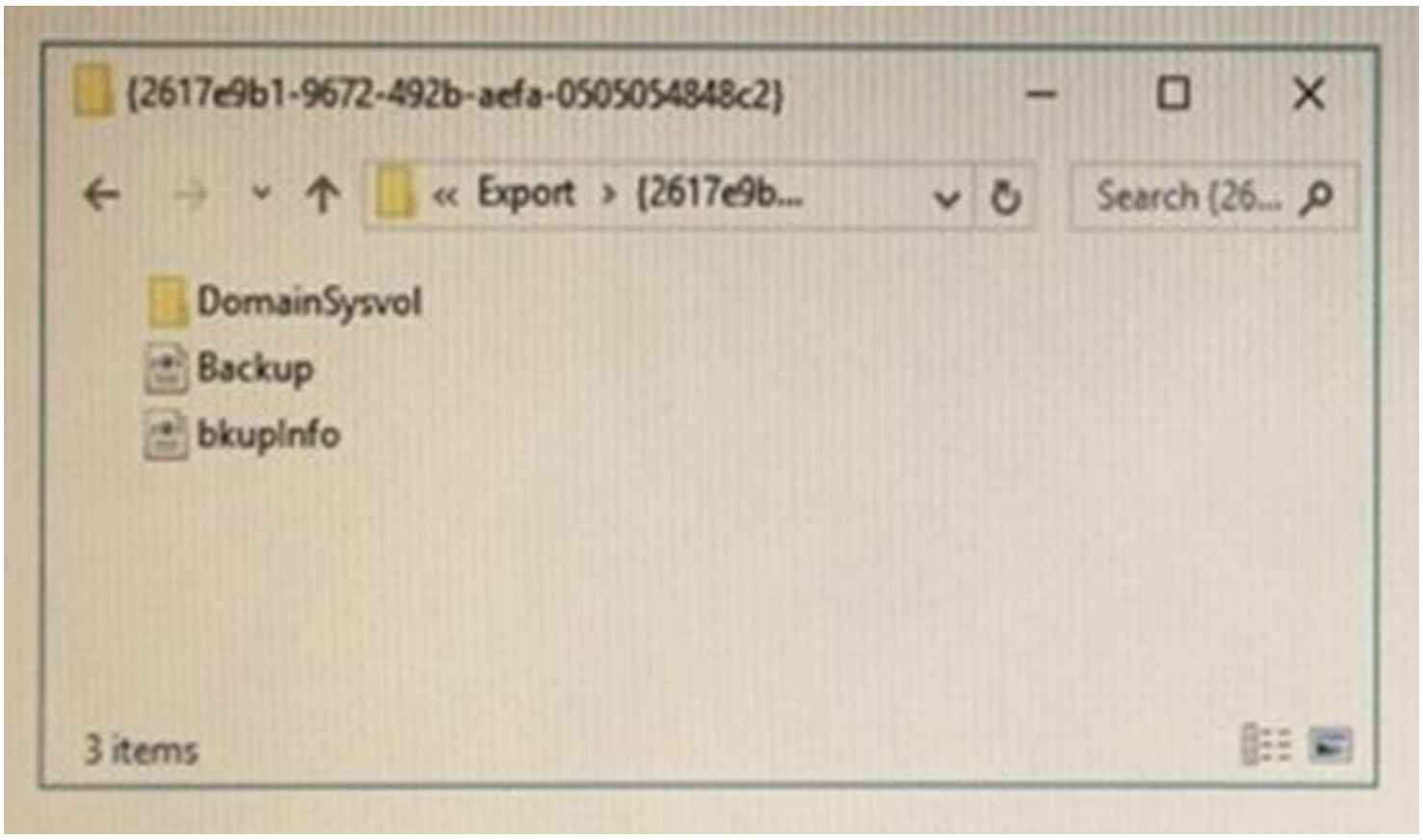
A. Provide a Privileged Access Workstation (PAW) for each user account in both forest
B. Join each PAW to the contoso.com domain.
C. Provide a Pnvileged Access Workstation (PAW) for each user in the contoso.com forest Join each PAW to the contoso.com domain.
D. Provide a Pnvileged Access Workstation (PAW) for each administrato
E. Join each PAW to the contoso.com domain.
F. Provide a Pnvileged Access Workstation (PAW) for each administrato
G. Join each PAW to the contosoadmin.com domain.

Answer: D

Explanation:
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securingprivilegedaccess- reference-material

- **Workstation Hardening** - Build the administrative workstations using the Privileged Access Workstations (through Phase 3), but change the domain membership to the administrative forest instead of the production environment.

NEW QUESTION 10
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

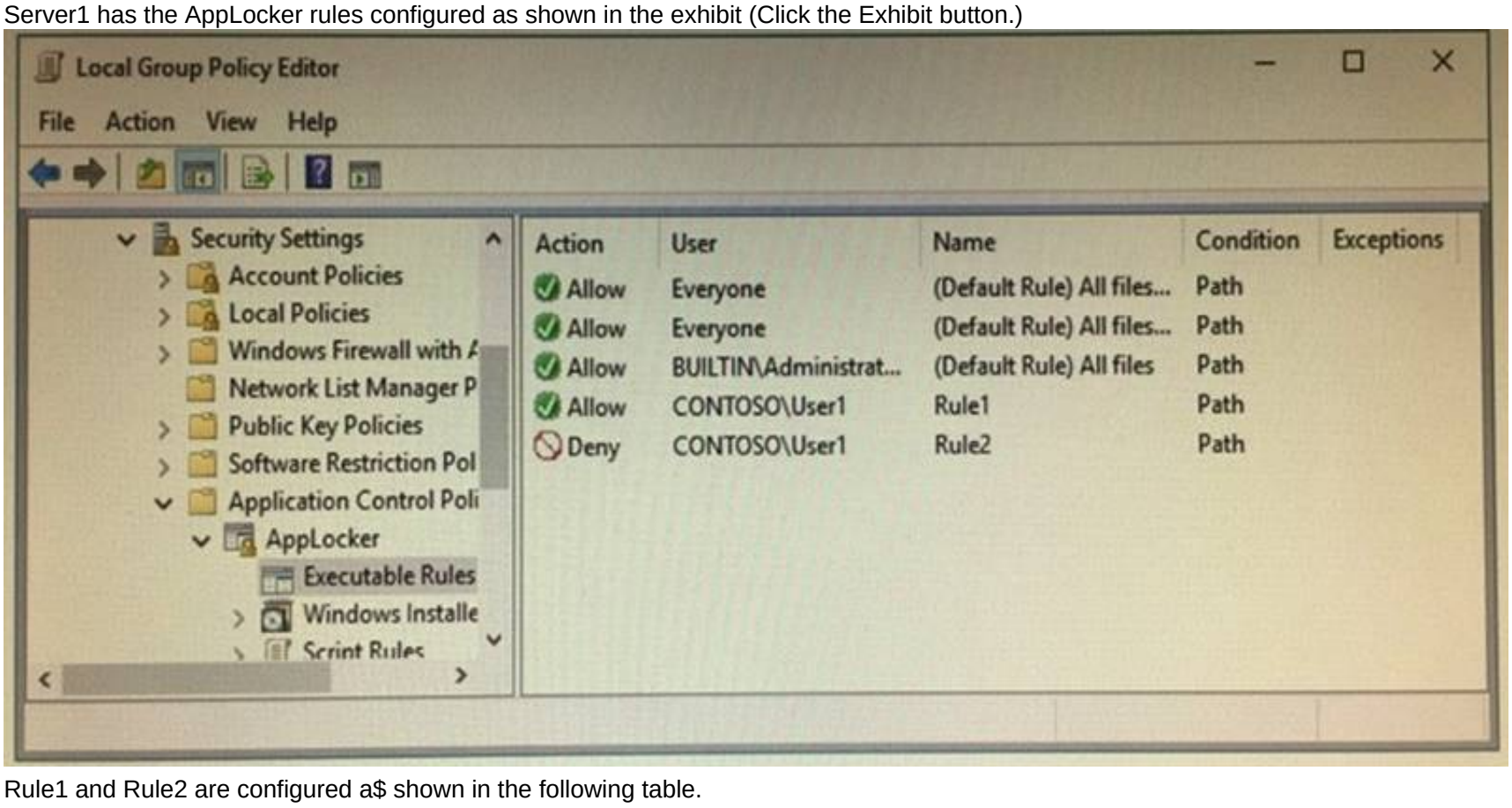
Explanation:
References:
https://anytecho.wordpress.com/2015/05/22/importing-group-policies-using-powershell-almost/

NEW QUESTION 10
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.
The services on Server1 are shown in the following output.

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

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

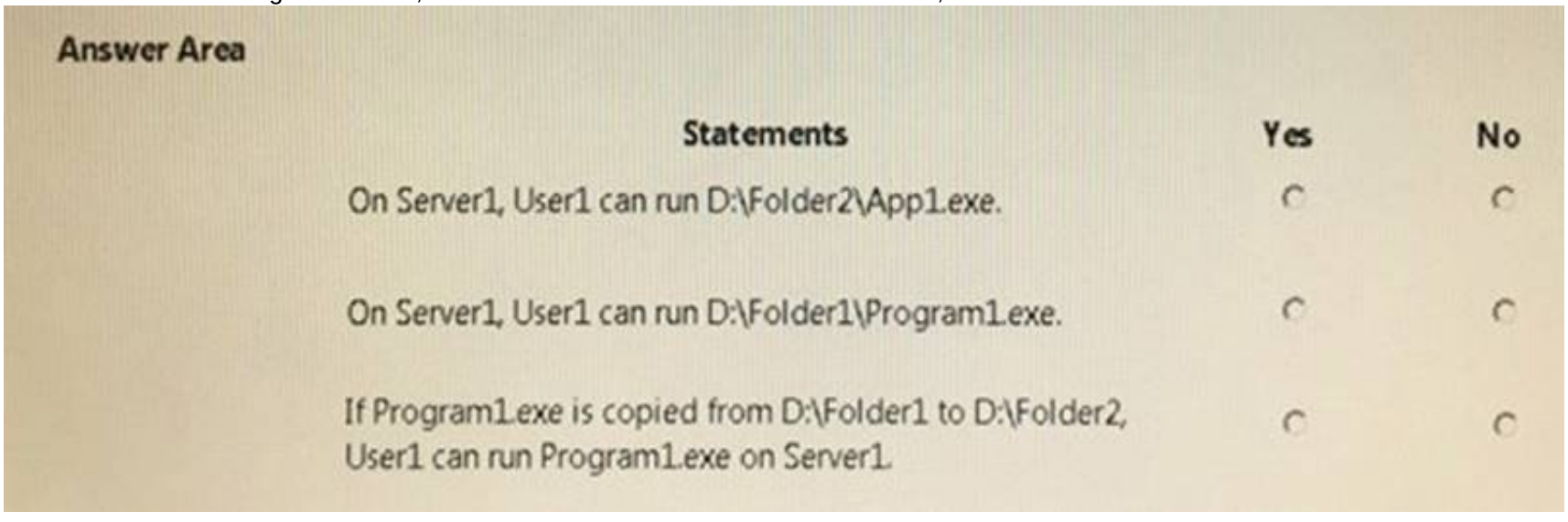
Server1 has the AppLocker rules configured as shown in the exhibit (Click the Exhibit button.)



Rule1 and Rule2 are configured a$ shown in the following table.

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

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

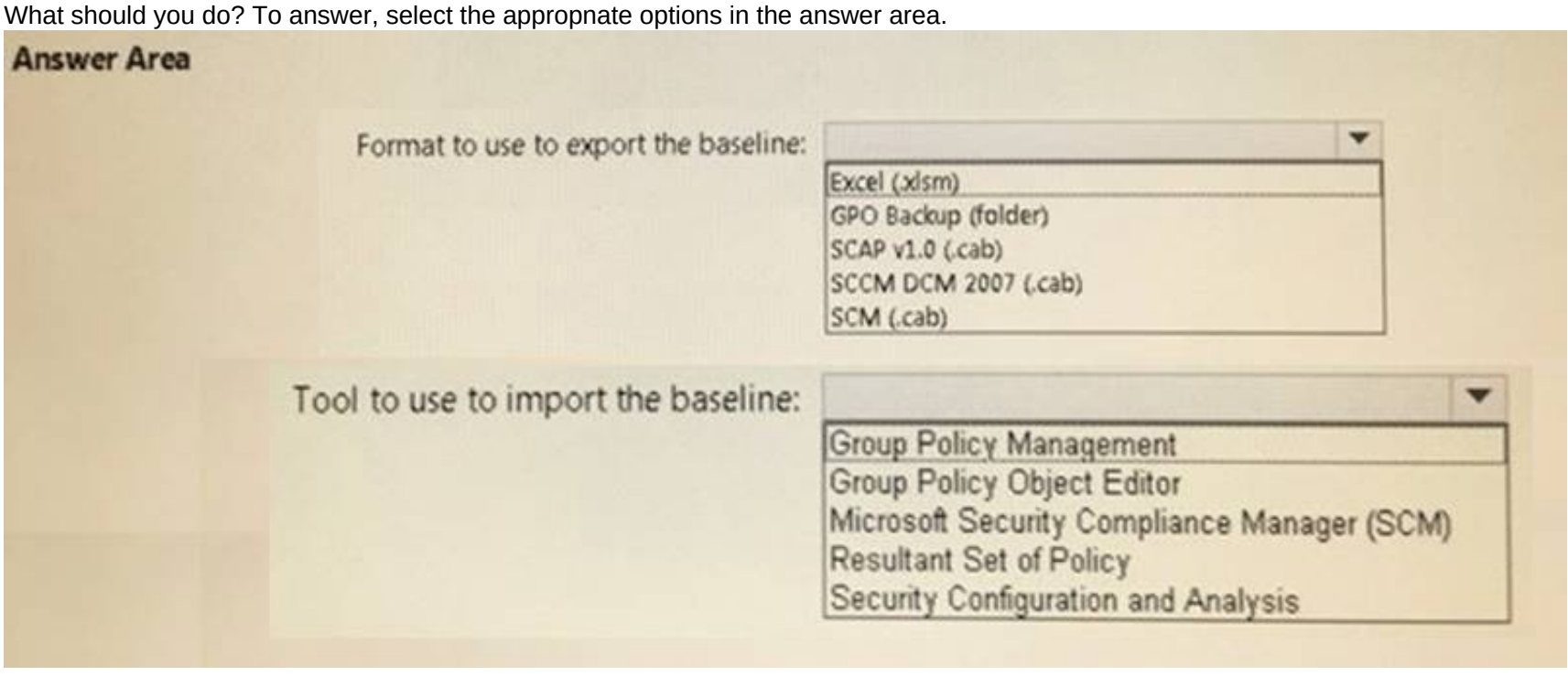


A. Mastered
B. Not Mastered

Answer: A

Explanation:
On Server1, User1 can run D:\\Folder2\\App1.exe : Yes On Server1, User1 can run D:\\Folder1\\Program1.exe : Yes
If Program1 is copied from D:\\Folder1 to D:\\Folder2, User1 can run Program1.exe on Server1 : NO
https://docs.microsoft.com/en-us/windows/device-security/applocker/configure-the-applicationidentity- service
The Application Identity service determines and verifies the identity of an app. Stopping this service will prevent AppLocker policies from being enforced.
In this question, Server1's Application Identity service is stopped, therefore, no more enforcement on AppLocker rules, everyone could run everything on Server1.

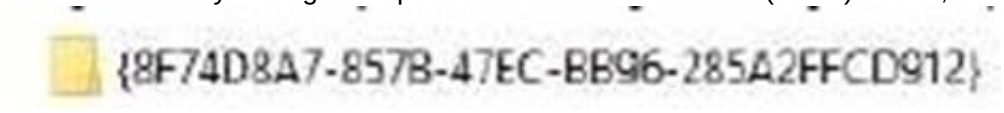
NEW QUESTION 15
HOTSPOT
Your network contains an Active Directory domain named contoso.com. You have an organizational unit (OU) named Secure that contains all servers.
You install Microsoft Security Compliance Manager (SCM) 4.0 on a server named Server1. You need to export the SCM Pnnt Server Secunty 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.



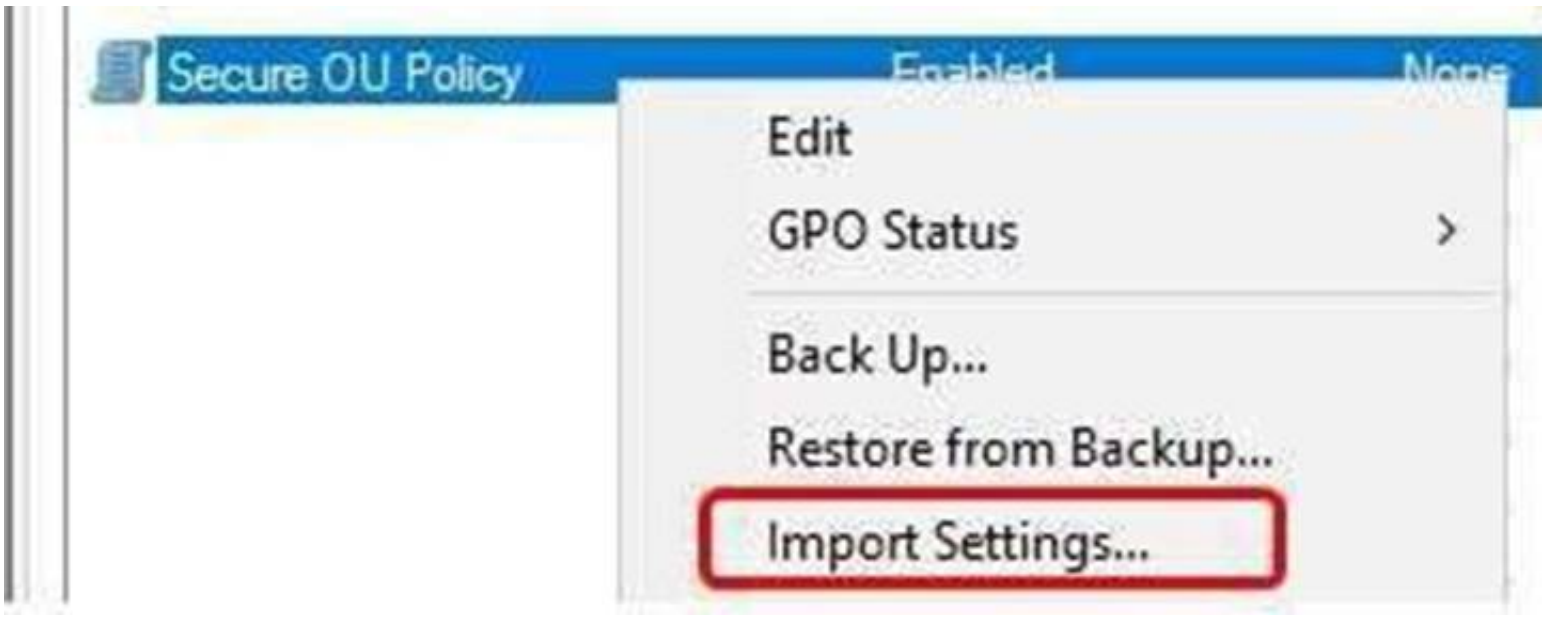
A. Mastered
B. Not Mastered

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 18
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server5 that has the Windows Server Update Services server role installed. You need to configure Windows Server Update Services (WSUS) on Server5 to use SSI. You install a certificate in the local Computer store.
Which two tools should you use? Each correct answer presents part of the solution.

