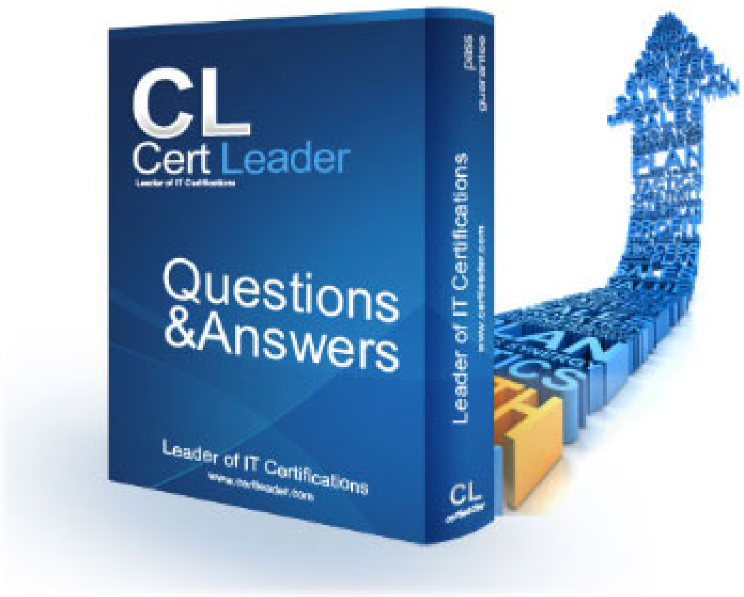
70-744 Dumps

Securing Windows Server 2016

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



NEW QUESTION 1
Note: This question is part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to It. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory forest named contoso.com. All servers run Windows Server 2016. The forest contains 2#W client computers that run Windows 10. All client computers are deployed (rom a customized Windows image.
You need to deploy 10 Privileged Access Workstations (PAWs). The solution must ensure that administrators can access several client applications used by all users.
Solution: You deploy 10 physical computers and configure each will as a virtualization host. You deploy the operating system on each host by using the customized Windows image. On each host you create a guest virtual machine and configure the virtual machine as a PAW.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 2
Note: This question is part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question In this section, you will NOT be able to return to It. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. Computer1 connects to a home network and a corporate network.
The corporate network uses the 172.16.0.0/24 address space internally. Computer1 runs an application named App1 that listens to port 8080.
You need to prevent connections to App1 when Computer1 is connected to the home network. Solution: From Group Policy Management, You create an Applocker rule.

A. Yes
B. No

Answer: B

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

NEW QUESTION 3
Note: This question It part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goats. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to It. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. Computer1 connects to a home network and a corporate network.
The corporate network uses the 17216.0.0/24 address space internally. Computer1 runs an application named App1 that listens to port 8080.
You need to prevent connections to App1 when Computer1 is connected to the home network. Solution: From Group Policy Management you create a software restriction policy.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 4
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question In this section, you will NOT be able to return to It. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. Computer1 connects to a home network and a corporate network.
The corporate network uses the 172.16.0.0/24 address space internally. Computer1 runs an application named App1 that listens to port 8080.
You need to prevent connections to App1 when Computer1 is connected to the home network. Solution: From Windows Firewall in the Control Panel, you add an application and allow the application to communicate through the firewall on a Private network.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

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

NEW QUESTION 5
Note: This question Is part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to It, As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains multiple Hyper-V hosts.
You need to deploy several critical line-to-business applications to the network to meet the following requirements:
*The resources of the applications must be isolated (rom the physical host.
*Each application must be prevented from accessing the resources of the other applications.
*The configurations of the applications must be accessible only from the operating system that hosts the application.
Solution: You deploy a separate Hyper-V container for each application. Does this meet the goal?

A. Yes
B. No

Answer: A

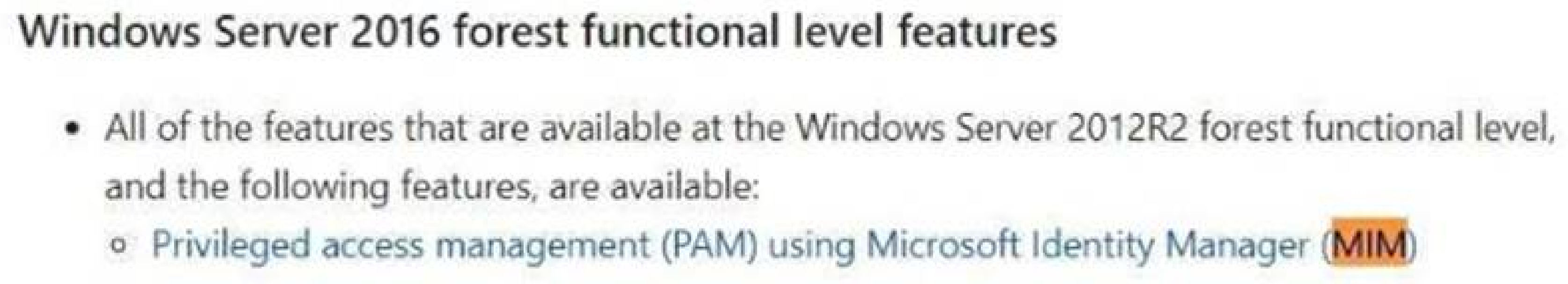
Explanation:
-The resources of the applications must be isolated from the physical host (ACHIEVED)
-Each application must be prevented from accessing the resources of the other applications. (ACHIEVED)
-The configurations of the applications must be accessible only from the operating system that hosts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

NEW QUESTION 6
Your network contains an Active Directory forest named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2016.
You create a new bastion forest named admin.contoso.com. The forest functional level of admin.contoso.com is Windows Server 2012 R2.
You need to implement a Privileged Access Management (PAM) solution.
Which two actions should you perform? Each correct answer presents part of the solution.

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

Answer: DE

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



Windows Server 2016 forest functional level features

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

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

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

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

Answer: AC

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

NEW QUESTION 9
Note: This question Is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is Independent of the other questions in this series. Information and details provided in a question apply only to that question.
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.
Server1 has a shared folder named Share1. You need to encrypt the contents of Share1. Which tool should you use?

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

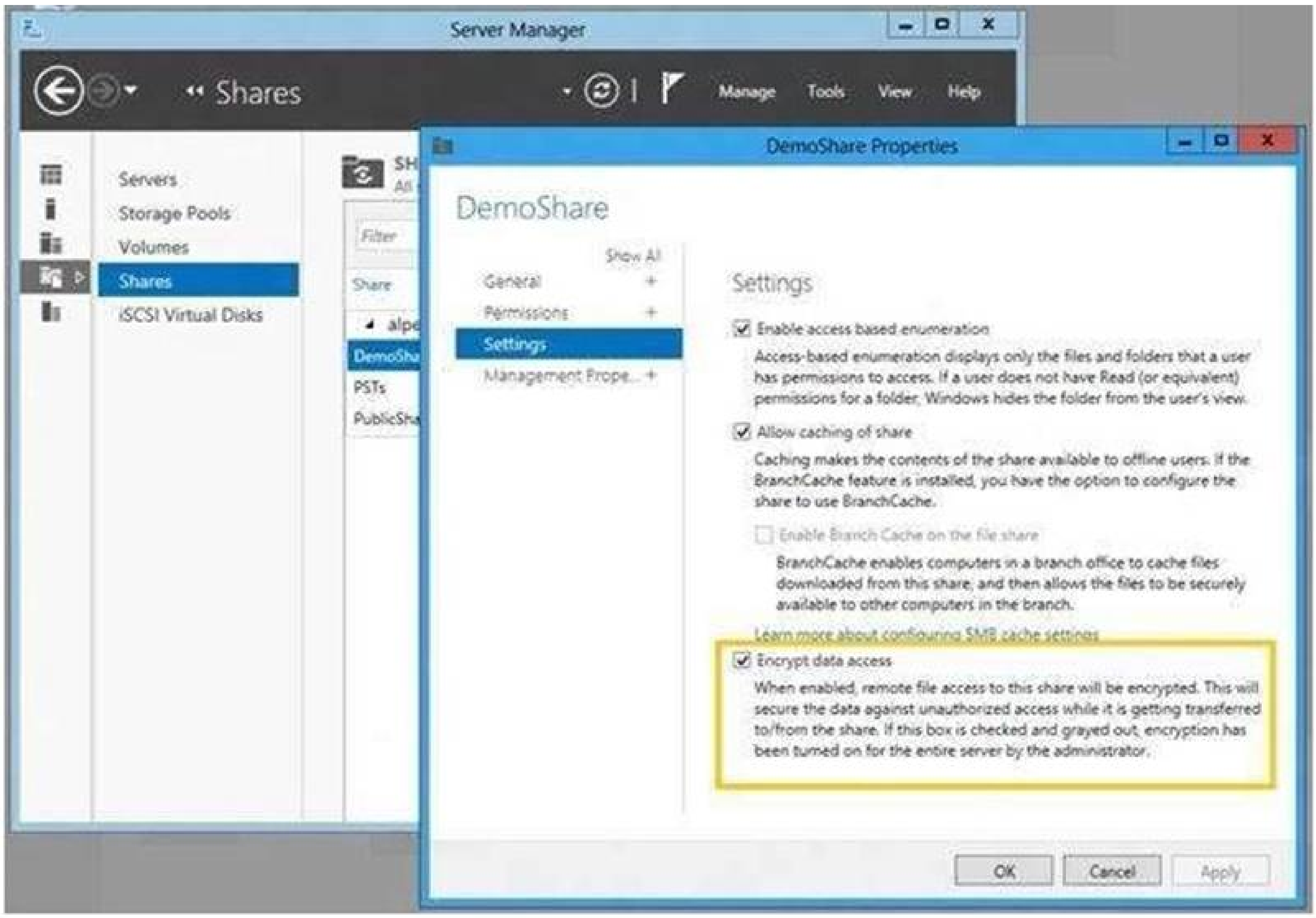
Answer: A

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

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

Answer: C

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



Settings

☑ Enable access based enumeration

Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

☑ Allow caching of share

Caching makes the contents of the share available to offline users. If the BranchCache feature is installed, you have the option to configure the share to use BranchCache.

□ Enable Branch Cache on the file share

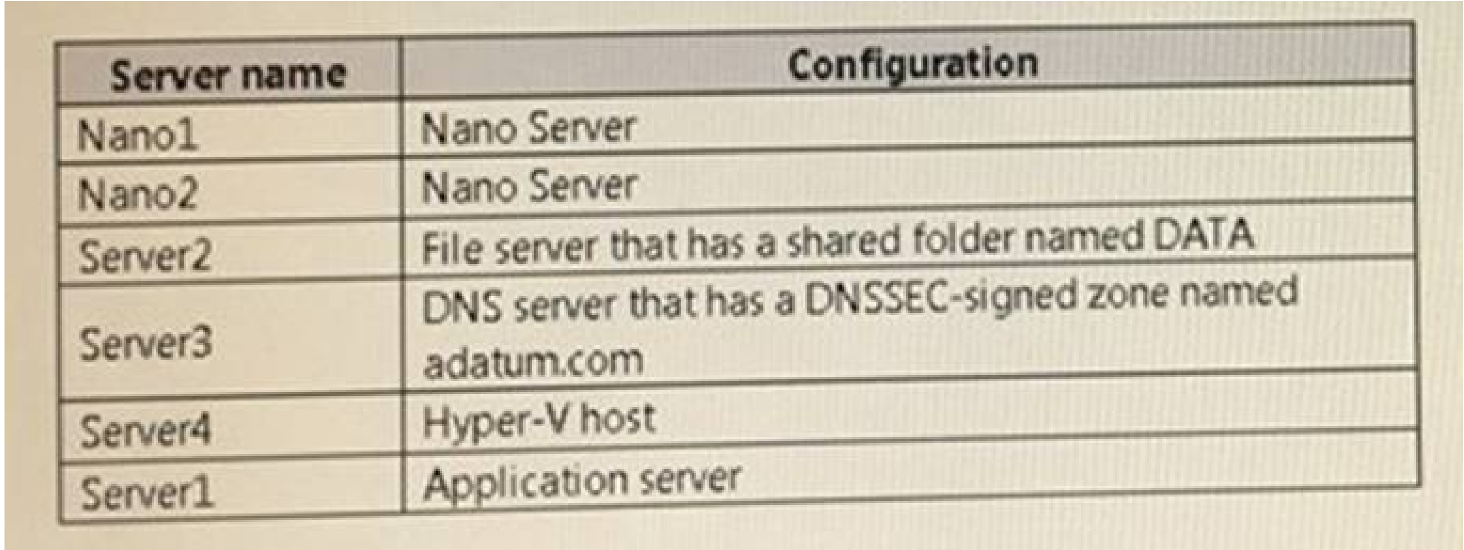
BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.

Learn more about configuring SMB cache settings

☑ Encrypt data access

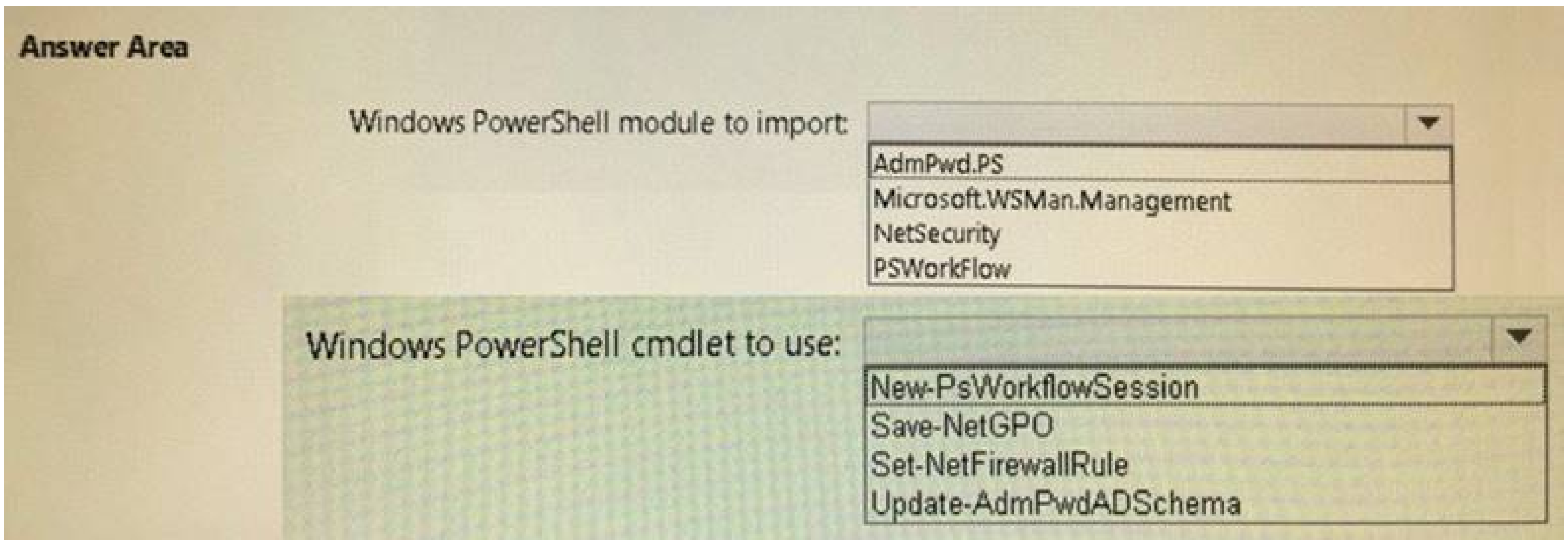
When enabled, remote file access to this share will be encrypted. This will secure the data against unauthorized access while it is getting transferred to/from the share. If this box is checked and grayed out, encryption has been turned on for the entire server by the administrator.

