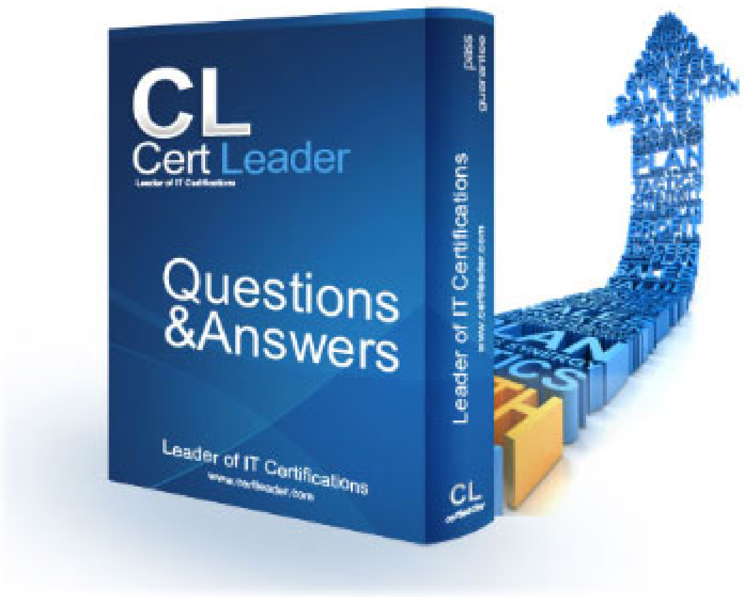
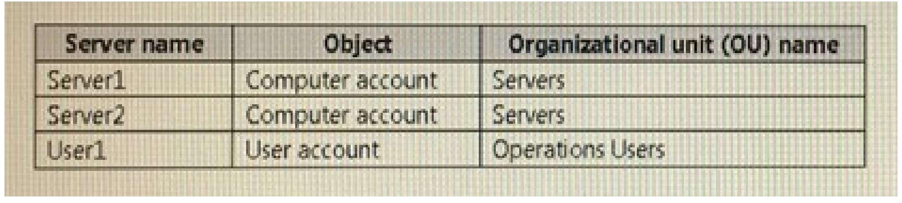
70-744 Dumps

Securing Windows Server 2016

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



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.



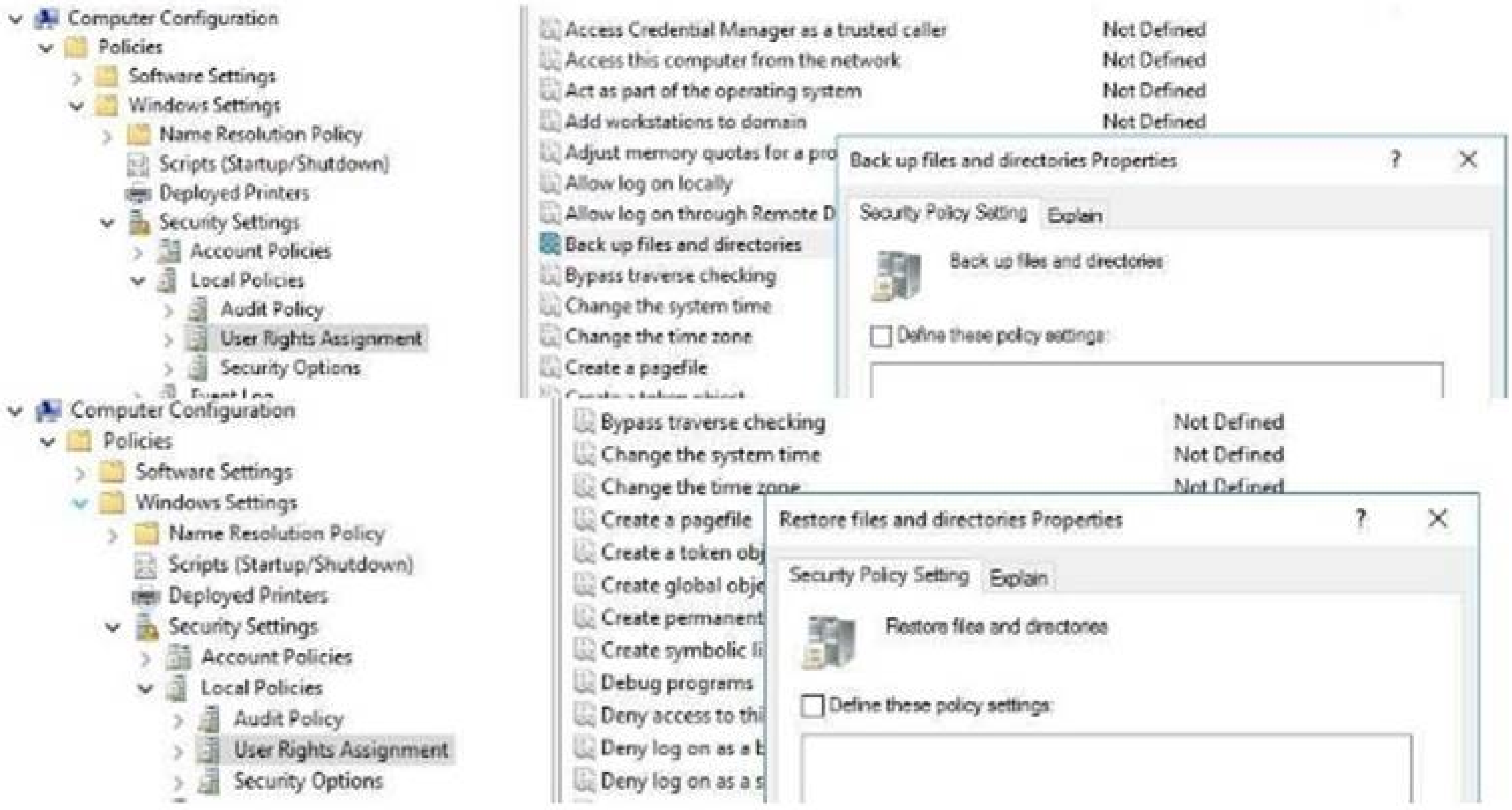
Server name	Object	Organizational unit (OU) name
Server1	Computer account	Servers
Server2	Computer account	Servers
User1	User account	Operations Users

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:



Access Credential Manager as a trusted caller Not Defined
Access this computer from the network Not Defined
Act as part of the operating system Not Defined
Add workstations to domain Not Defined
Adjust memory quotas for a pro
Allow log on locally
Allow log on through Remote D
Back up files and directories
Bypass traverse checking
Change the system time
Change the time zone
Create a pagefile

Back up files and directories Properties
Security Policy Setting Explain
Back up files and directories
□ Define these policy settings:

Bypass traverse checking Not Defined
Change the system time Not Defined
Change the time zone Not Defined
Create a pagefile
Create a token obj
Create global obje
Create permanent
Create symbolic li
Debug programs
Deny access to thi
Deny log on as a b
Deny log on as a s

Restore files and directories Properties
Security Policy Setting Explain
Restore files and directories
□ Define these policy settings:

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 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 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/

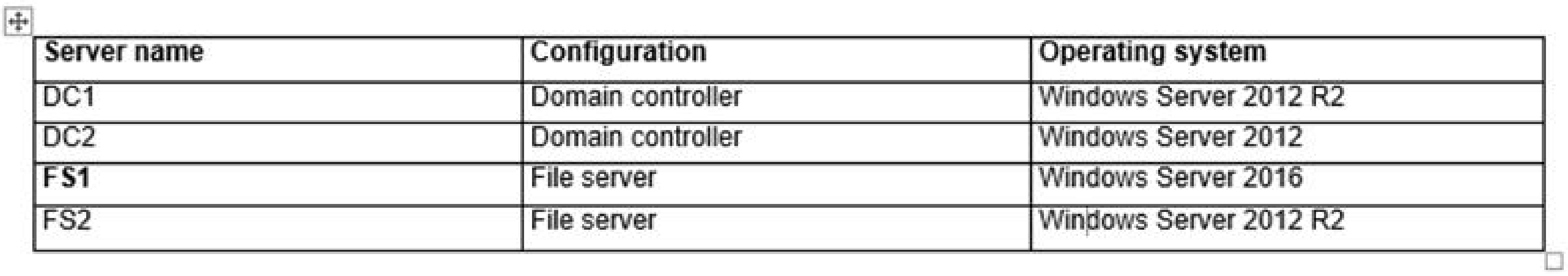
NEW QUESTION 4
Your network contains an Active Directory domain named contoso.com. The domain contains 100 servers.
You deploy the Local Administrator Password Solution (LAPS) to the network.
You deploy a new server named FinanceServer5, and join FinanceServerS to the domain.
You need to ensure that the passwords of the local administrators of FinanceServer5 are available to the LAPS administrators.
What should you do?

A. On FinanceServerS, register AdmPwd.dll.
B. On FmanceServerS, install the LAPS Windows PowerShell module.
C. In the domain, modify the permissions for the computer account of FmanceServer5.
D. In the domain, modify the permissions of the Domain Controllers organizational unit (OU).

Answer: A

Explanation:
References:
https://gallery.technet.microsoft.com/Step-by-Step-Deploy-Local-7c9ef772

NEW QUESTION 5
Your network contains an Active Directory domain named contoso.com. The domain contains four servers. The servers are configured as shown in the following table.



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

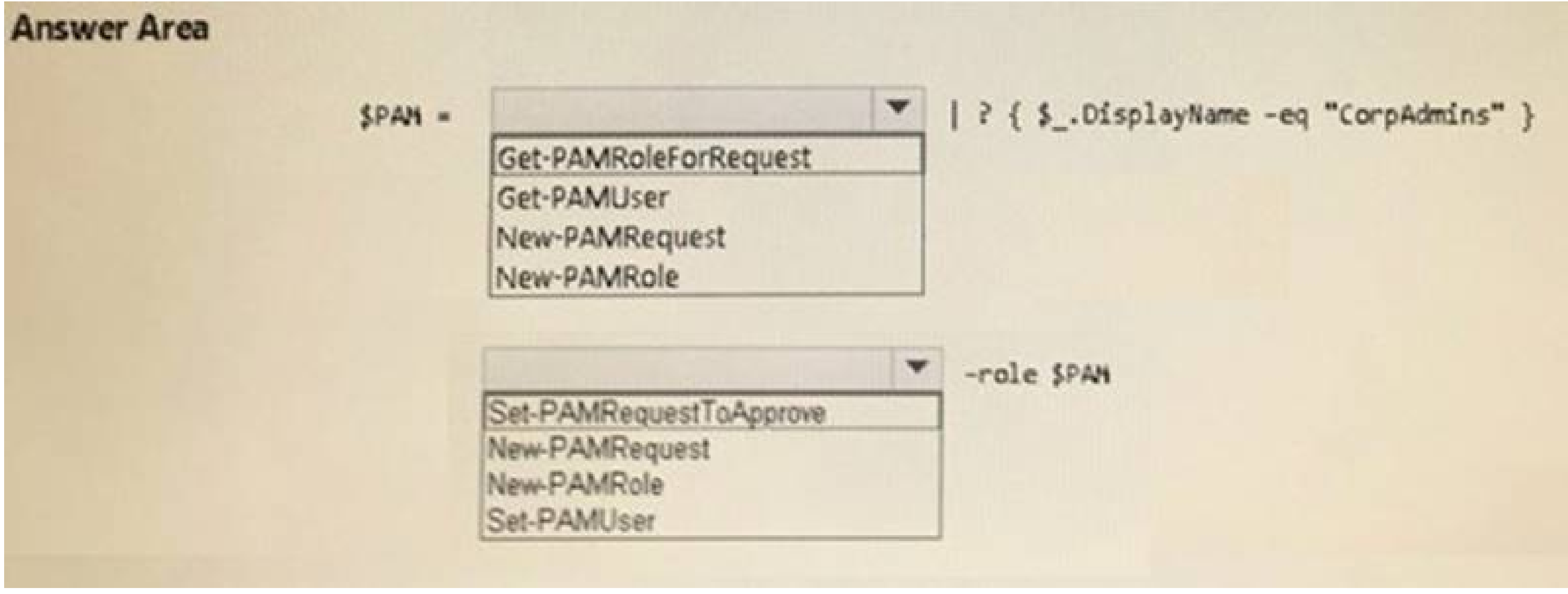
You need to manage FS1 and FS2 by using Just Enough Administration (JEA). What should you do before you can implement JEA?

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

Answer: C

Explanation:
https://msdn.microsoft.com/en-us/library/dn896648.aspx
The current release of JEA is available on the following platforms:
-Windows Server 2016 Technical Preview 5 and higher
-Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2* with Windows Management Framework 5.0 installed FS1 is ready to be managed by JEA, but FS2 need some extra work to do, either upgrade it to Windows Server 2016 or install Windows Management Framework 5.0 installed,

NEW QUESTION 6
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.



Answer Area

```
$PAM = [▼] | ? { $_.DisplayName -eq "CorpAdmins" }
[▼] -role $PAM
```

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

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

Answer: A

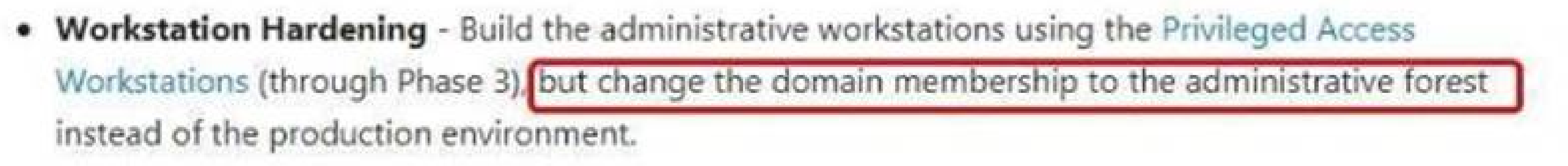
Explanation:
You have to “-Minimize the attack surface of the forest”, then you must create another forest for administrators.
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securingprivilegedaccess- reference-material#ESAE_BM
This section contains an approach for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

NEW QUESTION 8
Your network contains two single-domain Active Directory forests named contoso.com and contosoadmin.com. Contosoadmin.com contains all of the user accounts used to manage the servers in contoso.com.
You need to recommend a workstation solution that provides the highest level of protection from vulnerabilities and attacks.
What should you include in the recommendation?

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

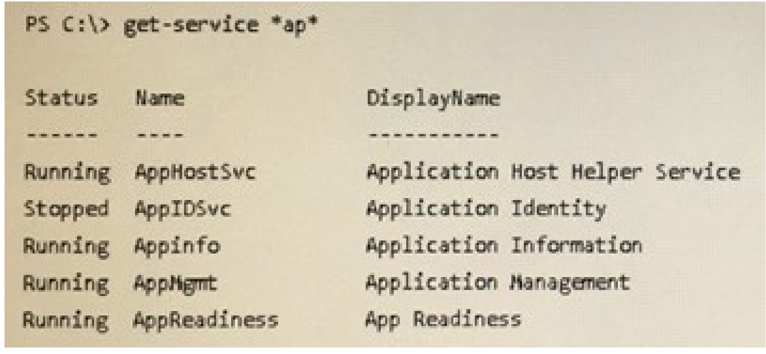
Answer: D

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



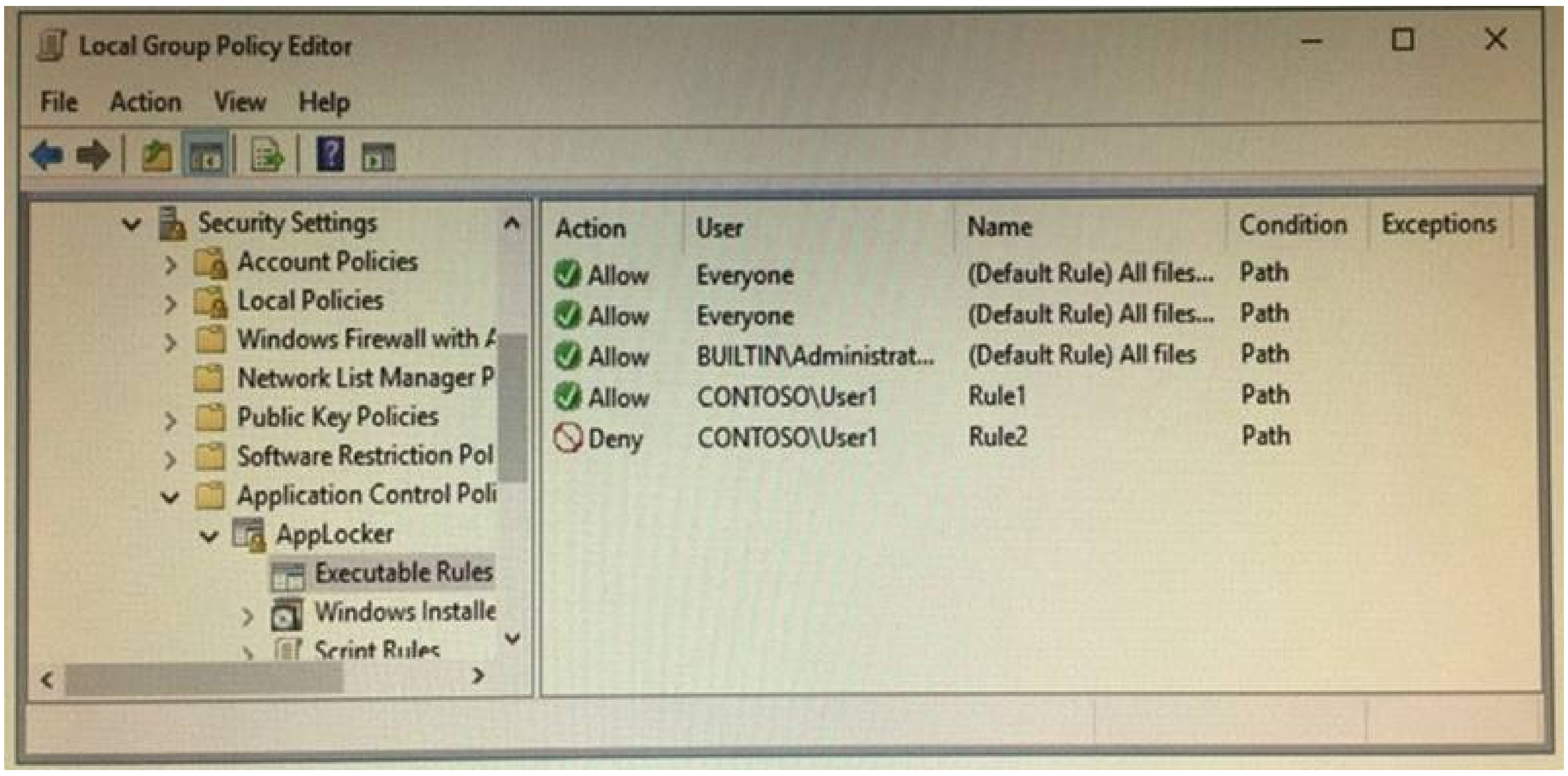
- **Workstation Hardening** - Build the administrative workstations using the Privileged Access Workstations (through Phase 3), but change the domain membership to the administrative forest instead of the production environment.