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

Answer: AC

Explanation:
By IIS Manager and “wsusutil configuressl” command https://technet.microsoft.com/en-us/library/bb633246.aspx To configure SSL on the WSUS server by using IIS 7.0
1) On the WSUS server, open Internet Information Services (IIS) Manager.
2) Expand Sites, and then expand the Web site for the WSUS server. We recommend that you use the WSUS Administration custom Web site, but the default Web
site might have been chosen when WSUS was being installed.
3) Perform the following steps on the APIRemoting30, ClientWebService, DSSAuthWebService, ServerSyncWebService, and SimpleAuthWebService virtual directories that reside under the WSUS Web site.
In Features View, double-click SSL Settings.
On the SSL Settings page, select the Require SSL checkbox. Ensure that Client certificates is set to Ignore.
In the Actions pane, click Apply.
4) Close Internet Information Services (IIS) Manager.
5) Run the following command from <WSUS Installation Folder>\\Tools: WSUSUtil.exe configuressl
<Intranet
FQDN of the software update point site system>.

NEW QUESTION 22
Your network contains an Active Directory domain named conioso.com. The domain contains 1,000 client computers that run Windows 8.1 and 1,000 client computers that run Windows 10.
You deploy a Windows Server Update Services (WSUS) server. You create a computer group tor each organizational unit (OU) that contains client computers.
You configure all of the client computers to receive updates from WSUS.
You discover that all of the client computers appear m the Unassigned Computers computer group in the Update Services console.
You need to ensure that the client computers are added automatically to the computer group that corresponds to the location of the computer account in Active Directory.
Which two actions should you perform? Each correct answer presents part of the solution.

A. From Group Policy objects (GPOs), configure the Enable client-side targeting setting.
B. From the Update Services console, configure the Computers option.
C. From Active Directory Users and Computers, create a domain local distribution group for each WSUS computer group.
D. From Active Directory Users and Computers, modify the flags attnbute of each OU.
E. From the Update Services console, run the WSUS Server Configuration Wizar

Answer: AB

NEW QUESTION 24
Note: This question Is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. Server1 has a volume named Volume1.
A central access policy named Policy1 is deployed to the domain. You need to apply Policy1 to Volume1.
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

Explanation:

"File Explorer" = "Windows Explorer".
https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/deploy-a-centralaccess- policy–demonstration-steps-#BKMK_1.4

NEW QUESTION 27
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 30
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 33
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

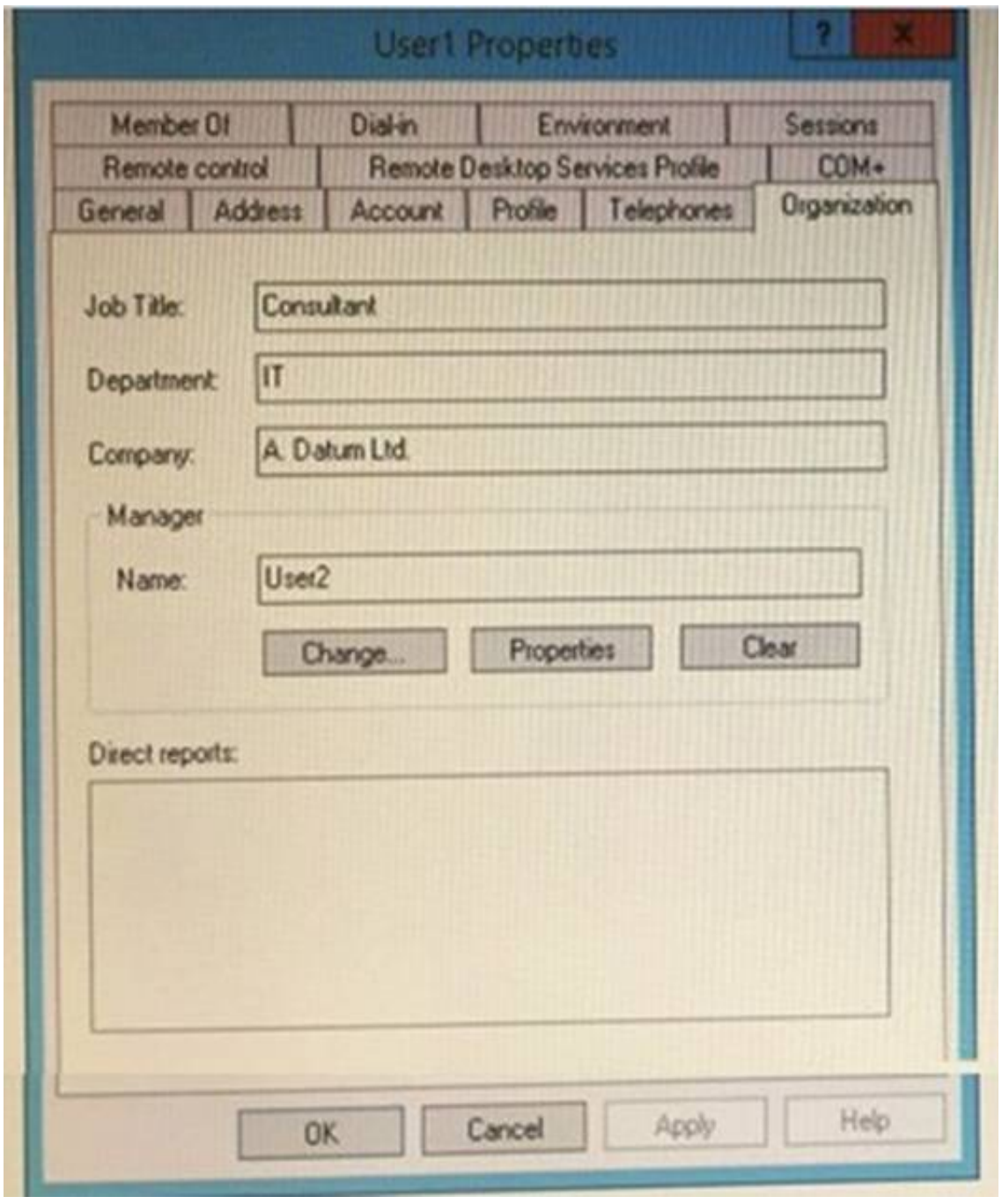
Explanation:
https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-prerequisites
ATA Center which is the first component to be deployed on Server1, requires the use of SSL protocol to communicate with ATA Gateway
To ease the installation of ATA, you can install self-signed certificates during 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 35
Your network contains an Active Directory domain named contoio.com. The domain contains a server named Server1 that runs Windows Server 2016.
You have an organizational unit (OU) named Administration that contains the computer account of Server1.
You import the Active Directory module to Served1.
You create a Group Policy object (GPO) named GPO1 You link GPO1 to the Administration OU. You need to log an event each time an Active Directory cmdlet is executed successfully from Server1. What should you do?

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

Answer: C

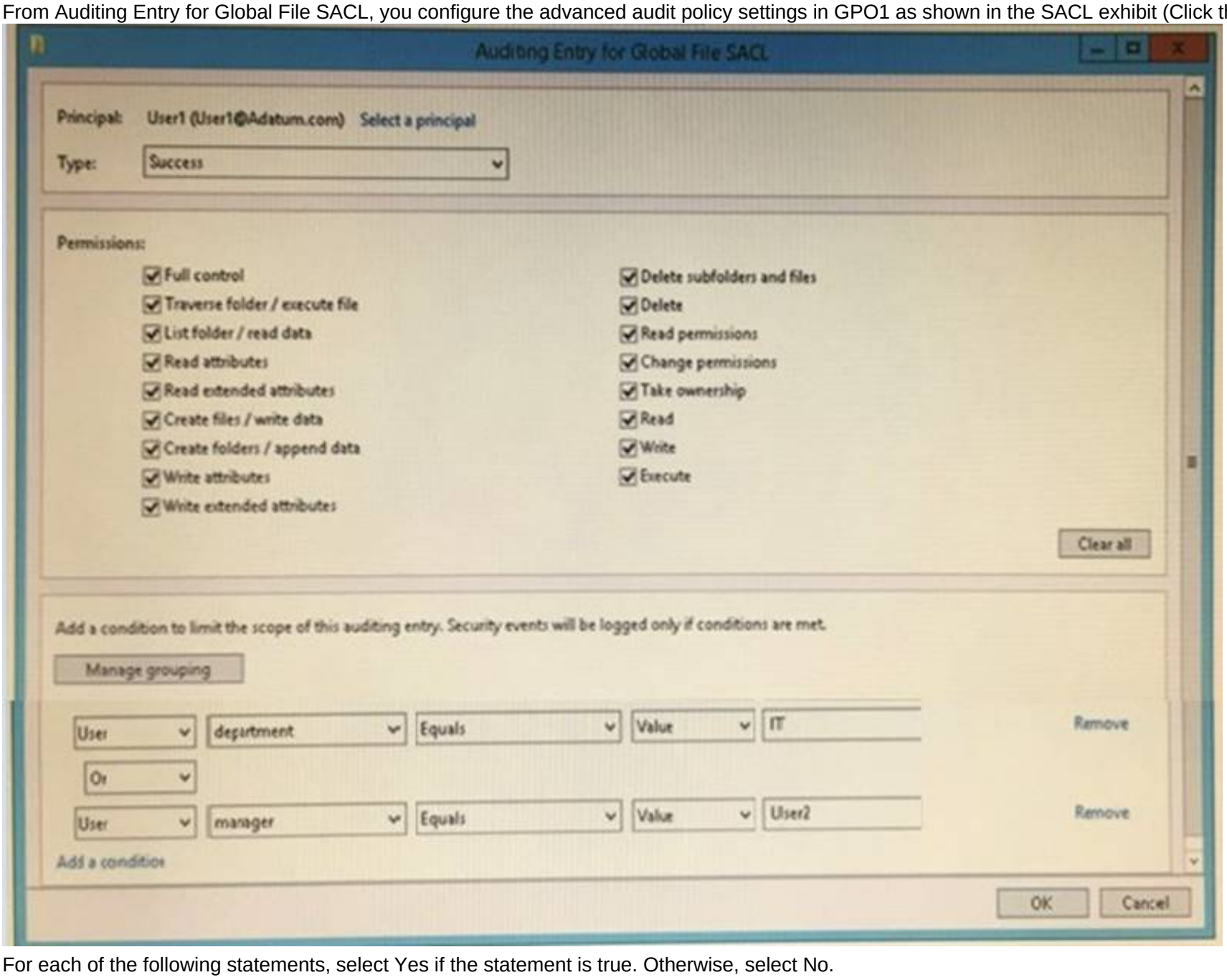
NEW QUESTION 37
HOTSPOT
Your network contains an Active Directory domain named adatum.com. The domain contains a file server named Server1 that runs Windows Server 2016.
You have an organizational unit (OU) named OU1 that contains Server1. You create a Group Policy object (GPO) named GPO1 and link GPO1 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.)



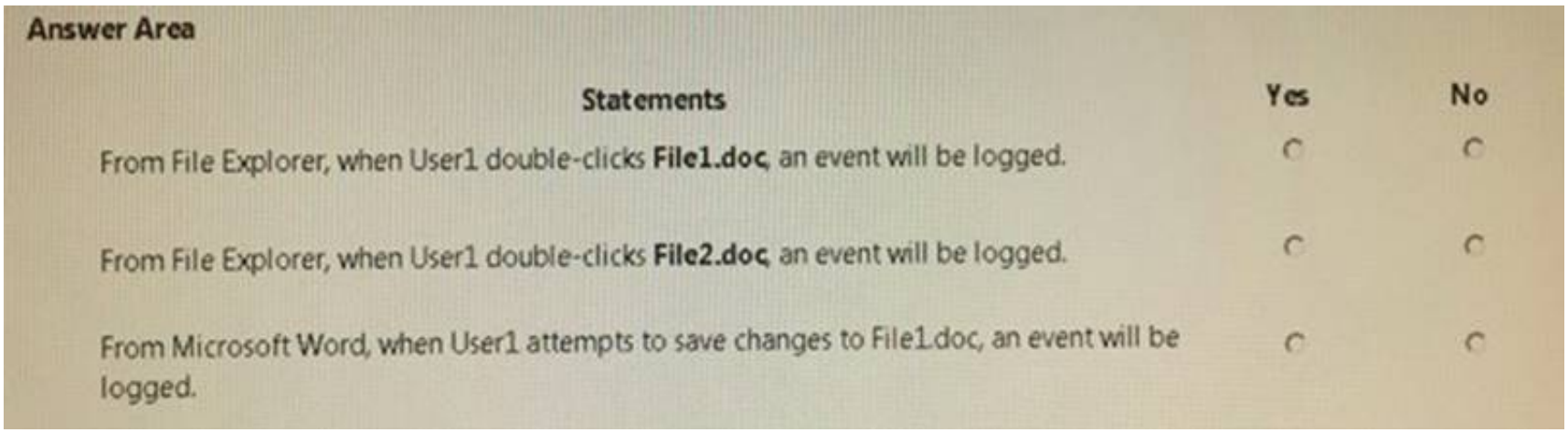
User1 has permissions to two files on Server1 configured as shown in the following table.

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

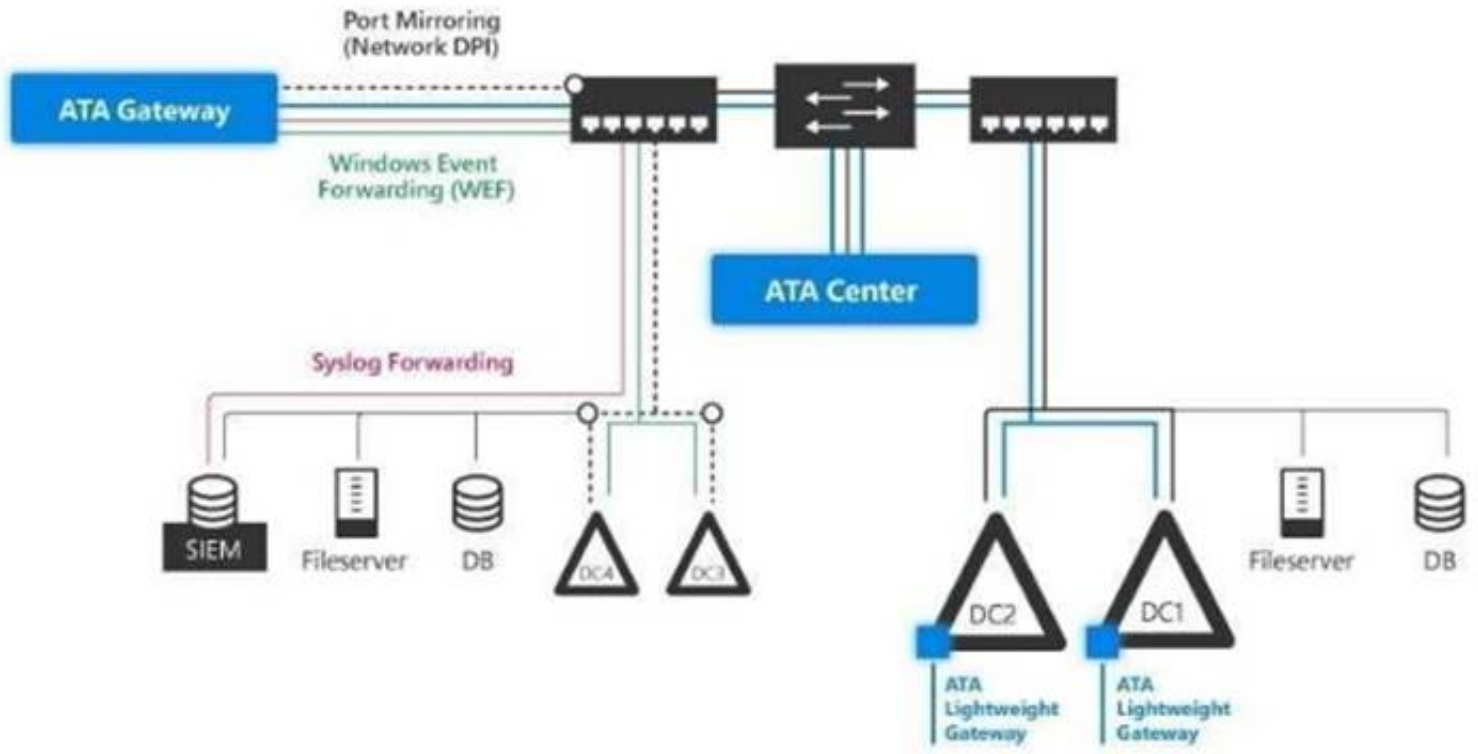
Explanation:
From File Explorer, when User1 double-clicks File1.doc. an event will be logged: Yes From File Explorer, when User1 double-clicks File2.doc. an event will be logged: No
From Microsoft Word, when User1 attempts to save changes to File1.doc, an event will be logged: No
From the SACL, only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

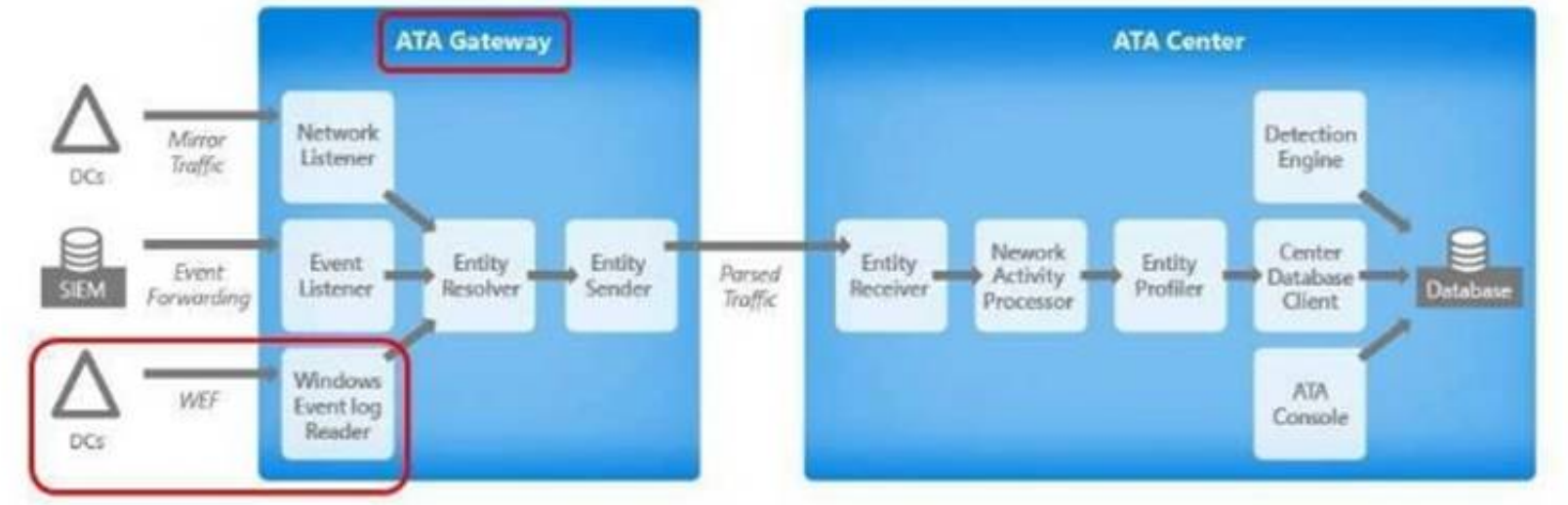
NEW QUESTION 40
Your network contains an Active Directory domain named contoso.com.
You are deploying Microsoft Advanced Threat Analytics (ATA) to the domain.
You install the ATA Center on server named Server1 and the ATA Gateway on a server named Served. You need to ensure that Server2 can collect NTLM 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.

