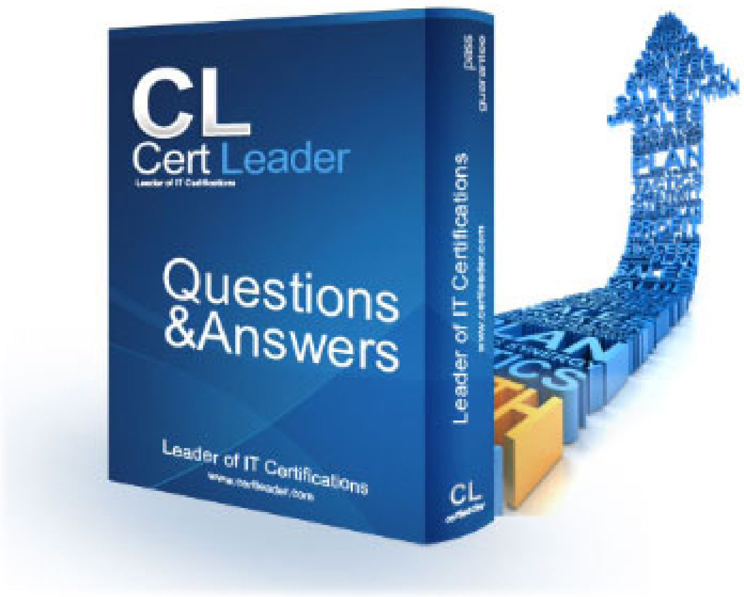
70-744 Dumps

Securing Windows Server 2016

https://www.certleader.com/70-744-dumps.html



NEW QUESTION 1
Note: This question It part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goats. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to It. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. Computer1 connects to a home network and a corporate network.
The corporate network uses the 17216.0.0/24 address space internally. 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 a software restriction policy.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Software Restriction Policy does not filter incoming network traffic, what you actually need is Windows Firewall Inbound Rule on the Private profile
References:
https://technet.microsoft.com/en-us/library/hh831534(v=ws.11).aspx

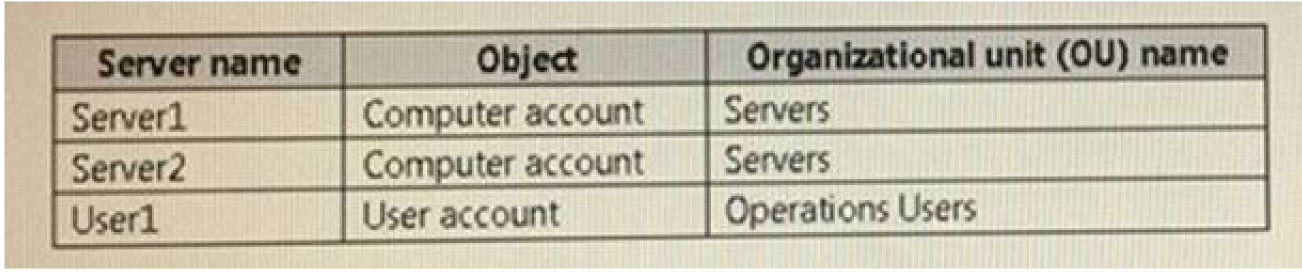
NEW QUESTION 2
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After 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 Windows Firewall in the Control Panel, you add an application and allow the application to communicate through the firewall on a Private network.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 3
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to It. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2016. All client computers run Windows 10.
The relevant objects in the domain are configured as shown in the following table.



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

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

A. Yes
B. No

Answer: B

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

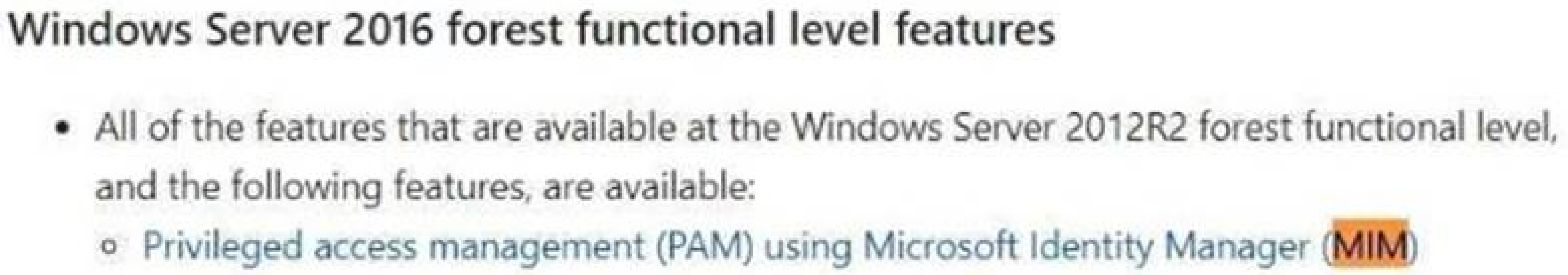
NEW QUESTION 4
Your network contains an Active Directory forest named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2016.
You create a new bastion forest named admin.contoso.com. The forest functional level of admin.contoso.com is Windows Server 2012 R2.
You need to implement a Privileged Access Management (PAM) solution.
Which two actions should you perform? Each correct answer presents part of the solution.

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

E. Raise the forest functional level of contoso.com.
F. Configure admin.contoso.com to trust contoso.co

Answer: DE

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



Windows Server 2016 forest functional level features

- All of the features that are available at the Windows Server 2012R2 forest functional level, and the following features, are available:
  - Privileged access management (PAM) using Microsoft Identity Manager (MIM)

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

NEW QUESTION 5
Your network contains an Active Directory domain named contoso.com. The domain contains five servers. All servers run Windows Server 2016.
A new secunty policy states that you must modify the infrastructure to meet the following requirements:
*Limit the nghts of administrators.
*Minimize the attack surface of the forest
*Support Multi-Factor authentication for administrators.
You need to recommend a solution that meets the new secunty policy requirements. What should you recommend deploying?

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

Answer: A

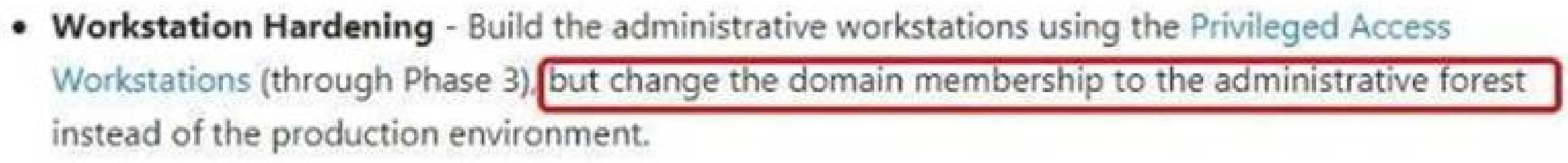
Explanation:
You have to “-Minimize the attack surface of the forest”, then you must create another forest for administrators.
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securingprivilegedaccess- reference-material#ESAE_BM
This section contains an approach for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

NEW QUESTION 6
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



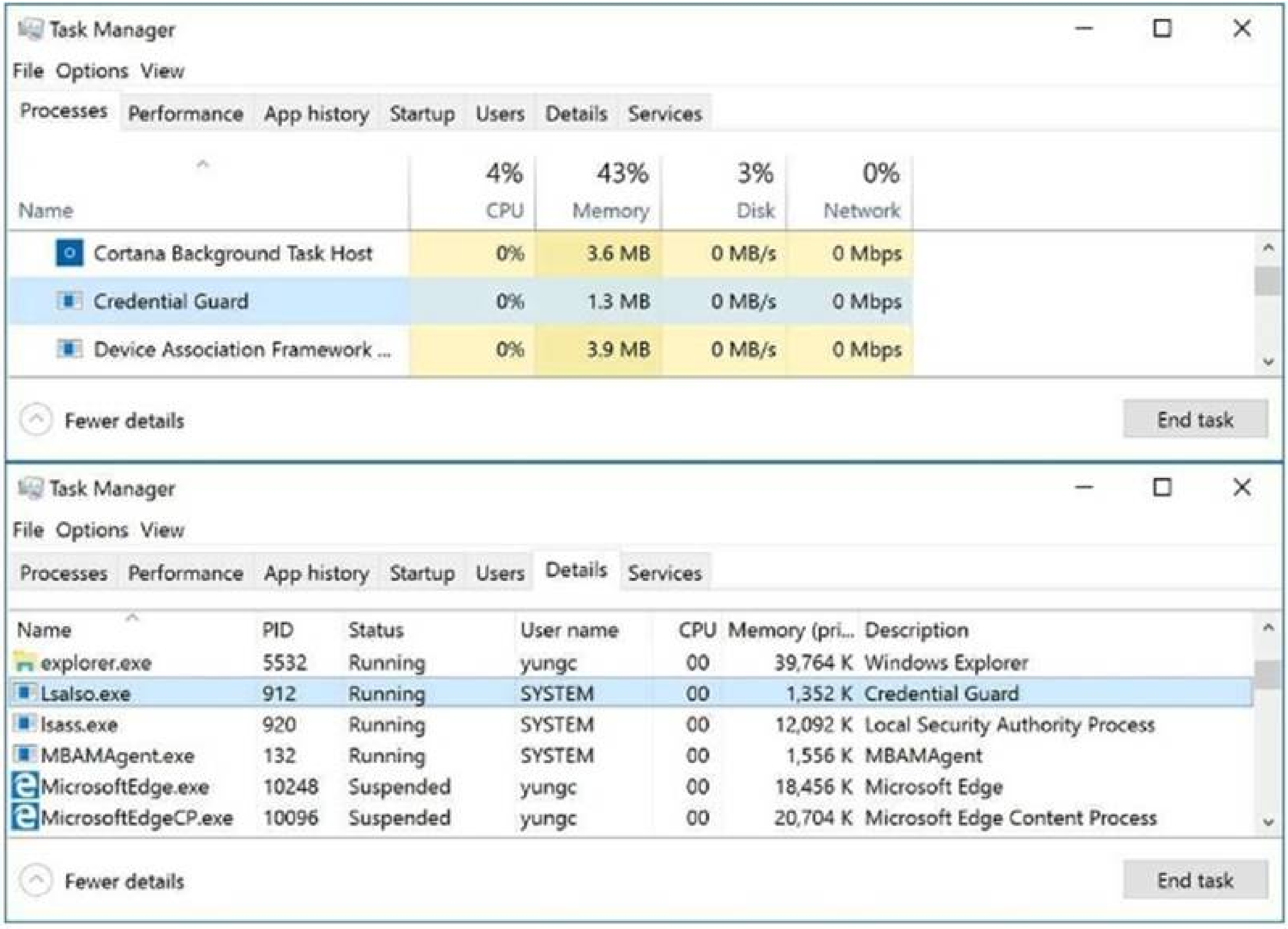
- **Workstation Hardening** - Build the administrative workstations using the Privileged Access Workstations (through Phase 3), but change the domain membership to the administrative forest instead of the production environment.

NEW QUESTION 7
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Serve1, that runs Windows Server 2016.
A technician is testing the deployment of Credential Guard on Server1. You need to verify whether Credential Guard is enabled on Server1. What should you do?

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

Answer: B

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


Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details
End task

Name	4% CPU	43% Memory	3% Disk	0% Network
Cortana Background Task Host	0%	3.6 MB	0 MB/s	0 Mbps
Credential Guard	0%	1.3 MB	0 MB/s	0 Mbps
Device Association Framework ...	0%	3.9 MB	0 MB/s	0 Mbps

Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details
End task

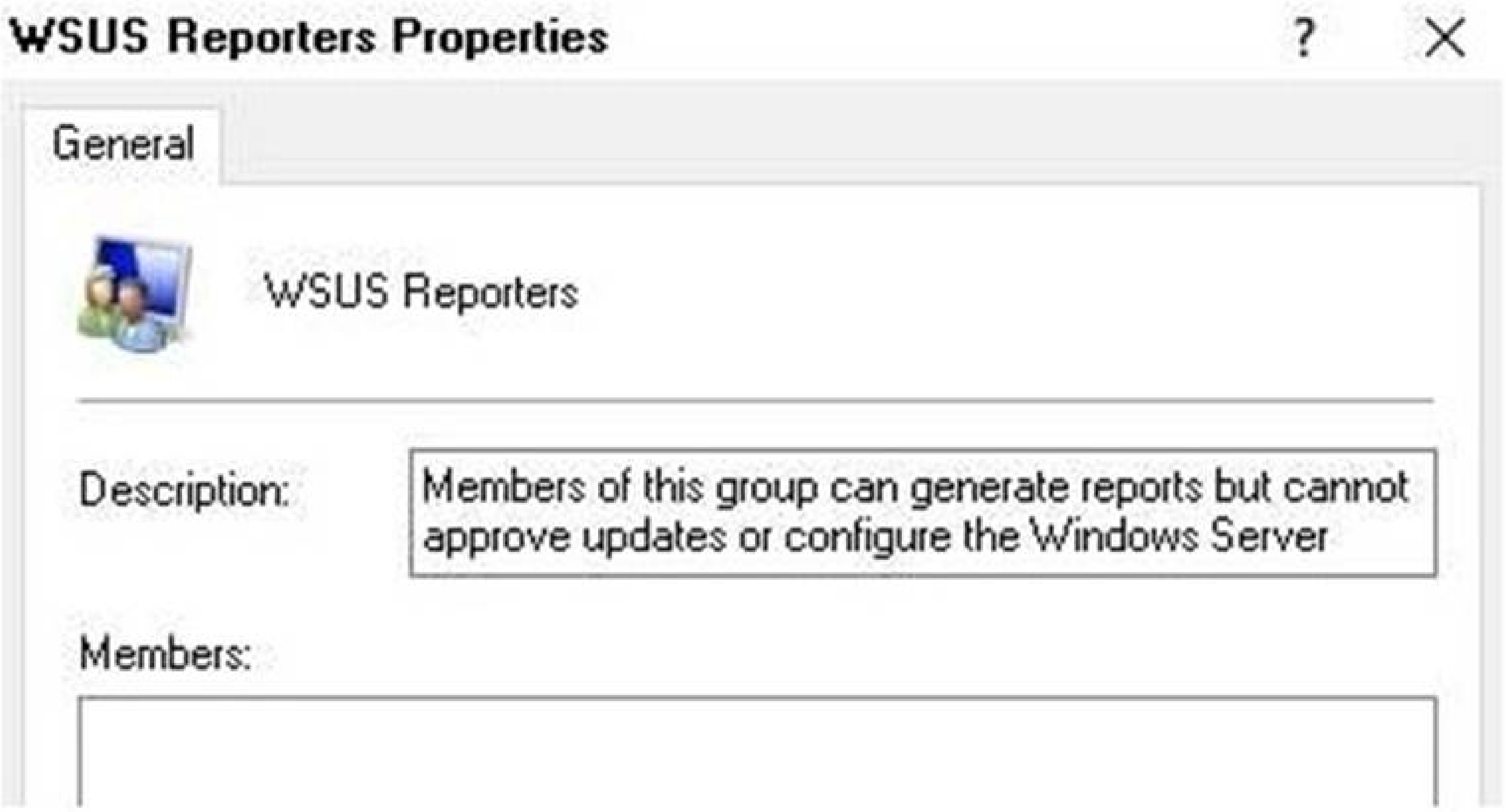
Name	PID	Status	User name	CPU	Memory (pri...	Description
explorer.exe	5532	Running	yungc	00	39,764 K	Windows Explorer
Lsalso.exe	912	Running	SYSTEM	00	1,352 K	Credential Guard
lsass.exe	920	Running	SYSTEM	00	12,092 K	Local Security Authority Process
MBAMAgent.exe	132	Running	SYSTEM	00	1,556 K	MBAMAgent
MicrosoftEdge.exe	10248	Suspended	yungc	00	18,456 K	Microsoft Edge
MicrosoftEdgeCP.exe	10096	Suspended	yungc	00	20,704 K	Microsoft Edge Content Process

NEW QUESTION 8
Your network contains an Active Directory domain named contoso.com.
You install the Windows Server Update Services server role on a member server named Server1. Server1 runs Windows Server 2016.
You need to ensure that a user named Used can perform the following tasks:
*View the Windows Server Update Services (WSUS) configuration.
*Generate WSUS update reports.
The solution must use the principle of least privilege. What should you do on Server1?