NEW QUESTION 9
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.



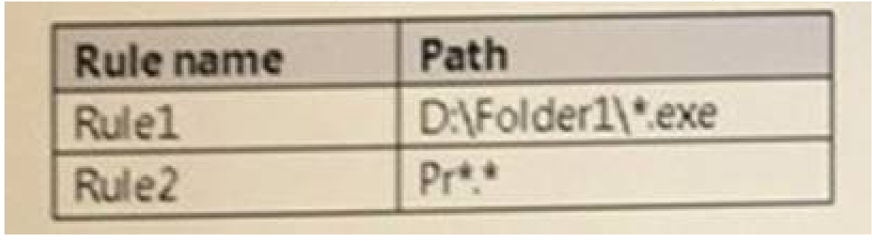
```
PS C:\> get-service *ap*

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.)



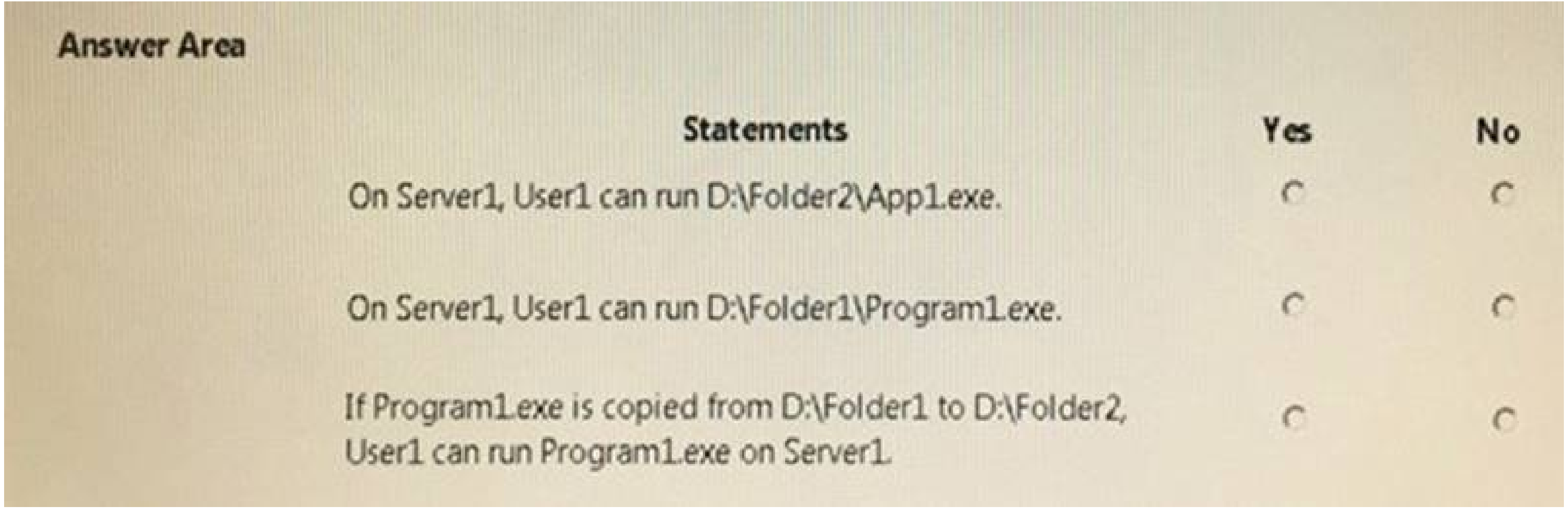
Action	User	Name	Condition	Exceptions
Allow	Everyone	(Default Rule) All files...	Path	
Allow	Everyone	(Default Rule) All files...	Path	
Allow	BUILTIN\Administrat...	(Default Rule) All files	Path	
Allow	CONTOSO\User1	Rule1	Path	
Deny	CONTOSO\User1	Rule2	Path	

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.

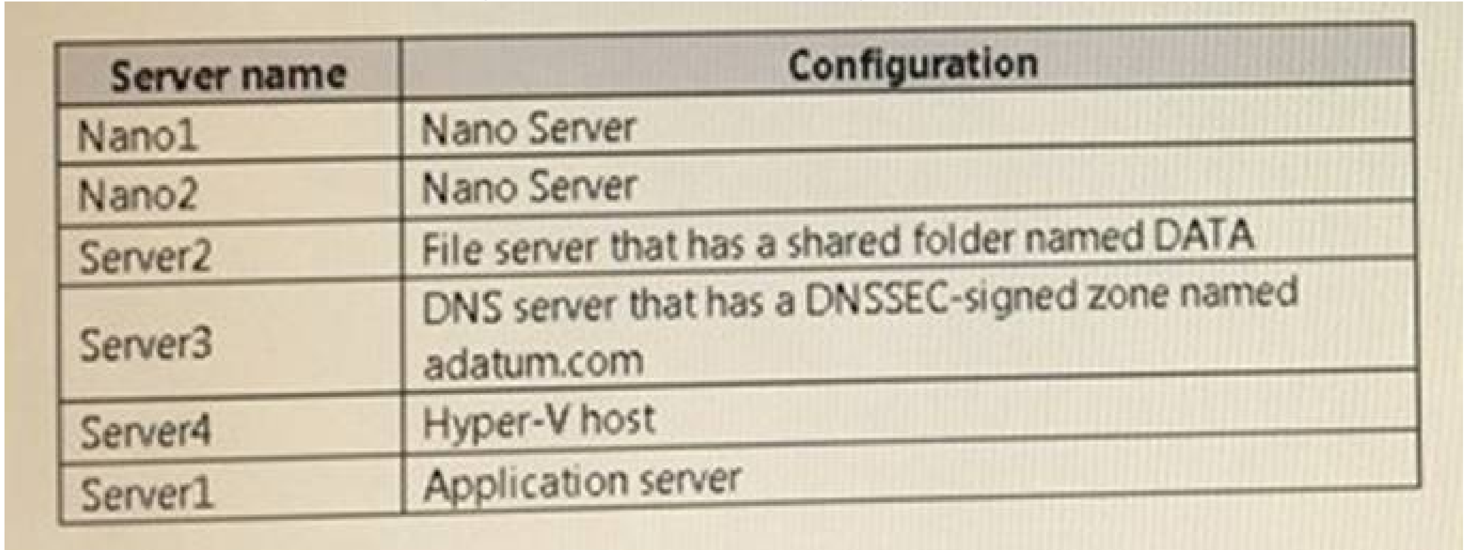
NEW QUESTION 10
Note: This question is part of a series of question that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is Independent of the other questions in this series. Information and details provided in a question 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

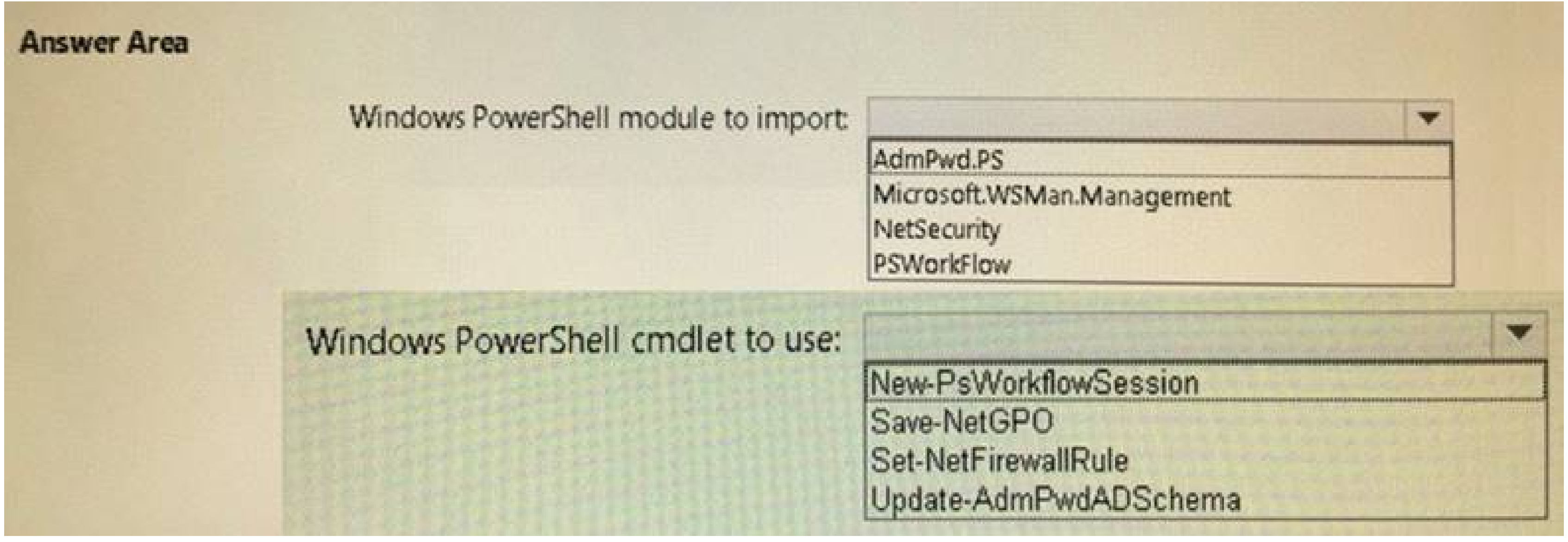
Explanation:
Automatic File Classification of FSRM
https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/deploy-automatic-fileclassification– demonstration-stepshttps://
blogs.technet.microsoft.com/filecab/2009/08/13/using-windows-powershell-scripts-for-fileclassification/

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



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

All servers run Windows Server 2016. All client computers run Windows 10.
You have an organizational unit (OU) named Marketing that contains the computers in the marketing department. You have an OU named Finance that contains the computers in the finance department. You have an OU named AppServers that contains application servers. A Group Policy object (GPO) named GP1 is linked to the Marketing OU. A GPO named GP2 is linked to the AppServers OU. You install Windows Defender on Nano1.
End of repeated scenario
You need to ensure that you can implement the Local Administrator Password Solution (LAPS) (or the finance department computers.
What should you do in the contoso.com forest? To answer, select the appropriate options in the answer area.



Answer Area

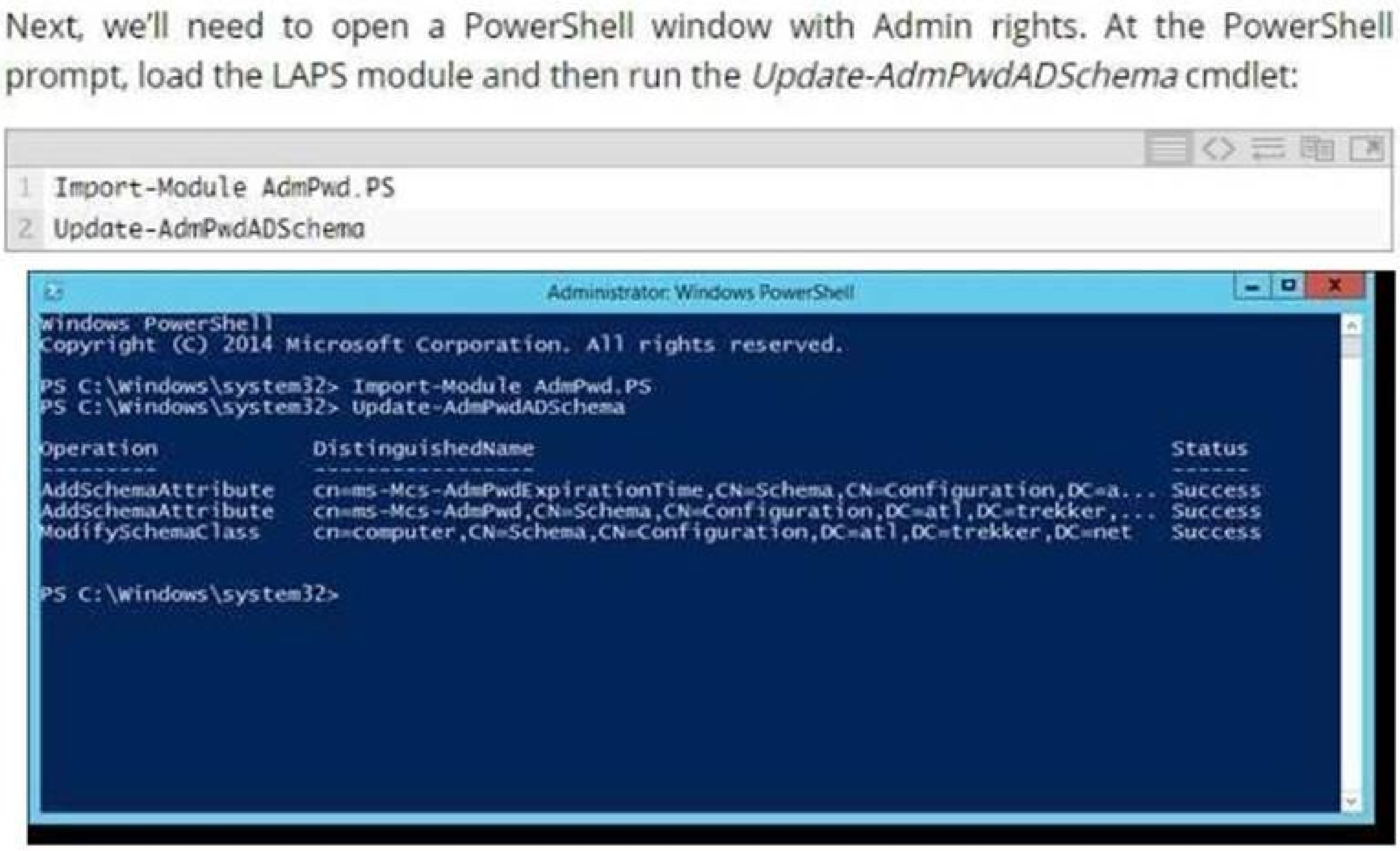
Windows PowerShell module to import:
- AdmPwd.PS
- Microsoft.WSMan.Management
- NetSecurity
- PSWorkFlow

Windows PowerShell cmdlet to use:
- New-PsWorkflowSession
- Save-NetGPO
- Set-NetFirewallRule
- Update-AdmPwdADSchema

A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://4sysops.com/archives/set-up-microsoft-laps-local-administrator-password-solution-in-activedirectory/



Next, we'll need to open a PowerShell window with Admin rights. At the PowerShell prompt, load the LAPS module and then run the *Update-AdmPwdADSchema* cmdlet:

```
Import-Module AdmPwd.PS
Update-AdmPwdADSchema
```

```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Import-Module AdmPwd.PS
PS C:\Windows\system32> Update-AdmPwdADSchema

Operation            DistinguishedName                                                  Status
---------            -----------------                                                  ------
AddSchemaAttribute   cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=a...  Success
AddSchemaAttribute   cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=atl,DC=trekker,...  Success
ModifySchemaClass    cn=computer,CN=Schema,CN=Configuration,DC=atl,DC=trekker,DC=net    Success


