Exam Questions 70-744

Securing Windows Server 2016

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

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 section, you will NOT be able to return to It. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. Computer1 connects to a home network and a corporate network.
The corporate network uses the 172.16.0.0/24 address space internally. Computer1 runs an application named App1 that listens to port 8080.
You need to prevent connections to App1 when Computer1 is connected to the home network. Solution: From Group Policy Management, You create an Applocker rule.

A. Yes
B. No

Answer: B

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

NEW QUESTION 3
Note: This question is part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question In this section, you will NOT be able to return to It. As a result, these questions will not appear In the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains multiple Hyper-V hosts.
You need to deploy several critical line-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 a separate Windows container for each application. Does this meet the goal?
A. Yes
B. No

Answer: A

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

NEW QUESTION 4
Note: This question Is part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to It, As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains multiple Hyper-V hosts.
You need to deploy several critical line-to-business applications to the network to meet the following requirements:
*The resources of the applications must be isolated (rom the physical host.
*Each application must be prevented from accessing the resources of the other applications.
*The configurations of the applications must be accessible only from the operating system that hosts the application.
Solution: You deploy a separate Hyper-V container for each application. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

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

NEW QUESTION 5
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?

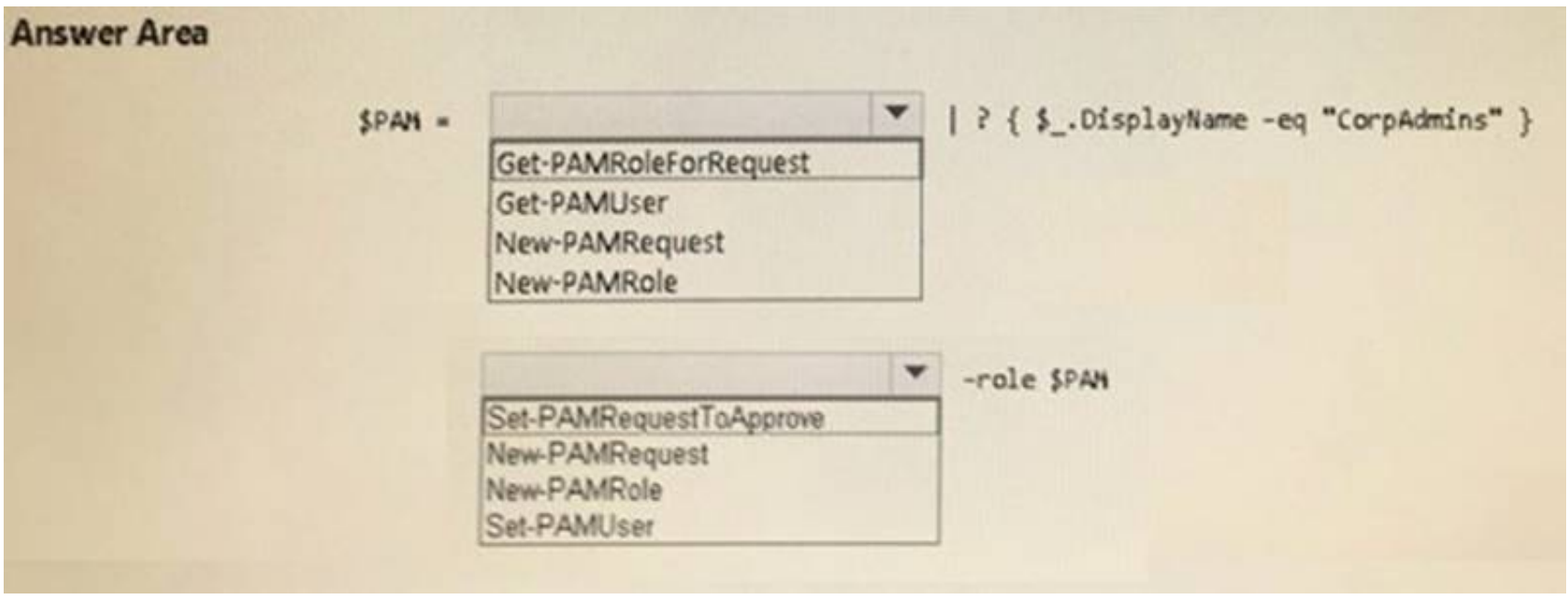
A. Instruct all users to sign in to a client computer by using a Microsoft account.
B. Move the computer accounts of all the client computers to a new organizational unit (OU). Remove the permissions to the new OU from the Domain Admins group.
C. Instruct all administrators to use a local Administrators 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 6
HOTSPOT
Your network contains an Active Directory forest named contoso.com. The forest has Microsoft Identity Manager (MIM) 2016 deployed. You implement Privileged Access Management (PAM).
You need to request privileged access from a client computer in contoso.com by using PAM.
How should you complete the Windows PowerShell script? To answer, select the appropriate options in the answer area.



A. Mastered
B. Not Mastered

Answer: A

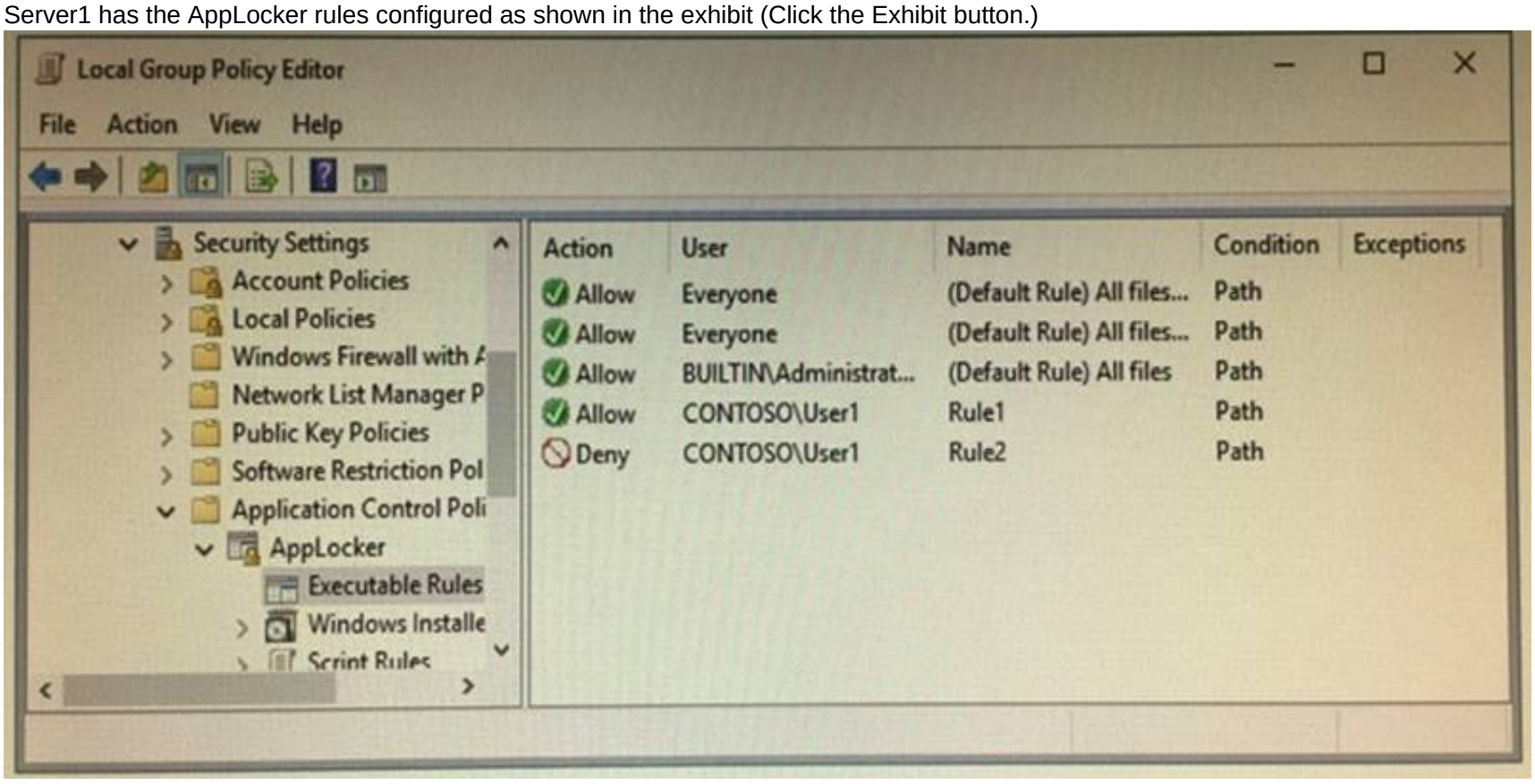
Explanation:
$PAM = Get-PAMRoleForRequest | ? {$_,DisplayName -eq “CorpAdmins” } New-PAMRequest -role $PAM
References:
https://technet.microsoft.com/en-us/library/mt604089.aspx https://technet.microsoft.com/en-us/library/mt604084.aspx

NEW QUESTION 7
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.
The services on Server1 are shown in the following output.

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

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

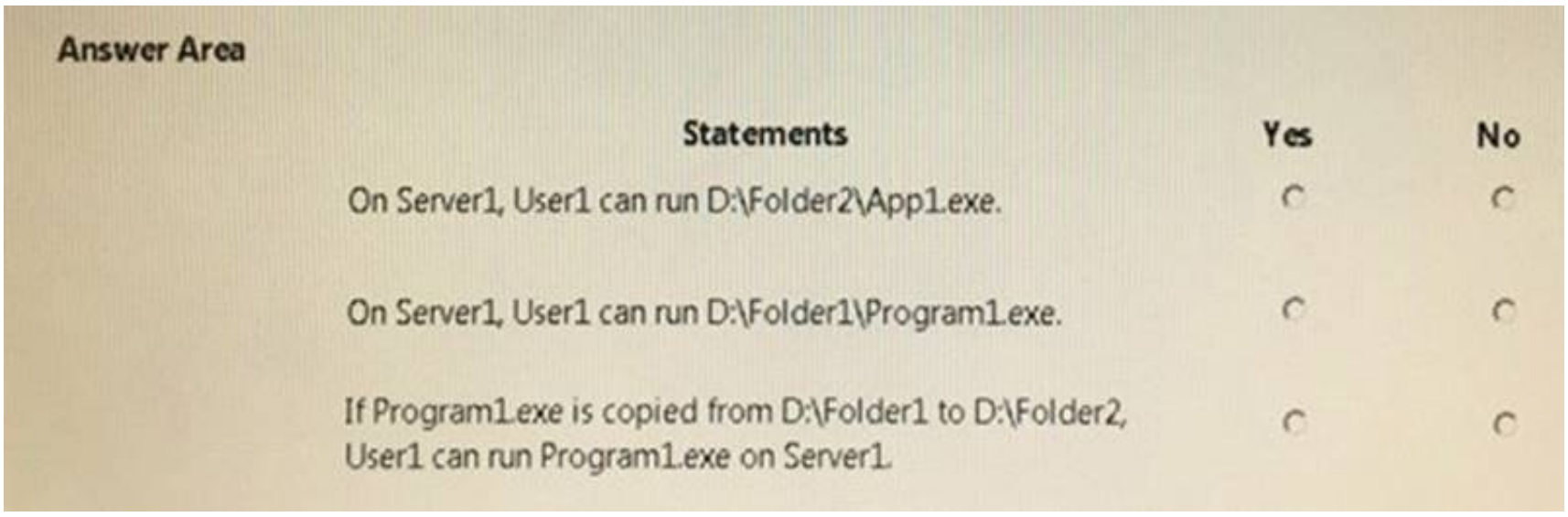
Server1 has the AppLocker rules configured as shown in the exhibit (Click the Exhibit button.)