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

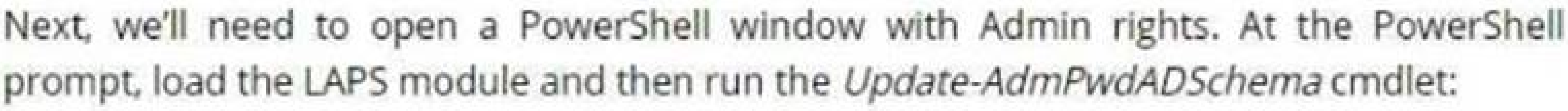
Windows PowerShell module to import:
- AdmPwd.PS
- Microsoft.WSMan.Management
- NetSecurity
- PSWorkFlow

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

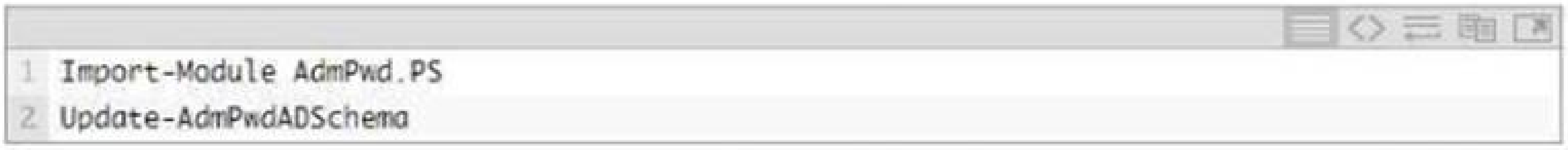
A. Mastered
B. Not Mastered

Answer: A

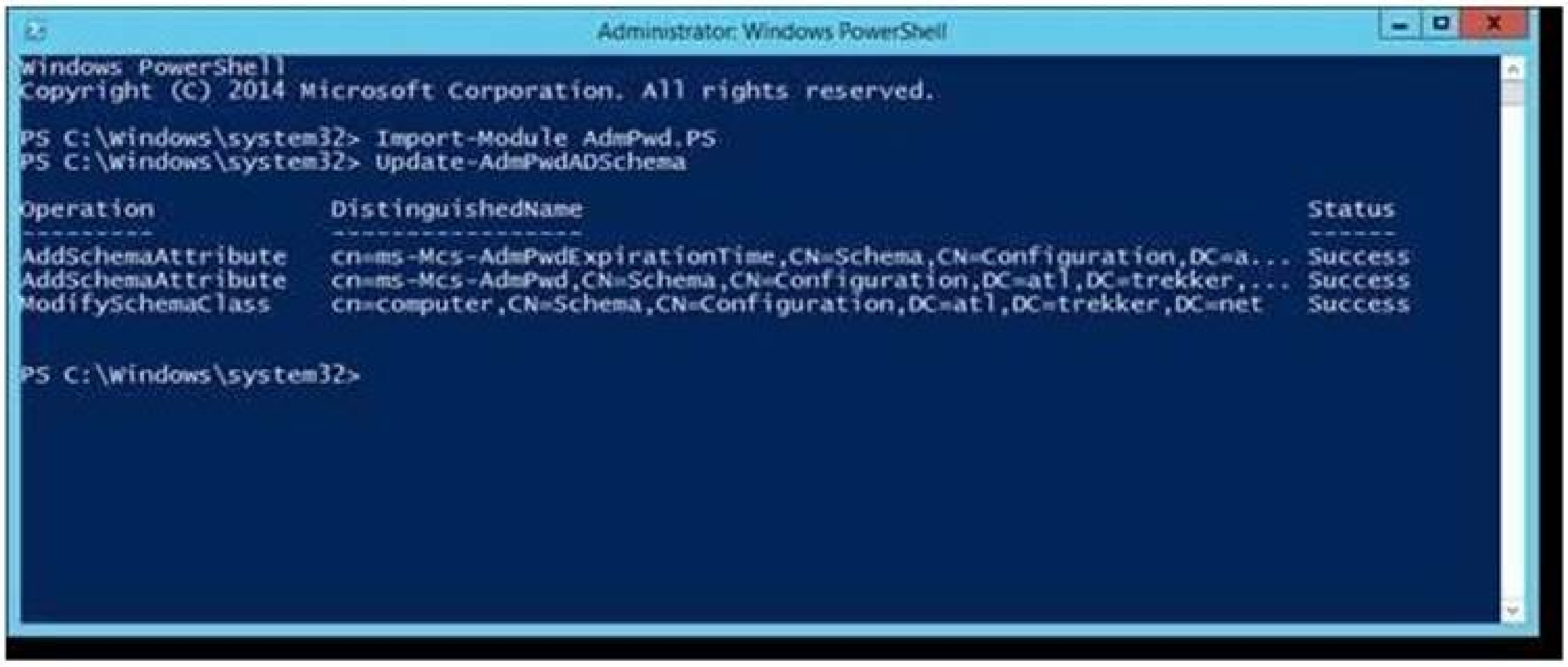
Explanation:
https://4sysops.com/archives/set-up-microsoft-laps-local-administrator-password-solution-in-activedirectory/



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
```



Administrator: Windows PowerShell

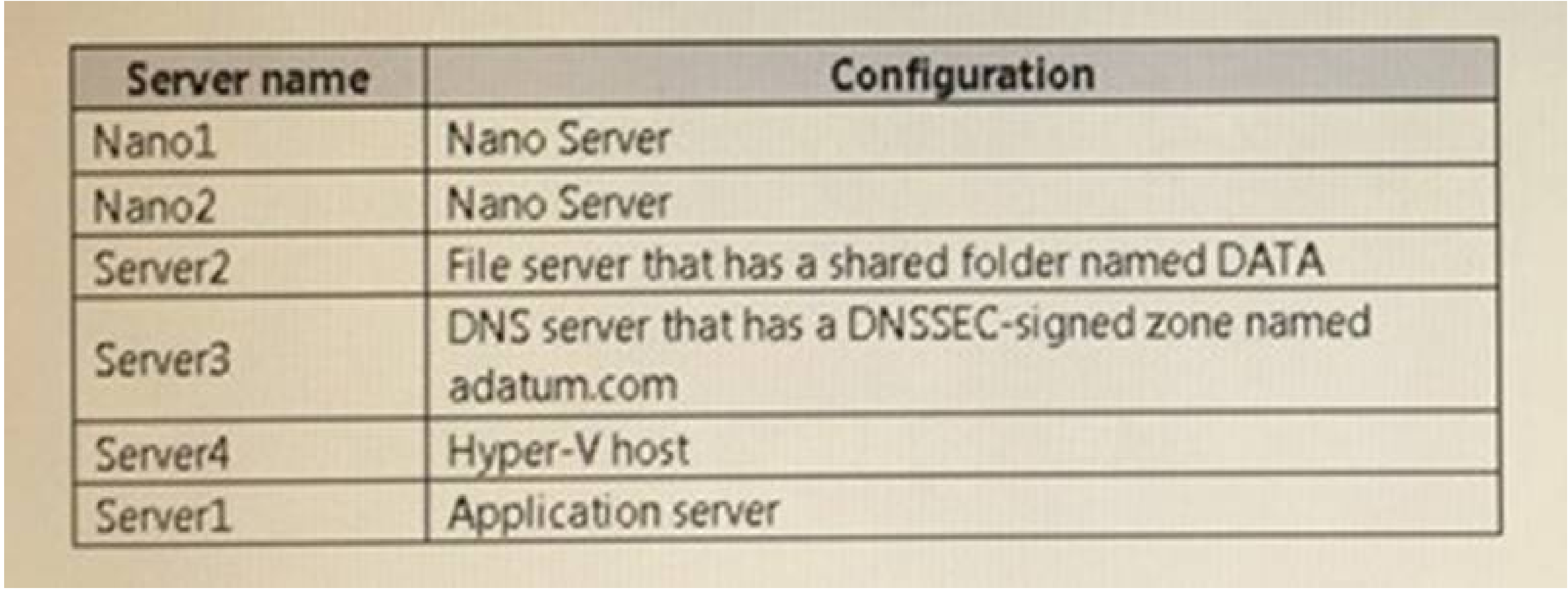
```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

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 14
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.
Start of repeated scenario
Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.
The domain contains the servers configured as shown in the following table.



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

All servers run Windows Server 2016. All client computers run Windows 10.

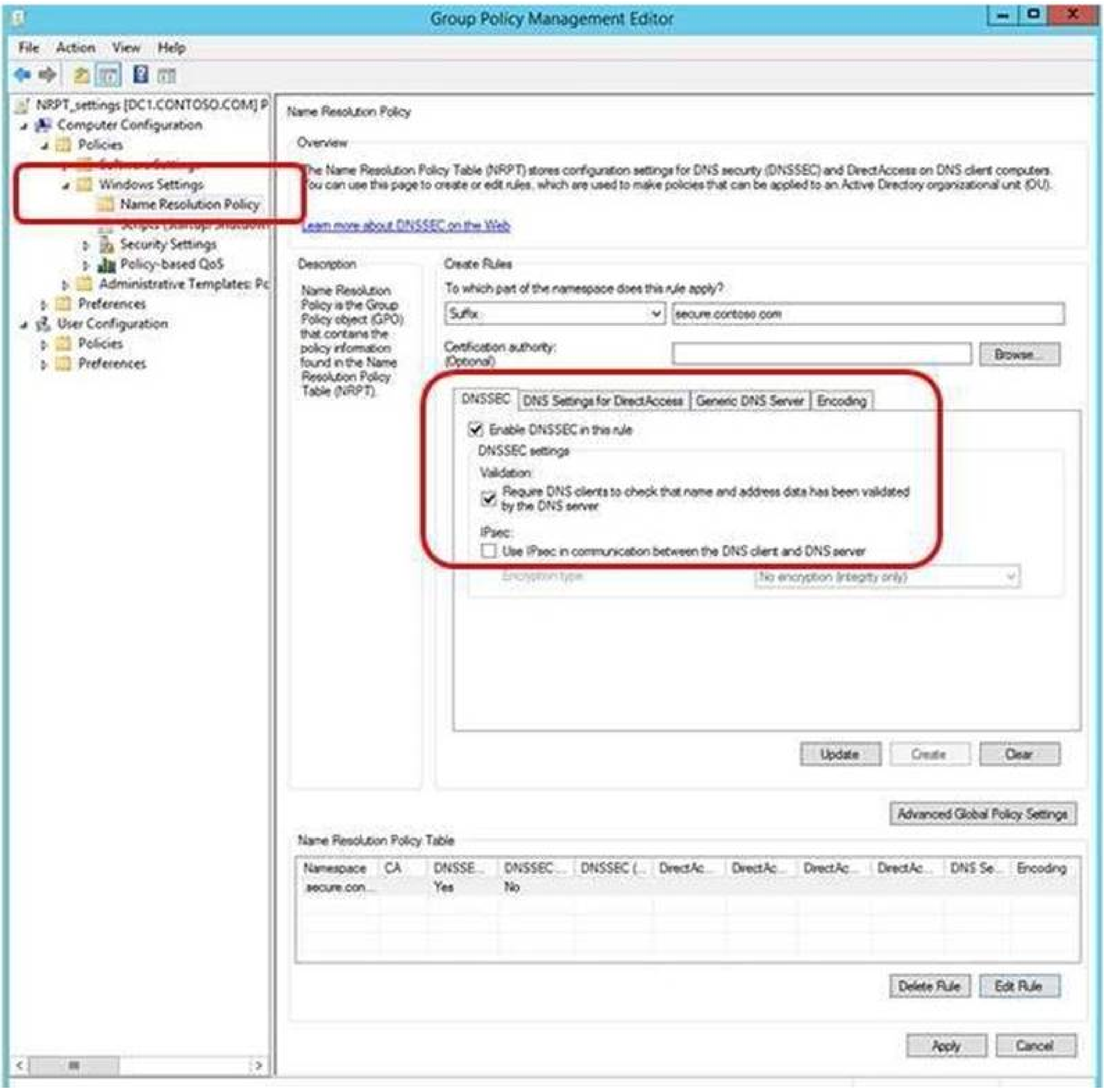
You have an organizational unit (OU) named Marketing that contains the computers in the marketing department You have an OU named Finance that contains the computers in the finance department You have an OU named AppServers that contains application servers. A Group Policy object (GPO) named GP1 is linked to the Marketing OU. A GPO named GP2 is linked to the AppServers OU. You install Windows Defender on Nano1.
End of repeated scenario
You need to 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.



Name Resolution Policy

Overview

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).

Description

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

Create Rules

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:

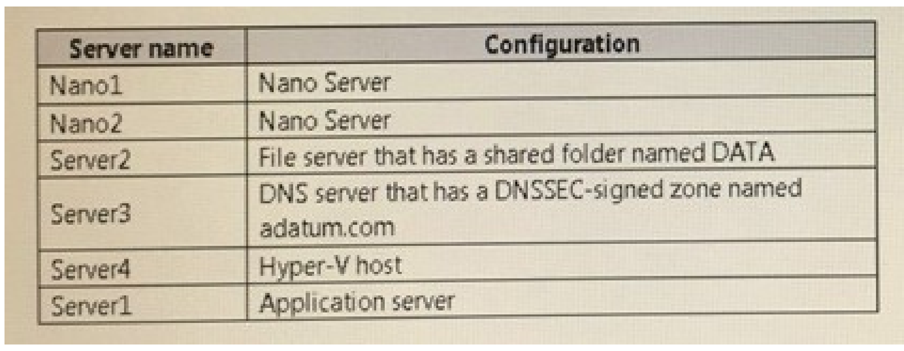
☐ Use IPsec in communication between the DNS client and DNS server

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 18
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.