PS C:\Windows\system32>
```

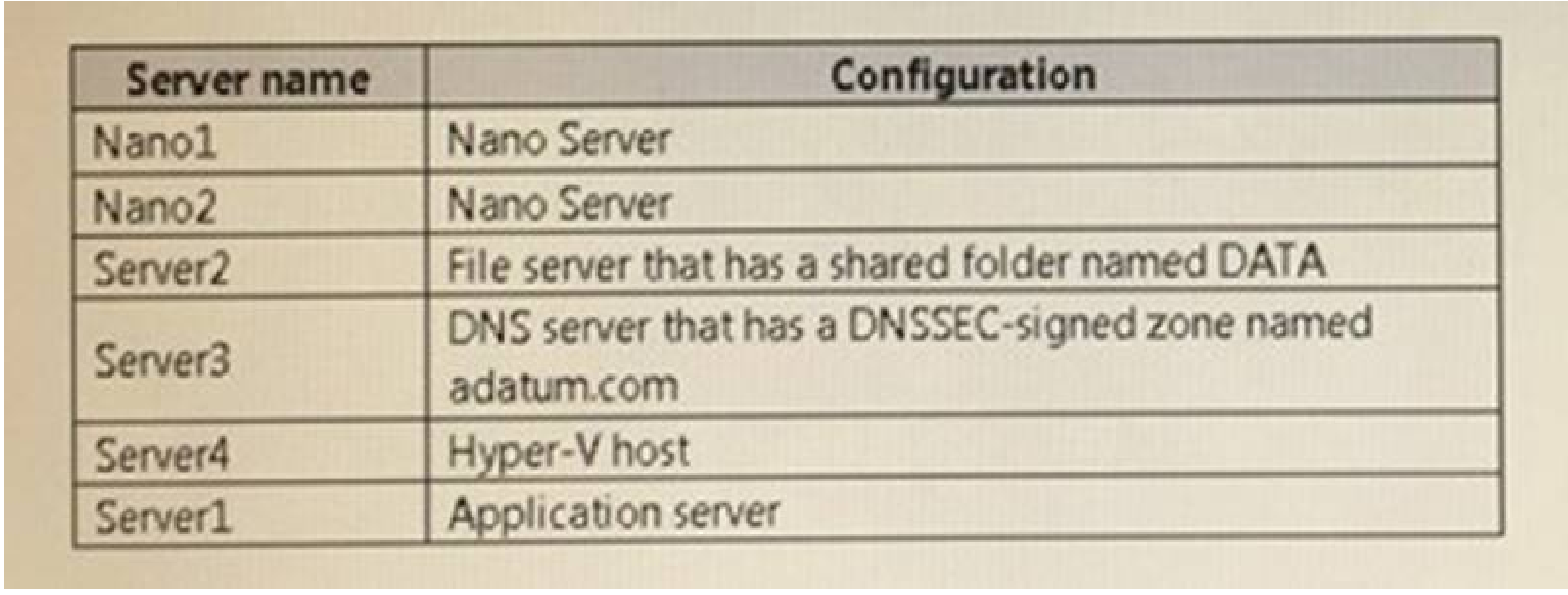
NEW QUESTION 13

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

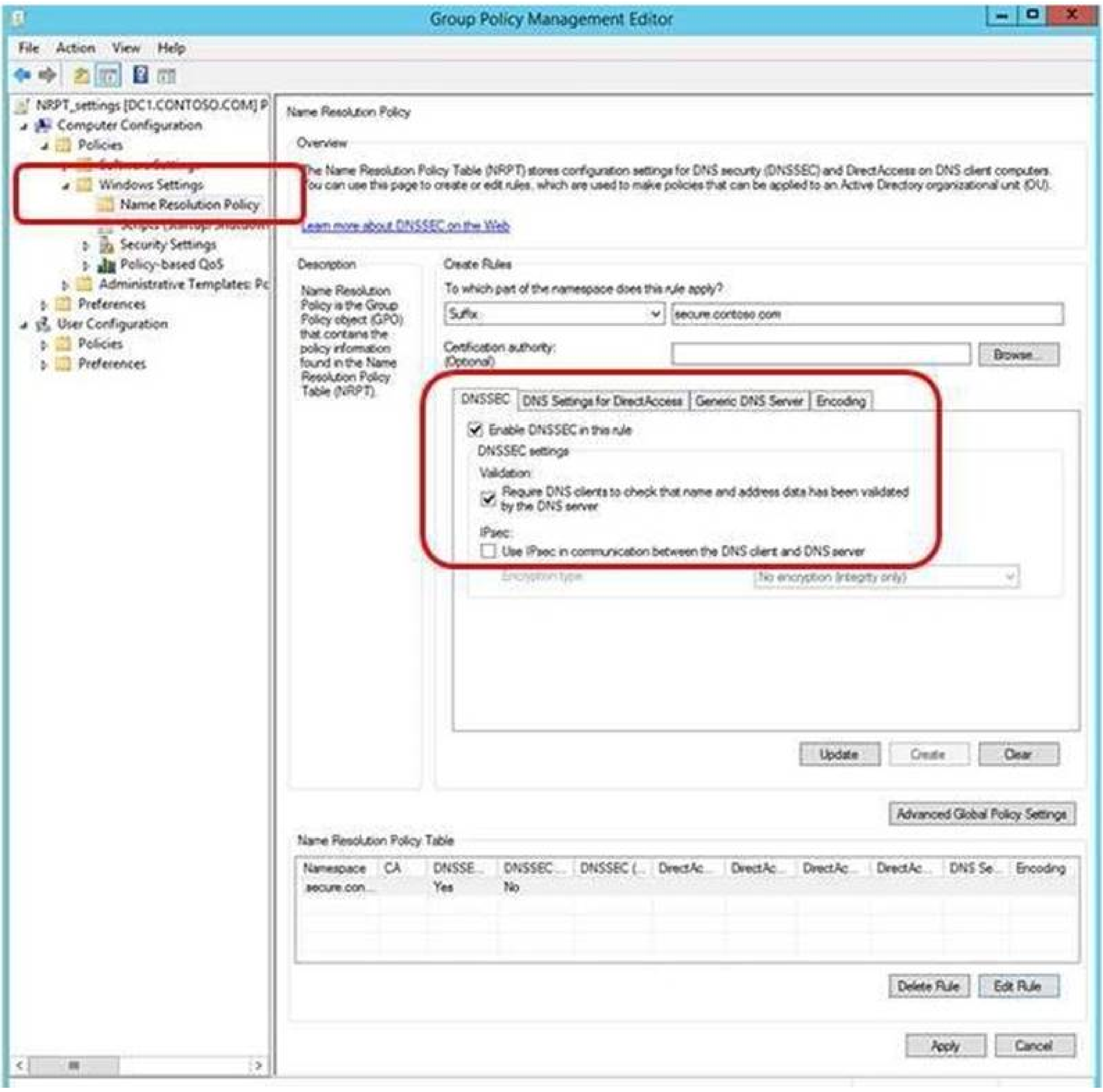
Answer: D

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.



The Name Resolution Policy Table (NRPT) stores configuration settings for DNS security (DNSSEC) and DirectAccess on DNS client computers. You can use this page to create or edit rules, which are used to make policies that can be applied to an Active Directory organizational unit (OU).

Name Resolution Policy is the Group Policy object (GPO) that contains the policy information found in the Name Resolution Policy Table (NRPT).

To which part of the namespace does this rule apply? Suffix: secure.contoso.com

Certification authority: (Optional)

☑ Enable DNSSEC in this rule

DNSSEC settings

Validation:

☑ Require DNS clients to check that name and address data has been validated by the DNS server

IPsec:

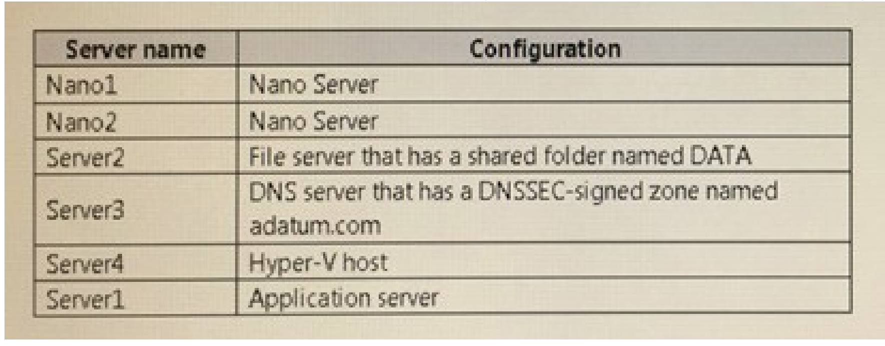
☐ Use IPsec in communication between the DNS client and DNS server

Encryption type: No encryption (integrity only)

Name Resolution Policy Table

Namespace	CA	DNSSE...	DNSSEC...	DNSSEC (...	DirectAc...	DirectAc...	DirectAc...	DirectAc...	DNS Se...	Encoding
secure.con...		Yes	No							

NEW QUESTION 16
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario b repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.
Start of repeated scenario
Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.
The domain contains the servers configured as shown m the following table.



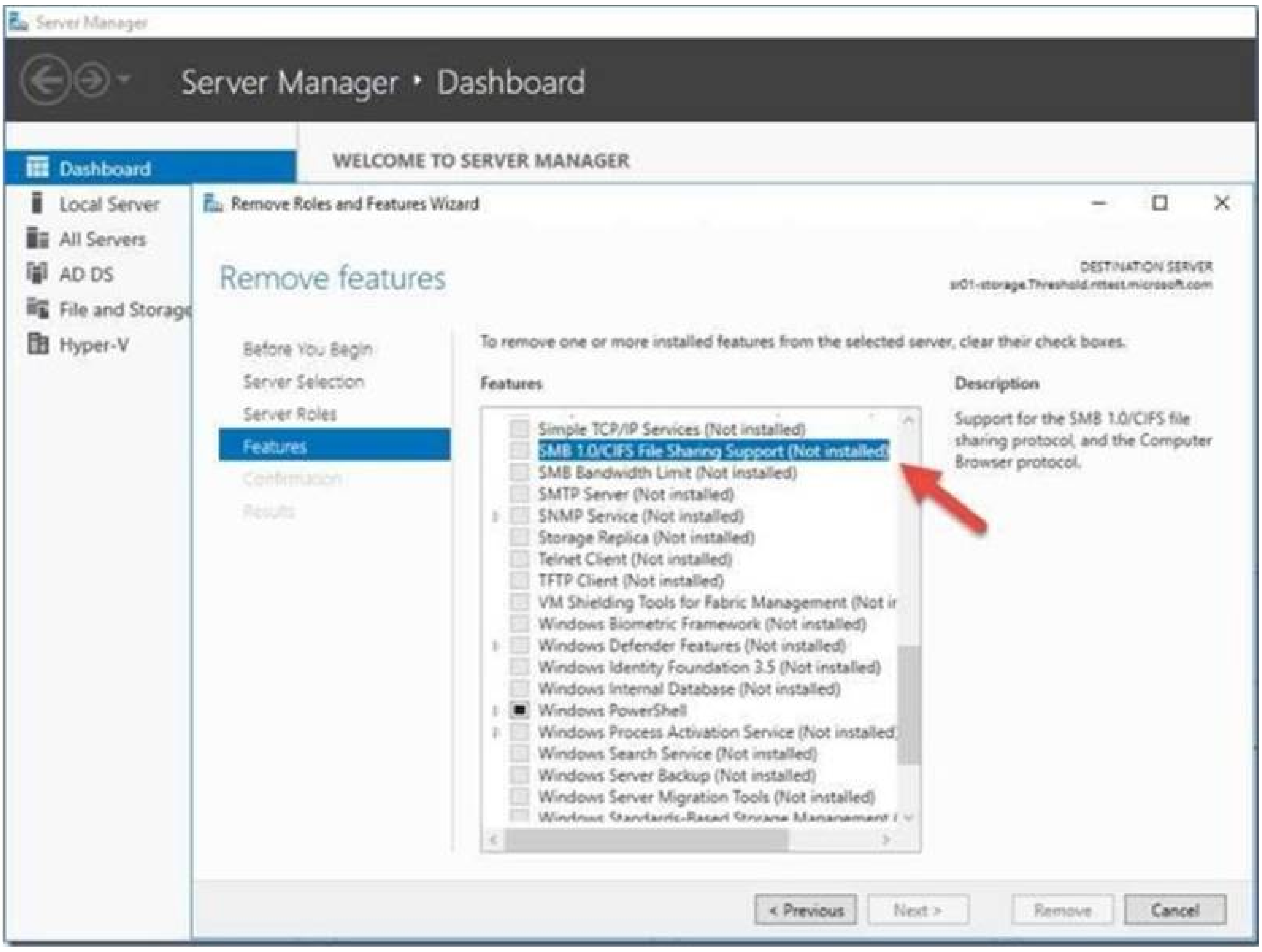
Server name	Configuration
Nano1	Nano Server
Nano2	Nano Server
Server2	File server that has a shared folder named DATA
Server3	DNS server that has a DNSSEC-signed zone named adatum.com
Server4	Hyper-V host
Server1	Application server

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

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

Answer: D

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



Server Manager

Server Manager • Dashboard

WELCOME TO SERVER MANAGER

Remove Roles and Features Wizard

Remove features

DESTINATION SERVER
sr01-storage.Threshold.nttest.microsoft.com

To remove one or more installed features from the selected server, clear their check boxes.

Features

☐ Simple TCP/IP Services (Not installed)
☐ SMB 1.0/CIFS File Sharing Support (Not installed)
☐ SMB Bandwidth Limit (Not installed)
☐ SMTP Server (Not installed)
☐ SNMP Service (Not installed)
☐ Storage Replica (Not installed)
☐ Telnet Client (Not installed)
☐ TFTP Client (Not installed)
☐ VM Shielding Tools for Fabric Management (Not ir
☐ Windows Biometric Framework (Not installed)
☐ Windows Defender Features (Not installed)
☐ Windows Identity Foundation 3.5 (Not installed)
☐ Windows Internal Database (Not installed)
■ Windows PowerShell
☐ Windows Process Activation Service (Not installed)
☐ Windows Search Service (Not installed)
☐ Windows Server Backup (Not installed)
☐ Windows Server Migration Tools (Not installed)
☐ Windows Standards-Based Storage Management (

Description

Support for the SMB 1.0/CIFS file sharing protocol, and the Computer Browser protocol.

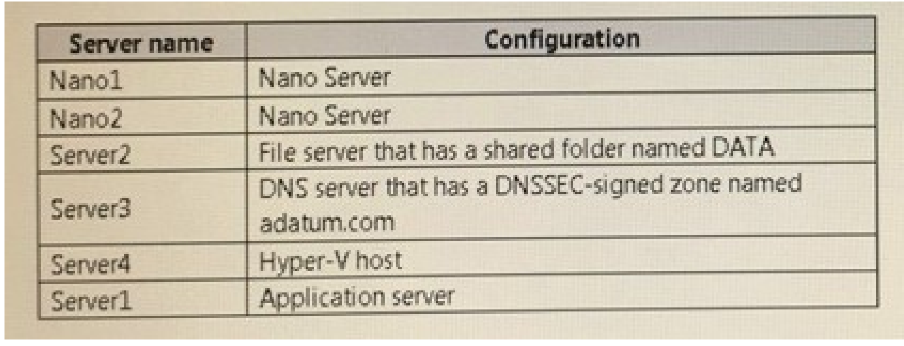
NEW QUESTION 21

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)

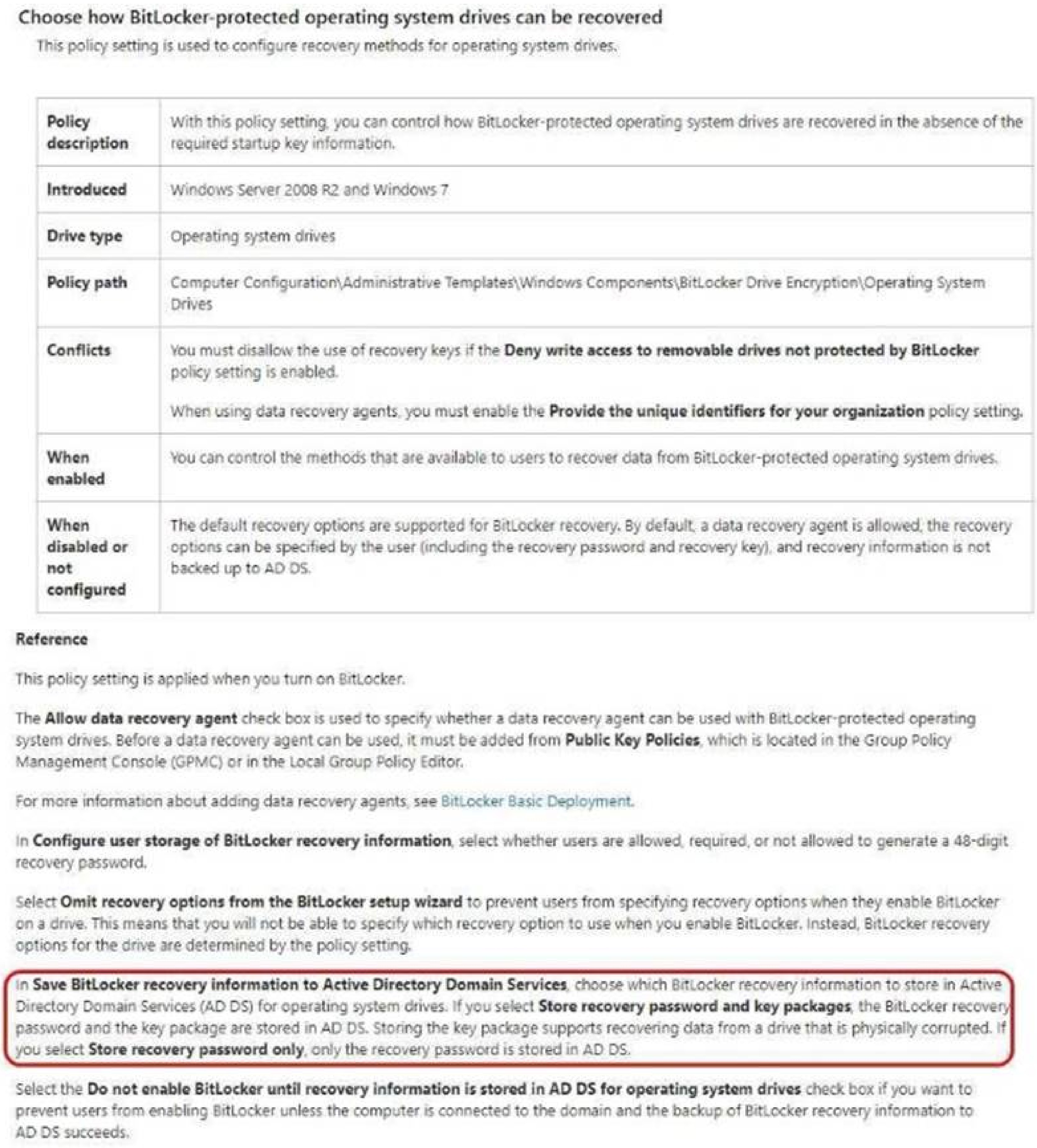
C. System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing

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.

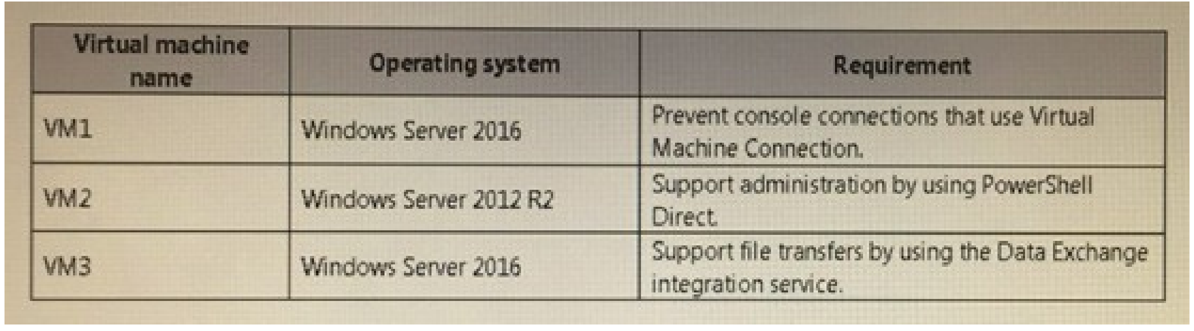
Select the **Do not enable BitLocker until recovery information is stored in AD DS for operating system drives** check box if you want to prevent users from enabling BitLocker unless the computer is connected to the domain and the backup of BitLocker recovery information to AD DS succeeds.

NEW QUESTION 22
Your network contains an Active Directory domain named contoio.com. The domain contains a server named Server1 that runs Windows Server 2016.
You have an organizational unit (OU) named Administration that contains the computer account of Server1.
You import the Active Directory module to Served1.
You create a Group Policy object (GPO) named GPO1 You link GPO1 to the Administration OU. You need to log an event each time an Active Directory cmdlet is executed successfully from Server1. What should you do?

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

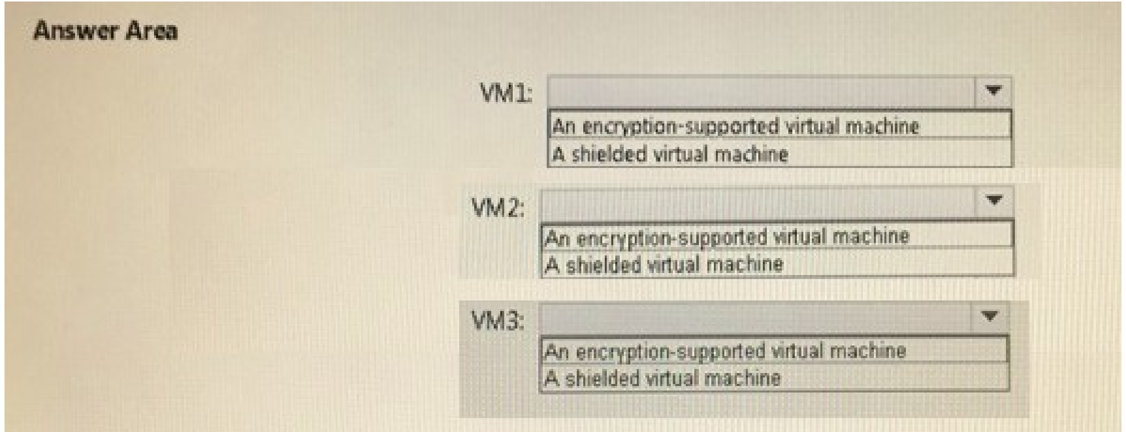
Answer: C

NEW QUESTION 27
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.



Answer Area

VM1:
- An encryption-supported virtual machine
- A shielded virtual machine

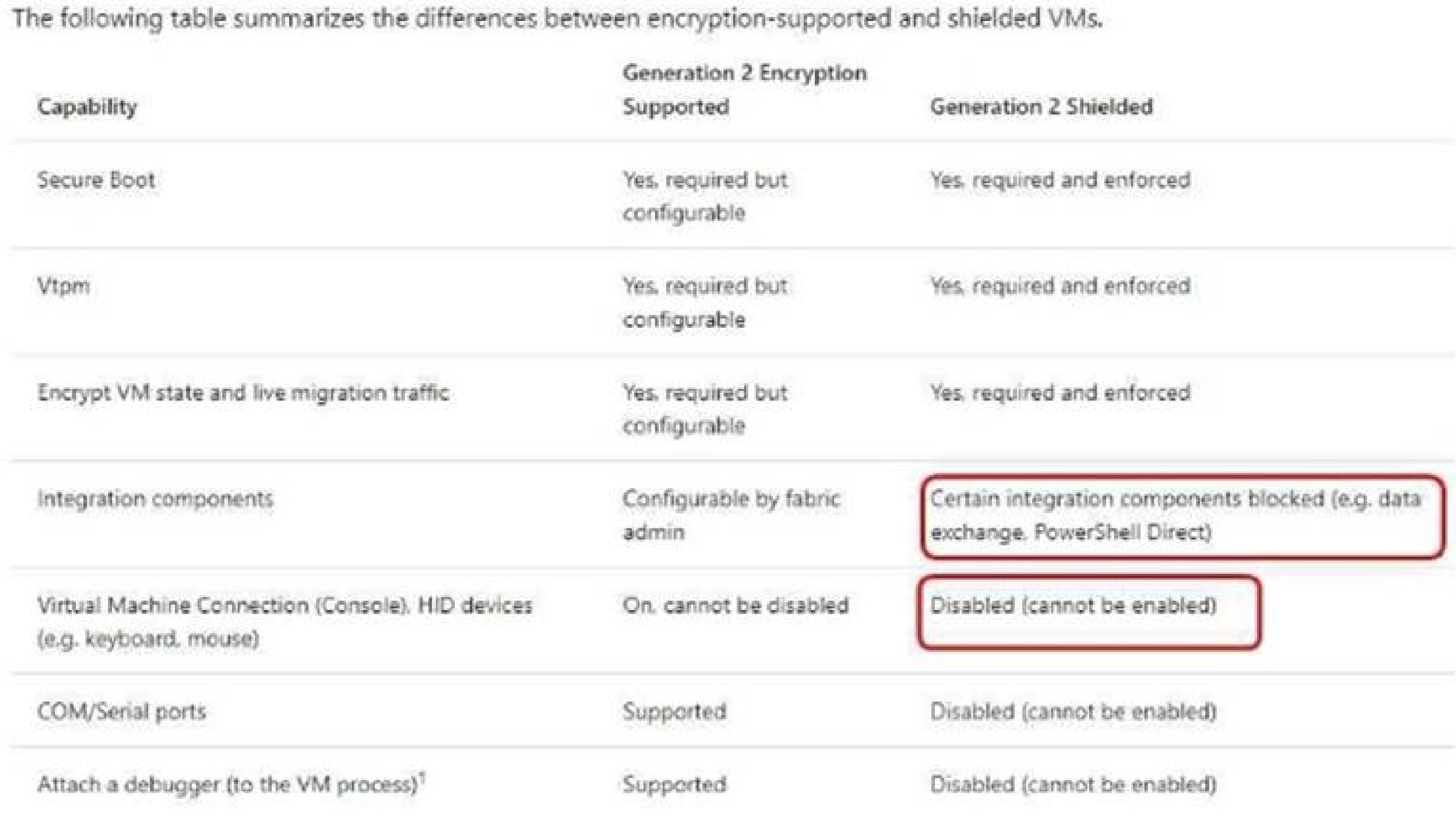
VM2:
- An encryption-supported virtual machine
- A shielded virtual machine

VM3:
- An encryption-supported virtual machine
- A shielded virtual machine

A. Mastered
B. Not Mastered

Answer: A

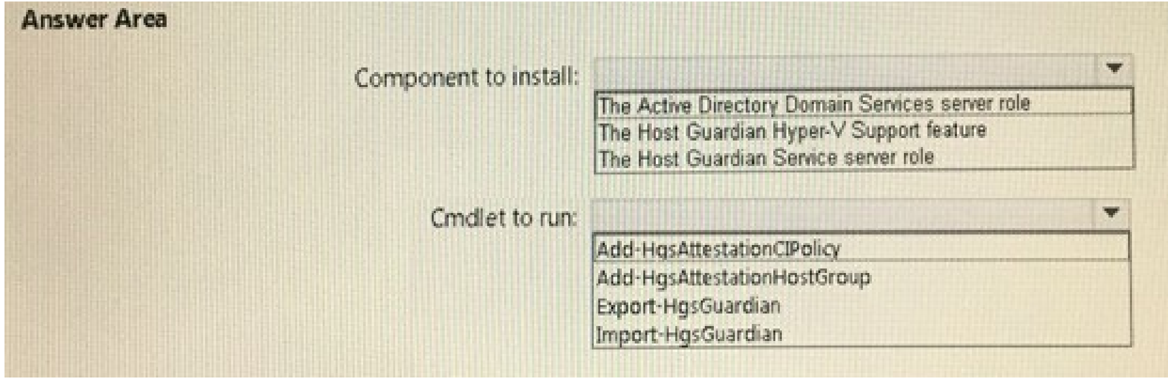
Explanation:
Shielded VM Prevents Virtual Machine connection and PowerShell Direct, it prevent the Hyper-V host to interact in any means with the Shielded VM.
https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shieldedvm/guarded-fabric-andshielded-vms



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 29
HOTSPOT
Your network contains two Active Directory forests named contoso.com and adatum.com. Contoso.com contains a Hyper-V host named Server1. Server1 is a member of a group named HyperHosts. Adatum.com contains a server named Server2. Server1 and Server2 run Windows Server 2016.
Contoso.com trusts adatum.com.
You plan to deploy shielded virtual machines to Server1 and to configure Admin-trusted attestation on Server2.