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

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

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



A. Mastered
B. Not Mastered

Answer: A

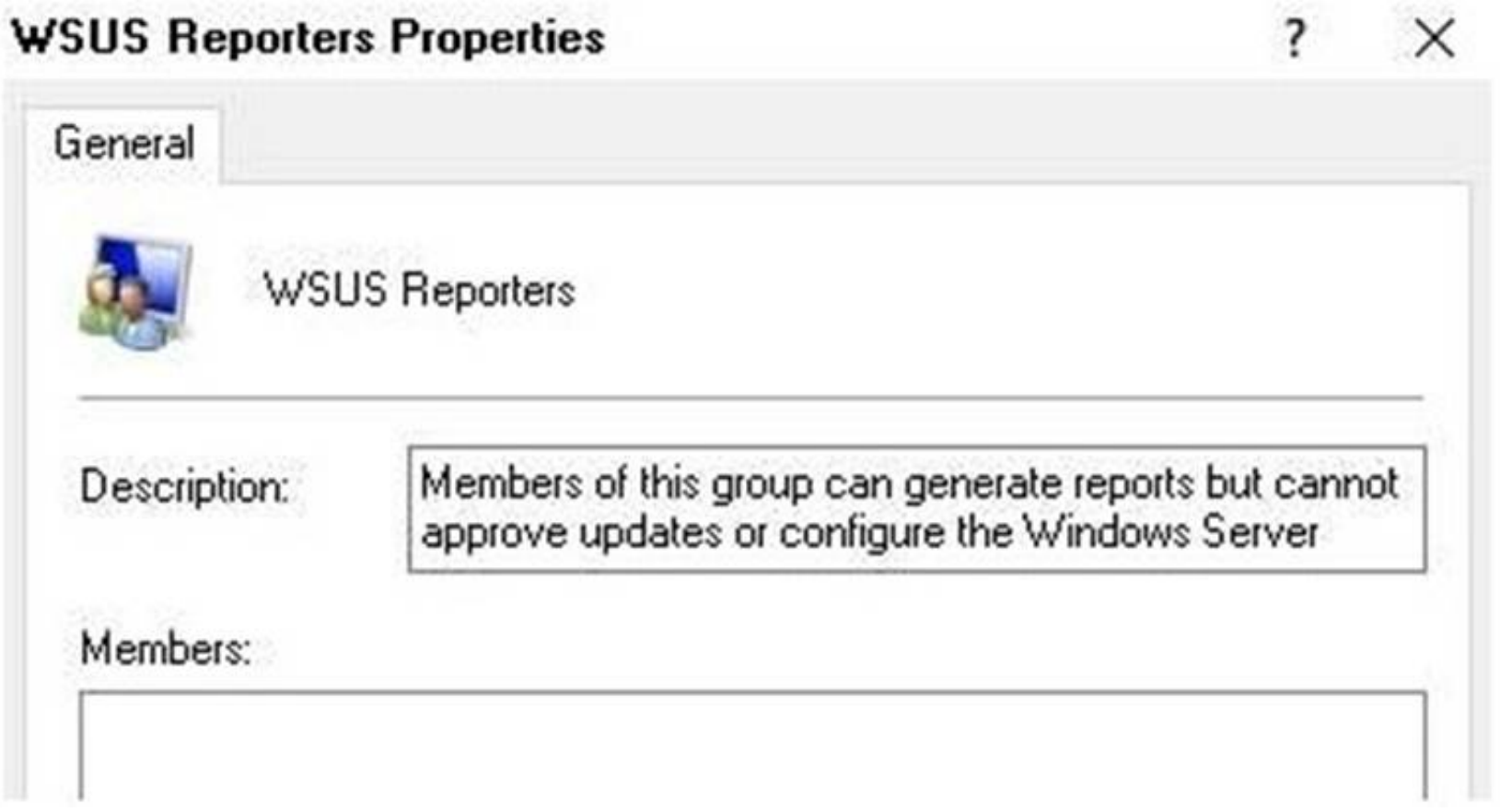
Explanation:
On Server1, User1 can run D:\\Folder2\\App1.exe : Yes On Server1, User1 can run D:\\Folder1\\Program1.exe : Yes
If Program1 is copied from D:\\Folder1 to D:\\Folder2, User1 can run Program1.exe on Server1 : NO
https://docs.microsoft.com/en-us/windows/device-security/applocker/configure-the-applicationidentity-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

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

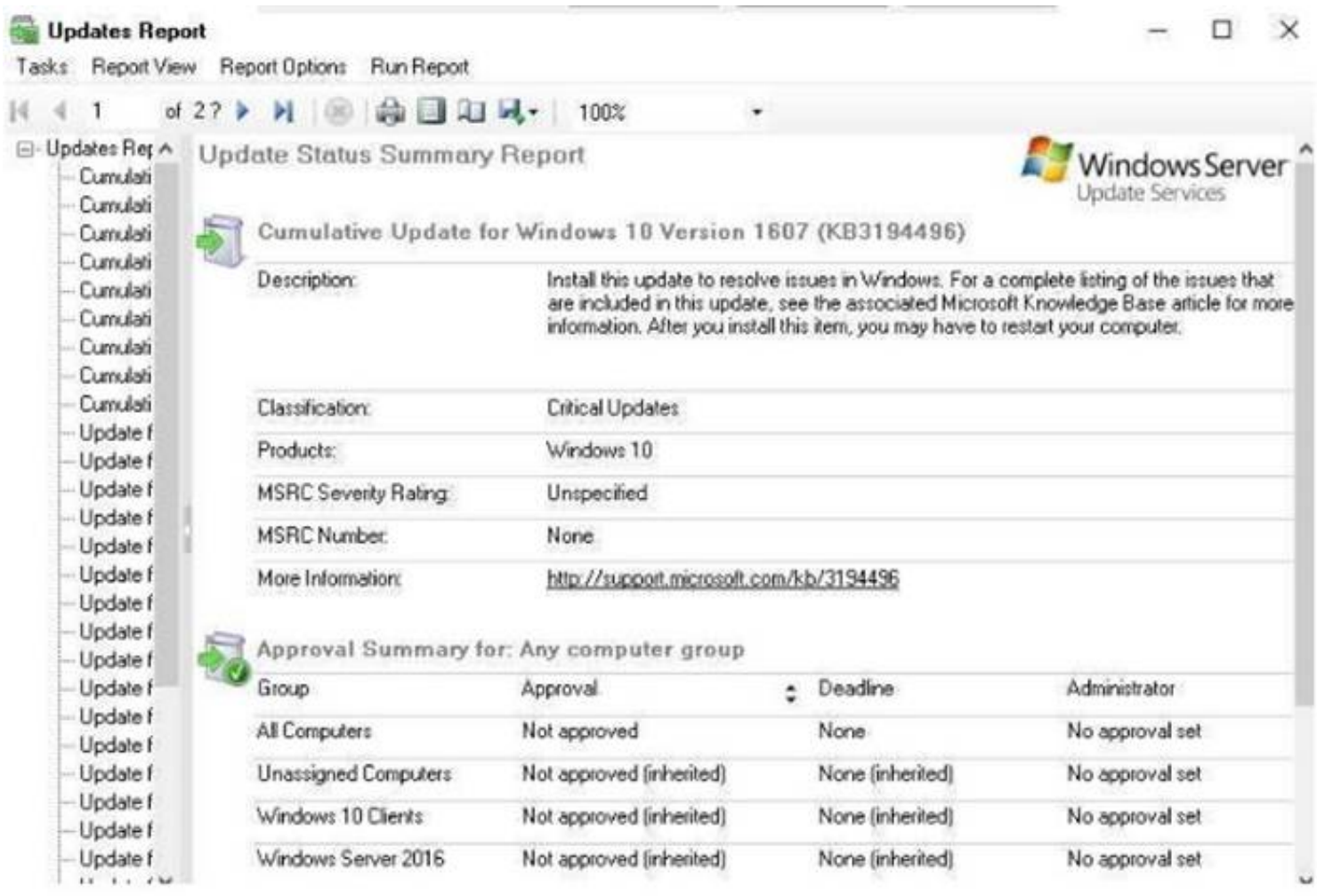
A. Modify the permissions of the ReportWebService virtual folder from the WSUS Administration website.
B. Add User1 to the WSUS Reporters local group.
C. Add User1 to the WSUS Administrators local group.
D. Run wsusutil.exe and specify the postinstall paramete

Answer: B

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



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

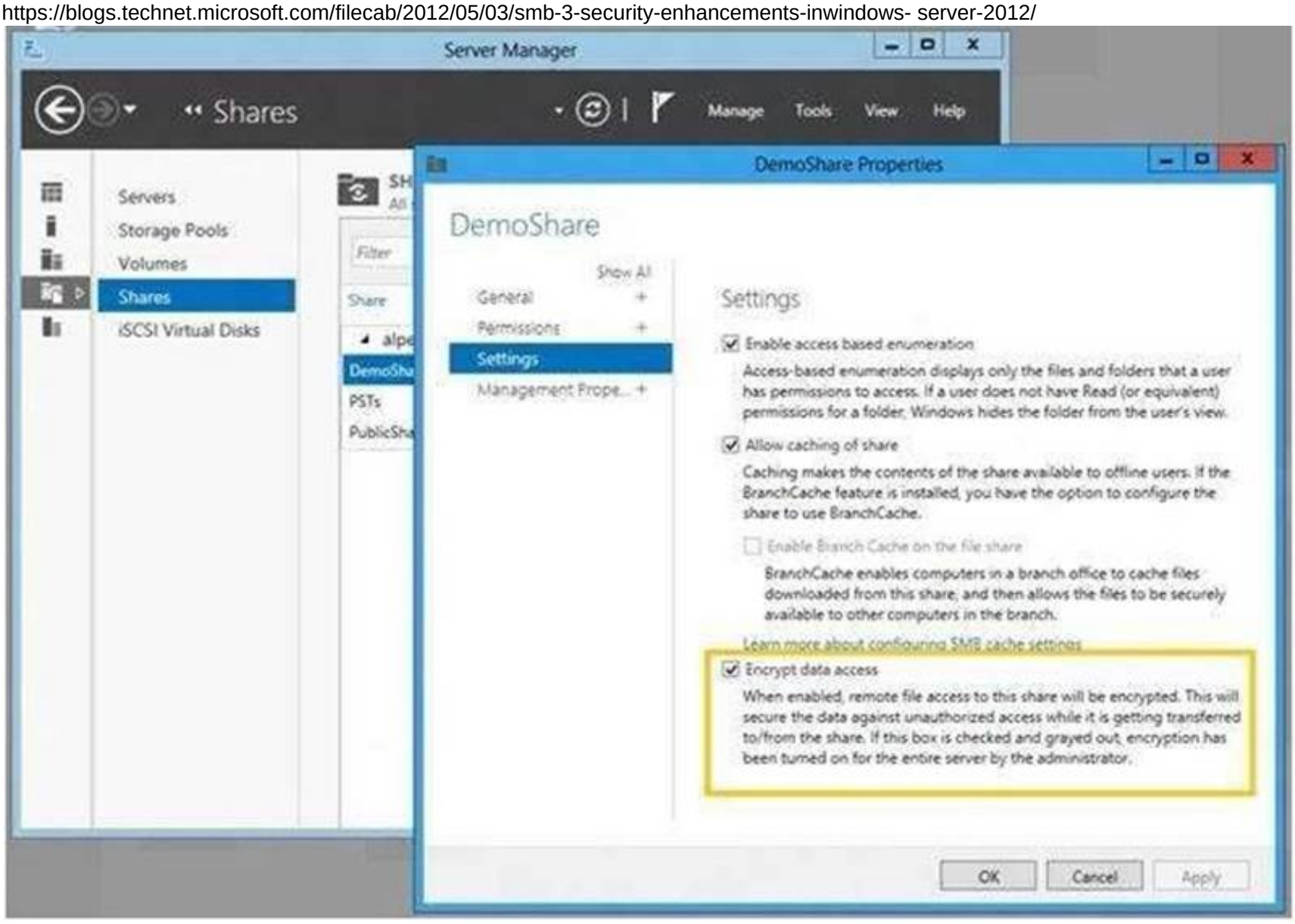


NEW QUESTION 9
Note: This question b part of a series of questions that use the same or simitar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question 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 question that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is Independent of the other questions in this series. Information and details provided in a question apply only to that question.
Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1 that runs Windows Server 2016. Server1 has a volume named Volume1.
Dynamic Access Control is configured. A resource property named Property1 was created in the domain.
You need to ensure that Property1 is set to a value of Big for all of the files in Volume1 that are larger than 10 MB.
Which tool should you use?