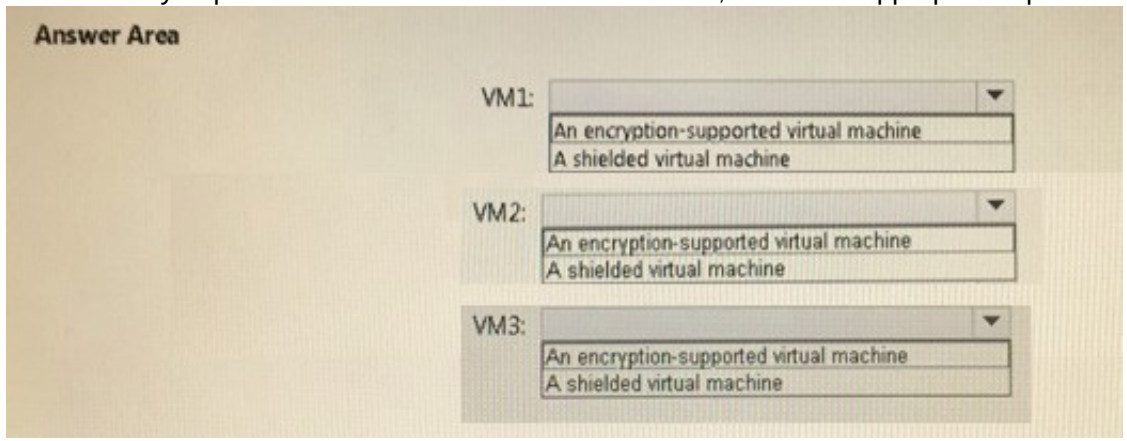




NEW QUESTION 43
HOTSPOT
You plan to deploy three encrypted virtual machines that use Secure Boot. The virtual machines will be configured as shown in the following table.

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

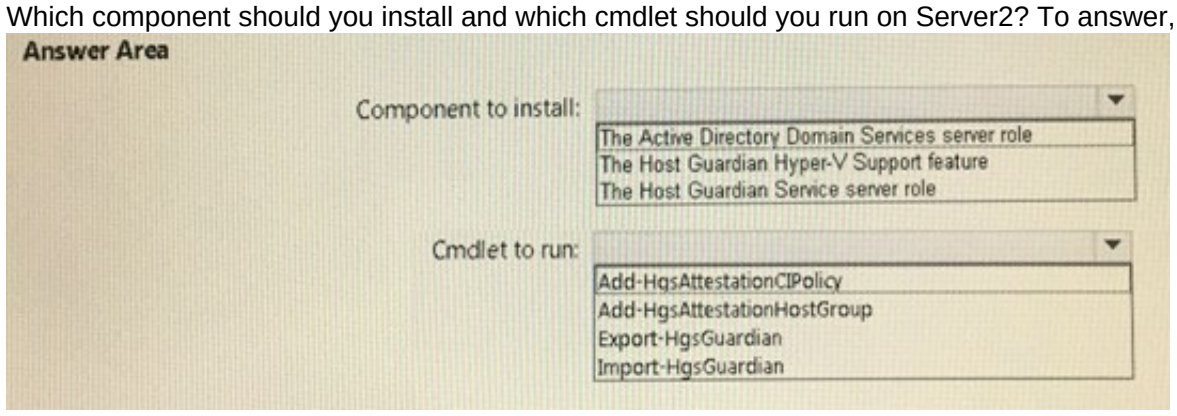
Answer: A

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 44
HOTSPOT
Your network contains two Active Directory forests named contoso.com and adatum.com. Contoso.com contains a Hyper-V host named Server1. Server1 is a member of a group named HyperHosts. Adatum.com contains a server named Server2. Server1 and Server2 run Windows Server 2016.
Contoso.com trusts adatum.com.
You plan to deploy shielded virtual machines to Server1 and to configure Admin-trusted attestation on Server2.
Which component should you install and which cmdlet should you run on Server2? To answer, select the appropriate options in the answer area.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Key for this question is Admin-trusted attestation or (AD mode) for guarded fabric “Server1.contoso.com”, while Server2.adatum.com is running the Host Guardian Service.

- **Hardware**: One host is required for initial deployment. To test Hyper-V live migration for shielded VMs, you must have at least two hosts.

  Hosts must have:
  - IOMMU and Second Level Address Translation (SLAT)
  - TPM 2.0
  - UEFI 2.3.1 or later
  - Configured to boot using UEFI (not BIOS or "legacy" mode)
  - Secure boot enabled

- **Operating system**: Windows Server 2016 Datacenter edition

  > ⓘ Important
  >
  > Make sure you install the latest cumulative update.

- **Role and features**: Hyper-V role and the Host Guardian Hyper-V Support feature. The Host Guardian Hyper-V Support feature is only available on Datacenter editions of Windows Server 2016.

https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shieldedvm/guarded-fabricguarded-host-prerequisites
https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shieldedvm/guarded-fabricconfirm-hosts-can-attest-successfully

A fabric administrator needs to confirm that Hyper-V hosts can run as guarded hosts. Complete the following steps on at least one guarded host:

1. If you have not already installed the Hyper-V role and Host Guardian Hyper-V Support feature install them with the following command:

```
Install-WindowsFeature Hyper-V, HostGuardian -IncludeManagementTools -Restart
```

2. Configure the host's Key Protection and Attestation URLs:

- **Through Windows PowerShell**: You can configure the Key Protection and Attestation URLs by executing the following command in an elevated Windows PowerShell console. For <FQDN>, use the Fully Qualified Domain Name (FQDN) of your HGS cluster (for example, hgs.relecloud.com, or ask the HGS administrator to run the **Get-HgsServer** cmdlet on the HGS server to retrieve the URLs).

```
Set-HgsClientConfiguration -AttestationServerUrl 'http://<FQDN>/Attestation' -KeyProtectionServerUrl
'http://<FQDN>/KeyProtection'
```

NEW QUESTION 48
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 51
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

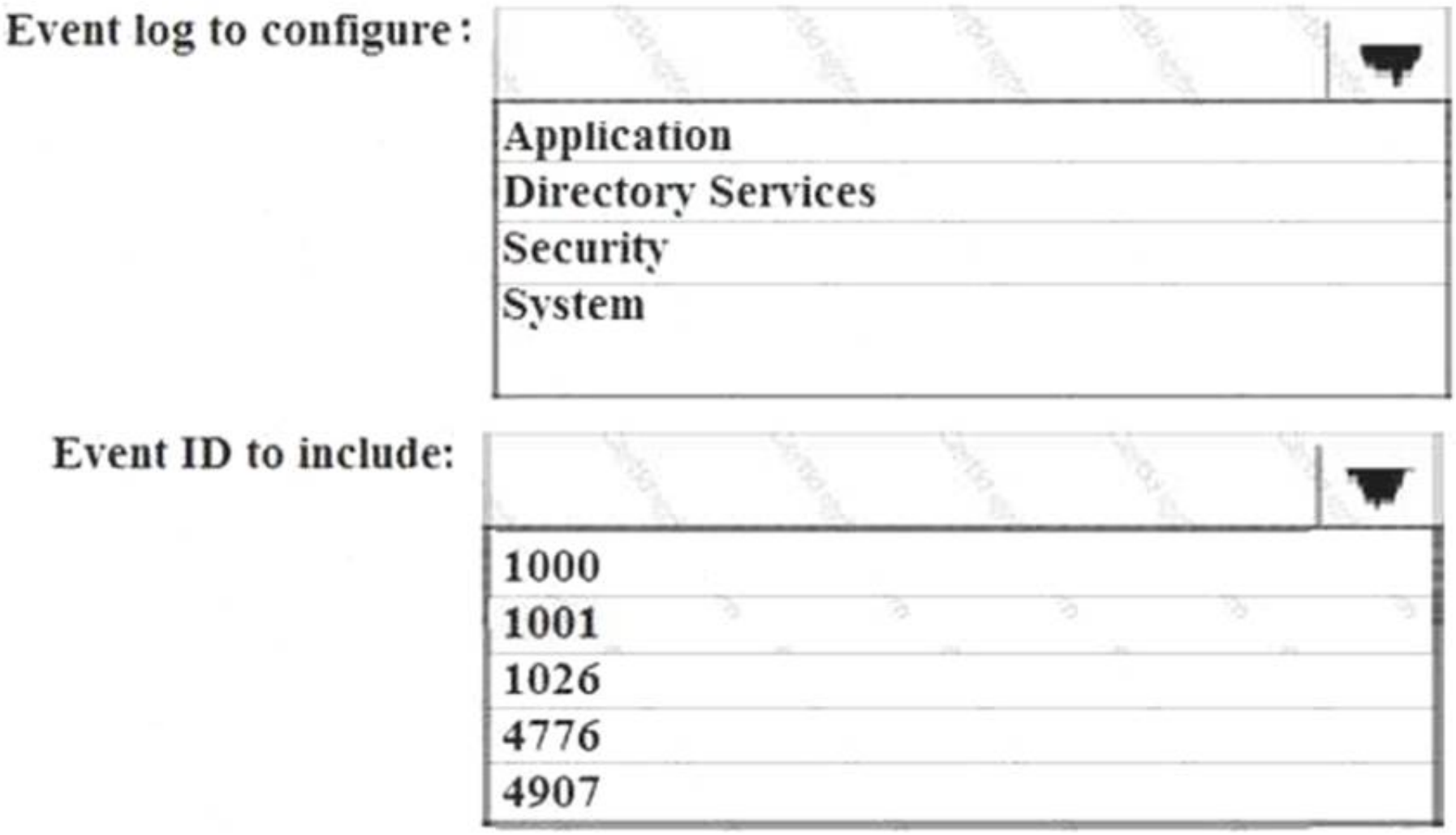
NEW QUESTION 55
Windows Firewall rules can be configured using PowerShell.
The “Set-NetFirewallProfile” cmdlet configures settings that apply to the per-profile configurations of the Windows Firewall with Advanced Security.
What is the default setting for the AllowInboundRules parameter when managing 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.

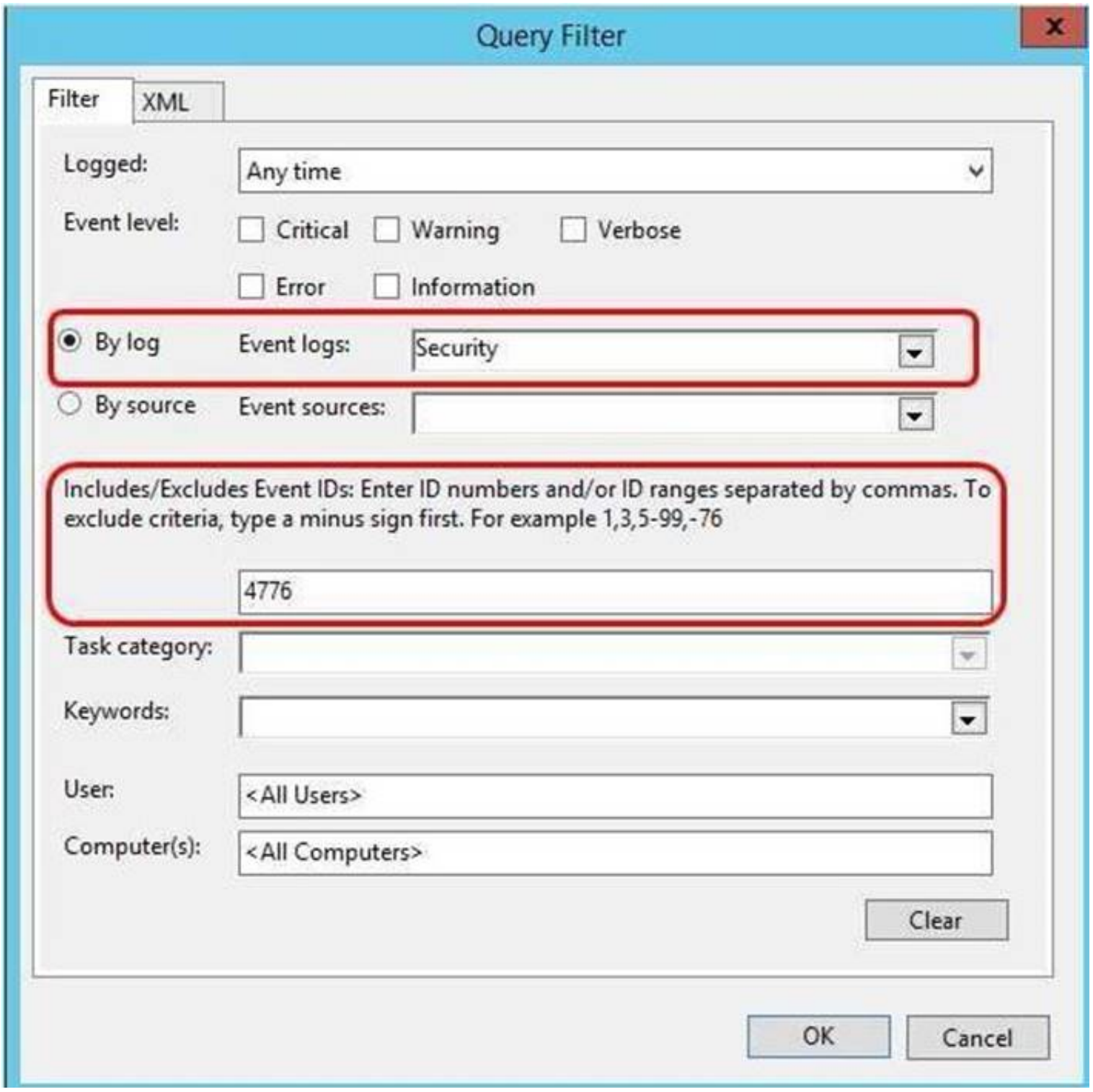
NEW QUESTION 58
HOTSPOT
Your network contains an Active Directory domain named contoso.com.
You are deploying Microsoft Advanced Threat Analytics (ATA) to the domain. You install the ATA Gateway on a server named Server1.
To assist in detecting Pass-the-Hash attacks, you plan to configure ATA Gateway to collect events. You need to configure the query filter for event subscriptions on Server1.
How should you configure the query filter? To answer, select the appropriate options in the answer aree.



A. Mastered
B. Not Mastered

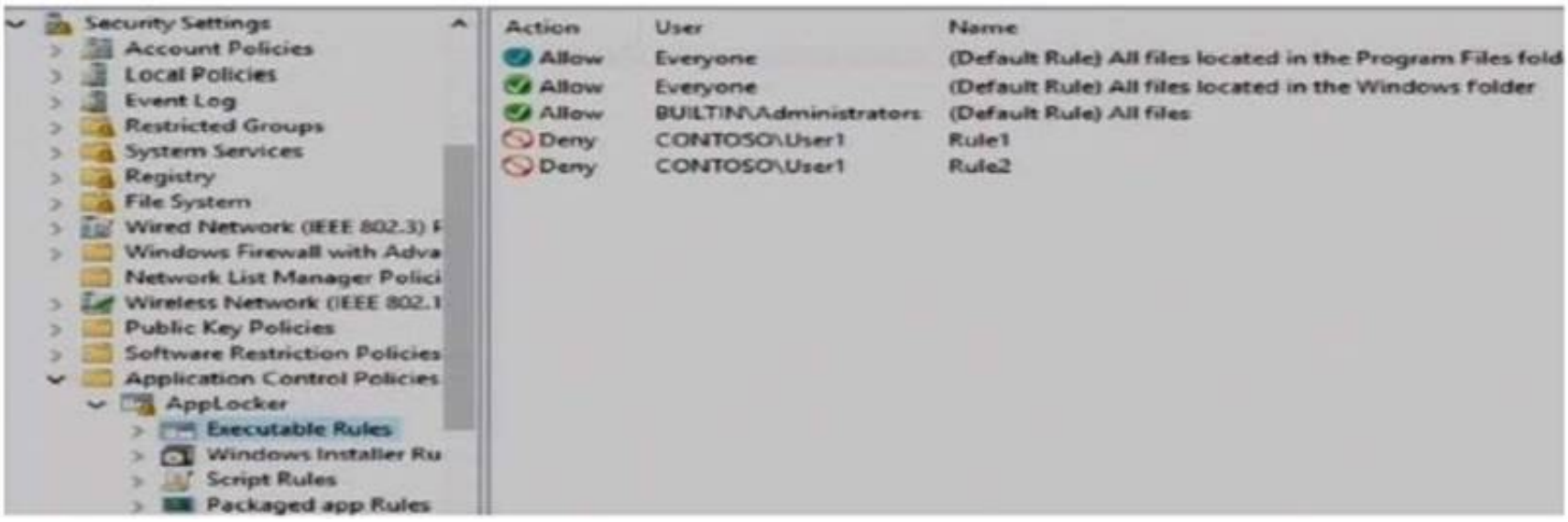
Answer: A

Explanation:
https://docs.microsoft.com/en-us/advanced-threat-analytics/configure-event-collection
To enhance detection capabilities, ATA needs the following Windows events: 4776, 4732, 4733, 4728, 4729, 4756, 4757.These can either be read automatically by the ATA Lightweight Gateway or in case the ATA Lightweight
Gateway is not deployed,
it can be forwarded to the ATA Gateway in one of two ways, by configuring the ATA Gateway to listen for SIEM events or by configuring Windows Event Forwarding.