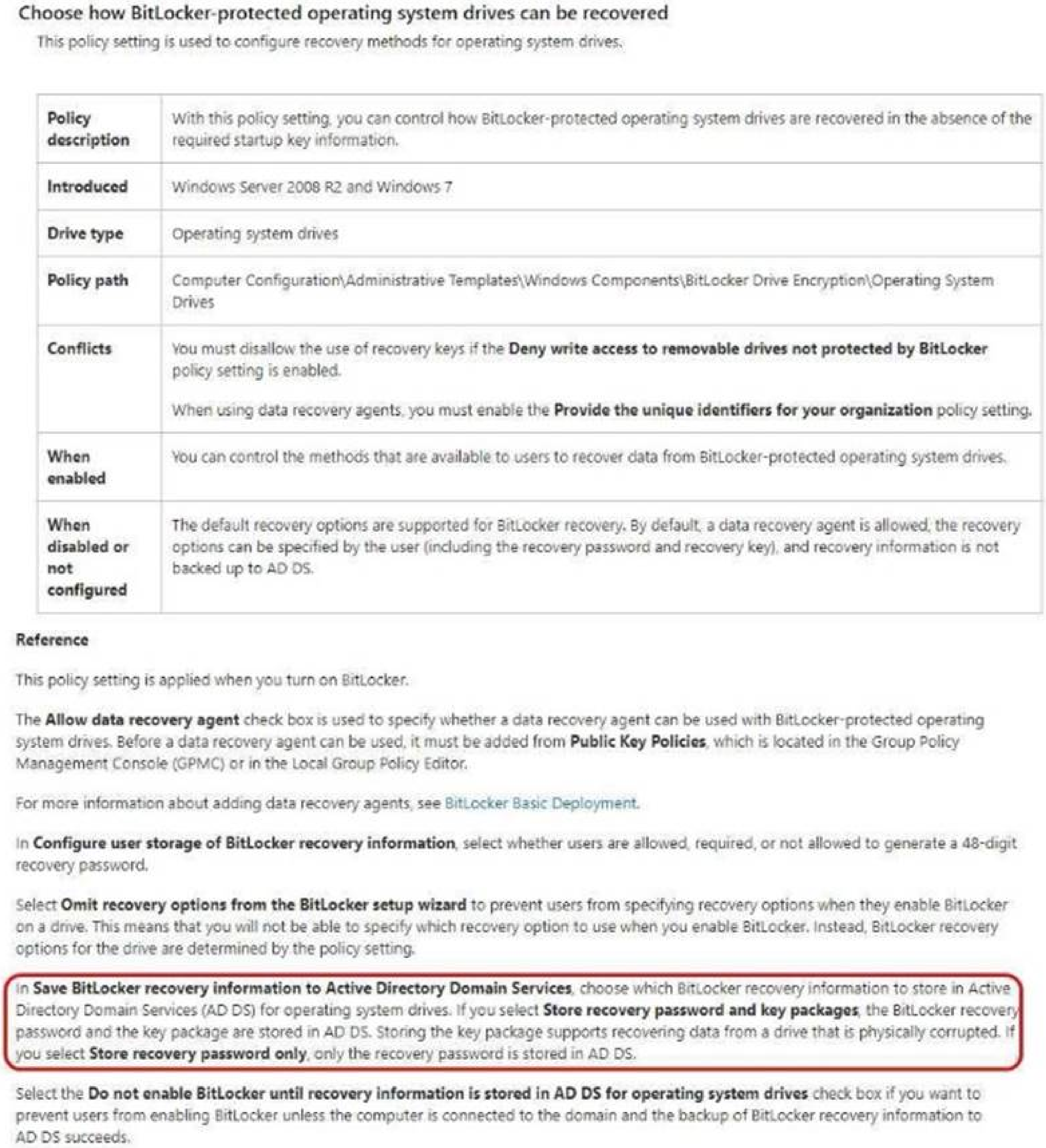
Server name	Configuration
Nano1	Nano Server
Nano2	Nano Server
Server2	File server that has a shared folder named DATA
Server3	DNS server that has a DNSSEC-signed zone named adatum.com
Server4	Hyper-V host
Server1	Application server

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.

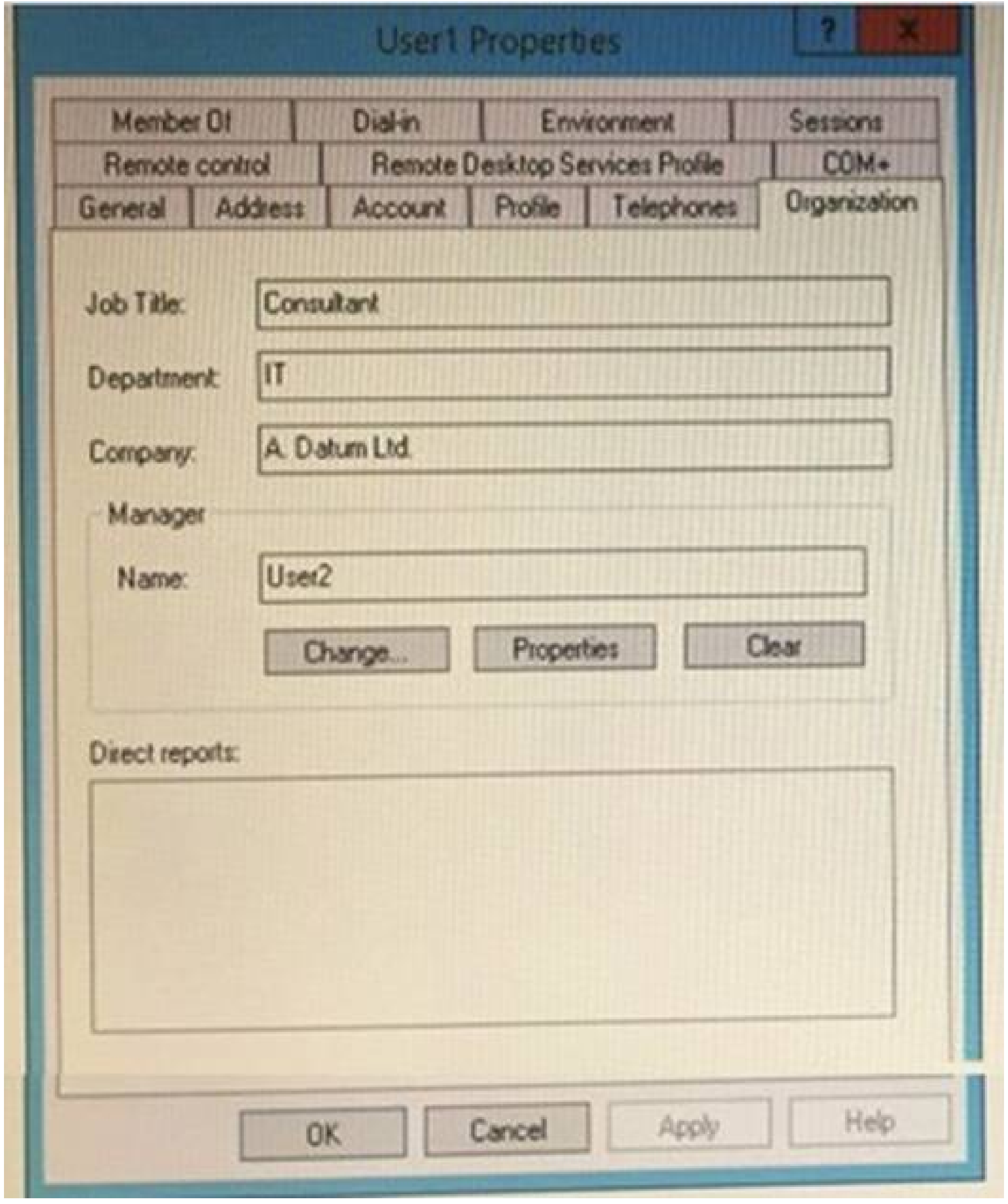
In **Configure user storage of BitLocker recovery information**, select whether users are allowed, required, or not allowed to generate a 48-digit recovery password.

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.

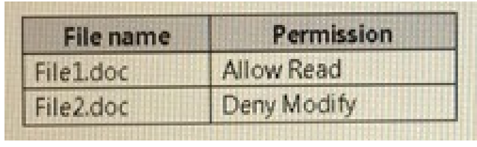
Select the **Do not enable BitLocker until recovery information is stored in AD DS for operating system drives** check box if you want to prevent users from enabling BitLocker unless the computer is connected to the domain and the backup of BitLocker recovery information to AD DS succeeds.

NEW QUESTION 23
HOTSPOT
Your network contains an Active Directory domain named adatum.com. The domain contains a file server named Server1 that runs Windows Server 2016.
You have an organizational unit (OU) named OU1 that contains Server1. You create a Group Policy object (GPO) named GPO1 and link GPO1 to OU1.
A user named User1 is a member of group named Group1. The properties of User1 are shown in the User1 exhibit (Click the Exhibit button.)



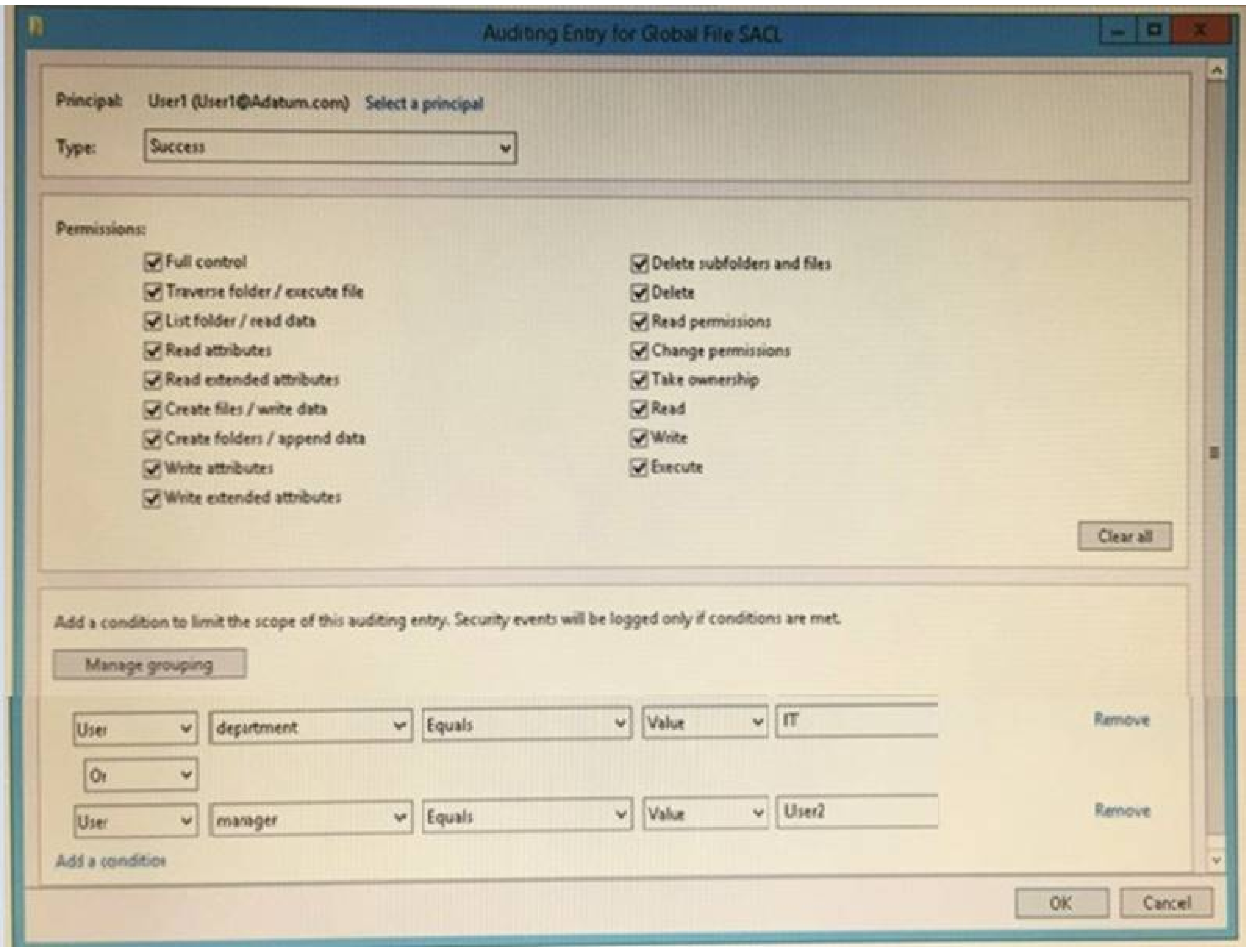
Job Title: Consultant
Department: IT
Company: A. Datum Ltd.
Manager
Name: User2
Direct reports:

User1 has permissions to two files on Server1 configured as shown in the following table.



File name	Permission
File1.doc	Allow Read
File2.doc	Deny Modify

From Auditing Entry for Global File SACL, you configure the advanced audit policy settings in GPO1 as shown in the SACL exhibit (Click the Exhibit button.)



Auditing Entry for Global File SACL

Principal: User1 (User1@Adatum.com) Select a principal

Type: Success

Permissions:

☑ Full control
☑ Traverse folder / execute file
☑ List folder / read data
☑ Read attributes
☑ Read extended attributes
☑ Create files / write data
☑ Create folders / append data
☑ Write attributes
☑ Write extended attributes
☑ Delete subfolders and files
☑ Delete
☑ Read permissions
☑ Change permissions
☑ Take ownership
☑ Read
☑ Write
☑ Execute

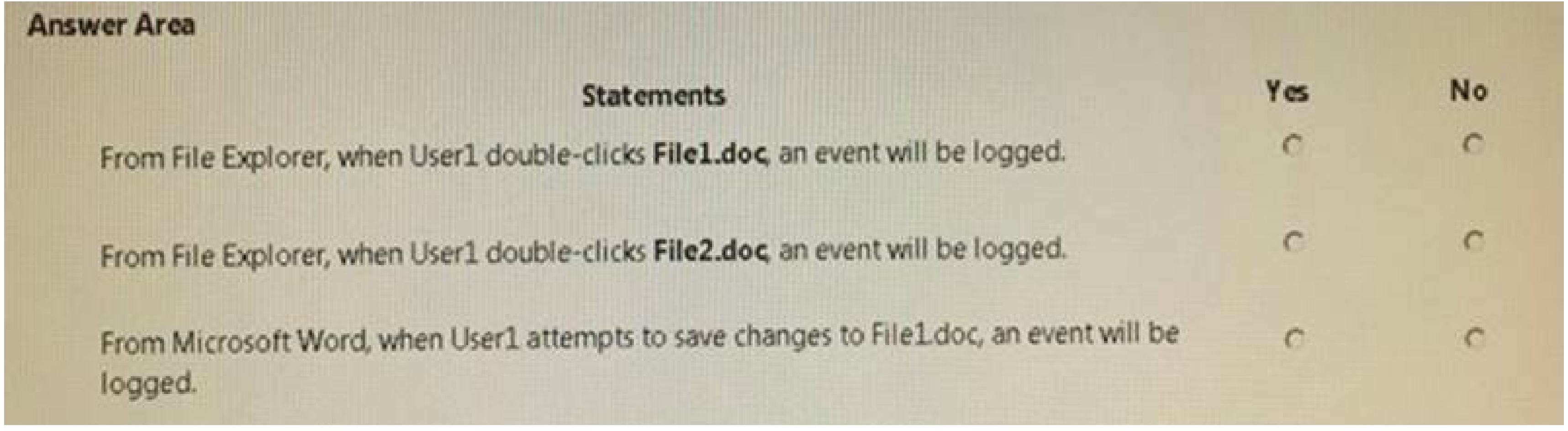
Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

User | department | Equals | Value | IT | Remove

Or

User | manager | Equals | Value | User2 | Remove

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



Answer Area

Statements	Yes	No
From File Explorer, when User1 double-clicks **File1.doc**, an event will be logged.	○	○
From File Explorer, when User1 double-clicks **File2.doc**, an event will be logged.	○	○
From Microsoft Word, when User1 attempts to save changes to File1.doc, an event will be logged.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
From File Explorer, when User1 double-clicks File1.doc. an event will be logged: Yes From File Explorer, when User1 double-clicks File2.doc. an event will be logged: No
From Microsoft Word, when User1 attempts to save changes to File1.doc, an event will be logged: No
From the SACL, only Successful operations by User1 will be logged “Type: Success”.