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

Answer: H

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

NEW QUESTION 10
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 12
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

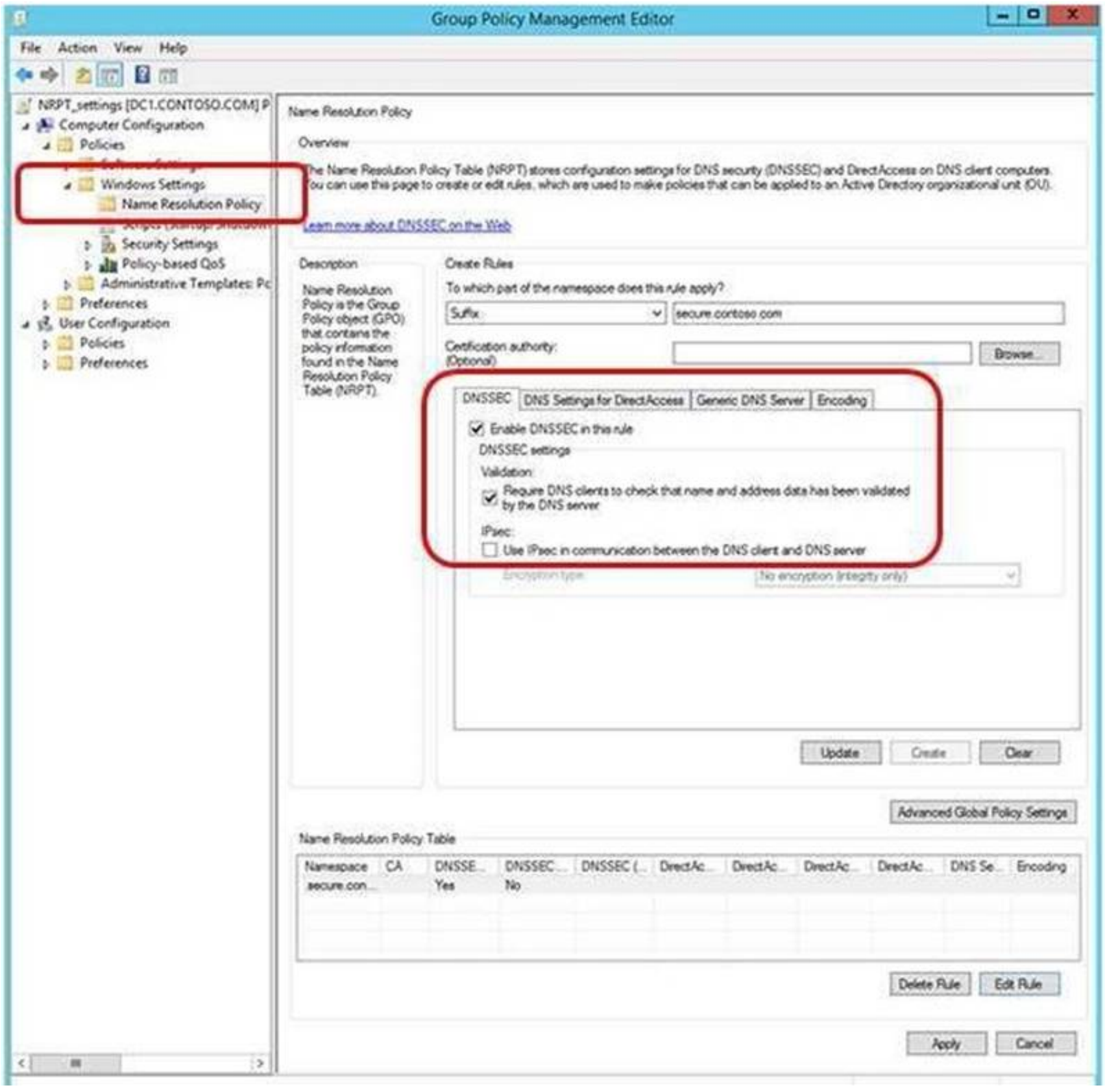
All servers run Windows Server 2016. All client computers run Windows 10.
You have an organizational unit (OU) named Marketing that contains the computers in the marketing department You have an OU named Finance that contains the computers in the finance department You have an OU named AppServers that 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 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 plan to implement BitLocker Drive Encryption (BitLocker) on the operating system volumes of the application servers.
You need to ensure that the BitLocker recovery keys are stored in Active Directory. Which Group Policy setting should you configure?

A. System cryptography; Force strong key protection (or user keys stored on the computer
B. Store Bittocker recovery information in Active Directory Domain Services (Windows Server 2008 and Windows Vista)
C. System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing
D. Choose how BitLocker-protected operating system drives can be recovered

Answer: D

Explanation:

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

Choose how BitLocker-protected operating system drives can be recovered

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

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

Reference

This policy setting is applied when you turn on BitLocker.

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

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

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

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

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

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

NEW QUESTION 19
Your network contains an Active Directory domain named contoso.com The domain contains five file servers that run Windows Server 2016.
You have an organizational unit (OU) named Finance that contains all of the servers. You create a Group Policy object (GPO) and link the GPO to the Finance OU.
You need to ensure that when a user in the finance department deletes a file from a file server, the event is logged. The solution must log only users who have a manager attribute of Ben Smith. Which audit policy setting should you configure in the GPO?

A. File system in Global Object Access Auditing
B. Audit Detailed File Share
C. Audit Other Account Logon Events
D. Audit File System in Object Access

Answer: C

NEW QUESTION 23
Your network contains an Active Directory forest named contoso.com. The forest functional level is Windows Server 2012. The forest contains a single domain.
The domain contains multiple Hyper-V hosts.
You plan to deploy guarded hosts.
You deploy a new server named Server22 to a workgroup.
You need to configure Server22 as a Host Guardian Service server.
What should you do before you initialize the Host Guardian Service on Server22?

A. Install the Active Directory Domain Services server role on Server22.
B. Obtain a certificate.
C. Raise the forest functional level.

D. Join Server22 to the domai

Answer: D

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

NEW QUESTION 27
____ 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 31
Windows Firewall rules can be configured using PowerShell.
The “Set-NetFirewallProfile” cmdlet configures settings that apply to the per-profile configurations of the Windows Firewall with Advanced Security.
What is the default setting for the AllowInboundRules parameter when managing a GPO?

A. FALSE
B. NotConfigured

Answer: B

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

NEW QUESTION 36
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 37
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.

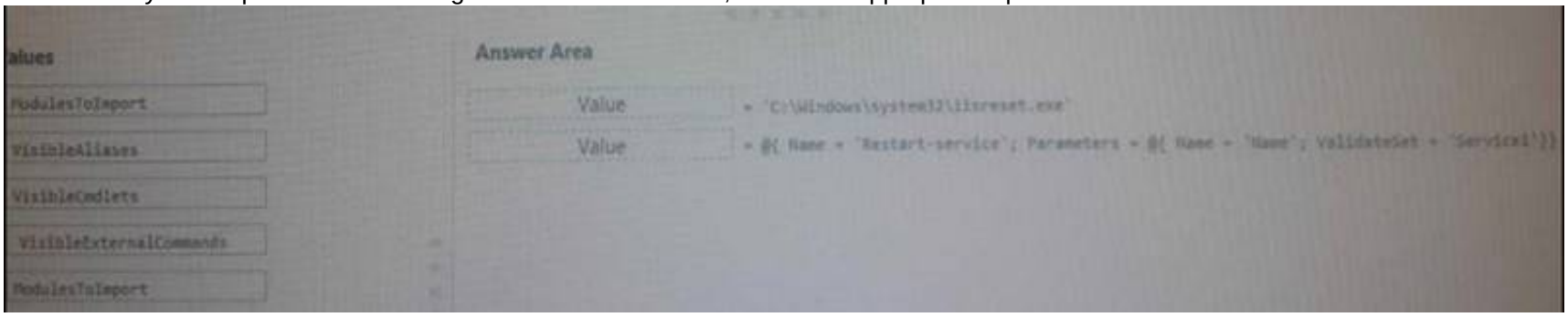
When you enable this policy setting on the domain controller, only authentication traffic to that domain controller will be logged.

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 41
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 45
You have a Hyper-V host named Hyperv1 that has a virtual machine named FS1. FS1 is a file server that contains sensitive data.
You need to secure FS1 to meet the following requirements:
-Prevent console access to FS1.
-Prevent data from being extracted from the VHDX file of FS1.
Which two actions should you perform? Each correct answer presents part of the solution.

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

Answer: AE

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

NEW QUESTION 46
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 50
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.

