Exam Questions 70-744

Securing Windows Server 2016

https://www.2passeasy.com/dumps/70-744/

NEW QUESTION 1
Note: This question b part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear In the review screen.
Your network contains an Active Directory domain named contow.com. All servers run Windows Server 2016. All client computers run Windows 10.
The relevant objects in the domain are configured as shown in the following table.

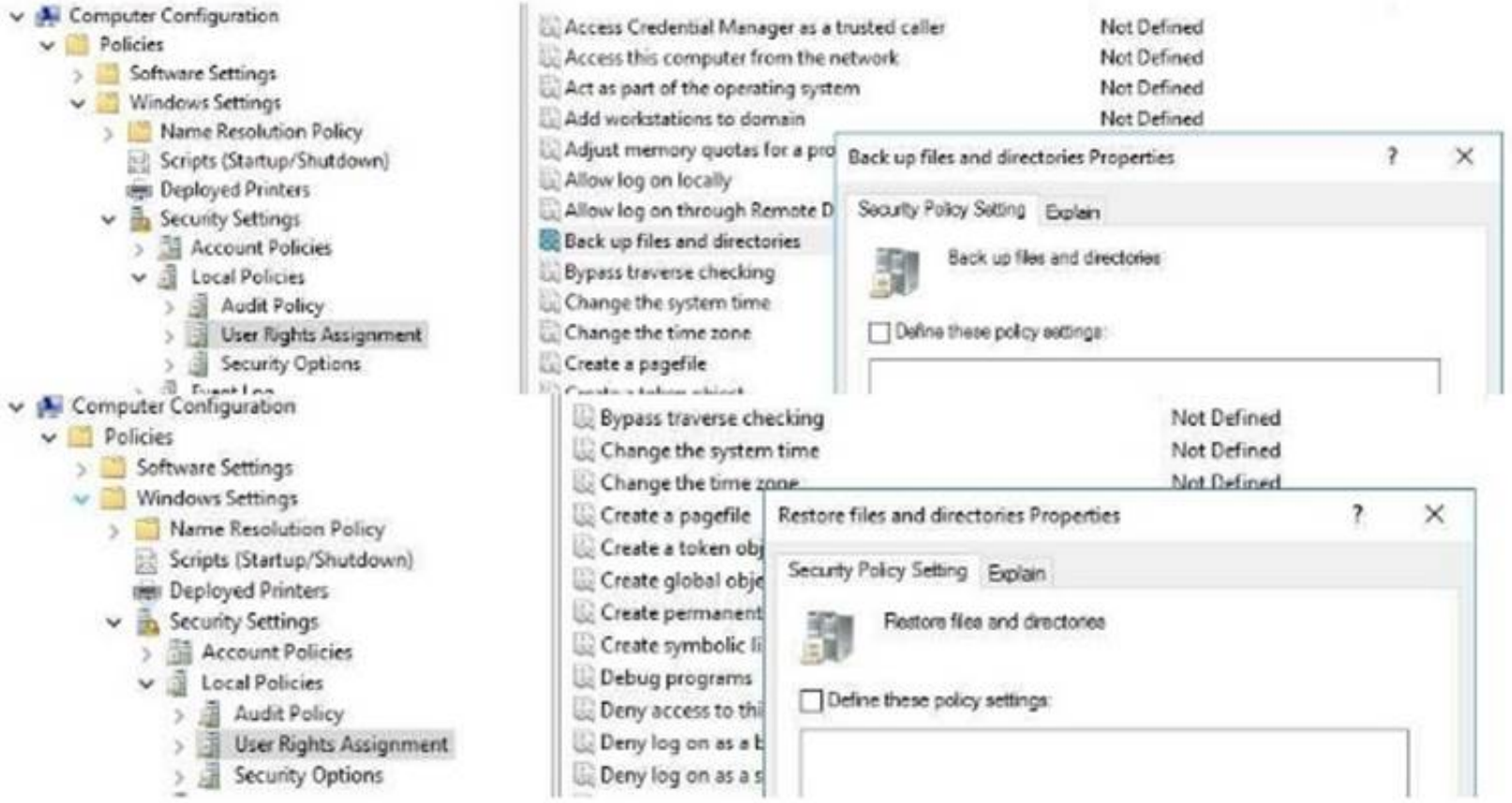
Server name	Object	Organizational unit (OU) name
Server1	Computer account	Servers
Server2	Computer account	Servers
User1	User account	Operations Users

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

A. Yes
B. No

Answer: A

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



NEW QUESTION 2
Note: Thb question Is part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you willNOTbeabletorrturntoit.Asa result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains multiple Hyper-V hosts.
You need to deploy several critical line-of-business applications to the network to meet the following requirements:
*The resources of the applications must be isolated from the physical host
*Each application must be prevented from accessing the resources of the other applications.
*The configurations of the applications must be accessible only from the operating system that hosts the application.
Solution: You deploy one Windows container to host all of the applications. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 3
Your network contains an Active Directory domain named contoso.com. The domain contains two
servers named Server1 and Server2 that run Windows Server 2016. Server1 is configured as a domain controller.
You configure Server1 as a Just Enough Administration (JEA) endpoint You configure the required JEA rights for a user named User1.
You need to tell User1 how to manage Active Directory objects from Server2. What should you tell User1 to do first on Server2?

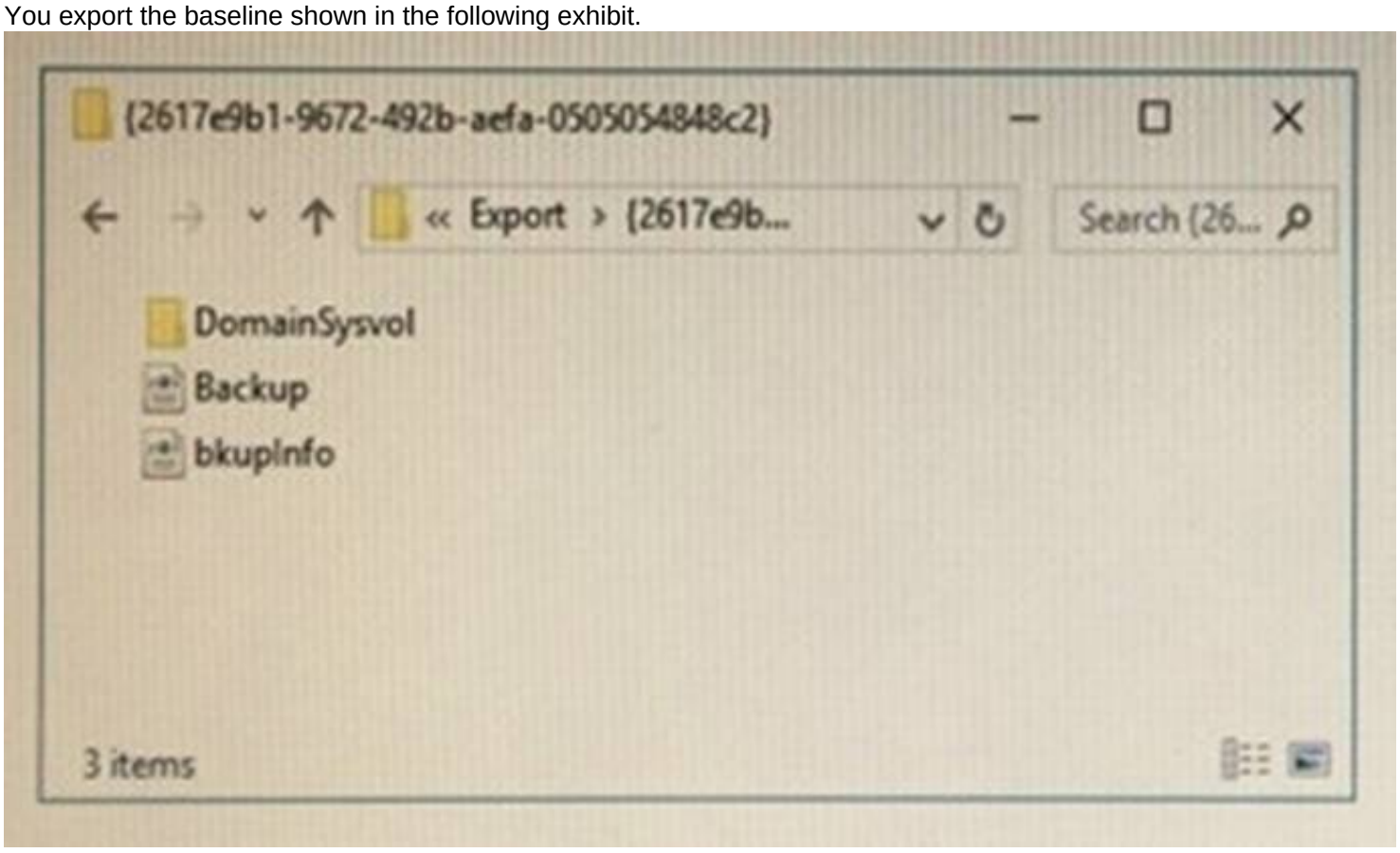
A. From a command prompt, run ntdsutil.exe.
B. From Windows PowerShell, run the Import-Module cmdlet.
C. From Windows PowerShell run the Enter-PSSession cmdlet.

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

Answer: C

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

NEW QUESTION 4
Vout network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2016.
The domain contains a server named Serverl that has Microsoft Security Compliance Manager (SCM)
4.0 installed.
You export the baseline shown in the following exhibit.



You have a server named Server2 that is a member of a workgroup.
You copy the (2617e9b1-9672-492b-aefa-0505054848c2) folder to Server2. You need to deploy the baseline settings to Server2.
What should you do?

A. Download, install, and then fun the Lgpo.exe command.
B. From Group Policy Management import a Group Policy object (GPO).
C. From Windows PowerShell, run the Restore-GPO cmdlet.
D. From Windows PowerShell, run the Import-GPO cmdlet.
E. From a command prompt run the secedit.exe command and specify the /import paramete

Answer: D

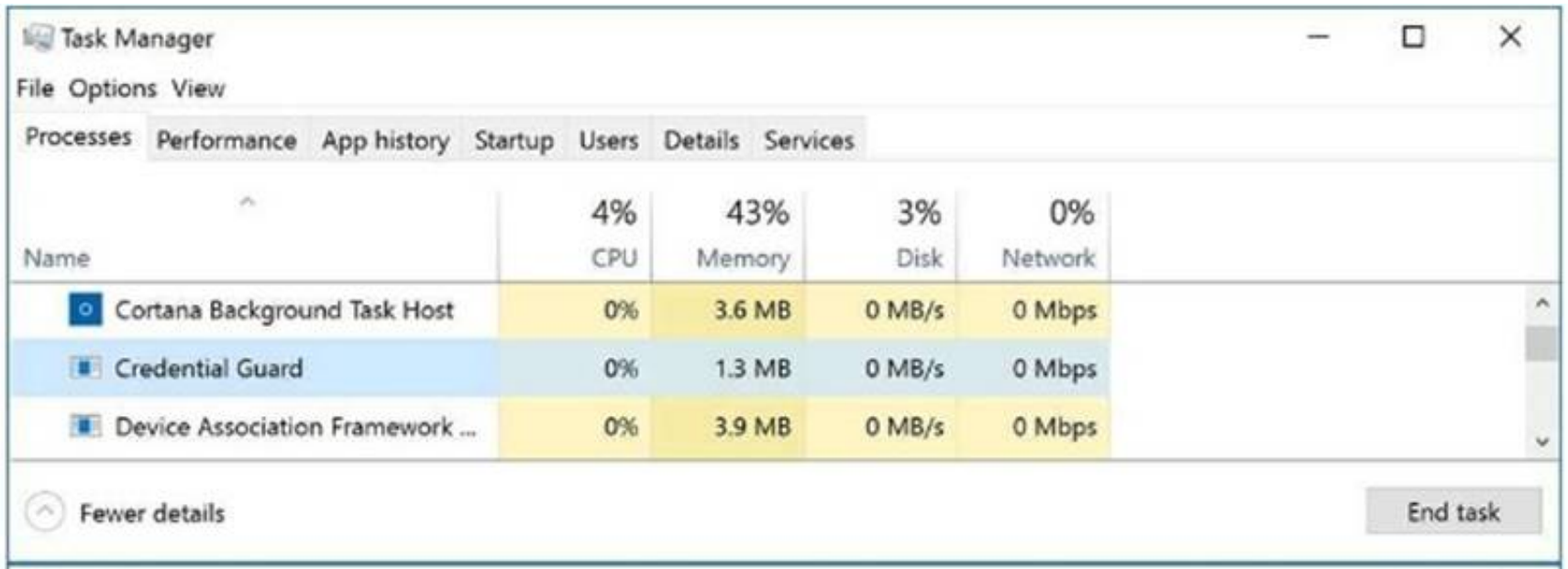
Explanation:
References:
https://anytecho.wordpress.com/2015/05/22/importing-group-policies-using-powershell-almost/

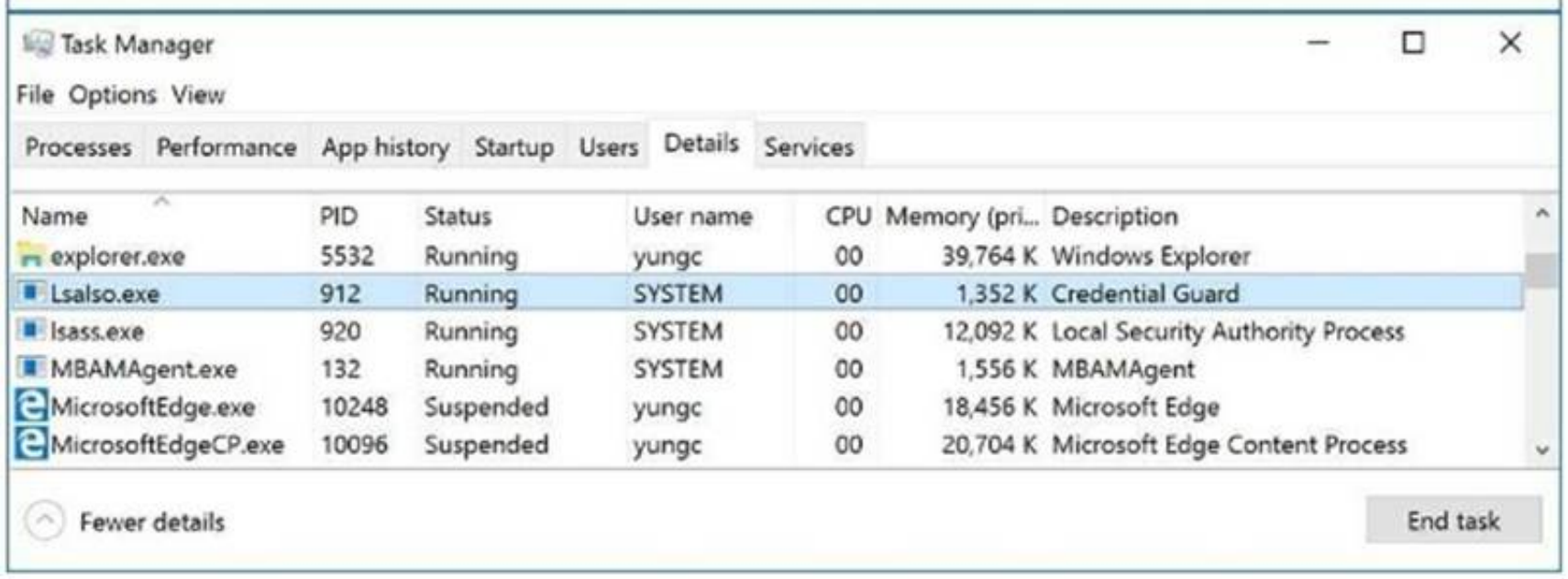
NEW QUESTION 5
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Serve1, that runs Windows Server 2016.
A technician is testing the deployment of Credential Guard on Server1. You need to verify whether Credential Guard is enabled on Server1. What should you do?

