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#W client computers that run Windows 10. All client computers are deployed (rom a customized Windows image.
You need to deploy 10 Privileged Access Workstations (PAWs). The solution must ensure that administrators can access several client applications used by all users.
Solution: You deploy 10 physical computers and configure each will as a virtualization host. You deploy the operating system on each host by using the customized Windows image. On each host you create a guest virtual machine and configure the virtual machine as a PAW.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 2
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. All servers run Windows
Server 2016. All client computers run Windows 10.
The relevant objects in the domain are configured as shown in the following table.

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

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

A. Yes
B. No

Answer: A

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

NEW QUESTION 3
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 4
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 5
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 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

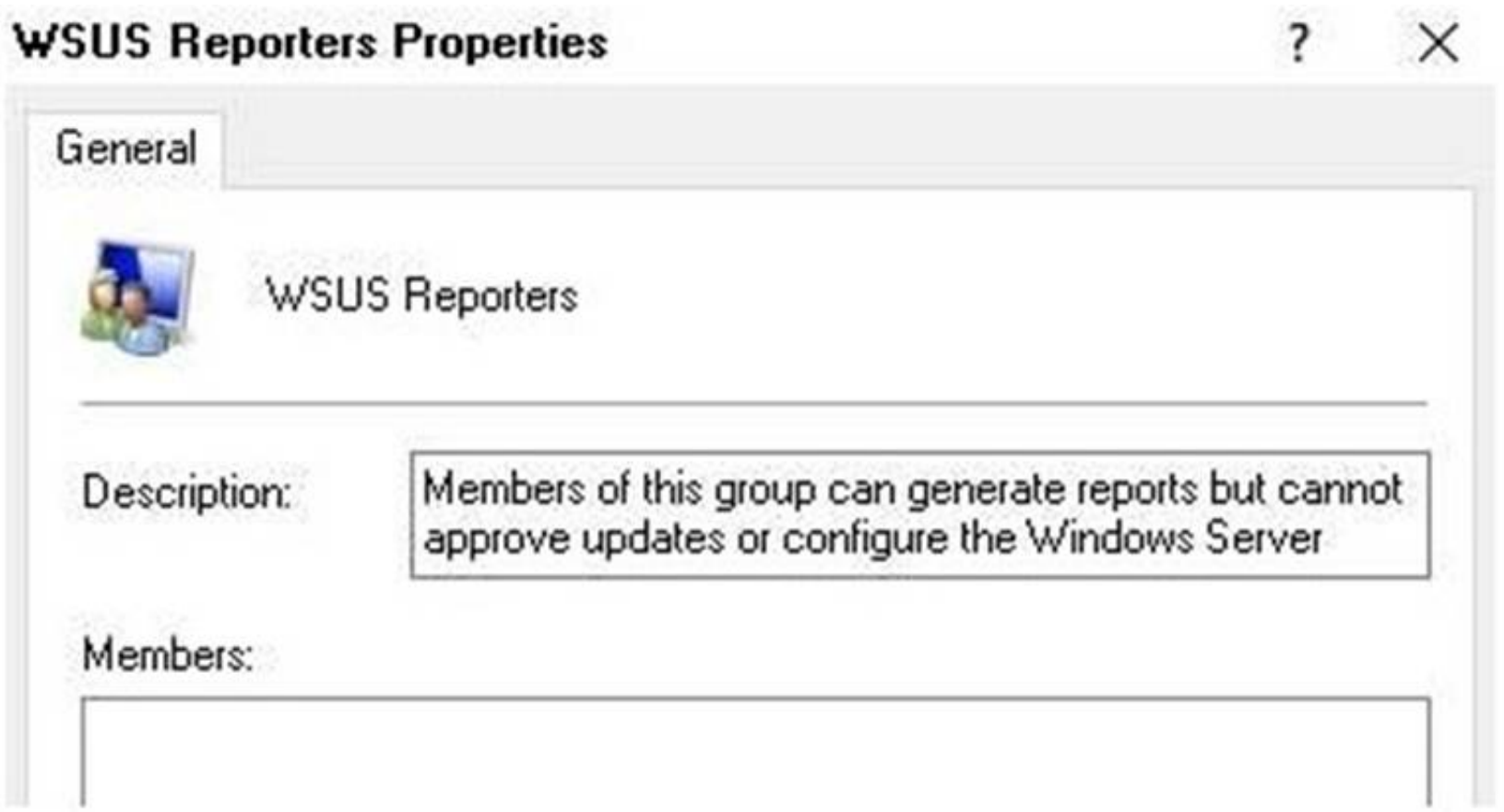
- **Workstation Hardening** - Build the administrative workstations using the Privileged Access Workstations (through Phase 3), but change the domain membership to the administrative forest instead of the production environment.

NEW QUESTION 7
Your network contains an Active Directory domain named contoso.com.
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?

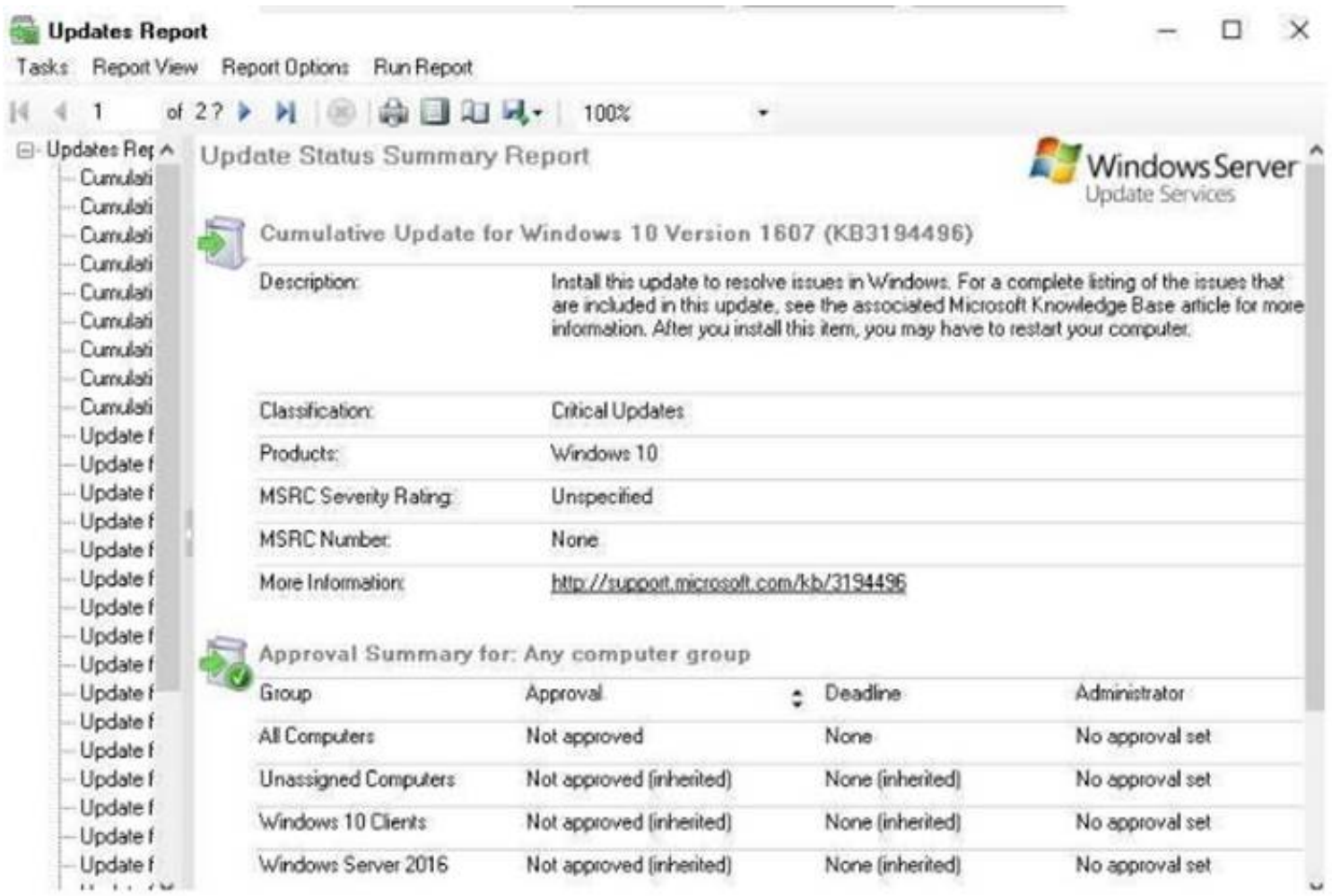
A. Modify the permissions of the ReportWebService virtual folder from the WSUS Administration website.
B. Add User1 to the WSUS Reporters local group.
C. Add User1 to the WSUS Administrators local group.
D. Run wsusutil.exe and specify the postinstall paramete