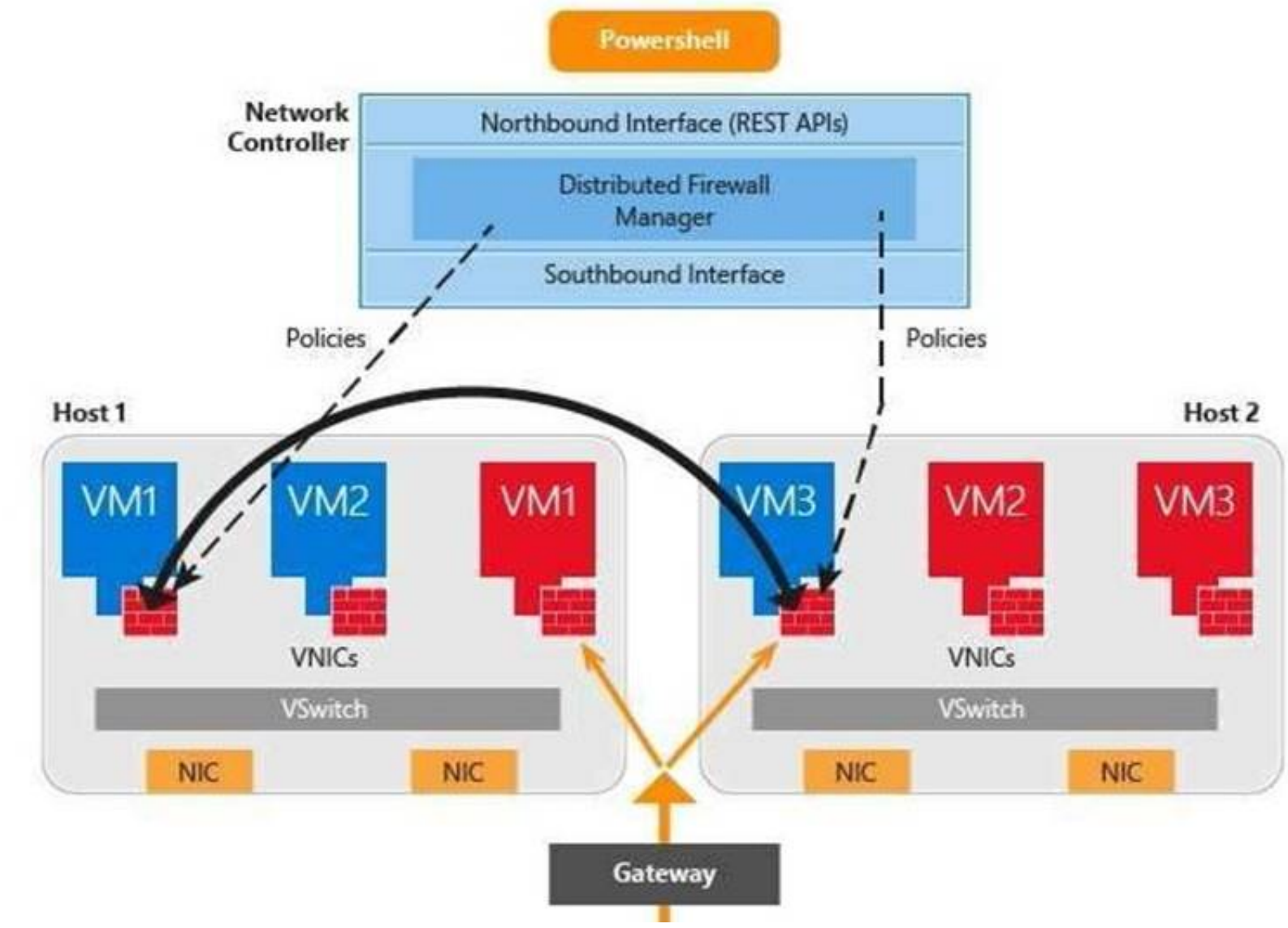
Server name	Platform	Windows Server 2016 edition
Server20	Physical	Standard
Server21	Physical	Standard
Server22	Virtual	Datacenter
Server23	Virtual	Datacenter

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



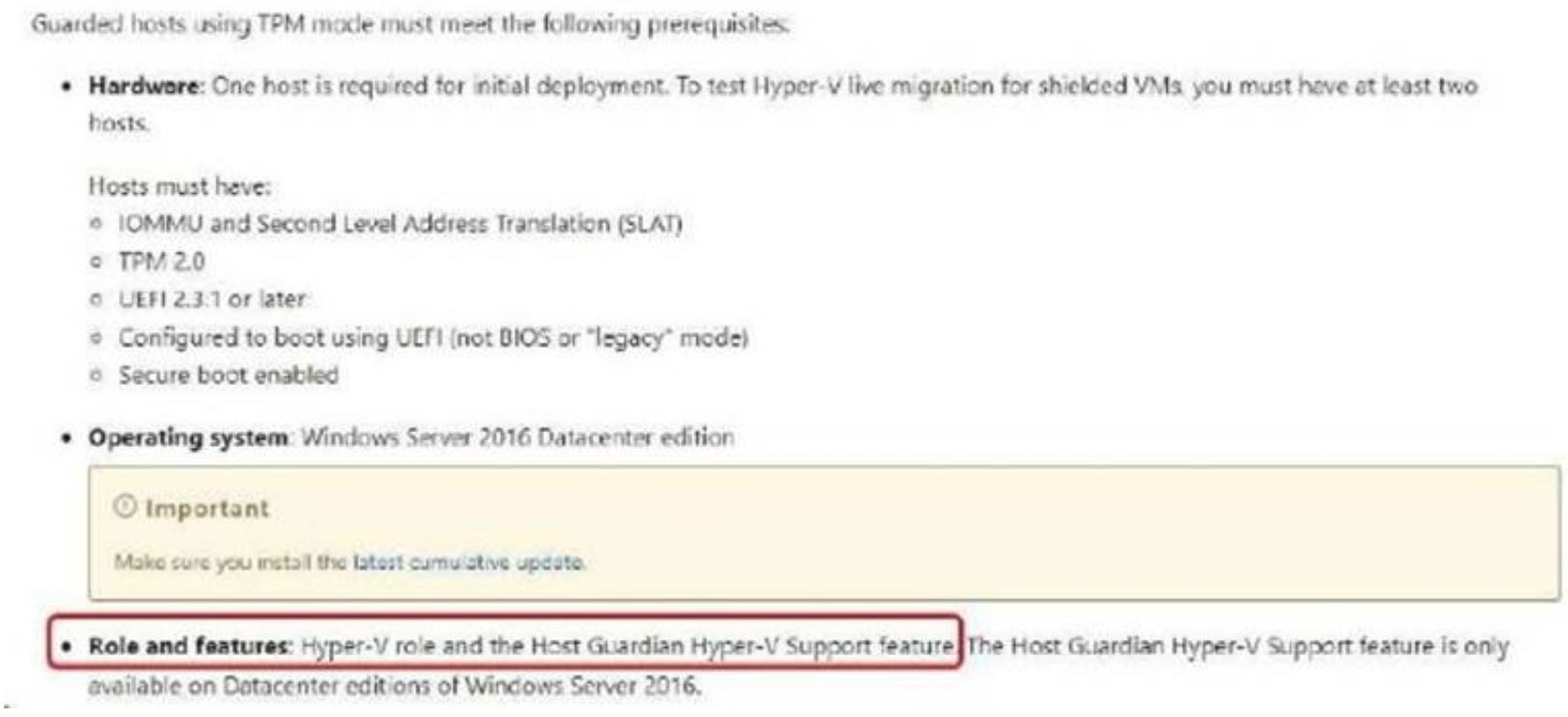
https://docs.microsoft.com/en-us/windows-server/networking/sdn/plan/installation-andpreparationrequirements- for-deploying-network-controller
Installation requirements
Following are the installation requirements for Network Controller.
For Windows Server 2016 deployments, you can deploy Network Controller 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 52
Your network contains an Active Directory domain named contoso.com. The domain contains several shielded virtual machines.
You deploy a new server named Server1 that runs Windows Server 2016. You install the Hyper-V server role on Server1.
You need to ensure that you can host shielded virtual machines on Server1. What should you install on Server1?

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

Answer: A

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


Guarded hosts using TPM mode must meet the following prerequisites:

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

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

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

  ⓘ Important

  Make sure you install the latest cumulative update.

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

NEW QUESTION 54

You are creating a Nano Server image for the deployment of 10 servers.
You need to configure the servers as guarded hosts that use Trusted Platform Module (TPM) attestation.
Which three packages should you include in the Nano Server image? Each correct answer presents part of the solution.

A. Microsoft-NanoServer-SecureStartup-Package
B. Microsoft-NanoServer-ShieldedVM-Package
C. Microsoft-NanoServer-Storage-Package
D. Microsoft-NanoServer-SCVMM-Compute-Package
E. Microsoft-NanoServer-SCVMM-Package
F. Microsoft-NanoServer-Compute-Package

Answer: ABF

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

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

NEW QUESTION 57
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2016. All client computers run Windows 10.
The relevant objects in the domain are configured as shown in the following table.

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

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

A. Yes
B. No

Answer: A

Explanation:
https://technet.microsoft.com/en-us/library/cc771990(v=ws.11).aspx Backup Operators
Members of this group can back up and restore files on a computer, regardless of any permissions that protect those files.
This is because the right to perform a backup takes precedence over all file permissions. Members of this group cannot change security settings.

NEW QUESTION 60
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?

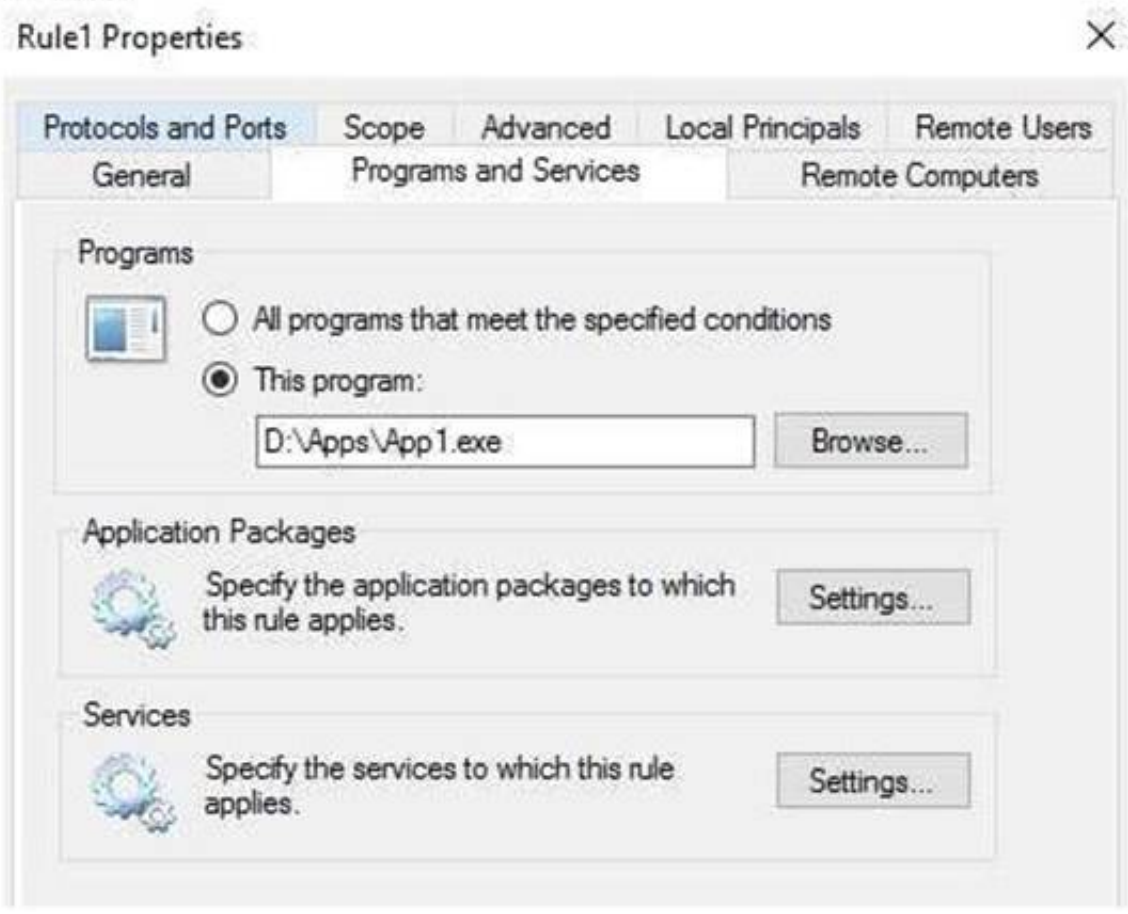
A. Yes
B. No

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 63
You have a server named Server1 that runs Windows Server 2016.
You need to identity whether any connection security rules are configured on Server1. Which cmdlet should you use?

A. Get-NetIPSecRule
B. Get-NetFirewallRule C.Get-NetFirewallProfile

C. Get-NetFirewallSetting
D. Get-NetFirewallPortFilter
E. Get-NetFirewallAddressFilter
F. Get-NetFirewallSecurityFilter
G. Get-NetFirewallApplicationFilter

Answer: A

Explanation:
https://technet.microsoft.com/en-us/itpro/powershell/windows/netsecurity/get-netipsecrule
Get-NetIPSecRule displays the existence and details of Connection Security Rules, as connection
security rules implements IPsec between computers (not using tunnel endpoints) or sites (using tunnel endpoints)

NEW QUESTION 68
You have a server named Server1 that runs Windows Server 2016. You need to view all of the inbound rules on Server1.
Which cmdlet should you use?