Event ID: 4776 NTLM authentication is being used against domain controller Event ID: 4732 A User is Added to Security-Enabled DOMAIN LOCAL Group, Event ID: 4733 A User is removed from Security-Enabled DOMAIN LOCAL Group Event ID: 4728 A User is Added or Removed from Security-Enabled Global Group
Event ID: 4729 A User is Removed from Security-Enabled GLOBAL Group
Event ID: 4756 A User is Added or Removed From Security-Enabled Universal Group Event ID: 4757 A User is Removed From Security-Enabled Universal Group

NEW QUESTION 62
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

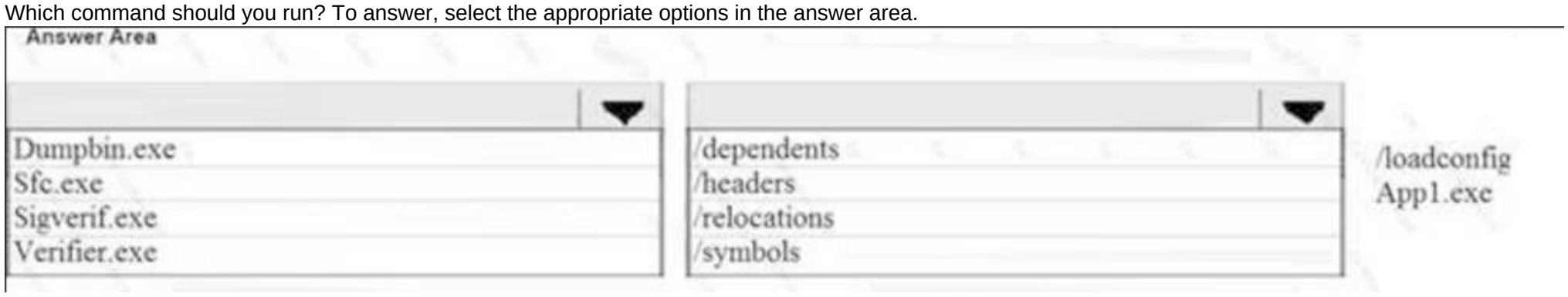
D. User1 can run D:\\Folder2\\App2.exe if App2.exe is moved to another folder
E. User1 can run D:\\Folder2\\App2.exe if App2.exe is renamed
F. User1 can run D:\\Folder2\\App2.exe if App2.exe is upgraded

Answer: AF

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

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.

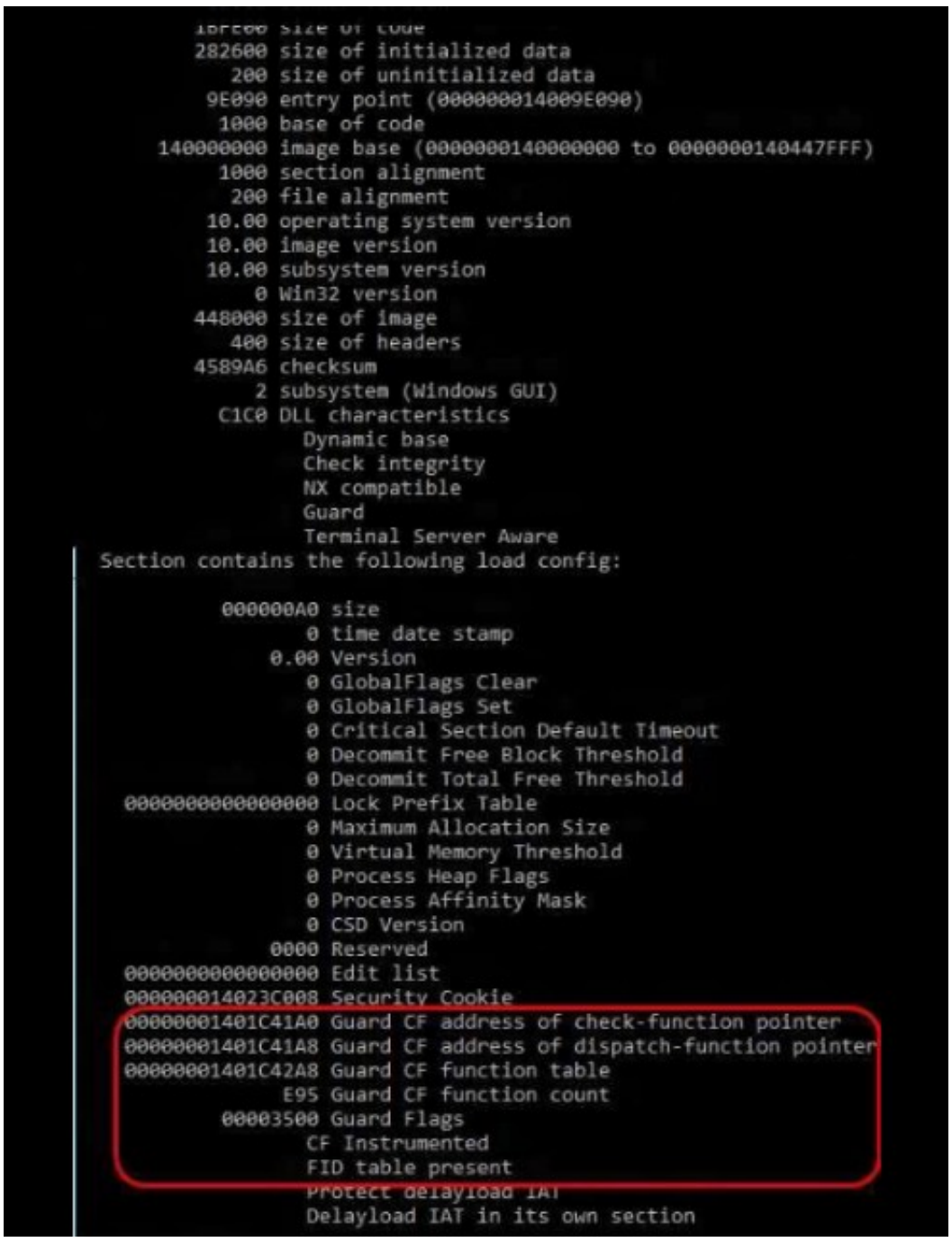
NEW QUESTION 65
HOTSPOT
Your network contains an Active Directory domain named contoso.com. You plan to deploy an application named App1.exe.
You need to verify whether Control Flow Guard is enabled for App1.exe.
Which command should you run? To answer, select the appropriate options in the answer area.



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 67
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 prepare the environment to support applying Update1 to the laptops only. What should you do? Choose Two.

A. Tool to use: Active Directory Administrative Center
B. Tool to use: Active Directory Users and Computers
C. Tool to use: Microsoft Intune
D. Tool to use: Update Services
E. Type of object to create: A computer group
F. Type of object to create: A distribution group
G. Type of object to create: A mobile device group
H. Type of object to create: A security group
I. Type of object to create: An OU

Answer: DE

Explanation:
https://technet.microsoft.com/en-us/library/cc708458(v=ws.10).aspx

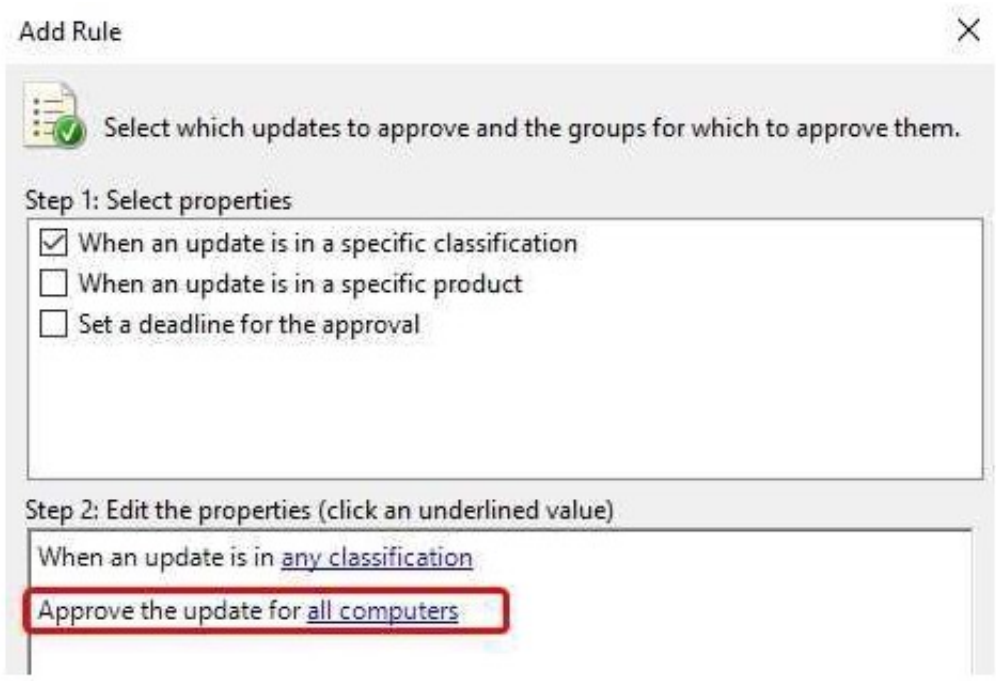
Automatically Approving Updates for Detection

When you select this option, you can create a rule that your WSUS server will automatically apply during synchronization. For the rule, you specify what updates you want to automatically approve for detection, by update classification and by computer group. This applies only to new updates, as opposed to revised updates. This setting is available on the **Automatic Approval Options** page.

On this page, you can also set a rule for automatically approving updates for installation. In the event that rules conflict (for example, you have specified the same update classification and same computer group combination in both the rule to automatically approve for detection and automatically approve for installation), then your WSUS server applies the rule to automatically approve for installation.

To automatically approve updates for detection

1. On the WSUS console toolbar, click **Options**, and then click **Automatic Approval Options**.
2. In **Updates**, under **Approve for Detection**, select the **Automatically approve updates for detection by using the following rule** check box (if it is not already selected).
3. If you want to specify update classifications to automatically approve during synchronization, do the following:
   - Next to **Classifications**, click **Add/Remove Classifications**.
   - In the **Add/Remove Classifications** dialog box, select the update classifications that you want to automatically approve, and then click **OK**.
4. If you want to specify the computer groups for which to automatically approve updates during synchronization:
   - Next to **Computer groups**, click **Add/Remove Computer Groups**.
   - In the **Add/Remove Computer Groups** dialog box, select the computer groups for which you want to automatically approve updates, and then click **OK**.
5. Under **Tasks**, click **Save settings**, and then click **OK**.



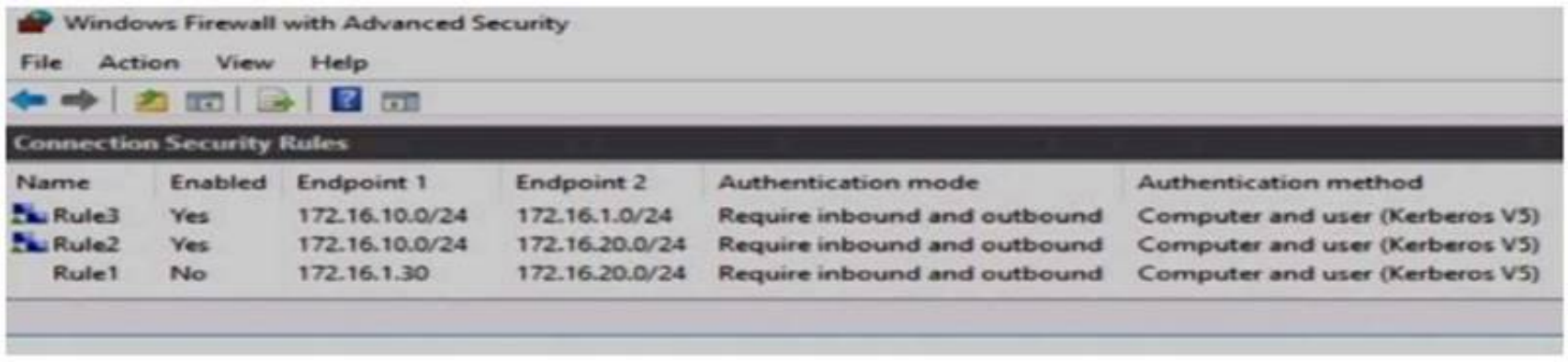
NEW QUESTION 68
HOTSPOT
Your network contains an Active Directory named contoso.com.
The domain contains the computers configured as shown in the following table.

Name	IP address
Server1	172.16.1.30
Computer1	172.16.10.60
Computer2	172.16.20.50

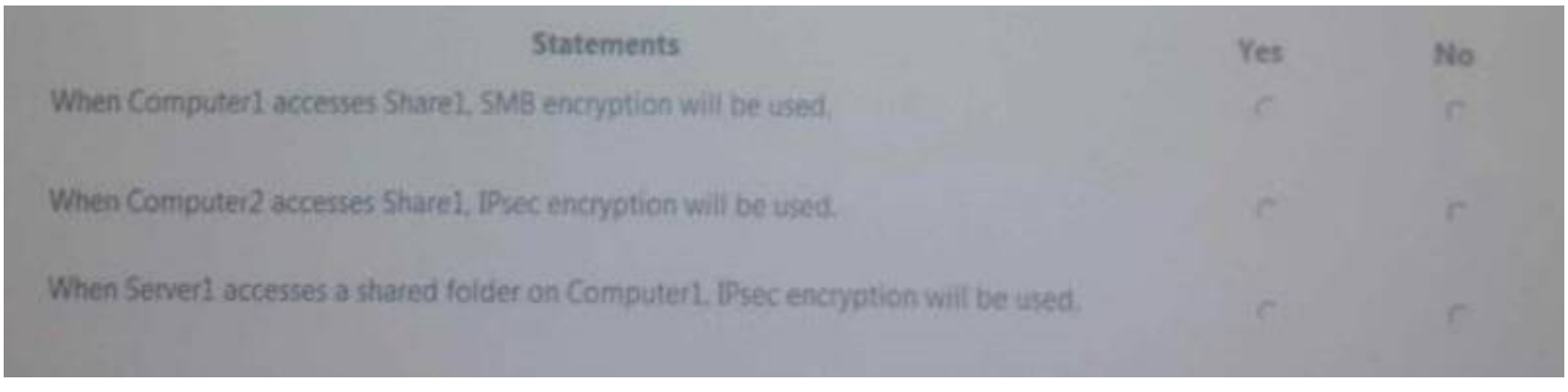
Server1 has a share named Share1 with the following configurations:-

PresetPathAcl	:System.Security.AccessControl.DirectorySecurity
ShareState	:Online
AvailabilityType	:NonClustered
ShareType	:FileSystemDirectory
FolderEnumerationMode	: Unrestricted
CachingMode	:Manual
SmbInstance	:Default
CATimeout	:0
ConcurrentUserLimit	:0
ContinuouslyAvailable	:False
CurrentUsers	:0
Description	:
EncryptData	:True
Name	:Share1
Path	:C:/Shares/Share1
Scoped	:False
ScopeName	:*
SecurityDescriptor	:O:BAG:DUD:(A;OICI;FA;;;WD)
ShadowCopy	:False
Special	:False
Temporary	:False
Volume	: \\?\Volume{18eb1d3f-0000-0000-0000-501f00000000}\
PSComputerName	:
CimClass	:ROOT/Microsoft/Windows/SMB:MSFT_SmbShare
CimInstanceProperties	:{AvailabilityType, CachingMode, CATimeout, ConcurrentUserLimit…}
CimSystemProperties	: Microsoft.Management.Infrastructure.CimSystemProperties

Server1, Computer1, and Computer2 have the connection security rules configured as shown in follow:-



Please Select the correct statement as below:



A. Mastered
B. Not Mastered

Answer: A

Explanation:
When Computer1 accesses Share1, SMB encryption will be used: YES When Computer2 accesses Share1, SMB encryption will be used: YES

When Server1 accesses a shared folder on Computer1, IPsec encryption will be used: NO
The shared folder “Share1” is configured with “EncryptData : True”, no matter which network the client resides, SMB 3 communication will be encrypted.
When Server1 access Computer1 over network, the original packet L3 IP Header is as follow:- 172.16.1.30 –> 172.16.10.60
These traffic does not match the enabled IPSec rule “Rule2” nor “Rule3”, and the only matching rule “Rule1” is disabled. So, no IPsec encryption will be achieved.

NEW QUESTION 72
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 77
You have a Hyper-V host named Hyperv1 that has a virtual machine named FS1. FS1 is a file server that contains sensitive data.
You need to secure FS1 to meet the following requirements:
-Prevent console access to FS1.
-Prevent data from being extracted from the VHDX file of FS1.
Which two actions should you perform? Each correct answer presents part of the solution.

A. Enable BitLocker Drive Encryption (BitLocker) for all the volumes on FS1
B. Disable the virtualization extensions for FS1
C. Disable all the Hyper-V integration services for FS1
D. On Hyperv1, enable BitLocker Drive Encryption (BitLocker) for the drive that contains the VHDX file for FS1.
E. Enable shielding for FS1

Answer: AE

Explanation:
-Prevent console access to FS1. –> Enable shielding for FS1
-Prevent data from being extracted from the VHDX file of FS1. –> Enable BitLocker Drive Encryption (BitLocker) for all the volumes on FS1

NEW QUESTION 80
You have two computers configured as shown in the following table.

Computer name	Operating system	Workgroup/domain
Client1	Windows 10 Pro, version 1607	Workgroup
Server1	Windows Server 2016 Standard	Domain named adatum.com

You need to ensure that the credentials that you use to establish Remote Desktop sessions from Client1 to Server1 are protected by using Remote CredentialGuard.

A. Join Client1 to the domain.
B. Remove Server1 from the domain.
C. Upgrade Server1 to Windows Server 2016 Datacenter.
D. Upgrade Client1 to Windows 10 Enterpris

Answer: A

Explanation:
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.

NEW QUESTION 84
Your data center contains 10 Hyper-V hosts that host 100 virtual machines.
You plan to secure access to the virtual machines by using the Datacenter Firewall service.
You have four servers available for the Datacenter Firewall service. The servers are configured as shown in the following table.