Answer: B

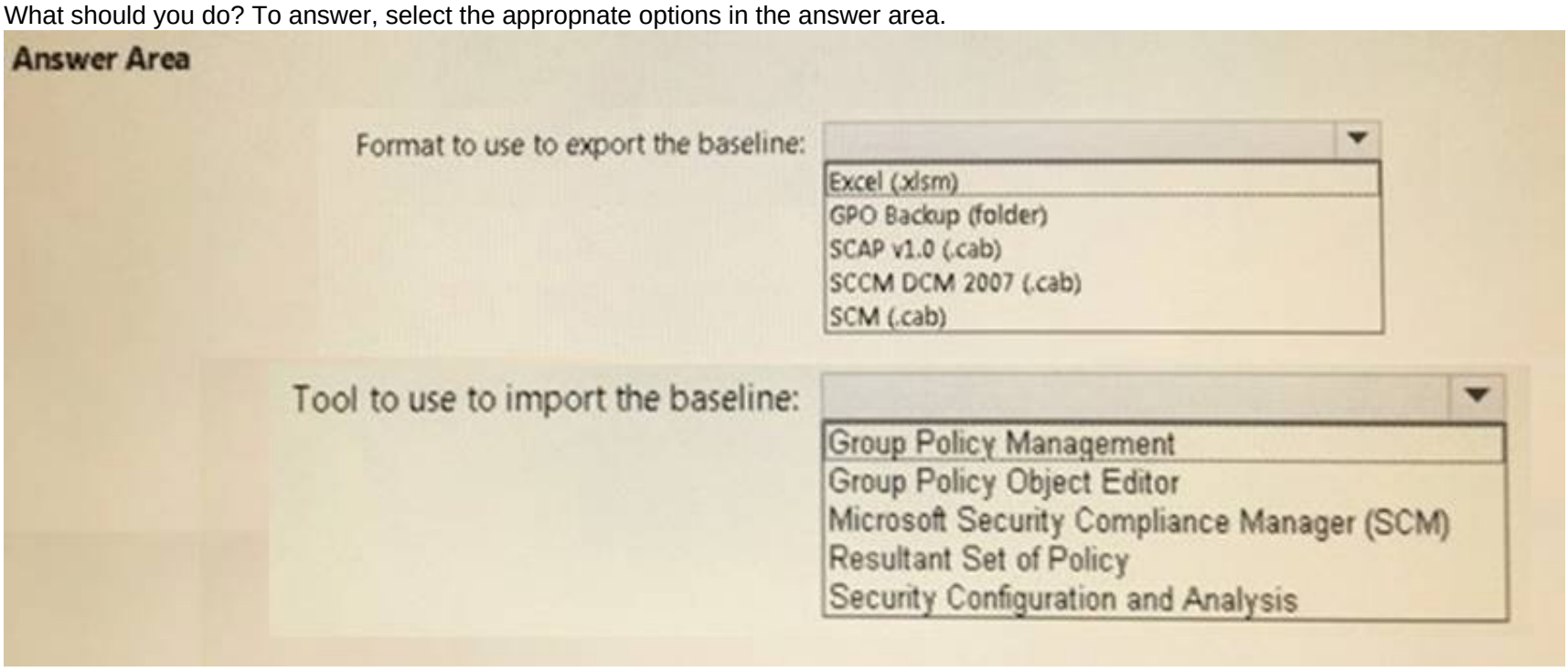
Explanation:
WSUS Reporters have read only access to the WSUS database and configuration



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



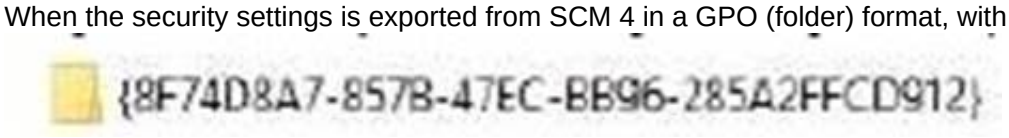
NEW QUESTION 8
HOTSPOT
Your network contains an Active Directory domain named contoso.com. You have an organizational unit (OU) named Secure that contains all servers.
You install Microsoft Security Compliance Manager (SCM) 4.0 on a server named Server1. You need to export the SCM Pnnt Server Secunty 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.



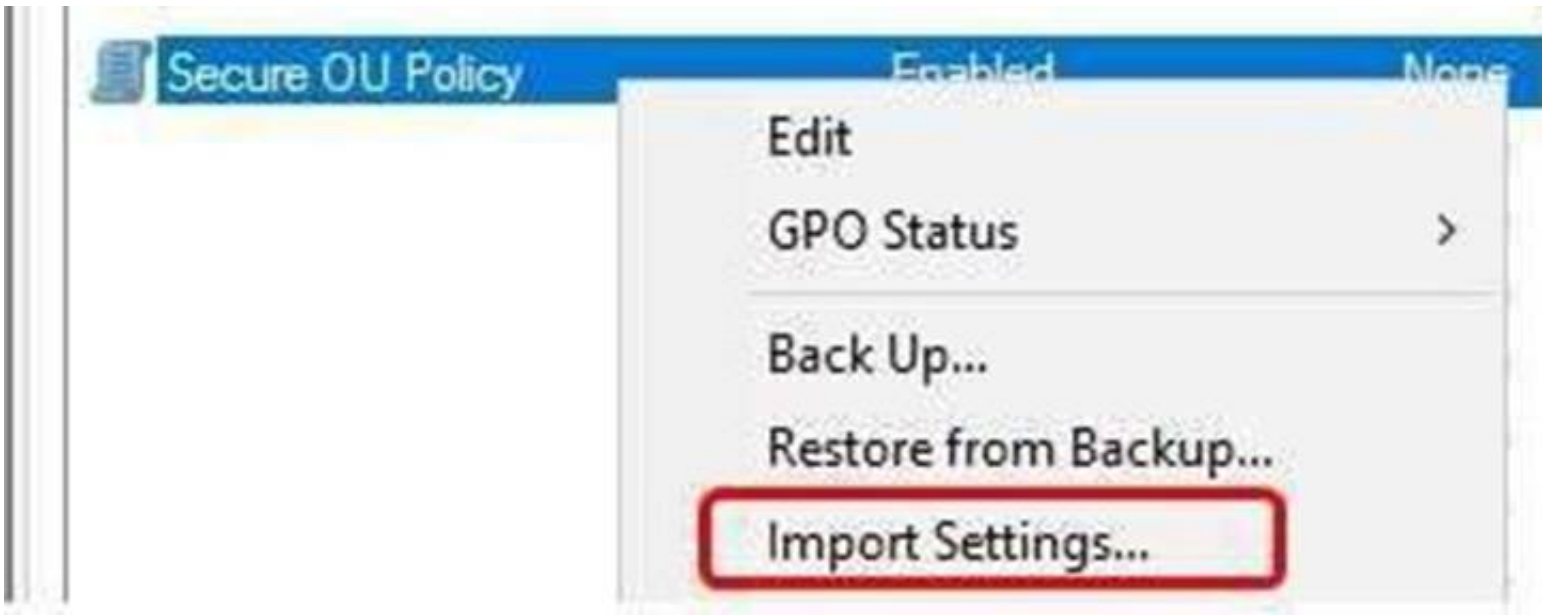
A. Mastered
B. Not Mastered

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 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

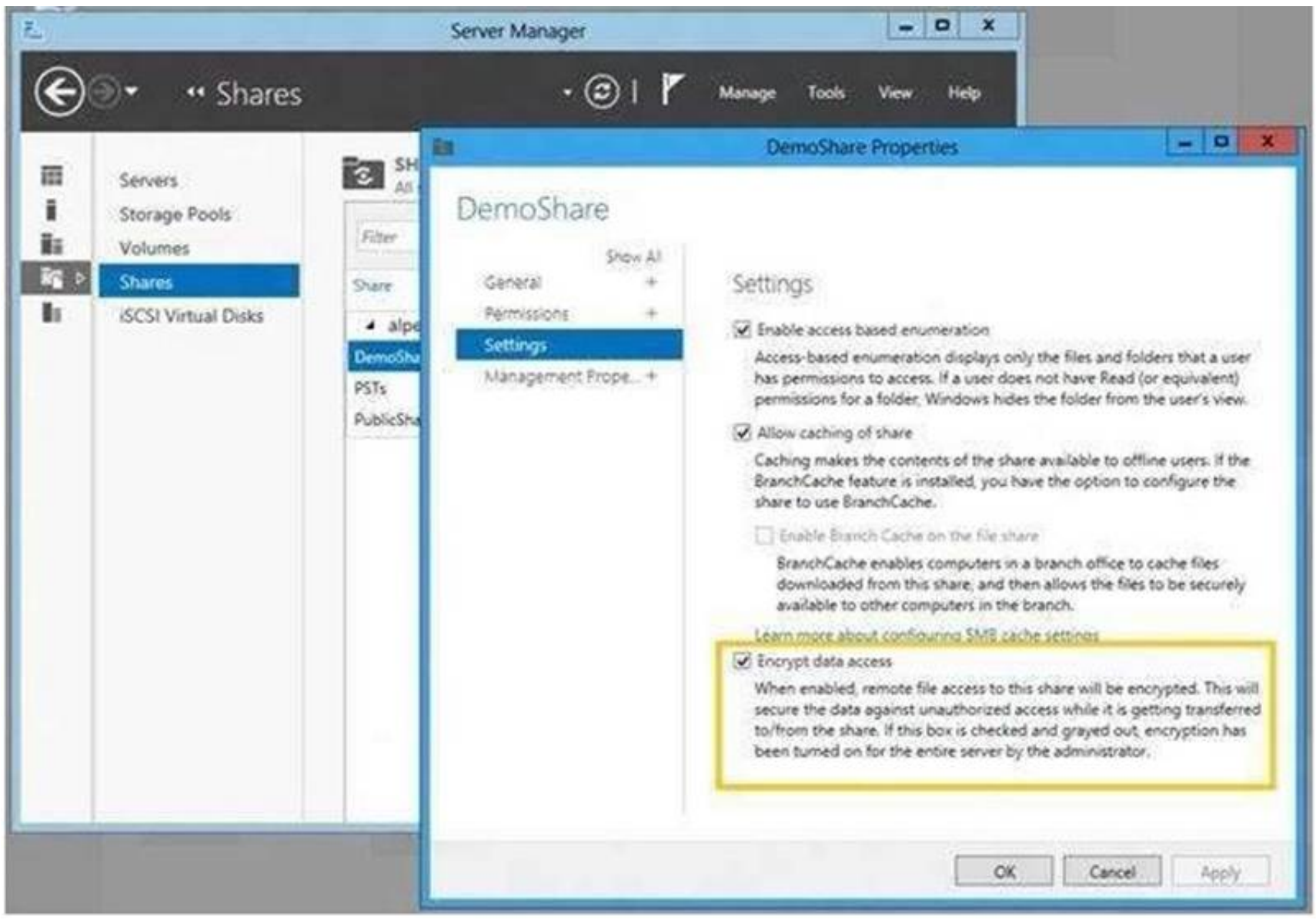
Answer: AB

NEW QUESTION 10
Note: This question b part of a series of questions that use the same or simitar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.
Your network contains an Active Directory domain named contoso.com The domain contains a server named Server1 that runs Windows Server 2016.
Server1 has a shared folder named Share1.
You need to ensure that all access to Share1 uses SMB Encryption. Which tool should you use?