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

Answer: B

Explanation:
WSUS Reporters have read only access to the WSUS database and configuration



WSUS Reporters Properties

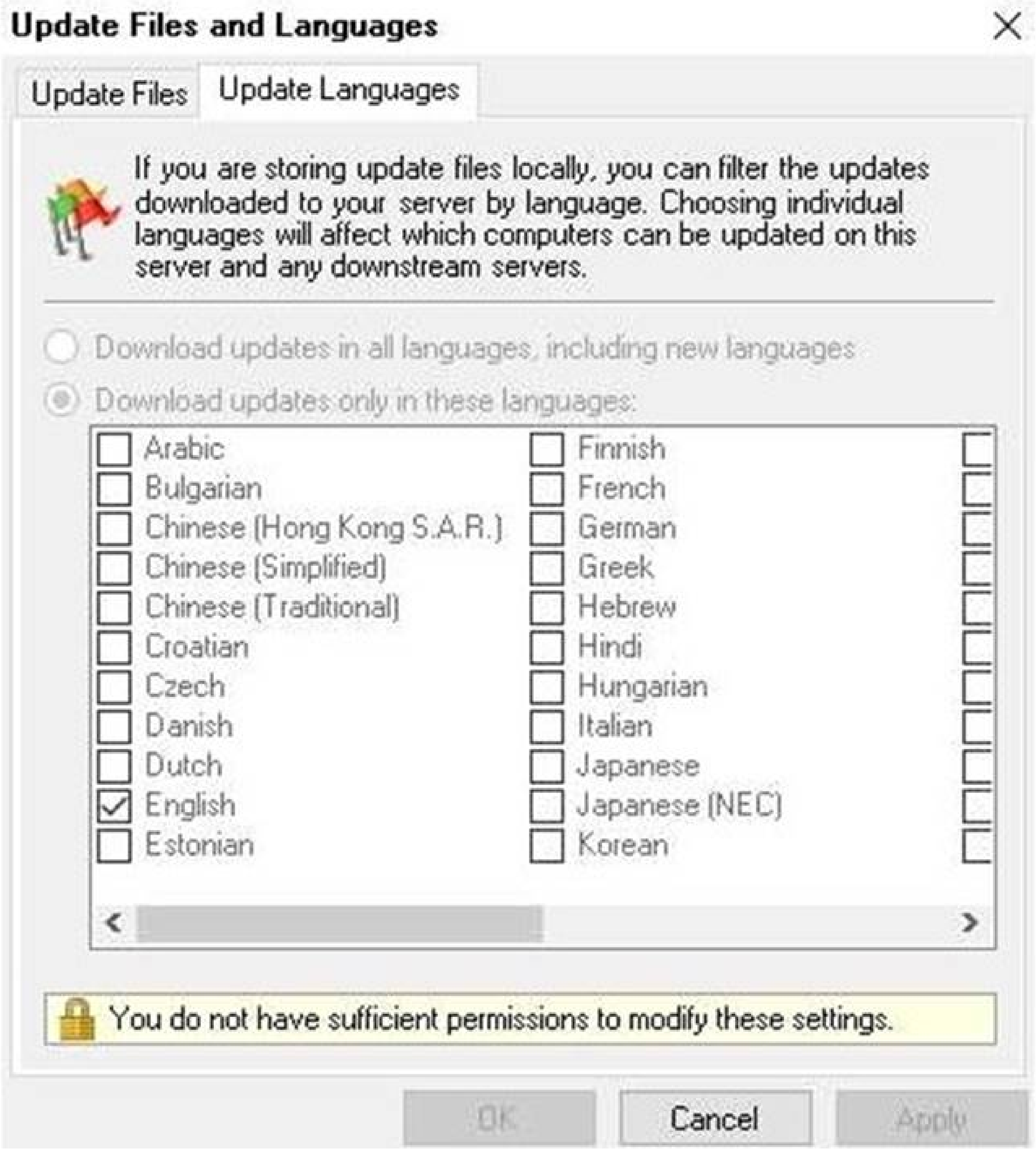
General

WSUS Reporters

Description: Members of this group can generate reports but cannot approve updates or configure the Windows Server

Members:

When a user with “WSUS Reporters” membership, he can view configuration and generate reports as follow:-



Update Files and Languages

Update Files | Update Languages

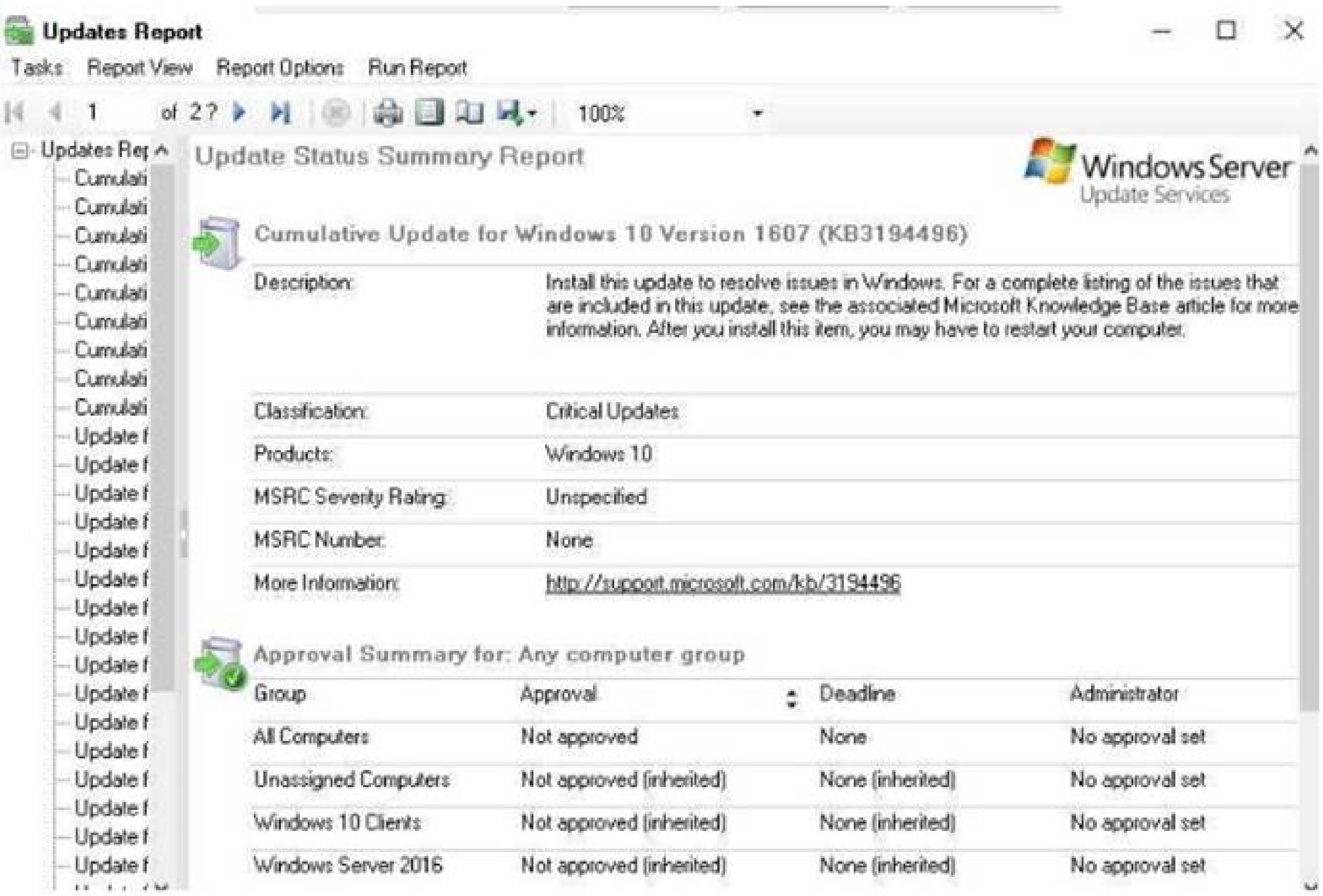
If you are storing update files locally, you can filter the updates downloaded to your server by language. Choosing individual languages will affect which computers can be updated on this server and any downstream servers.

○ Download updates in all languages, including new languages

● Download updates only in these languages:

□ Arabic
□ Bulgarian
□ Chinese (Hong Kong S.A.R.)
□ Chinese (Simplified)
□ Chinese (Traditional)
□ Croatian
□ Czech
□ Danish
□ Dutch
☑ English
□ Estonian
□ Finnish
□ French
□ German
□ Greek
□ Hebrew
□ Hindi
□ Hungarian
□ Italian
□ Japanese
□ Japanese (NEC)
□ Korean

You do not have sufficient permissions to modify these settings.



Update Status Summary Report

Cumulative Update for Windows 10 Version 1607 (KB3194496)

Description:	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.
Classification:	Critical Updates
Products:	Windows 10
MSRC Severity Rating:	Unspecified
MSRC Number:	None
More Information:	http://support.microsoft.com/kb/3194496

Approval Summary for: Any computer group

Group	Approval	Deadline	Administrator
All Computers	Not approved	None	No approval set
Unassigned Computers	Not approved (inherited)	None (inherited)	No approval set
Windows 10 Clients	Not approved (inherited)	None (inherited)	No approval set
Windows Server 2016	Not approved (inherited)	None (inherited)	No approval set

NEW QUESTION 9
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 10
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

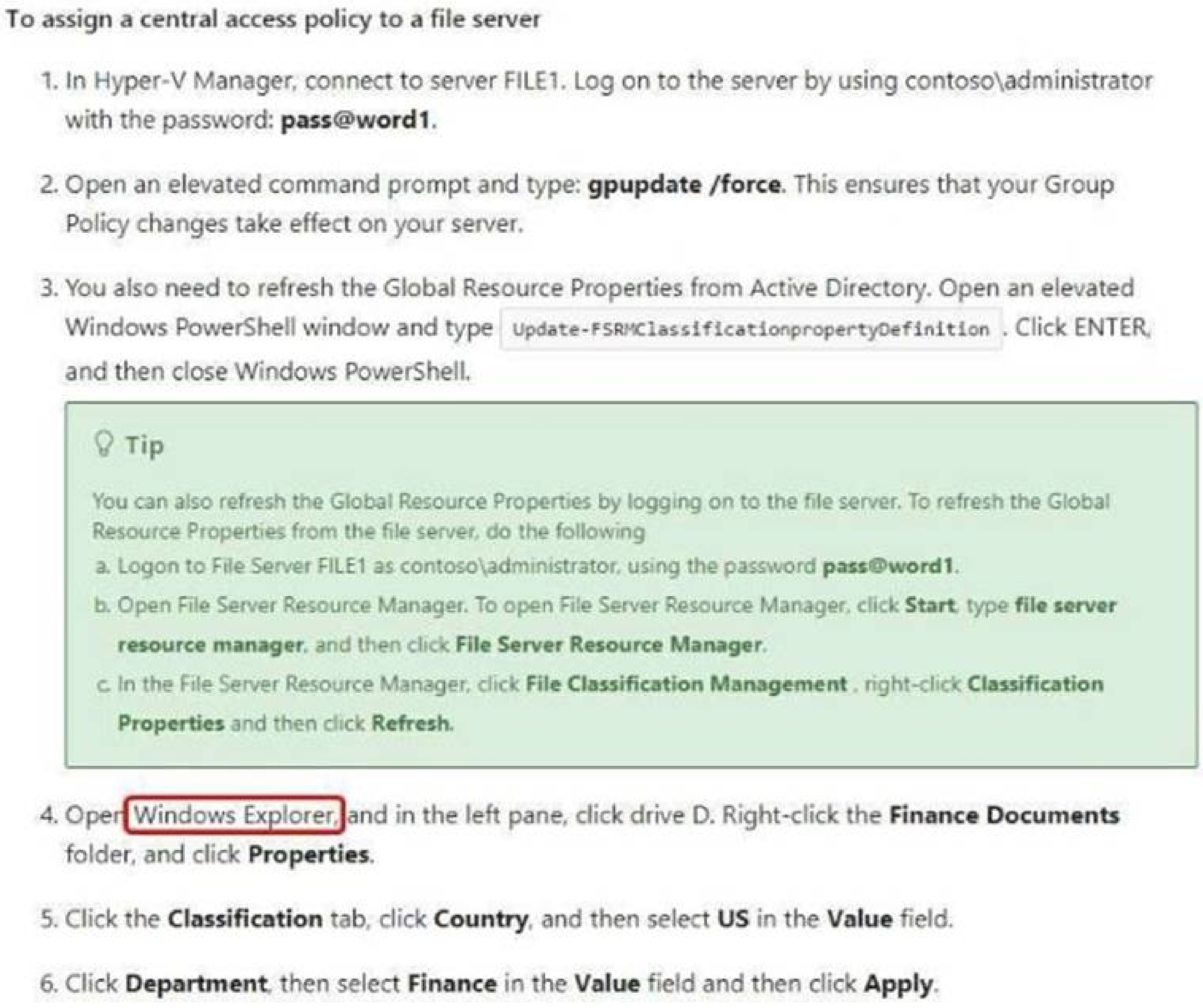
NEW QUESTION 10
Note: This question is port of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question In the series. Each question is Independent of the other questions In this series. Information and details provided in a question apply only to that question.
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016 and a Nano Server named Nano1. Nano1 has two volumes named C and D.
You are signed in to Server1.
You need to configure Data Deduplication on Nano1. Which tool should you use?

A. File Explorer
B. Shared Folders
C. Server Manager
D. Disk Management
E. Storage Explorer
F. Computer Management

G. System Configuration
H. File Server Resource Manager (FSRM)

Answer: C

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



To assign a central access policy to a file server

1. In Hyper-V Manager, connect to server FILE1. Log on to the server by using contoso\administrator with the password: **pass@word1**.

2. Open an elevated command prompt and type: **gpupdate /force**. This ensures that your Group Policy changes take effect on your server.

3. You also need to refresh the Global Resource Properties from Active Directory. Open an elevated Windows PowerShell window and type `Update-FSRMClassificationpropertyDefinition`. Click ENTER, and then close Windows PowerShell.

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

4. Open Windows Explorer, and in the left pane, click drive D. Right-click the **Finance Documents** folder, and click **Properties**.

5. Click the **Classification** tab, click **Country**, and then select **US** in the **Value** field.

6. Click **Department**, then select **Finance** in the **Value** field and then click **Apply**.

NEW QUESTION 12
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question Is independent of the other questions in this series. Information and details provided in a question apply only to that question.
Your network contains an Active Directory domain named contoso.com The domain contains a file server named Server1 that runs Windows Server 2016.
You need to create Work Folders on Server1. Which tool should you use?

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

Answer: C

NEW QUESTION 14
Note: This question is part of a series of question that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is Independent of the other questions in this series. Information and details provided in a question apply only to that question.
Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1 that runs Windows Server 2016.
Server1 has a volume named Volume1.
Dynamic Access Control is configured. A resource property named Property1 was created in the domain.
You need to ensure that Property1 is set to a value of Big for all of the files in Volume1 that are larger than 10 MB.
Which tool should you use?

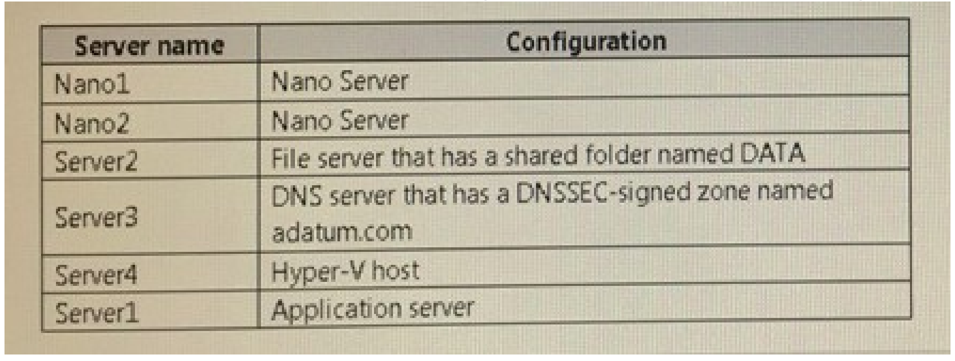
A. File Explorer
B. Shared Folders
C. Server Manager
D. Disk Management

E. Storage Explorer
F. Computer Management
G. System Configuration
H. File Server Resource Manager (FSRM)

Answer: H

Explanation:
Automatic File Classification of FSRM
https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/deploy-automatic-fileclassification– demonstration-stepshttps:// blogs.technet.microsoft.com/filecab/2009/08/13/using-windows-powershell-scripts-for-fileclassification/

NEW QUESTION 19
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer
choices, but the text of the scenario is exactly the same in each question in this series. Start of repeated scenario
Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.
The domain contains the servers configured as shown in the following table.



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

All servers run Windows Server 2016. All client computers run Windows 10.
You have an organizational unit (OU) named Marketing that contains the computers in the marketing department You have an OU named finance that contains the computers in the finance department You have an OU named AppServers that contains application servers. A Group Policy object (GPO) named GP1 is linked to the Marketing OU. A GPO named GP2 is linked to the AppServers OU. You install Windows Defender on Nano1.
End of repeated scenario
You need to exclude D:\Folder1 on Nano1 from being scanned by Windows Defender. Which cmdlet should you run?