Which component should you install and which cmdlet should you run on Server2? To answer, select the appropriate options in the answer area.



Answer Area

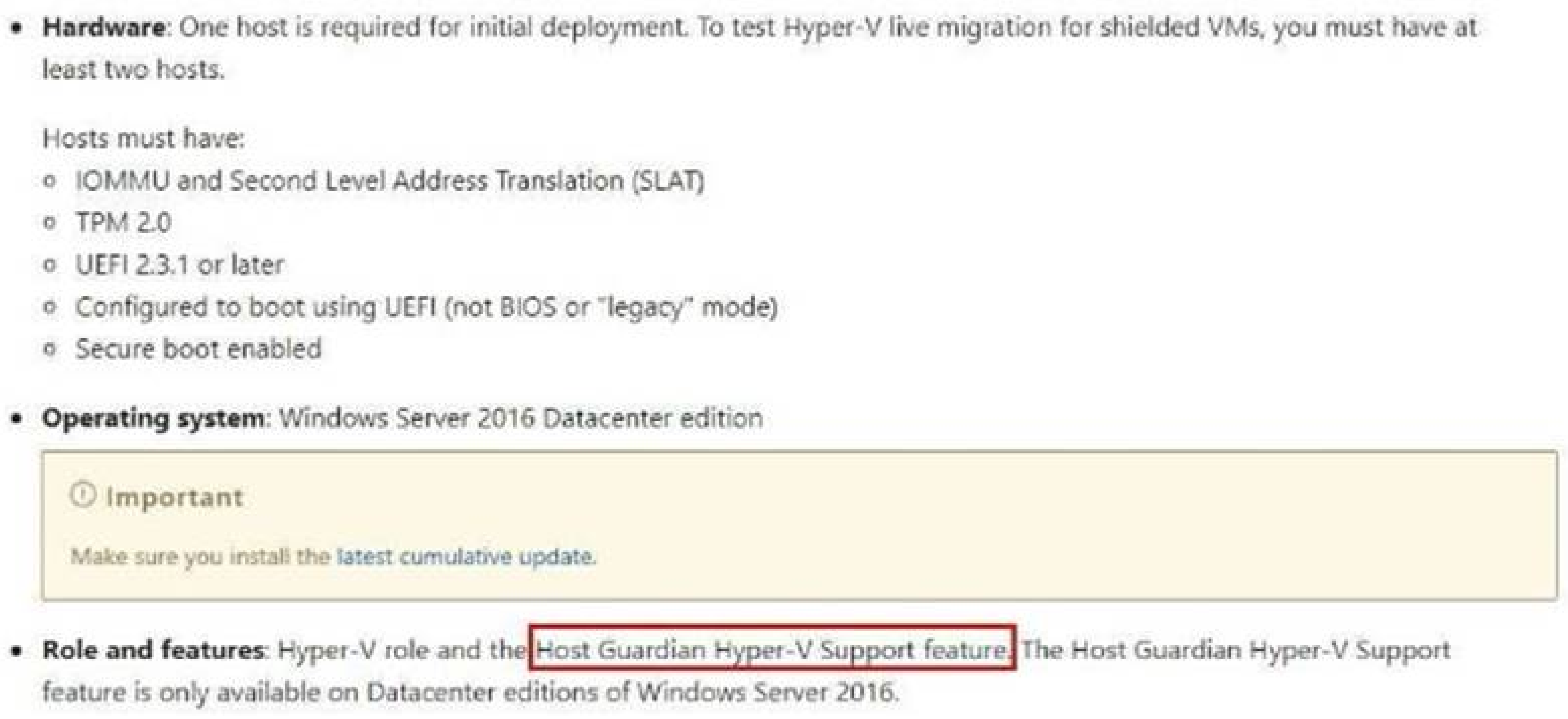
Component to install:
- The Active Directory Domain Services server role
- The Host Guardian Hyper-V Support feature
- The Host Guardian Service server role

Cmdlet to run:
- Add-HgsAttestationCIPolicy
- Add-HgsAttestationHostGroup
- Export-HgsGuardian
- Import-HgsGuardian

A. Mastered
B. Not Mastered

Answer: A

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



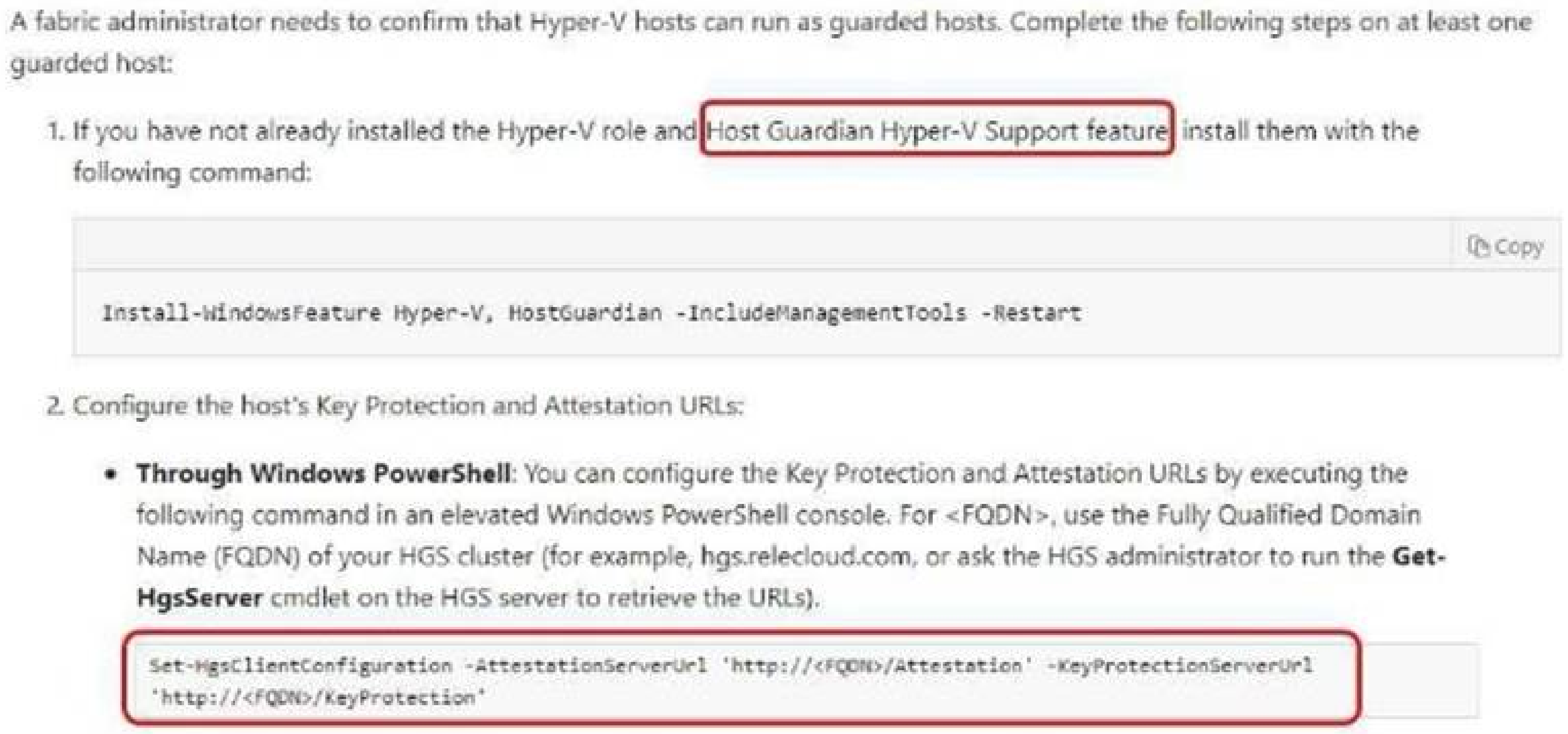
- **Hardware**: One host is required for initial deployment. To test Hyper-V live migration for shielded VMs, you must have at least two hosts.

  Hosts must have:
  - IOMMU and Second Level Address Translation (SLAT)
  - TPM 2.0
  - UEFI 2.3.1 or later
  - Configured to boot using UEFI (not BIOS or "legacy" mode)
  - Secure boot enabled
- **Operating system**: Windows Server 2016 Datacenter edition

  ⓘ Important

  Make sure you install the latest cumulative update.
- **Role and features**: Hyper-V role and the Host Guardian Hyper-V Support feature. The Host Guardian Hyper-V Support feature is only available on Datacenter editions of Windows Server 2016.

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



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

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

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

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

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

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

NEW QUESTION 34
The New-CIPolicy cmdlet creates a Code Integrity policy as an .xml file. If you do NOT supply either driver files or rules what will happen?

A. The cmdlet performs a system scan
B. An exception/warning is shown because either one is required
C. Nothing
D. The cmdlet searches the Code Integrity Audit log for drivers

Answer: A

Explanation:
If you do not supply either driver files or rules, this cmdlet performs a system scan similar to the Get- SystemDriver cmdlet.
The cmdlet generates rules based on Level. If you specify the Audit parameter, this cmdlet scans the Code Integrity Audit log instead.

NEW QUESTION 37
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 42
Windows PowerShell is a task-based command-line shell and scripting language designed especially for system administration.
Windows Defender comes with a number of different Defender-specific cmdlets that you can run through PowerShell to automate common tasks.
Which Cmdlet would you run first if you wanted to perform an offline scan?

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

Answer: A

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

NEW QUESTION 46
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 50
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 53
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

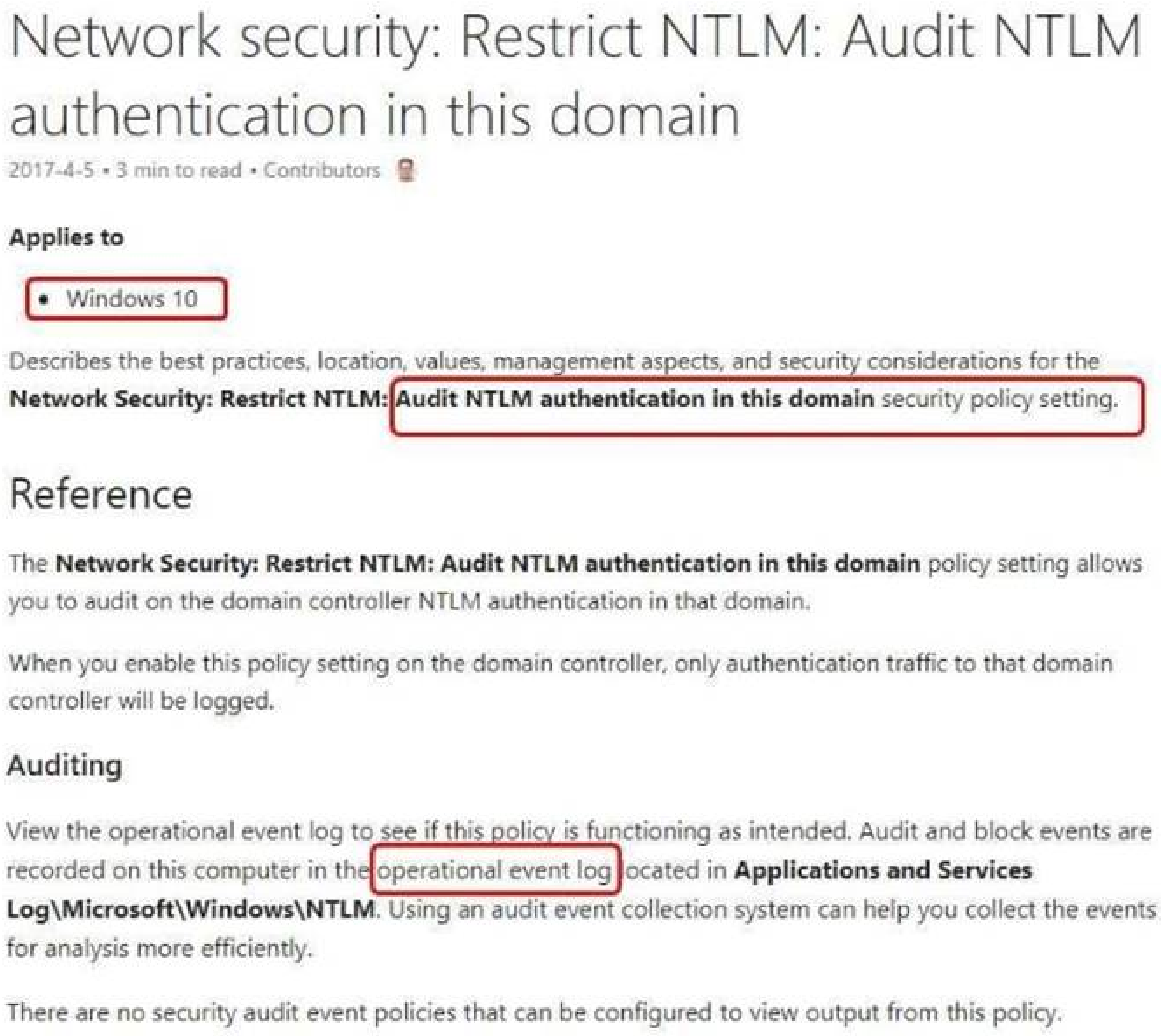
Answer: B

NEW QUESTION 55
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.

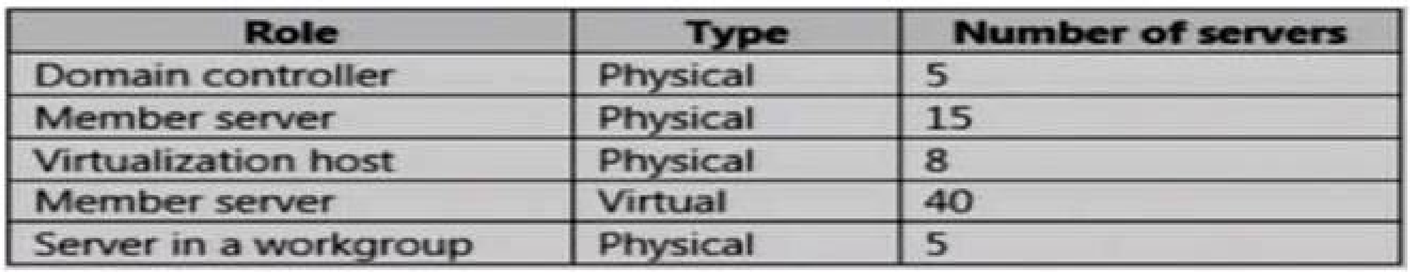
When you enable this policy setting on the domain controller, only authentication traffic to that domain controller will be logged.

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 56
You have the servers configured as shown in the following table.



Role	Type	Number of servers
Domain controller	Physical	5
Member server	Physical	15
Virtualization host	Physical	8
Member server	Virtual	40
Server in a workgroup	Physical	5

You purchase a Microsoft Azure subscription, and you create three Microsoft Operations Management Suite (OMS) workspaces named Workspace1, Workspace2, and Workspace3
You need to deploy Microsoft Monitoring Agent to the servers to meet the following requirements:
-Antimalware data from all the servers must be visible in Workspace1.
-Security and audit data from the domain controllers and the virtualization hosts must be visible in Workspace2.
-System update data from all the servers in all the workgroups must be visible in Workspace& How many OMS agents should you deploy?

A. 10
B. 33
C. 73
D. 45

Answer: C

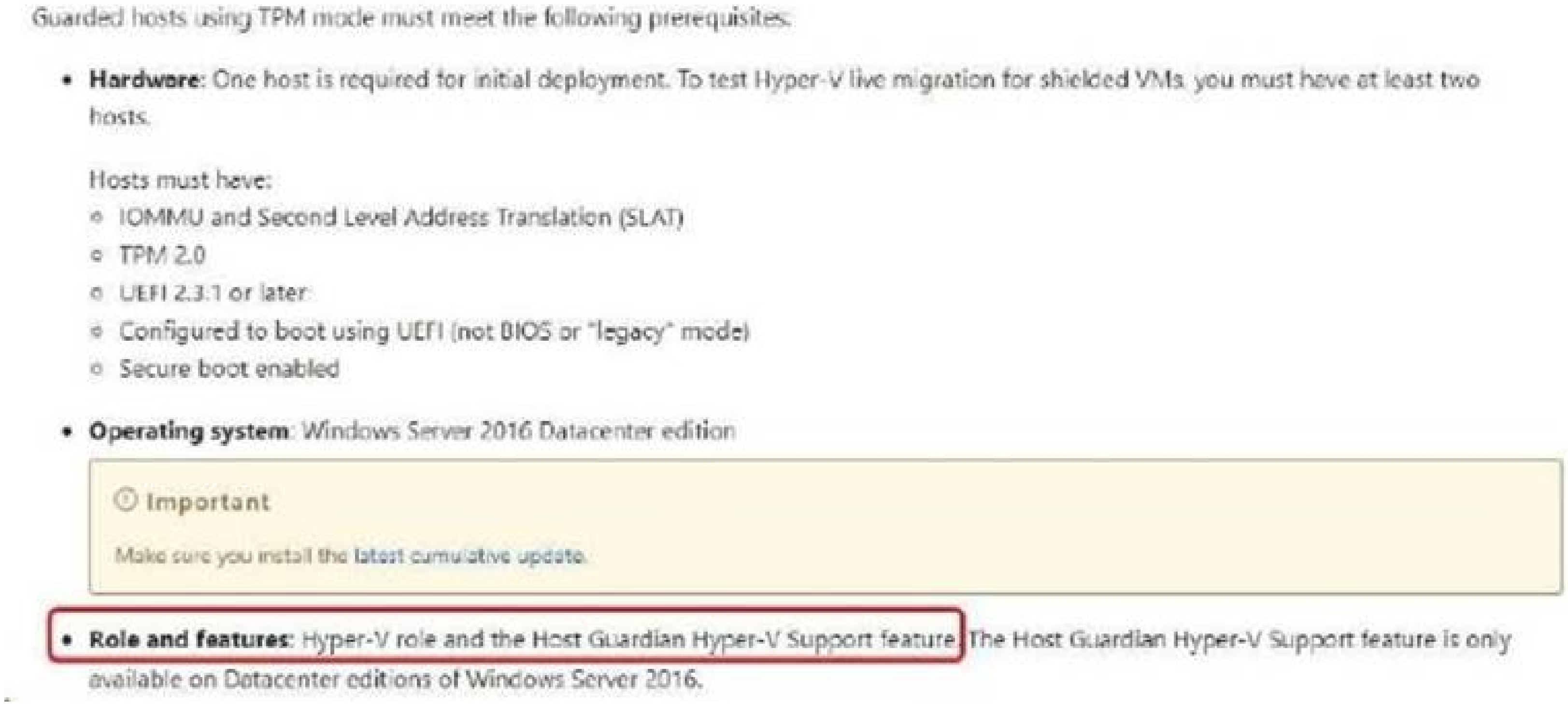
Explanation:
-Antimalware data from all the servers must be visible in Workspace1.
-Security and audit data from the domain controllers and the virtualization hosts must be visible in Workspace2.
-System update data from all the servers in all the workgroups must be visible in Workspace& “All the servers” mean all 5 domain controllers, plus all member servers (physical and virtual, domain and
workgroup) and virtualization hosts, so there are no exemptions.
All servers in the above table mentioned must install OMS Microsoft Monitoring agents

NEW QUESTION 59
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.

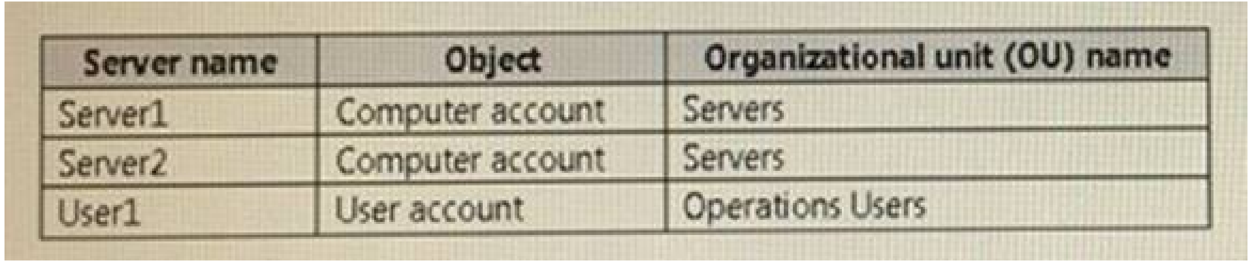
NEW QUESTION 64
Your network contains an Active Directory domain named contoso.com. The domain contains several Hyper-V hosts.
You deploy a server named Server22 to a workgroup. Server22 runs Windows Server 2016. You need to configure Server22 as the primary Host Guardian Service server.
Which three cmdlets should you run in sequence?

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

Answer: AEF

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

NEW QUESTION 69
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

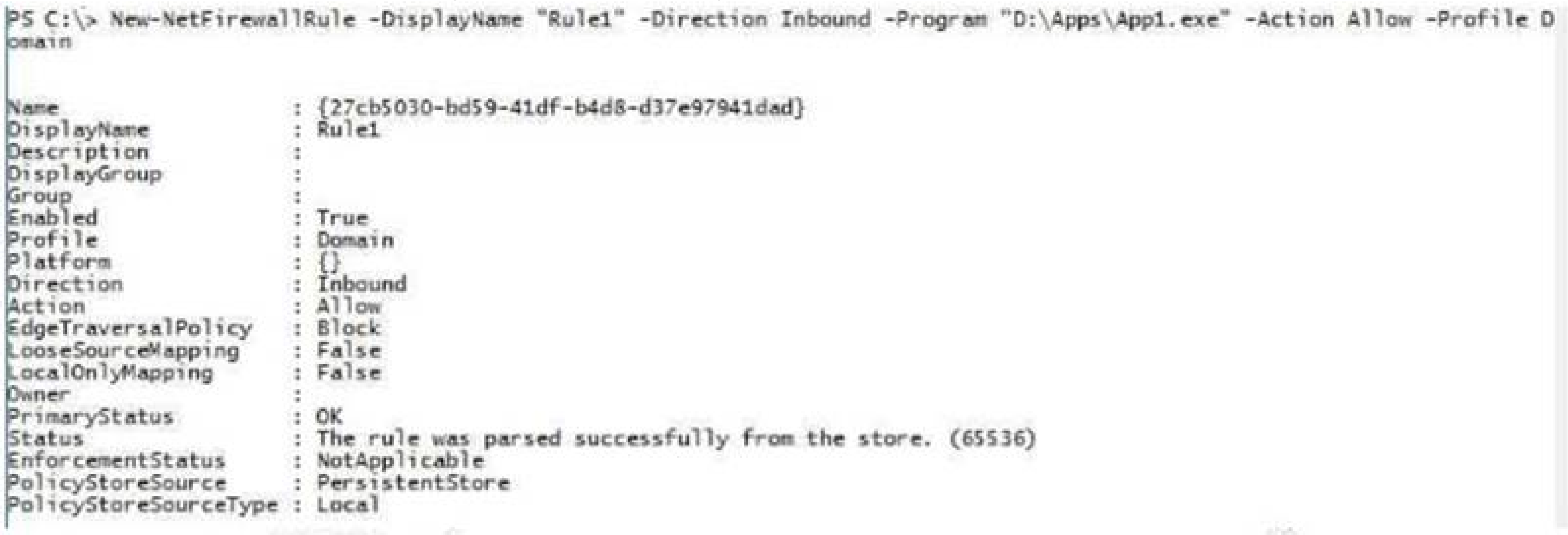
group cannot change security settings.

NEW QUESTION 72
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?

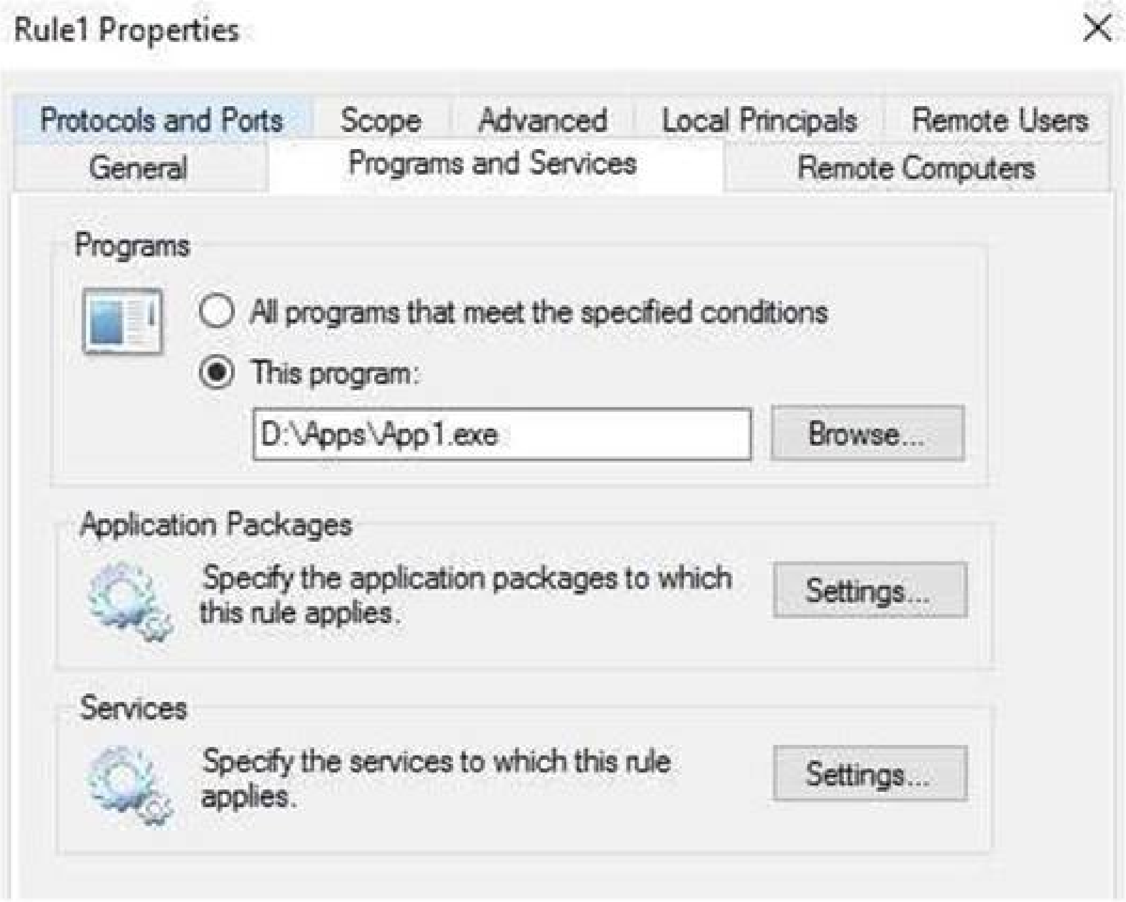
A. Yes
B. No

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
```