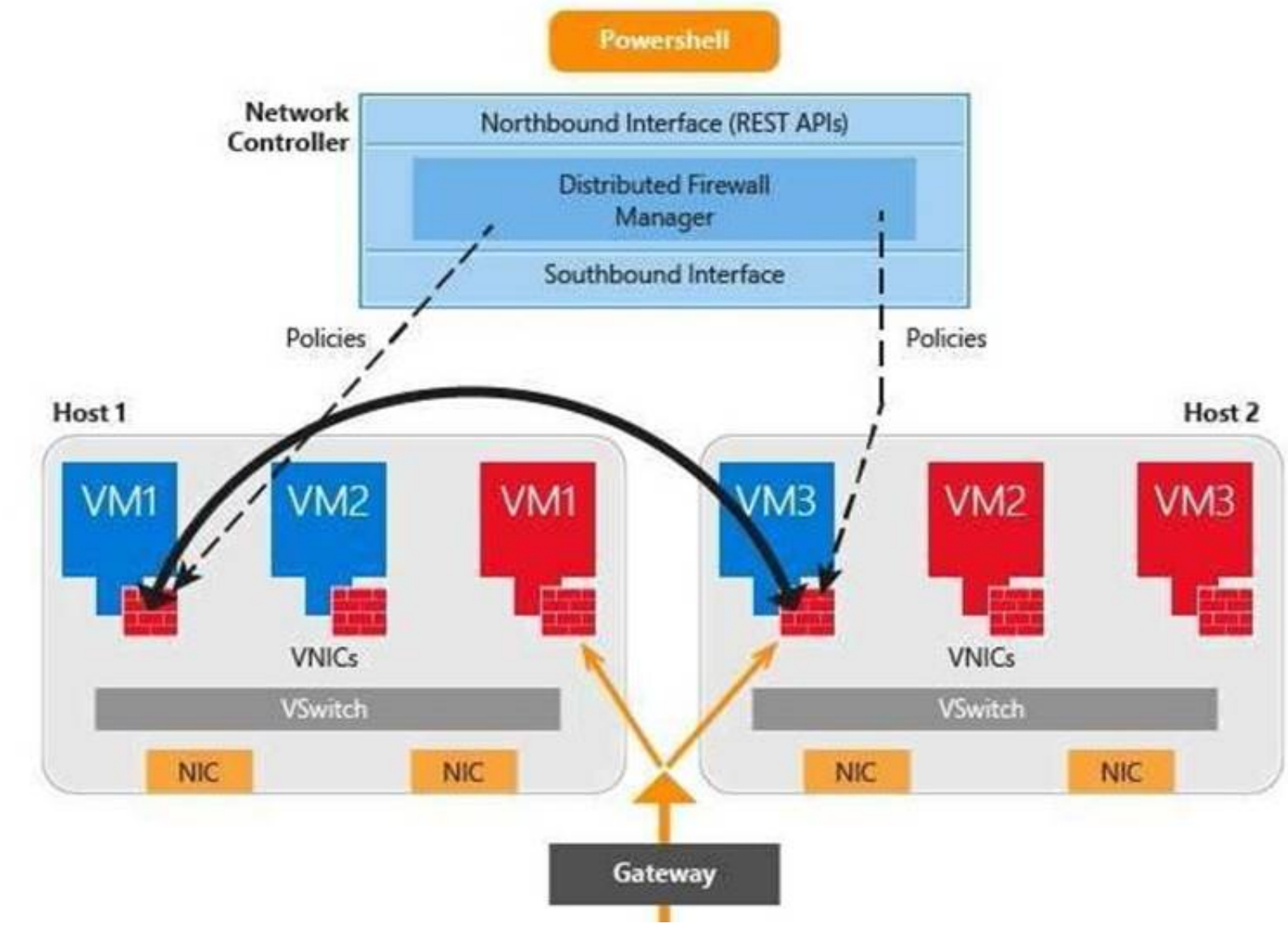
Server name	Platform	Windows Server 2016 edition
Server20	Physical	Standard
Server21	Physical	Standard
Server22	Virtual	Datacenter
Server23	Virtual	Datacenter

You need to install the required server roles for the planned deployment Which server role should you deploy? Choose Two.

A. Server role to deploy: Multipoint Services
B. Server role to deploy: Network Controller
C. Server role to deploy: Network Policy and Access Services
D. Servers on which to deploy the server role: Server20 and Server21
E. Servers on which to deploy the server role: Server22 and Server23

Answer: BE

Explanation:
Datacenter Firewall is a new service included with Windows Server 2016. It is a network layer, 5- tuple (protocol, source and destination port numbers, source and destination IP addresses), stateful, multitenant firewall. When deployed and offered as a service by the serviceprovider, tenant administrators can install and configure firewall policies to help protect their virtual networks from unwanted traffic originating from Internet and intranet networks.
https://docs.microsoft.com/en-us/windows-server/networking/sdn/technologies/networkcontroller/ networkcontroller
Network Controller Features
The following Network Controller features allow you to configure and manage virtual and physical network devices and services.
i) Firewall Management (Datacenter Firewall)
ii) Software Load Balancer Management
iii) Virtual Network Management
iv) RAS Gateway Management



https://docs.microsoft.com/en-us/windows-server/networking/sdn/plan/installation-andpreparationrequirements- for-deploying-network-controller
Installation requirements
Following are the installation requirements for Network Controller.
For Windows Server 2016 deployments, you can deploy Network Controller on one or more computers, one or more VMs, or a combination of computers and VMs.
All VMs and computers planned as Network Controller nodes must be running Windows Server 2016 Datacenter edition.

NEW QUESTION 88
Your network contains an Active Directory domain named contoso.com. The domain contains several shielded virtual machines.
You deploy a new server named Server1 that runs Windows Server 2016. You install the Hyper-V server role on Server1.
You need to ensure that you can host shielded virtual machines on Server1. What should you install on Server1?

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

Answer: A

Explanation:
This questions mentions “The domain contains several shielded virtual machines.”, which indicates a working Host Guardian Service deployment was completed.
https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shieldedvm/guarded-fabricguarded-host-prerequisites
For a new Hyper-V server to utilize an existing Host Guardian Service, install the “Host Guardian Hyper-V Support”.

Guarded hosts using TPM mode must meet the following prerequisites:

- **Hardware**: One host is required for initial deployment. To test Hyper-V live migration for shielded VMs, you must have at least two hosts.

  Hosts must have:
  - IOMMU and Second Level Address Translation (SLAT)
  - TPM 2.0
  - UEFI 2.3.1 or later
  - Configured to boot using UEFI (not BIOS or "legacy" mode)
  - Secure boot enabled

- **Operating system**: Windows Server 2016 Datacenter edition

  ⓘ Important

  Make sure you install the latest cumulative update.

- **Role and features**: Hyper-V role and the Host Guardian Hyper-V Support feature. The Host Guardian Hyper-V Support feature is only available on Datacenter editions of Windows Server 2016.

NEW QUESTION 92

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?

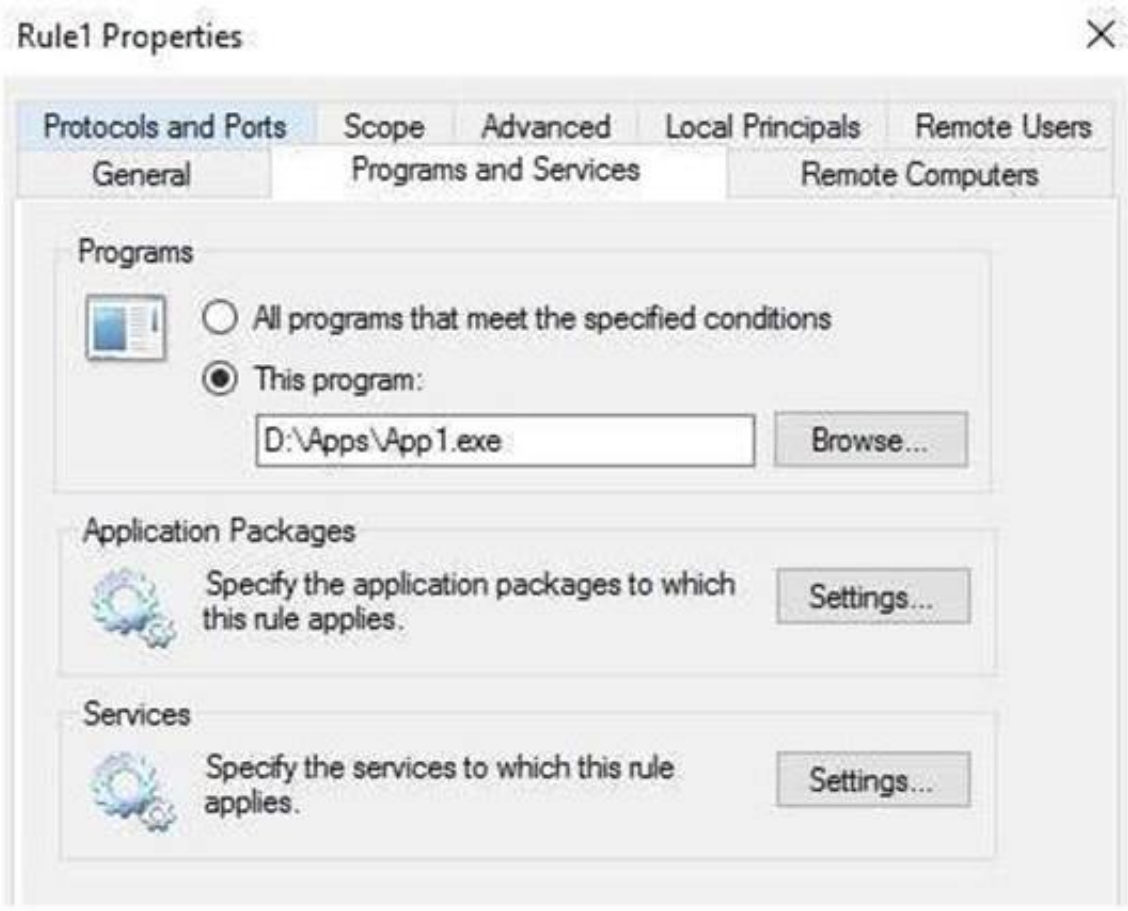
A. Yes
B. No

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 97
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 99
You have a server named Server1 that runs Windows Server 2016.
You need to identify whether ICMP traffic is exempt from IPsec on Server1. Which cmdlet should you use?

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

Answer: D

Explanation:
The Get-NetFirewallSetting cmdlet retrieves the global firewall settings of the target computer. The NetFirewallSetting object specifies properties that apply to the firewall and IPsec settings, no matter which
network profile is currently in use.
The global configurations include viewing the active profile, exemptions, specified certification validation levels, and user and computer authorization lists.

NEW QUESTION 102
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 103
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 104
Your network contains an Active Directory domain named contoso.com.
The domain contains four global groups named Group]..., 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:

Policy name	Security setting
Allow log on locally	Contoso\Group1, Administrators
Deny log on locally	Contoso\Group3
Access this computer from the network	Contoso\Group2, Administrators, Backup Operators
Deny access to this computer from the network	Contoso\Group4

You need to ensure that User1 can access the shares on Computer1. What should you do?

A. Modify the membership of Group1.
B. In GPO1, modify the Access this computer from the network user right
C. Modify the Deny access to this computer from the network user right.
D. Modify the Deny log on locally user right

Answer: B

Explanation:

You need to ensure that User1 can access the shares on Computer1, from network.
If not from network, where would you access a shared folder from? from Mars? from Space? from toilet?
Moreover, this question has explicitly state User1 is a member of Group3, and hence it is not possible for User1 to logon Computer1 locally to touch those shared folders on NTFS file system.
Only these two policies to be considered “Access this computer from network”, “Deny access to this computer from network”.1
There’s no option to modify the group member ship of “Group2”, “Administrators”, or “Backup Operators”, so we have to add a 4th entry “User1” to this policy setting “Access this computer from network”.

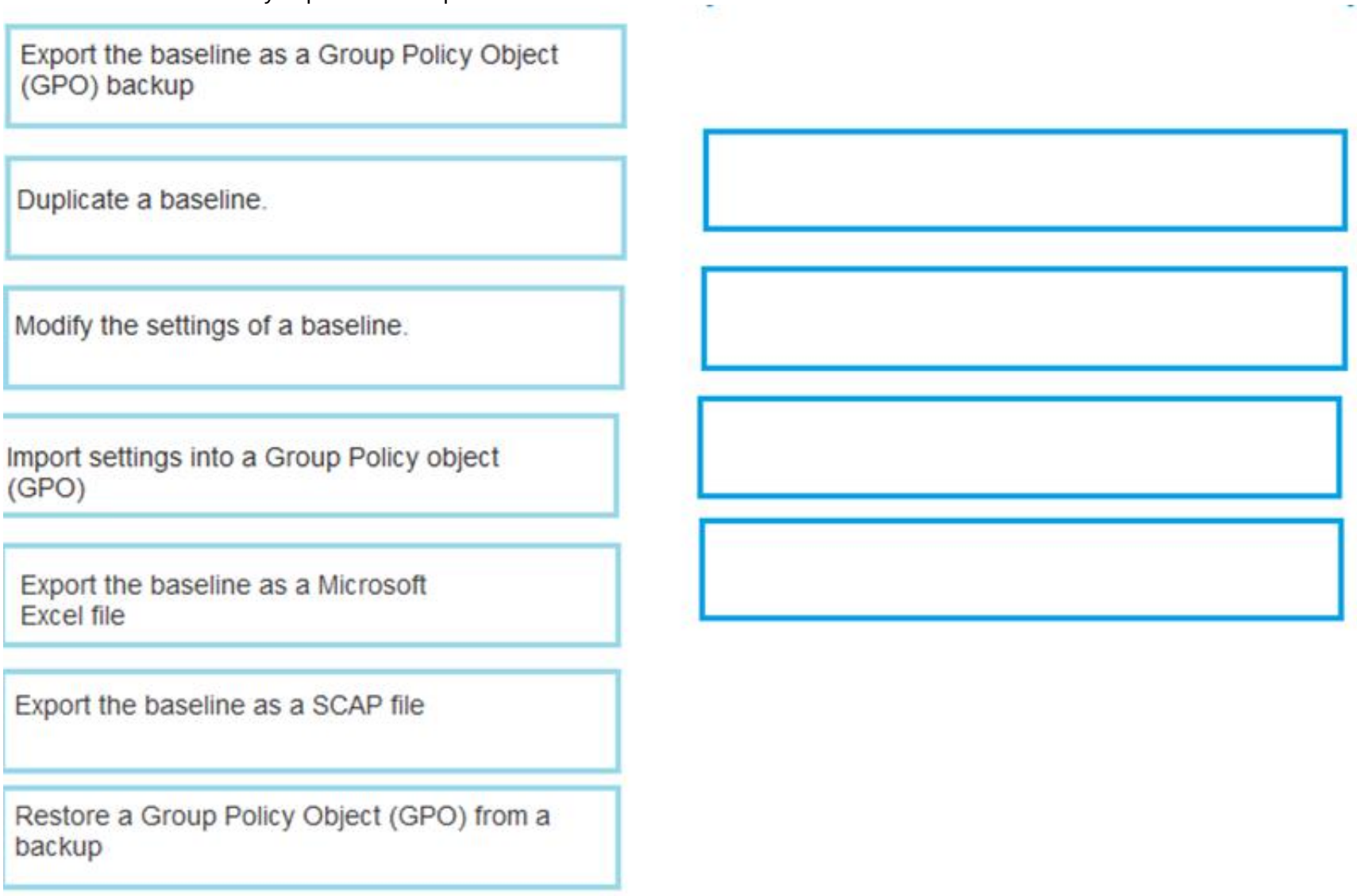
NEW QUESTION 106
Your network contains an Active Directory domain named contoso.com.
The domain contains a member server named Servers that runs Windows Server 2016. You need to configure Servers as a Just Enough Administration (JEA) endpoint.
Which two actions should you perform? Each correct answer presents part of the solution.

A. Create and export a Windows PowerShell session.
B. Deploy Microsoft Identity Manager (MIM) 2016
C. Create a maintenance Role Capability file
D. Generate a random Globally Unique Identifier (GUID)
E. Create and register a session configuration file.

Answer: CE

Explanation:
https://docs.microsoft.com/en-us/powershell/jea/role-capabilities https://docs.microsoft.com/en-us/powershell/jea/register-jea

NEW QUESTION 111
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:

Export the baseline as a Group Policy Object (GPO) backup

Duplicate a baseline.

Modify the settings of a baseline.

Import settings into a Group Policy object (GPO)

Export the baseline as a Microsoft Excel file

Export the baseline as a SCAP file

Restore a Group Policy Object (GPO) from a backup

Duplicate a baseline.

Modify the settings of a baseline.

Export the baseline as a Group Policy Object (GPO) backup

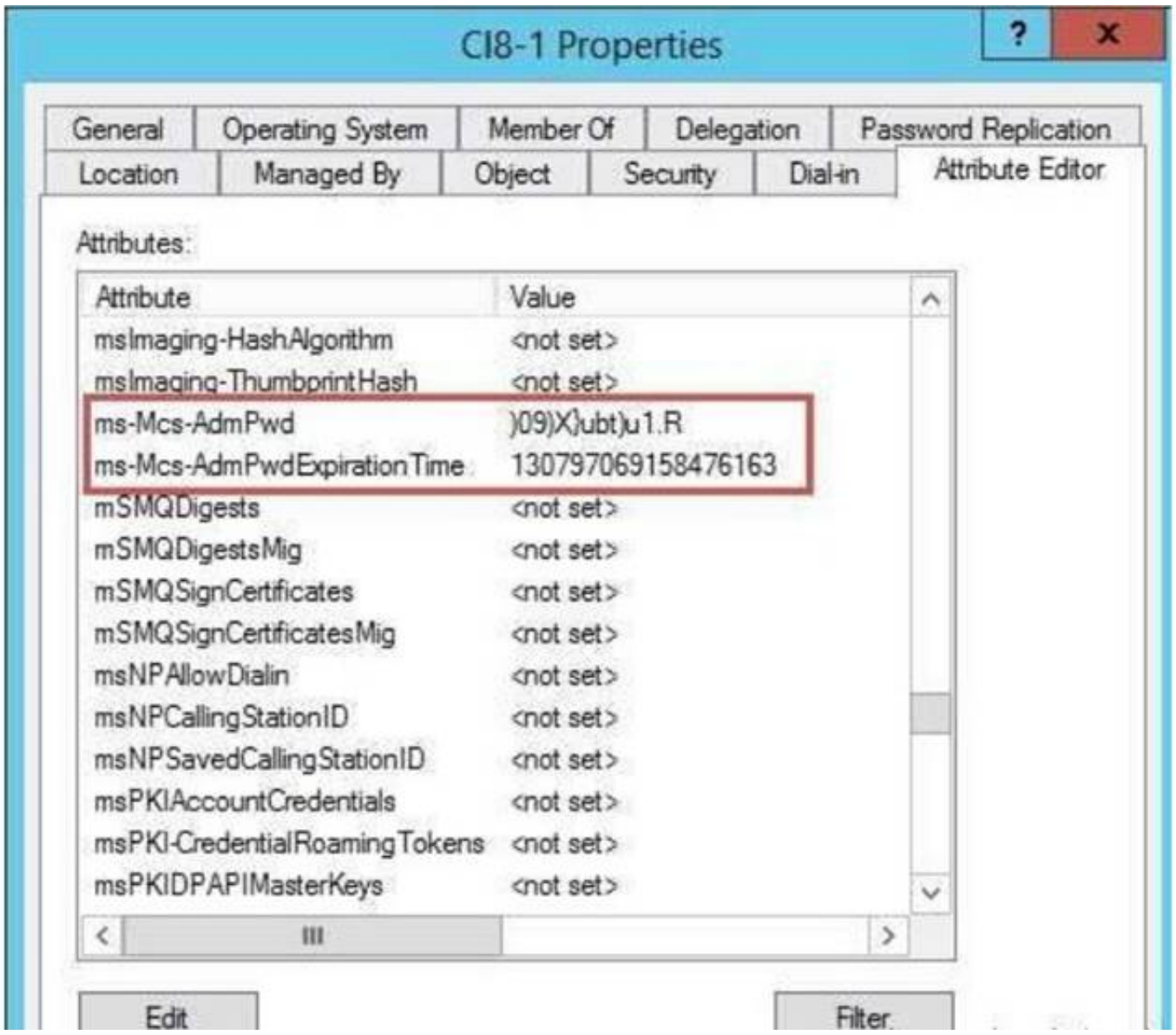
Import settings into a Group Policy object (GPO)

NEW QUESTION 112
Your network contains an Active Directory domain named contoso.com.
The domain contains a server named Server1 that runs Windows Server 2016.
The local administrator credentials of Server1 are managed by using the Local Administrator Password Solution (LAPS).
You need to retrieve the password of the Administrator account on Server1. What should you do?