A. Set-StorageSetting
B. Set-FsrmFileScreenException
C. Set-MpPreference
D. Set-DtcAdvancedSetting

Answer: C

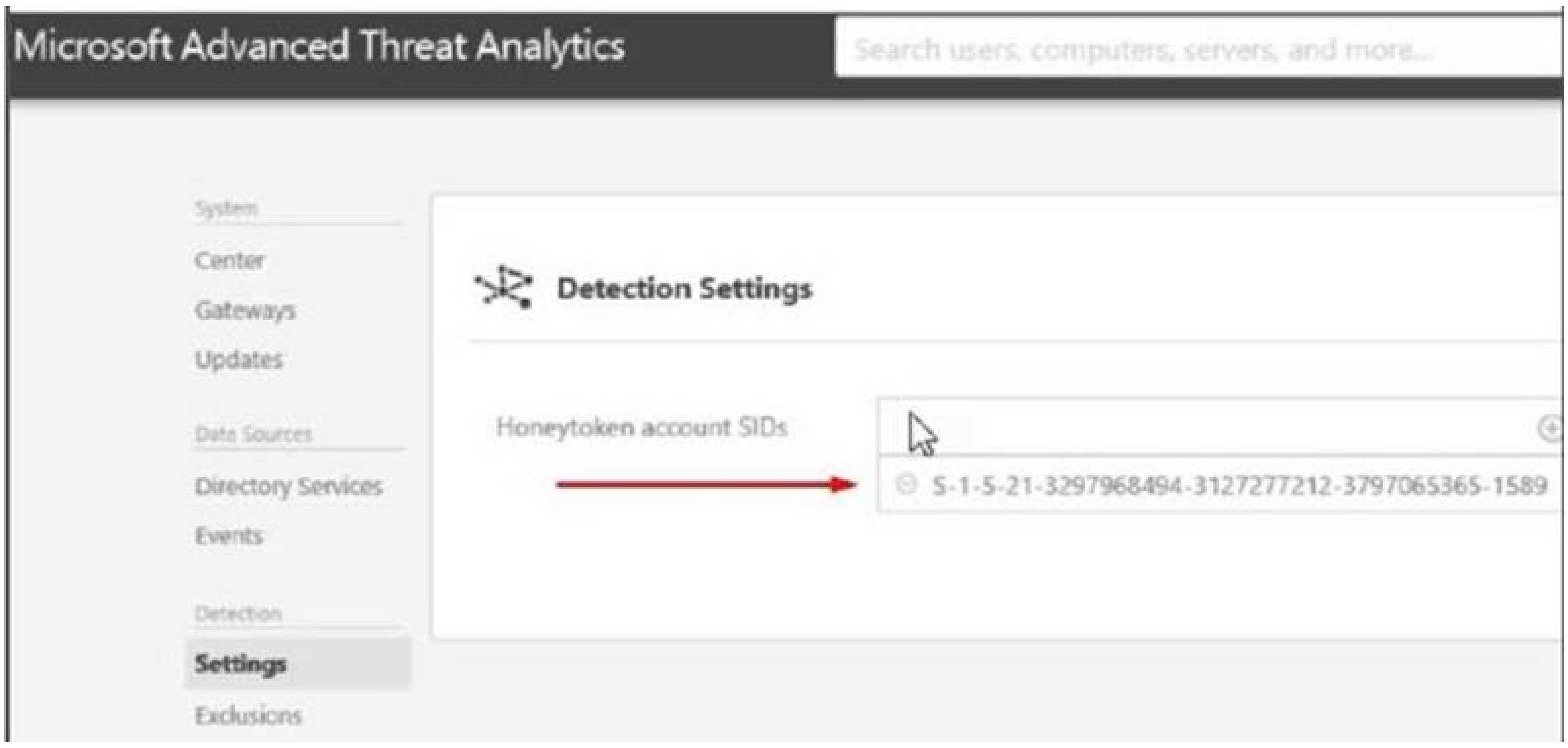
Explanation:
https://technet.microsoft.com/en-us/itpro/powershell/windows/defender/set-mppreference

NEW QUESTION 23
Your network contains an Active Directory domain named contoso.com. You are deploying Microsoft Advanced Threat Analytics (ATA).
You create a user named User1.
You need to configure the user account of User1 as a Honeytoken account. Which information must you use to configure the Honeytoken account?

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

Answer: C

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



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

NEW QUESTION 28
Your network contains an Active Directory forest named conloso.com. The network is connected to the Internet.
You have 100 point-of-sale (POS) devices that run Windows 10. The devices cannot access the Internet.
You deploy Microsoft Operations Management Suite (OMS).
You need to use OMS to collect and analyze data from the POS devices. What should you do first?

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

Answer: B

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

NEW QUESTION 33
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 35
Windows PowerShell is a task-based command-line shell and scripting language designed especially for system administration.
Windows Defender comes with a number of different Defender-specific cmdlets that you can run through PowerShell to automate common tasks.
Which Cmdlet would you run first if you wanted to perform an offline scan?

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

Answer: A

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

NEW QUESTION 39
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 42
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 43
Encryption-supported VMs are intended for use where the fabric administrators are fully trusted. For example, an enterprise might deploy a guarded fabric in order to ensure VM disks are encrypted at-rest for compliance purposes.
Shielded VMs are intended for use in fabrics where the data and state of the VM must be protected from both fabric administrators and untrusted software that might be running on the Hyper-V hosts. Is the Virtual Machine Connection (Console), HID devices (e.g. keyboard, mouse) ON or OFF for Encryption Supported VM’s?

A. Off
B. On

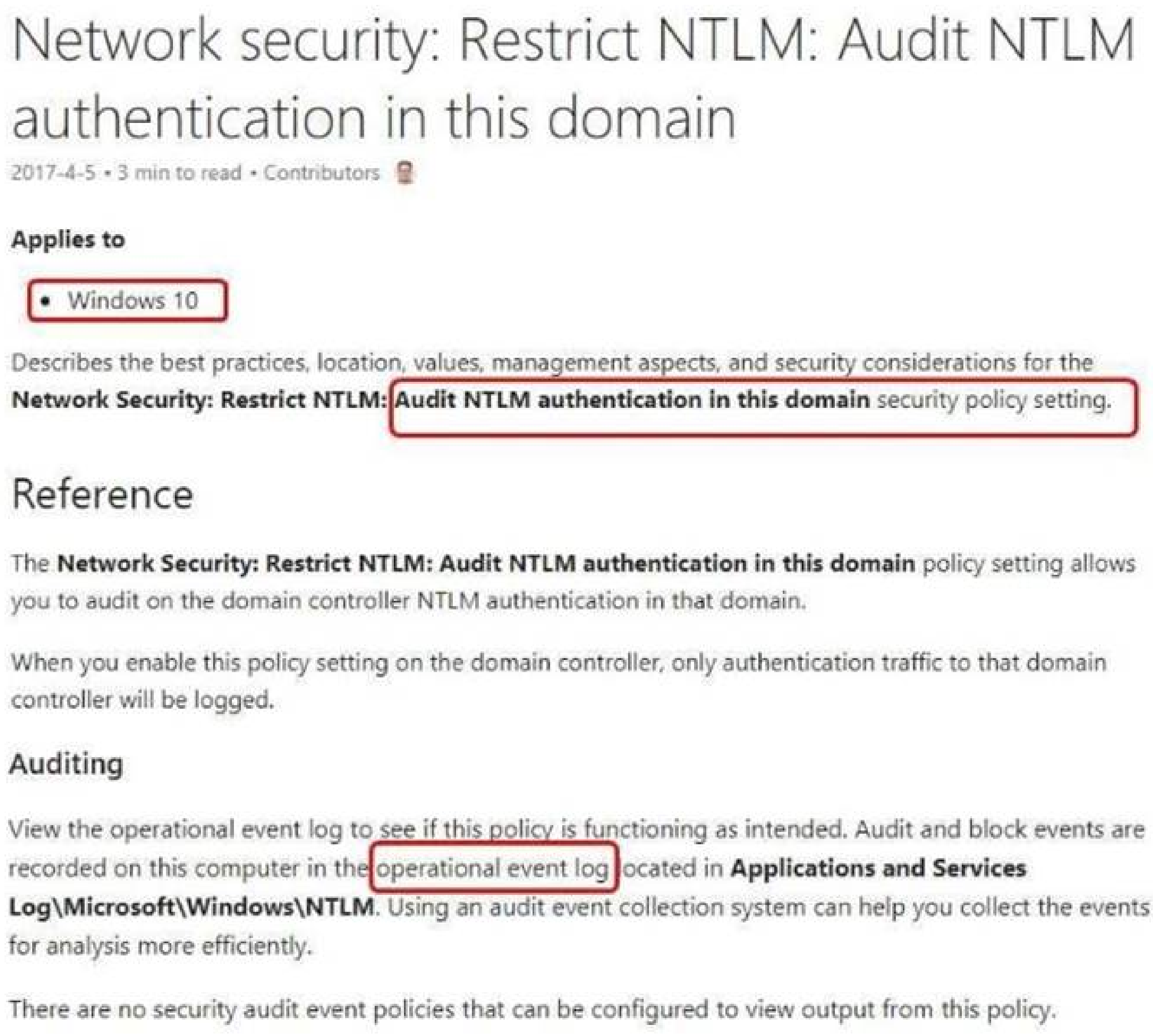
Answer: B

NEW QUESTION 46
Your network contains an Active Directory domain named contoso.com. The domain contains multiple servers that run multiple applications.
Domain user accounts are used to authenticate access requests to the servers. You plan to prevent NTLM from being used to authenticate to the servers. You start to audit NTLM authentication events for the domain.
You need to view all of the NTLM authentication events and to identify which applications authenticate by using NTLM.
On which computers should you review the event logs and which logs should you review?

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

Answer: AE

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



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

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

Applies to

- Windows 10

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

Reference

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

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

Auditing

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

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

NEW QUESTION 51
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

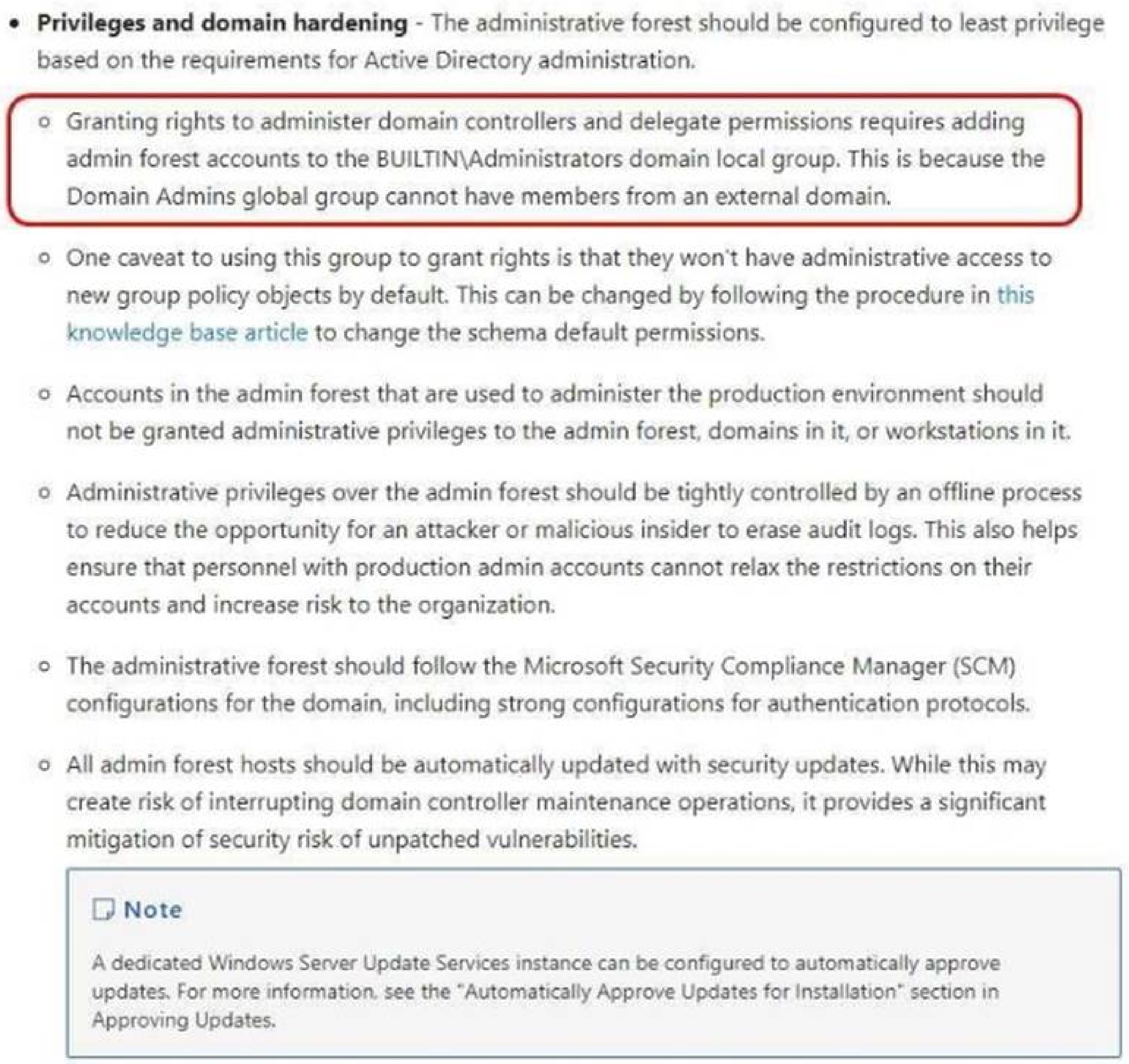
Explanation:
-Prevent console access to FS1. –> Enable shielding for FS1
-Prevent data from being extracted from the VHDX file of FS1. –> Enable BitLocker Drive Encryption (BitLocker) for all the volumes on FS1

NEW QUESTION 52
Your network contains an Active Directory forest named contoso.com. All servers run Windows Server 2016.
You implement a single-domain administrative forest named admin.contoso.com that has Enhanced Security Administrative Environment (ESAE) deployed.
You have an administrative user named Admin1 in admin.contoso.com.
You need to ensure that Admin1 can manage the domain controllers in contoso.com. To which group should you add Admin1?

A. Contoso\\Domain Admins
B. Admin\\Administrators
C. Admin\\Domain Admins
D. Contoso\\Administrators

Answer: D

Explanation:
admin.contoso.com (NetBIOS domain name “ADMIN\\”) is the administrative domain. contoso.com (NetBIOS domain name “CONTOSO\\”) is the corporate resource domain. See below.
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securingprivilegedaccess- reference-material

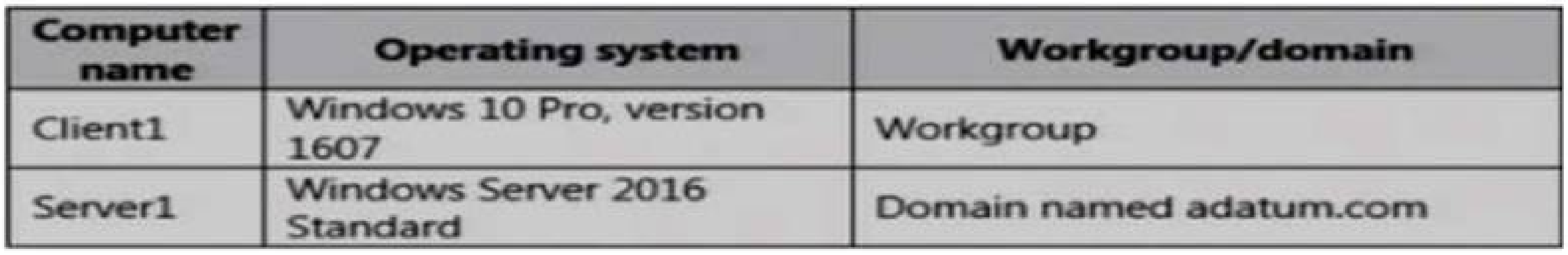


- **Privileges and domain hardening** - The administrative forest should be configured to least privilege based on the requirements for Active Directory administration.
  - Granting rights to administer domain controllers and delegate permissions requires adding admin forest accounts to the BUILTIN\Administrators domain local group. This is because the Domain Admins global group cannot have members from an external domain.
  - One caveat to using this group to grant rights is that they won't have administrative access to new group policy objects by default. This can be changed by following the procedure in this knowledge base article to change the schema default permissions.
  - Accounts in the admin forest that are used to administer the production environment should not be granted administrative privileges to the admin forest, domains in it, or workstations in it.
  - Administrative privileges over the admin forest should be tightly controlled by an offline process to reduce the opportunity for an attacker or malicious insider to erase audit logs. This also helps ensure that personnel with production admin accounts cannot relax the restrictions on their accounts and increase risk to the organization.
  - The administrative forest should follow the Microsoft Security Compliance Manager (SCM) configurations for the domain, including strong configurations for authentication protocols.
  - All admin forest hosts should be automatically updated with security updates. While this may create risk of interrupting domain controller maintenance operations, it provides a significant mitigation of security risk of unpatched vulnerabilities.

Note

A dedicated Windows Server Update Services instance can be configured to automatically approve updates. For more information, see the "Automatically Approve Updates for Installation" section in Approving Updates.

NEW QUESTION 54
You have two computers configured as shown in the following table.