Rule1 Properties

Programs

○ All programs that meet the specified conditions

● This program:

D:\Apps\App1.exe

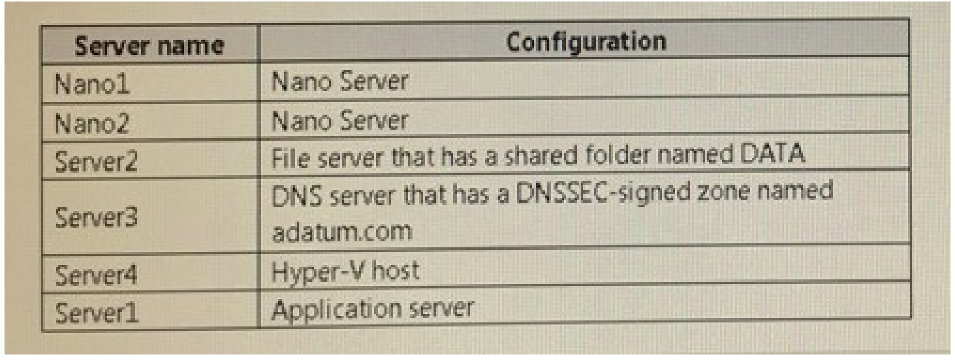
Application Packages

Specify the application packages to which this rule applies.

Services

Specify the services to which this rule applies.

NEW QUESTION 75
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.
Start of repeated scenario
Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.
The domain contains the servers configured as shown in the following table.



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

All servers run Windows Server 2016. All client computers run Windows 10.
You have an organizational unit (OU) named Marketing that contains the computers in the marketing department You have an OU named finance that contains the computers in the finance department You have an OU named AppServers that contains application servers. A Group Policy object (GPO) named GP1 is linked to

the Marketing OU. A GPO named GP2 is linked to the AppServers OU. You install Windows Defender on Nano1.
End of repeated scenario
You need to ensure that when a configuration change is made on Nano2, Nano2 will revert back to the original configuration automatically.
What should you do first?