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

Answer: B

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

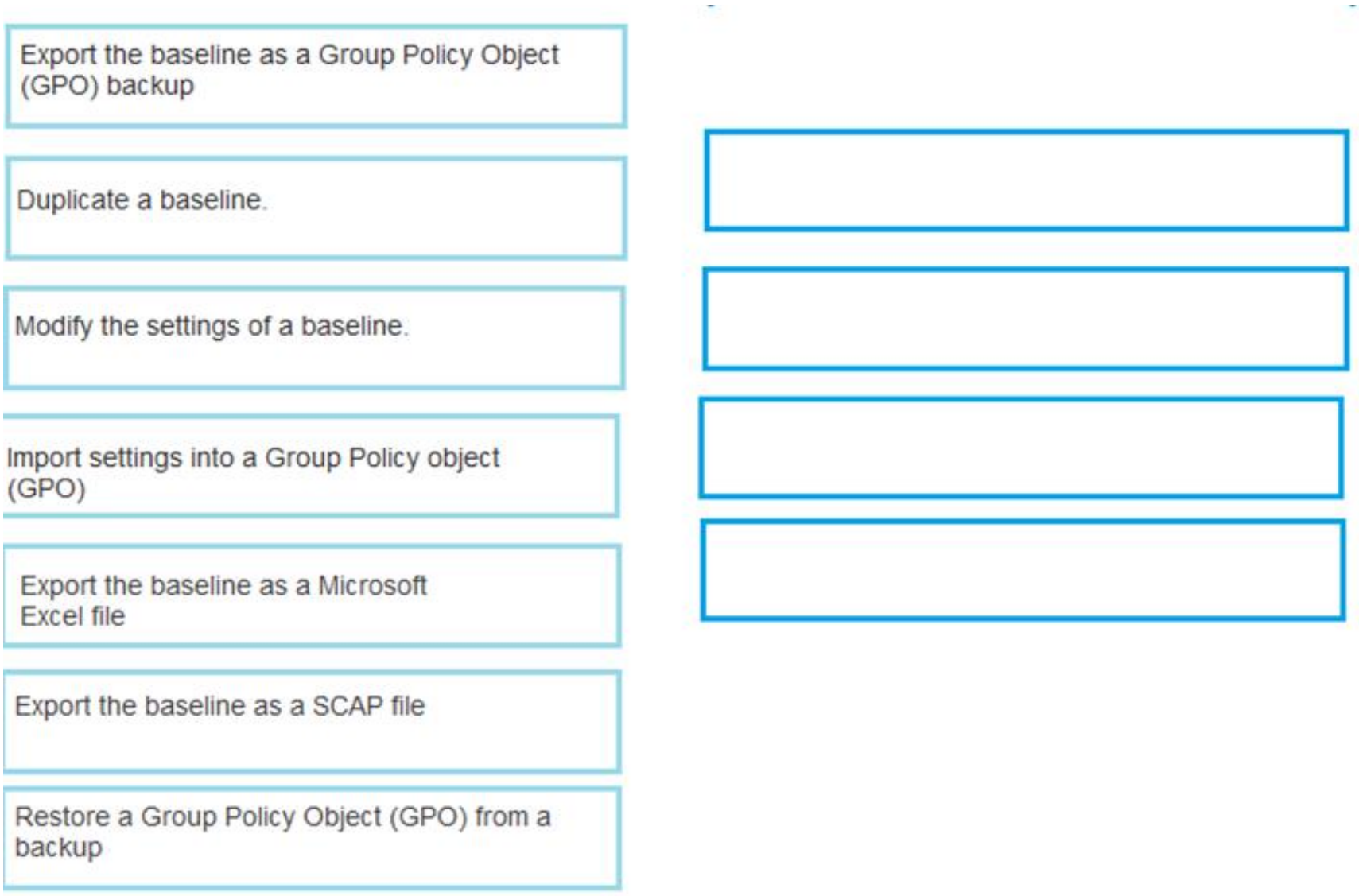
NEW QUESTION 73
Your network contains an Active Directory domain named contoso.com.
The domain contains a member server named Servers that runs Windows Server 2016. You need to configure Servers as a Just Enough Administration (JEA) endpoint.
Which two actions should you perform? Each correct answer 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

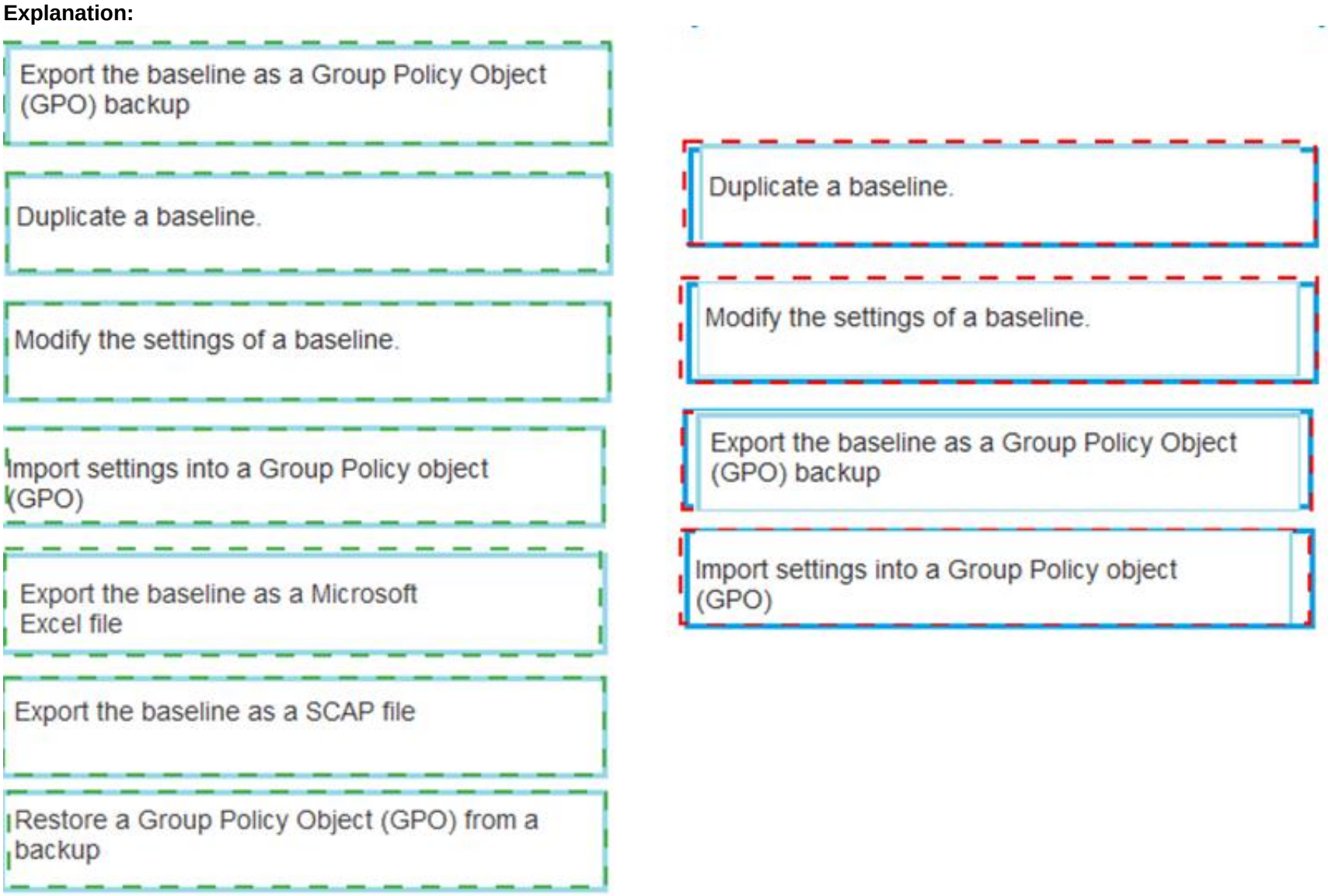
NEW QUESTION 74
DRAG DROP
Your network contains an Active Directory domain.
You install Security Compliance Manager (SCM) 4.0 on a server that runs Windows Server 2016. You need to modify a baseline, and then make the baseline available as a domain policy.
Which four actions should you perform in sequence?



A. Mastered
B. Not Mastered

Answer: A

Explanation:



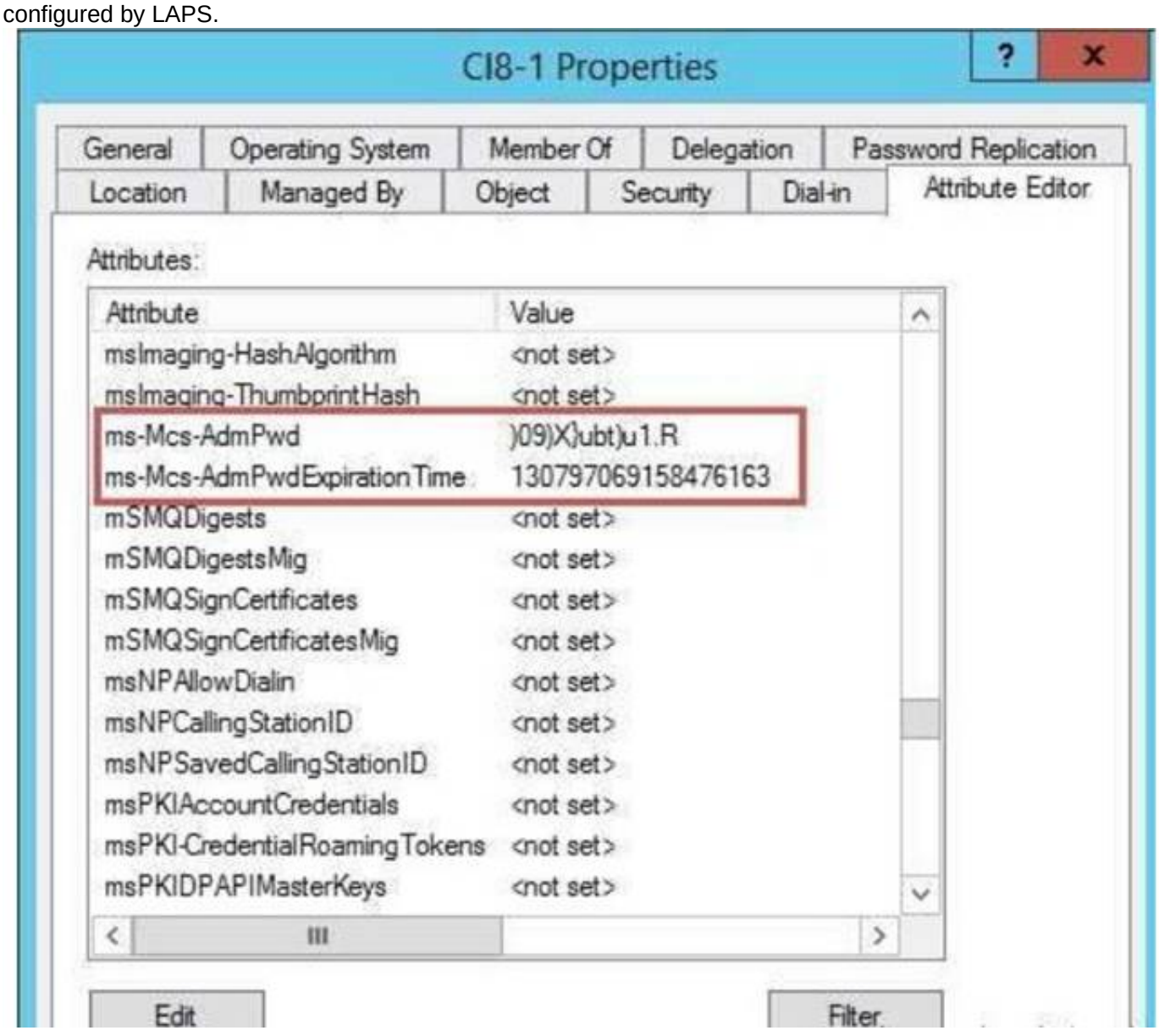
NEW QUESTION 75
Your network contains an Active Directory domain named contoso.com.
The domain contains a server named Server1 that runs Windows Server 2016.
The local administrator credentials of Server1 are managed by using the Local Administrator Password Solution (LAPS).
You need to retrieve the password of the Administrator account on Server1. What should you do?