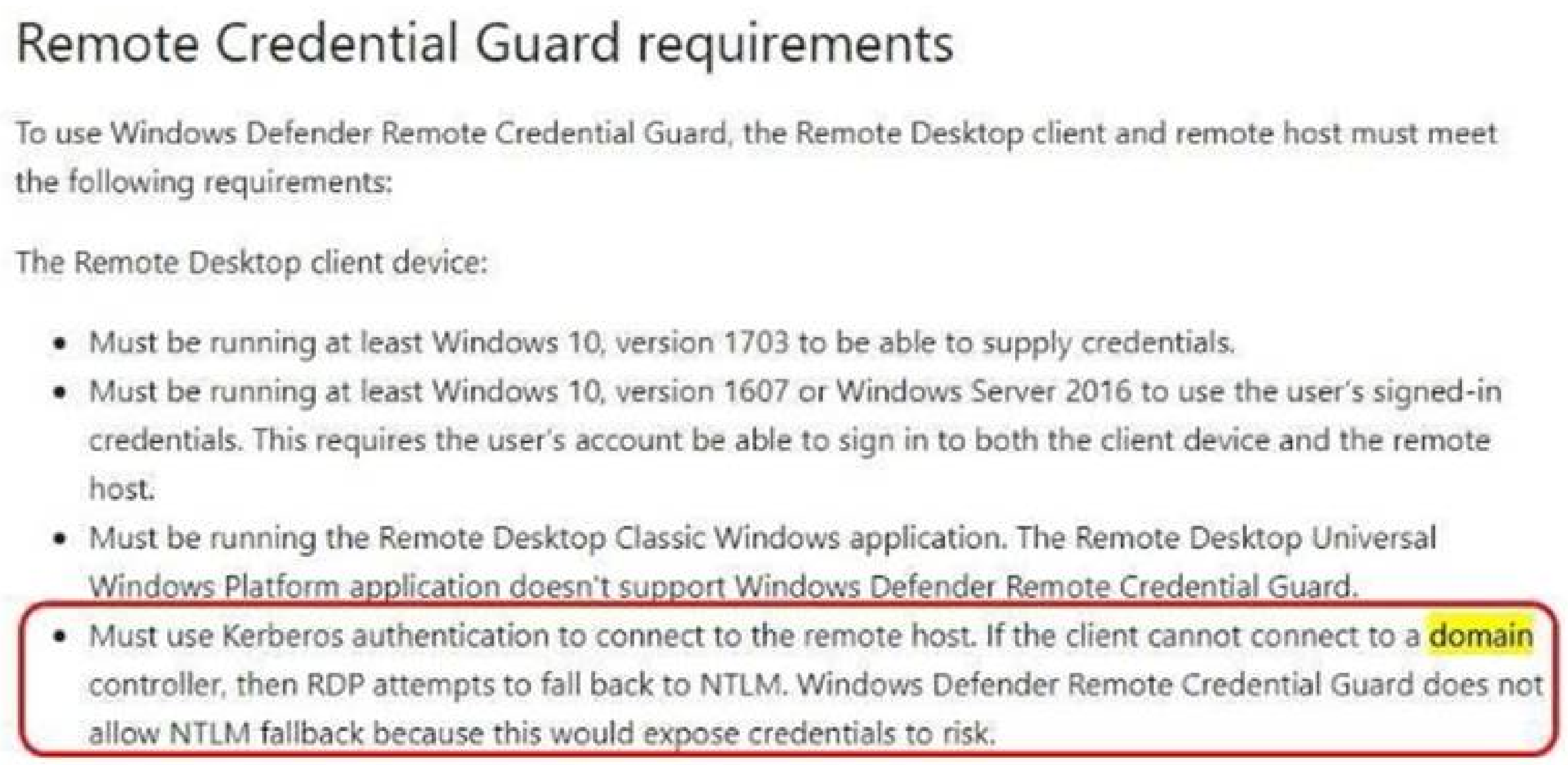
Computer name	Operating system	Workgroup/domain
Client1	Windows 10 Pro, version 1607	Workgroup
Server1	Windows Server 2016 Standard	Domain named adatum.com

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.

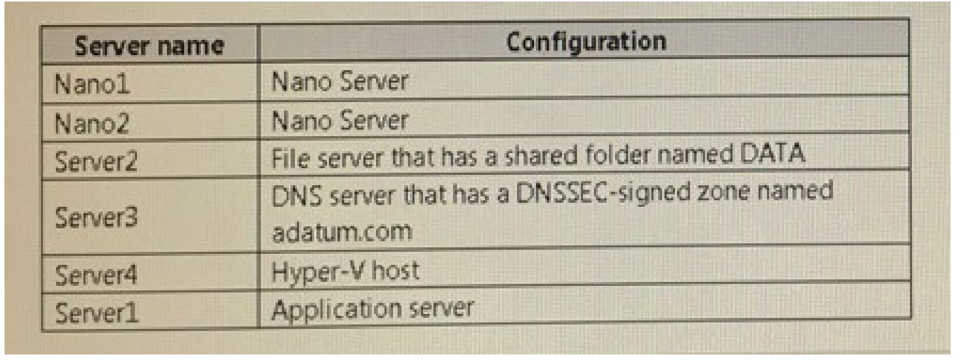
NEW QUESTION 56
Your network contains an Active Directory domain named contoso.com. The domain contains several Hyper-V hosts.
You deploy a server named Server22 to a workgroup. Server22 runs Windows Server 2016. You need to configure Server22 as the primary Host Guardian Service server.
Which three cmdlets should you run in sequence?

A. Install-HgsServer
B. Install-Module
C. Install-Package
D. Enable-WindowsOptionalFeature
E. Install-ADDSDomainController
F. Initialize-HgsServer

Answer: AEF

Explanation:
Correct order of actions:
1. Install-ADDSDomainController , as Server22 is a workgroup computer, create a new domain on it first.
2. Install-HgsServer
3. Initialize-HgsServer
https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shieldedvm/guarded-fabricsetting-up-the-host-guardian-service-hgs
https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shieldedvm/guarded-fabricinstall-hgs-default
Install-HgsServer
https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shieldedvm/guarded-fabricinitialize-hgs-tpm-mode-default
Initialize-HgsServer

NEW QUESTION 57
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.
Start of repeated scenario
Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.
The domain contains the servers configured as shown in the following table.



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

All servers run Windows Server 2016. All client computers run Windows 10.
You have an organizational unit (OU) named Marketing that contains the computers in the marketing department You have an OU named finance that contains the computers in the finance department You have an OU named AppServers that contains application servers. A Group Policy object (GPO) named GP1 is linked to the Marketing OU. A GPO named GP2 is linked to the AppServers OU. You install Windows Defender on Nano1.
End of repeated scenario
You need to ensure that when a configuration change is made on Nano2, Nano2 will revert back to the original configuration automatically.
What should you do first?

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

Answer: B

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

NEW QUESTION 60
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

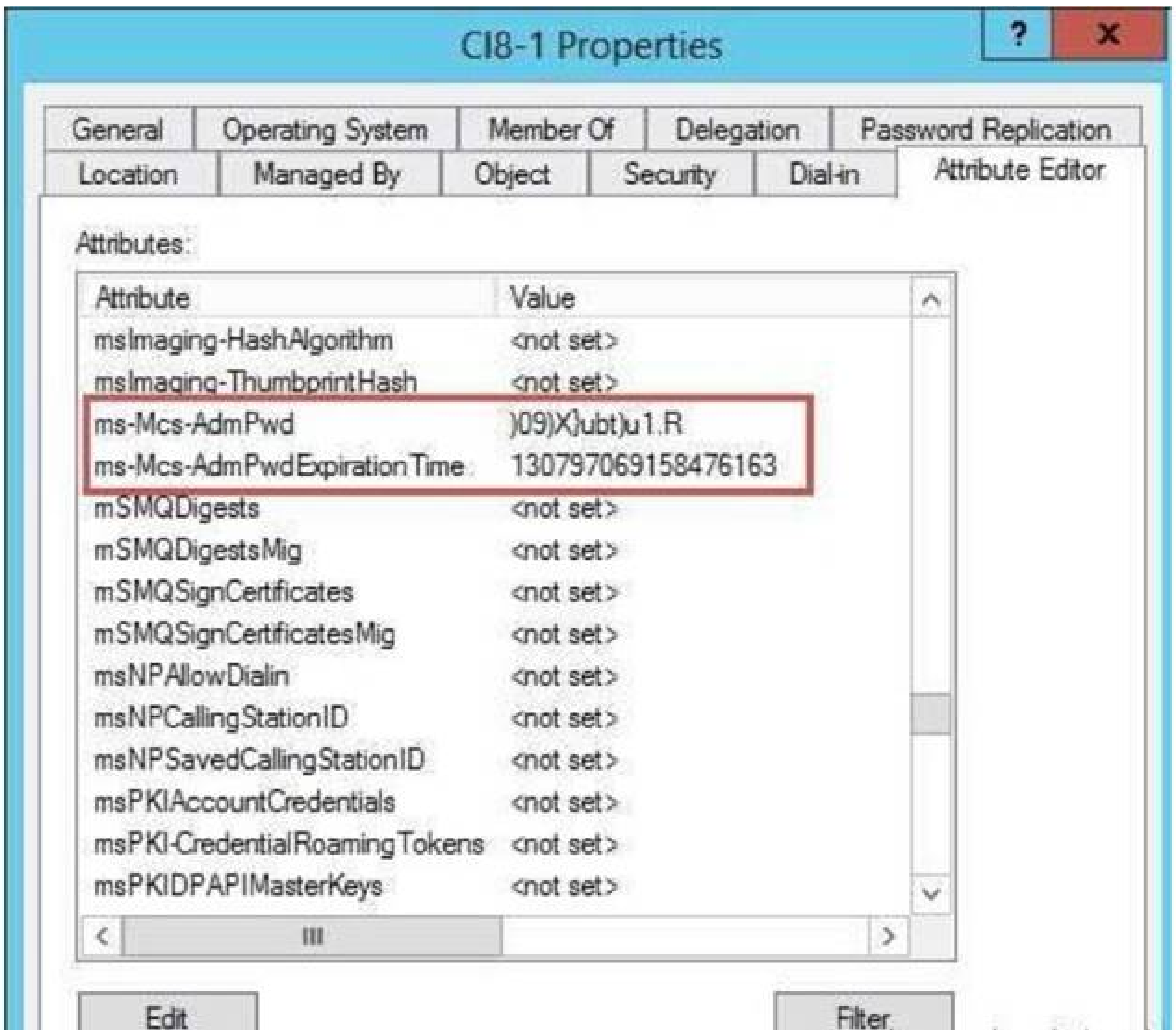
Explanation:
Get-NetFirewallRule -Direction Inbound <— view inbound rules for all profiles The following examples shows inbound rule for specific firewall profile. Get-NetFirewallRule -Direction Inbound | where {$_.Profile -eq “Domain”} Get-NetFirewallRule -Direction Inbound | where {$_.Profile -eq “Public”}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

NEW QUESTION 61
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.



Attributes:

Attribute	Value
msImaging-HashAlgorithm	<not set>
msImaging-ThumbprintHash	<not set>
ms-Mcs-AdmPwd	)09)X}ubt)u1.R
ms-Mcs-AdmPwdExpirationTime	130797069158476163
mSMQDigests	<not set>
mSMQDigestsMig	<not set>
mSMQSignCertificates	<not set>
mSMQSignCertificatesMig	<not set>
msNPAllowDialin	<not set>
msNPCallingStationID	<not set>
msNPSavedCallingStationID	<not set>
msPKIAccountCredentials	<not set>
msPKI-CredentialRoamingTokens	<not set>
msPKIDPAPIMasterKeys	<not set>

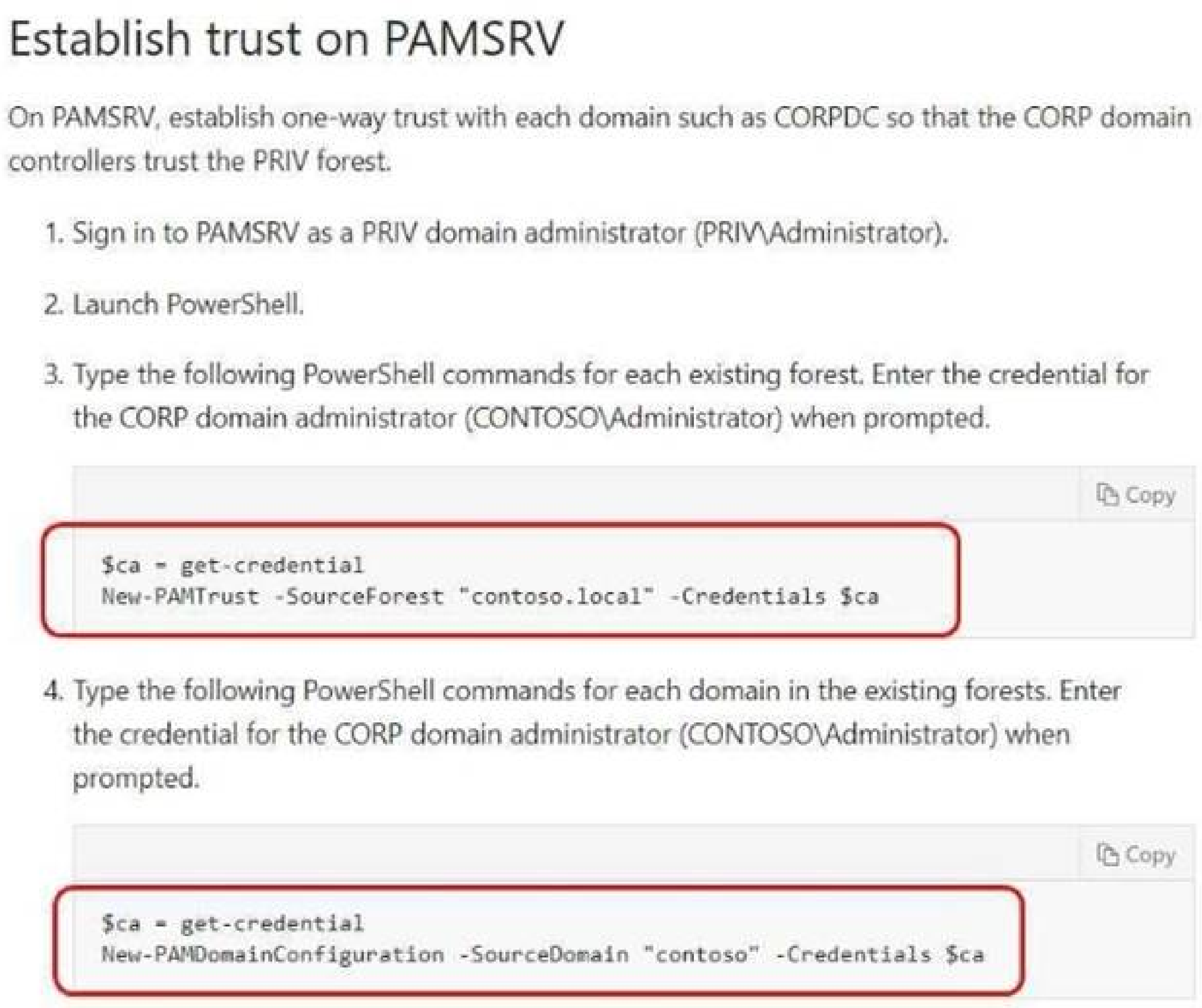
NEW QUESTION 63

Your network contains an Active Directory forest named contoso.com. The forest contains three domains. All domain controllers run Windows Server 2016.
You deploy a second Active Directory forest named admin.contoso.com.
The forest contains a domain member server named Server1. Server1 has Microsoft Identity Manager (MIM) 2016 deployed.
You need to implement Privileged Access Management (PAM) and to use admin.contoso.com as an administrative forest.
Which two actions should you perform? Each correct answers presents part of the solution.

A. From a domain controller in contoso.co
B. run the New-PAMTrust cmdlet.
C. From Server1, run the New-PAMDomainConfiguration cmdlet
D. From a domain controller in admin.contoso.com, run the New-PAMTrust cmdlet.
E. From a domain controller in contoso.com, run the New-PAMDomainConfiguration cmdlet.
F. From a domain controller in admin.contoso.com, run the New-PAMDomainConfiguration cmdlet
G. From Server1, run the New-PAMTrust cmdlet

Answer: BF

Explanation:
https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/configuring-mim-environmentfor- pam
https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/step-5-establish-trust-betweenpriv- corpforests



Establish trust on PAMSRV

On PAMSRV, establish one-way trust with each domain such as CORPDC so that the CORP domain controllers trust the PRIV forest.