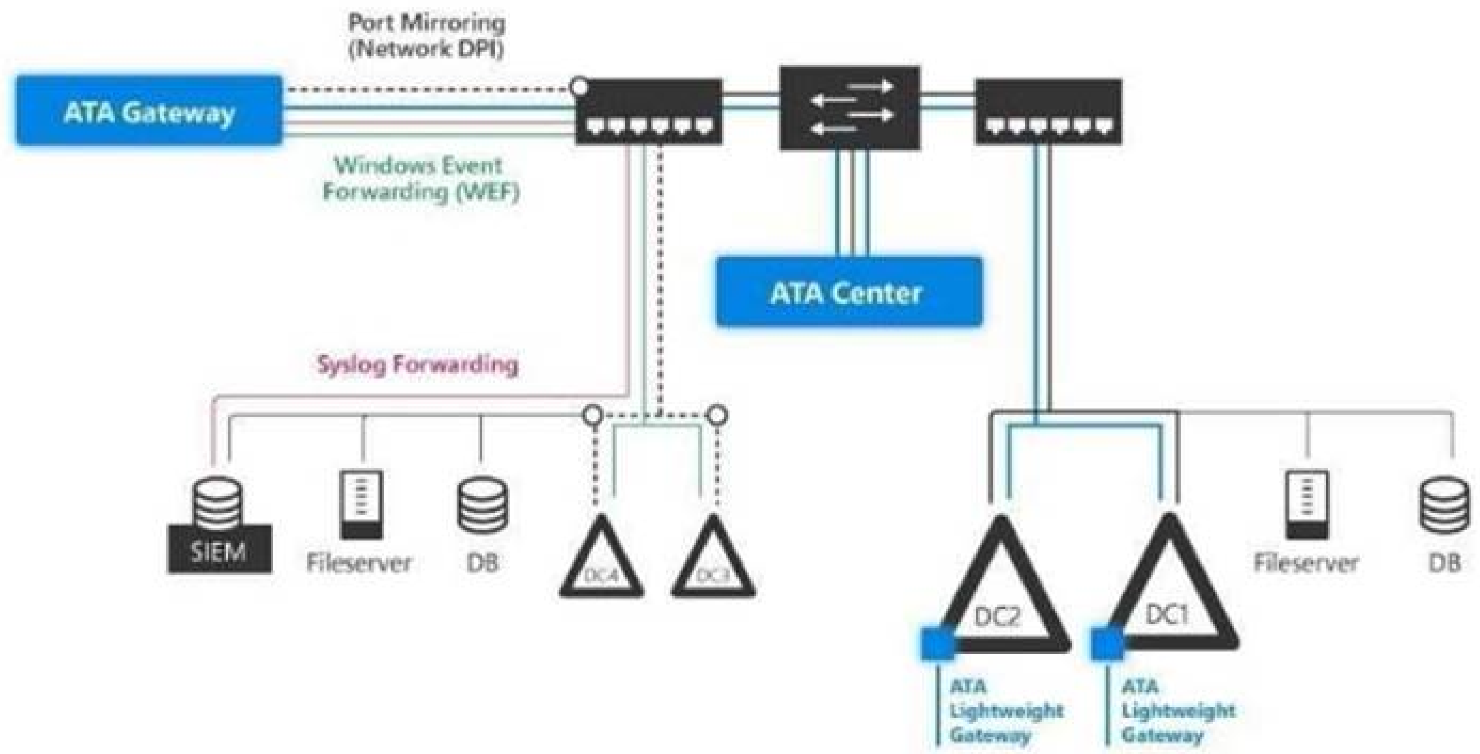
NEW QUESTION 26
Your network contains an Active Directory domain named contoso.com.
You are deploying Microsoft Advanced Threat Analytics (ATA) to the domain.
You install the ATA Center on server named Server1 and the ATA Gateway on a server named Served. You need to ensure that Server2 can collect NTLM authentication events.
What should you configure?

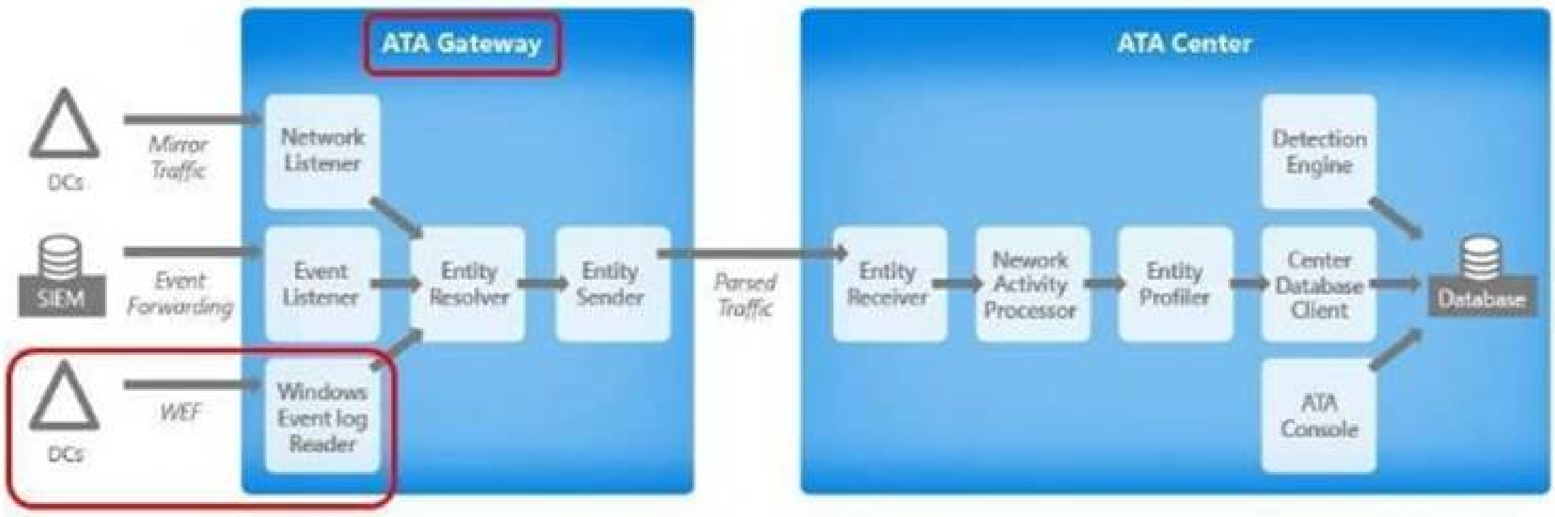
A. the domain controllers to forward Event ID 4776 to Server2
B. the domain controllers to forward Event ID 1000 to Server1
C. Server2 to forward Event ID 1026 to Server1
D. Server1 to forward Event ID 1000 to Server2

Answer: A

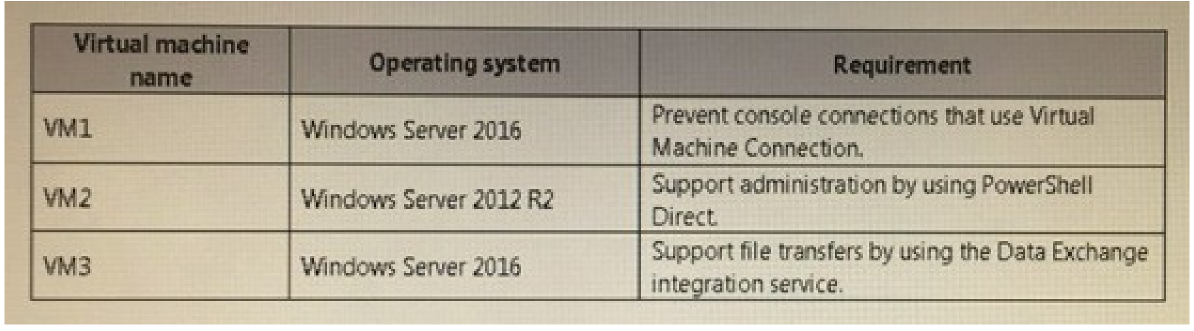
Explanation:
https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-architecture
ATA monitors your domain controller network traffic by utilizing port mirroring to an ATA Gateway using physical or virtual switches.

If you deploy the ATA Lightweight Gateway directly on your domain controllers, it removes the requirement for port mirroring.
In addition, ATA can leverage Windows events (forwarded directly from your domain controllers or from a SIEM server) and analyze the data for attacks and threats.
See the GREEN line in the following figure, forward event ID 4776 which indicates NTLM authentication is being used to ATA Gateway Server2.



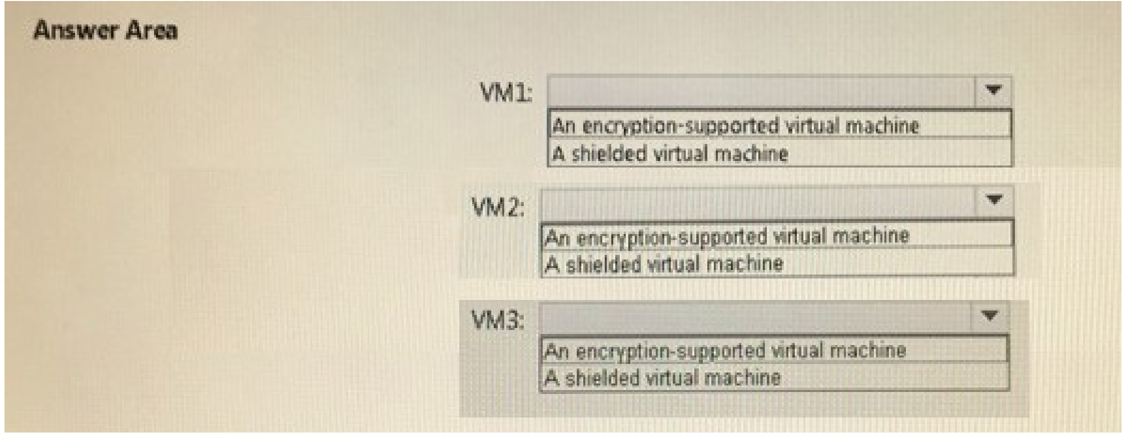


NEW QUESTION 29
HOTSPOT
You plan to deploy three encrypted virtual machines that use Secure Boot. The virtual machines will be configured as shown in the following table.



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

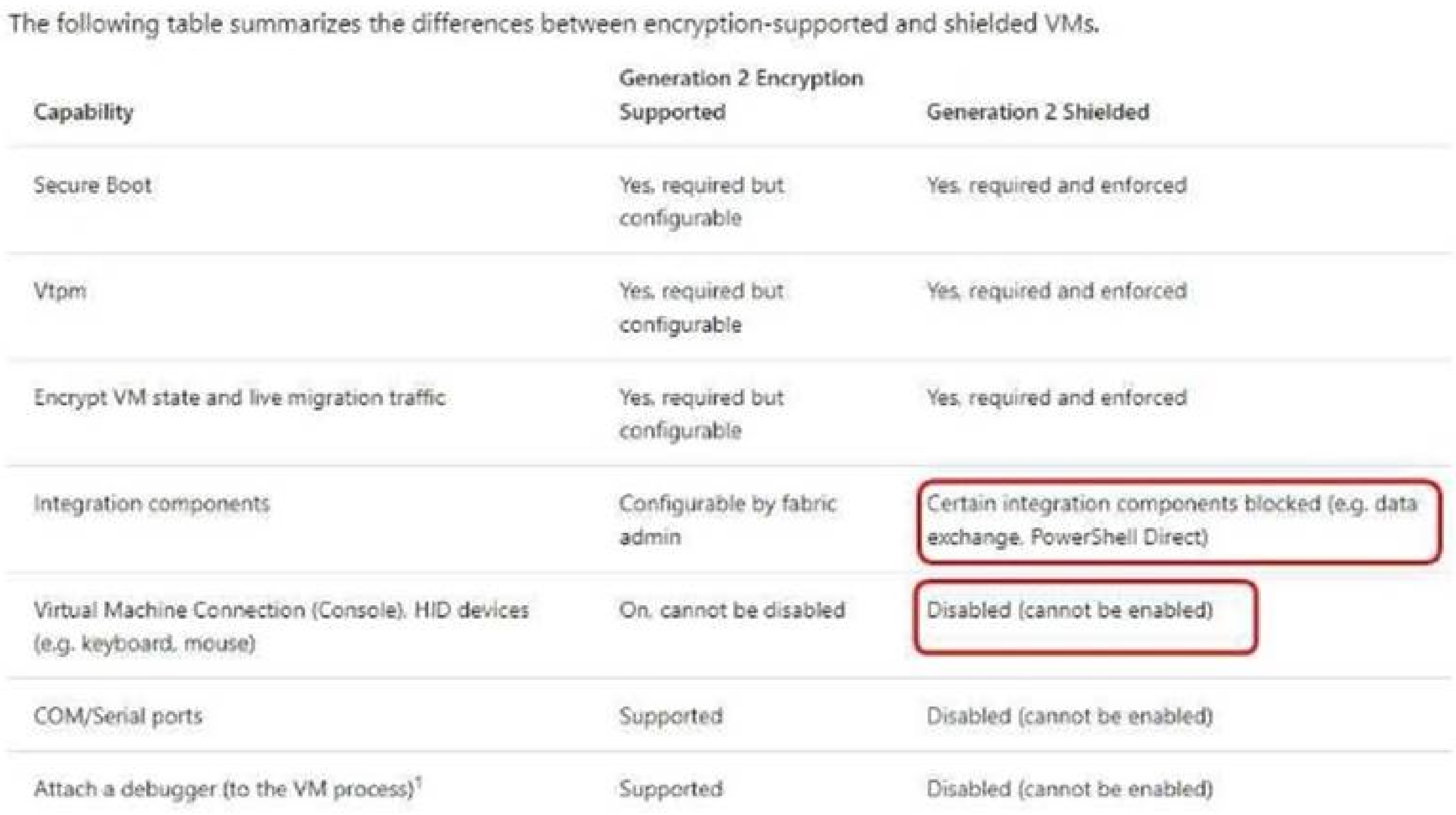
VM2:
- An encryption-supported virtual machine
- A shielded virtual machine