A. From Windows PowerShell on Server1, run the Get-ADFineGrainedPasswordPolicy cmdlet and specify the -Credential parameter.

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

Answer: C

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

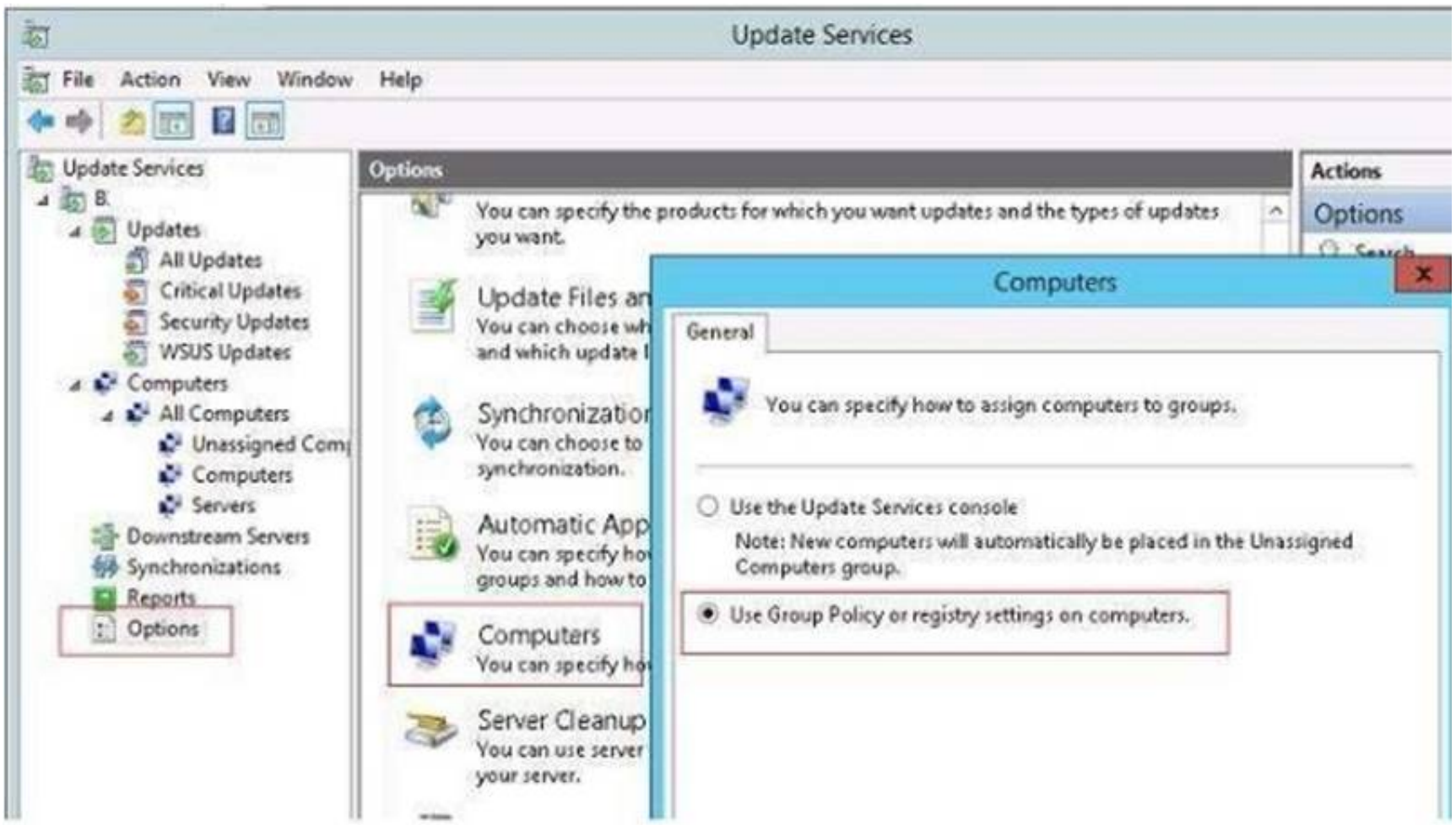


NEW QUESTION 79
Your network contains an Active Directory domain.
The domain contains two organizational units (OUs) named ProdOU and TestOU.
All production servers are in ProdOU. All test servers are in TestOU. A server named Server1 is in TestOU.
You have a Windows Server Update Services (WSUS) server 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?

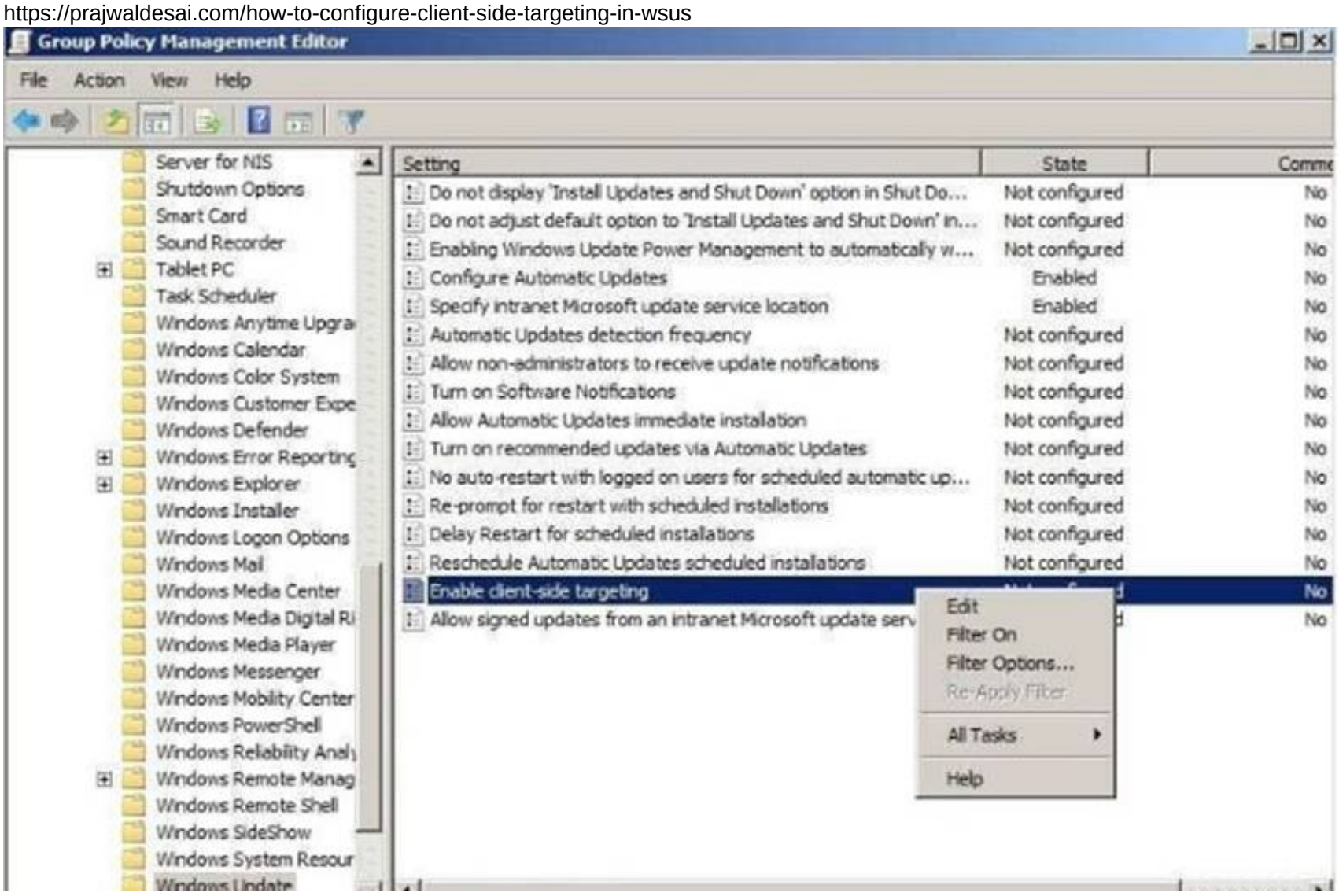
A. Turn off auto-restart for updates during active hours by using Group Policy objects (GPOs).
B. Configure client-side targeting by using Group Policy objects (GPOs).
C. Create computer groups by using the Update Services console.
D. Run wuauclt.exe /detectnow on each server after the server is moved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

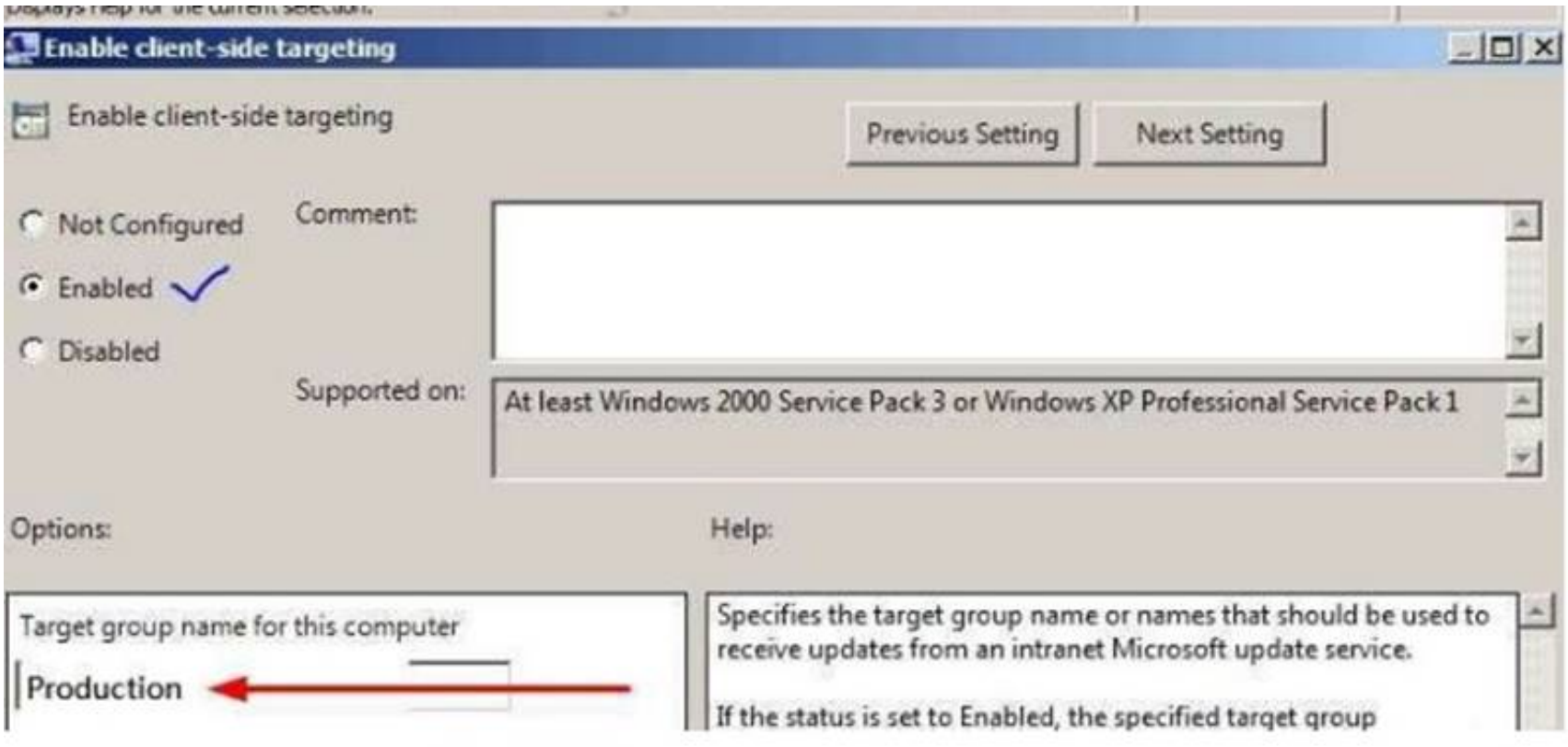
Answer: B

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 80
Your network contains an Active Directory domain named contoso.com. The domain contains 100 servers.
You deploy the Local Administrator Password Solution (LAPS) to the network You need to view the password of the local administrator of a server named Server5.
Which tool should you use?