1. Sign in to PAMSRV as a PRIV domain administrator (PRIV\Administrator).

2. Launch PowerShell.

3. Type the following PowerShell commands for each existing forest. Enter the credential for the CORP domain administrator (CONTOSO\Administrator) when prompted.

```
$ca = get-credential
New-PAMTrust -SourceForest "contoso.local" -Credentials $ca
```

4. Type the following PowerShell commands for each domain in the existing forests. Enter the credential for the CORP domain administrator (CONTOSO\Administrator) when prompted.

```
$ca = get-credential
New-PAMDomainConfiguration -SourceDomain "contoso" -Credentials $ca
```

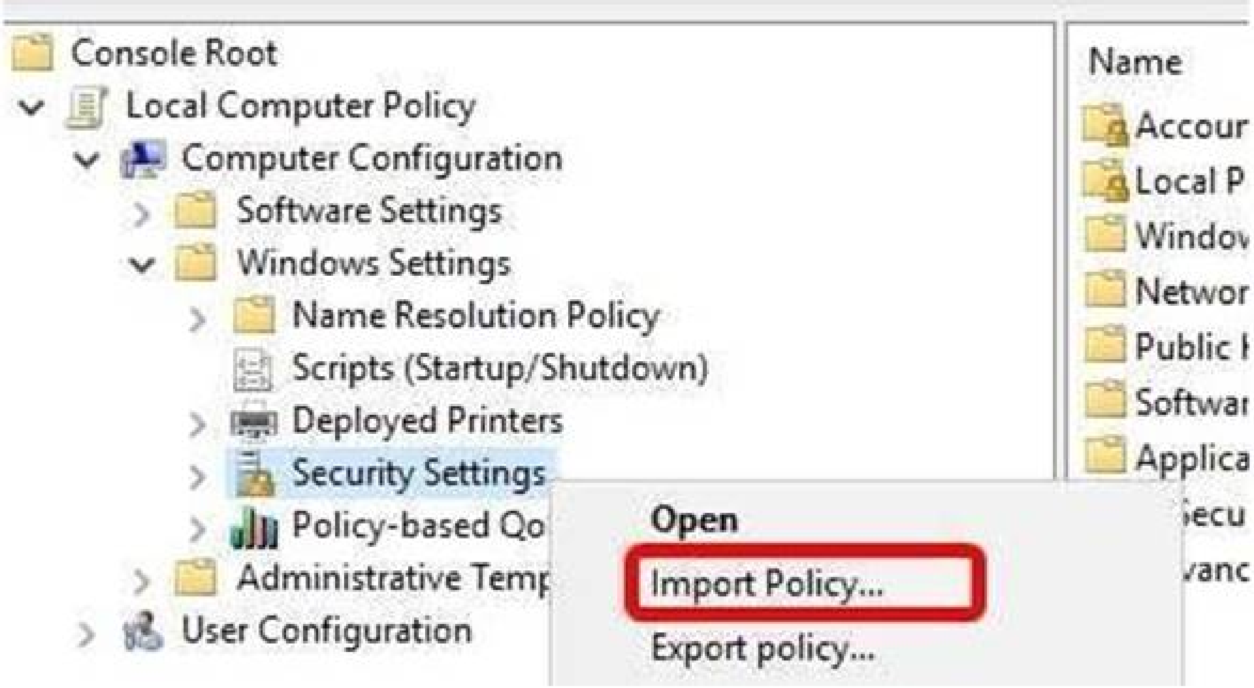
NEW QUESTION 64

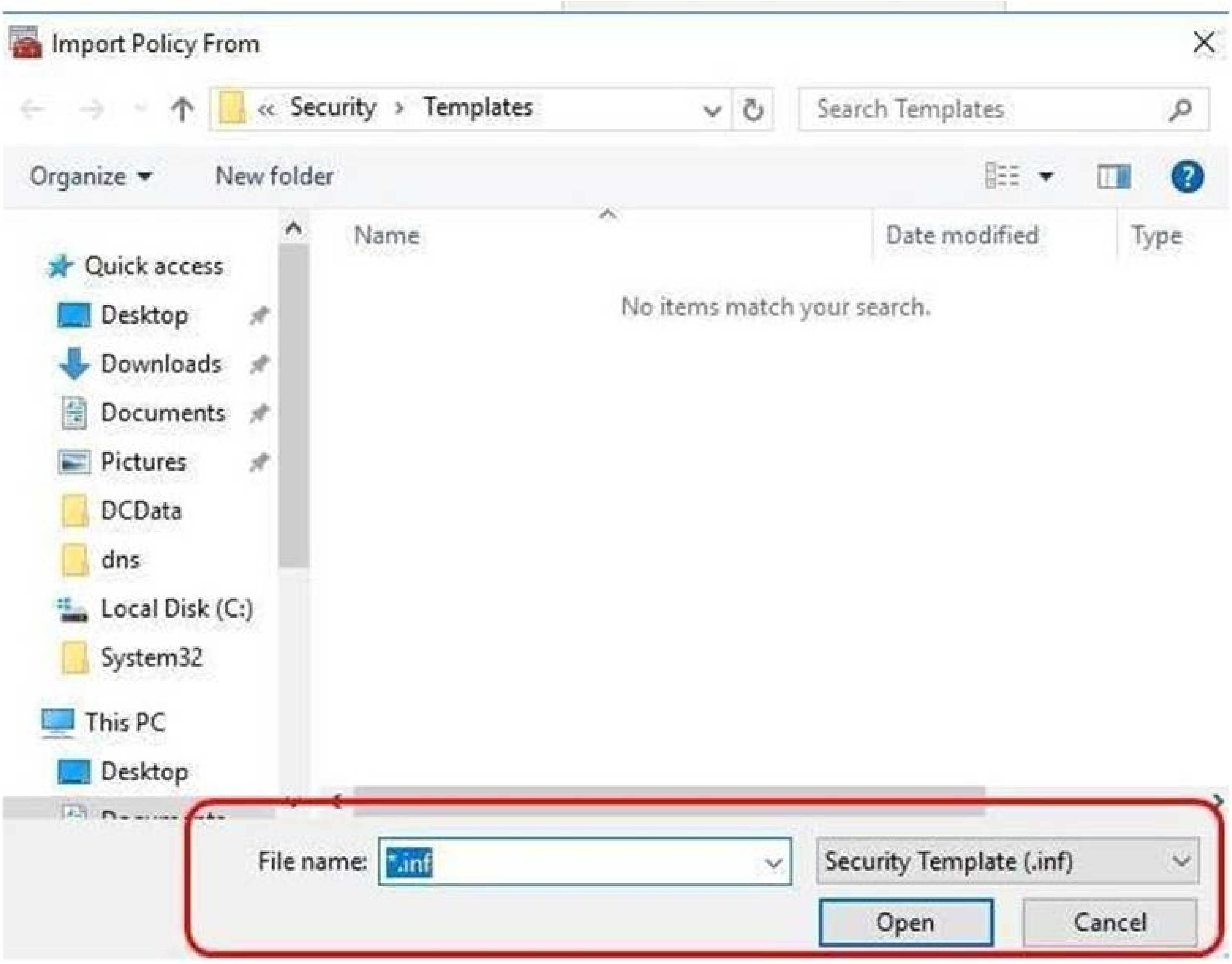
Your network contains an internal network and a perimeter network. The internal network contains an Active Directory forest named contoso.com.
You deploy five servers to the perimeter network.
All of the servers run Windows Server 2016 and are the members of a workgroup.
You need to apply a security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



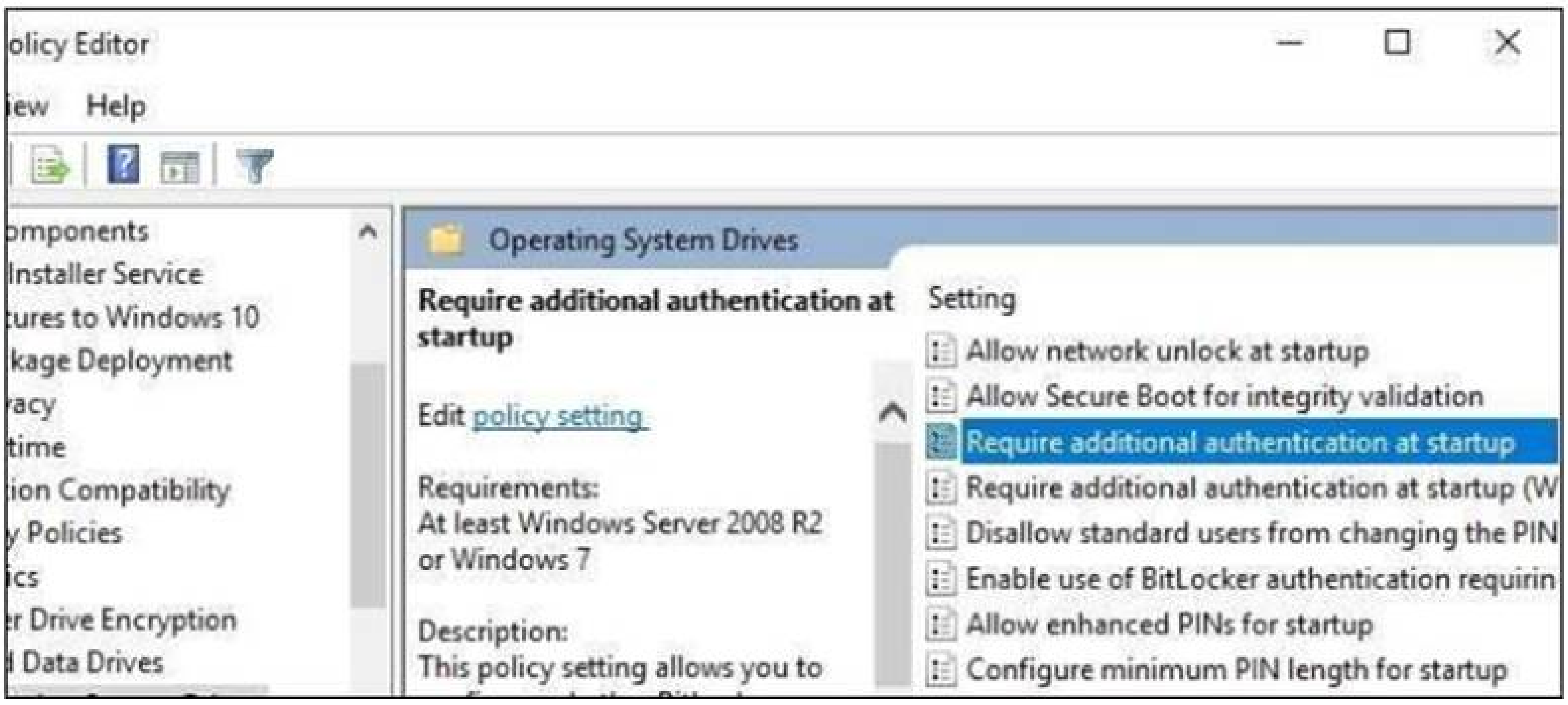


NEW QUESTION 69
You have a Hyper-V host named Server1 that runs Windows Server 2016. Server1 has a generation 2 virtual machine named VM1 that runs Windows 10.
You need to ensure that you can turn on BitLocker Drive Encryption (BitLocker) for drive C: on VM1. What should you do?

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.



Require additional authentication at startup

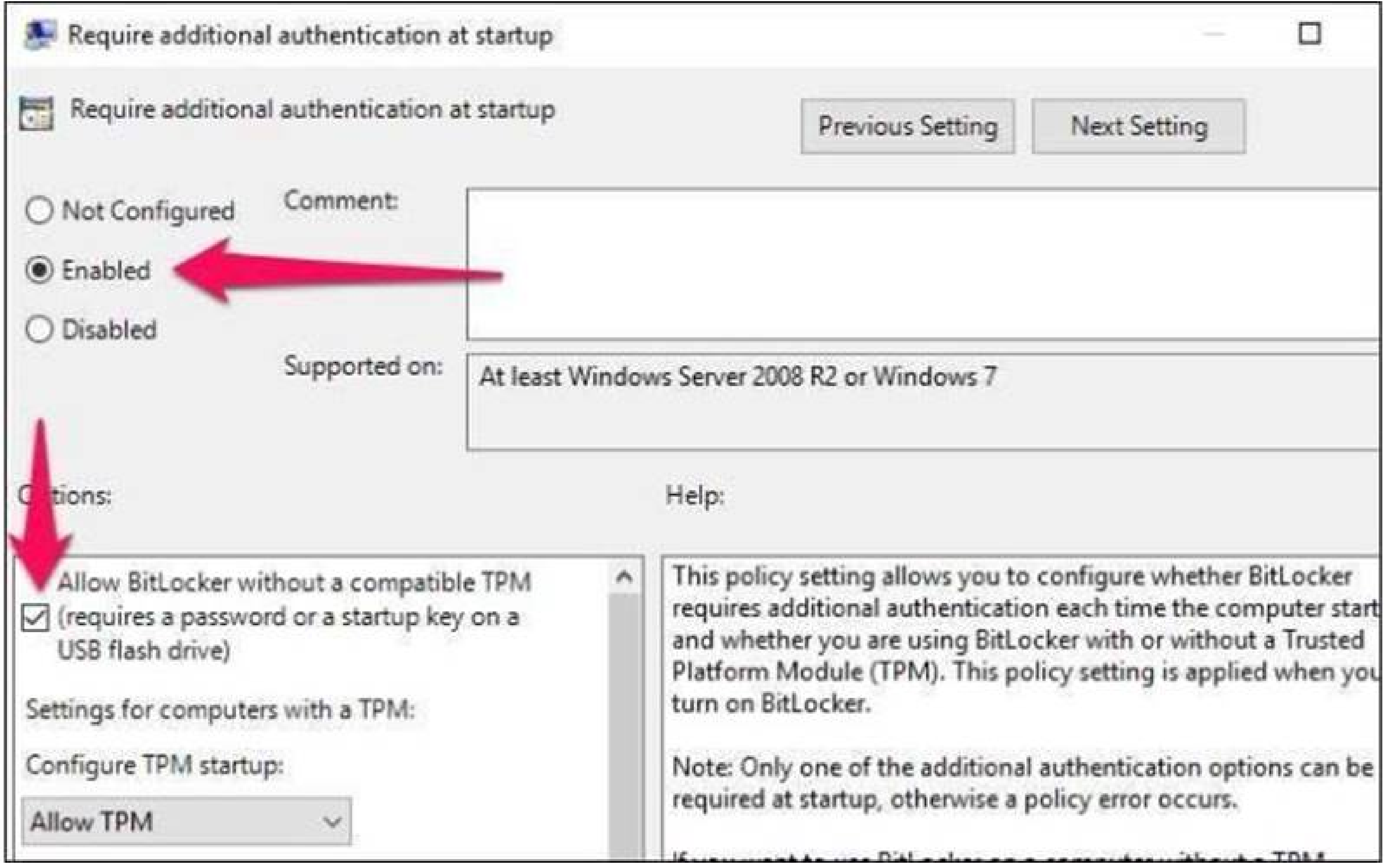
Edit policy setting

Requirements:
At least Windows Server 2008 R2 or Windows 7

Description:
This policy setting allows you to

Setting
- Allow network unlock at startup
- Allow Secure Boot for integrity validation
- Require additional authentication at startup
- Require additional authentication at startup (W
- Disallow standard users from changing the PIN
- Enable use of BitLocker authentication requirin
- Allow enhanced PINs for startup
- Configure minimum PIN length for startup

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



Require additional authentication at startup

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2008 R2 or Windows 7

Options:

☑ Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)

Settings for computers with a TPM:

Configure TPM startup:

Allow TPM

Help:

This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer start and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.

Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.

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 74
Your network contains an Active Directory domain named contoso.com.
The domain contains 10 computers that are in an organizational unit (OU) named OU1. You deploy the Local Administrator Password Solution (LAPS) client to the computers.
You link a Group Policy object (GPO) named GPO1 to OU1, and you configure the LAPS password policy settings in GPO1.
You need to ensure that the administrator passwords on the computers in OU1 are managed by using LAPS.
Which two actions should you perform? Each correct answer presents part of the solution.

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

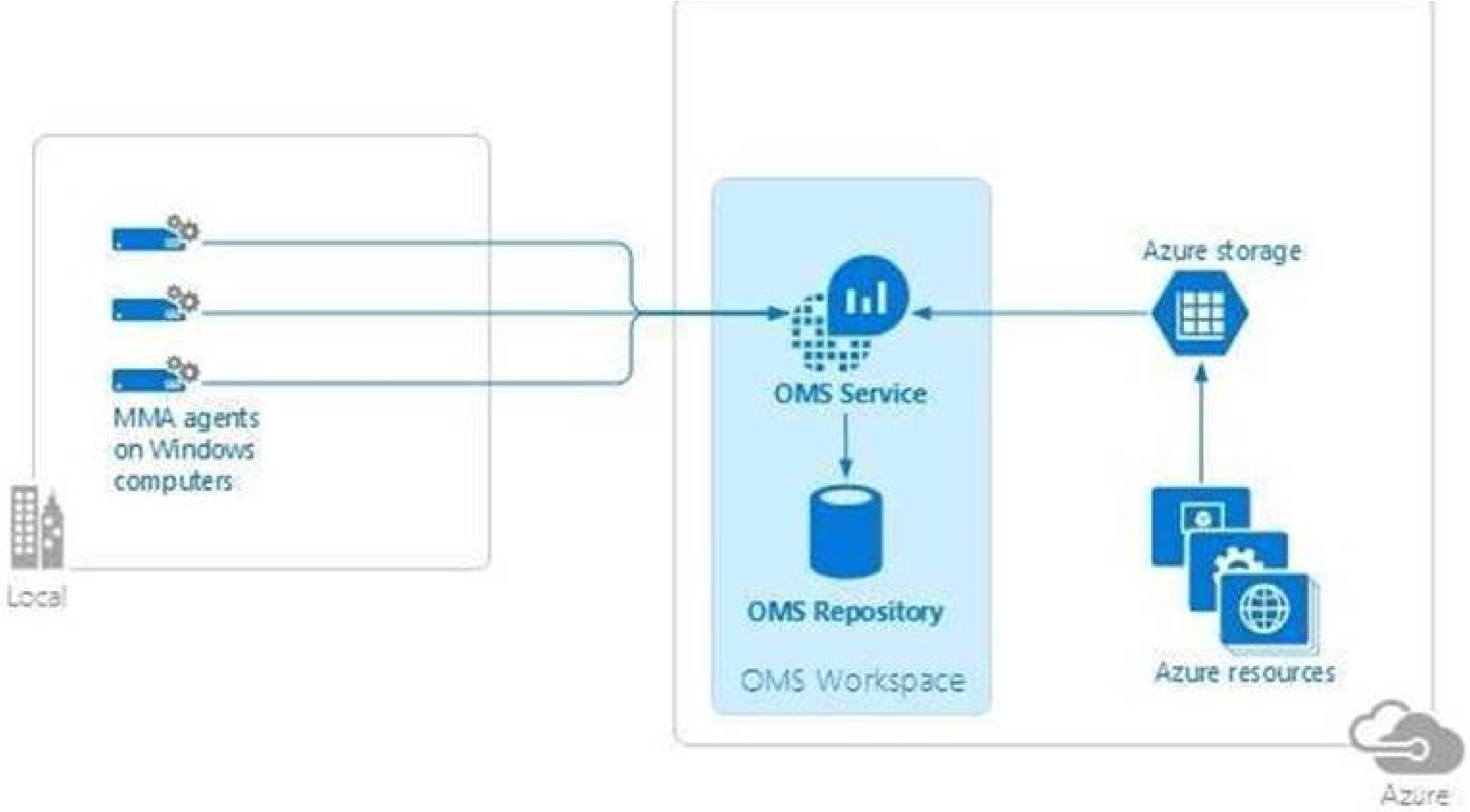
Answer: BE

NEW QUESTION 78
Your network contains an Active Directory domain named contoso.com.
You deploy a server named Server1 that runs Windows Server 2016. Server1 is in a workgroup. You need to collect the logs from Server1 by using Log Analytics in Microsoft Operations Management Suite (OMS).
What should you do first?