A. From Windows PowerShell on Server1, run the Get-ADFineGrainedPasswordPolicy cmdlet and specify the -Credential parameter.
B. From Windows PowerShell on Server1, run the Get-ADUser cmdlet and specify the -Credential parameter.
C. From Active Directory Users and Computers, open the properties at Server1 and view the value at the msMcs-AdmPwd attribute
D. From Active Directory Users and Computers, open the properties of Administrator and view the value of the userPassword attribute

Answer: C

Explanation:
The “ms-Mcs-AdmPwd” attribute of a computer account in Active Directory Users and Computers stores the local Administrator password of a computer, which is configured by LAPS.



NEW QUESTION 114
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 need to view the password of the local administrator of a server named Server5.
Which tool should you use?

A. Active Directory Users and Computers
B. Computer Management
C. Accounts from the Settings app
D. Server Manager

Answer: A

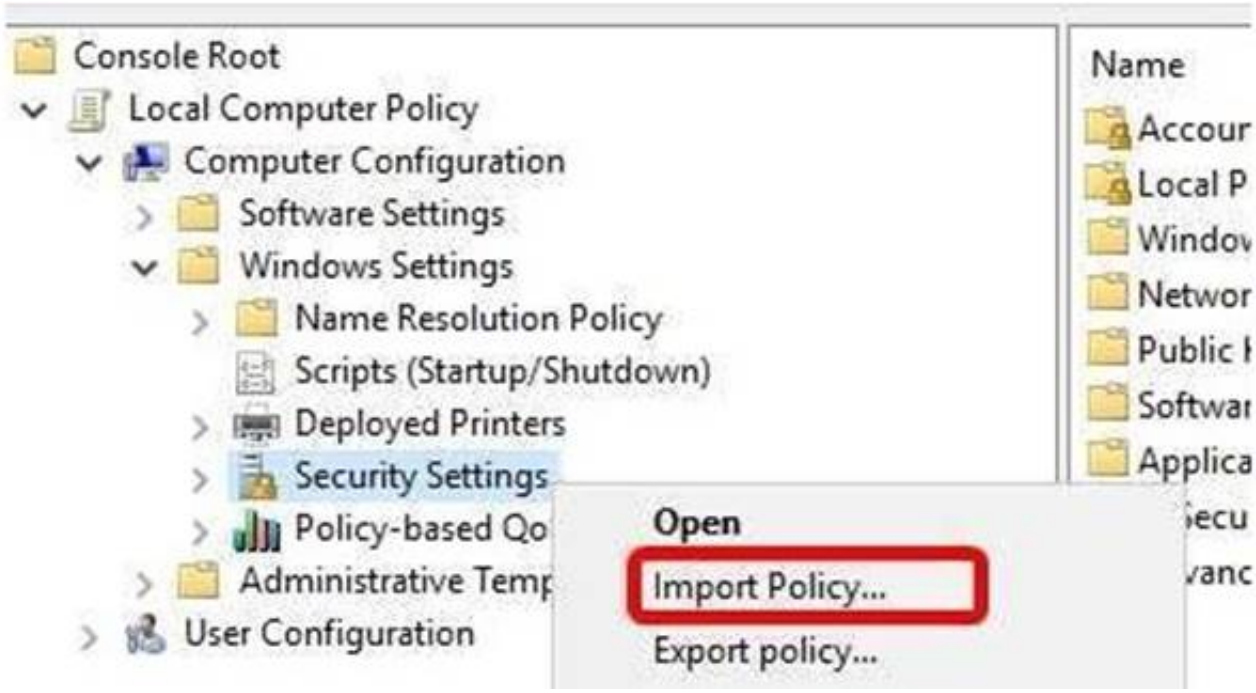
Explanation:
Use “Active Directory Users and Computers” to view the attribute value of “ms-MCS-adminpwd” of the Server5 computer account
https://blogs.technet.microsoft.com/askpfeplat/2015/12/28/local-administrator-password-solutionlapsimplementation- hints-and-security-nerd-commentaryincludingmini-threat-model/

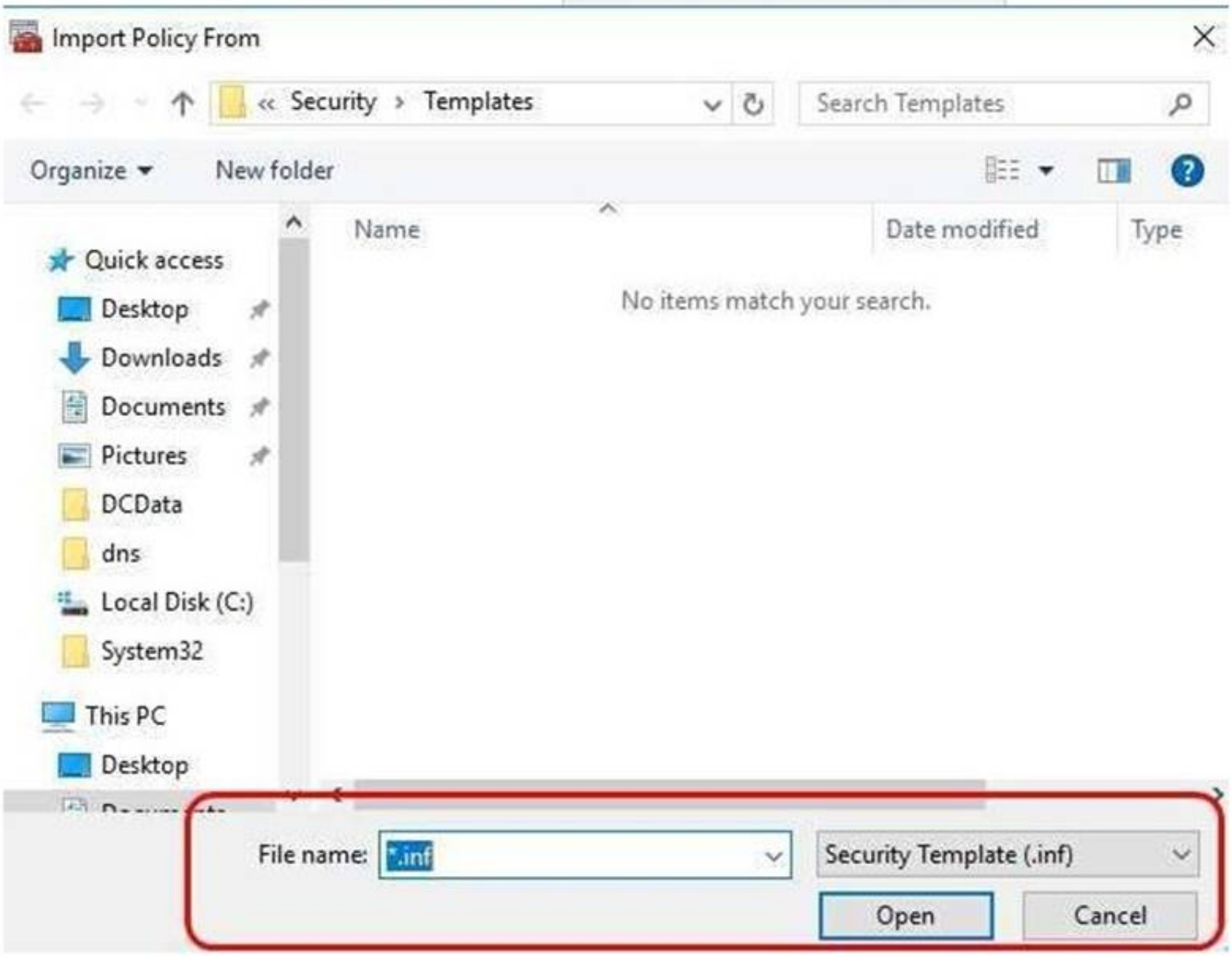
NEW QUESTION 116
Your network contains an internal network and a perimeter network. The internal network contains an Active Directory forest named contoso.com.
You deploy five servers to the perimeter network.
All of the servers run Windows Server 2016 and are the members of a workgroup.
You need to 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



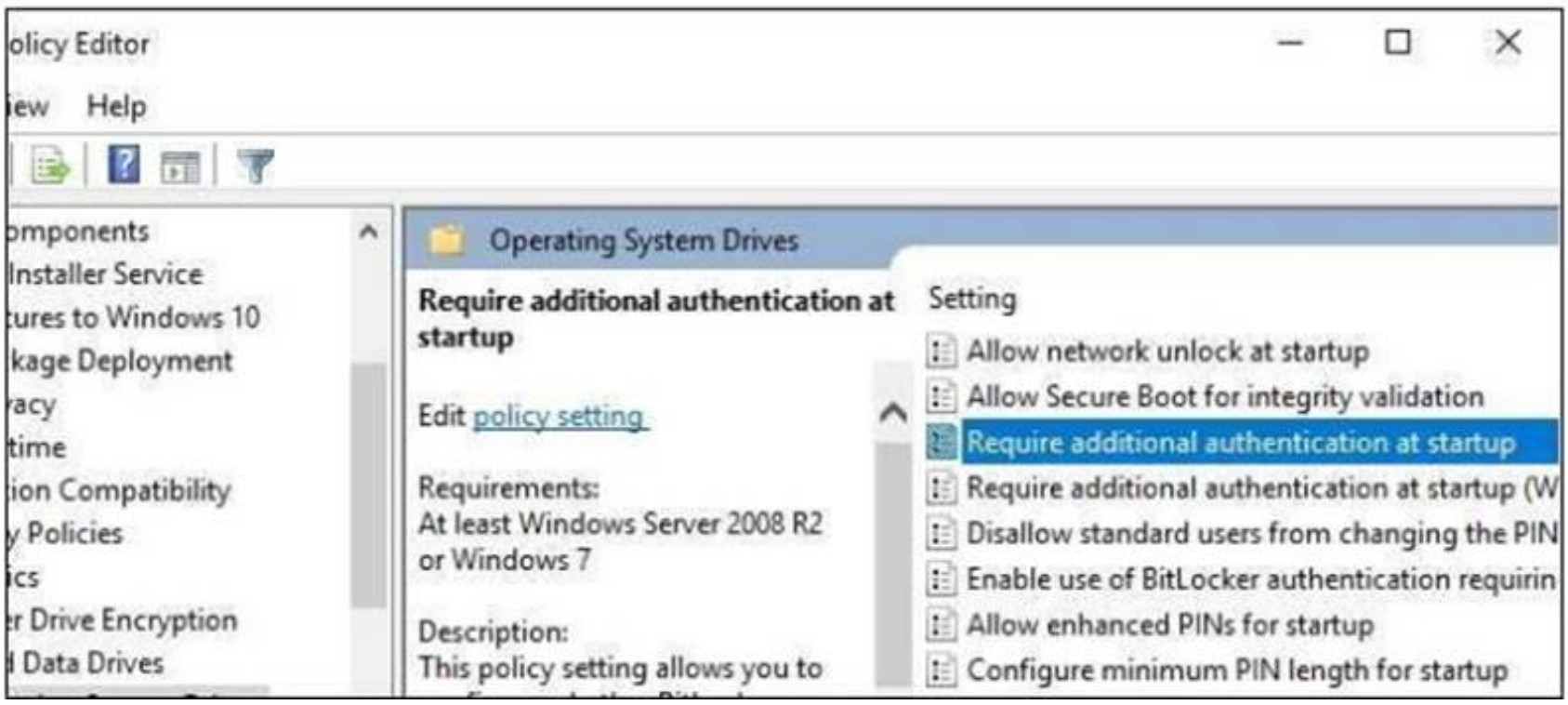


NEW QUESTION 121
You have a Hyper-V host named Server1 that runs Windows Server 2016. Server1 has a generation 2 virtual machine named VM1 that runs Windows 10.
You need to ensure that you can turn on BitLocker Drive Encryption (BitLocker) for drive C: on VM1. What should you do?

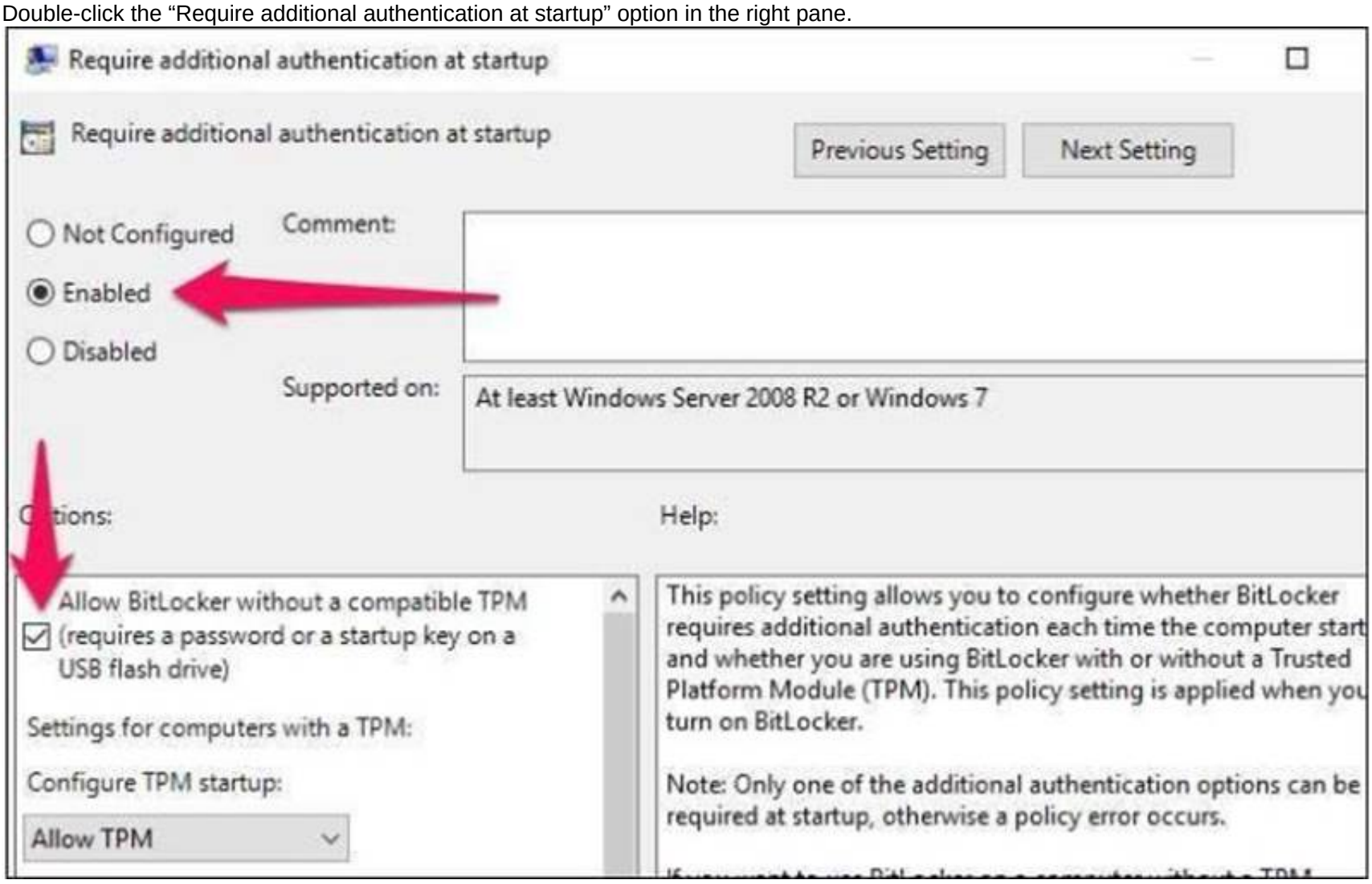
A. From Server1, install the BitLocker feature.
B. From Server1, enable nested virtualization for VM1.
C. From VM1, configure the Require additional authentication at startup Group Policy setting.
D. From VM1, configure the Enforce drive encryption type on fixed data drives Group Policy settin

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.

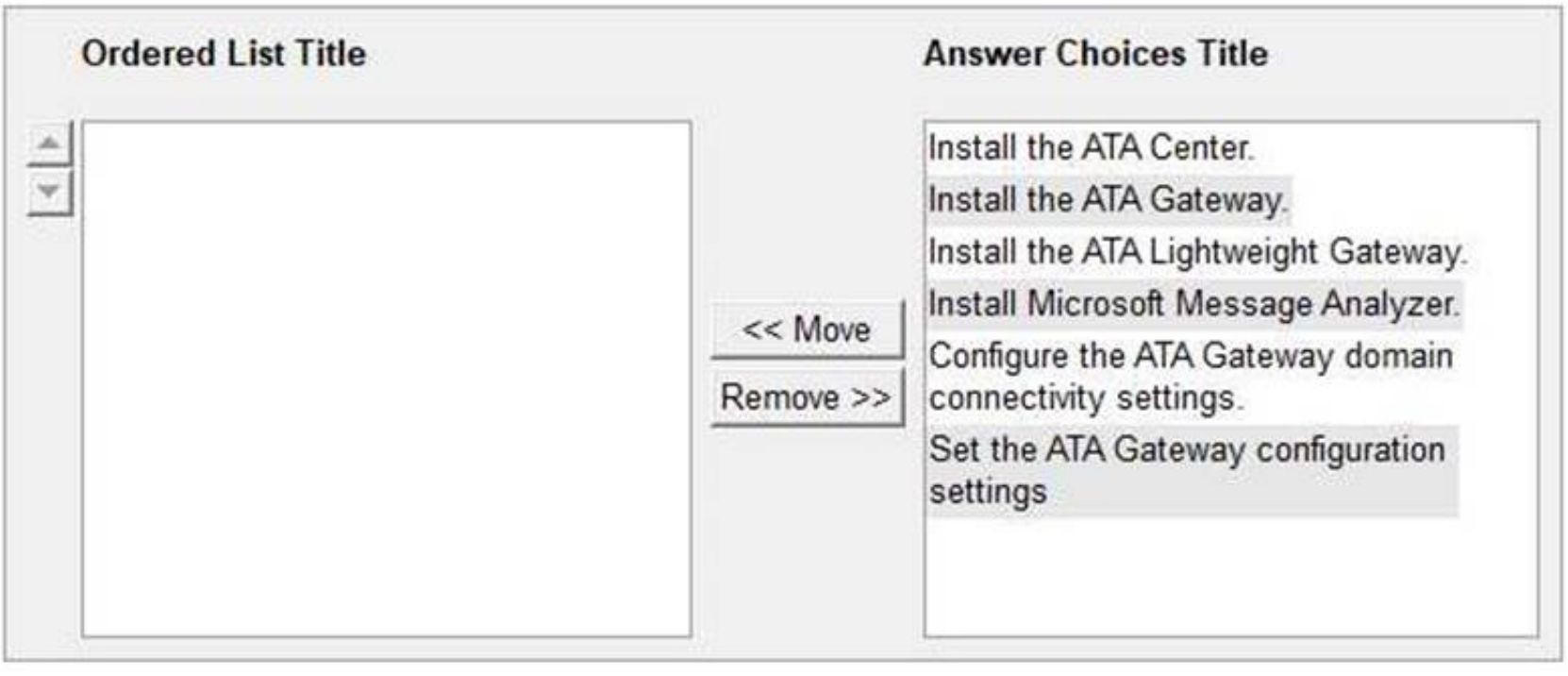


Double-click the “Require additional authentication at startup” option in the right pane.