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

Answer: C

Explanation:
https://blogs.technet.microsoft.com/filecab/2012/05/03/smb-3-security-enhancements-inwindows- server-2012/



NEW QUESTION 10
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario b repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.
Start of repeated scenario
Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.
The domain contains the servers configured as shown m the following table.

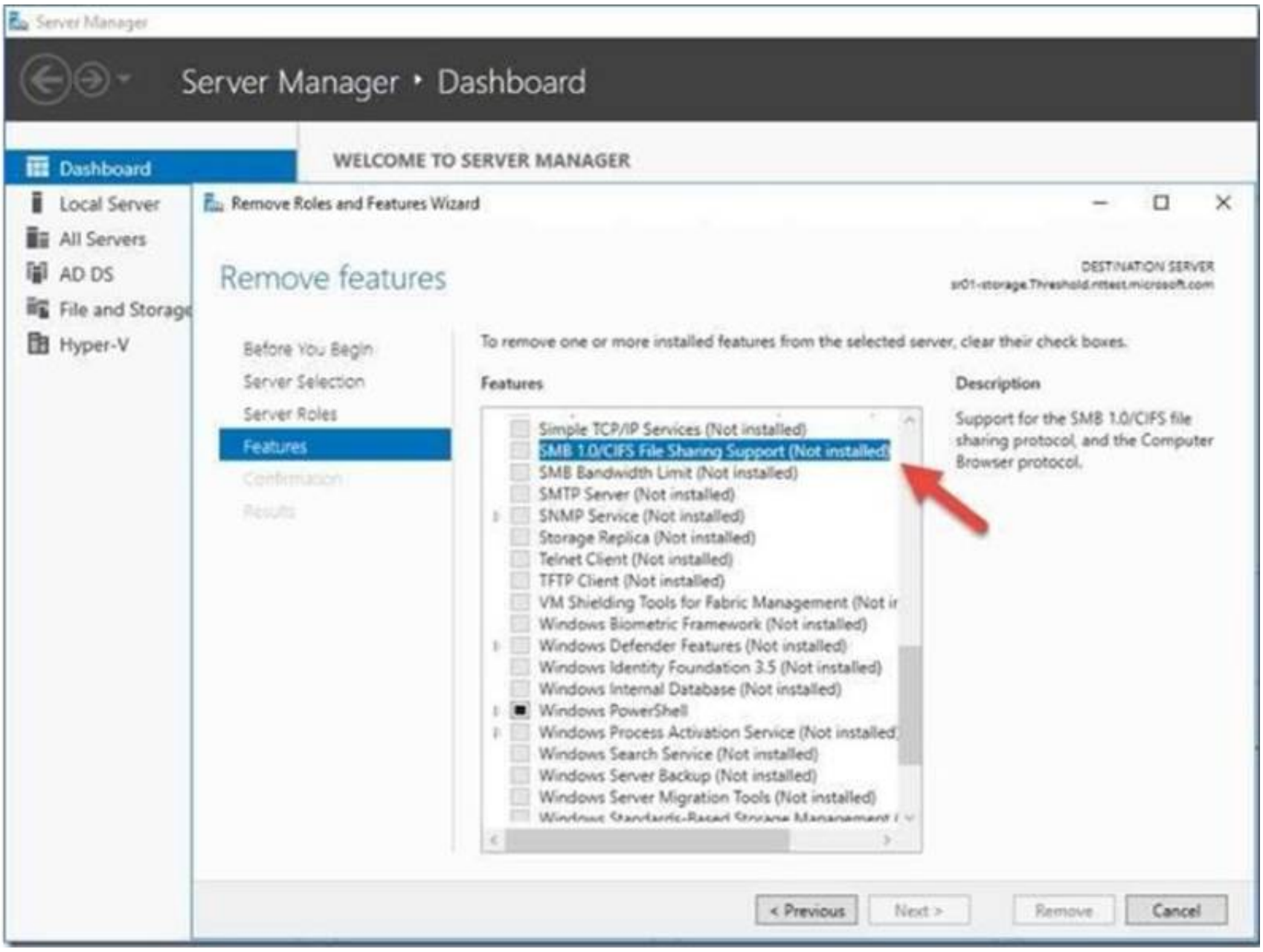
Server name	Configuration
Nano1	Nano Server
Nano2	Nano Server
Server2	File server that has a shared folder named DATA
Server3	DNS server that has a DNSSEC-signed zone named adatum.com
Server4	Hyper-V host
Server1	Application server

All servers run Windows Server 2016. All client computers run Windows 10.
You have an organizational unit (OU) named Marketing that contains the computers in the marketing department You have an OU named Finance that contains the computers in the finance department You have an OU named AppServers that contains application servers. A Group Policy object (GPO) named GP1 is linked to the Marketing OU. A GPO named GP2 is linked to the AppServers OU. You install Windows Defender on Nano1.
End of repeated scenario
You need to disable SMB 1.0 on Server2. What should you do?

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

Answer: D

Explanation:
https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-andsmbv3- inwindows-and-windows



NEW QUESTION 14
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

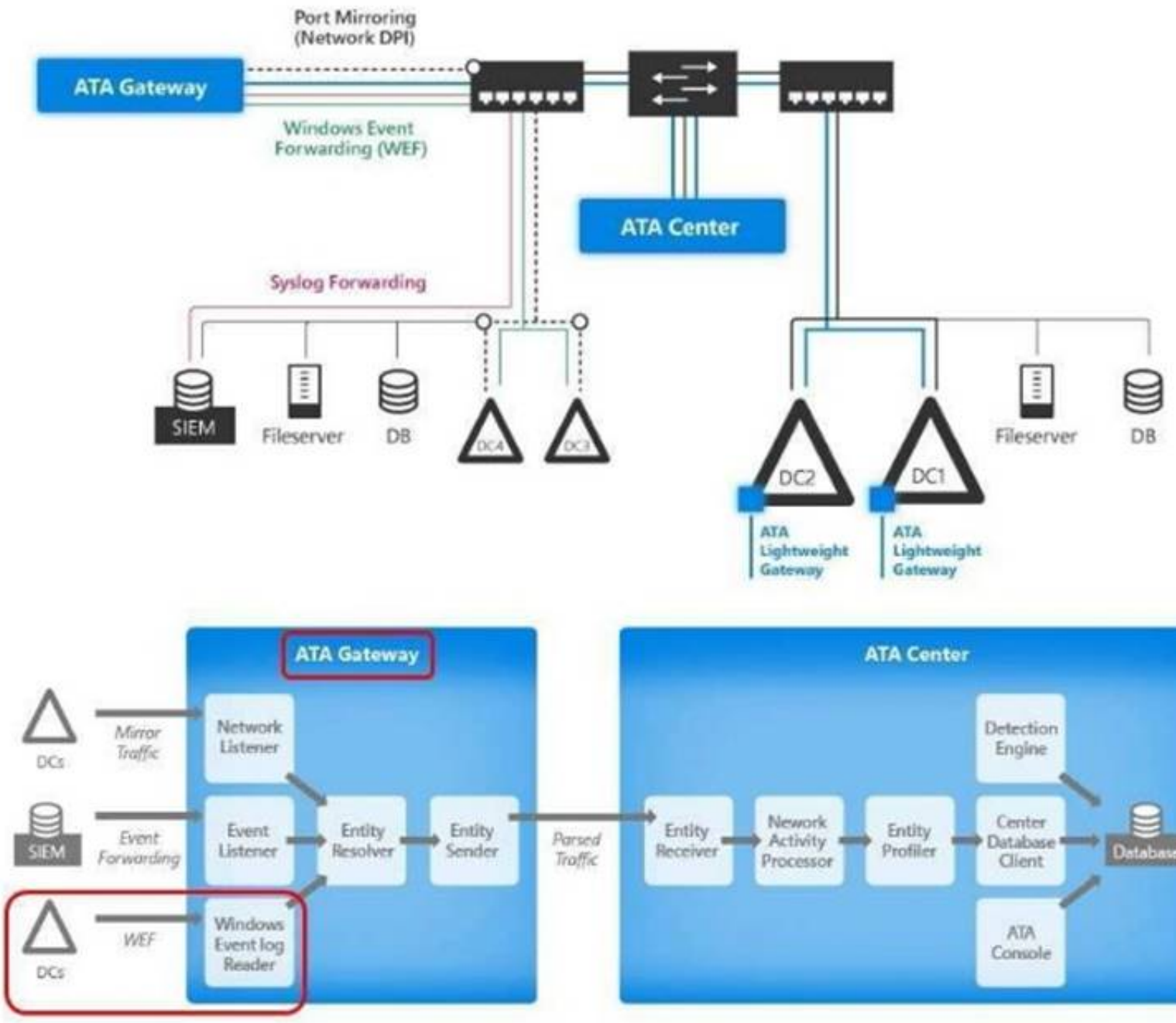
Explanation:
https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-prerequisites
ATA Center which is the first component to be deployed on Server1, requires the use of SSL protocol to
communicate with ATA Gateway
To ease the installation of ATA, you can install self-signed certificates during 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 16
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?