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

Answer: B

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

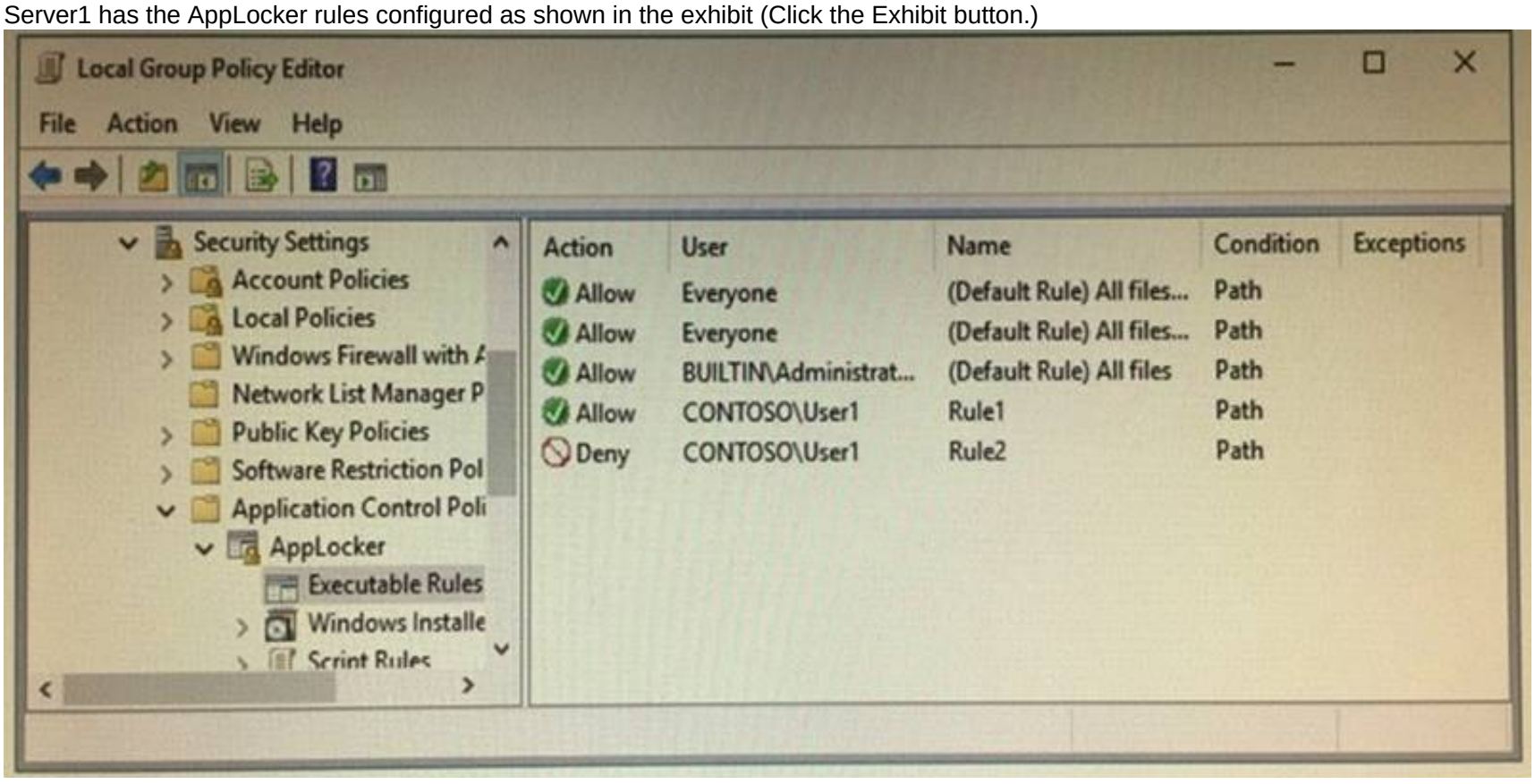




NEW QUESTION 6
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.
The services on Server1 are shown in the following output.

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

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

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



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

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

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

Answer Area

Statements	Yes	No
On Server1, User1 can run D:\Folder2\App1.exe.	○	○
On Server1, User1 can run D:\Folder1\Program1.exe.	○	○
If Program1.exe is copied from D:\Folder1 to D:\Folder2, User1 can run Program1.exe on Server1.	○	○

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 7
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.

Answer Area

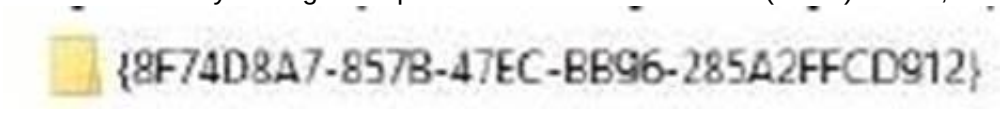
Format to use to export the baseline:
- Excel (.xlsm)
- GPO Backup (folder)
- SCAP v1.0 (.cab)
- SCCM DCM 2007 (.cab)
- SCM (.cab)

Tool to use to import the baseline:
- Group Policy Management
- Group Policy Object Editor
- Microsoft Security Compliance Manager (SCM)
- Resultant Set of Policy
- Security Configuration and Analysis

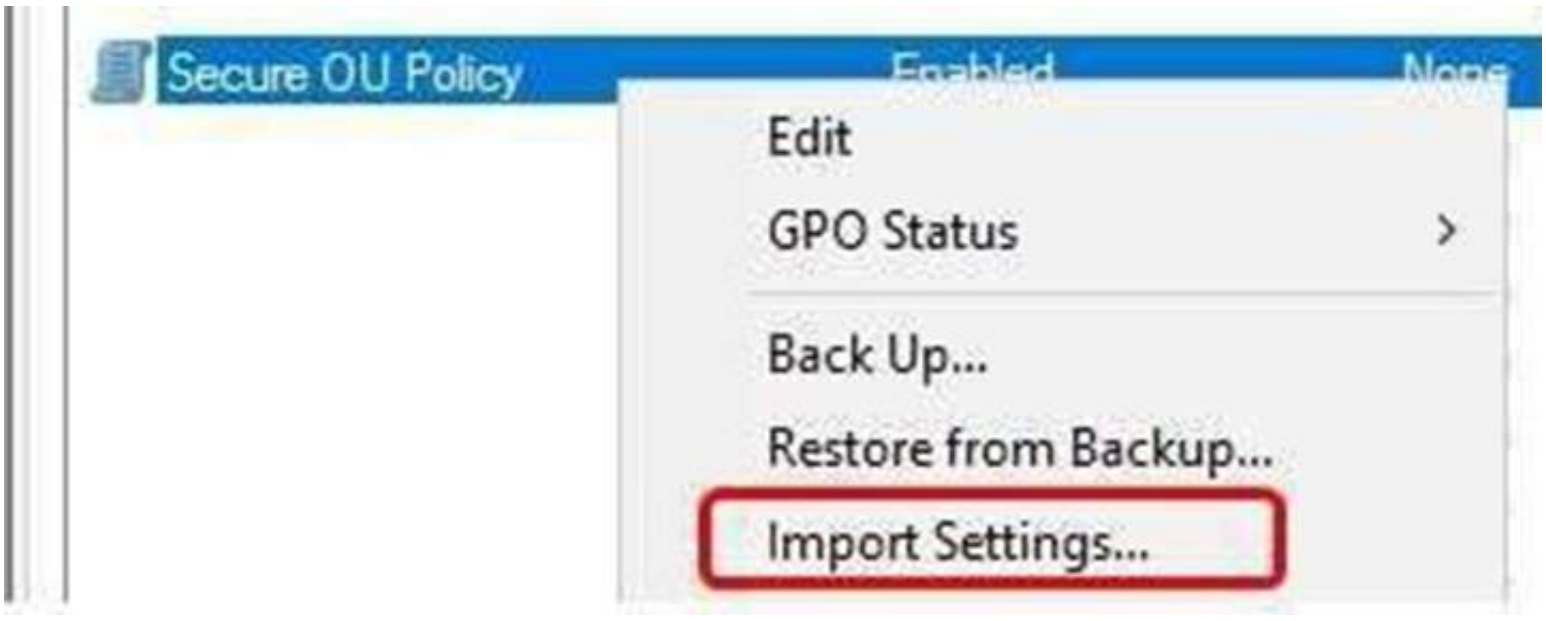
A. Mastered
B. Not Mastered

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 8
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server5 that has the Windows Server Update Services server role installed. You need to configure Windows Server Update Services (WSUS) on Server5 to use SSI. You install a certificate in the local Computer store.
Which two tools should you use? Each correct answer presents part of the solution.

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

Answer: AC

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

NEW QUESTION 9
Note: This question Is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. Server1 has a volume named Volume1.
A central access policy named Policy1 is deployed to the domain. You need to apply Policy1 to Volume1.
Which tool should you use?

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

Answer: A

Explanation:

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

NEW QUESTION 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 14
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 16
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

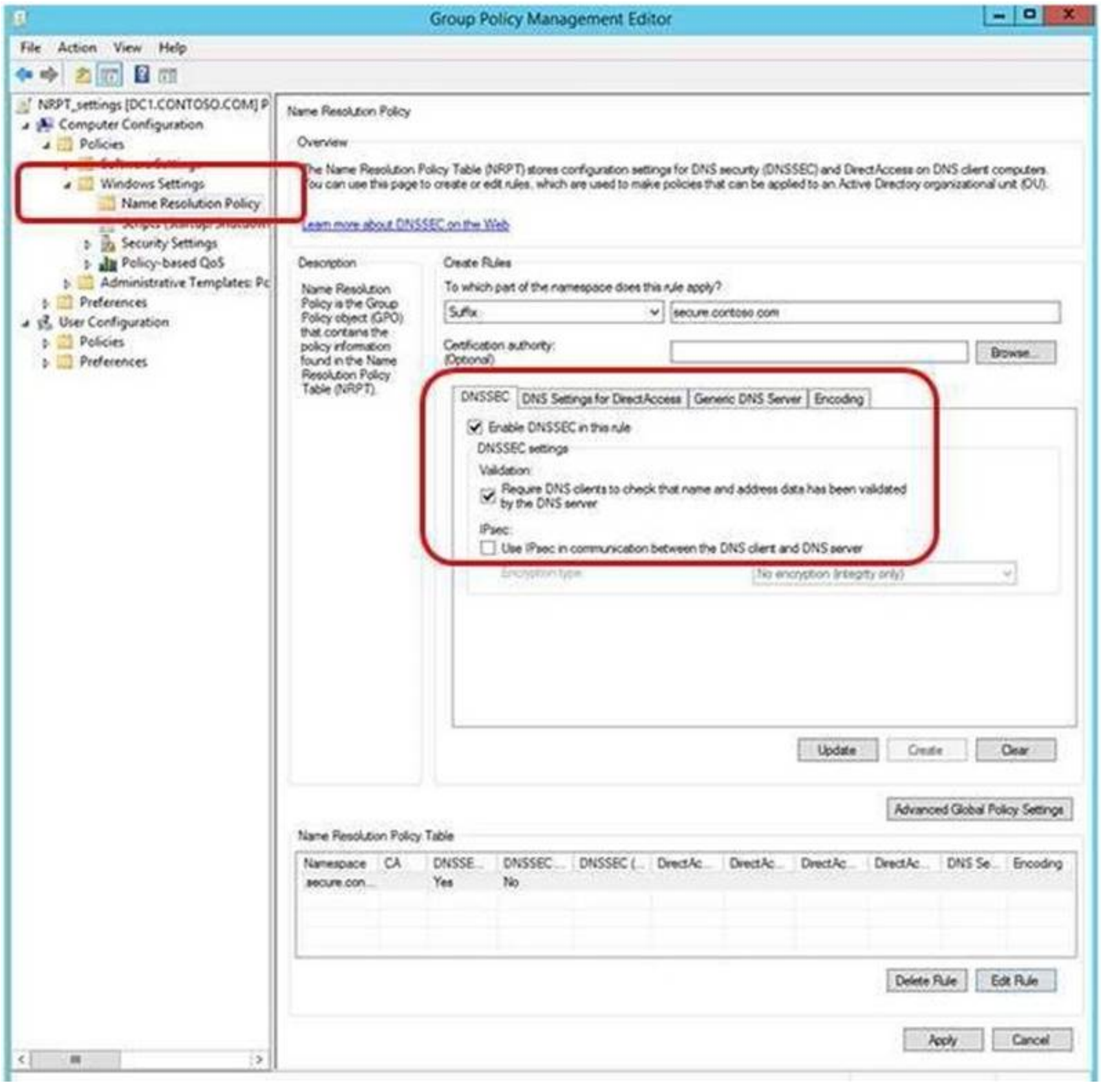
All servers run Windows Server 2016. All client computers run Windows 10.
You have an organizational unit (OU) named Marketing that contains the computers in the marketing department You have an OU named Finance that contains the computers in the finance department You have an OU named AppServers that 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 the marketing department computers validate DNS responses from adatum.com.
Which setting should you configure in the Computer Configuration node of GP1?

A. TCPIP Settings from Administrative Templates
B. Connection Security Rule from Windows Settings
C. DNS Client from Administrative Templates
D. Name Resolution Policy from Windows Settings

Answer: D

Explanation:

The NRPT is a table that contains rules that you can configure to specify DNS settings or special behavior for names or namespaces.
The NRPT can be configured using the Group Policy Management Editor under Computer Configuration \\Policies\\Windows Settings\\Name Resolution Policy, or with Windows PowerShell.
If a DNS query matches an entry in the NRPT, it is handled according to settings in the policy. Queries that do not match an NRPT entry are processed normally.
You can use the NRPT to require that DNSSEC validation is performed on DNS responses for queries in the namespaces that you specify.



NEW QUESTION 20
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.

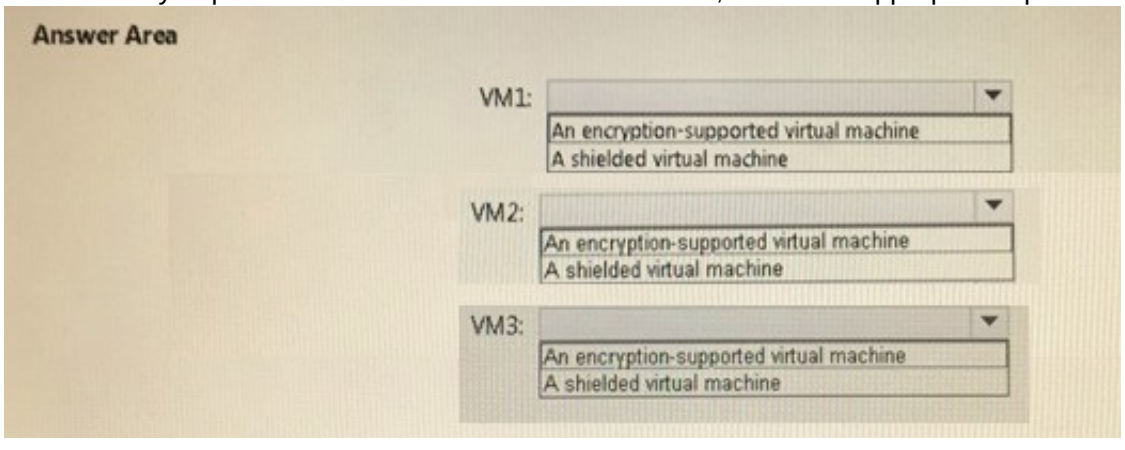
Answer: B

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 23
HOTSPOT
You plan to deploy three encrypted virtual machines that use Secure Boot. The virtual machines will be configured as shown in the following table.

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

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



A. Mastered
B. Not Mastered

Answer: A

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

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

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

NEW QUESTION 27
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 32
A shielding data file (also called a provisioning data file or PDK file) is an encrypted file that a tenant or VM owner creates to protect important VM configuration information.
A fabric administrator uses the shielding data file when creating a shielded VM, but is unable to view or use the information contained in the file.
Which information can be stored in the shielding data file?