A. Join Server1 to the domain.
B. Create a Data Collector Set.
C. Install Microsoft Monitoring Agent on Server1.
D. Create an event subscriptio

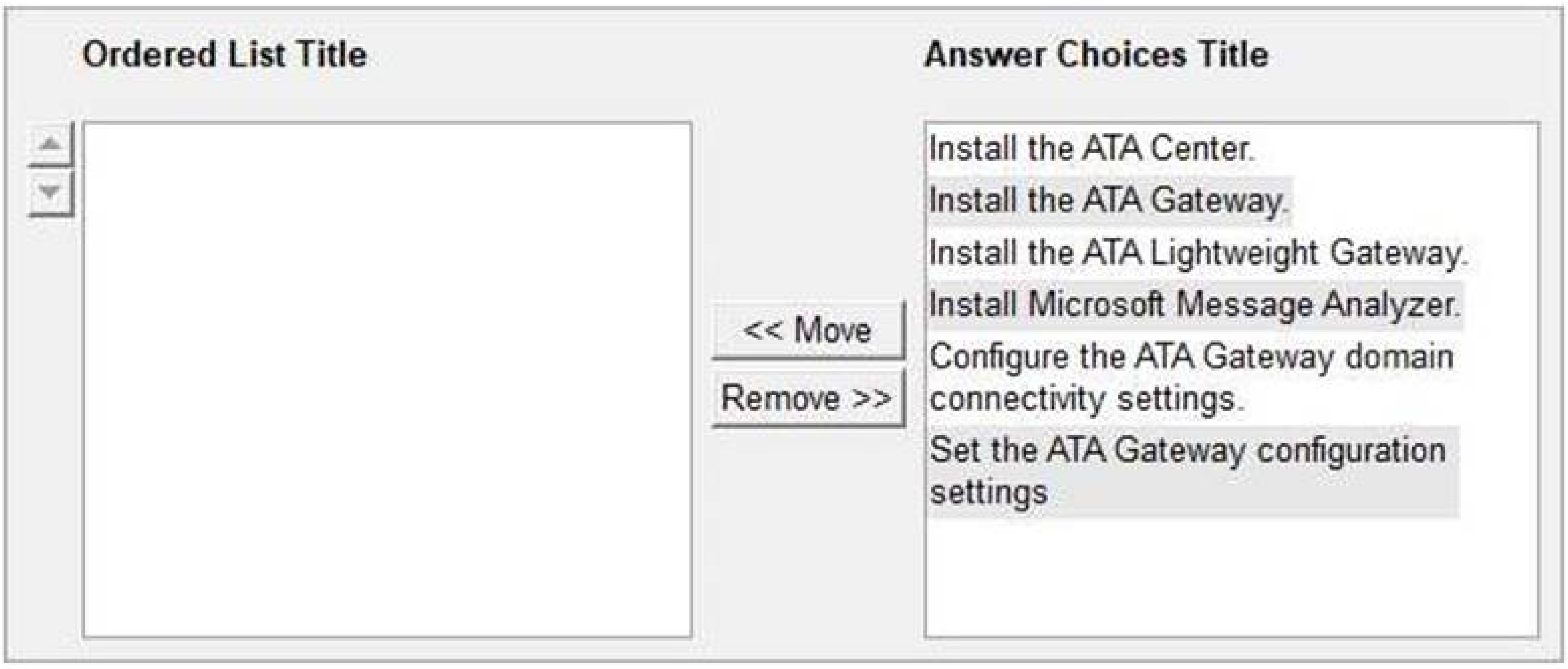
Answer: C

Explanation:
https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-windows-agents
You need to install and connect Microsoft Monitoring Agent for all of the computers that you



You can install the OMS MMA on stand-alone computers, servers, and virtual machines.

NEW QUESTION 80
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?

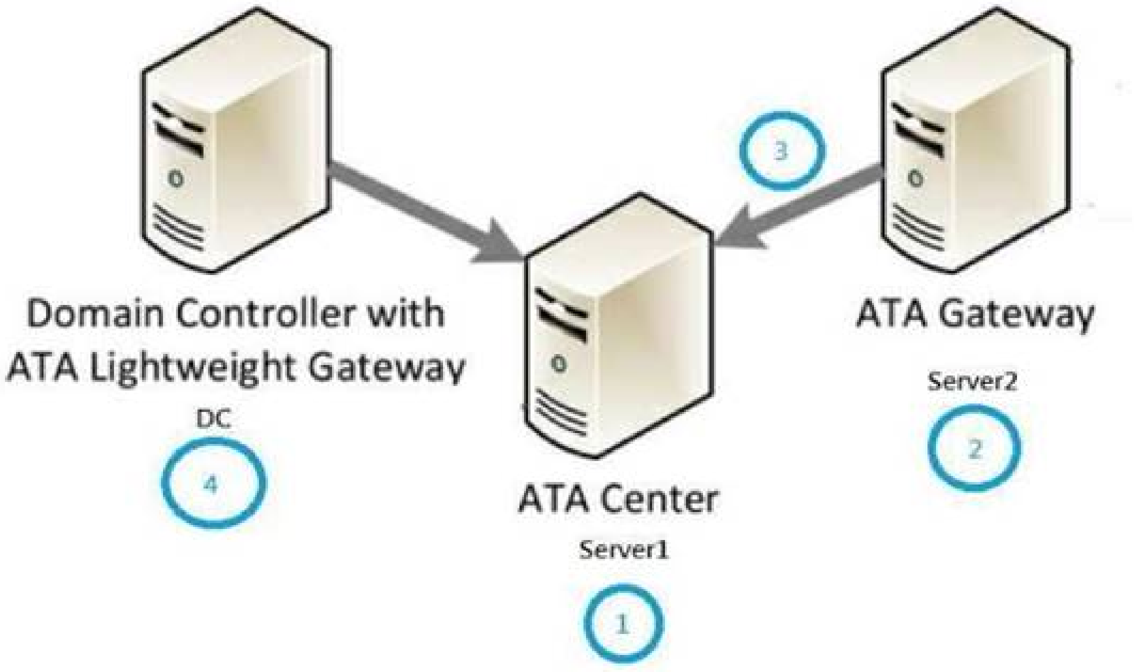


Install the ATA Center.
Install the ATA Gateway.
Install the ATA Lightweight Gateway.
Install Microsoft Message Analyzer.
Configure the ATA Gateway domain connectivity settings.
Set the ATA Gateway configuration settings

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 84
You have a server named Server1 that runs Windows Server 2016.
You need to install Security Compliance Manager (SCM) 4.0 on Server1. What should you install on Server1 first?

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

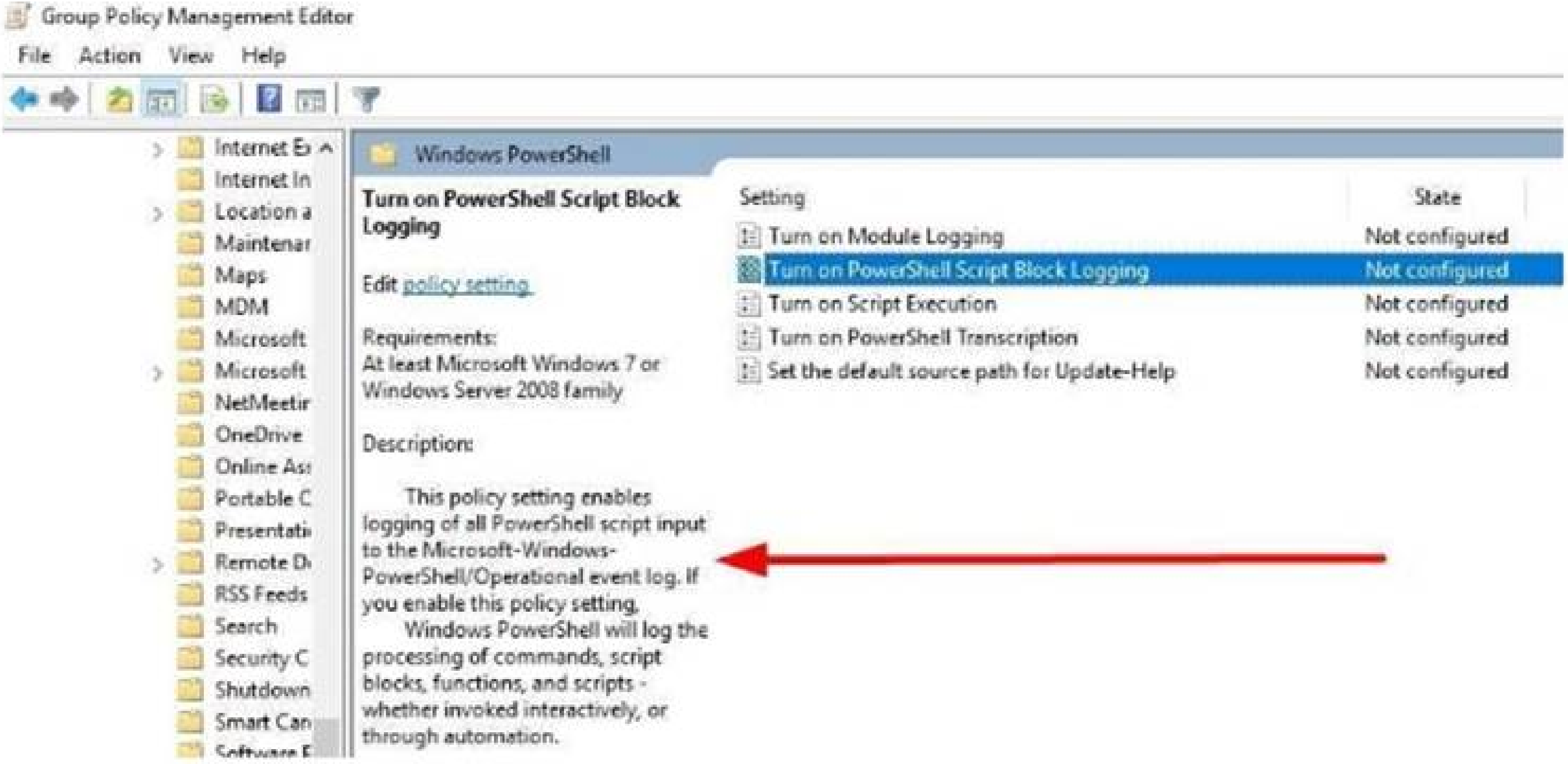
Answer: A

NEW QUESTION 86
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.



Windows PowerShell

Turn on PowerShell Script Block Logging

Edit policy setting

Requirements:
At least Microsoft Windows 7 or Windows Server 2008 family

Description:

This policy setting enables logging of all PowerShell script input to the Microsoft-Windows-PowerShell/Operational event log. If you enable this policy setting, Windows PowerShell will log the processing of commands, script blocks, functions, and scripts - whether invoked interactively, or through automation.

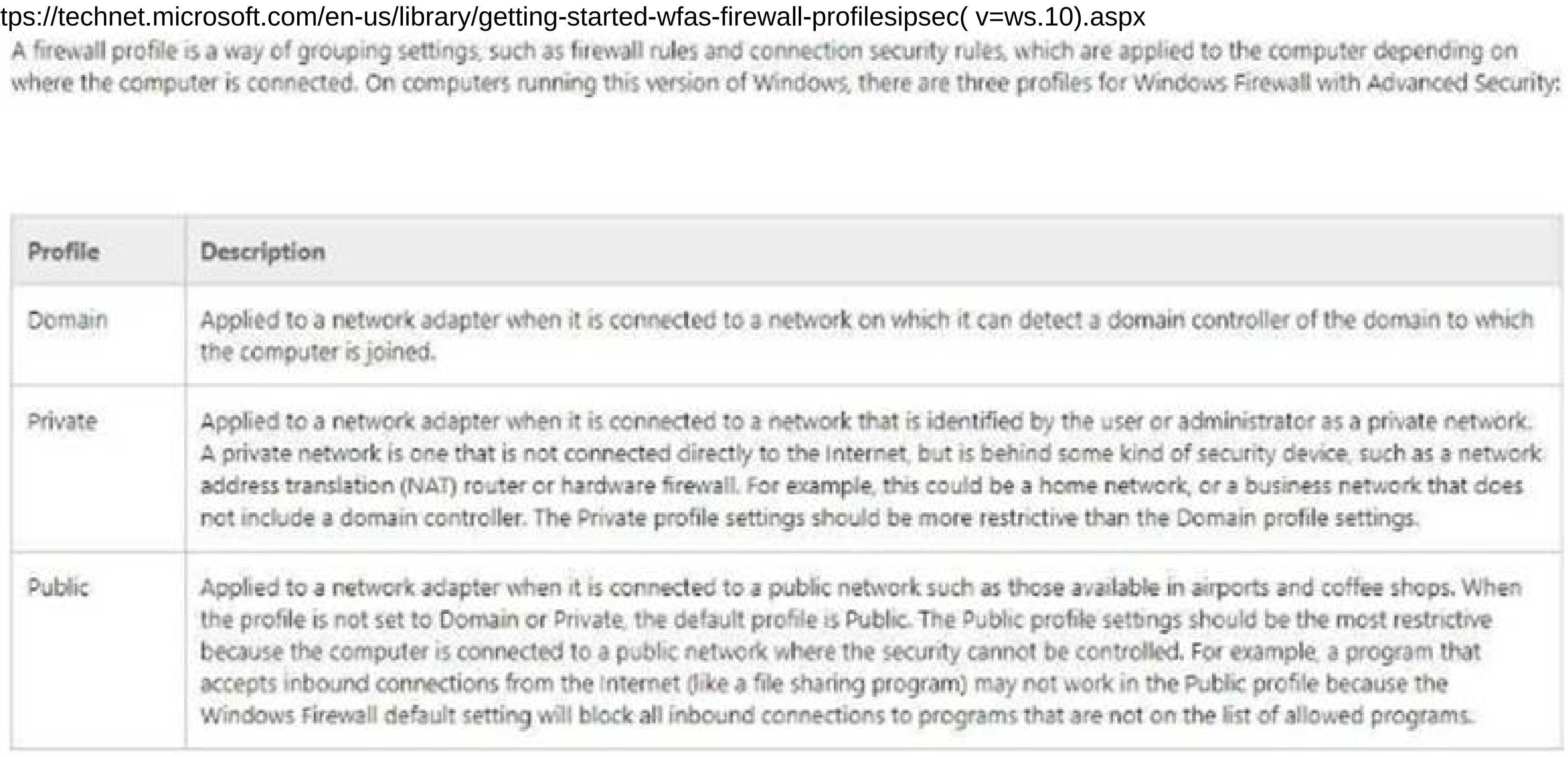
Setting	State
Turn on Module Logging	Not configured
Turn on PowerShell Script Block Logging	Not configured
Turn on Script Execution	Not configured
Turn on PowerShell Transcription	Not configured
Set the default source path for Update-Help	Not configured

NEW QUESTION 89
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. The network uses the 172.16.0.0/16 address space.
Computer1 has an application named App1.exe that is located in D:\\Apps\\. App1.exe is configured to accept connections on TCP port 8080.
You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.
Solution: You configure an inbound rule that allows the TCP protocol on port 8080, uses a scope of 172.16.0.0/16 for local IP addresses, and applies to a private profile.
Does this meet the goal?