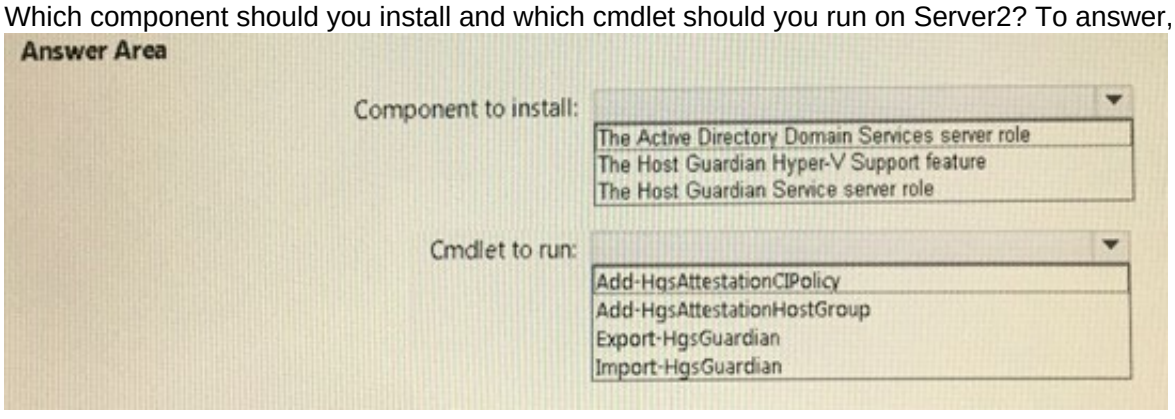
A. the domain controllers to forward Event ID 4776 to Server2
B. the domain controllers to forward Event ID 1000 to Server1
C. Server2 to forward Event ID 1026 to Server1
D. Server1 to forward Event ID 1000 to Server2

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 19
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 23
Read the following statement carefully and answer YES or NO.
You create a rule “Allow Everyone to run Windows except Registry Editor” that allows everyone in the organization to run Windows but does not allow anyone to run Registry Editor.
The effect of this rule would prevent users such as help desk personnel from running a program that is necessary for their support tasks.
To resolve this problem, you create a second rule that applies to the Helpdesk user group: “Allow Helpdesk to run Registry Editor.”
However, if you created a deny rule that did not allow any users to run Registry Editor, would the deny rule override the second rule that allows the Helpdesk user group to run Registry Editor?

A. NO
B. YES

Answer: B

NEW QUESTION 26
____ enables easier management for BitLocker enabled desktops and servers in a domain environment by providing automatic unlock of operating system volumes at system reboot when connected to a wired corporate network. This feature requires the client hardware to have a DHCP driver implemented in its UEFI firmware.

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

Answer: A

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

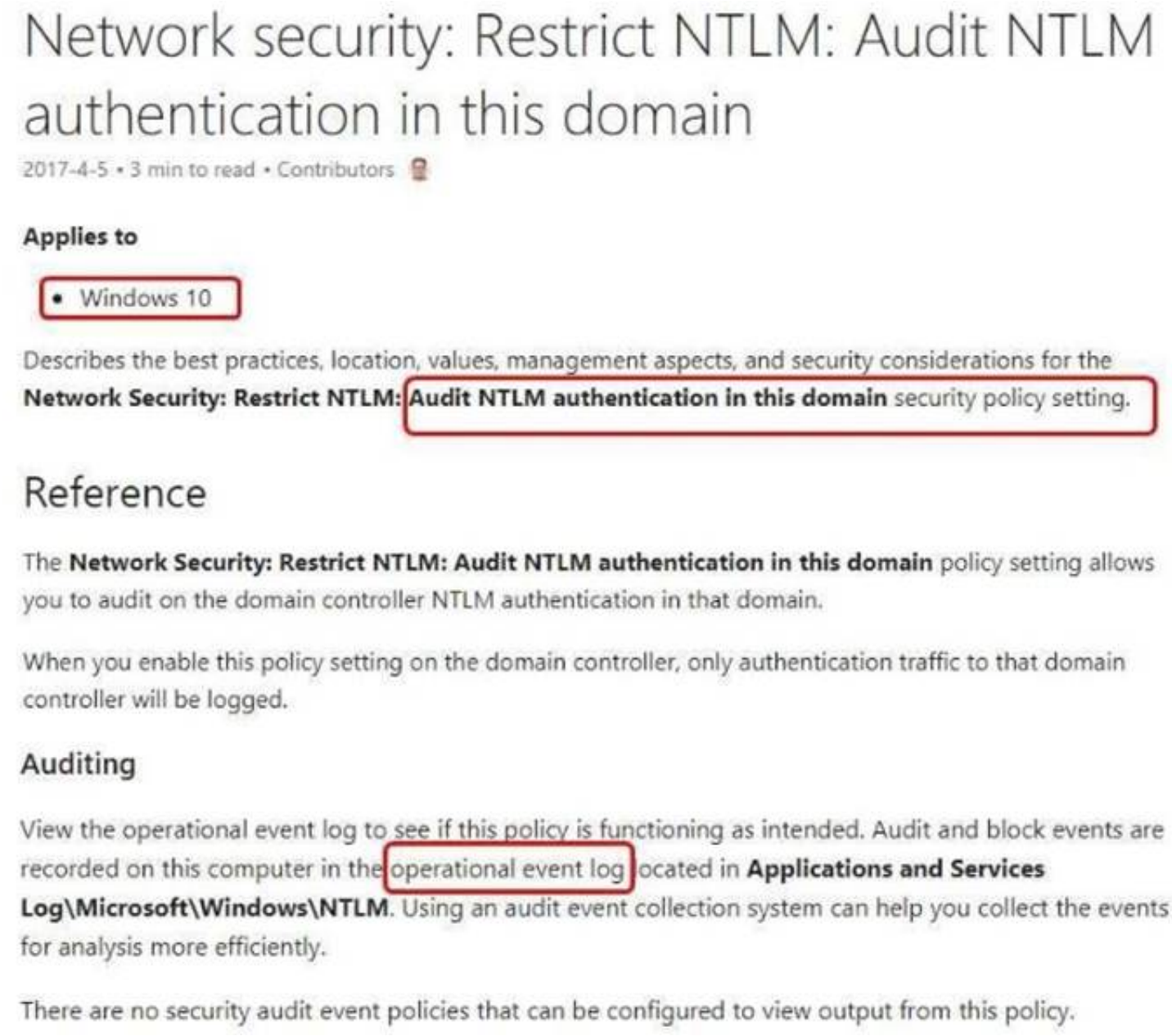
NEW QUESTION 28
Your network contains an Active Directory domain named contoso.com. The domain contains multiple servers that run multiple applications.

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.

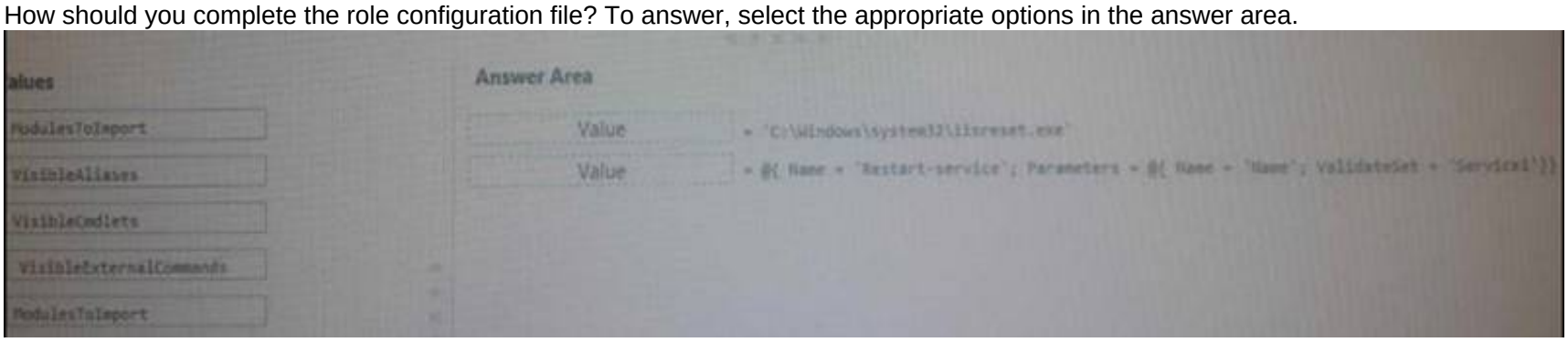
When you enable this policy setting on the domain controller, only authentication traffic to that domain controller will be logged.

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.

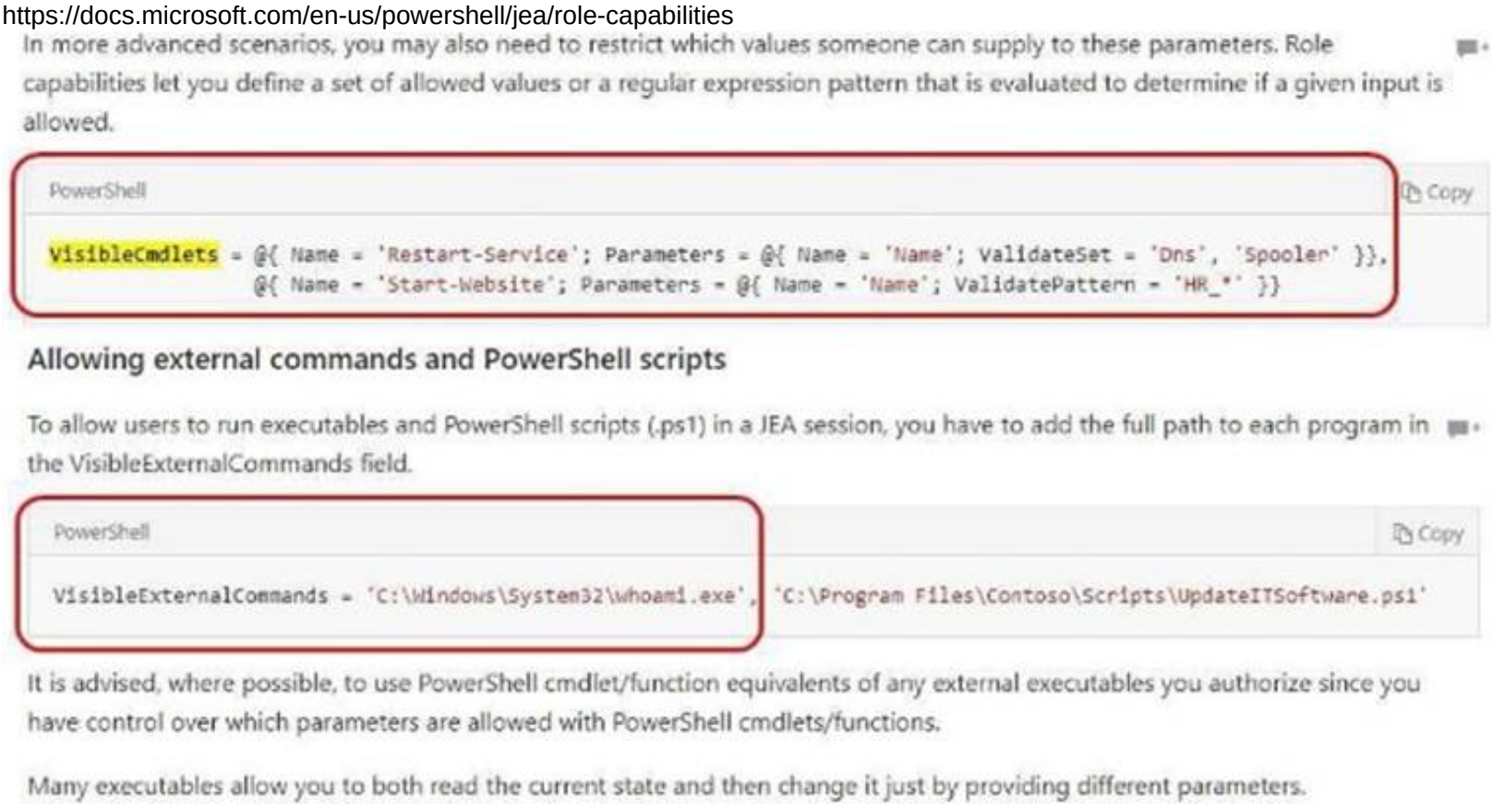
NEW QUESTION 31
DRAG DROP
You configure Just Enough Administration (JEA).
You need to ensure that a non-administrator user can perform the following actions:
-Restart Internet Information Services (IIS)
-Restart a custom service named Service1.
How should you complete the role configuration file? To answer, select the appropriate options in the answer area.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
VisibleExternalCommands = 'C:\\Windows\\system32\\iisreset.exe'
VisibleCmdlets = @{ Name 'Restart-service' ; Parameters @{ Name = 'Name'; ValidateSet = 'Service1'}}
https://docs.microsoft.com/en-us/powershell/jea/role-capabilities