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

Answer: A

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

NEW QUESTION 82
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 86
You have a server named Server1 that runs Windows Server 2016.
You need to install Security Compliance Manager (SCM) 4.0 on Server1. What should you install on Server1 first?

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

Answer: A

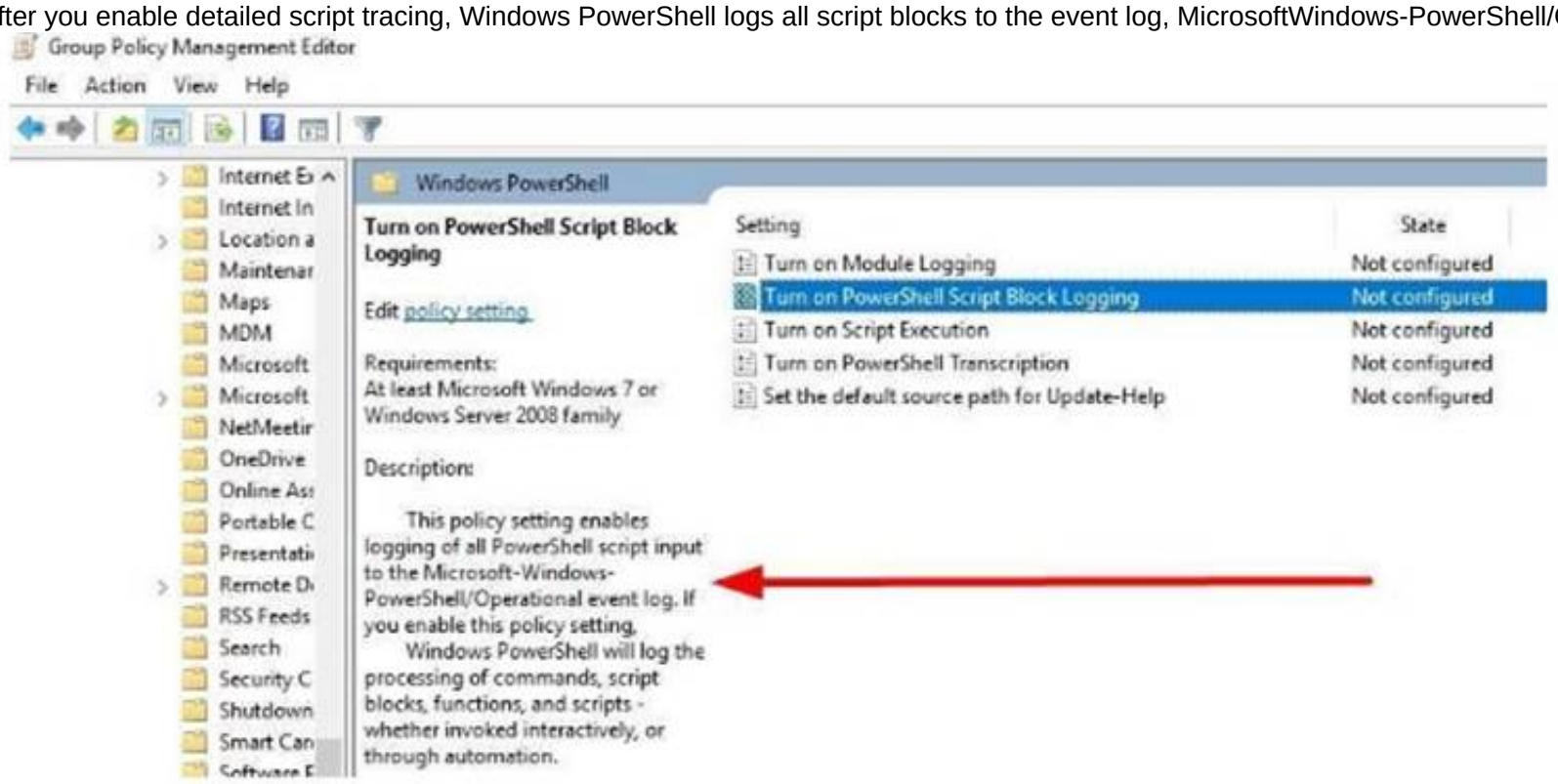
NEW QUESTION 90
You enable and configure PowerShell Script Block Logging.
You need to view which script blocks were executed by using Windows PowerShell scripts. What should you do?

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 95
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. The network uses the 172.16.0.0/16 address space.
Computer1 has an application named App1.exe that is located in D:\\Apps\\. App1.exe is configured to accept connections on TCP port 8080.
You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.
Solution: You configure an inbound rule that allows the TCP protocol on port 8080 and applies to all profiles
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 97
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that has Microsoft Security Compliance Manager (SCM) 4.0 installed. The domain contains domain controllers that run Windows Server 2016.
A Group Policy object (GPO) named GPO1 is applied to all of the domain controllers.
GPO1 has a Globally Unique Identifier (GUID) of 7ABCDEFG-1234-5678-90AB-005056123456. You need to create a new baseline that contains the settings from GPO1. What should you do first?

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

Answer: B

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

NEW QUESTION 102
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 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 107
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 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 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 115
Your network contains an Active Directory forest named corp.contoso.com.
You are implementing Privileged Access Management (PAM) by using a bastion forest named priv.contoso.com.
You need to create shadow groups in priv.contoso.com. Which cmdlet should you use?

A. New-RoleGroup
B. New-ADGroup
C. New-PamRole
D. New-PamGroup

Answer: D

Explanation:
https://social.technet.microsoft.com/wiki/contents/articles/33363.mim-2016-privileged-accessmanagementpam- faq.aspx
https://docs.microsoft.com/en-us/powershell/identitymanager/mimpam/vlatest/new-pamgroup

NEW QUESTION 120
You have the Windows Server 2016 operating system images as following table.

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

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

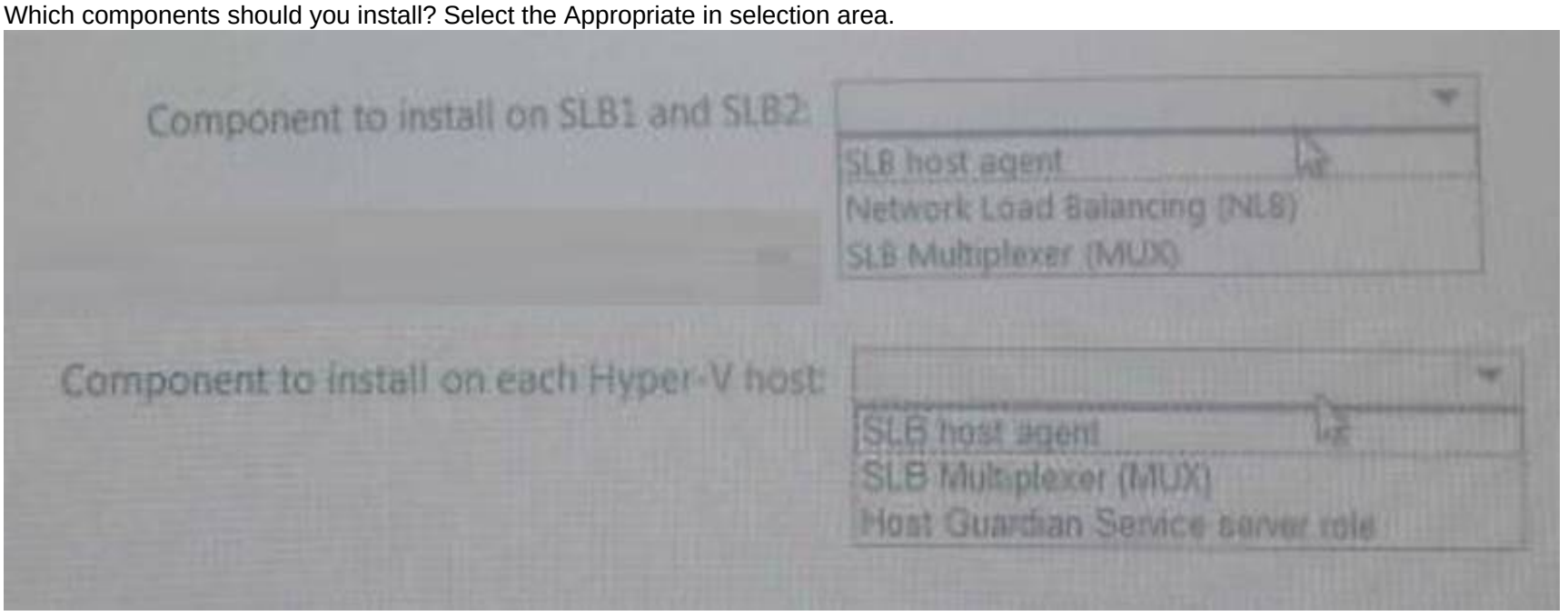
A. image1
B. image2
C. image3
D. image4

Answer: C

Explanation:
https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shieldedvm/ guarded-fabricprepare-for-hgs