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 33

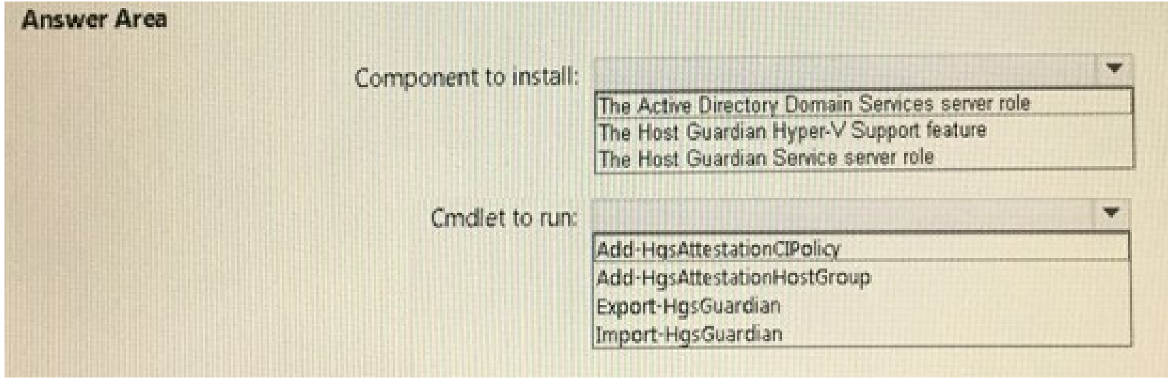
HOTSPOT

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

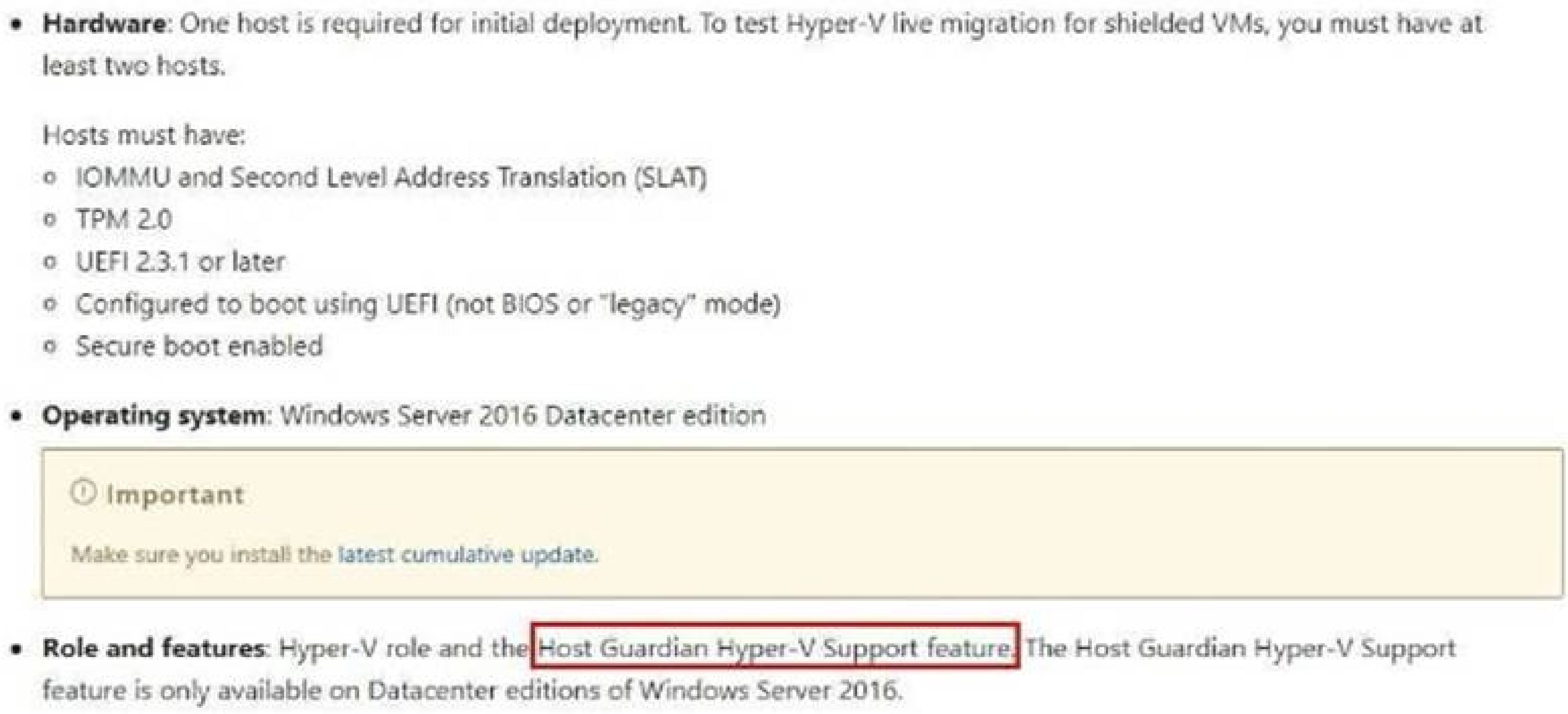
A. Mastered

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.

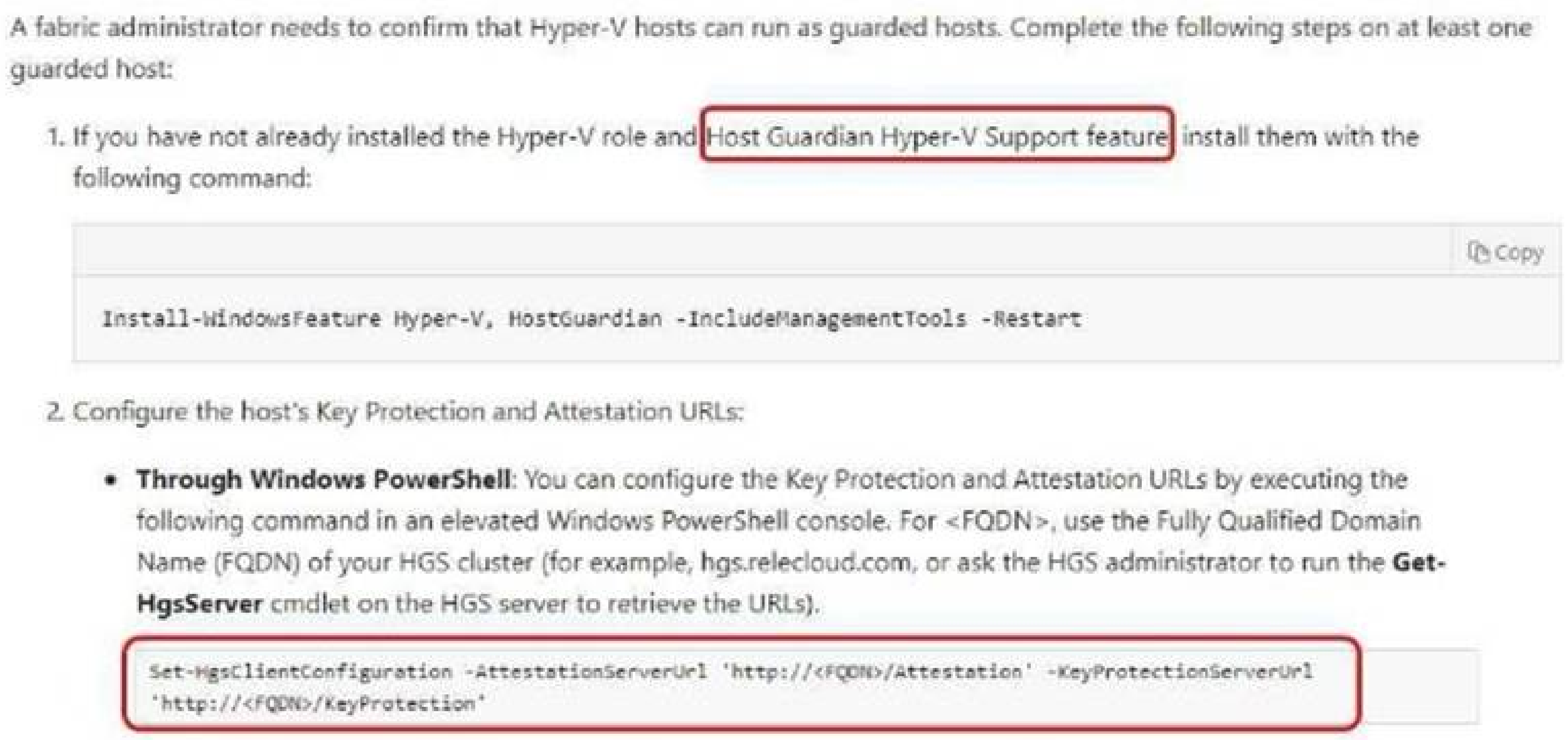


- **Hardware**: One host is required for initial deployment. To test Hyper-V live migration for shielded VMs, you must have at least two hosts.

  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 36
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 40
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 41
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

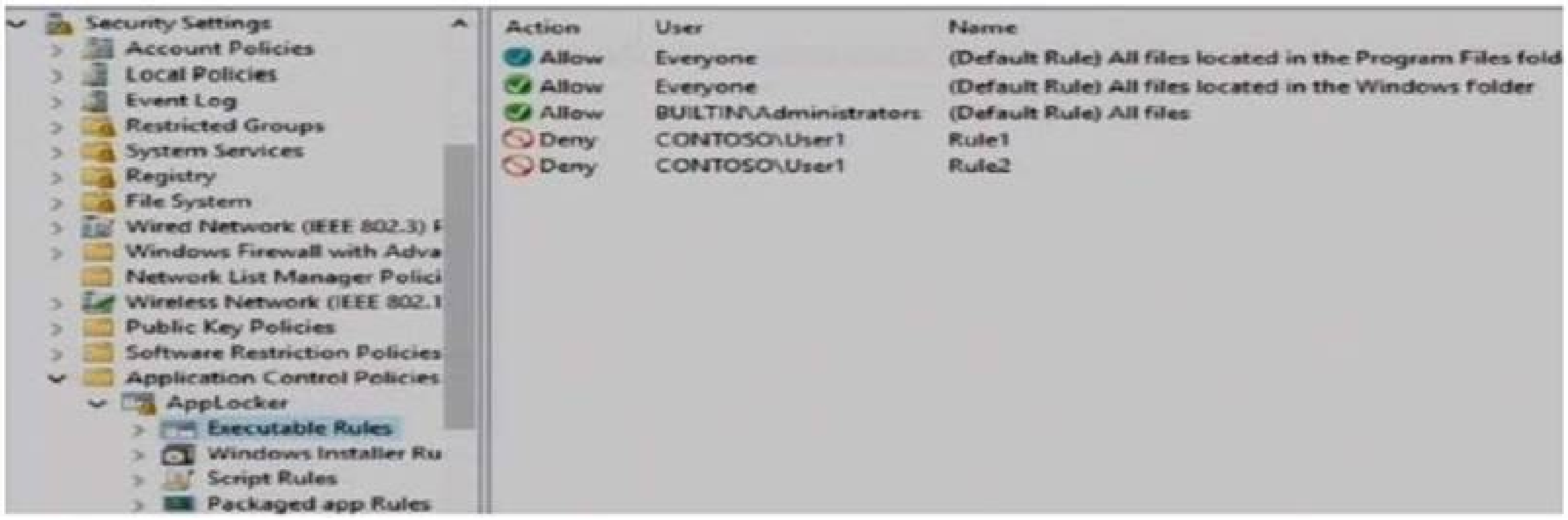
Explanation:
The default setting when managing a computer is True. When managing a GPO, the default setting is NotConfigured. The NotConfigured value is only valid when configuring a Group Policy Object (GPO). This parameter removes the setting from the GPO, which results in the policy not changing the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

NEW QUESTION 45
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

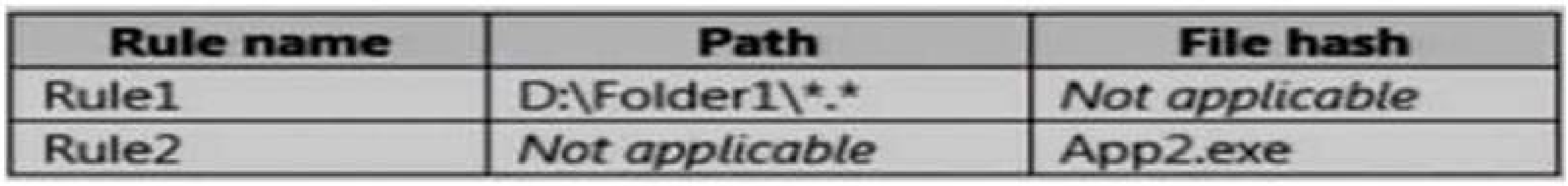
Answer: B

NEW QUESTION 48
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. A user named User1 is a member of the local Administrators group. Server1 has the AppLocker rules
configured as shown in follow:



Action	User	Name
Allow	Everyone	(Default Rule) All files located in the Program Files fold
Allow	Everyone	(Default Rule) All files located in the Windows folder
Allow	BUILTIN\Administrators	(Default Rule) All files
Deny	CONTOSO\User1	Rule1
Deny	CONTOSO\User1	Rule2

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



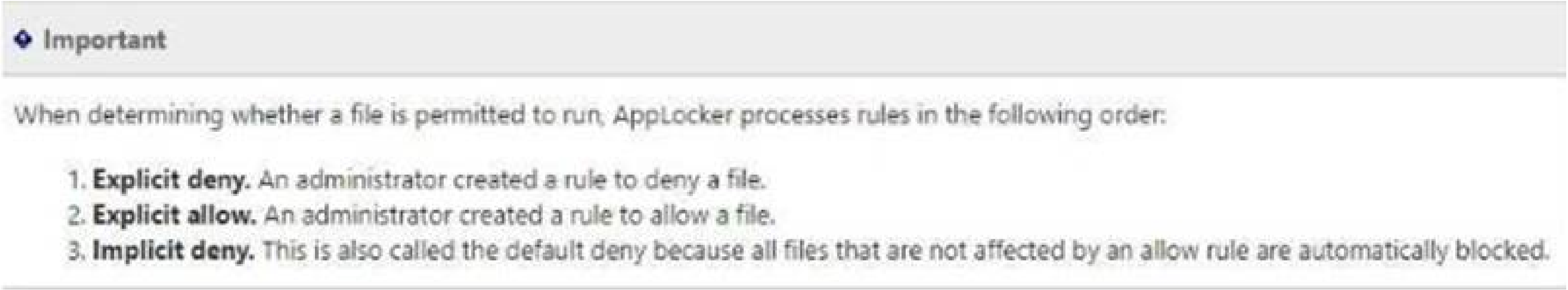
Rule name	Path	File hash
Rule1	D:\Folder1\*.*	*Not applicable*
Rule2	*Not applicable*	App2.exe