A. Administrator credentials
B. All of these
C. A Key Protector
D. Unattend.xml

Answer: B

NEW QUESTION 34
____ 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 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 41
The “Network Security: Restrict NTLM: NTLM authentication in this domain” policy setting allows you to deny or allow NTLM authentication within a domain from this domain controller.
Which value would you choose so that the domain controller will deny all NTLM authentication logon attempts using accounts from this domain to all servers in the domain.
The NTLM authentication attempts will be blocked and will return an NTLM blocked error unless the server name is on the exception list in the Network security: Restrict NTLM: Add server exceptions in this domain policy setting.

A. Deny for domain accounts
B. Deny for domain accounts to domain servers
C. Deny all
D. Deny for domain servers

Answer: B

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 a server named Server1 that runs Windows Server 2016. A user named User1 is a member of the local Administrators group. Server1 has the AppLocker rules
configured as shown in follow:

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

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

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

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

Answer: AF

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

Important

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

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

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

NEW QUESTION 49
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.

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

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.
All laptops are protected by using BitLocker Drive Encryption (BitLocker).
You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.
An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1.
A GPO named GP2 is linked to OU2.
All computers receive updates from Server1. You create an update rule named Update1.
You enable deep script block logging for Windows PowerShell.
In which event log will PowerShell code that is generated dynamically appear?

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

Answer: A

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

NEW QUESTION 50
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.

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

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

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

Answer: DE

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

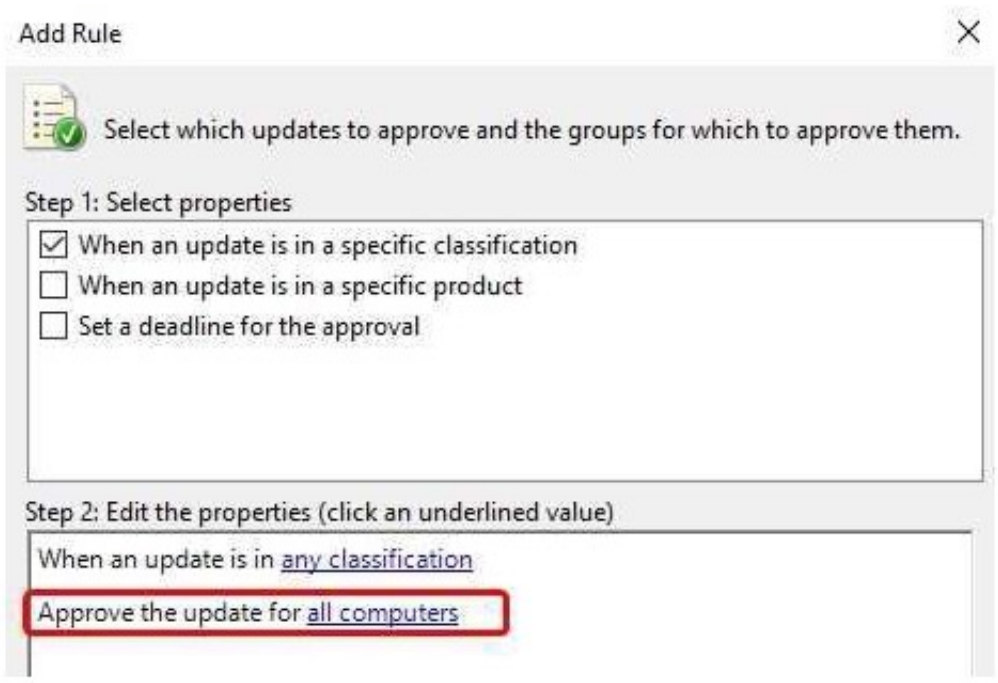
Automatically Approving Updates for Detection

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

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

To automatically approve updates for detection

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



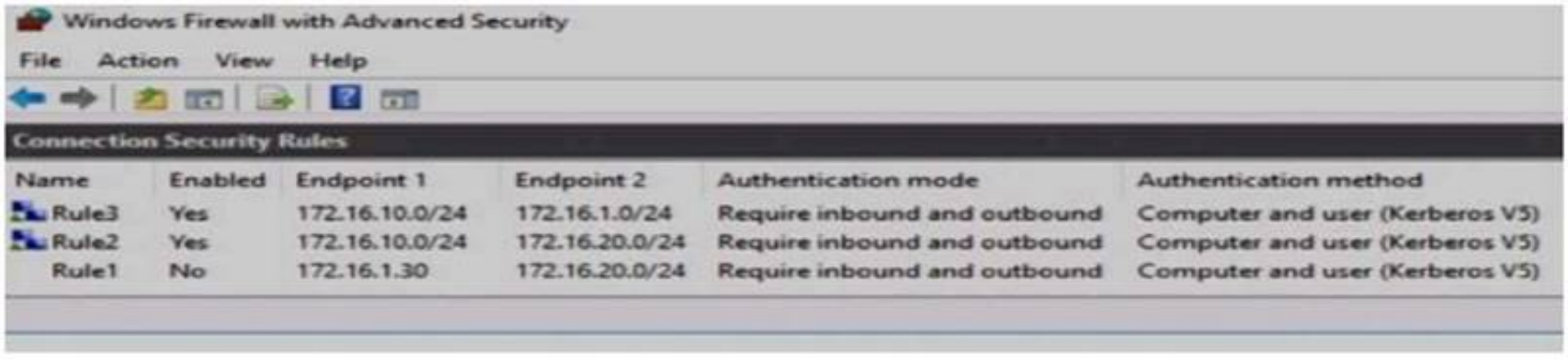
NEW QUESTION 51
HOTSPOT
Your network contains an Active Directory named contoso.com.
The domain contains the computers configured as shown in the following table.

Name	IP address
Server1	172.16.1.30
Computer1	172.16.10.60
Computer2	172.16.20.50

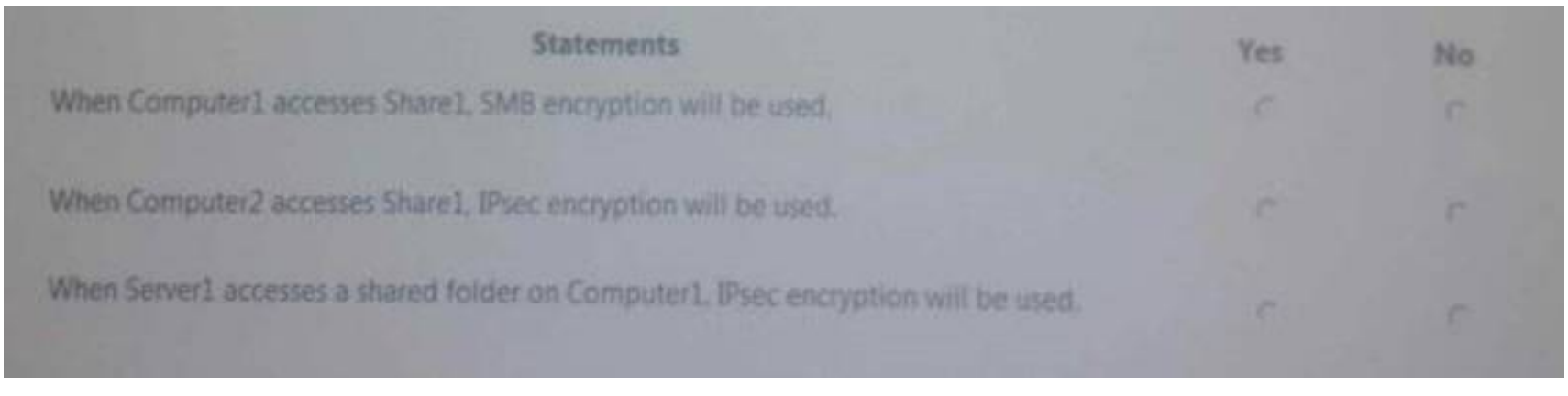
Server1 has a share named Share1 with the following configurations:-

```
PresetPathAc1              :System.Security.AccessControl.DirectorySecurity
ShareState                 :Online
AvailabilityType           :NonClustered
ShareType                  :FileSystemDirectory
FolderEnumerationMode      : Unrestricted
CachingMode                :Manual
SmbInstance                :Default
CATimeout                  :0
ConcurrentUserLimit        :0
ContinuouslyAvailable      :False
CurrentUsers               :0
Description                :
EncryptData                :True
Name                       :Share1
Path                       :C:/Shares/Share1
Scoped                     :False
ScopeName                  :*
SecurityDescriptor         :O:BAG:DUD:(A;OICI;FA;;;WD)
ShadowCopy                 :False
Special                    :False
Temporary                  :False
Volume                     : \\?\Volume{18eb1d3f-0000-0000-0000-501f00000000}\
PSComputerName             :
CimClass                   :ROOT/Microsoft/Windows/SMB:MSFT_SmbShare
CimInstanceProperties      :{AvailabilityType, CachingMode, CATimeout,
                           ConcurrentUserLimit…}
CimSystemProperties        : Microsoft.Management.Infrastructure.CimSystemPro
                             perties
```

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



Please Select the correct statement as below:



A. Mastered
B. Not Mastered

Answer: A

Explanation:
When Computer1 accesses Share1, SMB encryption will be used: YES When Computer2 accesses Share1, SMB encryption will be used: YES
When Server1 accesses a shared folder on Computer1, IPsec encryption will be used: NO
The shared folder “Share1” is configured with “EncryptData : True”, no matter which network the client resides, SMB 3 communication will be encrypted.
When Server1 access Computer1 over network, the original packet L3 IP Header is as follow:- 172.16.1.30 –> 172.16.10.60
These traffic does not match the enabled IPSec rule “Rule2” nor “Rule3”, and the only matching rule “Rule1” is disabled. So, no IPsec encryption will be achieved.

NEW QUESTION 55
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.

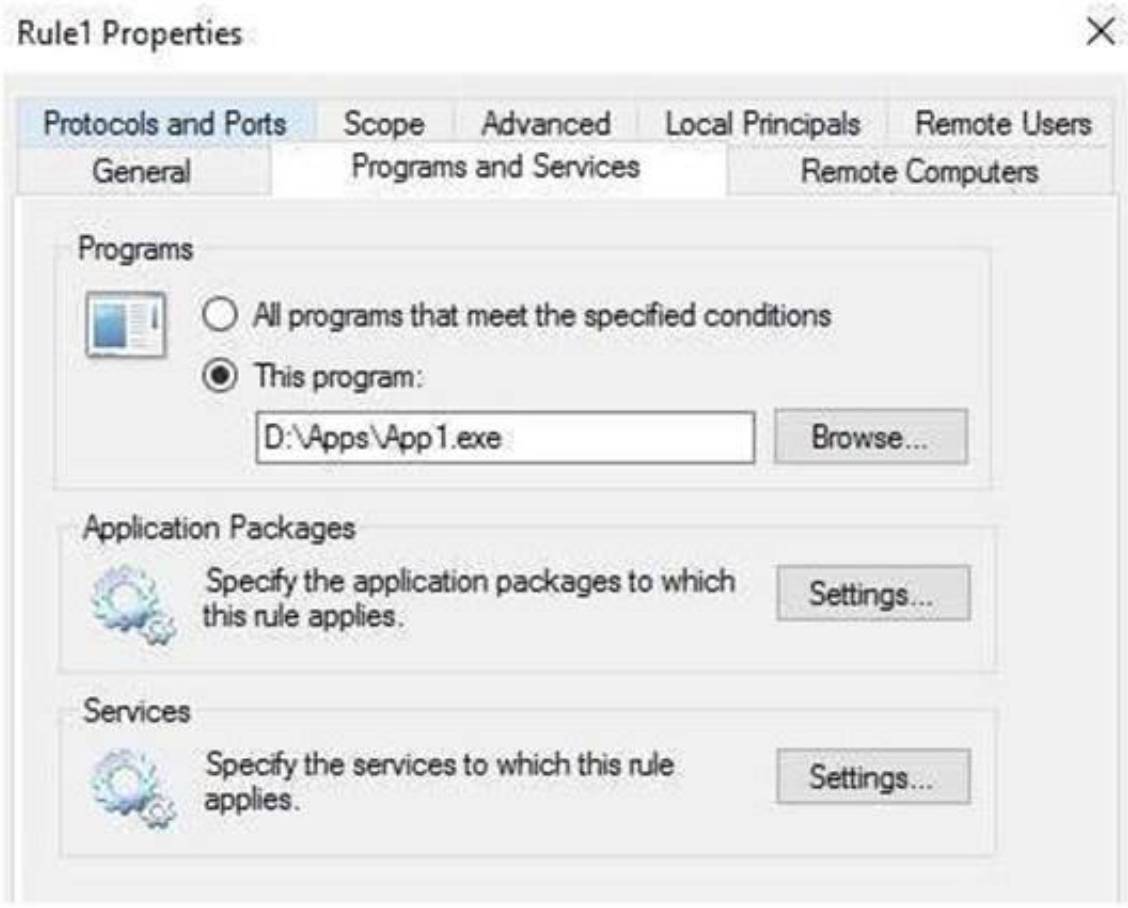
> **Note**
>
> A dedicated Windows Server Update Services instance can be configured to automatically approve updates. For more information, see the "Automatically Approve Updates for Installation" section in Approving Updates.

NEW QUESTION 56
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. Computer1 connects to a home network and a corporate network.
The corporate network uses the 172.16.0.0/24 address space internally. Computer1 runs an application named App1 that listens to port 8080.
You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.
Solution: You run the command New-NetFirewallRule -DisplayName “Rule1” -Direction Inbound - Program “D:\\Apps\\App1.exe” –Action Allow -Profile Domain
Does this meet the goal?
A. Yes
B. No

Answer: A

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

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


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



NEW QUESTION 61
You have a server named Server1 that runs Windows Server 2016. Server1 has the Windows Server Update Services server role installed.
Windows Server Update Services (WSUS) updates for Server1 are stored on a volume named D. The hard disk that contains volume D fails.
You replace the hard disk. You recreate volume D and the WSUS folder hierarchy in the volume. You need to ensure that the updates listed in the WSUS console are available in the WSUS folder. What should you run?

A. wsusutil.exe /import
B. wsusutil.exe /reset
C. Set-WsusServerSynchronization
D. Invoke-WsusServerCleanup

Answer: B

Explanation:
https://technet.microsoft.com/en-us/library/cc720466%28v=ws.10%29.aspx?f=255&MSPPError=- 2147217396
WSUSutil.exe is a tool that you can use to manage your WSUS server from the command line.
WSUSutil.exe
is located in the %drive%\\Program Files\\Update Services\\Tools folder on your WSUS server.
You can run specific commands with WSUSutil.exe to perform specific functions, as summarized in the following table.
The syntax you would use to run WSUSutil.exe with specific commands follows the table.