A. Yes
B. No

Answer: B

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



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

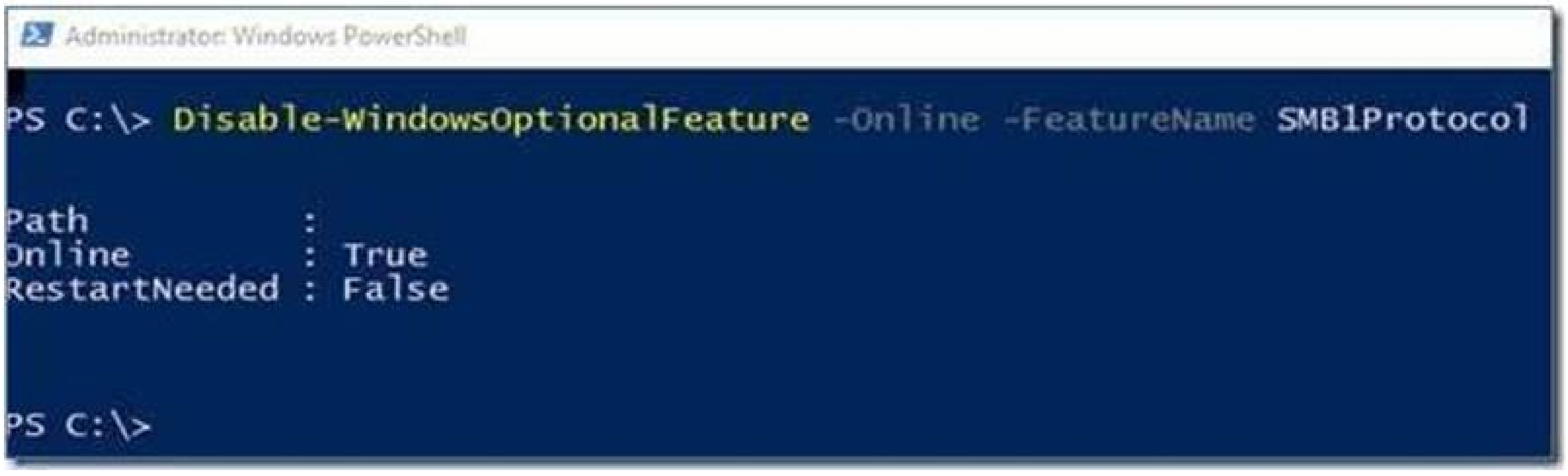
Profile	Description
Domain	Applied to a network adapter when it is connected to a network on which it can detect a domain controller of the domain to which the computer is joined.
Private	Applied to a network adapter when it is connected to a network that is identified by the user or administrator as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

NEW QUESTION 90
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



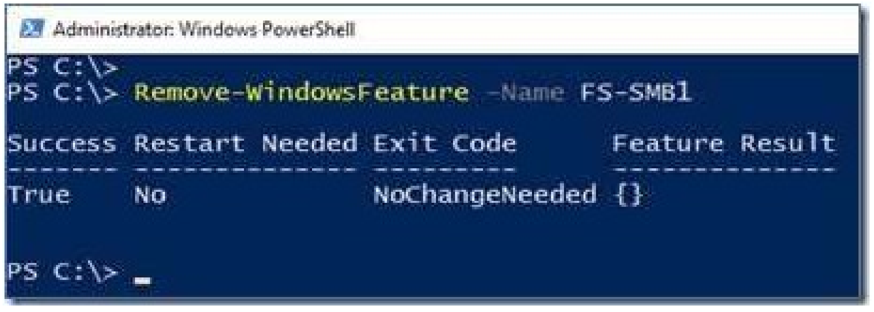
```
PS C:\> Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol


Path          :
Online        : True
RestartNeeded : False



PS C:\>
```

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



```
PS C:\>
PS C:\> Remove-WindowsFeature -Name FS-SMB1

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             NoChangeNeeded {}


PS C:\> _
```

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

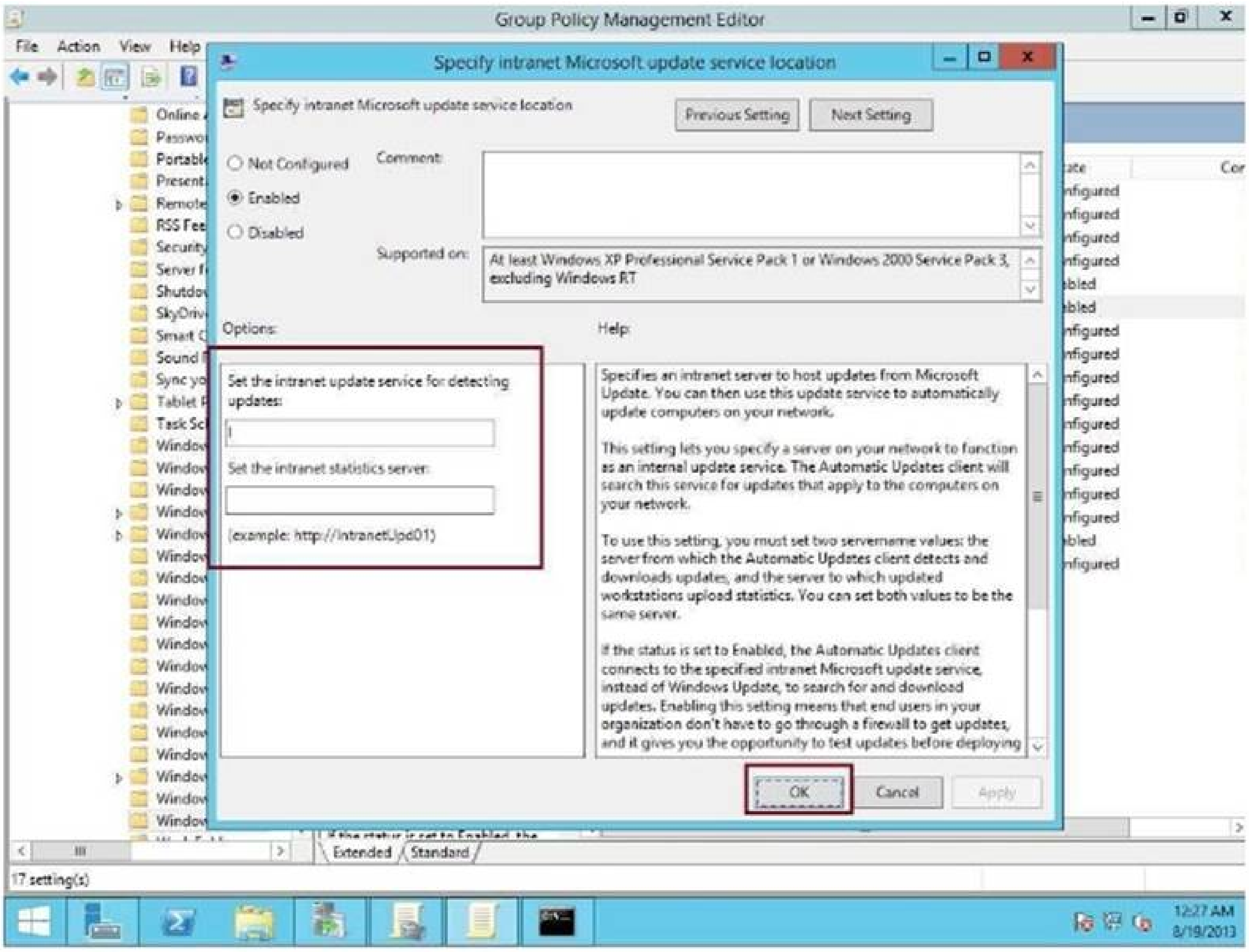
NEW QUESTION 92
Your network contains an Active Directory domain named contoso.com.The domain contains 1,000 client computers that run either Windows 8.1 or Windows 10.
You have a Windows Server Update Services (WSUS) deployment All client computers receive updates from WSUS.
You deploy a new WSUS server 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



Specify intranet Microsoft update service location

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, excluding Windows RT

Options:

Set the intranet update service for detecting updates:

Set the intranet statistics server:

(example: http://IntranetUpd01)

Help:

Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.

This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.

To use this setting, you must set two servername values: the server from which the Automatic Updates client detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server.

If the status is set to Enabled, the Automatic Updates client connects to the specified intranet Microsoft update service, instead of Windows Update, to search for and download updates. Enabling this setting means that end users in your organization don't have to go through a firewall to get updates, and it gives you the opportunity to test updates before deploying

NEW QUESTION 93
Your network contains an Active Directory domain named contoso.com.
The domain contains 10 servers that run Windows Server 2016 and 800 client computers that run Windows 10.
You need to configure the domain to meet the following requirements:
-Users must be locked out from their computer if they enter an incorrect password twice.
-Users must only be able to unlock a locked account by using a one-time password that is sent to their mobile phone.
You deploy all the components of Microsoft Identity Manager (MIM) 2016.
Which three actions should you perform before you deploy the MIM add-ins and extensions? Each correct answer presents part of the solution.

A. From a Group Policy object (GPO), configure Public Key Policies
B. Deploy a Multi-Factor Authentication provider and copy the required certificates to the MIM server.
C. From the MIM Portal, configure the Password Reset AuthN Workflow.
D. Deploy a Multi-Factor Authentication provider and copy the required certificates to the client computers.
E. From a Group Policy object (GPO), configure Security Setting

Answer: BCE

Explanation:
-Users must be locked out from their computer if they enter an incorrect password twice. (E)
-Users must only be able to unlock a locked account by using a one-time password that is sent to their mobile phone. (B and C), detailed configuration process in the following web page.
https://docs.microsoft.com/en-us/microsoft-identity-manager/working-with-self-servicepasswordreset# prepare-mim-to-work-with-multi-factor-authentication

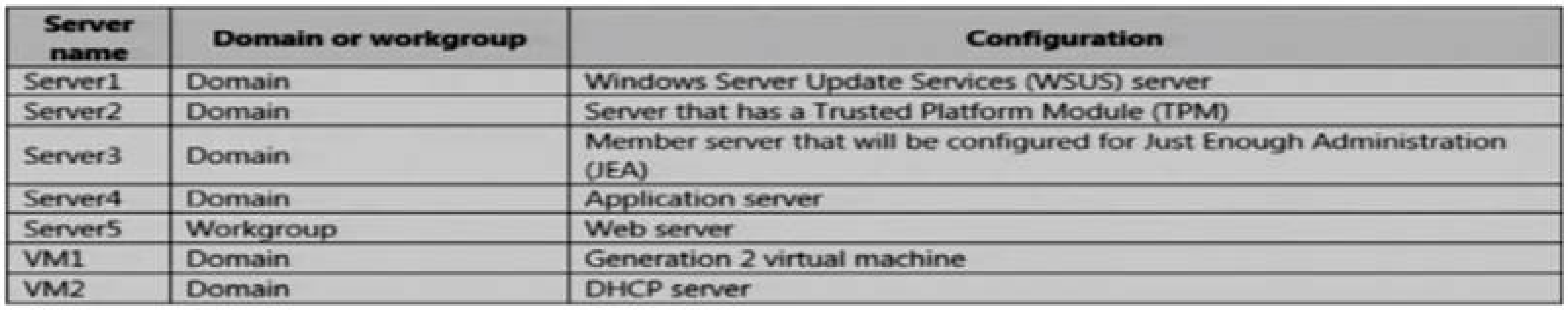
NEW QUESTION 94
Your network contains an Active Directory domain named contoso.com. The domain contains 100 servers.
You deploy the Local Administrator Password Solution (LAPS) to the network.
You discover that the members of a group named FinanceAdministrators can view the password of the local Administrator 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 95
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 96
You are building a guarded fabric. You need to configure Admin-trusted attestation. Which cmdlet should you use?

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

Answer: A

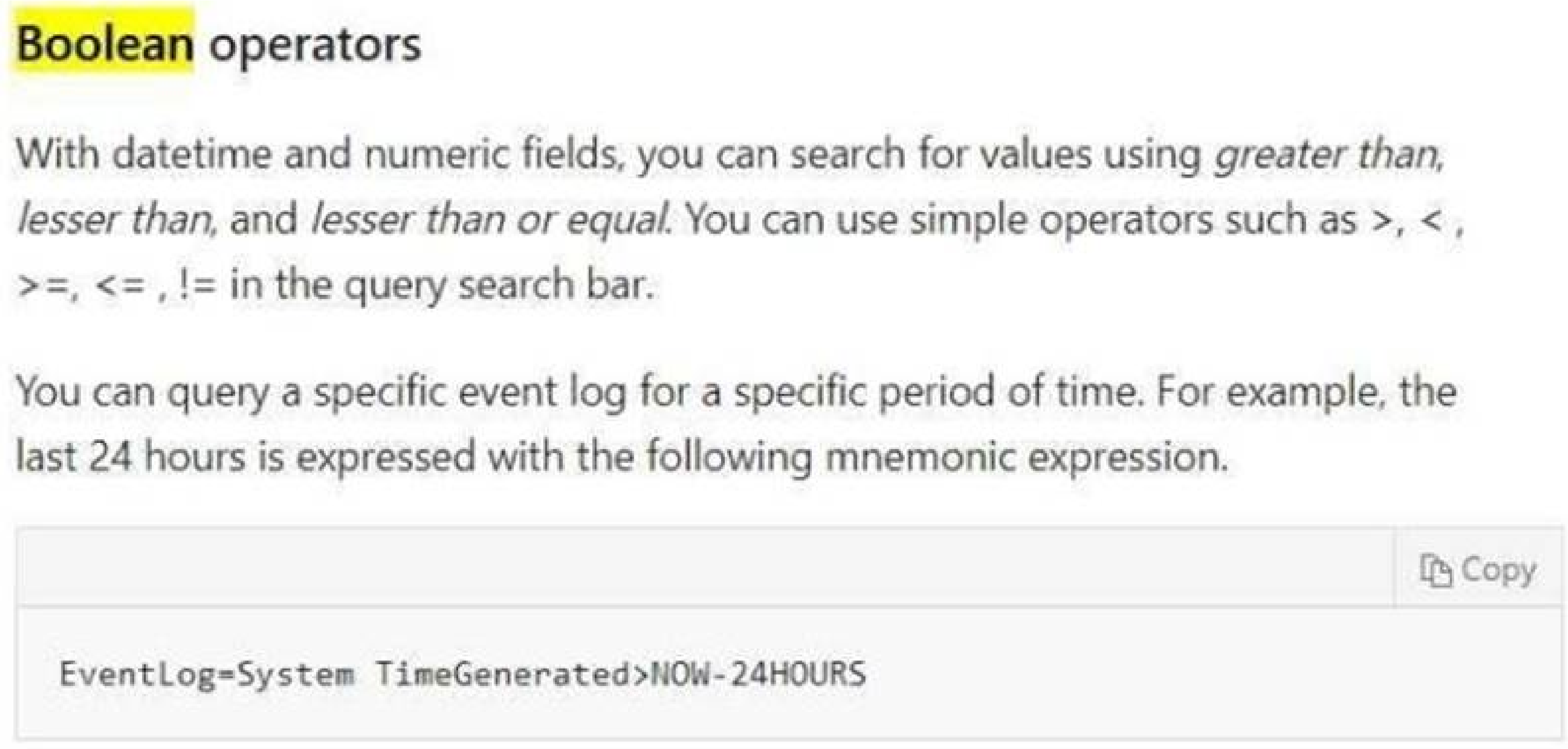
Explanation:
Authorize Hyper-V hosts using Admin-trusted attestation
https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shieldedvm/ guarded-fabric-addhost-information-for-admin-trusted-attestation

NEW QUESTION 100
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.

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

NEW QUESTION 103
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”

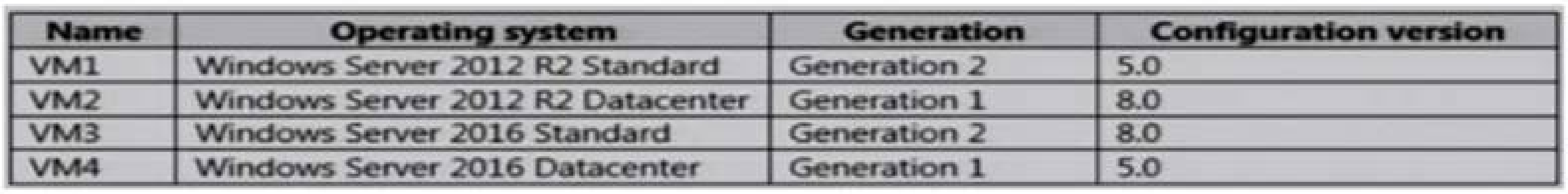
NEW QUESTION 105
Your network contains several secured subnets that are disconnected from the Internet.
One of the secured subnets contains a server named Server1 that runs Windows Server 2016.
You implement Log Analytics in Microsoft Operations Management Suite (OMS) for the servers that connect to 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 110
You have a Hyper-V host named Server1 that runs Windows Server 2016. Server1 hosts the virtual machines configured as shown in the following table.