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

Answer: B

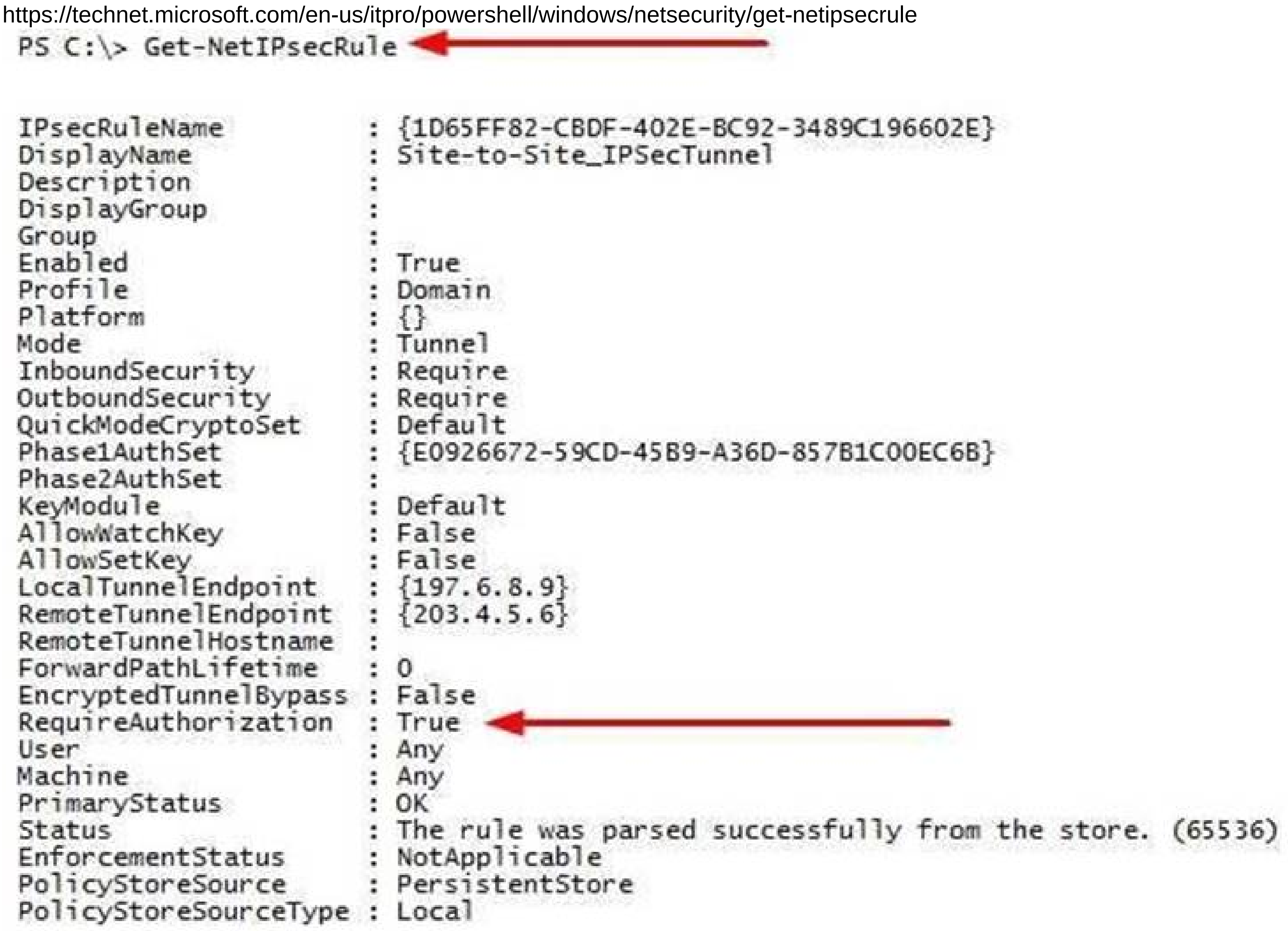
Explanation:
Using PowerShell DSC (Desire State Configuration) to mitigate configuration drift on Nano Server requires
additional steps, like installing the support package “Microsoft-NanoServer-DSC-Package” https://docs.microsoft.com/en-us/powershell/dsc/nanodsc
DSC on Nano Server is an optional package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

NEW QUESTION 80
You have a server named Server1 that runs Windows Server 2016.
You need to identify whether IPsec tunnel authorization is configured on Server1. Which cmdlet should you use?

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

Answer: A

Explanation:
https://technet.microsoft.com/en-us/itpro/powershell/windows/netsecurity/get-netipsecrule



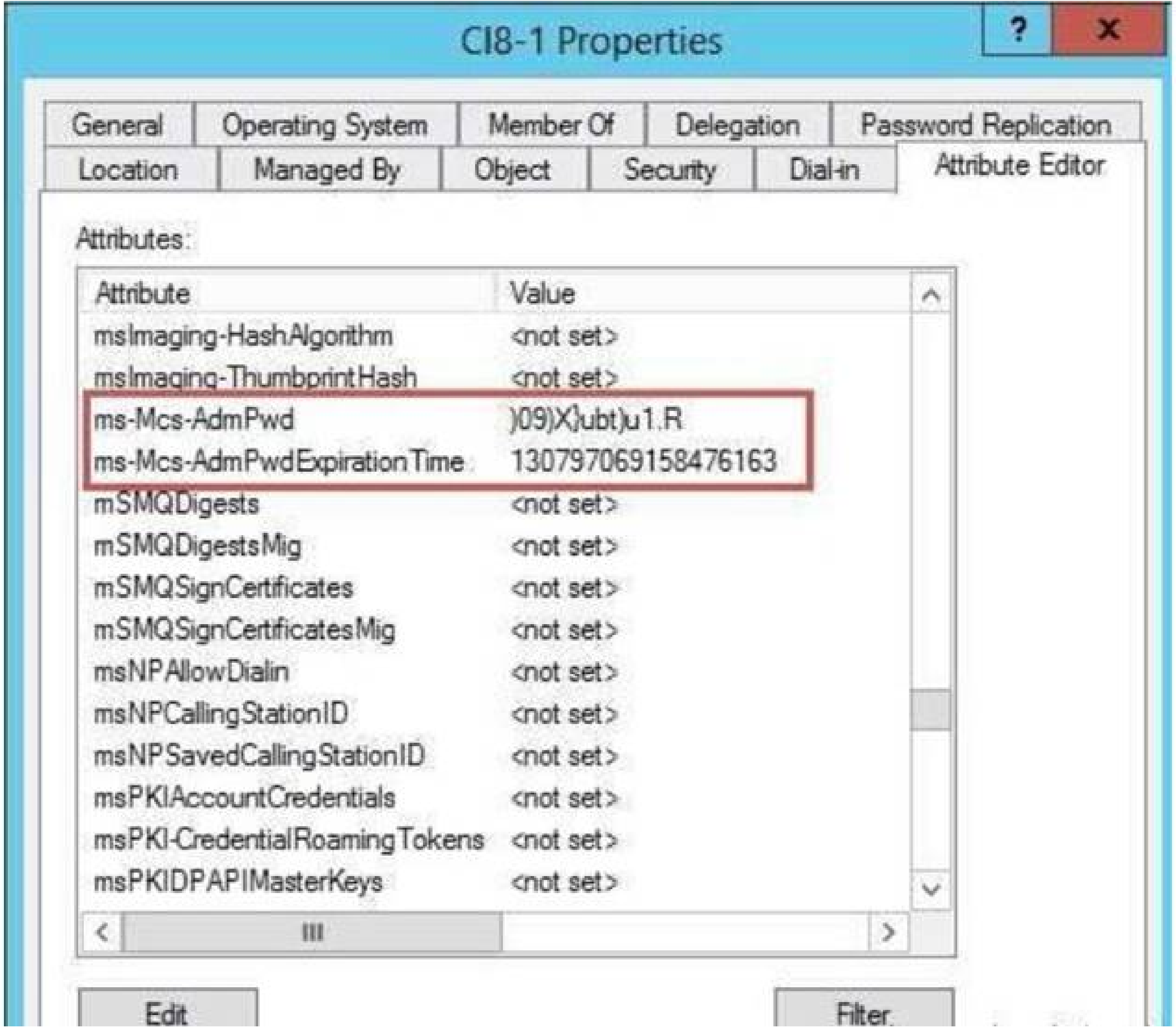
```
PS C:\> Get-NetIPsecRule


IPsecRuleName          : {1D65FF82-CBDF-402E-BC92-3489C196602E}
DisplayName            : Site-to-Site_IPSecTunnel
Description            :
DisplayGroup           :
Group                  :
Enabled                : True
Profile                : Domain
Platform               : {}
Mode                   : Tunnel
InboundSecurity        : Require
OutboundSecurity       : Require
QuickModeCryptoSet     : Default
Phase1AuthSet          : {E0926672-59CD-45B9-A36D-857B1C00EC6B}
Phase2AuthSet          :
KeyModule              : Default
AllowWatchKey          : False
AllowSetKey            : False
LocalTunnelEndpoint    : {197.6.8.9}
RemoteTunnelEndpoint   : {203.4.5.6}
RemoteTunnelHostname   :
ForwardPathLifetime    : 0
EncryptedTunnelBypass  : False
RequireAuthorization   : True
User                   : Any
Machine                : Any
PrimaryStatus          : OK
Status                 : The rule was parsed successfully from the store. (65536)
EnforcementStatus      : NotApplicable
PolicyStoreSource      : PersistentStore
PolicyStoreSourceType  : Local
```

NEW QUESTION 82
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

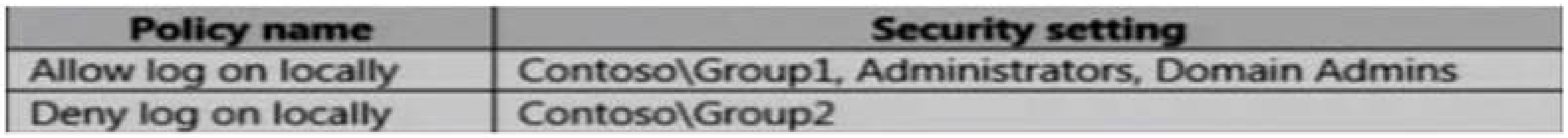
Answer: C

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.



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

NEW QUESTION 87
Your network contains an Active Directory domain named contoso.com.
The domain contains two global groups named Group1 and Group2. A user named User1 is a member of Group1
You have an organizational unit (OU) named OU1 that contains the computer accounts of computers that contain sensitive data. A Group Policy object (GPO) named GPO1 is linked to OU1. OU1 contains a computer account named Computer1.
GPO1 has the User Rights Assignment configured as shown in the following table.



Policy name	Security setting
Allow log on locally	Contoso\Group1, Administrators, Domain Admins
Deny log on locally	Contoso\Group2

You need to prevent User1 from signing in to Computer1. What should you do?

A. From Default Domain Policy, modify the Allow log on locally user right
B. On Computer1, modify the Deny log on locally user right.
C. From Default Domain Policy, modify the Deny log on locally user right
D. Remove User1 to Group2.

Answer: D

Explanation:
https://technet.microsoft.com/en-us/library/cc957048.aspx “Deny log on locally”
Computer Configuration\\Windows Settings\\Security Settings\\Local Policies\\User Rights Assignment
Determines which users are prevented from logging on at the computer.
This policy setting supercedes the Allow Log on locally policy setting if an account is subject to both policies.
Therefore, adding User1 to Group2 will let User1 to inherit both policy, and then prevent User1 to sign in to Computer1.

NEW QUESTION 92
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 97
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 101
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

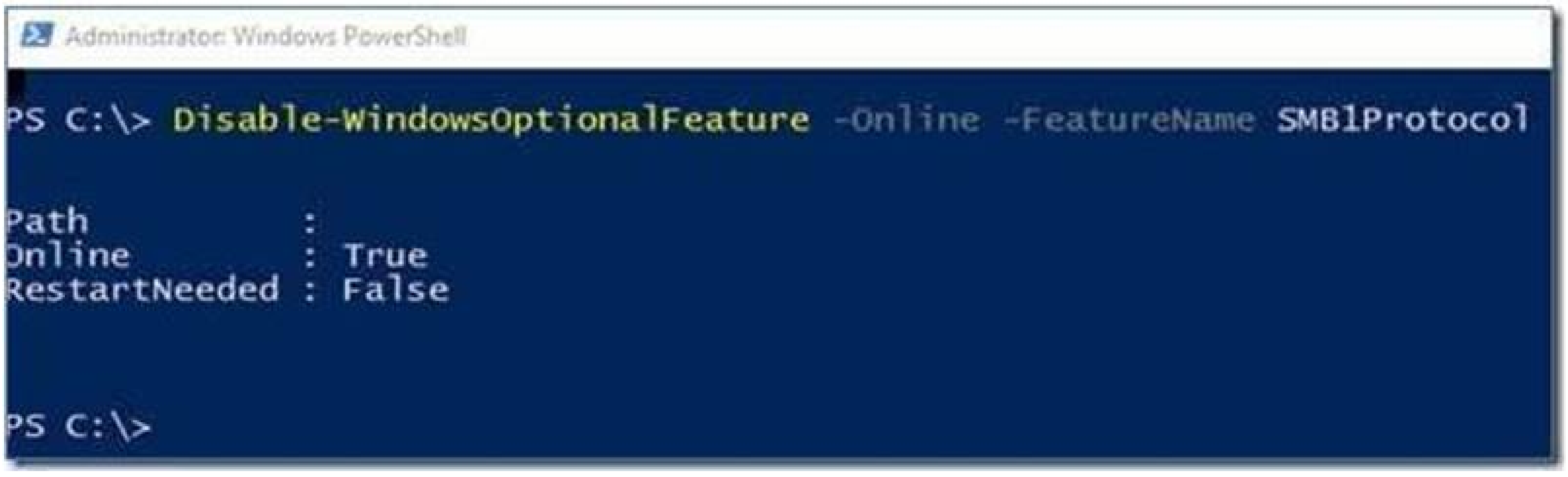
Explanation:
https://docs.microsoft.com/en-us/powershell/module/Microsoft.PowerShell.Core/getpssessioncapability? view=powershell-5.0.
The Get-PSSessionCapability cmdlet gets the capabilities of a specific user on a constrained session configuration.
Use this cmdlet to audit customized session configurations 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 102
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. You need to prevent NTLM authentication on Server1.
Solution: From Windows PowerShell, you run the Disable-WindowsOptionalFeature cmdlet. Does this meet the goal?

A. Yes
B. No

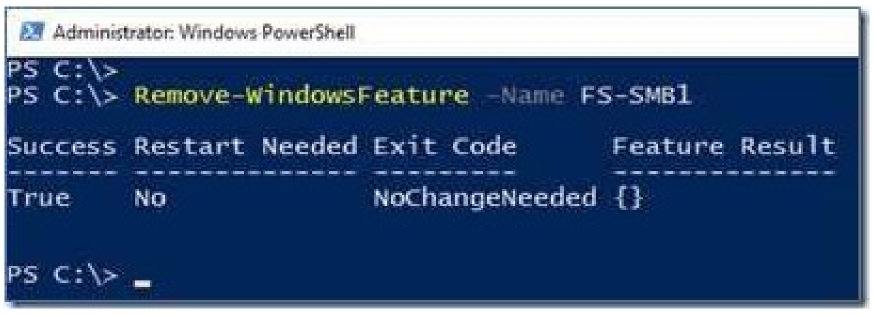
Answer: B

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



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


Path          :
Online        : True
RestartNeeded : False



PS C:\>
```

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



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

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


PS C:\> _
```

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

NEW QUESTION 105
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

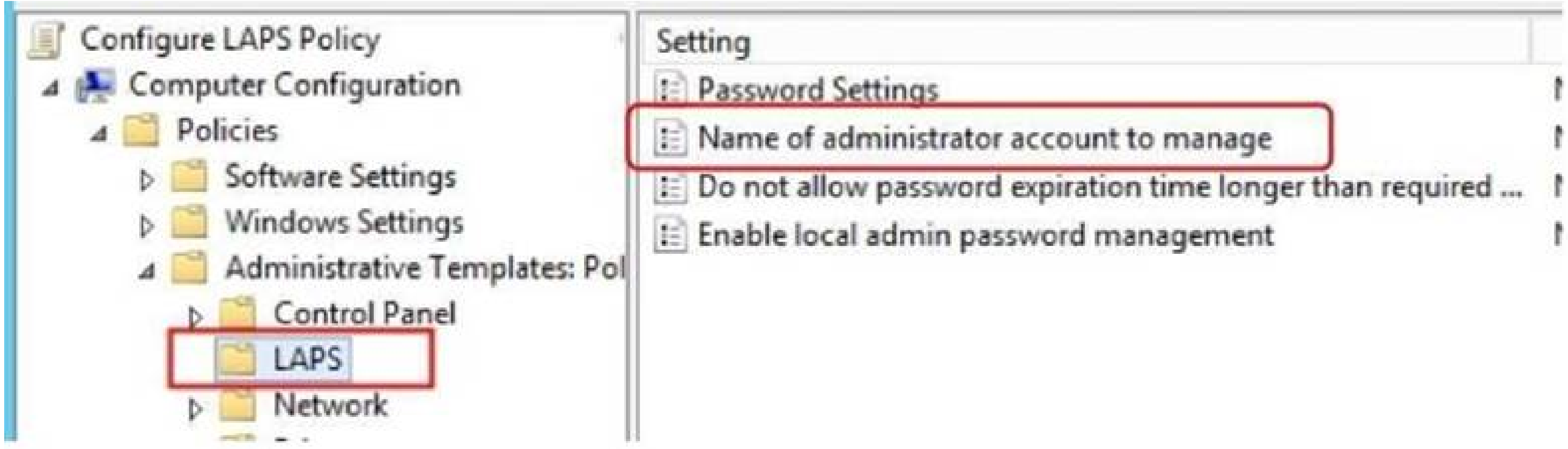
Explanation:
https://technet.microsoft.com/en-us/library/hh489604.aspx Import Your GPOs
You can import current settings from your GPOs and compare these to the Microsoft recommended best practices.
Start with a GPO backup that you would commonly create in the Group Policy Management Console (GPMC).
Take 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 107
Your network contains an Active Directory domain named contoso.com. All servers in the domain run Windows Server 2016.All client computers run Windows 10.
Your company has deployed the Local Administrator Password Solution (LAPS).
Client computers in the finance department are located in an organizational unit (OU) named Finance.
Each finance computer has a custom administrative account named FinAdmin. You discover that the FinAdmin accounts are not managed by LAPS.
You need to ensure that the FinAdmin accounts are managed by LAPS. What should you do?