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

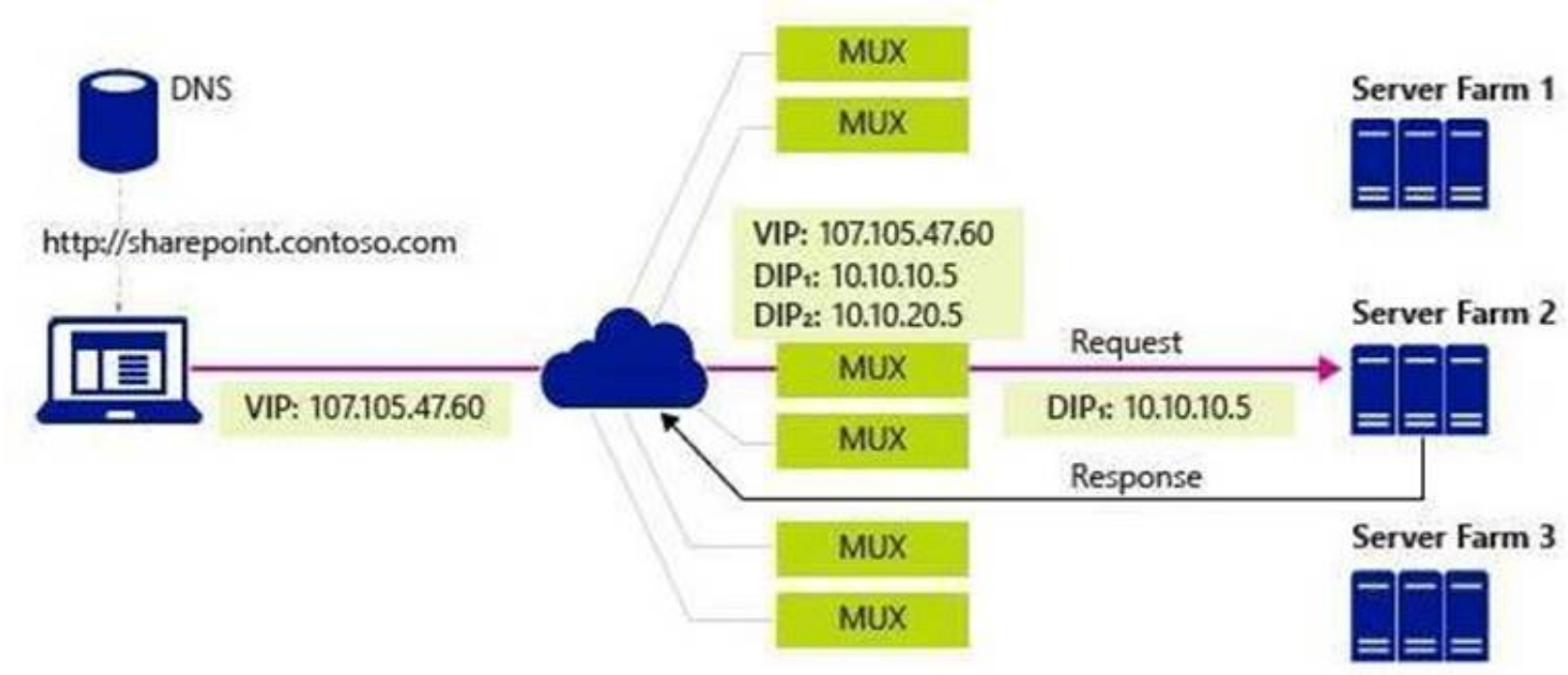
NEW QUESTION 125
HOTSPOT
You have 10 Hyper-V hosts that run Windows Server 2016.
Each Hyper-V host has eight virtual machines that run a distributed web application named App1. You plan to implement a Software Load Balancing (SLB) solution for client access to App1. You deploy two new virtual machines 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.



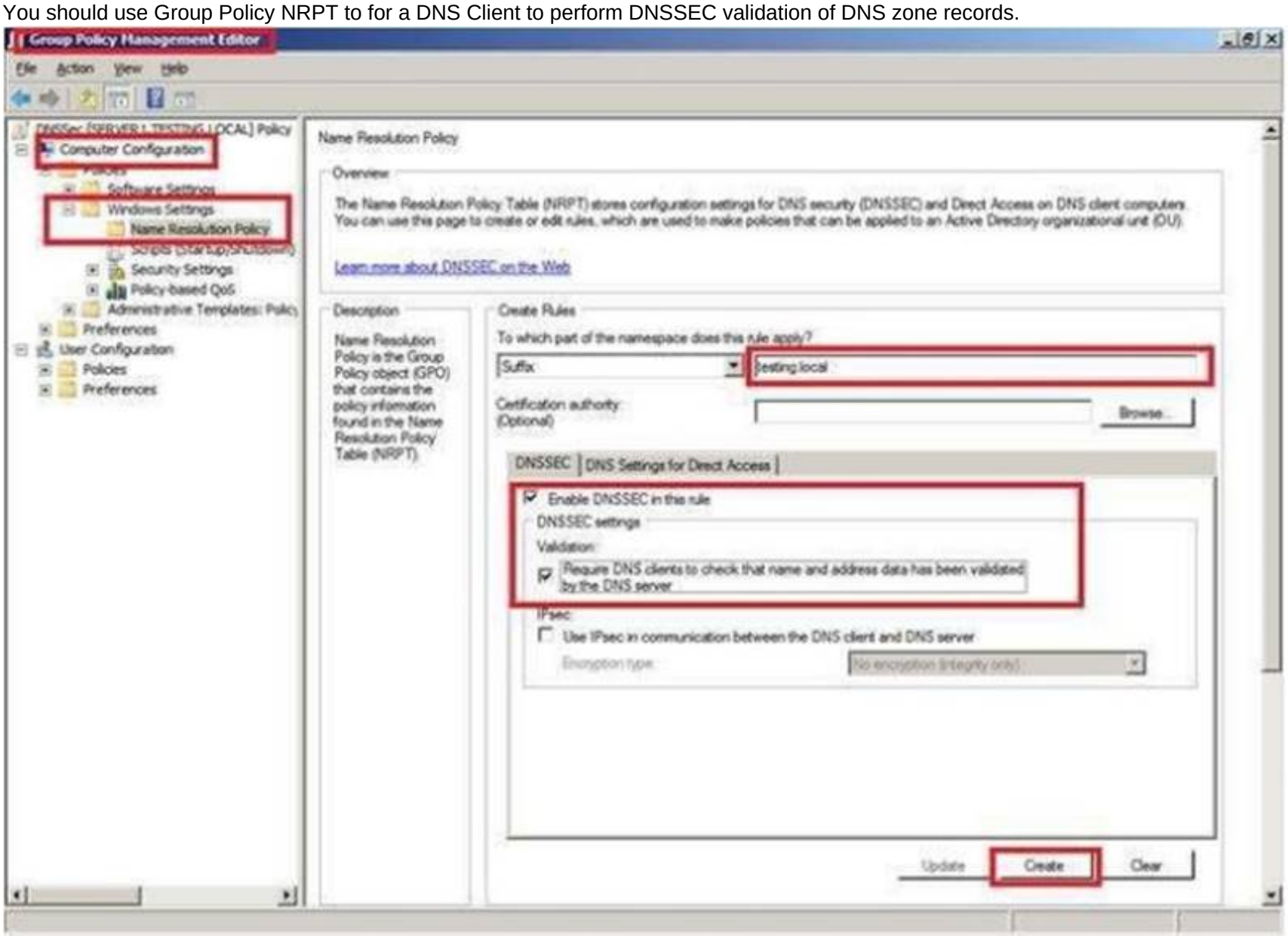
NEW QUESTION 128

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 130
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 135
You network contains an Active Directory forest named contoso.com.
All domain controllers run Windows Server 2016 Member servers run either Windows Server 2012 R2 or Windows Server 2016.
Client computers run either Windows 8.1 or Windows 10.
You need to ensure that when users access files in shared folders on the network, the files are encrypted when they are transferred over the network.
Solution: You enable SMB encryption on all the computers in domain. Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 138
Your network contains an Active Directory domain named contoso.com.
You download Microsoft Security Compliance Toolkit 1.0 and all the security baselines.
You need to deploy one of the security baselines to all the computers in an organizational unit (OU) named OU1.
What should you do?

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

Answer: B

Explanation:

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

NEW QUESTION 140
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You manage a file server that runs Windows Server 2016. The file server contains the volumes configured as shown in the following table.

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

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

A. Yes
B. No

Answer: A

Explanation:

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

NEW QUESTION 145
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 146
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 151
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 154
DRAG DROP
Your network contains an Active Directory domain named contoso.com. The domain contains a user named User1 and a computer named Computer1. Remote Server Administration Tools (RSAT) is installed on Computer1.
You need to add User1 as a data recovery agent in the domain.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

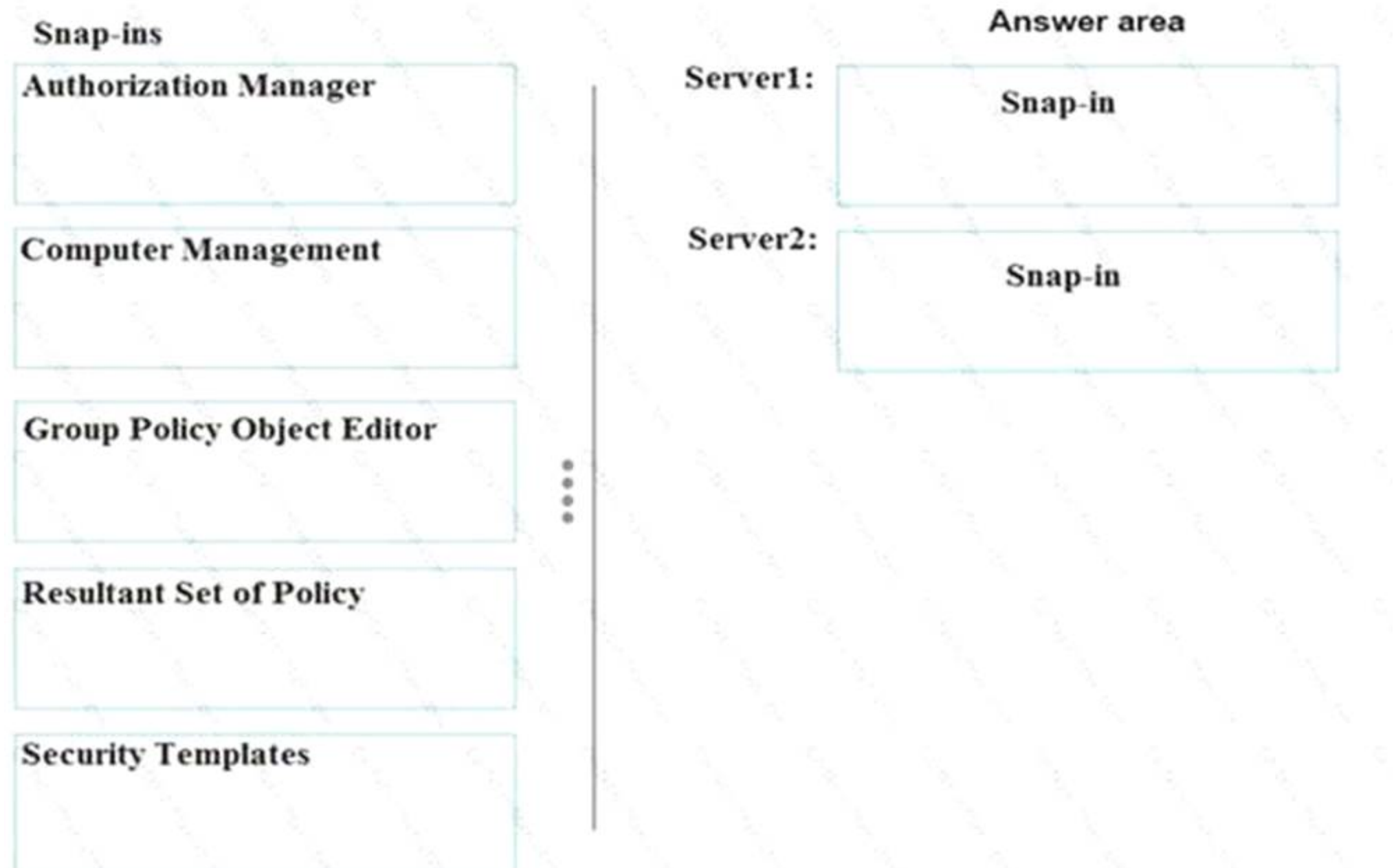
A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 156
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 159
.....

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