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.

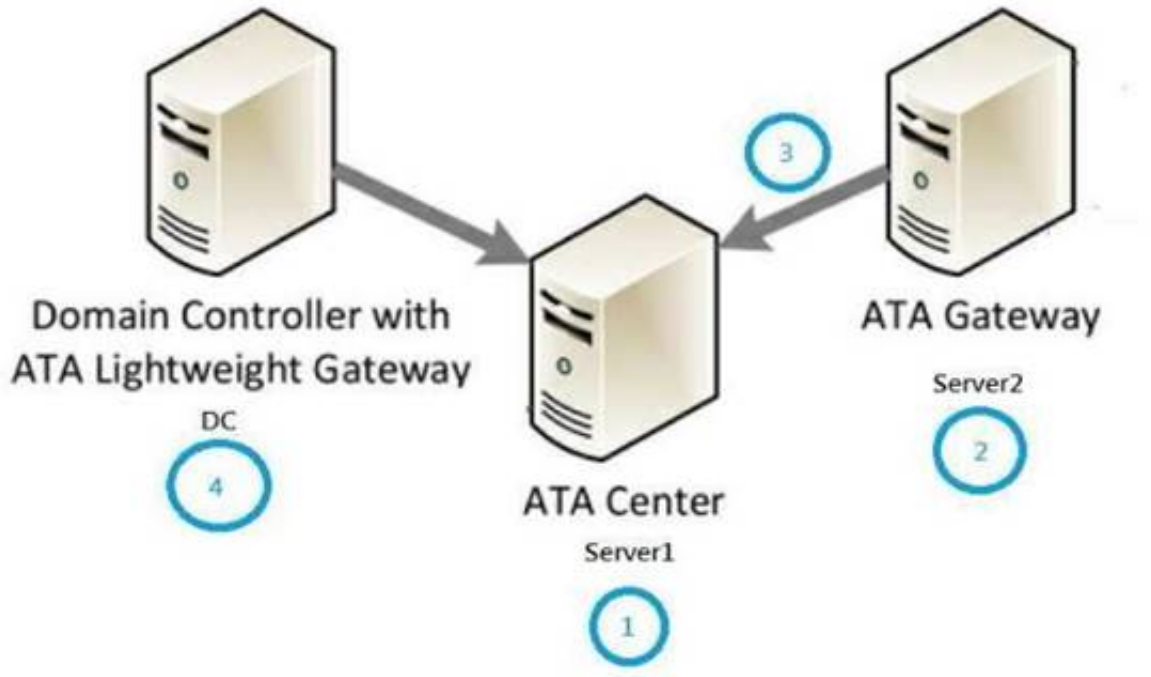
NEW QUESTION 124
DRAG DROP
Your network contains an Active Directory domain named contoso.com.
The domain contains two servers named Server1 and Server2 that run Windows Server 2016. You need to install Microsoft Advanced Threat Analytics (ATA) on Server1 and Server2. Which four actions should you perform 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 125
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1.
On Server1, administrators plan to use several scripts that have the .ps1 extension.
You need to ensure that when code is generated from the scripts, an event containing the details of
the code is logged in the Operational log.
Which Group Policy setting or settings should you configure?

A. Enable Protected Event Logging
B. Audit Process Creation and Audit Process Termination
C. Turn on PovverShell Script Block Logging
D. Turn on PowerShell Transcription

Answer: C

Explanation:
https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit_script
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 log,
Microsoft-Windows-PowerShell/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 GPO Administrative Templates -> Windows Components -> Windows PowerShell).
Answer D is incorrect, since Transcription (Start-Transcript -path <FilePath>) uses a custom output location

instead of Event Viewer \\ Operational Log

NEW QUESTION 129
You have a server named Server1 that runs Windows Server 2016. You configure Just Enough Administration (JEA) on Server1.
You need to view a list of commands that will be available to a user named User1 when User1 establishes a JEA session to Server1.
Which cmdlet should you use?

A. Trace-Command
B. Get-PSSessionCapability
C. Get-PSSessionConfiguration
D. Show-Command

Answer: B

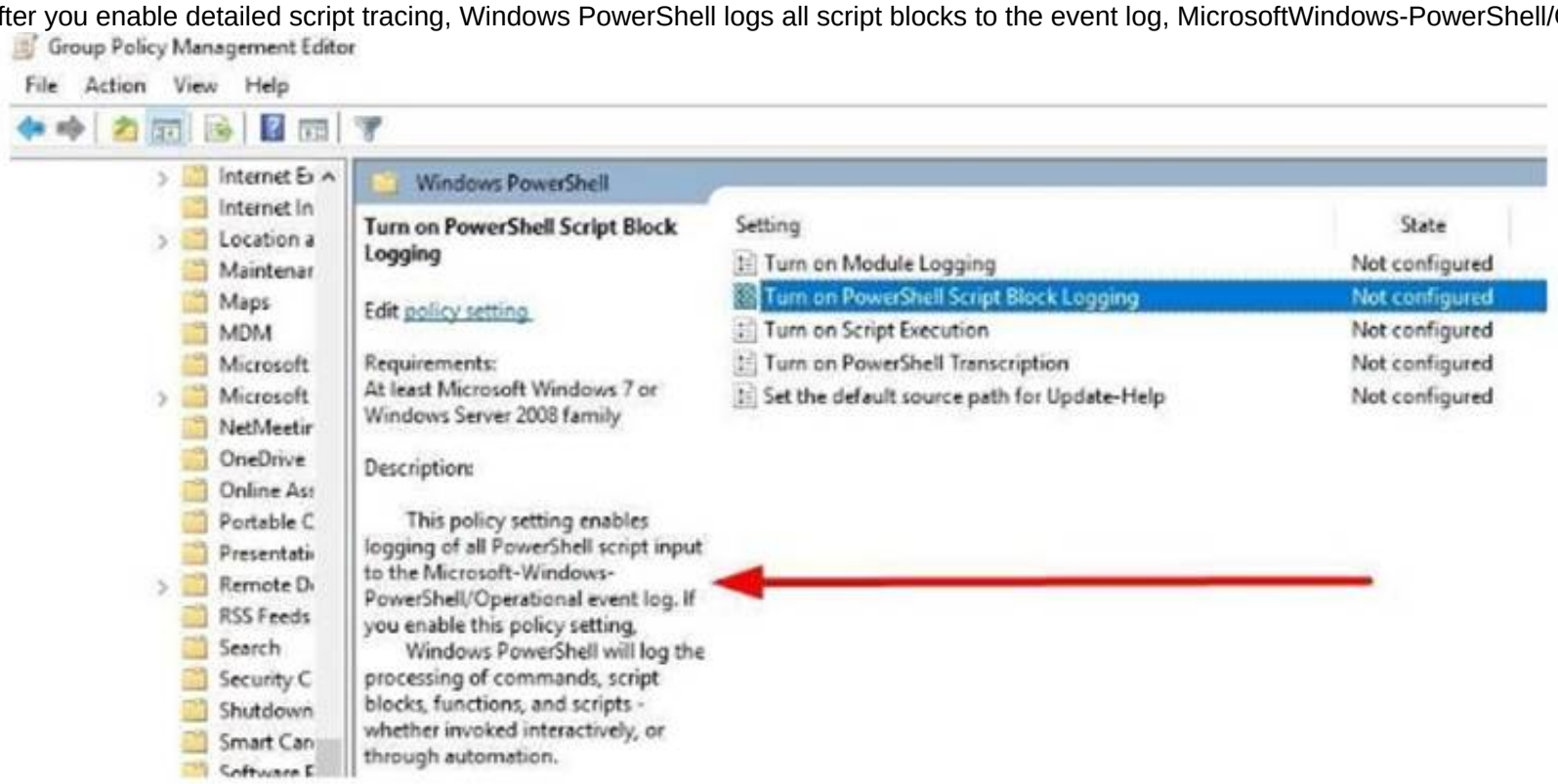
Explanation:
https://docs.microsoft.com/en-us/powershell/module/Microsoft.PowerShell.Core/getpssessioncapability? view=powershell-5.0.
The Get-PSSessionCapability cmdlet gets the capabilities of a specific user on a constrained session configuration.
Use this cmdlet to audit customized session configurations for users.
Starting in Windows PowerShell 5.0, you can use the RoleDefinitions property in a session configuration (.pssc) file.
Using this property lets you grant users different capabilities on a single constrained endpoint based on groupmembership.
The Get-PSSessionCapability cmdlet reduces complexity when auditing these endpoints by letting you
determine the exact capabilities granted to a user.
This command is used by I.T. Administrator (The “You” mention in the question) to verify configuration for a
User.

NEW QUESTION 133
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 136
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

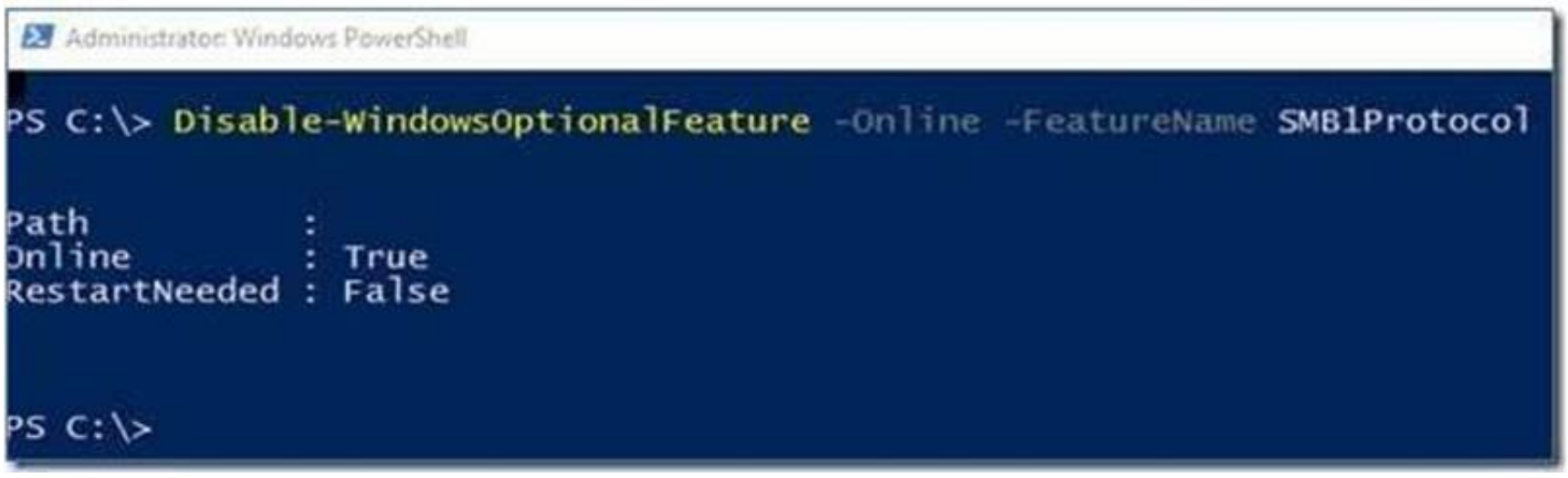
Explanation:
No, as Server4 is a Windows Server 2012R2 which does not meet the requirements of Remote Credential Guard.
https://docs.microsoft.com/en-us/windows/access-protection/remote-credential-guard Remote Credential Guard requirements
To use Windows Defender Remote Credential Guard, the Remote Desktop 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 140
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?

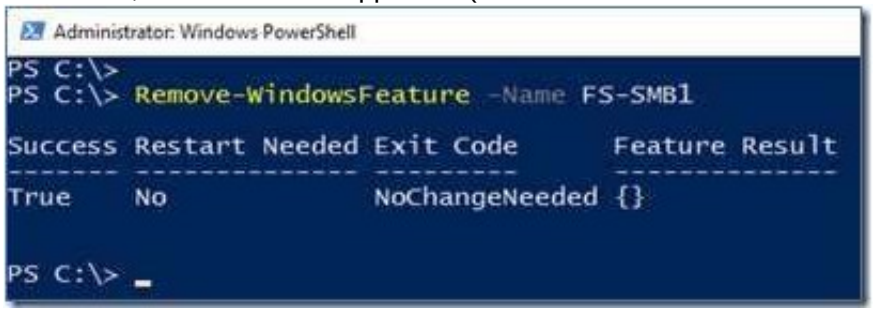
A. Yes
B. No

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



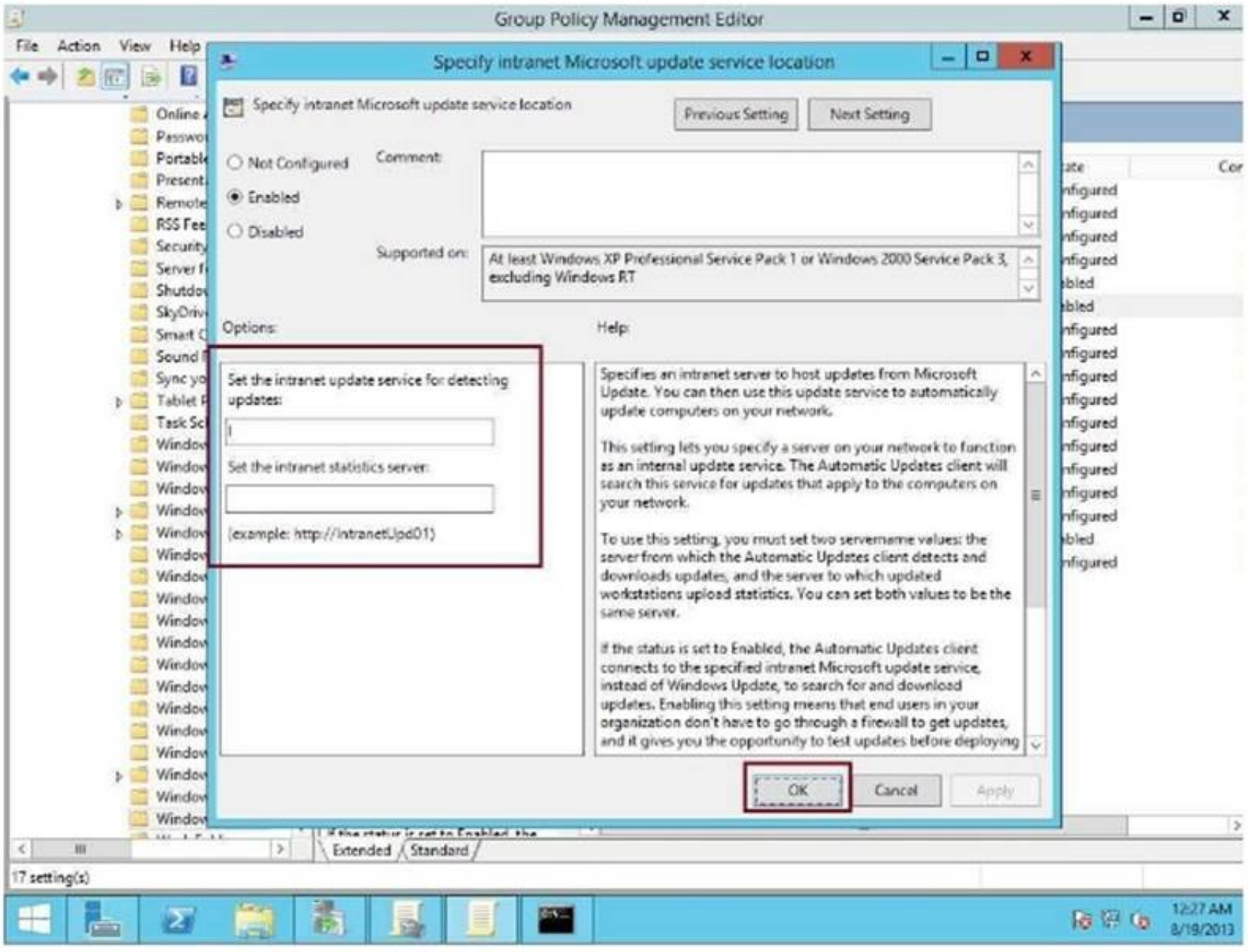
Even if SMB1 is removed, SMB2 and SMB3 could still run NTLM authentication! Therefore, answer is a"NO".

NEW QUESTION 141
Your network contains an Active Directory domain named contoso.com.The domain contains 1,000 client computers that run either Windows 8.1 or Windows 10.
You have a Windows Server Update Services (WSUS) deployment All client computers receive updates from WSUS.
You deploy a new WSUS server named WSUS2.
You need to configure all of the client computers that run Windows 10 to send WSUS reporting data to WSUS2.
What should you configure?

A. an approval rule
B. a computer group
C. a Group Policy object (GPO)
D. a synchronization rule

Answer: C

Explanation:
https://technet.microsoft.com/en-us/library/cc708574(v=ws.10).aspx
Under "Set the intranet update service for detecting updates", type http://wsus:8530 Under "Set the intranet statistics server", type http://wsus2:8531



NEW QUESTION 143
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2016.
You need to prevent direct .NET scripts invoked by interactive Windows PowerShell sessions from running on the servers.
What should you do for each server?

A. Create an AppLocker rule.
B. Create a Code Integrity rule.
C. Disable PowerShell Remoting.
D. Modify the local Kerberos policy setting

Answer: C

NEW QUESTION 148
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that has Microsoft Security Compliance Manager (SCM) 4.0 installed. The domain contains domain controllers that run Windows Server 2016.
A Group Policy object (GPO) named GPO1 is applied to all of the domain controllers.
GPO1 has a Globally Unique Identifier (GUID) of 7ABCDEFG-1234-5678-90AB-005056123456. You need to create a new baseline that contains the settings from GPO1. What should you do first?