Command	What it enables you to do	When you might use it
export	The first of the two parts that make up the export / import process. The **export** command enables you to export update metadata to an export package file. You cannot use this parameter to export update files, update approvals, or server settings.	• On an ongoing basis, if you are running a network with limited or restricted Internet connectivity
import	The second of the two parts that make up the export/import process. The **import** command imports update metadata to a server from an export package file created on another WSUS server. This synchronizes the destination WSUS server without using a network connection.	• On an ongoing basis, if you are running a network with limited or restricted connectivity
migratesus	This command migrates update approvals from a SUS 1.0 server to a WSUS server.	• If you are upgrading your implementation SUS 1.0 to WSUS.
moveconten t	Changes the file system location where the WSUS server stores update files, and optionally copies any update files from the old location to the new location	• Hard drive is full • Disk fails
reset	Checks that every update metadata row in the database has corresponding update files stored in the file system. If update files are missing or have been corrupted, WSUS downloads the update files again.	• After restoring the WSUS database. • When troubleshooting

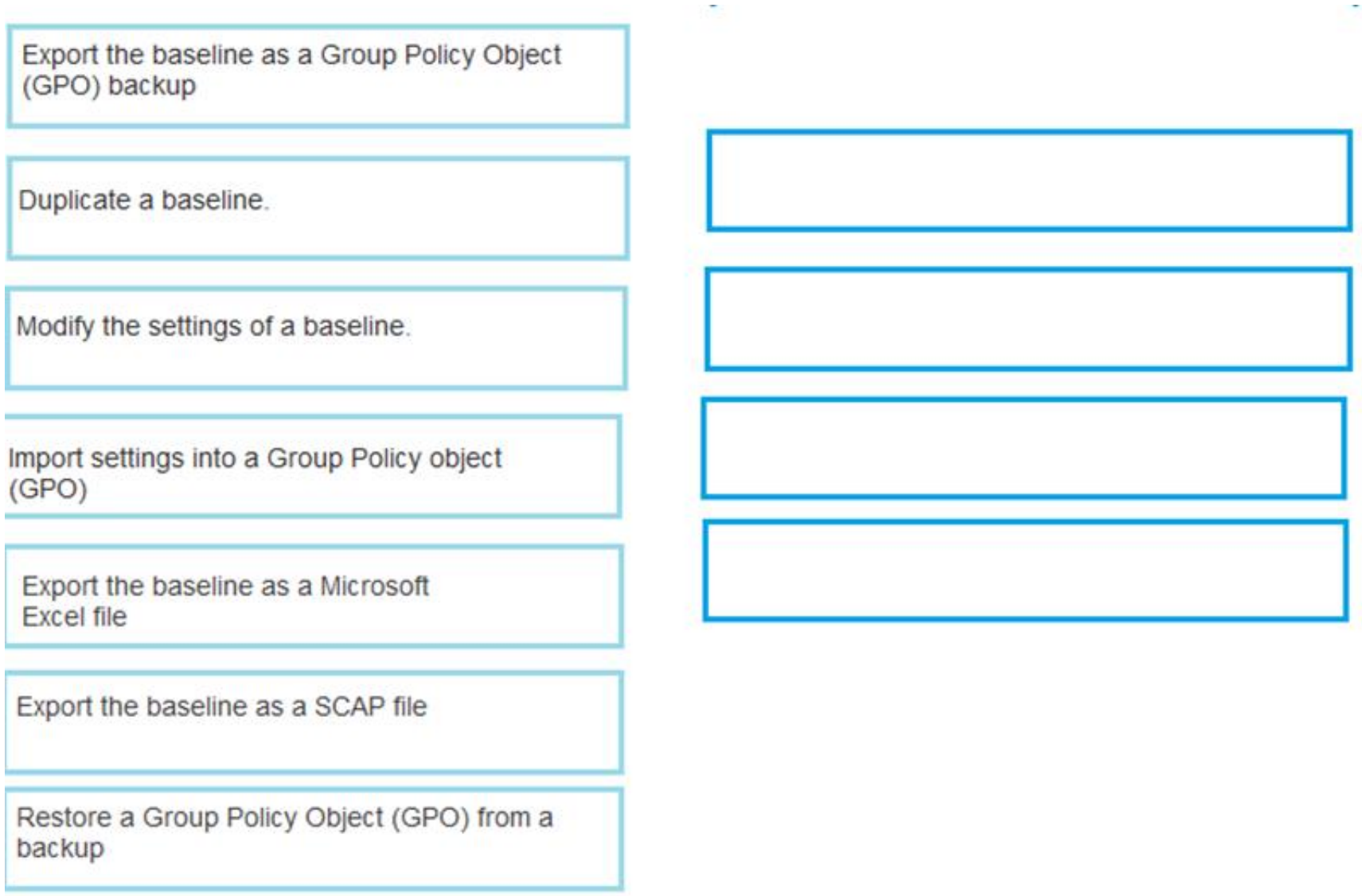
NEW QUESTION 66
Your network contains an Active Directory domain named contoso.com.
The domain contains a member server named Servers that runs Windows Server 2016. You need to configure Servers as a Just Enough Administration (JEA) endpoint.
Which two actions should you perform? Each correct answer presents part of the solution.

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

Answer: CE

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

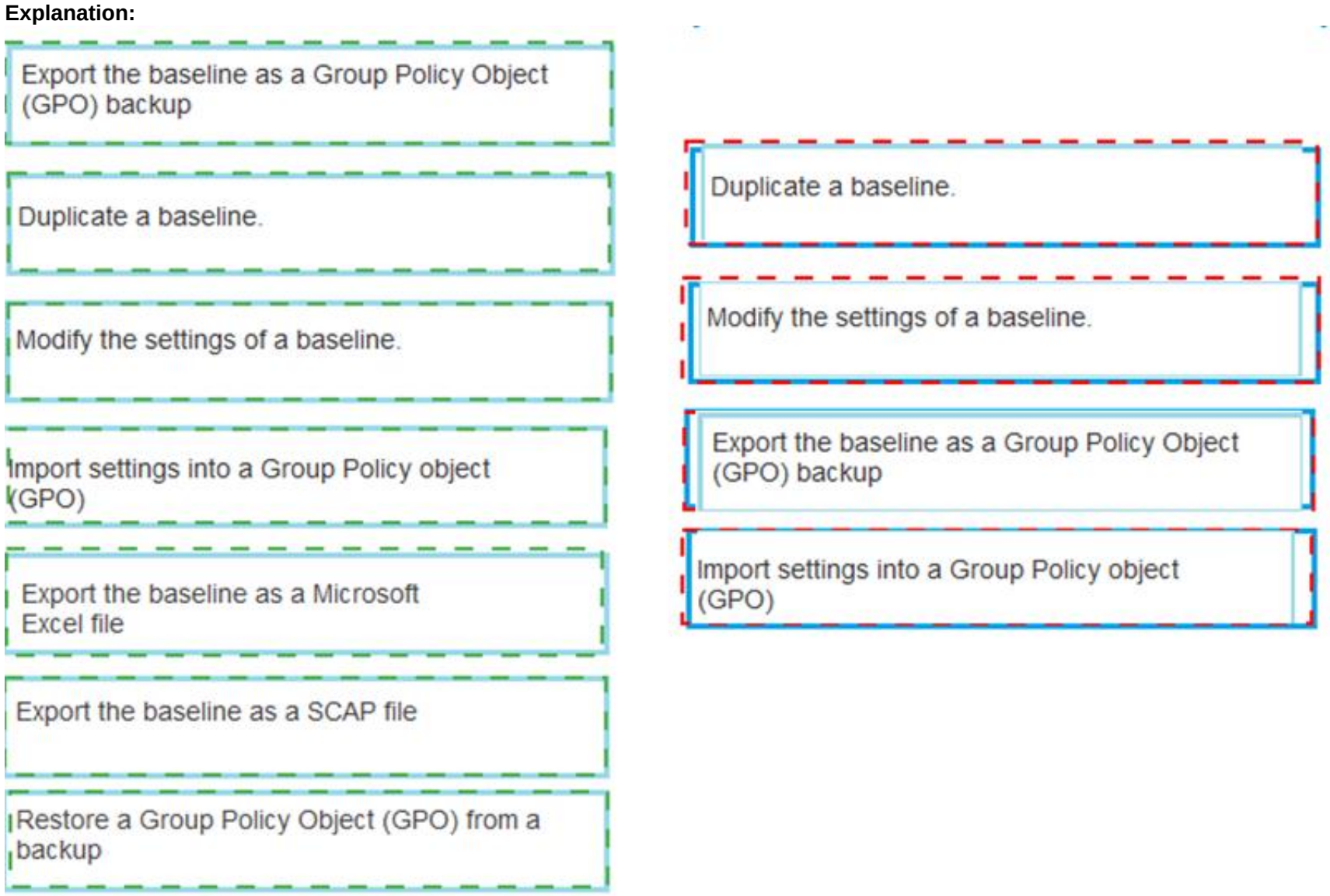
NEW QUESTION 67
DRAG DROP
Your network contains an Active Directory domain.
You install Security Compliance Manager (SCM) 4.0 on a server that runs Windows Server 2016. You need to modify a baseline, and then make the baseline available as a domain policy.
Which four actions should you perform in sequence?



A. Mastered
B. Not Mastered

Answer: A

Explanation:



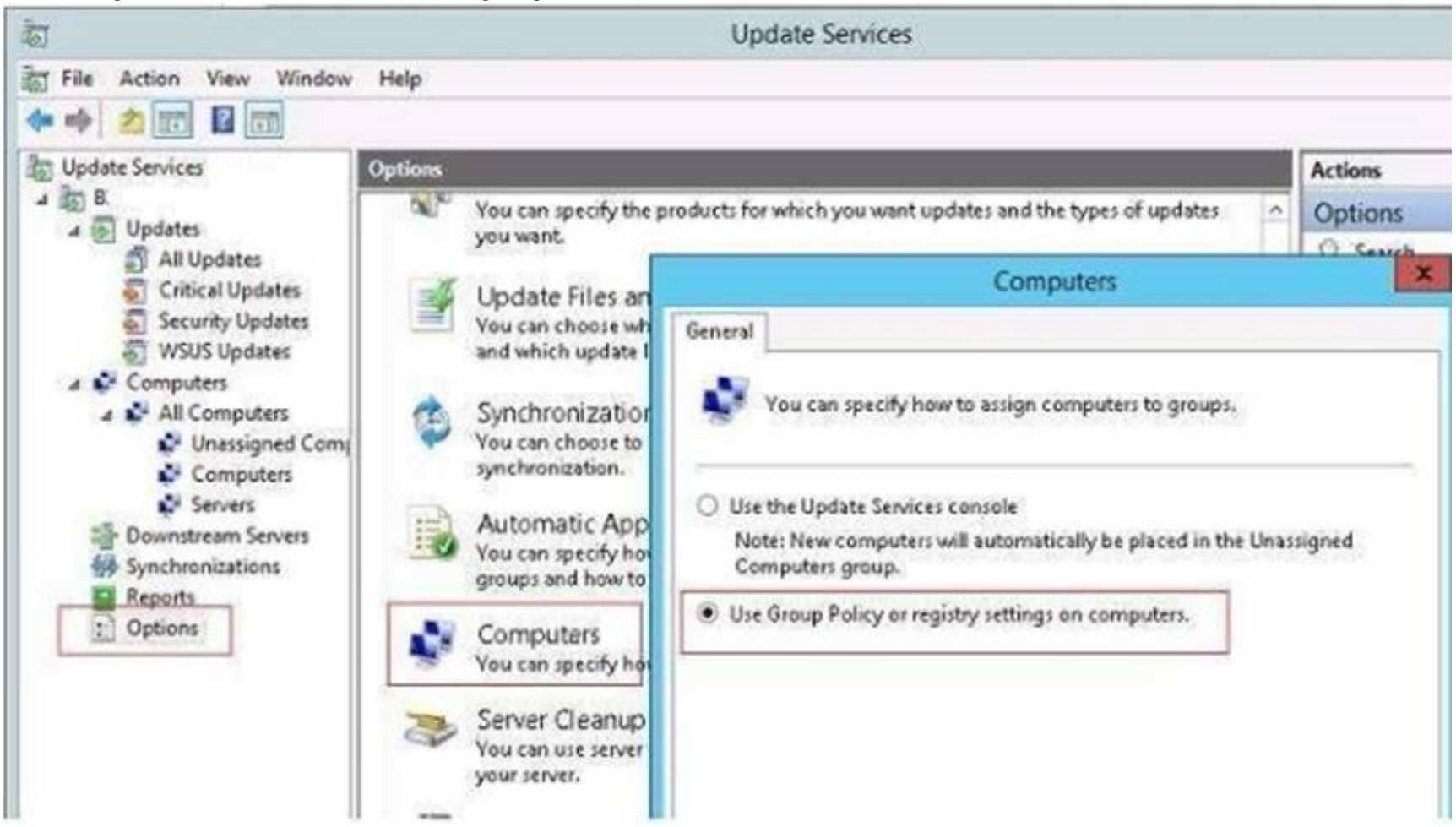
NEW QUESTION 69
Your network contains an Active Directory domain.
The domain contains two organizational units (OUs) named ProdOU and TestOU.
All production servers are in ProdOU. All test servers are in TestOU. A server named Server1 is in TestOU.
You have a Windows Server Update Services (WSUS) server 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?

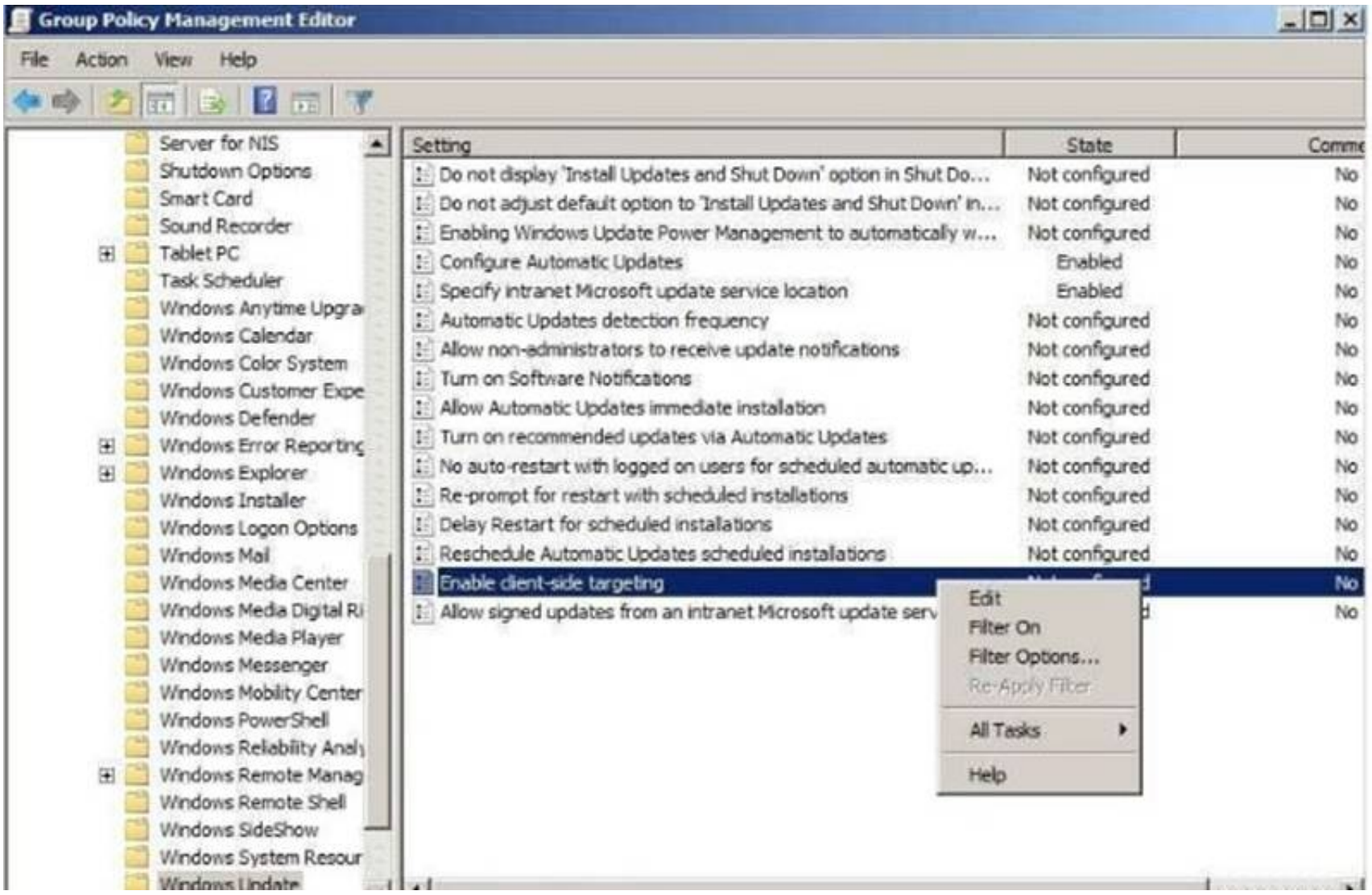
A. Turn off auto-restart for updates during active hours by using Group Policy objects (GPOs).
B. Configure client-side targeting by using Group Policy objects (GPOs).
C. Create computer groups by using the Update Services console.
D. Run wuauclt.exe /detectnow on each server after the server is moved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