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

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

Answer: AF

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



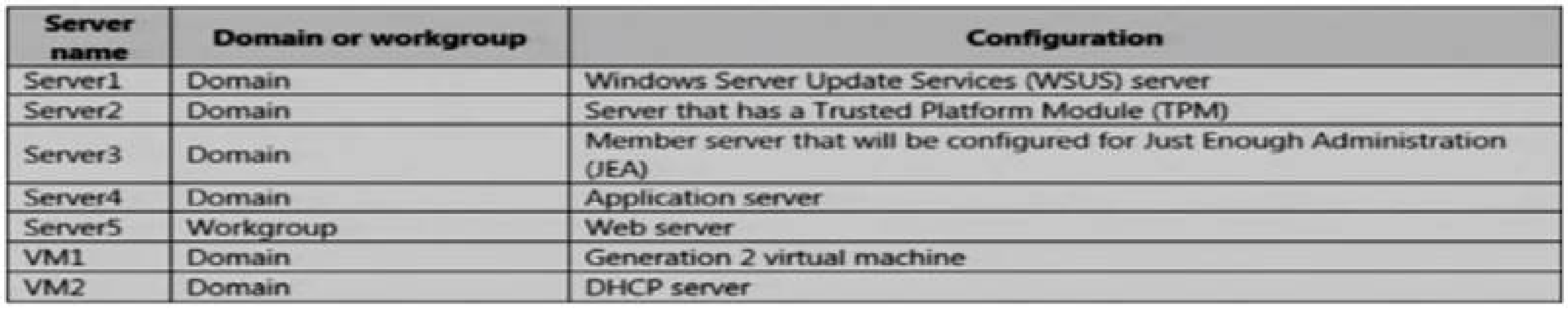
◆ Important

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

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

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

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



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

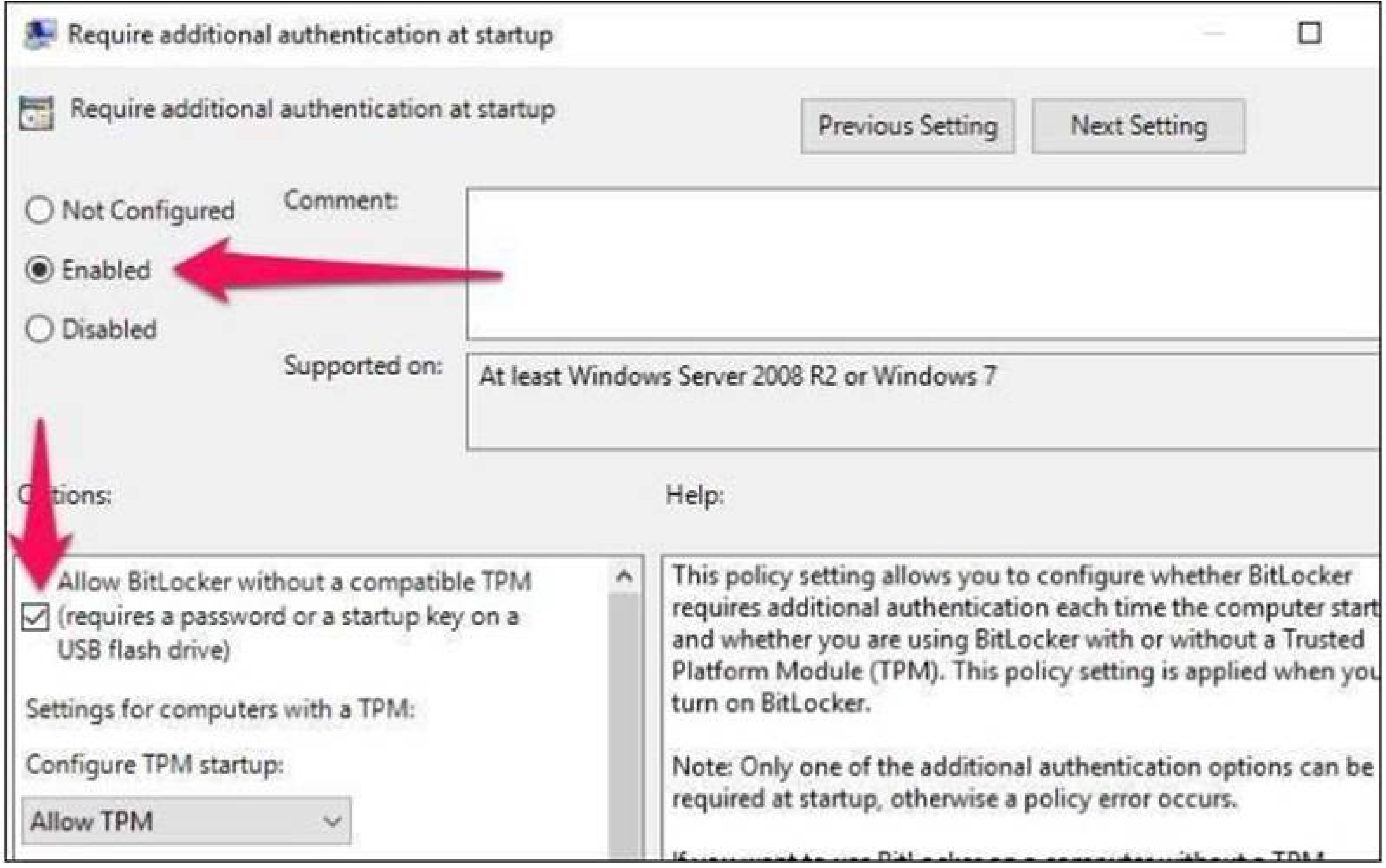
All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.
All laptops are protected by using BitLocker Drive Encryption (BitLocker).
You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.
An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1.
A GPO named GP2 is linked to OU2.
All computers receive updates from Server1. You create an update rule named Update1.
You need to ensure that you can encrypt the operating system drive of VM1 by using BitLocker. Which Group Policy should you configure?

A. Configure use of hardware-based encryption for operating system drives
B. Configure TPM platform validation profile for native UEFI firmware configurations

C. Require additional authentication at startup
D. Configure TPM platform validation profile for BIOS-based firmware configurations

Answer: C

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


Require additional authentication at startup

Require additional authentication at startup

○ Not Configured
● Enabled
○ Disabled

Comment:

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

Options:

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

Settings for computers with a TPM:

Configure TPM startup: Allow TPM

Help:

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

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

If you want to use BitLocker on a computer without a TPM

NEW QUESTION 53
You have a Hyper-V host named Hyperv1 that has a virtual machine named FS1. FS1 is a file server that contains sensitive data.
You need to secure FS1 to meet the following requirements:
-Prevent console access to FS1.
-Prevent data from being extracted from the VHDX file of FS1.
Which two actions should you perform? Each correct answer presents part of the solution.

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

Answer: AE

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

NEW QUESTION 55
Your company has an accounting department.
The network contains an Active Directory domain named contoso.com. The domain contains 10 servers.
You deploy a new server named Server11 that runs Windows Server 2016.
Server11 will host several network applications and network shares used by the accounting department.
You need to recommend a solution for Server11 that meets the following requirements:
-Protects Server11 from address spoofing and session hijacking
-Allows only the computers in We accounting department to connect to Server11 What should you recommend implementing?

A. AppLocker rules
B. Just Enough Administration (JEA)
C. connection security rules
D. Privileged Access Management (PAM)

Answer: C

Explanation:
In IPsec connection security rule, the IPsec protocol verifies the sending host IP address by utilize integrity functions like Digitally signing all packets.
If unsigned packets arrives Server11, those are possible source address spoofed packets, when using connection security rule in-conjunction with inbound firewall

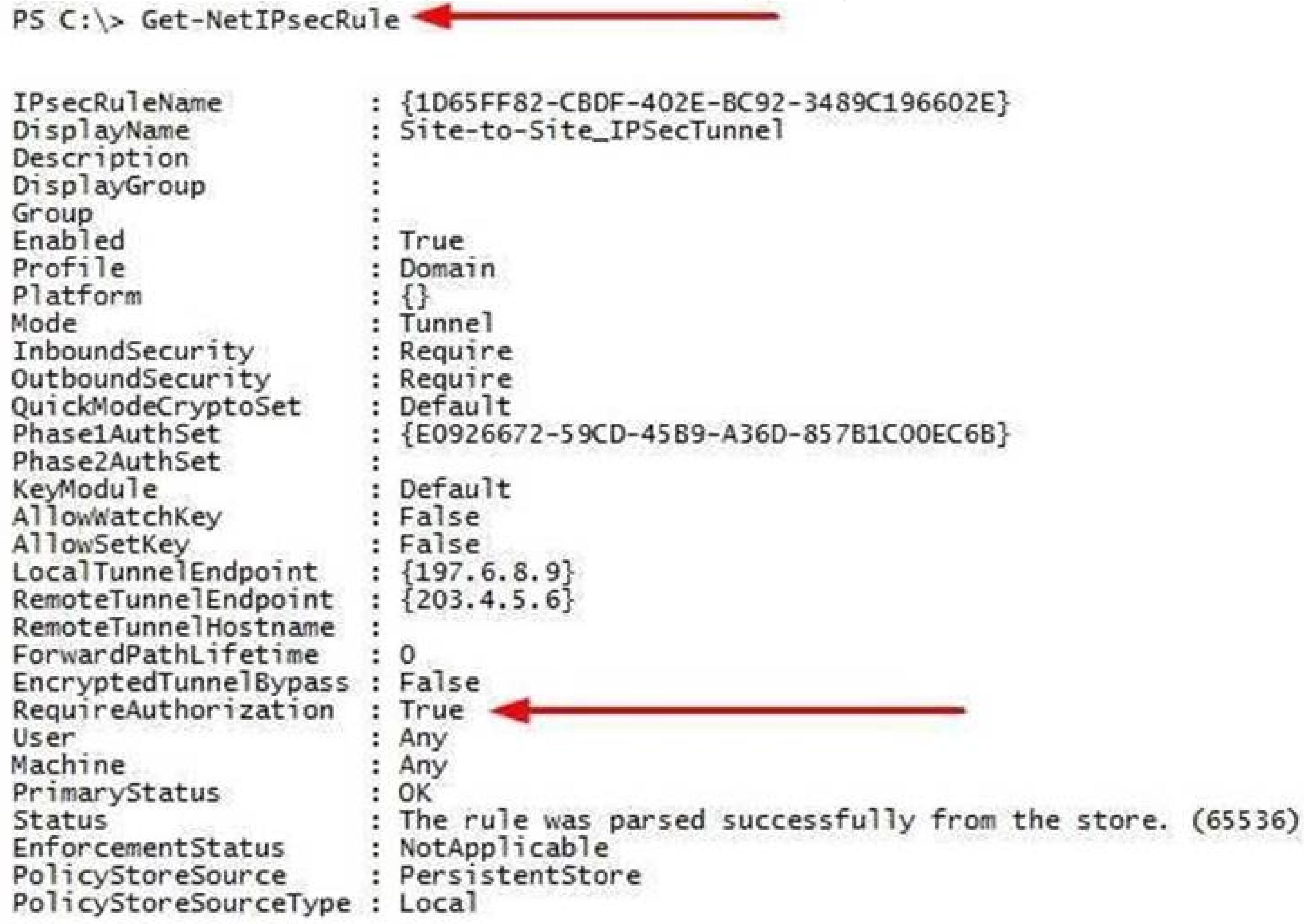
rules, you can kill those un-signed packets with the action “Allow connection if it is secure” to prevent spoofing and session hijacking attacks.