In more advanced scenarios, you may also need to restrict which values someone can supply to these parameters. Role capabilities let you define a set of allowed values or a regular expression pattern that is evaluated to determine if a given input is allowed.

```
PowerShell                                                                    Copy

VisibleCmdlets = @{ Name = 'Restart-Service'; Parameters = @{ Name = 'Name'; ValidateSet = 'Dns', 'Spooler' }},
                 @{ Name = 'Start-Website'; Parameters = @{ Name = 'Name'; ValidatePattern = 'HR_*' }}
```

Allowing external commands and PowerShell scripts

To allow users to run executables and PowerShell scripts (.ps1) in a JEA session, you have to add the full path to each program in the VisibleExternalCommands field.

```
PowerShell                                                                    Copy

VisibleExternalCommands = 'C:\Windows\System32\whoami.exe', 'C:\Program Files\Contoso\Scripts\UpdateITSoftware.ps1'
```

It is advised, where possible, to use PowerShell cmdlet/function equivalents of any external executables you authorize since you have control over which parameters are allowed with PowerShell cmdlets/functions.

Many executables allow you to both read the current state and then change it just by providing different parameters.

NEW QUESTION 36
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.

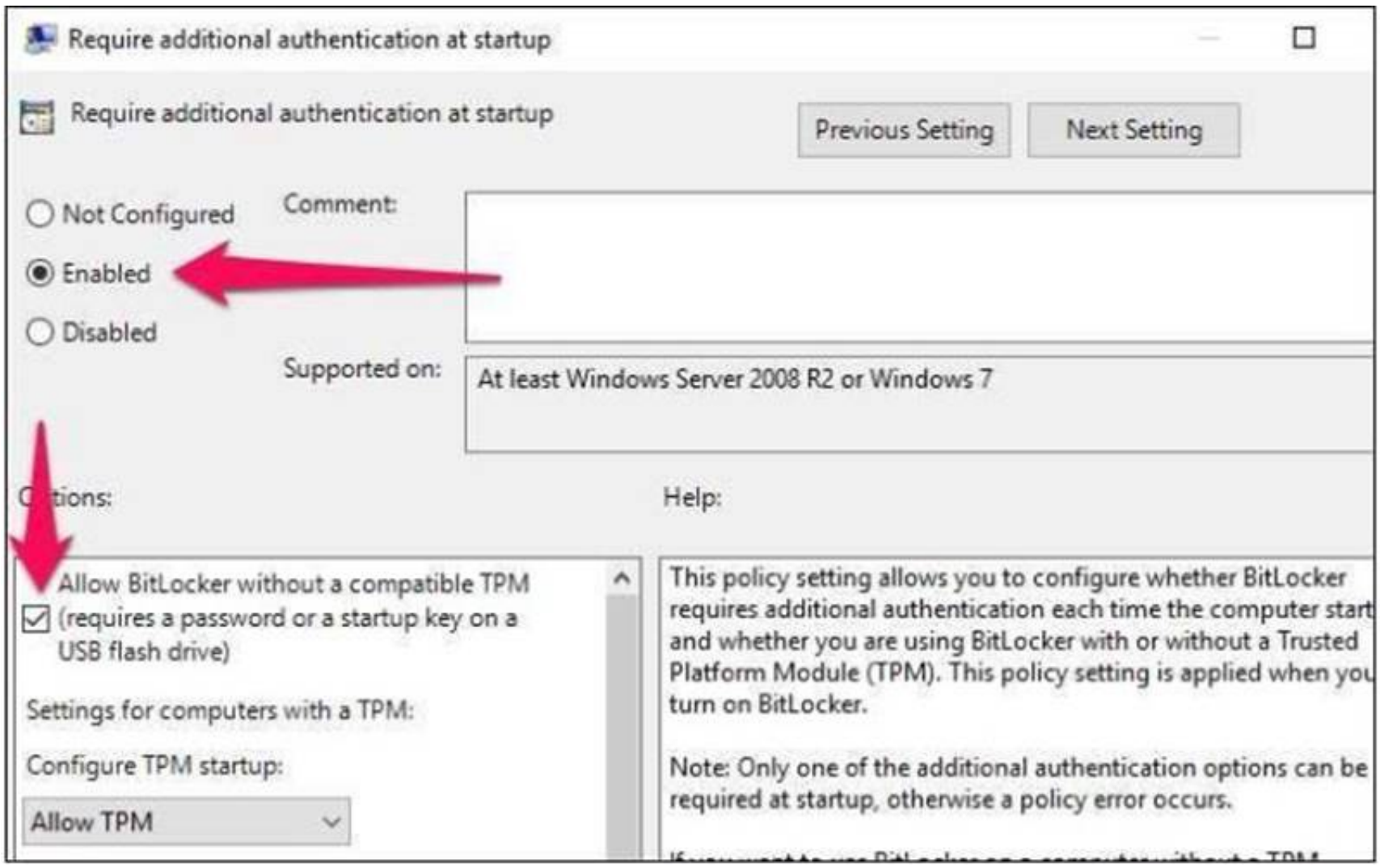
Server name	Domain or workgroup	Configuration
Server1	Domain	Windows Server Update Services (WSUS) server
Server2	Domain	Server that has a Trusted Platform Module (TPM)
Server3	Domain	Member server that will be configured for Just Enough Administration (JEA)
Server4	Domain	Application server
Server5	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 encrypt the operating system drive of VM1 by using BitLocker. Which Group Policy should you configure?

A. Configure use of hardware-based encryption for operating system drives
B. Configure TPM platform validation profile for native UEFI firmware configurations
C. Require additional authentication at startup
D. Configure TPM platform validation profile for BIOS-based firmware configurations

Answer: C

Explanation:
As there is not a choice "Enabling Virtual TPM for the virtual machine VM1", then we have to use a fall-back method for enabling BitLocker in VM1.
https://www.howtogeek.com/howto/6229/how-to-use-bitlocker-on-drives-without-tpm/



NEW QUESTION 41
Your network contains an Active Directory domain named contoso.com. The domain contains multiple servers that run either Windows Server 2012 or Windows Server 2012 R2.
You plan to implement Just Enough Administration (JEA) to manage all of the servers.
What should you install on each server to ensure that the servers can be managed by using JEA?