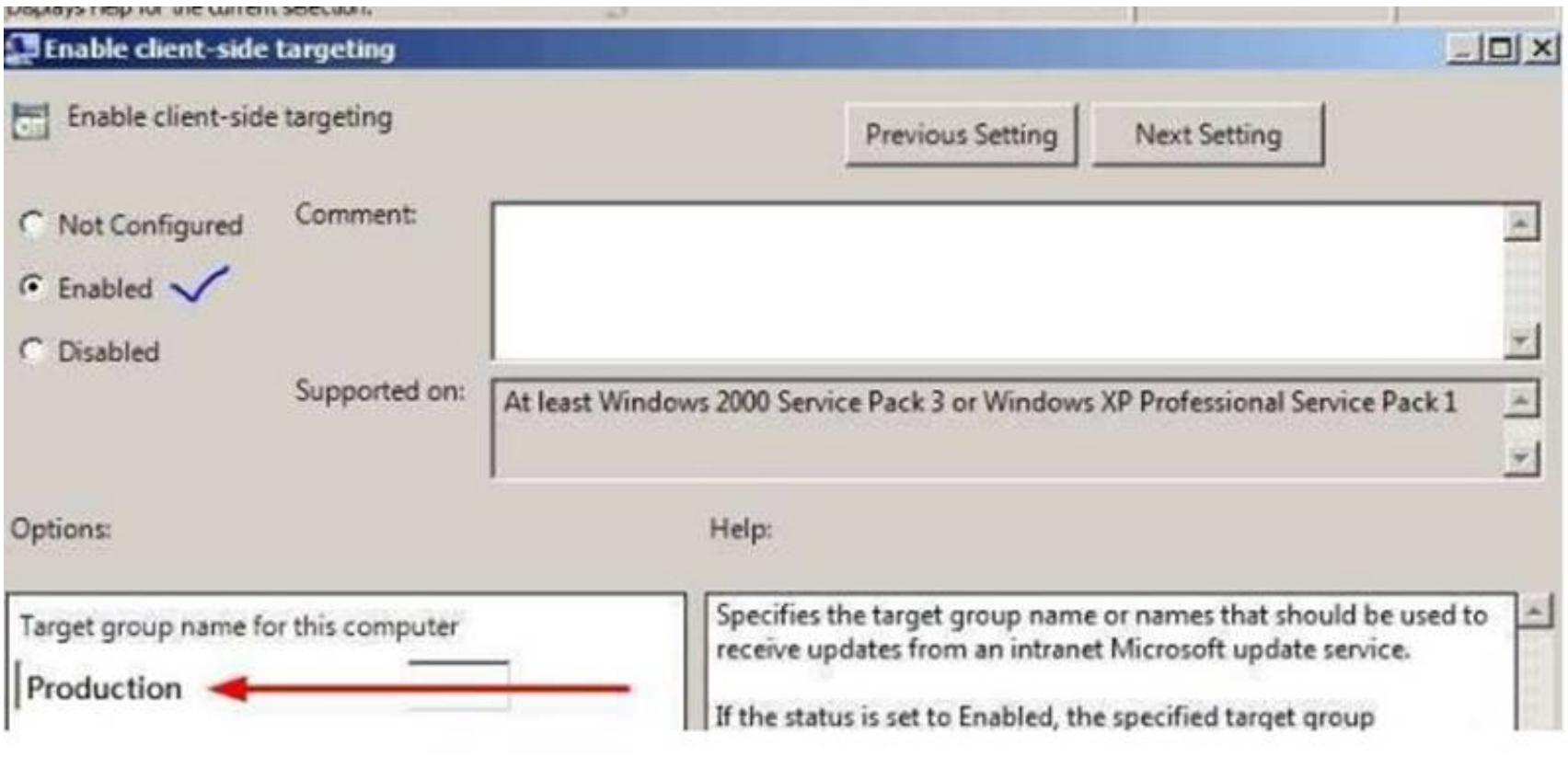
Answer: B

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 73
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 77
Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2. The domain contains the servers configured as shown in the following table.

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

You have an organizational unit (OU) named Marketing that contains the computers in the marketing department.
You have an OU named Finance that contains the computers in the finance department. You have an OU named AppServers that contains application servers.
A Group Policy object (GPO) named GP1 is linked to the Marketing OU. A GPO named GP2 is linked to the AppServers OU.
You install Windows Defender on Nano1.
You need to configure Nano1 as a Hyper-V Host. Which command should you run?

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

Answer: E

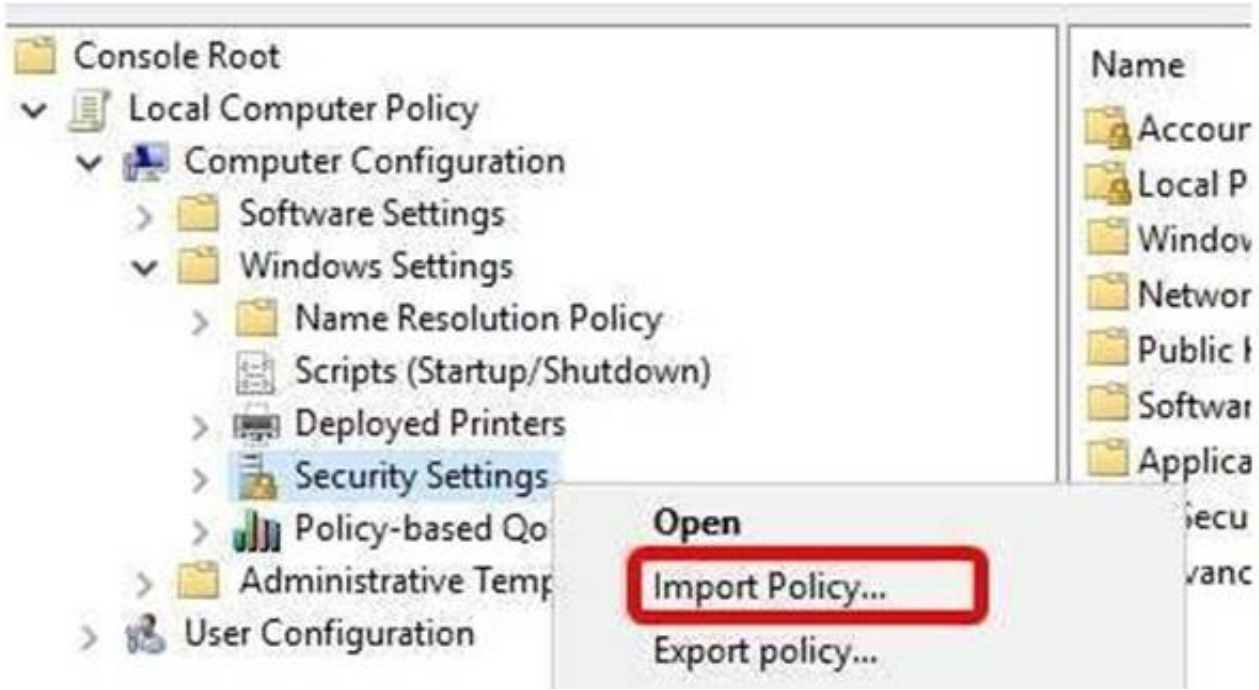
Explanation:
https://docs.microsoft.com/en-us/windows-server/get-started/deploy-nano-server#BKMK_online The Nano Server package “Microsoft-NanoServer-Compute-Package” includes the Hyper-V role for a Nano
Server host.
Moreover, the Install-WindowsFeature or Add-WindowsFeature cmdlet are NOT available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

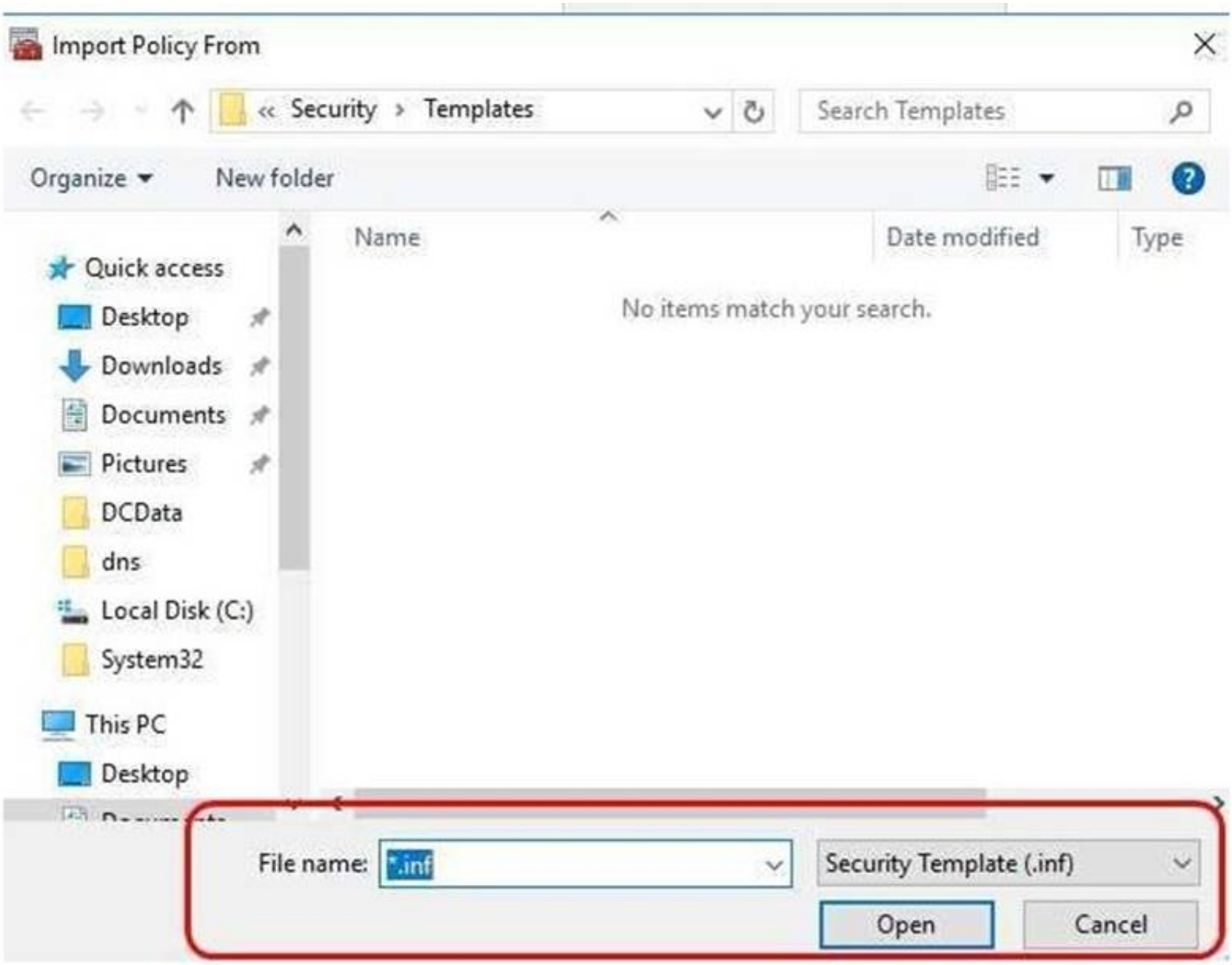
NEW QUESTION 78
Your network contains an internal network and a perimeter network. The internal network contains an Active Directory forest named contoso.com.
You deploy five servers to the perimeter network.
All of the servers run Windows Server 2016 and are the members of a workgroup.
You need to apply 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



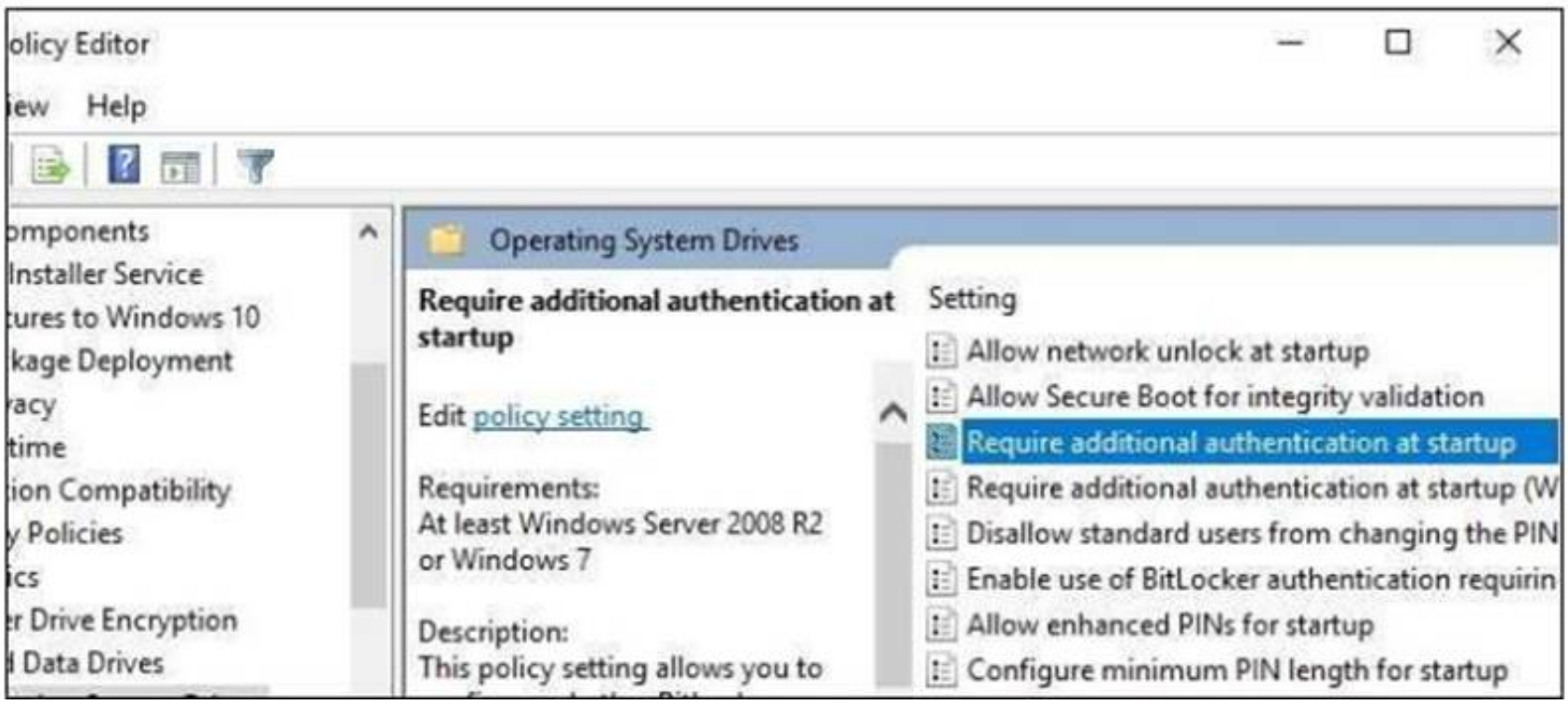


NEW QUESTION 80
You have a Hyper-V host named Server1 that runs Windows Server 2016. Server1 has a generation 2 virtual machine named VM1 that runs Windows 10.
You need to ensure that you can turn on BitLocker Drive Encryption (BitLocker) for drive C: on VM1. What should you do?