NEW QUESTION 60
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

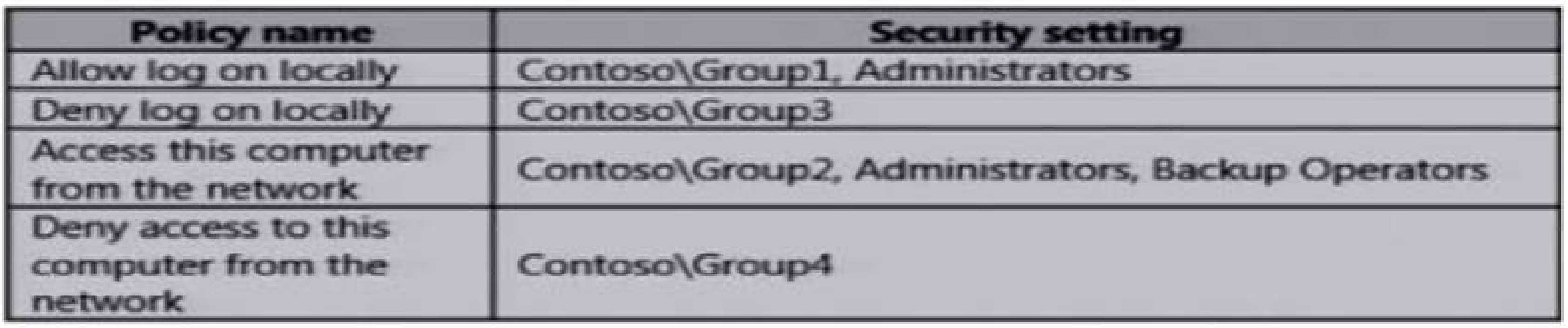
Explanation:
https://technet.microsoft.com/en-us/itpro/powershell/windows/netsecurity/get-netipsecrule



```
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 62
Your network contains an Active Directory domain named contoso.com.
The domain contains four global groups named Group].., Group2, Group3, and Group4.A user named User1 is a member of Group3.
You have an organizational unit (OU) named OU1 that contains computer accounts.
A Group Policy object (GPO) named GPO1 is linked to OU1. OU1 contains a computer account named Computer1.
GPO1 has the User Rights Assignment configured as shown in the following table:



Policy name	Security setting
Allow log on locally	Contoso\Group1, Administrators
Deny log on locally	Contoso\Group3
Access this computer from the network	Contoso\Group2, Administrators, Backup Operators
Deny access to this computer from the network	Contoso\Group4

You need to ensure that User1 can access the shares on Computer1. What should you do?

A. Modify the membership of Group1.
B. In GPO1, modify the Access this computer from the network user right
C. Modify the Deny access to this computer from the network user right.
D. Modify the Deny log on locally user right

Answer: B

Explanation:
You need to ensure that User1 can access the shares on Computer1, from network.

If not from network, where would you access a shared folder from? from Mars? from Space? from toilet?
Moreover, this question has explicitly state User1 is a member of Group3, and hence it is not possible for User1 to logon Computer1 locally to touch those shared folders on NTFS file system.
Only these two policies to be considered “Access this computer from network”, “Deny access to this computer from network”.1
There’s no option to modify the group member ship of “Group2”, “Administrators”, or “Backup Operators”, so we have to add a 4th entry “User1” to this policy setting “Access this computer from network”.

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

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

Answer: CE

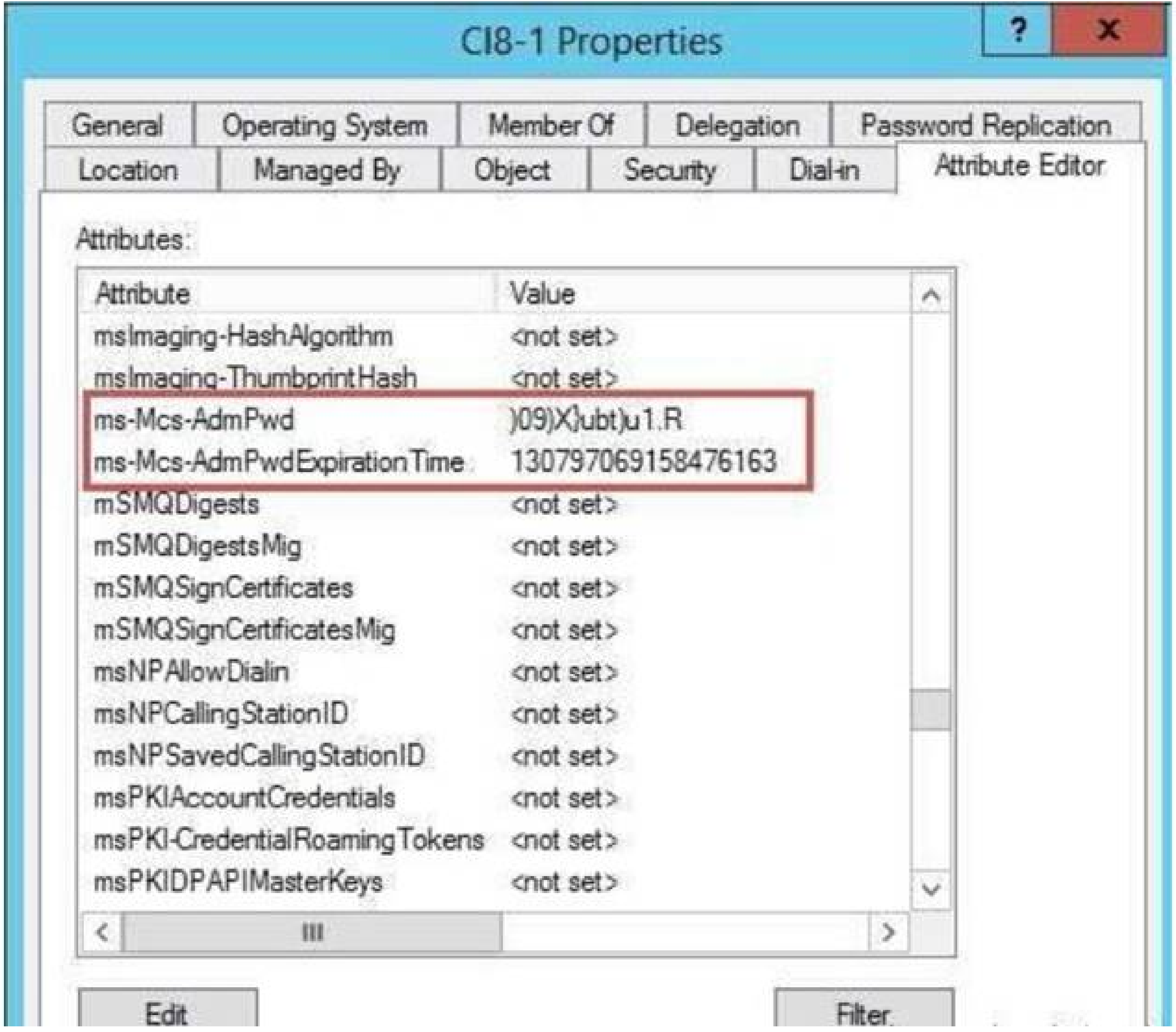
Explanation:
https://docs.microsoft.com/en-us/powershell/jea/role-capabilities https://docs.microsoft.com/en-us/powershell/jea/register-jea

NEW QUESTION 70
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>

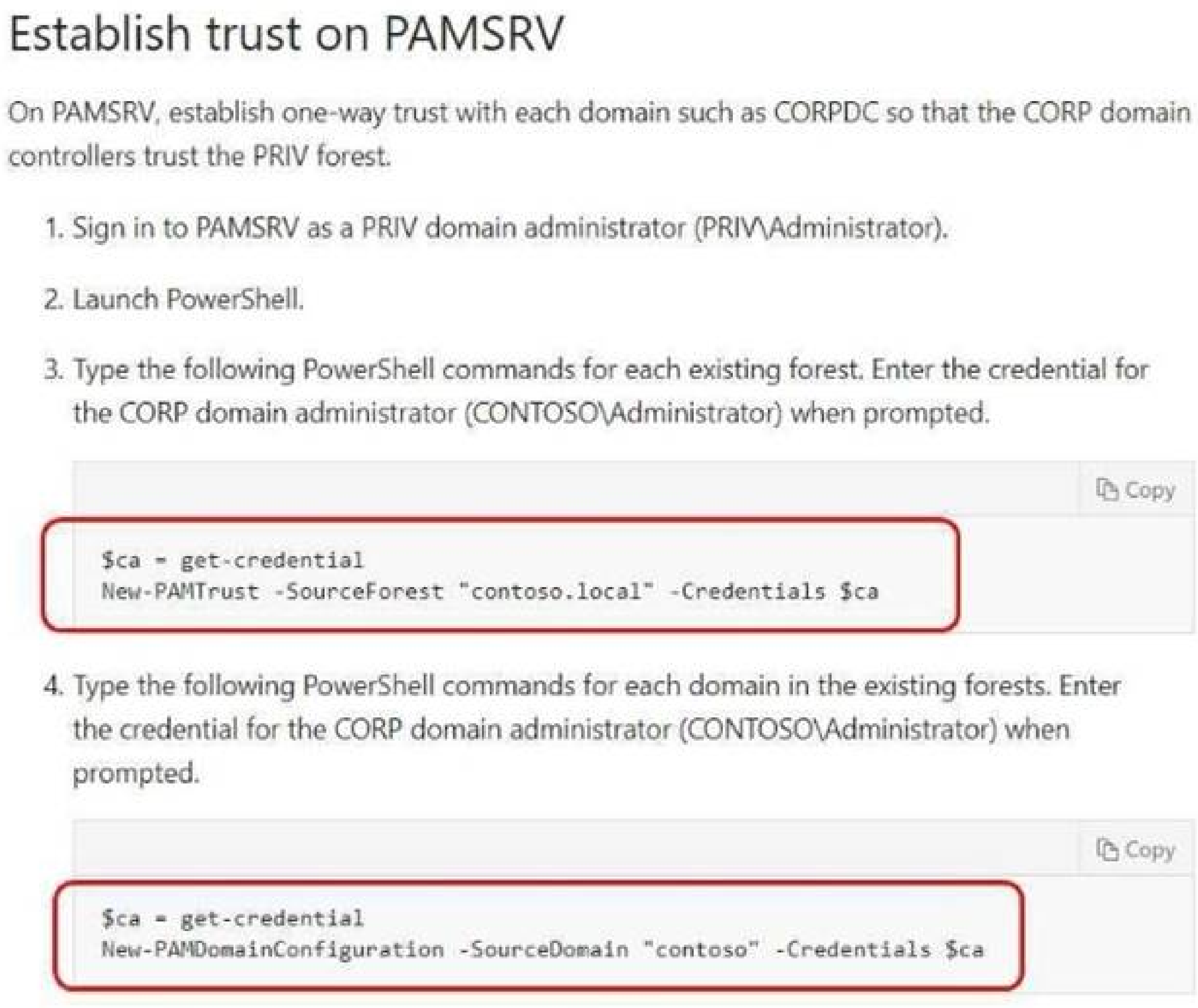
NEW QUESTION 74
Your network contains an Active Directory forest named contoso.com. The forest contains three domains. All domain controllers run Windows Server 2016.
You deploy a second Active Directory forest named admin.contoso.com.

The forest contains a domain member server named Server1. Server1 has Microsoft Identity Manager (MIM) 2016 deployed.
You need to implement Privileged Access Management (PAM) and to use admin.contoso.com as an administrative forest.
Which two actions should you perform? Each correct answers presents part of the solution.

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

Answer: BF

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



Establish trust on PAMSRV

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

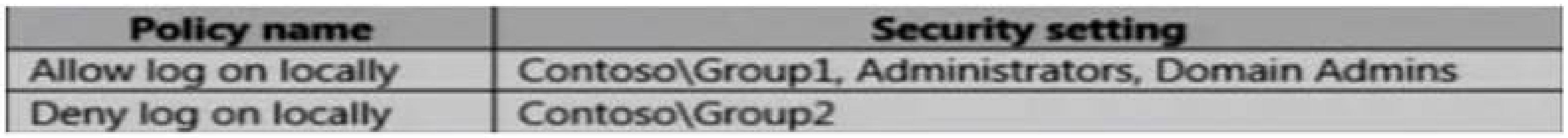
1. Sign in to PAMSRV as a PRIV domain administrator (PRIV\Administrator).
2. Launch PowerShell.
3. Type the following PowerShell commands for each existing forest. Enter the credential for the CORP domain administrator (CONTOSO\Administrator) when prompted.

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

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

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

NEW QUESTION 76
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 81
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

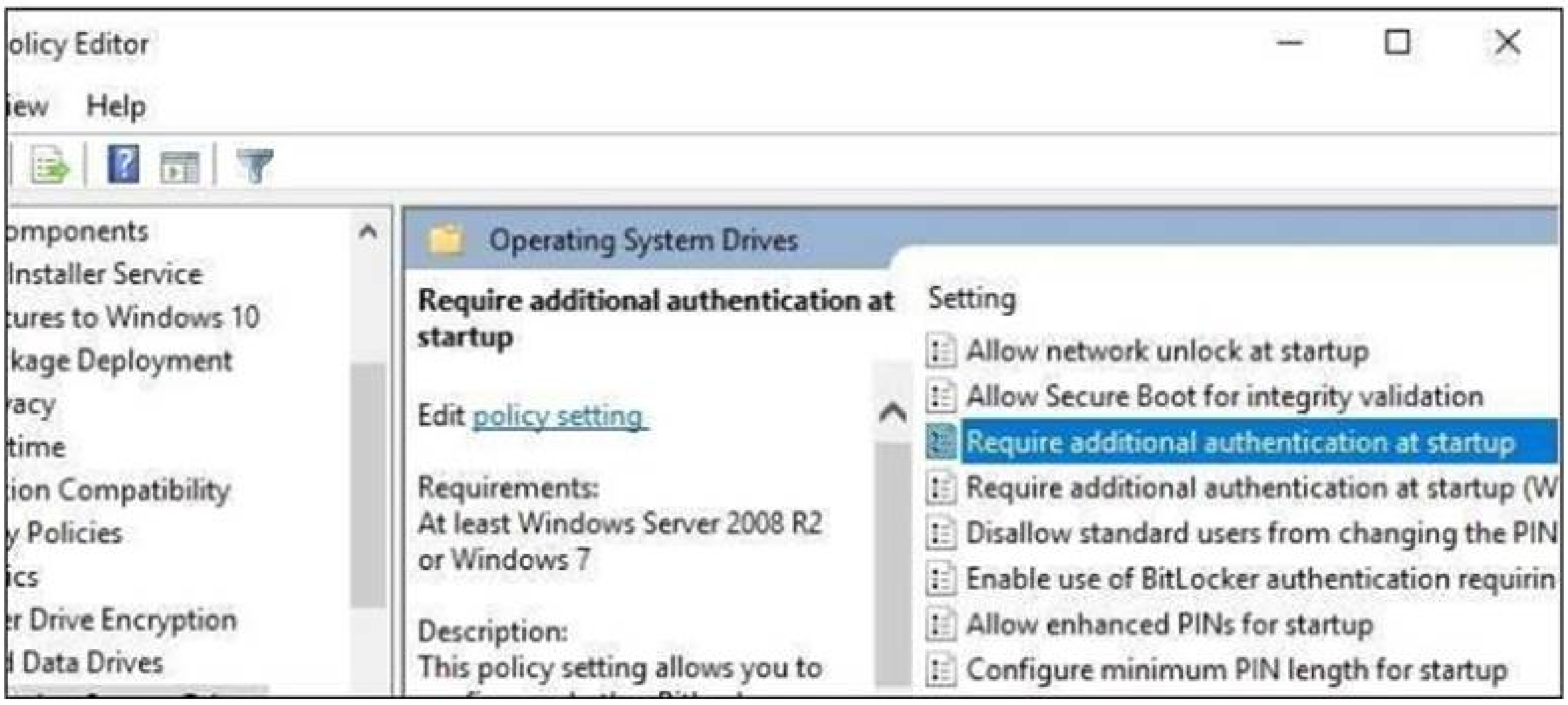
Explanation:
When Computer1 is configured to require Remote Credential Guard, you cannot use NTLM authentication to specify (or impersonate) another user account when connecting to Server1.
Therefore, you have to sign in to Computer1 as “ServerAdmin1” and use Kerberos for authenticating to RDP server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

NEW QUESTION 82
You have a Hyper-V host named Server1 that runs Windows Server 2016. Server1 has a generation 2 virtual machine named VM1 that runs Windows 10.
You need to ensure that you can turn on BitLocker Drive Encryption (BitLocker) for drive C: on VM1. What should you do?

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

Answer: C

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



omponents
Installer Service
tures to Windows 10
kage Deployment
acy
time
ion Compatibility
y Policies
ics
r Drive Encryption
l Data Drives

Operating System Drives

Require additional authentication at startup

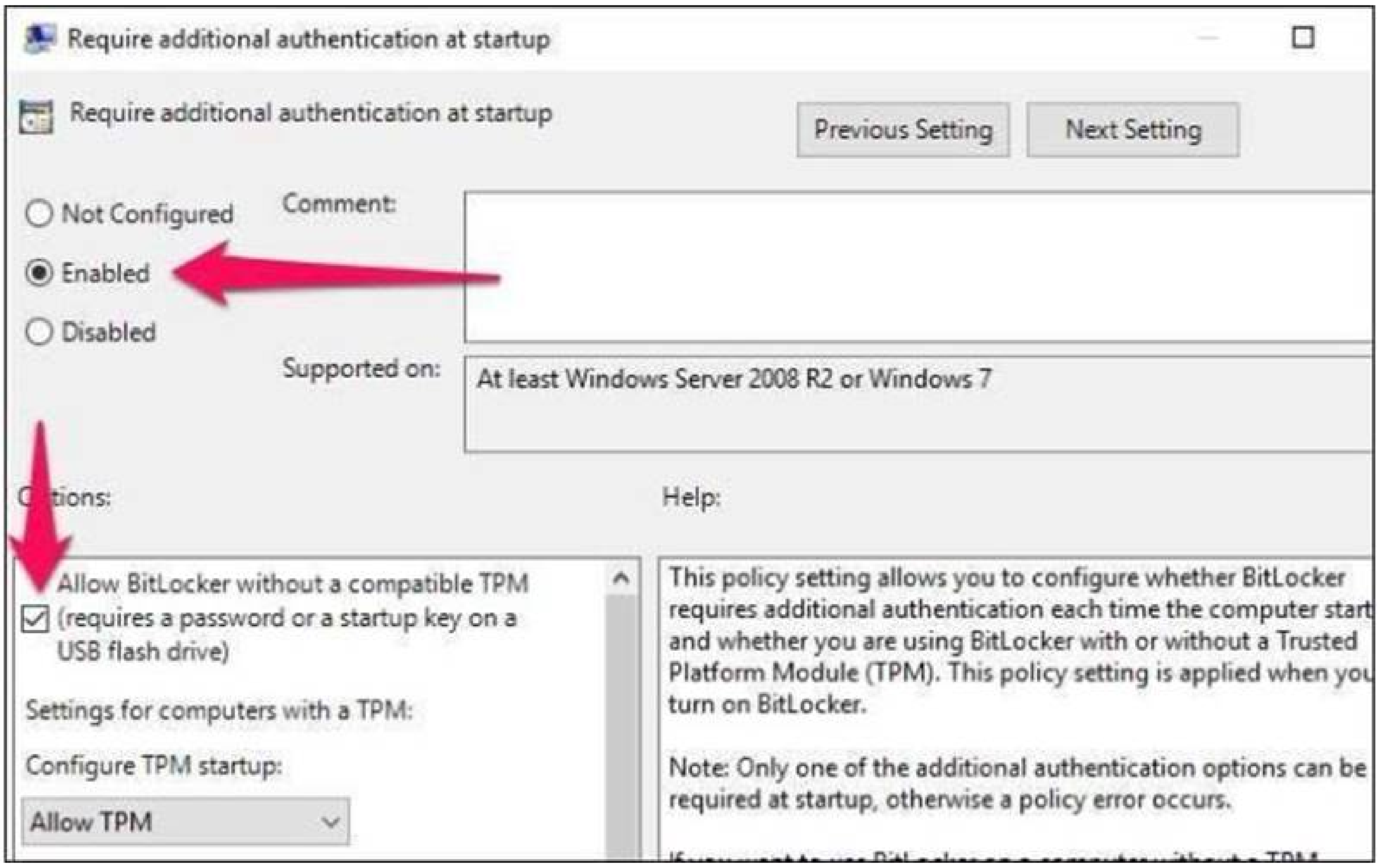
Edit policy setting

Requirements:
At least Windows Server 2008 R2 or Windows 7

Description:
This policy setting allows you to

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

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



Require additional authentication at startup

Require additional authentication at startup

○ Not Configured
● Enabled
○ Disabled

Comment:

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

Options:

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

Settings for computers with a TPM:

Configure TPM startup: Allow TPM

Help:

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

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

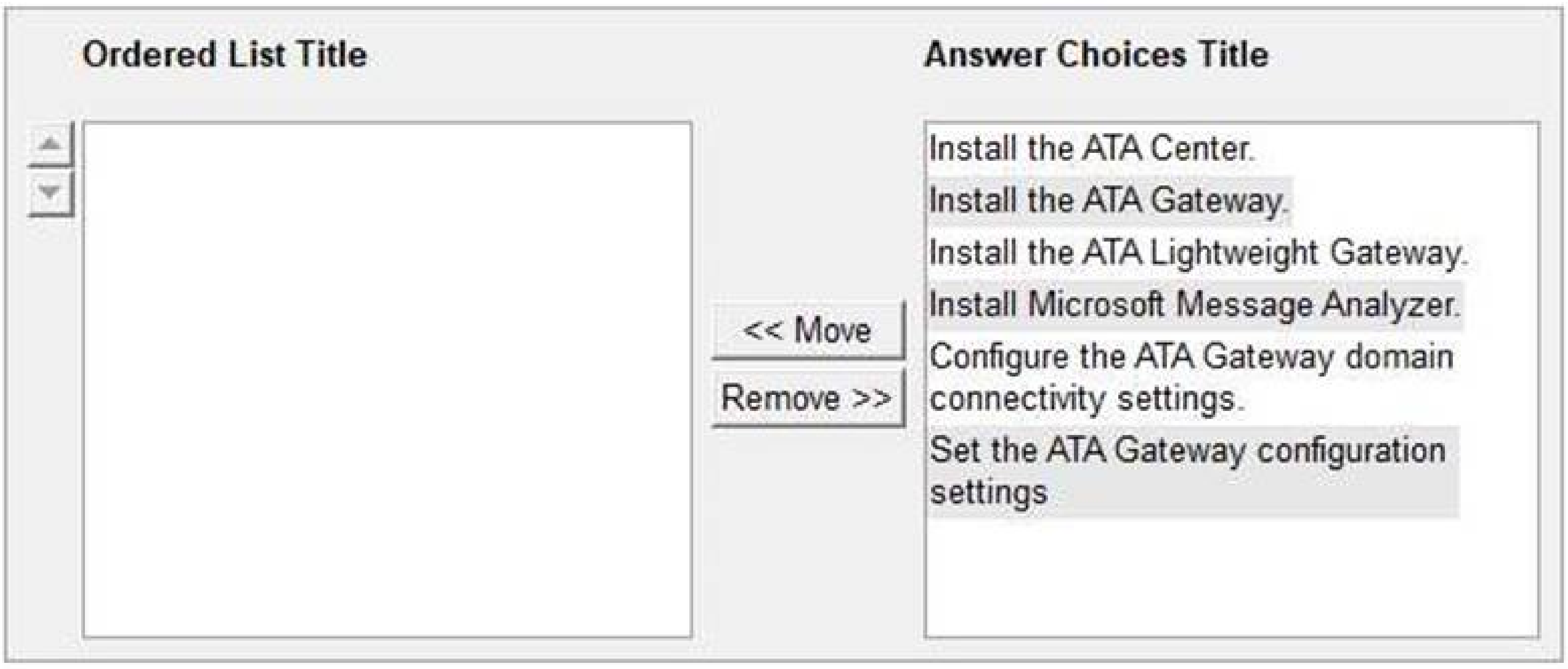
Select “Enabled” at the top of the window, and ensure the “Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)” checkbox is enabled here.
Click “OK” to save your changes. You can now close the Group Policy Editor window. Your change takes effect immediately—you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

NEW QUESTION 85