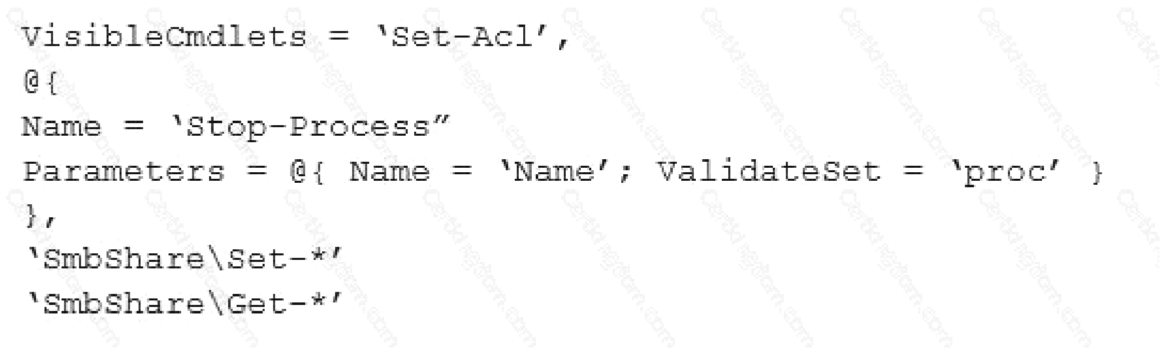
A. On the finance computers, register the AdmPwd.ps Windows PowerShell module and then run the ResetAdmPwdPassword cmdlet
B. Modify the Password Policy in a Group Policy object (GPO).
C. Modify the LAPS settings in a Group Policy object (GPO).
D. On the finance computer
E. rename the FinAdmin accounts to Administrato

Answer: C

Explanation:
Use the GPO Setting “Name of administrator account to manage” for LAPS to manage secondary administrative accounts which is not named as “Administrator”


Configure LAPS Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Pol
Control Panel
LAPS
Network
Setting
Password Settings
Name of administrator account to manage
Do not allow password expiration time longer than required ...
Enable local admin password management

NEW QUESTION 109
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.



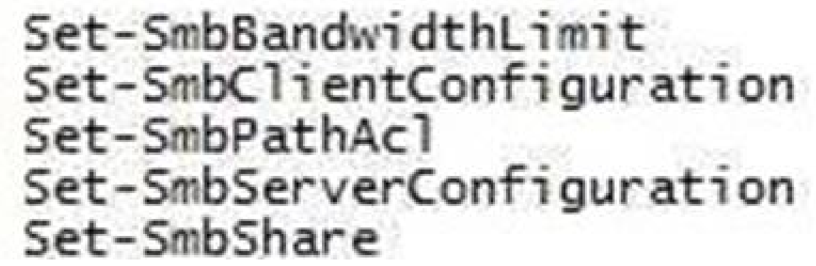
```
VisibleCmdlets = 'Set-Acl',
@{
Name = 'Stop-Process"
Parameters = @{ Name = 'Name'; ValidateSet = 'proc' }
},
'SmbShare\Set-*'
'SmbShare\Get-*'
```

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 113
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

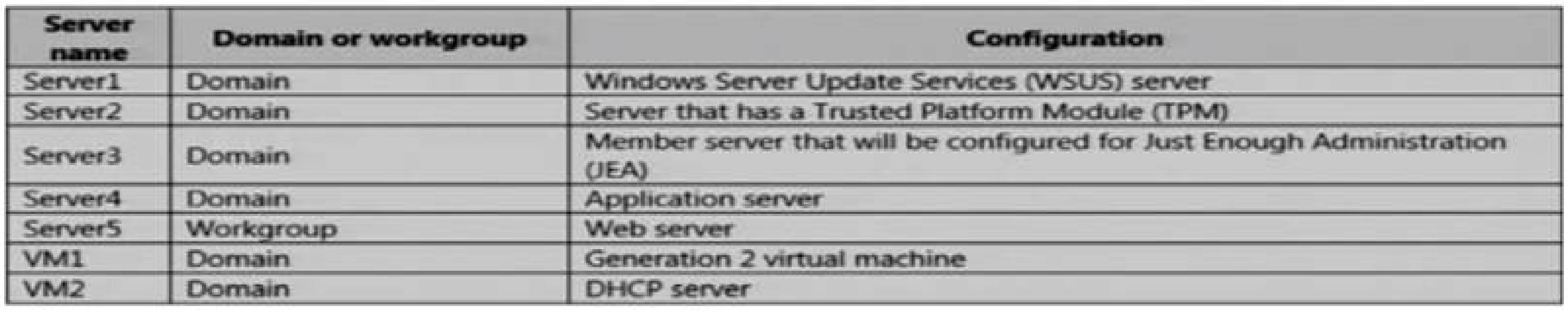
NEW QUESTION 117
Your network contains an Active Directory domain named contoso.com. The domain contains 100 servers.
You deploy the Local Administrator Password Solution (LAPS) to the network.
You discover that the members of a group named FinanceAdministrators can view the password of the local Administrator 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 119
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.



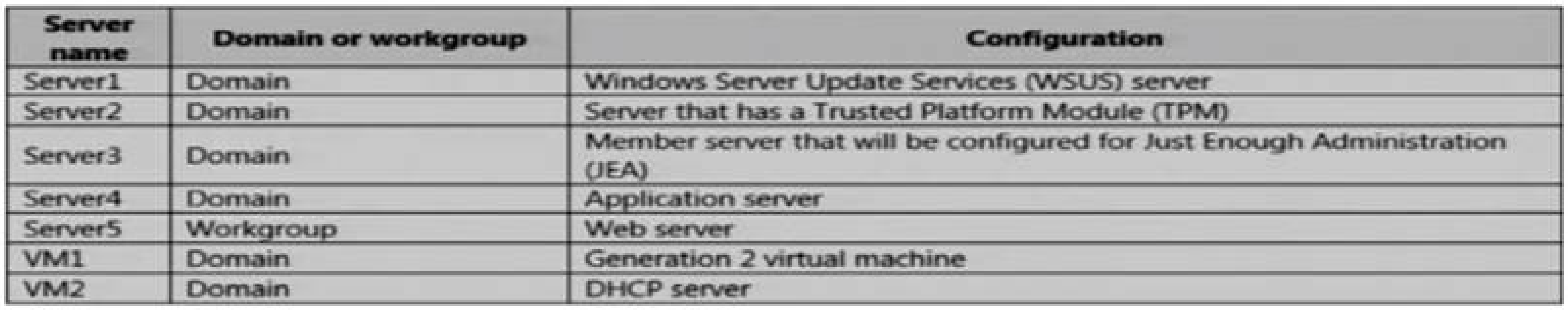
Server name	Domain or workgroup	Configuration
Server1	Domain	Windows Server Update Services (WSUS) server
Server2	Domain	Server that has a Trusted Platform Module (TPM)
Server3	Domain	Member server that will be configured for Just Enough Administration (JEA)
Server4	Domain	Application server
Server5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

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.
All laptops are protected by using BitLocker Drive Encryption (BitLocker).You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.
An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1.
A GPO named GP2 is linked to OU2.
All computers receive updates from Server1. You create an update rule named Update1.
You need to create a Role Capability file on Server3. Which file should you create?

A. File1.xml
B. File1.ini
C. File1.ps1
D. File1.psrc

Answer: D

NEW QUESTION 124
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

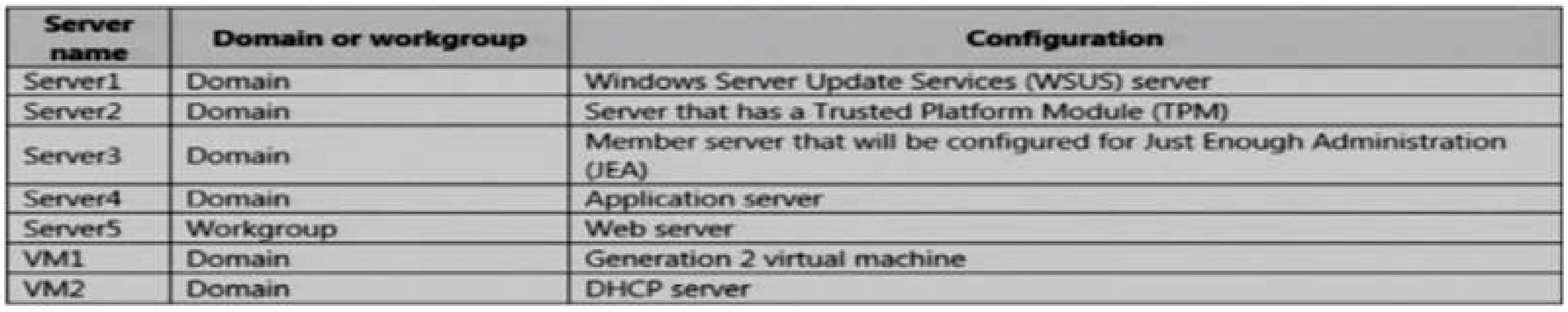
All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.
All laptops are protected by using BitLocker Drive Encryption (BitLocker).You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.
An OU named OU2 contains 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 AppLocker rules will apply to the marketing department computers. What should you do?

A. From the properties of OU2, modify the Security settings.
B. In GP2, configure the Startup type for the Application Identity service.
C. From the properties of OU2, modify the COM+ partition Set
D. In GP2, configure the Startup type for the Application Management servic

Answer: B

Explanation:
https://docs.microsoft.com/en-us/windows/device-security/applocker/configure-the-applicationidentity- service Because AppLocker uses this service “Application Identity” to verify the attributes of
a file, you must configure it to start automatically in at least one Group Policy object (GPO) that applies AppLocker rules.

NEW QUESTION 129
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

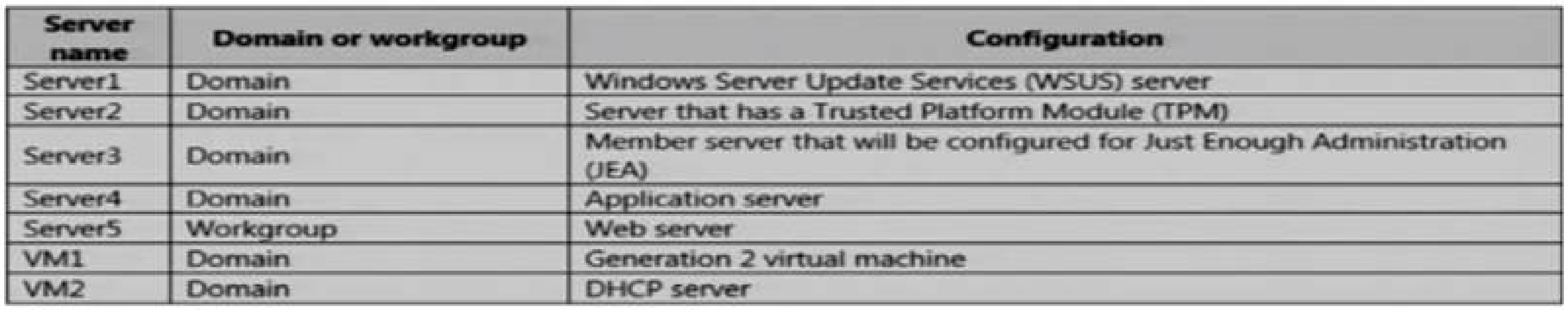
All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.
All laptops are protected by using BitLocker Drive Encryption (BitLocker).You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.
An OU named OU2 contains 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

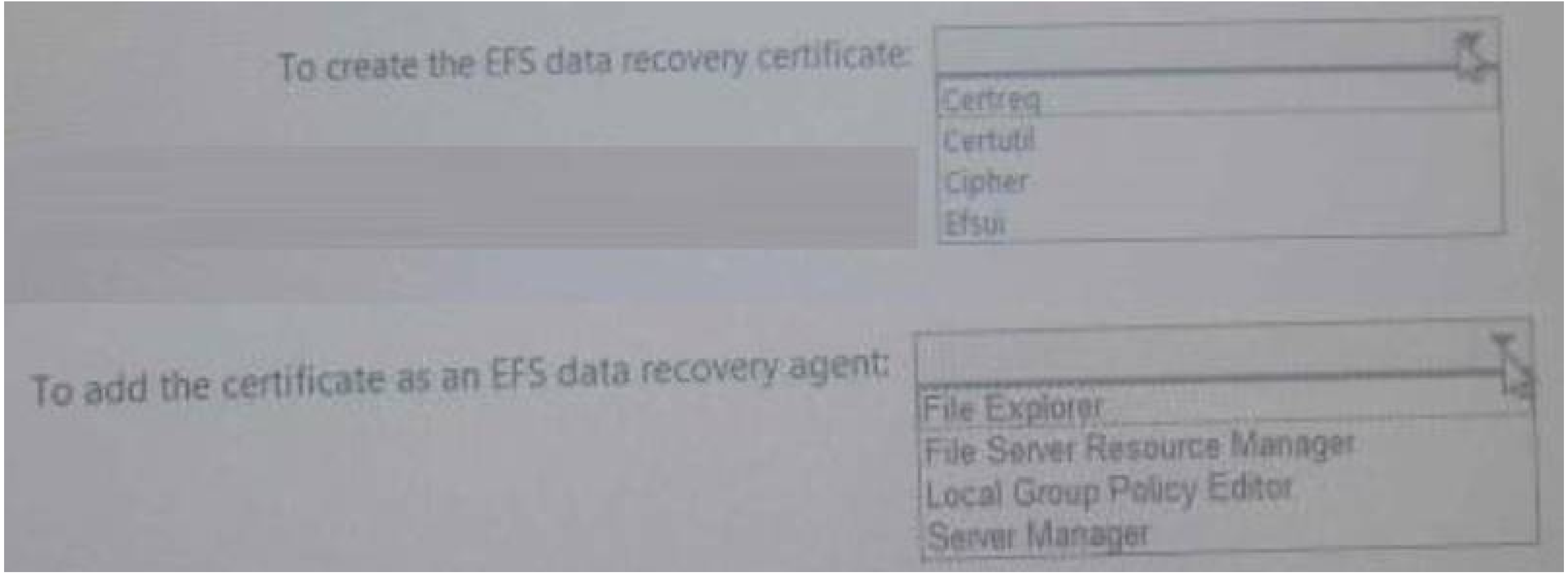
Explanation:
https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit_script
While Windows PowerShell already has the LogPipelineExecutionDetails Group Policy setting to log the
invocation of cmdlets, PowerShell’s scripting language has plenty of features that you might want to log and/or audit.
The 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 134
HOTSPOT
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.



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

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.
All laptops are protected by using BitLocker Drive Encryption (BitLocker).You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.
An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1.
A GPO named GP2 is linked to OU2.
All computers receive updates from Server1. You create an update rule named Update1.
You need to create an Encrypting File System (EFS) data recovery certificate and then add the certificate as an EFS data recovery agent on Server5.
What should you use on Server5? To answer, select the appropriate options in the answer area.



To create the EFS data recovery certificate:

To add the certificate as an EFS data recovery agent:

A. Mastered
B. Not Mastered

Answer: A

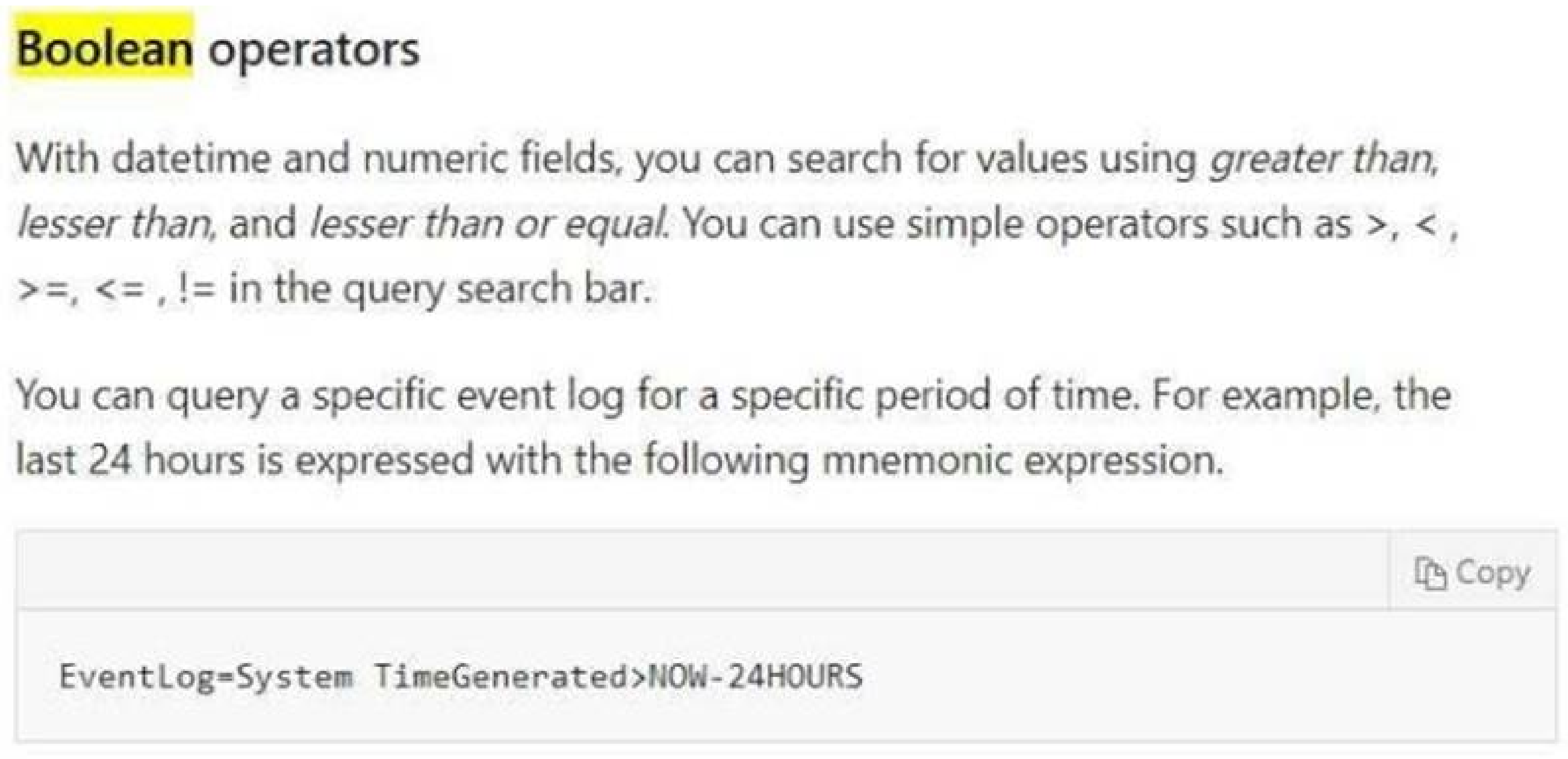
Explanation:
https://docs.microsoft.com/en-us/windows/threat-protection/windows-informationprotection/ create-and-verifyan-efs-dra-certificatecipher /R

NEW QUESTION 136
You implement Log Analytics in Microsoft Operations Management Suite (OMS) on all servers that run Windows Server 2016.
You need to generate a daily report that identifies which servers restarted during the last 24 hours. Which query should you use?