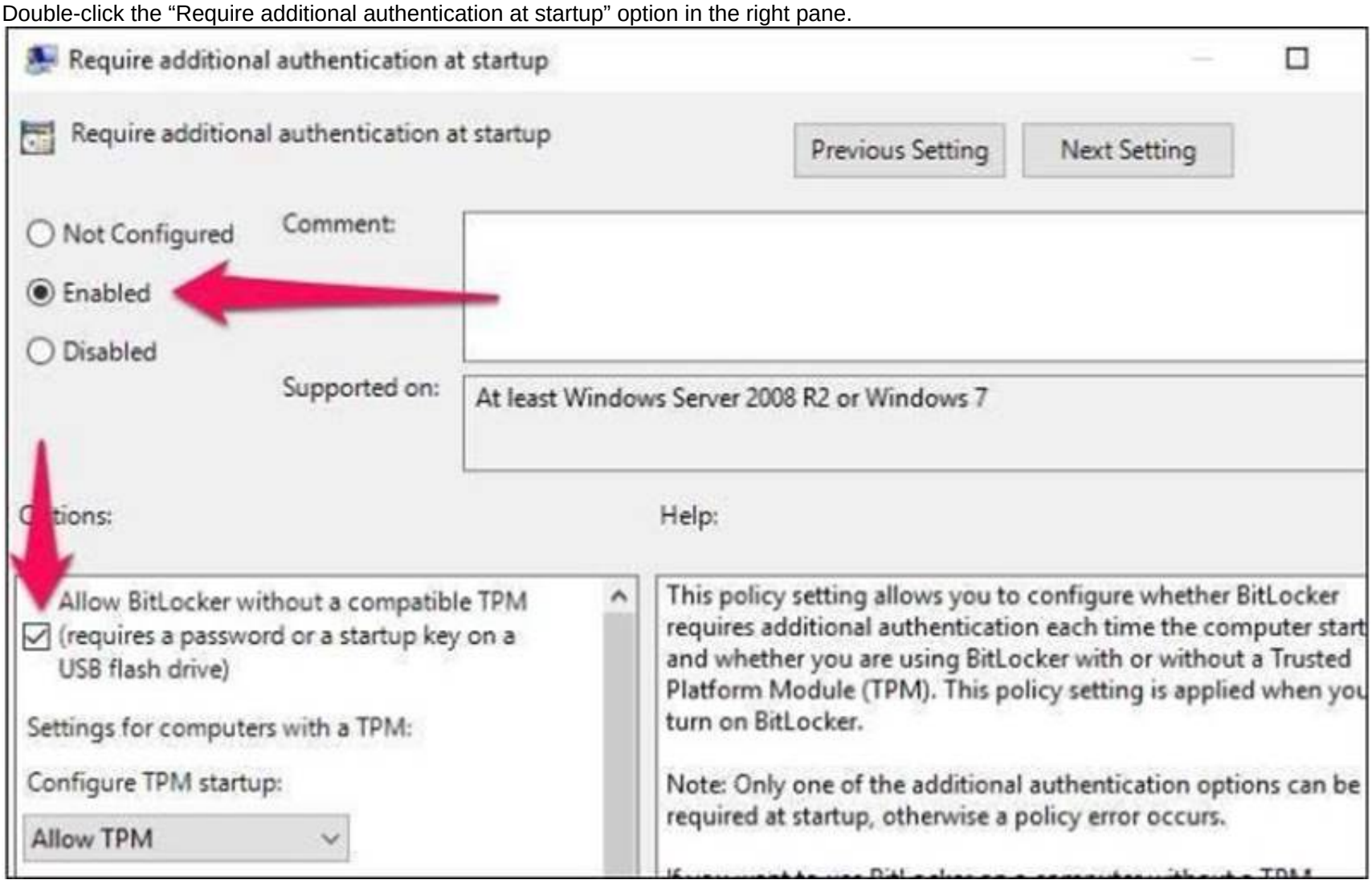
A. From Server1, install the BitLocker feature.
B. From Server1, enable nested virtualization for VM1.
C. From VM1, configure the Require additional authentication at startup Group Policy setting.
D. From VM1, configure the Enforce drive encryption type on fixed data drives Group Policy settin

Answer: C

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



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



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

NEW QUESTION 81
Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1 that runs Windows Server 2016.Server1 has a shared folder named Share1. You plan to create a subfolder in Share1 for each domain user.
You need to limit each user to using 100 MB of data in their respective subfolder.
The solution must enable the users to be notified when they use 80 percent of the available space in the subfolder.
Which tool should you use?

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

Answer: H

NEW QUESTION 84
You have a guarded fabric and a Host Guardian Service server named HGS1.
You deploy a Hyper-V host named Hyper1, and configure Hyper1 as part of the guarded fabric. You plan to deploy the first shielded virtual machine. You need to ensure that you can run the virtual machine on Hyper1.
What should you do?

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

Answer: A

Explanation:
https://blogs.technet.microsoft.com/datacentersecurity/2016/06/06/step-by-step-creating-shieldedvms- withoutvmm/
The first step is to get the HGS guardian metadata from the HGS server, and use it to create the Key protector.
To do this, run the following PowerShell command
on a guarded host or any machine that can reach the HGS server:
Invoke-WebRequest http://<HGSServer">FQDN>/KeyProtection/service/metadata/2014- 07/metadata.xml –
OutFile C:\\HGSGuardian.xml Shield the VM
Each shielded VM has a Key Protector which contains one owner guardian, and one or more HGS guardians.
The steps below illustrate the process of getting the guardians, create the Key Protector in order to shield the VM.
Run the following cmdlets on a tenant host “Hyper1”:
SVM is the VM name which to be shielded
$VMName = ‘SVM’
Turn off the VM first. You can only shield a VM when it is powered off Stop-VM –VMName $VMName
Create an owner self-signed certificate
$Owner = New-HgsGuardian –Name ‘Owner’ –GenerateCertificates
Import the HGS guardian
$Guardian = Import-HgsGuardian -Path ‘C:\\HGSGuardian.xml’ -Name ‘TestFabric’ – AllowUntrustedRoot
Create a Key Protector, which defines which fabric is allowed to run this shielded VM
$KP = New-HgsKeyProtector -Owner $Owner -Guardian $Guardian -AllowUntrustedRoot
Enable shielding on the VM
Set-VMKeyProtector –VMName $VMName –KeyProtector $KP.RawData
Set the security policy of the VM to be shielded
Set-VMSecurityPolicy -VMName $VMName -Shielded $true
Enable vTPM on the VM
Enable-VMTPM -VMName $VMName

NEW QUESTION 86
You have a server named Server1 that runs Windows Server 2016. You configure Just Enough Administration (JEA) on Server1.
You need to view a list of commands that will be available to a user named User1 when User1 establishes a JEA session to Server1.
Which cmdlet should you use?

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

Answer: B

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

NEW QUESTION 91
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:

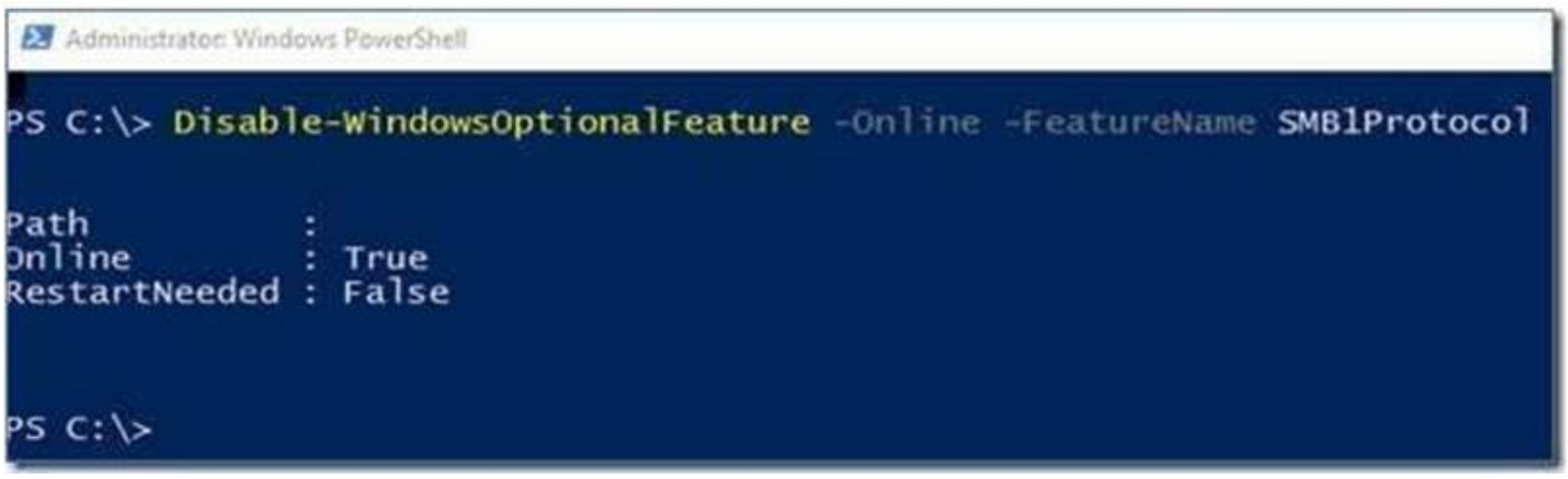
Profile	Description
Domain	Applied to a network adapter when it is connected to a network on which it can detect a domain controller of the domain to which the computer is joined.
Private	Applied to a network adapter when it is connected to a network that is identified by the user or administrator as 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 96
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. You need to prevent NTLM authentication on Server1.
Solution: From Windows PowerShell, you run the Disable-WindowsOptionalFeature cmdlet. Does this meet the goal?

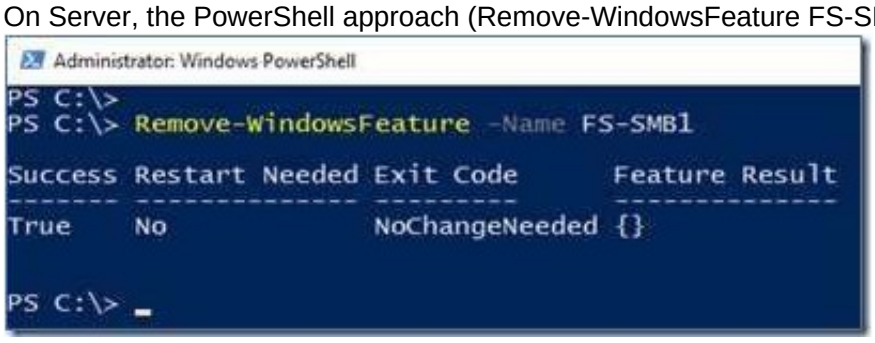
A. Yes
B. No

Answer: B

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



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



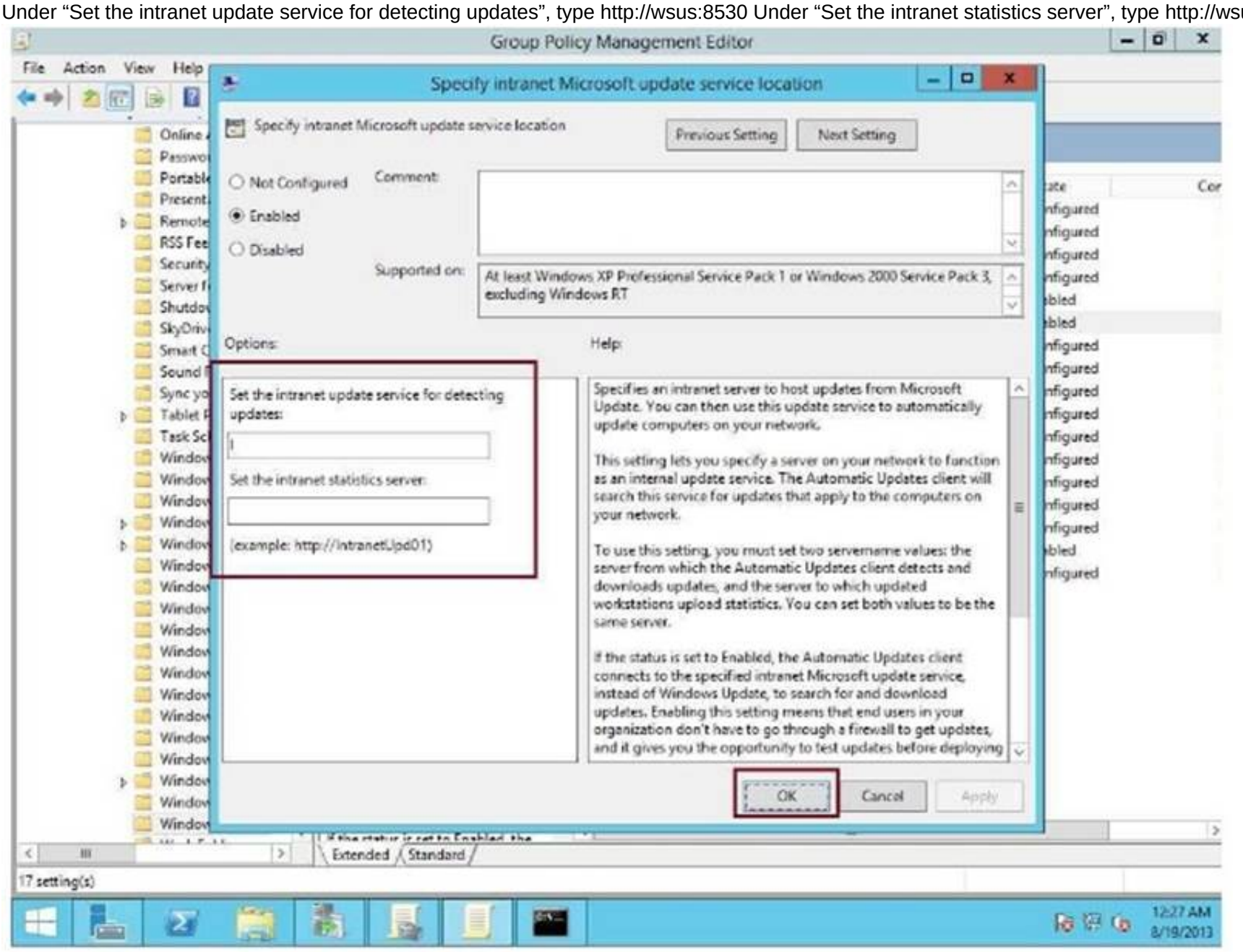
Even if SMB1 is removed, SMB2 and SMB3 could still run NTLM authentication! Therefore, answer is a“NO”.

NEW QUESTION 98
Your network contains an Active Directory domain named contoso.com.The domain contains 1,000 client computers that run either Windows 8.1 or Windows 10.
You have a Windows Server Update Services (WSUS) deployment All client computers receive updates from WSUS.
You deploy a new WSUS server named WSUS2.
You need to configure all of the client computers that run Windows 10 to send WSUS reporting data to WSUS2.
What should you configure?

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

Answer: C

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



NEW QUESTION 100
You have a server named Server1 that runs Windows Server 2016.
You need to identify the default action for the inbound traffic when Server1 connects to the domain. Which cmdlet should you use?

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

Answer: C

NEW QUESTION 104
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 105
HOTSPOT
You have a Hyper-V host named Server1 that runs Windows Server 2016. A new security policy states that all the virtual machines must be encrypted.
Server1 hosts the virtual machines configured as shown in the following table.

Name	Operating system	Virtual machine generation	Virtual machine configuration version
VM1	Windows Server 2012 R2 Standard	Generation 2	7.0
VM2	Windows Server 2012 R2 Datacenter	Generation 1	7.1
VM3	Windows Server 2016 Standard	Generation 2	5.0

An administrator runs the following commands. Get -VM | Stop-VM
Get -VM | Update-VMVersion Get -VM | Start-VM
For each of the following statements, Select Yes, if the statement is true. Otherwise Select No.