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

Answer: D

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

NEW QUESTION 44
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

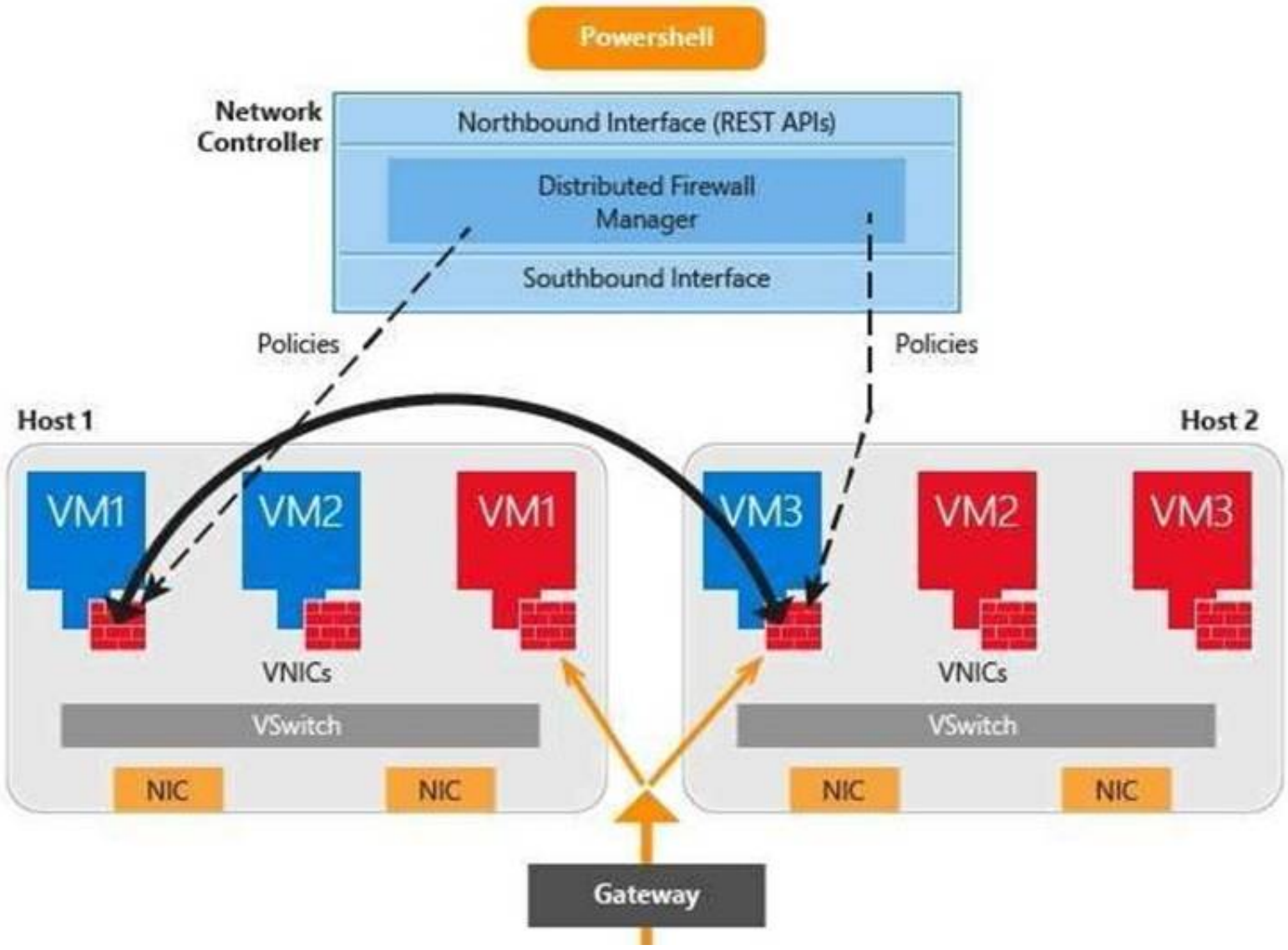
You need to install the required server roles for the planned deployment Which server role should you deploy? Choose Two.

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 48
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”.

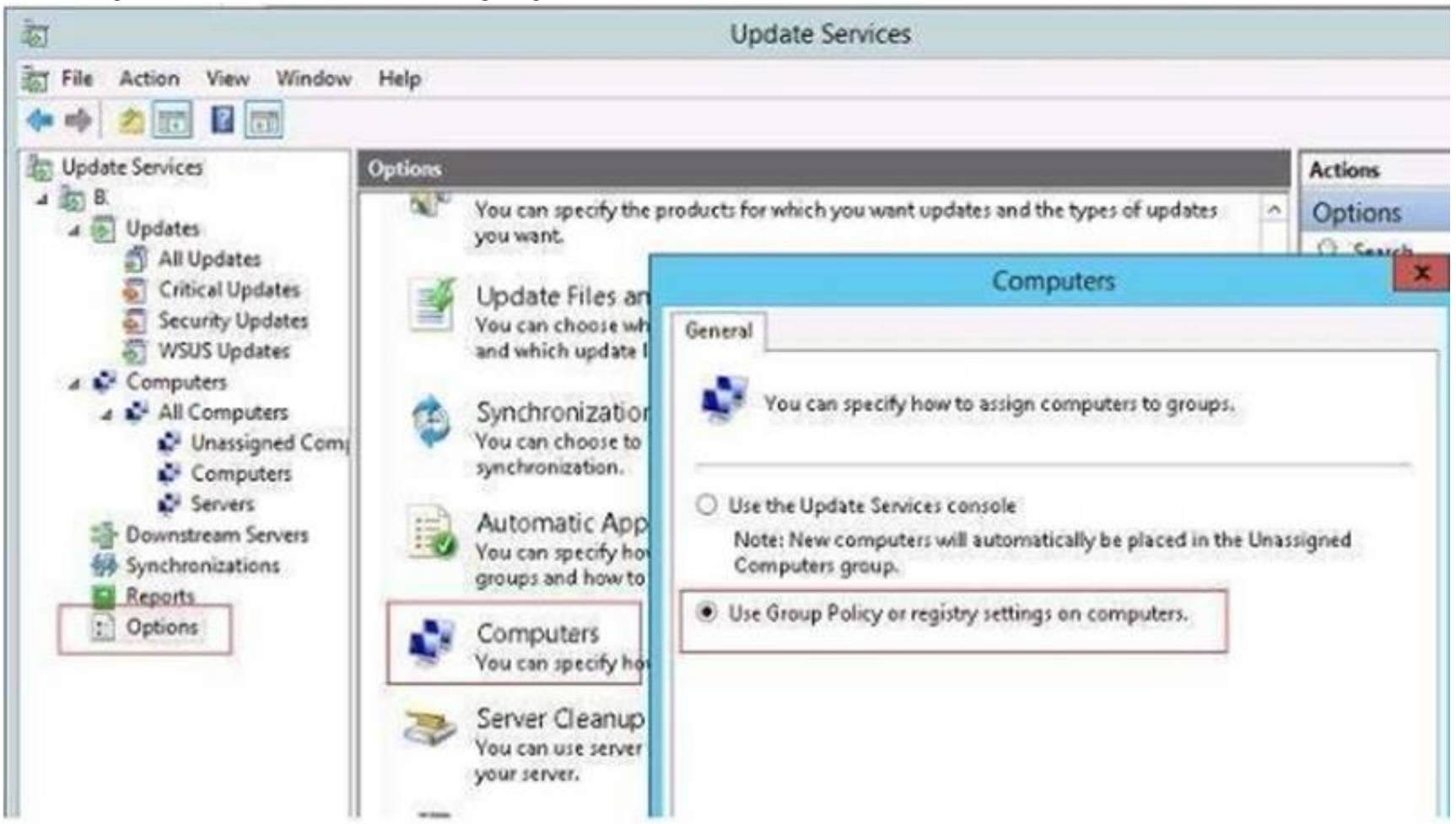
NEW QUESTION 52
Your network contains an Active Directory domain.
The domain contains two organizational units (OUs) named ProdOU and TestOU.

All production servers are in ProdOU. All test servers are in TestOU. A server named Server1 is in TestOU.
You have a Windows Server Update Services (WSUS) server named WSUS1 that runs Windows Server 2016.
All servers receive updates from WSUS1.
WSUS is configured to approve updates for computers in the Test computer group automatically. Manual approval is required for updates to the computers in the Production computer group.
You move Server1 to ProdOU, and you discover that updates continue to be approved and installed automatically on Server1.
You need to ensure that all the servers in ProdOU only receive updates that are approved manually. What should you do?

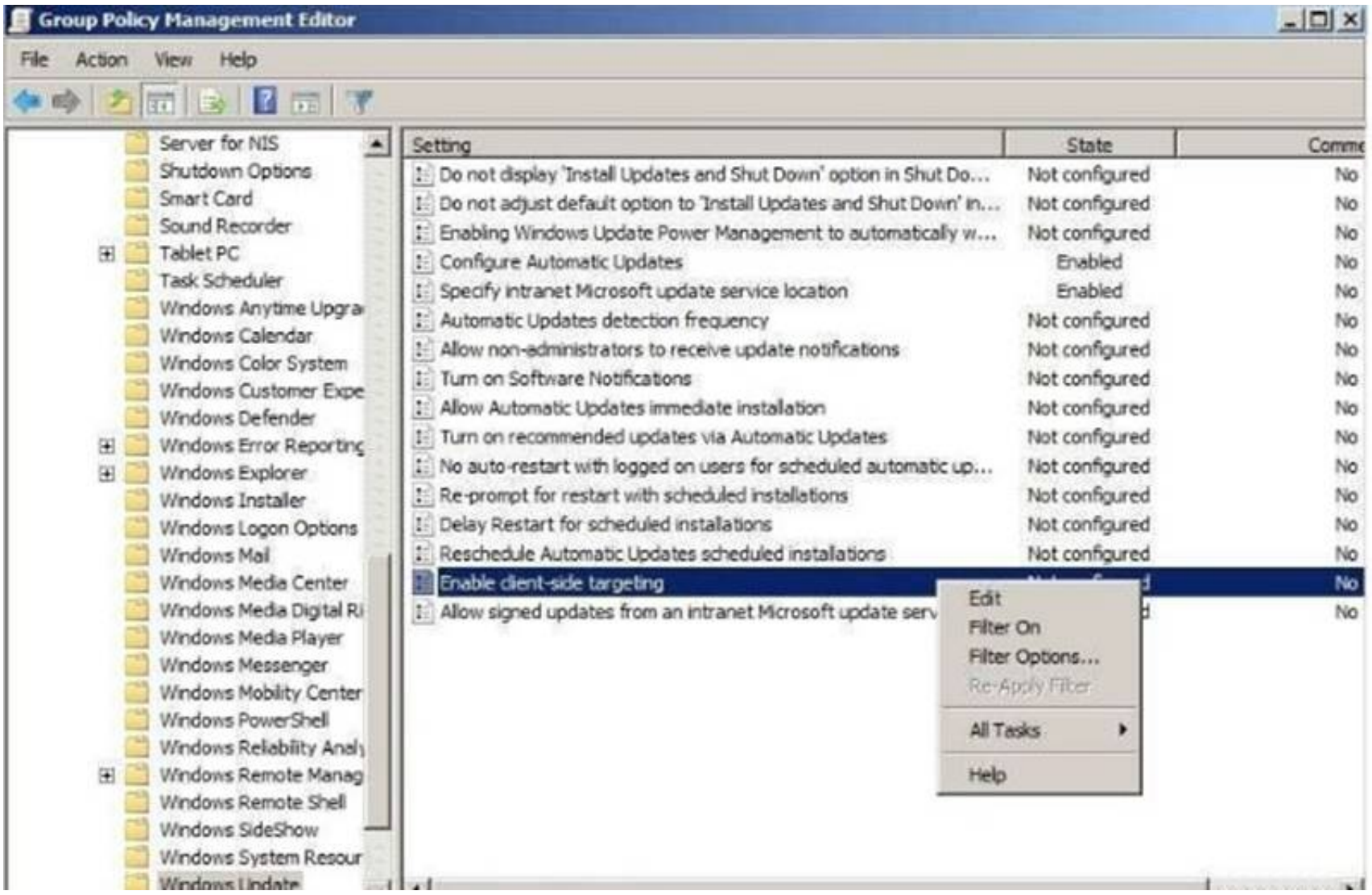
A. Turn off auto-restart for updates during active hours by using Group Policy objects (GPOs).
B. Configure client-side targeting by using Group Policy objects (GPOs).
C. Create computer groups by using the Update Services console.
D. Run wuauclt.exe /detectnow on each server after the server is moved to a different O