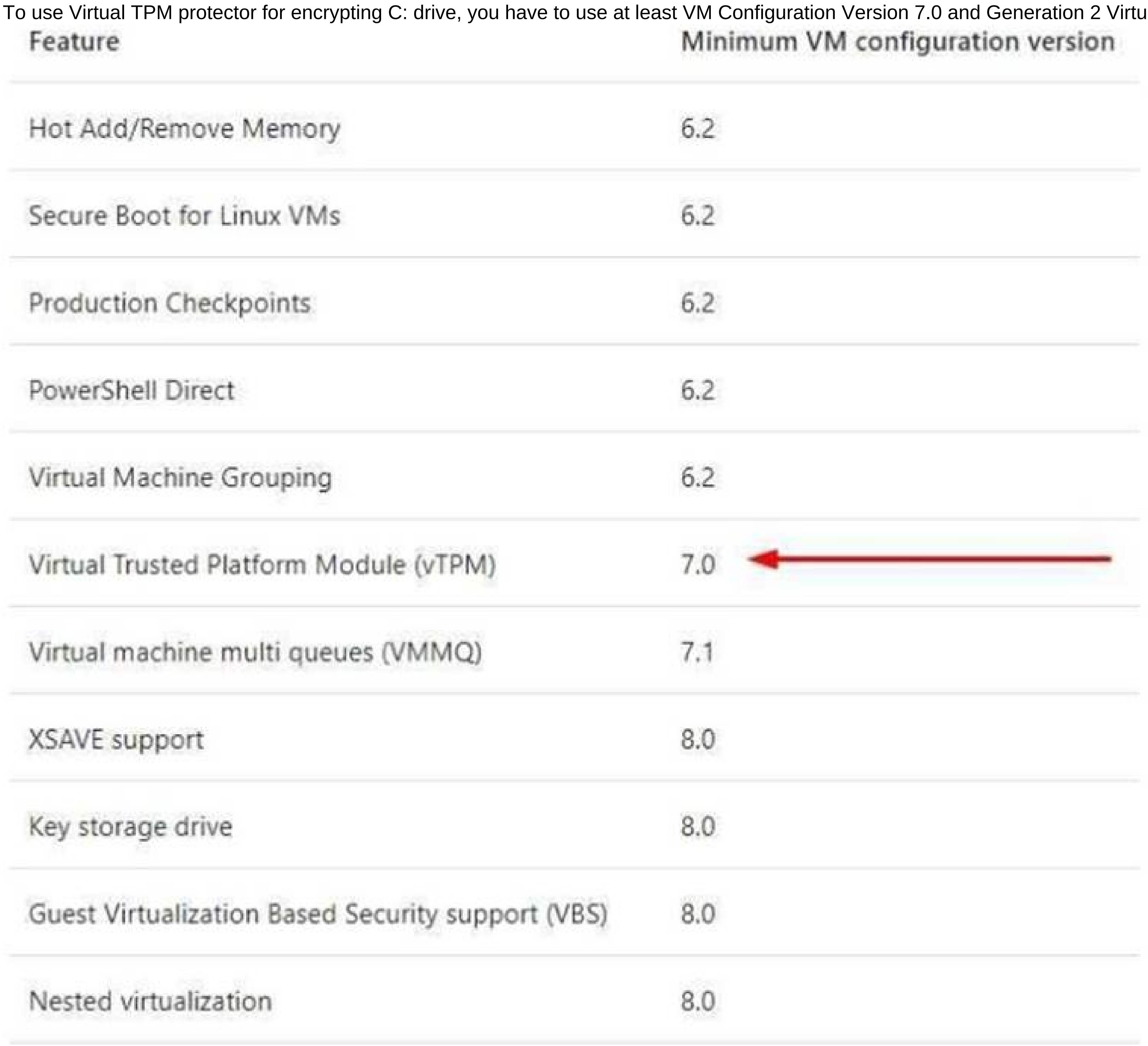
Name	Operating system	Generation	Configuration version
VM1	Windows Server 2012 R2 Standard	Generation 2	5.0
VM2	Windows Server 2012 R2 Datacenter	Generation 1	8.0
VM3	Windows Server 2016 Standard	Generation 2	8.0
VM4	Windows Server 2016 Datacenter	Generation 1	5.0

All the virtual machines have two volumes named C and D.
You plan to implement BitLocker Drive Encryption (BitLocker) on the virtual machines. Which virtual machines can have their volumes protected by using BitLocker? Choose Two.

A. Virtual machines that can have volume C protected by using BitLocker and a Trusted Platform Module (TPM) protector: VM3 only
B. Virtual machines that can have volume C protected by using BitLocker and a Trusted Platform Module (TPM) protector: VM1 and VM3 only
C. Virtual machines that can have volume C protected by using BitLocker and a Trusted Platform Module (TPM) protector: VM2 and VM3 only
D. Virtual machines that can have volume C protected by using BitLocker and a Trusted Platform Module (TPM) protector: VM2 and VM4 only
E. Virtual machines that can have volume C protected by using BitLocker and a Trusted Platform Module (TPM) protector: VM2, VM3 and VM4 only
F. Virtual machines that can have volume C protected by using BitLocker and a Trusted Platform Module (TPM) protector: VM1, VM2, VM3 and VM4
G. Virtual machines that can have volume D protected by using BitLocker: VM3 only
H. Virtual machines that can have volume D protected by using BitLocker: VM1 and VM3 only
I. Virtual machines that can have volume D protected by using BitLocker: VM2 and VM3 only
J. Virtual machines that can have volume D protected by using BitLocker: VM2 and VM4 only
K. Virtual machines that can have volume D protected by using BitLocker: VM2, VM3 and VM4 only
L. Virtual machines that can have volume D protected by using BitLocker: VM1, VM2, VM3 and VM4

Answer: AG

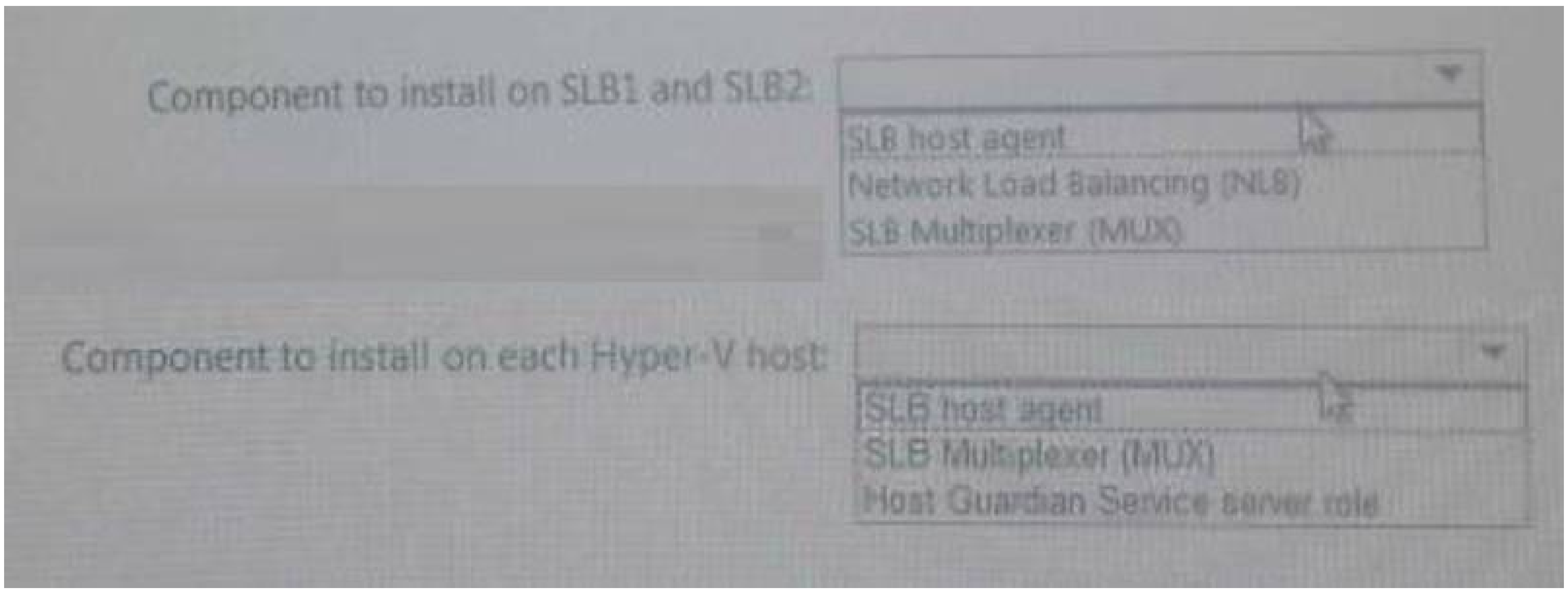
Explanation:
https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/deploy/upgrade-virtualmachine- versionin-hyper-v-on-windows-or-windows-server
To use Virtual TPM protector for encrypting C: drive, you have to use at least VM Configuration Version 7.0 and Generation 2 Virtual machines.



Feature	Minimum VM configuration version
Hot Add/Remove Memory	6.2
Secure Boot for Linux VMs	6.2
Production Checkpoints	6.2
PowerShell Direct	6.2
Virtual Machine Grouping	6.2
Virtual Trusted Platform Module (vTPM)	7.0
Virtual machine multi queues (VMMQ)	7.1
XSAVE support	8.0
Key storage drive	8.0
Guest Virtualization Based Security support (VBS)	8.0
Nested virtualization	8.0

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.

NEW QUESTION 112
HOTSPOT
You have 10 Hyper-V hosts that run Windows Server 2016.
Each Hyper-V host has eight virtual machines that run a distributed web application named App1. You plan to implement a Software Load Balancing (SLB) solution for client access to App1. You deploy two new virtual machines named SLB1 and SLB2.
You need to install the required components on the Hyper-V hosts and the new servers for the planned implementation.
Which components should you install? Select the Appropriate in selection area.



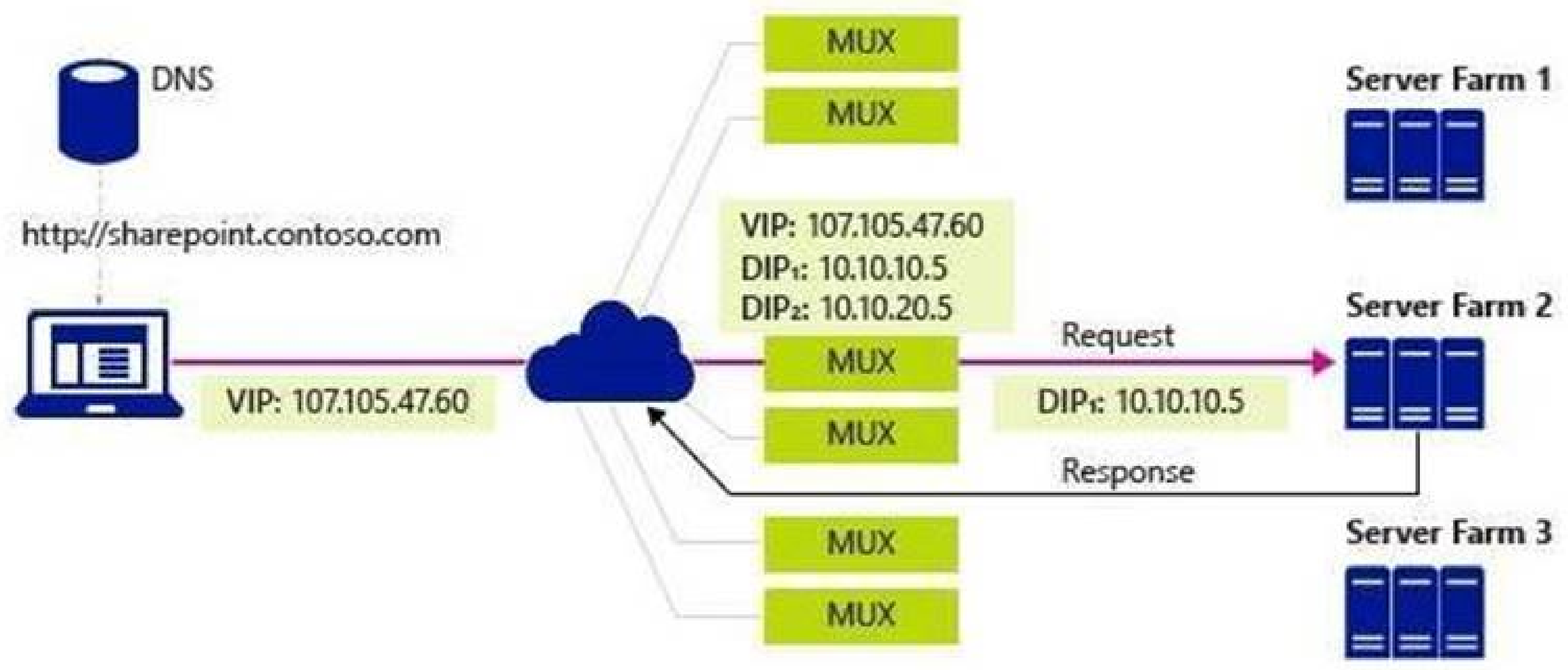
Component to install on SLB1 and SLB2:

Component to install on each Hyper-V host:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://blogs.technet.microsoft.com/tip_of_the_day/2016/06/28/tip-of-the-day-demystifyingsoftware- definednetworking-terms-the-components/
https://technet.microsoft.com/en-us/library/mt632286.aspx
SLB Host Agent – When you deploy SLB, you must use System Center, Windows PowerShell, or another management application to deploy the SLB Host Agent on every Hyper-V host computer.
You can install the SLB Host Agent on all versions of Windows Server 2016 that provide Hyper-V support, including Nano Server.
SLB MUX – Part of the Software Load Balancer (SLB on Windows Server 2016, the SLB MUX processes inbound network traffic and maps VIPs (virtual IPs) to DIPs (datacenter IPs), then forwards the traffic to the correct DIP. Each MUX also uses BGP to publish VIP routes to edge routers. BGP Keep Alive notifies MUXes when a MUX fails, which allows active MUXes to redistribute the load in case of a MUX failure – essentially providing load balancing for the load balancers.



NEW QUESTION 114
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 117
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 121
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.
You need to allow network administrators to use Just Enough Administration (JEA) to change the
TCP/IP settings on Server1. The solution must use the principle of least privilege. How should you configure the session configuration file?

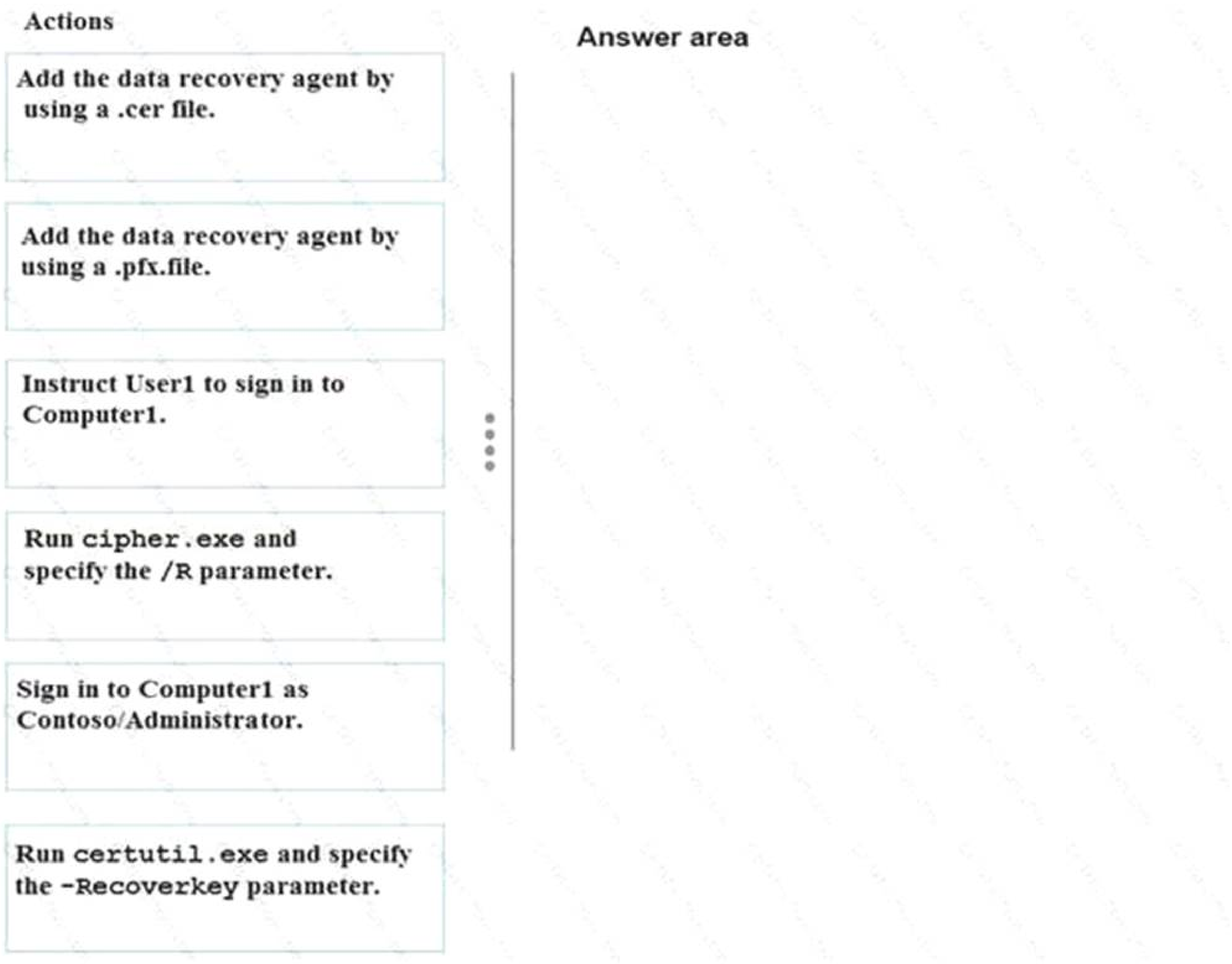
A. Set RunAsVirtualAccount to $false and set RunAsVirtualAccountGroups to Contoso\Network Configuration Operators.
B. Set RunAsVirtualAccount to $true and set RunAsVirtualAccountGroups to Contoso\Network Configuration Operators.
C. Set RunAsVirtualAccount to $false and set RunAsVirtualAccountGroups to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

Answer: D

Explanation:

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

NEW QUESTION 122
DRAG DROP
Your network contains an Active Directory domain named contoso.com. The domain contains a user named User1 and a computer named Computer1. Remote Server Administration Tools (RSAT) is installed on Computer1.
You need to add User1 as a data recovery agent in the domain.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

Add the data recovery agent by using a .cer file.

Add the data recovery agent by using a .pfx.file.

Instruct User1 to sign in to Computer1.

Run cipher.exe and specify the /R parameter.

Sign in to Computer1 as Contoso/Administrator.

Run certutil.exe and specify the -Recoverkey parameter.

Answer area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 123
......