Statements	Yes	No
You can configure VM1 as an encryption-supported virtual machine.	○	○
You can configure VM2 as an encryption-supported virtual machine.	○	○
You can configure VM3 as an encryption-supported virtual machine.	○	○

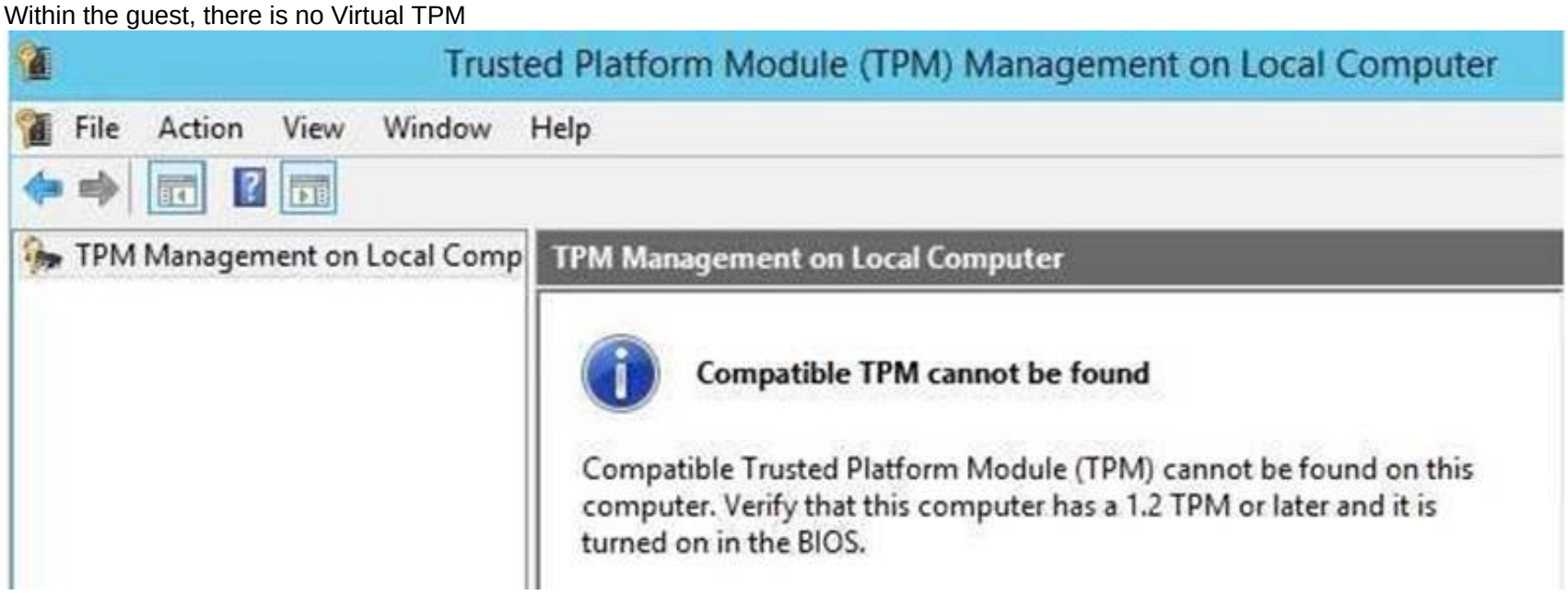
A. Mastered
B. Not Mastered

Answer: A

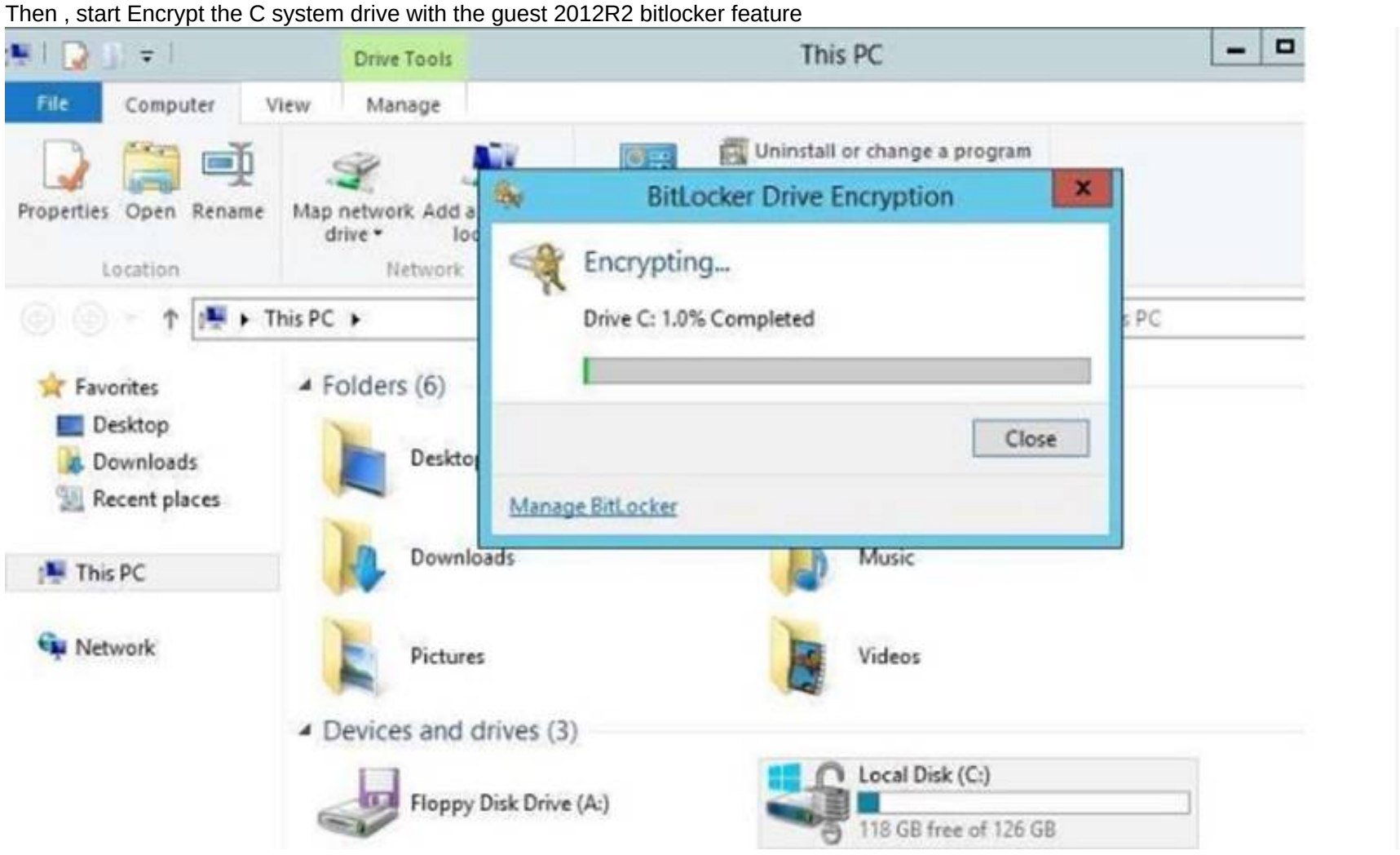
Explanation:
After the “Update-VMVersion” is executed against all three virtual machines, they become:- VM1 Generation 2 Version 8
VM2 Generation 1 Version 8
VM3 Generation 2 Version 8
Pay attention to VM2, and the question has not mention to use TPM protector. You can configure this VM as Encryption Supported by using a Key Storage Drive added to the virtual machine setting.

```
PS C:\WINDOWS\system32> Get-VM | FL


Name              : 2012R2_G1_v8
State             : Off
CpuUsage          : 0
MemoryAssigned    : 0
MemoryDemand      : 0
MemoryStatus      :
Uptime            : 00:00:00
Status            : □□□□
ReplicationState  : Disabled
Generation        : 1



PS C:\WINDOWS\system32> Get-VM | Get-VMKeyStorageDrive


ControllerLocation : 1
ControllerNumber   : 0
ControllerType     : IDE
Name               : □□ on IDE controller number 0 at location 1
Path               :
PoolName           :
Id                 : Microsoft:824779CC-3D03-4A5E-B324-F7CF518F5C5E\83F8638B-8DCA-4152-9EDA-2CA883303984\0\1\D
VMId               : 824779cc-3d03-4a5e-b324-f7cf518f5c5e
VMName             : 2012R2_G1_v8
VMSnapshotId       : 00000000-0000-0000-0000-000000000000
VMSnapshotName     :
CimSession         : CimSession: .
ComputerName       : TIGERPOWERBOOK
IsDeleted          : False
VMCheckpointId     : 00000000-0000-0000-0000-000000000000
VMCheckpointName   :


PS C:\WINDOWS\system32> _
```

Within the guest, there is no Virtual TPM



Then , start Encrypt the C system drive with the guest 2012R2 bitlocker feature



After the encryption is completed:-

NEW QUESTION 108
Your network contains an Active Directory forest named contoso.com. The forest functional level is Windows Server 2012.
The forest contains 20 member servers that are configured as file servers. All domain controllers run Windows Server 2016.
You create a new forest named contosoadmin.com.
You need to use the Enhanced Security Administrative Environment (ESAE) approach for the administration of the resources in contoso.com.
Which two actions should you perform? Each correct answer presents part of the solution.

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

Answer: AC

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

NEW QUESTION 109
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 111
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 112
The Job Title attribute for a domain user named User1 has a value of Sales Manager. User1 runs whoami /claims and receives the following output:

USER CLAIMS INFORMATION				
Claim Name	Claim ID	Flags	Type	Values
"Country"	ad://ext/Country:88d469316297e518		String	"US"
Kerberos support for Dynamic Access Control on this device has been disabled.				

Kerberos support for Dynamic Access Control on this device has been disabled.
You need to ensure that the security token of User1 has a claim for Job Title. What should you do?

A. From Windows PowerShell, run the New-ADClaimTransformPolicy cmdlet and specify the -Name parameter
B. From Active Directory Users and Computers, modify the properties of the User1 account.
C. From Active Directory Administrative Center, add a claim type.
D. From a Group Policy object (GPO), configure KDC support for claims, compound authentication, and Kerberos armoring.

Answer: C

Explanation:
From the output, obviously, a claim type is missing (or disabled) so that the domain controller is not issuing
tickets with the "Job Title" claim type.