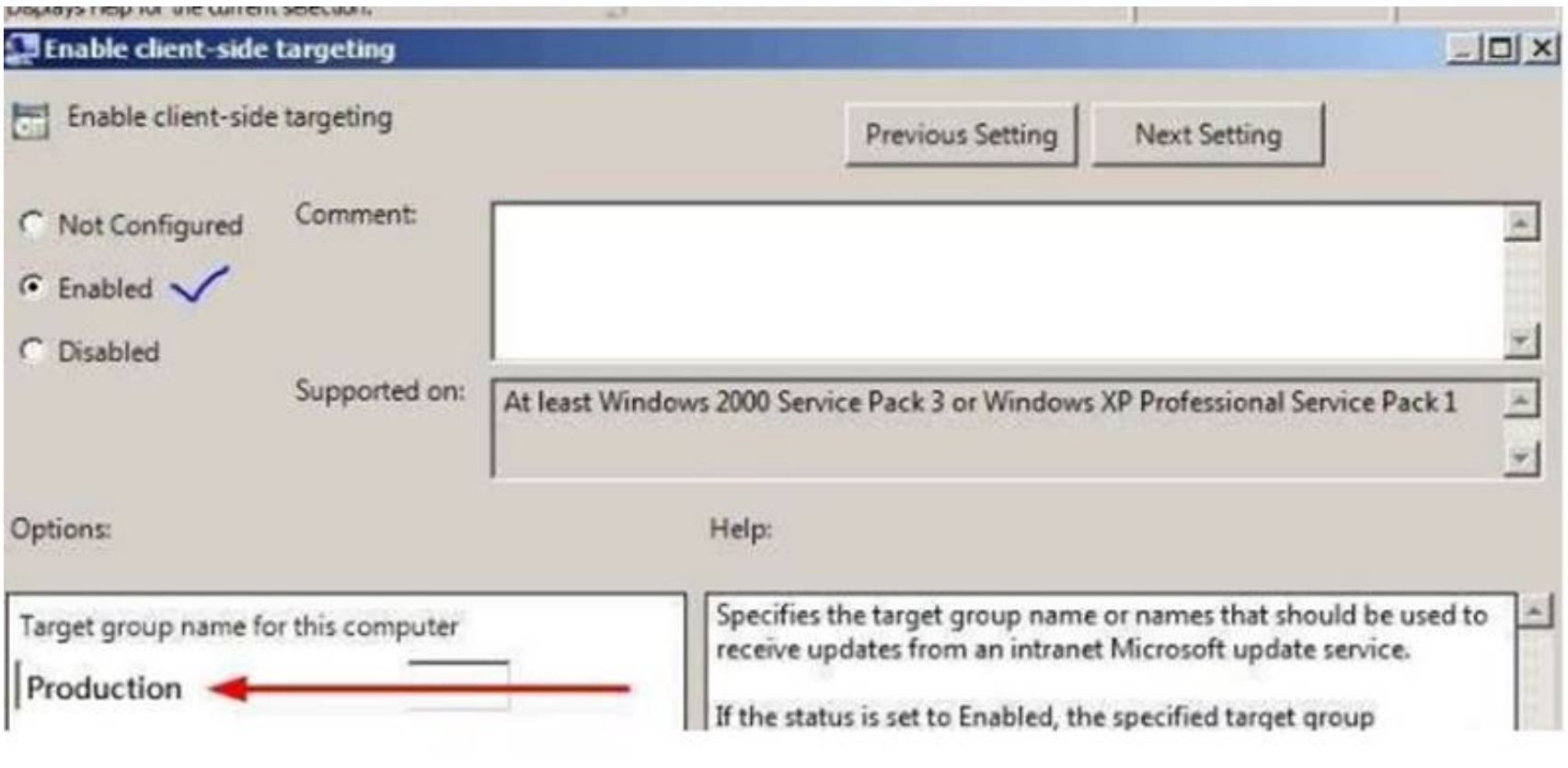
Answer: B

Explanation:
Updates in WSUS are approved against “Computer Group” , not AD OUs. For this example, to prevent Server1 to install automatically approved updates, you have to remove Server1 from “Test” computer group and add Server1 into “Production” computer group in WSUS console, manually or use the WSUS GPO Client-Side Targeting feature.
https://technet.microsoft.com/en-us/library/cc720450%28v=ws.10%29.aspx?f=255&MSPPError=- 2147217396
With client-side targeting, you enable client-computers to add themselves to the computer groups you create in the WSUS console.
You can enable client-side targeting through Group Policy (in an Active Directory network environment) or by editing registry entries (in a non-Active Directory network environment) for the client computers.
When the WSUS client computers connect to the WSUS server, they will add themselves into the correct computer group.
Client-side targeting is an excellent option if you have many client computers and want to automate the process of assigning them to computer groups.
First, configure WSUS to allow Client Site Targeting.



Secondly, configure GPO to affect “ProdOU” , so that Server1 add itself to “Production” computer group.
https://prajwaldesai.com/how-to-configure-client-side-targeting-in-wsus





NEW QUESTION 53
Your network contains an Active Directory domain named contoso.com. The domain contains servers that run
Windows Server 2016.
You enable Remote Credential Guard on a server named Server1.
You have an administrative computer named Computer1 that runs Windows 10. Computer1 is configured to require Remote Credential Guard.
You sign in to Computer1 as Contoso\\User1.
You need to establish a Remote Desktop session to Server1 as Contoso\\ServerAdmin1. What should you do first?

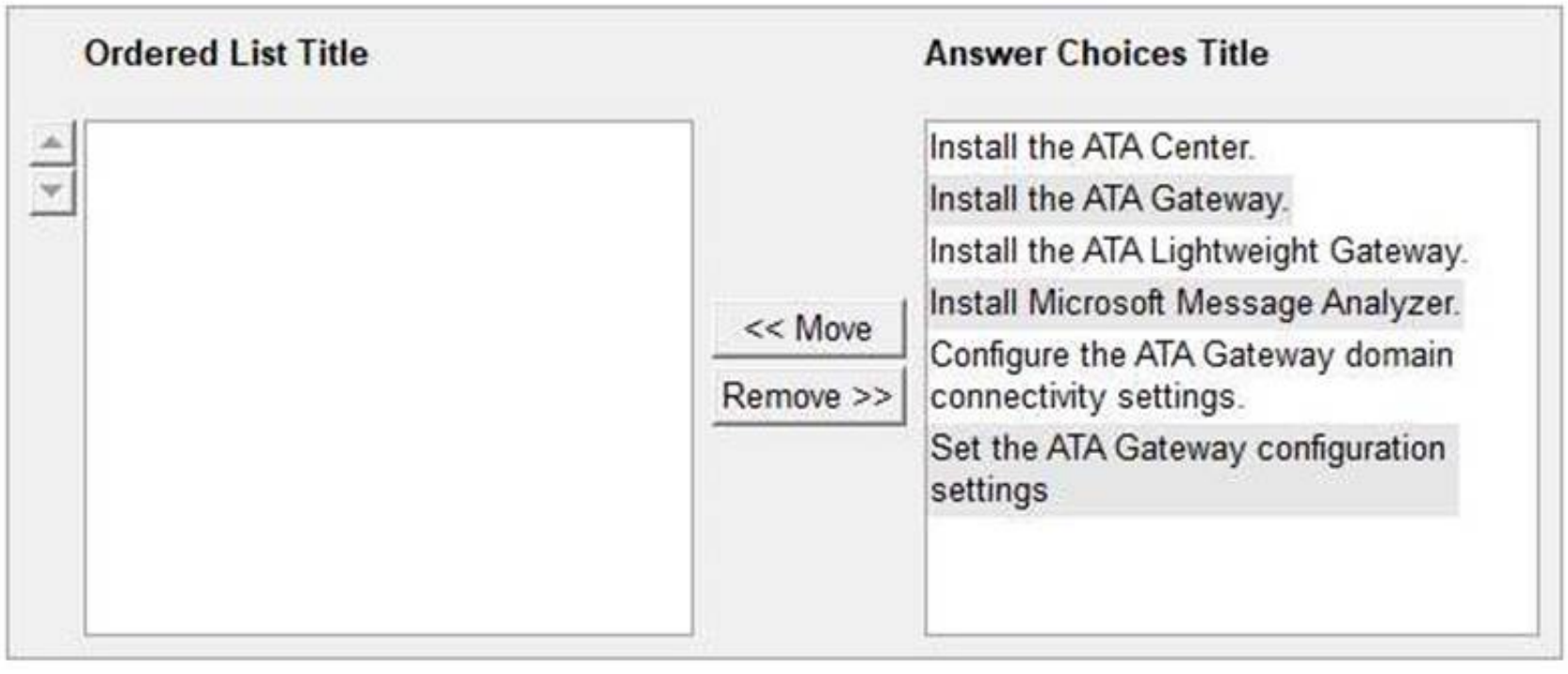
A. Install the Universal Windows Platform (UWP) Remote Desktop application
B. Turn on virtualization based security
C. Run the mstsc.exe /remoteGuard
D. Sign in to Computer1 as Contoso\\ServerAdmin1

Answer: D

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

NEW QUESTION 57
DRAG DROP
Your network contains an Active Directory domain named contoso.com.