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

Answer: C

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



Boolean operators

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

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

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

NEW QUESTION 140
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

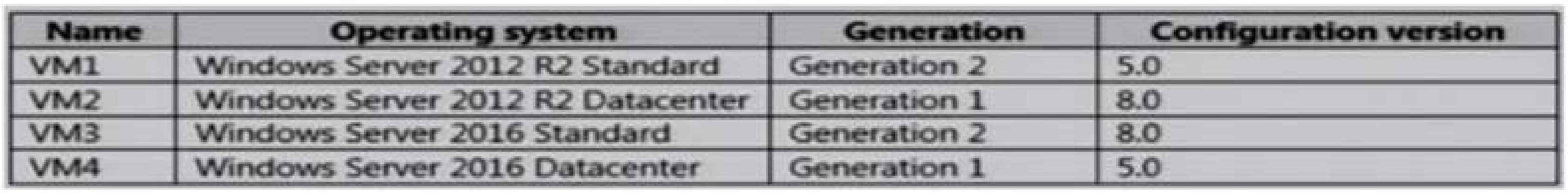
NEW QUESTION 144
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.
You have an organizational unit (OU) named Administration that contains the computer account of Server1.
You import the Active Directory module to Server1.
You create a Group Policy object (GPO) named GPO1. You link GPO1 to the Administration OU. You need to log an event each time an Active Directory cmdlet executed successfully from Server1. What should you do?

A. From Advanced Audit Policy in GPO1. configure auditing for other privilege use events.
B. Run the Add-NetEventProvider -Name “Microsoft-Active-Directory” -MatchAnyKeyword PowerShell command.
C. From Advanced Audit Policy in GPO1, configure auditing for directory service changes.
D. From Administrative Templates in GPO1, configure a Windows PowerShell polic

Answer: D

Explanation:
In the following GPO location, you can enable the setting “Turn on Module Logging” to record an
event each
time the PowerShell executes a cmdlet of a specific PowerShell module, for example “ActiveDirectory”.
“Computer Configuration\\Administrative Templates\\Windows Components\\Windows PowerShell”

NEW QUESTION 145
You have a Hyper-V host named Server1 that runs Windows Server 2016. Server1 hosts the virtual machines configured as shown in the following table.



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

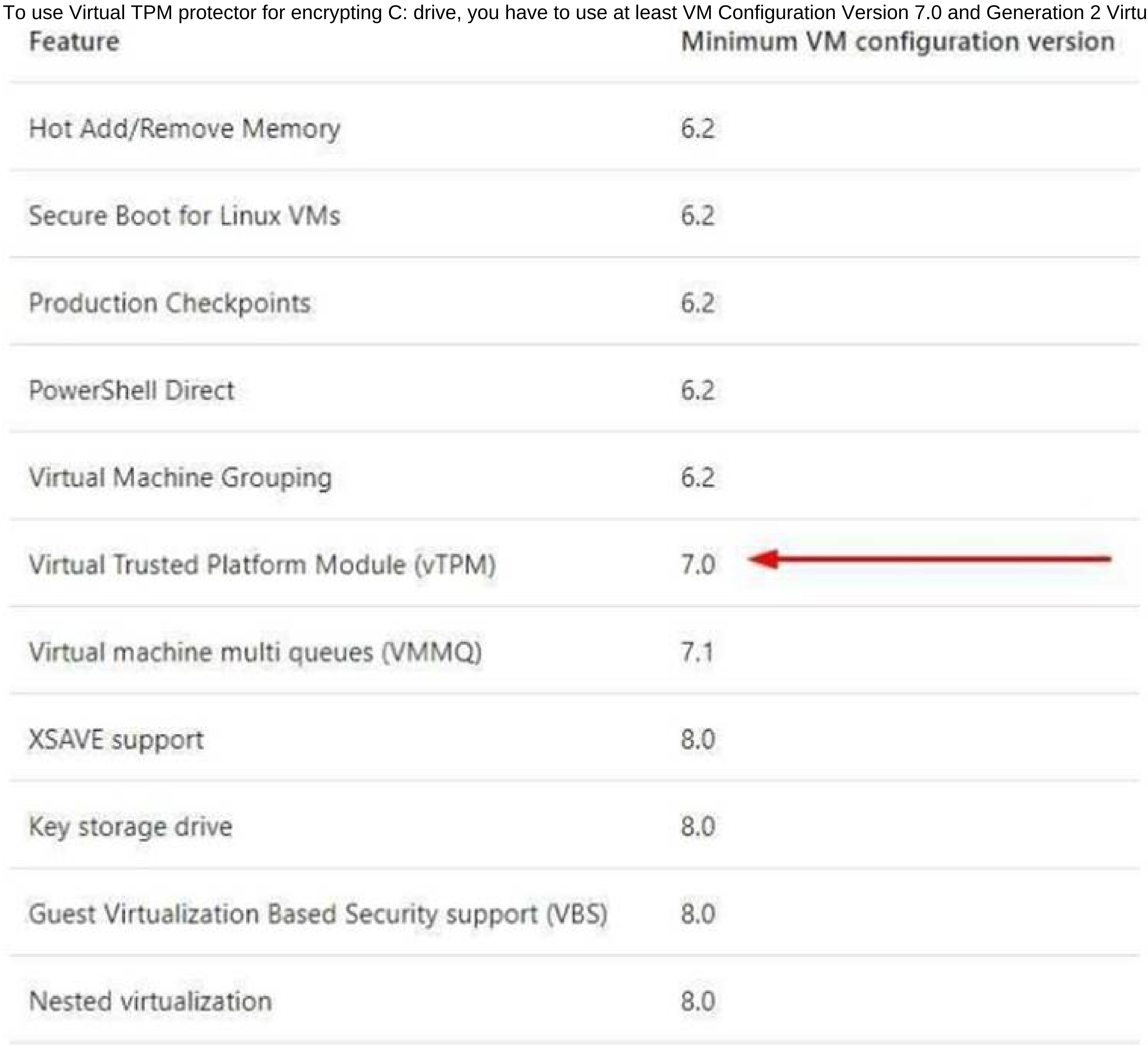
All the virtual machines have two volumes named C and D.
You plan to implement BitLocker Drive Encryption (BitLocker) on the virtual machines. Which virtual machines can have their volumes protected by using BitLocker? Choose Two.

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

G. Virtual machines that can have volume D protected by using BitLocker: VM3 only
H. Virtual machines that can have volume D protected by using BitLocker: VM1 and VM3 only
I. Virtual machines that can have volume D protected by using BitLocker: VM2 and VM3 only
J. Virtual machines that can have volume D protected by using BitLocker: VM2 and VM4 only
K. Virtual machines that can have volume D protected by using BitLocker: VM2, VM3 and VM4 only
L. Virtual machines that can have volume D protected by using BitLocker: VM1, VM2, VM3 and VM4

Answer: AG

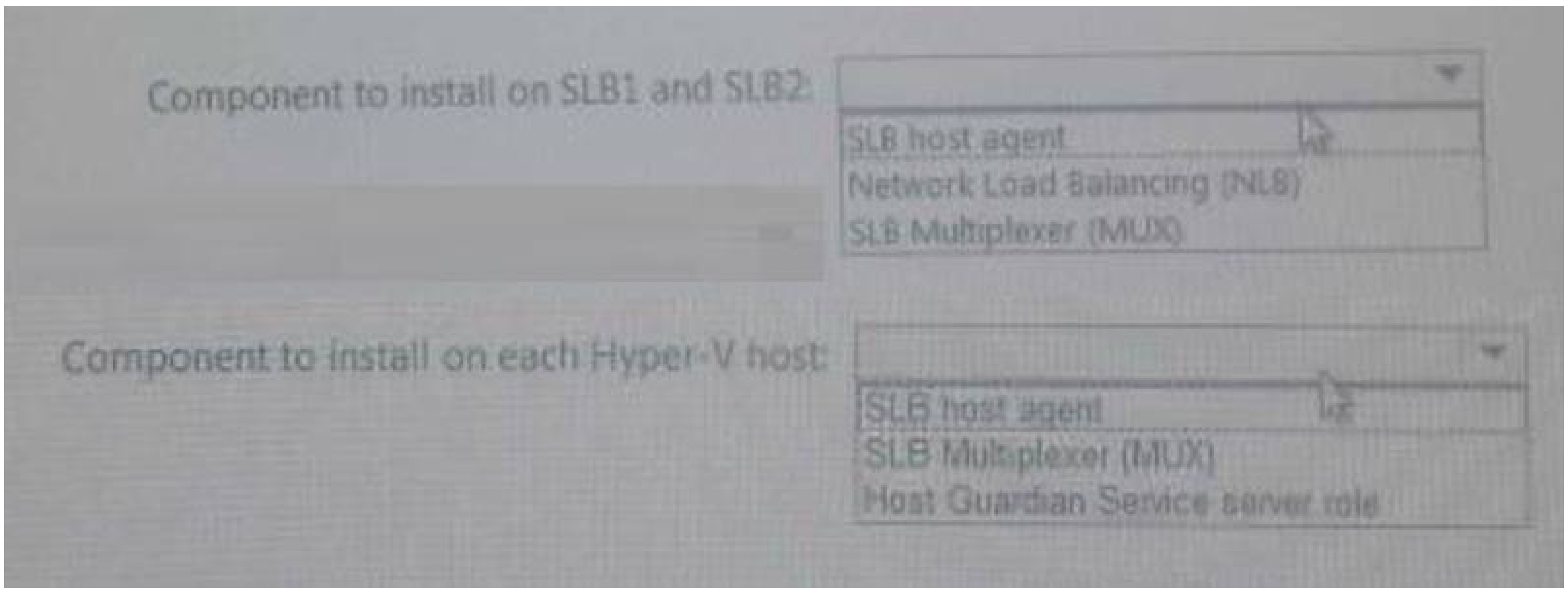
Explanation:
https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/deploy/upgrade-virtualmachine- versionin-hyper-v-on-windows-or-windows-server
To use Virtual TPM protector for encrypting C: drive, you have to use at least VM Configuration Version 7.0 and Generation 2 Virtual machines.



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

https://www.howtogeek.com/howto/6229/how-to-use-bitlocker-on-drives-without-tpm/
If you don’t use TPM for protecting a drive, there is no such Virtual TPM or VM Generation, or VM Configuration version requirement, you can even use Bitlocker without TPM Protector with earlier versions of Windows.

NEW QUESTION 149
HOTSPOT
You have 10 Hyper-V hosts that run Windows Server 2016.
Each Hyper-V host has eight virtual machines that run a distributed web application named App1. You plan to implement a Software Load Balancing (SLB) solution for client access to App1. You deploy two new virtual machines named SLB1 and SLB2.
You need to install the required components on the Hyper-V hosts and the new servers for the planned implementation.
Which components should you install? Select the Appropriate in selection area.



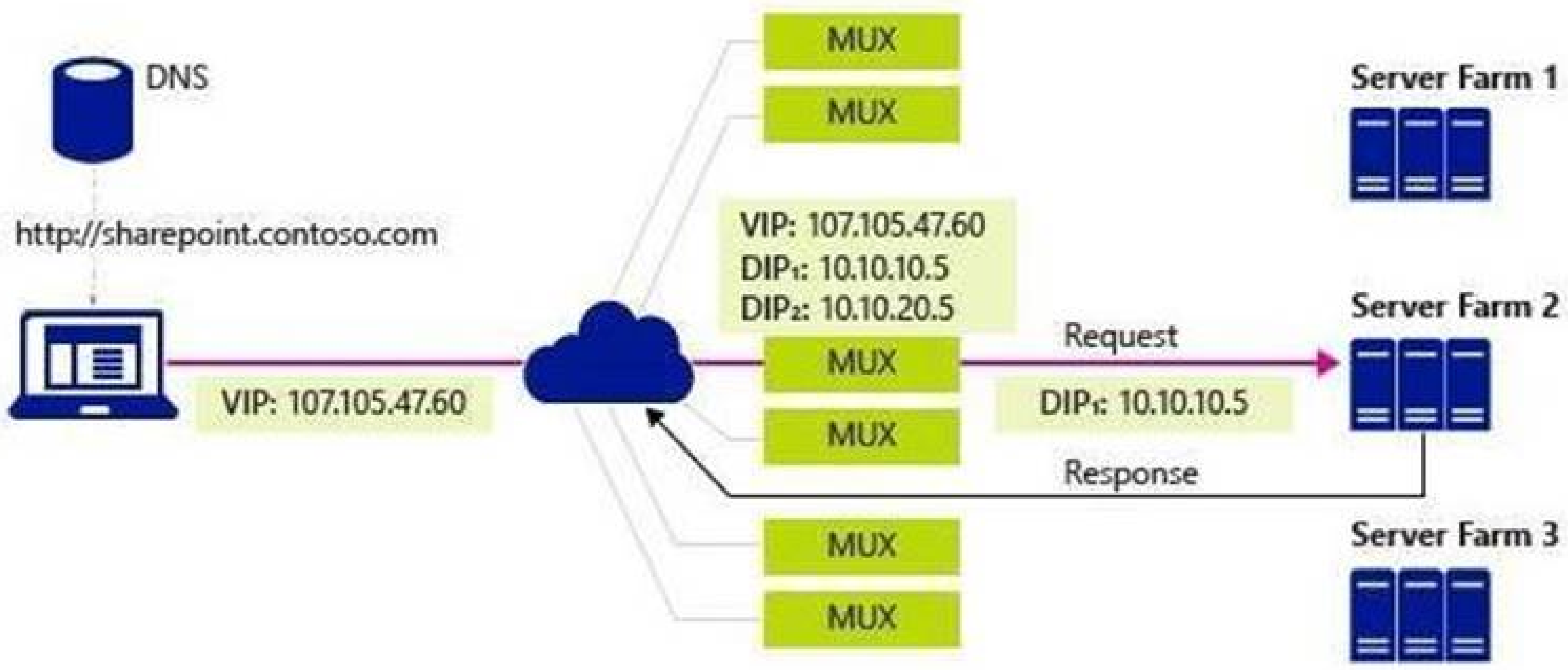
Component to install on SLB1 and SLB2:
- SLB host agent
- Network Load Balancing (NLB)
- SLB Multiplexer (MUX)

Component to install on each Hyper-V host:
- SLB host agent
- SLB Multiplexer (MUX)
- Host Guardian Service server role

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.



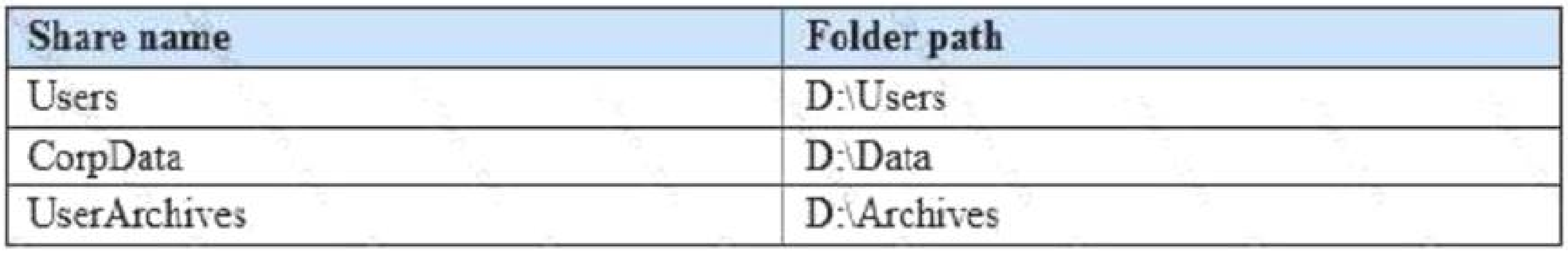
NEW QUESTION 153
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. You need to prevent NTLM authentication on Server1.
Solution: From Windows PowerShell, you run the New-ADAuthenticationPolicy cmdlet. Does this 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 154
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?

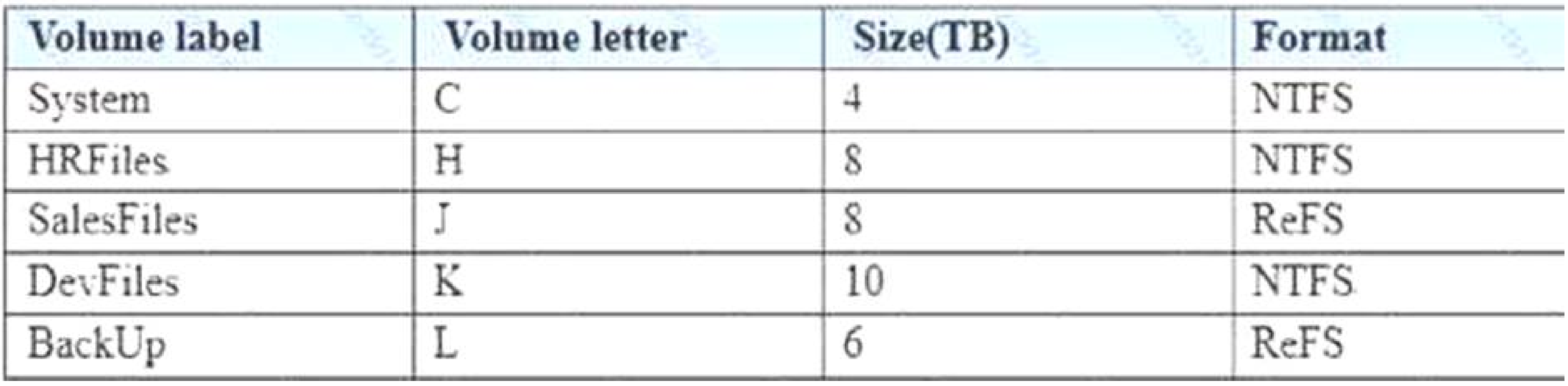
A. From File Explorer, open the properties of volume D, and then modify the Quota settings.
B. Install the File Server Resource Manager role service, and then create a file screen.
C. From File Explorer, open the properties of D:\Users, and then modify the Advanced sharing settings.
D. Install the File 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 159
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 Lock-BitLocker cmdlet.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

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

NEW QUESTION 160
You have a file server named FS1 that runs Windows Server 2016. You plan to disable SMB 1.0 on the server.
You need to verify which computers access FS1 by using SMB 1.0. What should you run first?

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

Answer: D

NEW QUESTION 164
......