A. Copy the \\\\contoso.com\\sysvol\\contoso.com\\Policies\\{7ABCDEFG-1234-5678-90AB- 005056123456} folder to Server1.
B. From Group Policy Management, create a backup of GPO1.
C. From Windows PowerShell, run the Copy-GPO cmdlet
D. Modify the permissions of the \\\\contoso.com\\sysvol\\contoso.com\\Policies\\{7ABCDEFG- 1234-5678-90AB-005056123456}

Answer: B

Explanation:
https://technet.microsoft.com/en-us/library/hh489604.aspx Import Your GPOs
You can import current settings from your GPOs and compare these to the Microsoft recommended best practices.
Start with a GPO backup that you would commonly create in the Group Policy Management Console (GPMC).
Take note of the folder to which the backup is saved. In SCM, select GPO Backup, browse to the GPO folder's Globally Unique Identifier (GUID) and select a name for the GPO when it's imported.
SCM will preserve any ADM files and GP Preference files (those with non-security settings that SCM doesn't parse) you're storing with your GPO backups. It saves them in a subfolder within the user's public folder. When you export the baseline as a GPO again, it also restores all the associated files.

NEW QUESTION 152
You have a server named Server1 that runs Windows Server 2016.
You need to identify the default action for the inbound traffic when Server1 connects to the domain. Which cmdlet should you use?

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

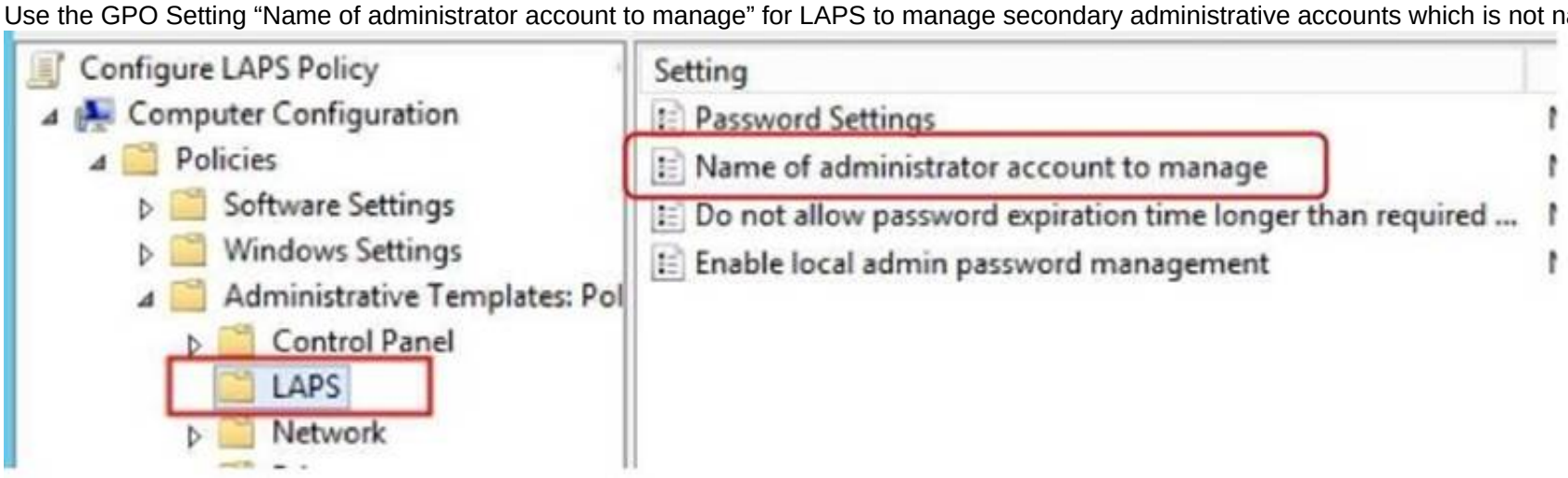
Answer: C

NEW QUESTION 154
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 158
Your network contains an Active Directory domain named contoso.com. The domain contains 100 servers.
You deploy the Local Administrator Password Solution (LAPS) to the network.
You discover that the members of a group named FinanceAdministrators can view the password of the local Administrator accounts on the servers in an organizational unit (OU) named FinanceServers. You need to prevent the FinanceAdministrators members from viewing the local administrators’ passwords on the servers in FinanceServers.
Which permission should you remove from FinanceAdministrators?

A. List contents
B. All extended rights
C. Read all properties
D. Read permissions

Answer: B

Explanation:
https://blogs.technet.microsoft.com/askpfeplat/2015/12/28/local-administrator-password-solutionQuestions
& Answers PDF P-123
lapsimplementation-hints-and-security-nerd-commentaryincludingmini-threat-model/ Access to the password is granted via the “Control Access” right on the attribute.
Control Access is an “Extended Right” in Active Directory, which means if a user has been granted the “All
Extended Rights” permission they’ll be able to see passwords even if you didn’t give them permission.

NEW QUESTION 161
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 166
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 ensure that you can view Windows PowerShell code that was generated dynamically and executed on the computers in OU1.
What would you configure in GP1?

A. Object Access\\Audit Application Generated from the advanced audit policy
B. Turn on PowerShell Script Block Logging from the PowerShell settings
C. Turn on Module Logging from the PowerShell settings
D. Object Access\\Audit Other Object Access Events from the advanced audit policy

Answer: B

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 log,
Microsoft-Windows-PowerShell/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 168
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2016.
The Microsoft Advanced Threat Analytics (ATA) Center service is installed on Server1. The domain contains the users shown in the following table.

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

You are installing ATA Gateway on Server2.
You need to specify a Gateway Registration account. Which account should you use?

A. User1
B. User2
C. User3
D. User4
E. User5
F. User6
G. User7
H. User8

Answer: F

Explanation:
https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-role-groups

Activity	Microsoft Advanced Threat Analytics Administrators	Microsoft Advanced Threat Analytics Users	Microsoft Advanced Threat Analytics Viewers
Login	Available	Available	Available
Provide Input for Suspicious Activities	Available	Available	Not available
Change status of Suspicious Activities	Available	Available	Not available
Share/Export suspicious activity via email/get link	Available	Available	Not available
Change status of Monitoring Alerts	Available	Available	Not available
Update ATA Configuration	Available	Not available	Not available

The user who installed ATA will be able to access the management portal (ATA Center) as members of the "Microsoft Advanced Threat Analytics Administrators" local group on the ATA Center server.

NEW QUESTION 170
You implement Log Analytics in Microsoft Operations Management Suite (OMS) on all servers that run Windows Server 2016.
You need to generate a daily report that identifies which servers restarted during the last 24 hours. Which query should you use?

A. EventLog=Application EventId:6009 Type:Event TimeGenerated>NOW+24HOURS
B. EventLog=Application EventId:6009 Type:Event TimeGenerated>NOW-24HOURS
C. EventLog=System EventId:6009 Type:Event TimeGenerated>NOW-24HOURS
D. EventLog=System EventId:6009 Type:Event TimeGenerated>NOW+24HOURS

Answer: C

Explanation:
https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-log-searches Computer restart events are stored in "System" eventlog instead of Application even log. "NOW-24HOURS" clause matches all events generated in the last 24 hours.

Boolean operators

With datetime and numeric fields, you can search for values using *greater than*, *lesser than*, and *lesser than or equal*. You can use simple operators such as >, < , >=, <= , != in the query search bar.

You can query a specific event log for a specific period of time. For example, the last 24 hours is expressed with the following mnemonic expression.

Copy

```
EventLog=System TimeGenerated>NOW-24HOURS
```

NEW QUESTION 172
You have a file server named Server1 that runs Windows Server 2016. A new policy states that ZIP files must not be stored on Server1.
An administrator creates a file screen filter as shown in the following output

Active	: False
Description	:
IncludeGroup	: {Compressed Files}
MatchesTemplate	: False
Notification	: {MSFT_FSRMAction, MSFT_FSRMAction}
Path	: C:\
Template	
PSComputerName	

You need to prevent users from storing ZIP files on Server1, what should you do?

A. Enable Quota Management on all the drives.
B. Add a template to the filter.
C. Change the filter to active.
D. Configure File System (Global Object Access Auditing).

Answer: C

Explanation:
“Active : False”, then it is a Passive Filescreen filther which will not block unwanted file types.

NEW QUESTION 176
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 181
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 182
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. You need to prevent NTLM authentication on Server1.
Solution: From a Group Policy, you configure the Security Options. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 185
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. You need to prevent NTLM authentication on Server1.
Solution: From Windows PowerShell, you run the New-ADAuthenticationPolicy cmdlet. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
ADDS Authentication Policy does not provide ability to prevent the use of NTLM authentication.

NEW QUESTION 186
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 with Advanced Security, you create an inbound rule. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 189
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 SMB encryption on all the computers in domain. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
SMB Encryption could be enabled on a per-computer wide basis, after you have enabled SMB encryption on a server-level basis, you could not disable encryption for any specific shared folder.
To enable Global level encryption on the server: Set-SmbServerConfiguration -EncryptData 1

NEW QUESTION 194
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 195
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 196
Your network has an internal network and a perimeter network. Only the servers on the perimeter network can access the Internet. You create a Microsoft Operations Management Suite (OMS) instance in Microsoft Azure.
You deploy Microsoft Monitoring Agent to all the servers on both the networks. You discover that only the servers on the perimeter network report to OMS. You

need to ensure that all the servers report to OMS.
What should you do?

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

Answer: A

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

NEW QUESTION 200
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You manage a file server that runs Windows Server 2016. The file server contains the volumes configured as shown in the following table.

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

You need to encrypt DevFiles by using BitLocker Drive Encryption (ButLocker). Solution: You run the Enable-BitLocker cmdlet.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

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

NEW QUESTION 202
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.
You need to prevent NTLM authentication on Server1.
Solution: From a Group Policy, you configure the Kerberos Policy. Does this meet the goal?

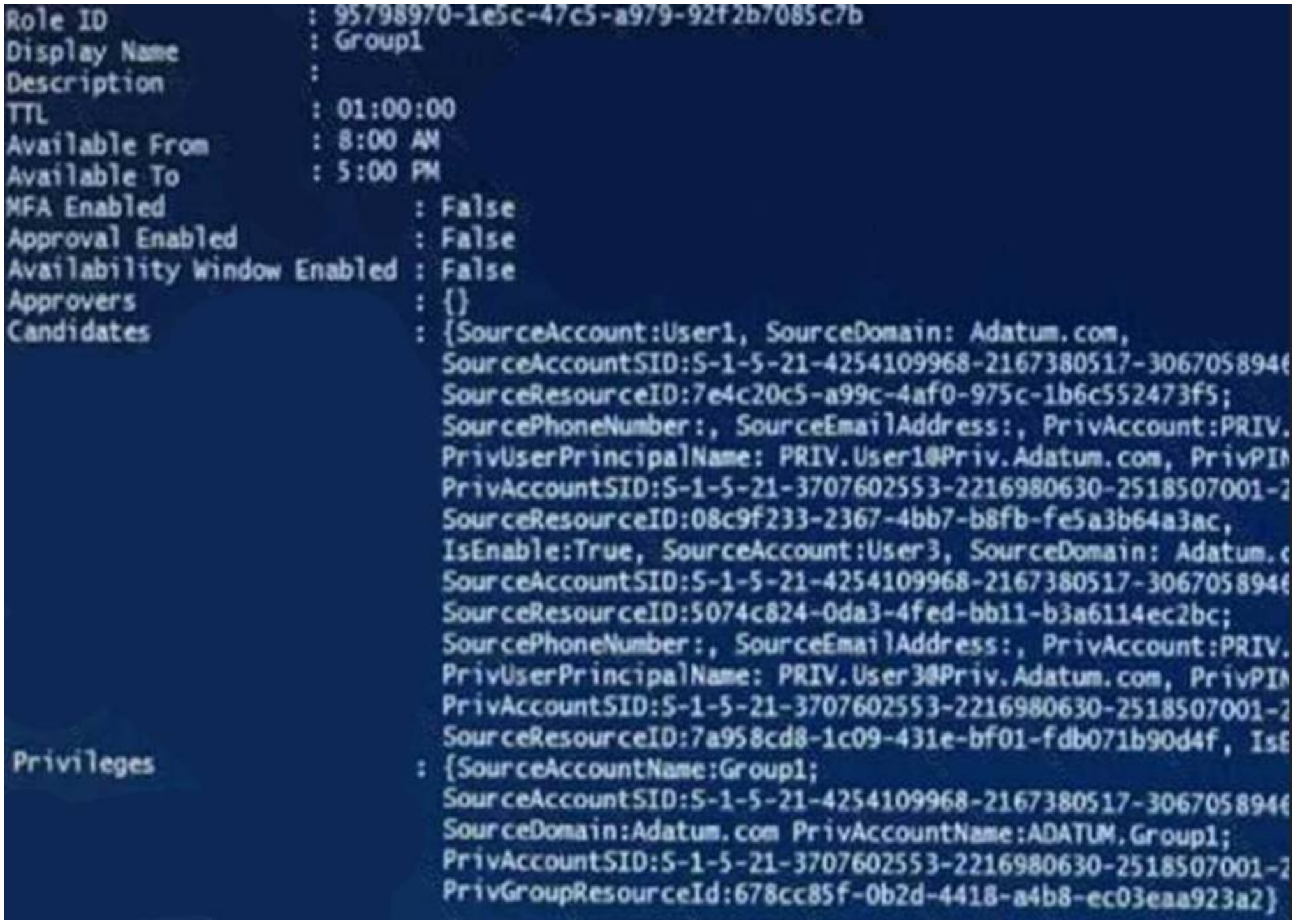
A. Yes
B. No

Answer: B

Explanation:

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

NEW QUESTION 206
HOTSPOT
Your network contains two Active Directory forests named adatum.com and priv.adatum.com. You deploy Microsoft Identity Manager (MIM) 2016 to the priv.adatum.com domain, and you implement Privileged Access Management (PAM).
You create a PAM role named Group1 as shown in the following exhibit.



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

Answer Area

If Priv.User1 requests the Group1 PAM role at 07:00, **[answer choice].**

- **the request will be denied**
- **Priv.User1 will be added to Group1 immediately**
- **Priv.User1 will be added to Group1 as soon as the request is approved**
- **Priv.User1 will be added to Group1 at 8:00**

If Priv.User2 requests the Group1 PAM role at 09:00, **[answer choice].**

- **the request will be denied**
- **Priv.User2 will be added to Group1 immediately**
- **Priv.User2 will be added to Group1 as soon as the request is approved**

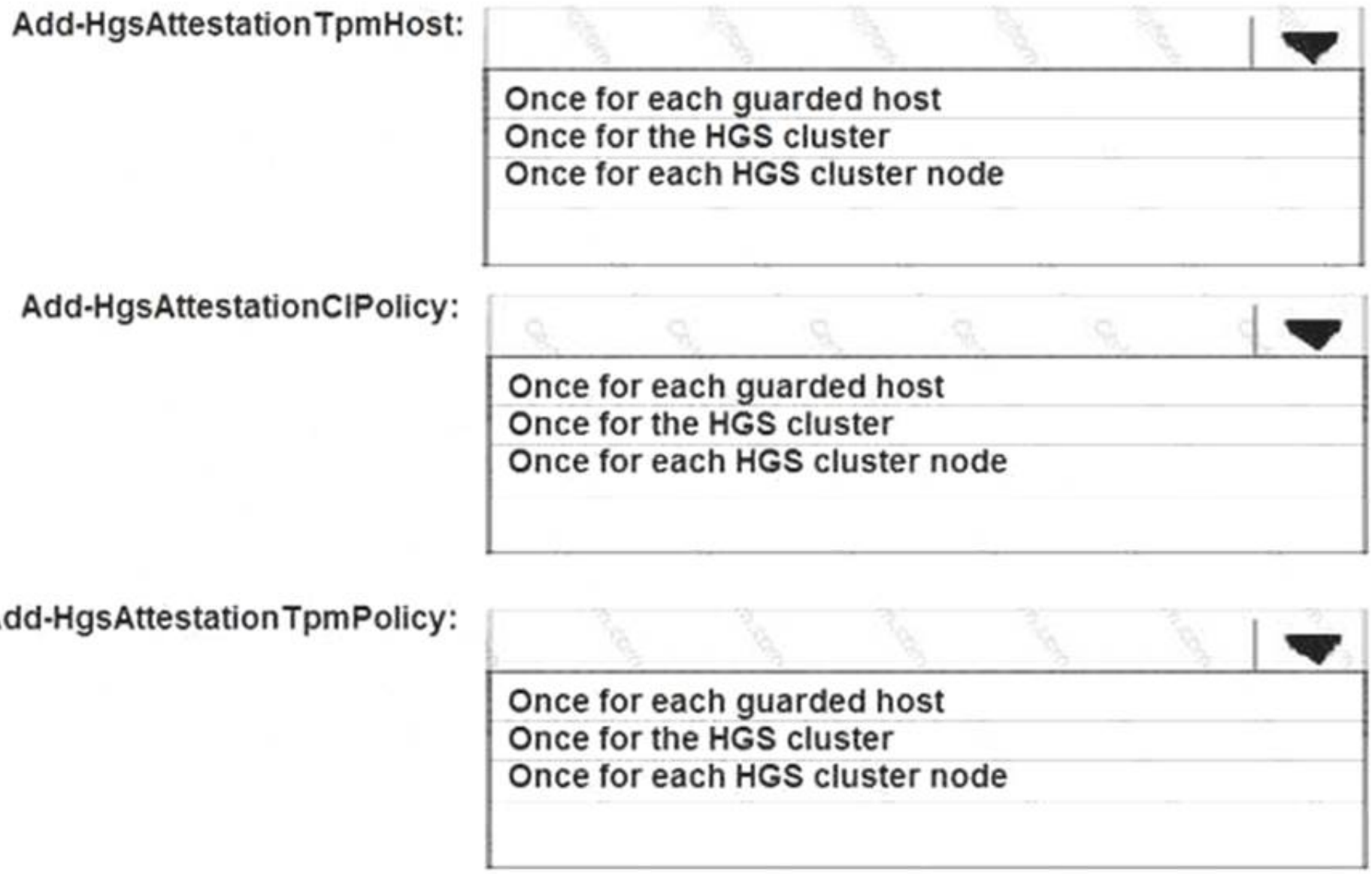
A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:https://tlktechidentitythoughts.wordpress.com/2016/09/07/mim-2016-setting-upprivileged- access-management-pam-in-an-existing-domain-using-the-built-in-pam-tool/

NEW QUESTION 208
HOTSPOT

You plan to implement a guarded fabric in TPM-trusted attestation mode. The fabric will contain a three-node Host Guardian Service (HGS) cluster and four guarded hosts.
All the hosts will have matching hardware and will run the same workload. You need to add the hosts to the HGS cluster.
What is the minimum number of times you must run each cmdlet to implement the HGS cluster? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:
https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shieldedvm/ guarded-fabric-tpm-trusted-attestation-capturing-hardware

NEW QUESTION 209
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 213
You have a file server named FS1 that runs Windows Server 2016. You plan to disable SMB 1.0 on the server.
You need to verify which computers access FS1 by using SMB 1.0. What should you run first?

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

Answer: D

NEW QUESTION 215
.....

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