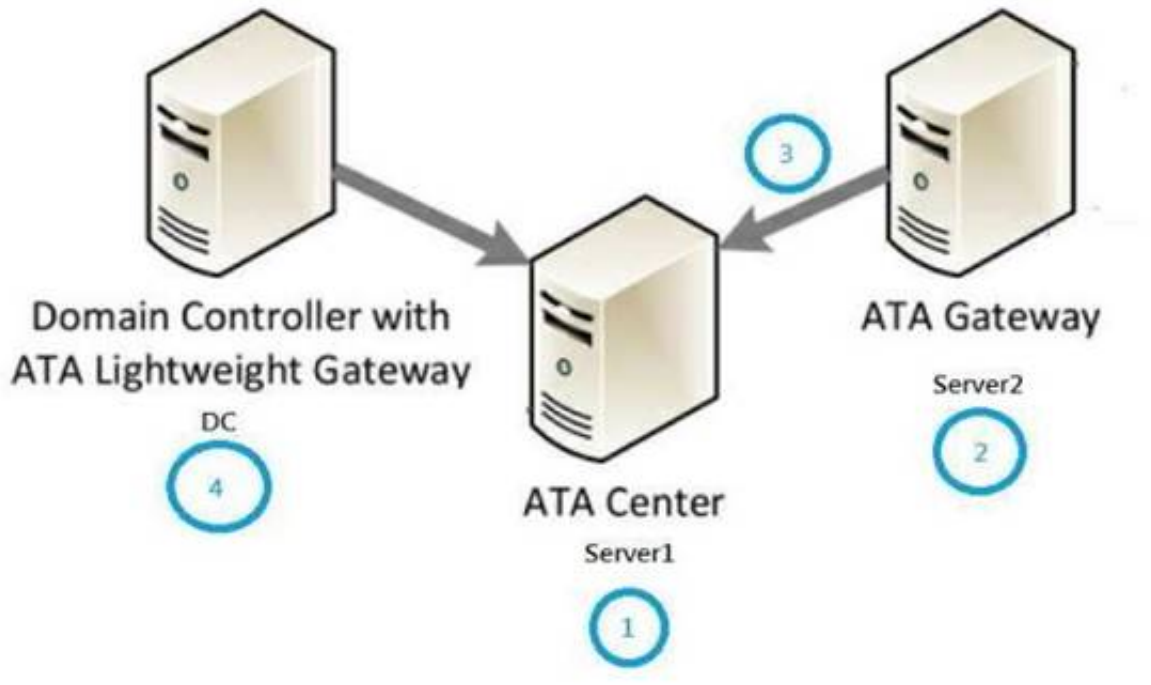
The domain contains two servers named Server1 and Server2 that run Windows Server 2016. You need to install Microsoft Advanced Threat Analytics (ATA) on Server1 and Server2. Which four actions should you perform in sequence?



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.

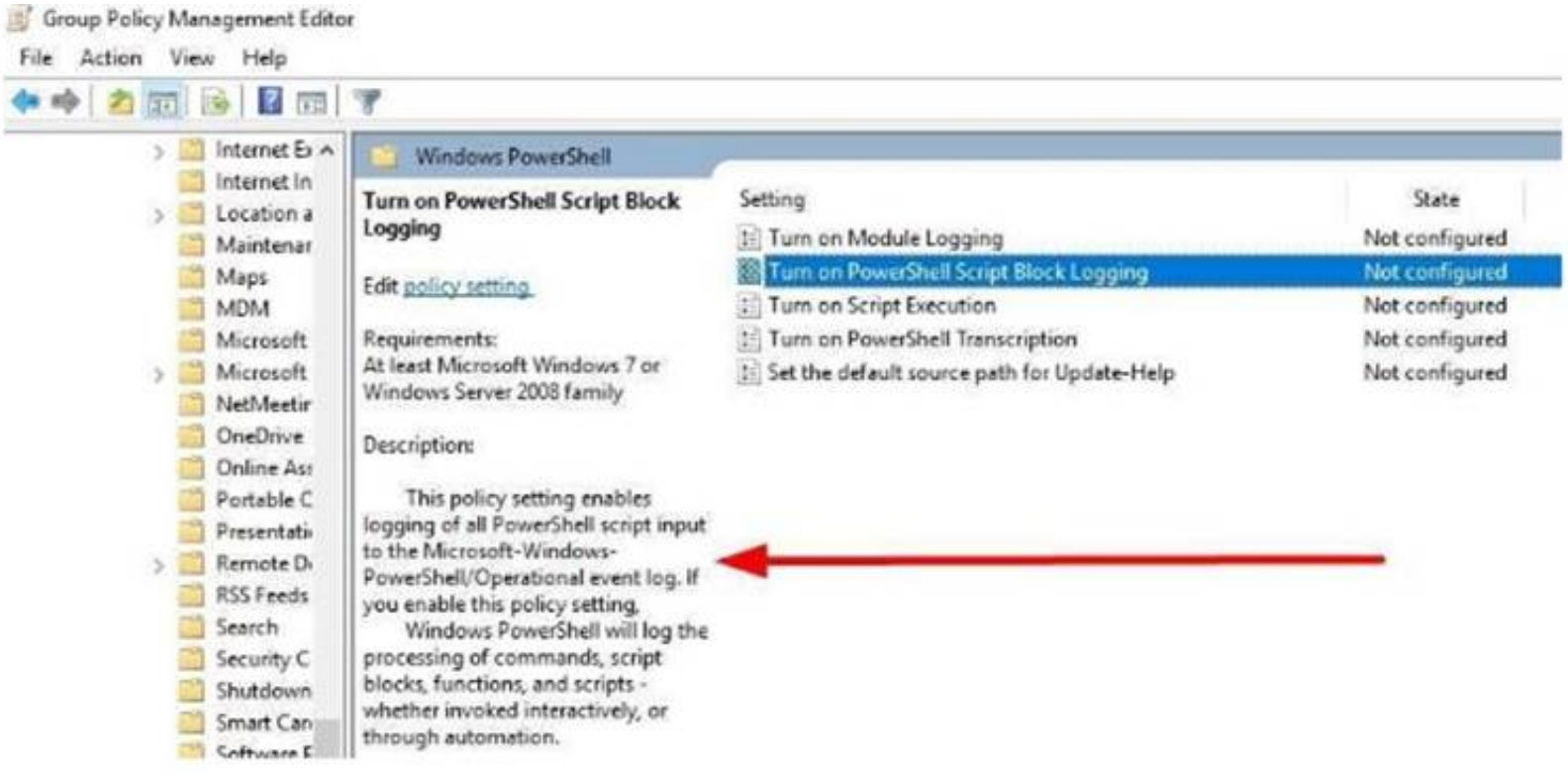


NEW QUESTION 60
You enable and configure PowerShell Script Block Logging.
You need to view which script blocks were executed by using Windows PowerShell scripts. What should you do?

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 65
You have a server named Server1 that runs Windows Server 2016.
You need to identify whether any inbound rules on Server1 require that users be authenticated before they can connect to the server. Which cmdlet should you use?

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

Answer: B

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

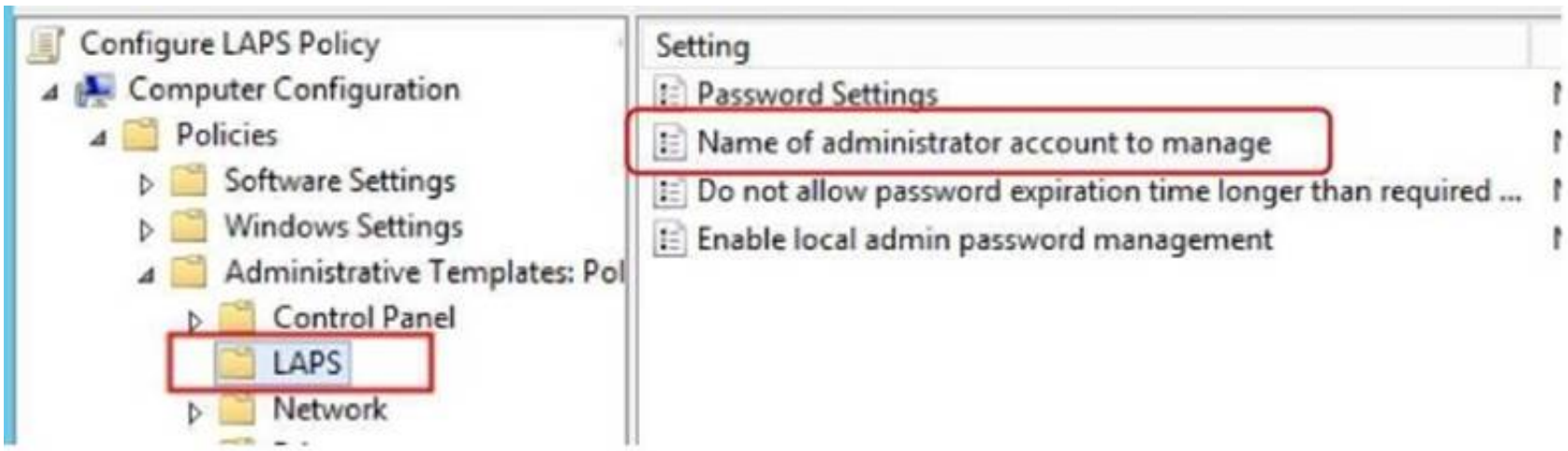
```
PS C:\> Get-NetFirewallRule -DisplayName TEST | Get-NetFirewallSecurityFilter


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



PS C:\>
```

NEW QUESTION 68
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 69
You implement Just Enough Administration (JEA) on several file servers that run Windows Server 2016.
The Role Capability file from a server named Server5 contains the following code.

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

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

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

Answer: B

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

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

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

NEW QUESTION 70
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 71
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.

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

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

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

Answer: B

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

NEW QUESTION 72
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 77
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 79
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 80
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows10.
The network uses the 172.16.0.0/16 address space.
Computer1 has an application named App1.exe that is located in D:\Apps\. App1.exe is configured to accept connections on TCP port 8080.
You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.
Solution: You run the New-NetFirewallRule –DisplayName "Rule1" –Direction Inbound –Program "D:\Apps\App1.exe" –Action Allow -Profile Domain command. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 85
.....

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