NEW QUESTION 116
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
```

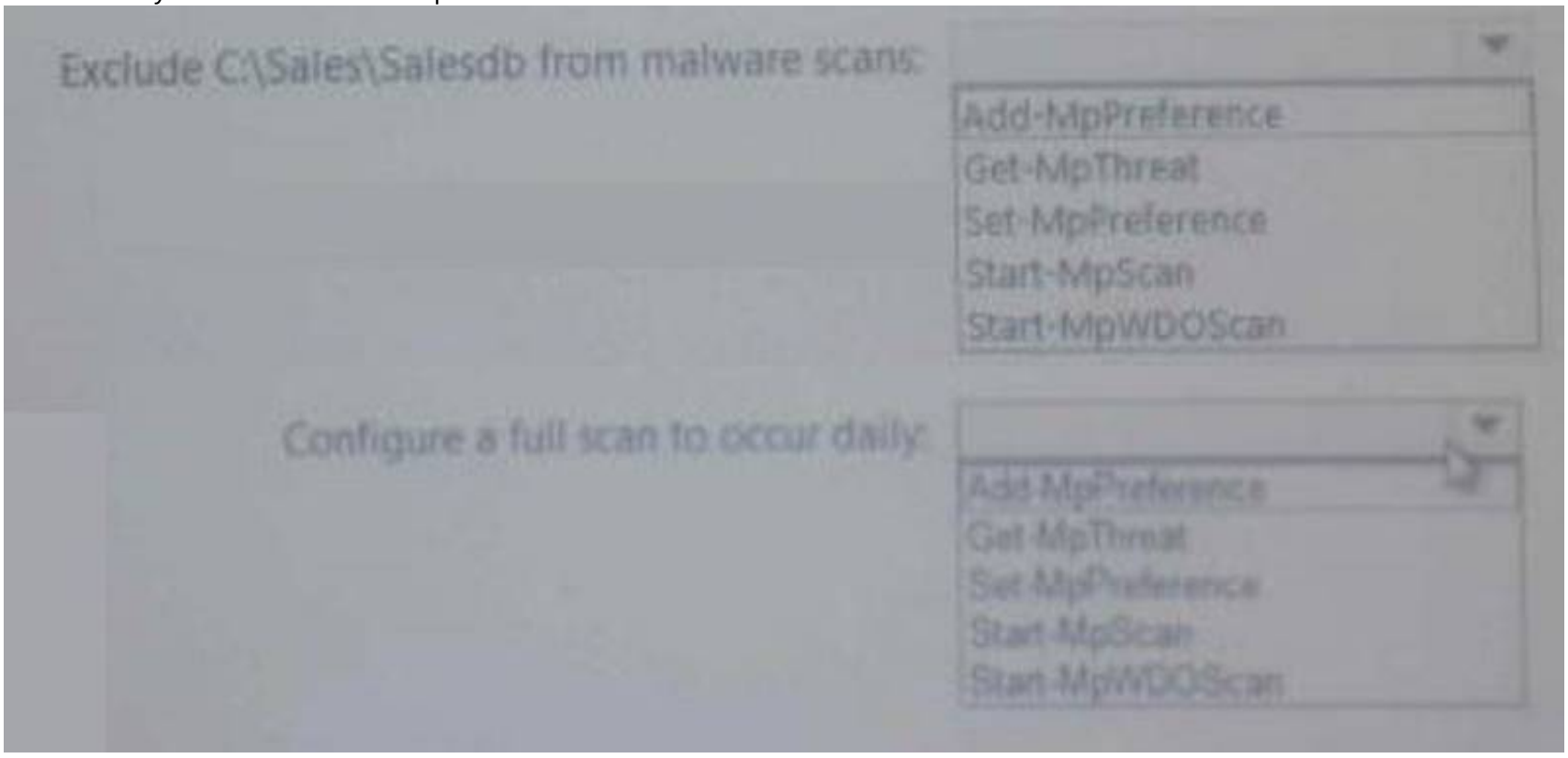
NEW QUESTION 118
Your network contains several secured subnets that are disconnected from the Internet.
One of the secured subnets contains a server named Server1 that runs Windows Server 2016.
You implement Log Analytics in Microsoft Operations Management Suite (OMS) for the servers that connect to 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 121
HOTSPOT
You have 100 computers that run Windows 10 and are members of a workgroup. You need to configure Windows Defender to meet the following requirements:
-Exclude a C:\\Sales\\Salesdb from malware scans.
-Configure a full scan to occur daily.
What should you run to meet each requirement?



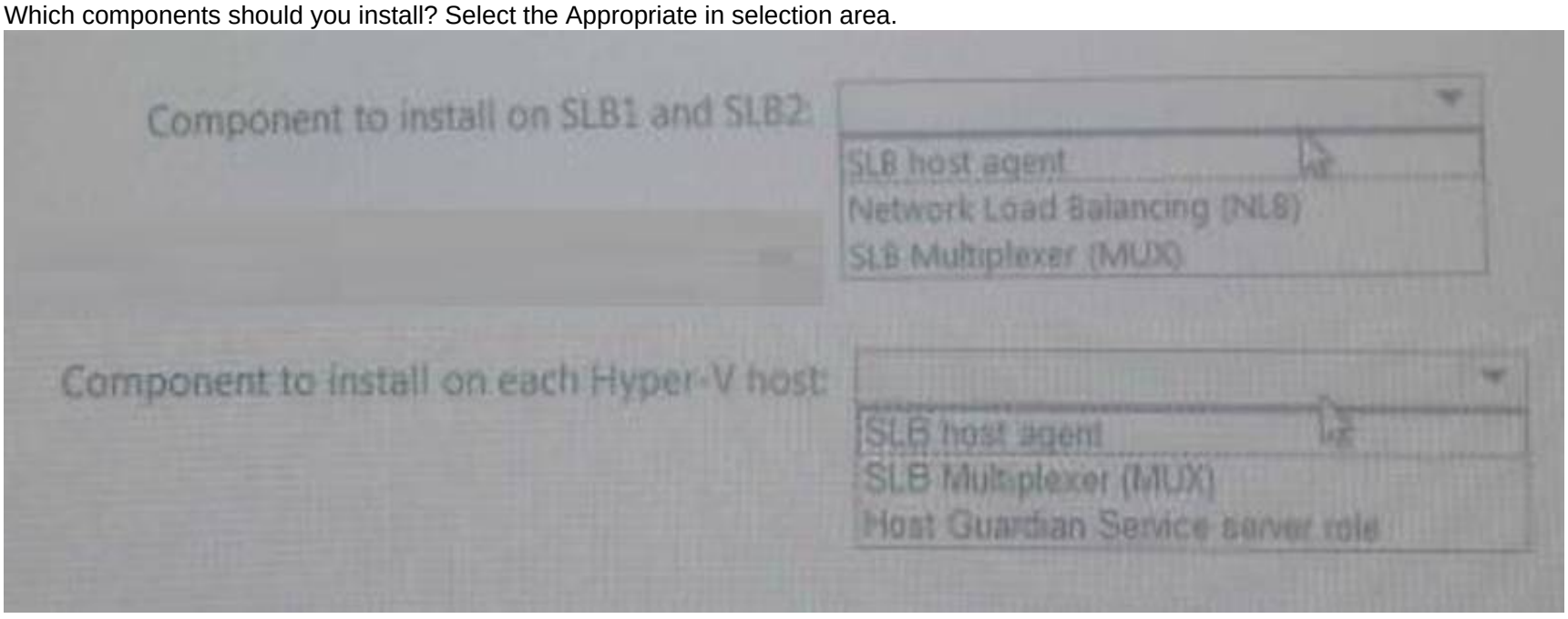
A. Mastered

B. Not Mastered

Answer: A

Explanation:
https://technet.microsoft.com/en-us/itpro/powershell/windows/defender/set-mppreference Set-MpPreference -ExclusionPath C:\\Sales\\Salesdb
Set-MpPreference -RemediationScheduleDay Everyday

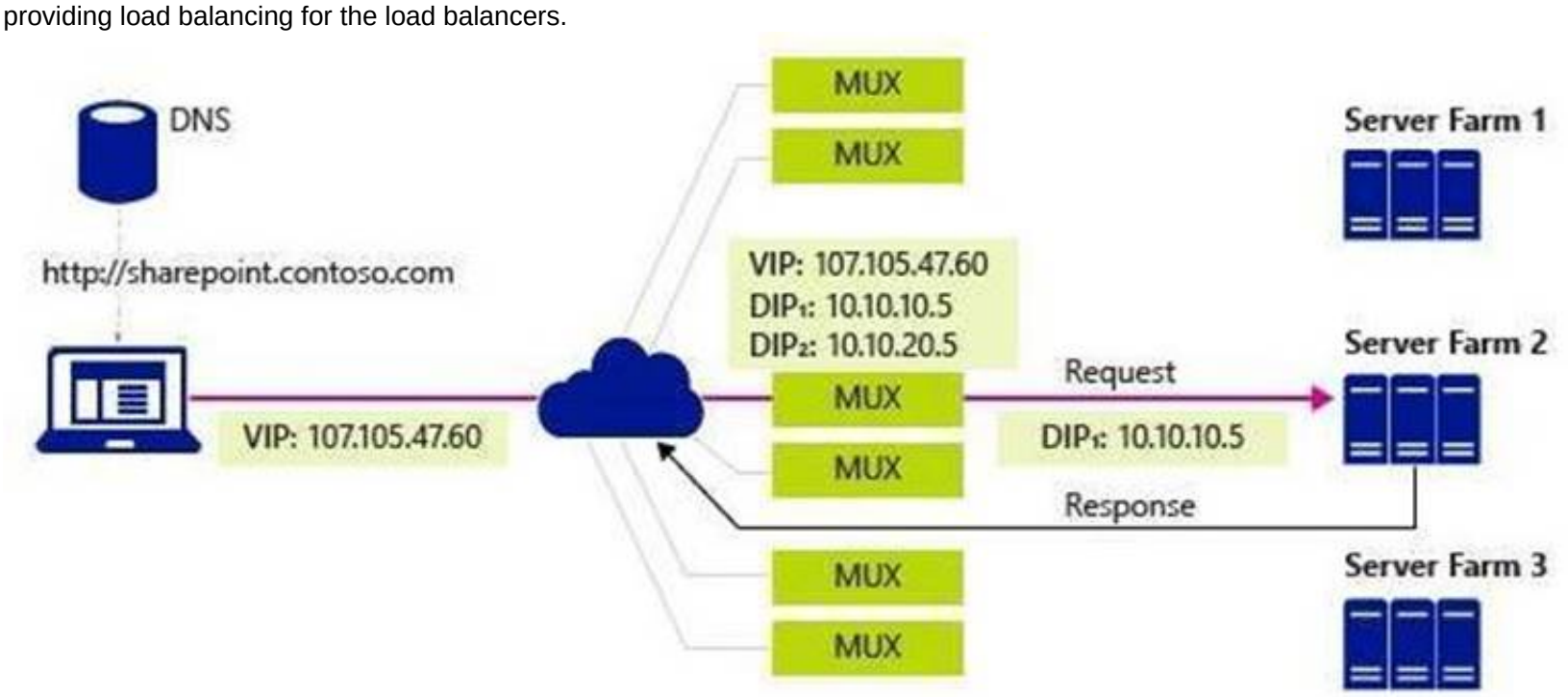
NEW QUESTION 126
HOTSPOT
You have 10 Hyper-V hosts that run Windows Server 2016.
Each Hyper-V host has eight virtual machines that run a distributed web application named App1. You plan to implement a Software Load Balancing (SLB) solution for client access to App1. You deploy two new virtual machines 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.



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.

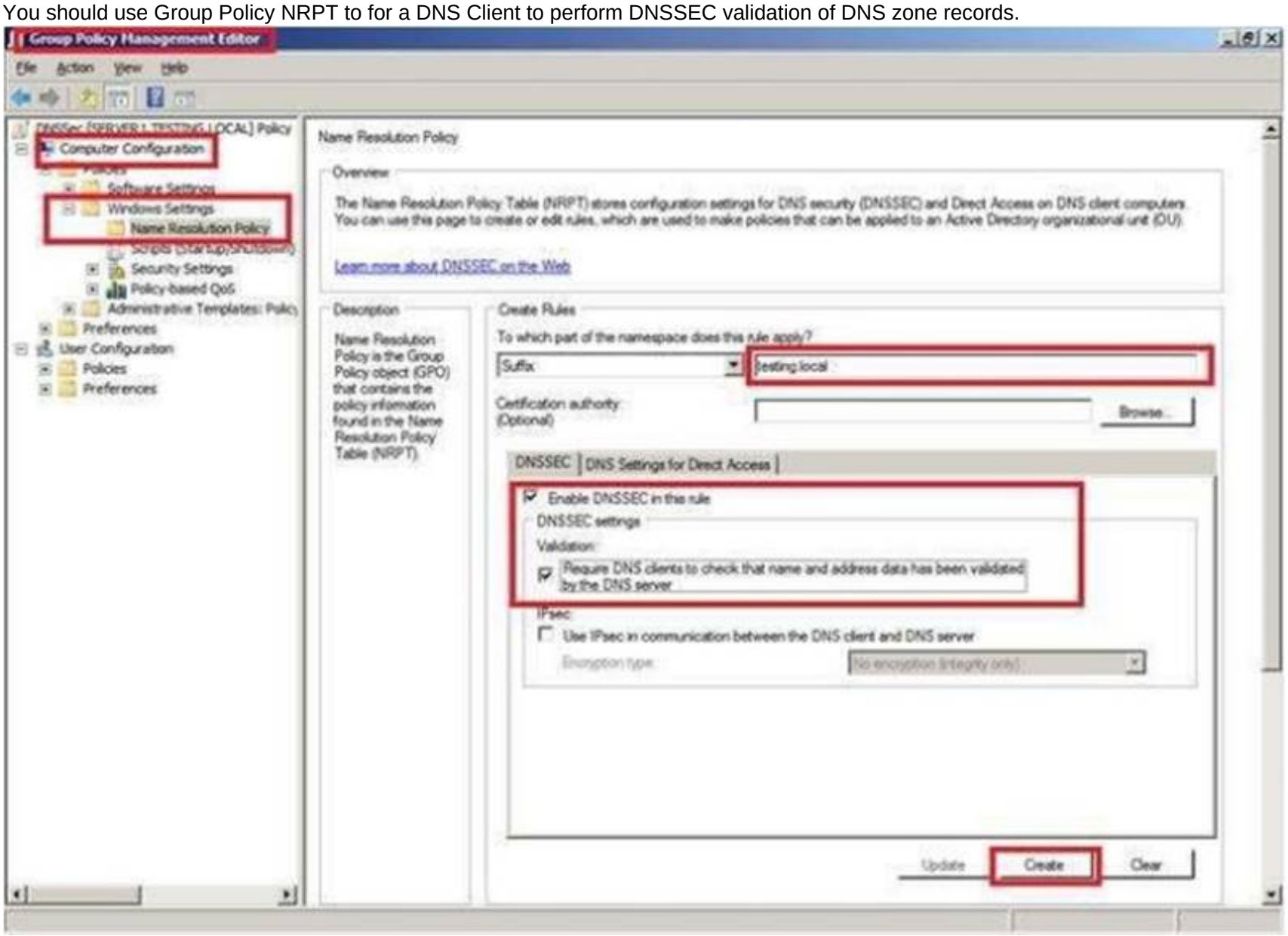


NEW QUESTION 128
Your network contains an Active Directory domain named contoso.com. The domain contains two DNS servers that run Windows Server 2016. The servers host two zones named contoso.com and admin.contoso.com. You sign both zones.
You need to ensure that all client computers in the domain validate the zone records when they query the zone.
What should you deploy?

A. a Microsoft Security Compliance Manager (SCM) policy
B. a zone transfer policy
C. a Name Resolution Policy Table (NRPT)
D. a connection security rule

Answer: C

Explanation:
You should use Group Policy NRPT to for a DNS Client to perform DNSSEC validation of DNS zone records.



NEW QUESTION 133
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 134
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. You need to prevent NTLM authentication on Server1.
Solution: From Windows PowerShell, you run the New-ADAuthenticationPolicy cmdlet. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 138
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. The network uses the 172.16.0.0/16 address space.
Computer1 has an application named App1.exe that is located in D:\\Apps\\. App1.exe is configured to accept connections on TCP port 8080.
You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.
Solution: You run the New-NetFirewallRule –DisplayName “Rule1” –Direction Inbound –LocalPort 8080 –Protocol TCP –Action allow –Profile Domain Command.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 141
You have a virtual machine named FS1 that runs Windows Server 2016. FS1 has the shared folders shown in the following table.

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 146
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You manage a file server that runs Windows Server 2016. The file server contains the volumes configured as shown in the following table.

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

You need to encrypt DevFiles by using BitLocker Drive Encryption (ButLocker). Solution: You run the manage-bde.exe command and specify the –on parameter. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

References:
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/managebde- on

NEW QUESTION 147
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.
You need to prevent NTLM authentication on Server1.
Solution: From a Group Policy, you configure the Kerberos Policy. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

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

NEW QUESTION 150
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. The domain has Dynamic Access Control enabled.

Server1 contains a folder named C:\Folder1. Folder1 is shared as Share1.
You need to audit all access to the contents of Folder1 from Server2. The solution must minimize the number of event log entries.
Which two audit policies should you enable on Server1? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: BE

Explanation:

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

NEW QUESTION 155
Your network contains an Active Directory domain named contoso.com.
The domain contains four global groups named Group1, Group2, Group3, and Group4. A user named User1 is a member of Group3.
You have an organizational unit (OU) named OU1 that contains computer accounts. A Group Policy object (GPO) named GPO1 is linked to OU1. OU1 contains a computer account named Computer1. GPO1 has the User Rights Assignment configured as shown in the following table.

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

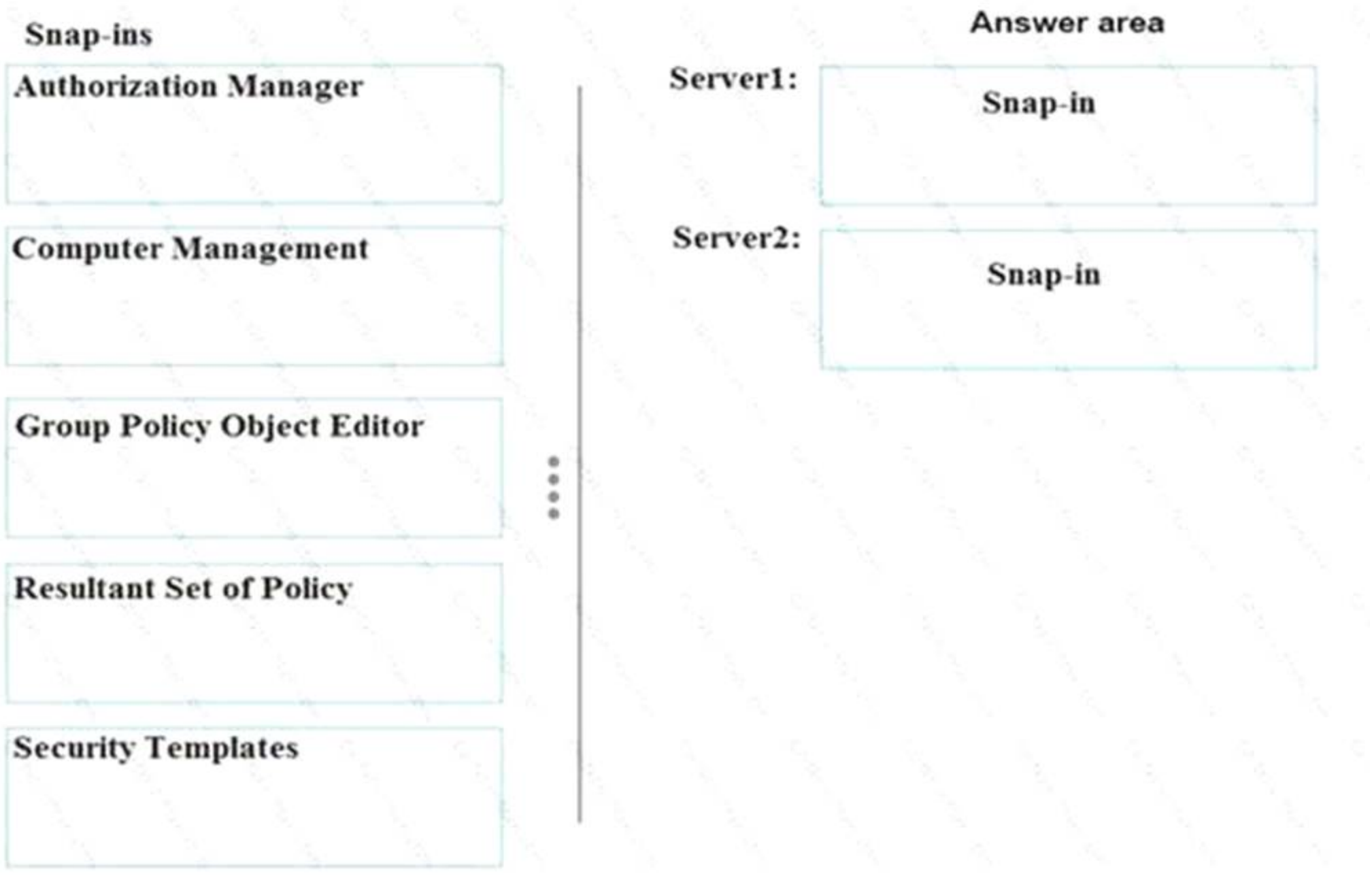
Answer: B

NEW QUESTION 156
Your network contains an Active Directory domain named contoso.com. The domain contains a certification authority (CA).
You need to implement code integrity policies and sign them by using certificates issued by the CA. You plan to use the same certificate to sign policies on multiple computers.
You duplicate the Code Signing certificate template and name the new template CodeIntegrity. How should you configure the CodeIntegrity template?

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

Answer: D

NEW QUESTION 161
DRAG DROP
You have two servers named Server1 and Server2 that run Windows Server 2016. The servers are in a workgroup.
You need to create a security template that contains the security settings of Server1 and to apply the template to Server2. The solution must minimize administrative effort.
Which snap-in should you use for each server? To answer, drag the appropriate snap-ins to the correct servers. Each snap-in may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 162
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 70-744 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 70-744 Product From:

https://www.2passeasy.com/dumps/70-744/

Money Back Guarantee

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