Your network contains an Active Directory domain named contoso.com.
The domain contains 10 computers that are in an organizational unit (OU) named OU1. You deploy the Local Administrator Password Solution (LAPS) client to the computers.
You link a Group Policy object (GPO) named GPO1 to OU1, and you configure the LAPS password policy settings in GPO1.
You need to ensure that the administrator passwords on the computers in OU1 are managed by using LAPS.
Which two actions should you perform? Each correct answer presents part of the solution.

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

Answer: BE

NEW QUESTION 90
DRAG DROP
Your network contains an Active Directory domain named contoso.com.
The domain contains two servers named Server1 and Server2 that run Windows Server 2016. You need to install Microsoft Advanced Threat Analytics (ATA) on Server1 and Server2. Which four actions should you perform in sequence?



Ordered List Title

Answer Choices Title

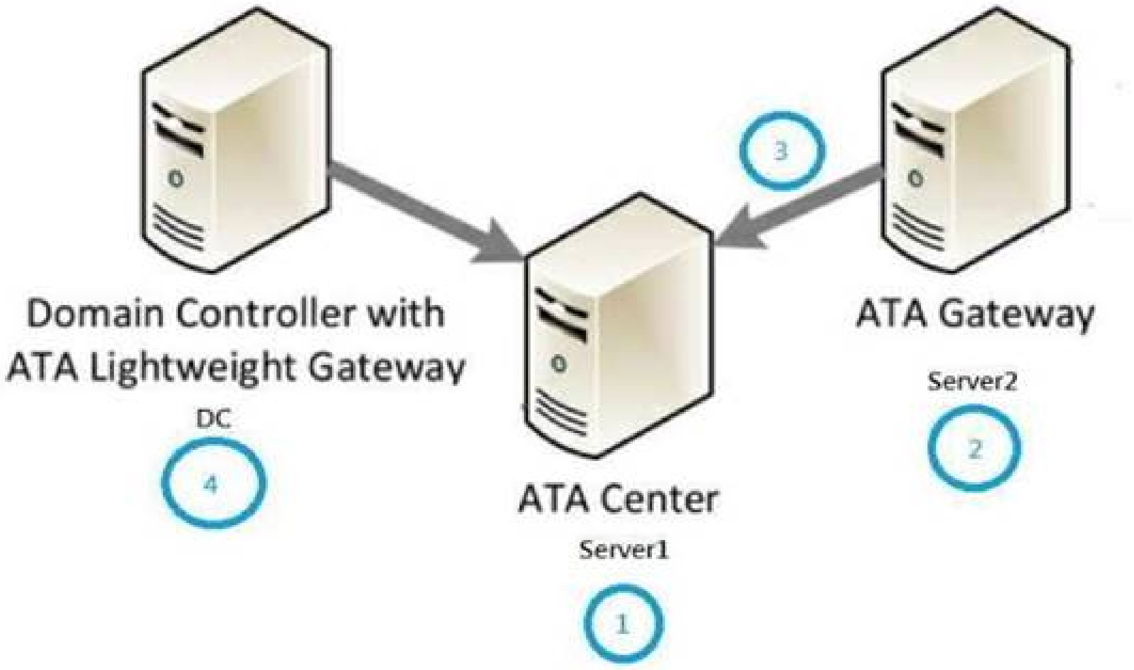
Install the ATA Center.
Install the ATA Gateway.
Install the ATA Lightweight Gateway.
Install Microsoft Message Analyzer.
Configure the ATA Gateway domain connectivity settings.
Set the ATA Gateway configuration settings

A. Mastered

B. Not Mastered

Answer: A

Explanation:
Correct Order of Actions:-
1. Install ATA Center (on Server1 for example)
2. Install ATA Gateway (on Server2 for example, if Server2 has internet connectivity)
3. Set the ATA Gateway configuration settings. (Register Server2 ATA Gateway to Server1's ATA Center)
4. Install the ATA Lightweight Gateway.
Since there are not switch-based port mirroring choice used to capture domain controller's inbound and outbound traffic,
installing ATA Lightweight Gateway on DCs to forward security related events to ATA Center is necessary.



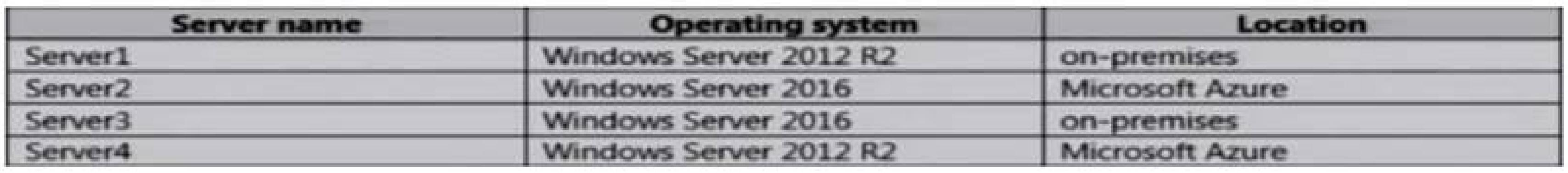
NEW QUESTION 93
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1.
On Server1, administrators plan to use several scripts that have the .ps1 extension.
You need to ensure that when code is generated from the scripts, an event containing the details of the code is logged in the Operational log.
Which Group Policy setting or settings should you configure?

A. Enable Protected Event Logging
B. Audit Process Creation and Audit Process Termination
C. Turn on PovverShell Script Block Logging
D. Turn on PowerShell Transcription

Answer: C

Explanation:
https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit_script
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 GPO Administrative Templates -> Windows Components -> Windows PowerShell).
Answer D is incorrect, since Transcription (Start-Transcript -path <FilePath>) uses a custom output location instead of Event Viewer \\ Operational Log

NEW QUESTION 97
Your network contains an Active Directory domain named contoso.com. All client computers run Windows 10.
You plan to deploy a Remote Desktop connection solution for the client computers.
You have four available servers in the domain that can be configured as Remote Desktop servers. The servers are configured as shown in the following table.



Server name	Operating system	Location
Server1	Windows Server 2012 R2	on-premises
Server2	Windows Server 2016	Microsoft Azure
Server3	Windows Server 2016	on-premises
Server4	Windows Server 2012 R2	Microsoft Azure

You need to ensure that all Remote Desktop connections can be protected by using Remote Credential Guard.
Solution: You deploy the Remote Desktop connection solution by using Server4. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
No, as Server4 is a Windows Server 2012R2 which does not meet the requirements of Remote Credential Guard.

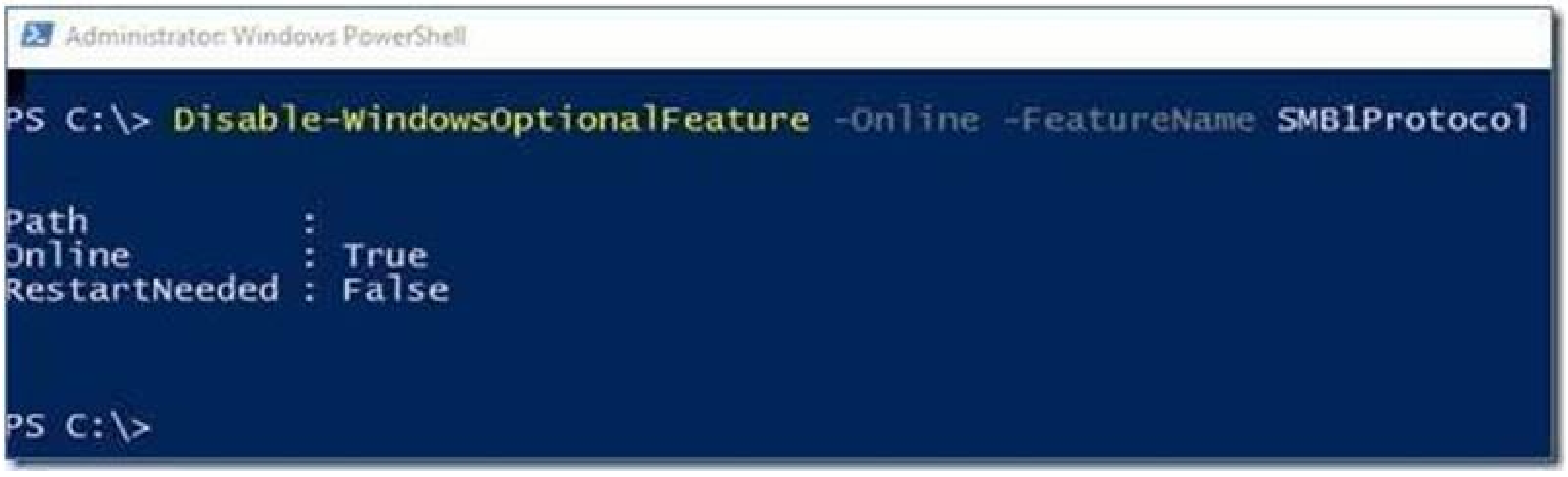
https://docs.microsoft.com/en-us/windows/access-protection/remote-credential-guard Remote Credential Guard requirements
To use Windows Defender Remote Credential Guard, the Remote Desktop client and remote host must meet the following requirements:
The Remote Desktop client device:
Must be running at least Windows 10, version 1703 to be able to supply credentials.
Must be running at least Windows 10, version 1607 or Windows Server 2016 to use the user's signed-in credentials. This requires the user's account be able to sign in to both the client device and the remote host.
Must be running the Remote Desktop Classic Windows application. The Remote Desktop Universal Windows Platform application doesn't support Windows Defender Remote Credential Guard.
Must use Kerberos authentication to connect to the remote host. If the client cannot connect to a domain controller, then RDP attempts to fall back to NTLM.
Windows Defender Remote Credential Guard does not allow NTLM fallback because this would expose credentials to risk.
The Remote Desktop remote host:
Must be running at least Windows 10, version 1607 or Windows Server 2016. Must allow Restricted Admin connections.
Must allow the client's domain user to access Remote Desktop connections. Must allow delegation of non-exportable credentials.

NEW QUESTION 99
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



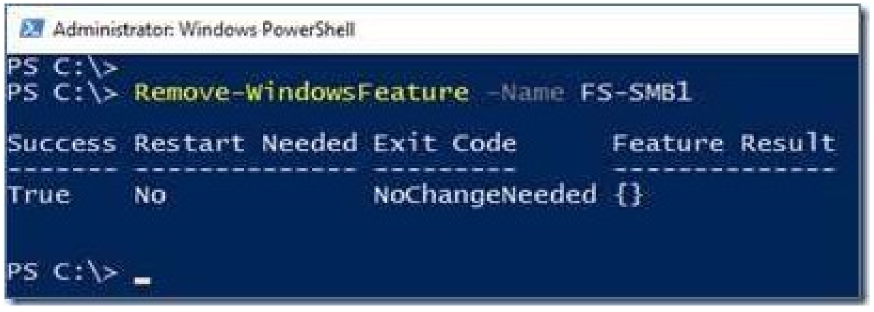
```
PS C:\> Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol


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 104
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2016.
You need to prevent direct .NET scripts invoked by interactive Windows PowerShell sessions from running on the servers.
What should you do for each server?

A. Create an AppLocker rule.
B. Create a Code Integrity rule.
C. Disable PowerShell Remoting.
D. Modify the local Kerberos policy setting

Answer: C

NEW QUESTION 106
You have a server named Server1 that runs Windows Server 2016.
You need to identify the default action for the inbound traffic when Server1 connects to the domain. Which cmdlet should you use?

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

G. Get-NetFirewallApplicationFilter

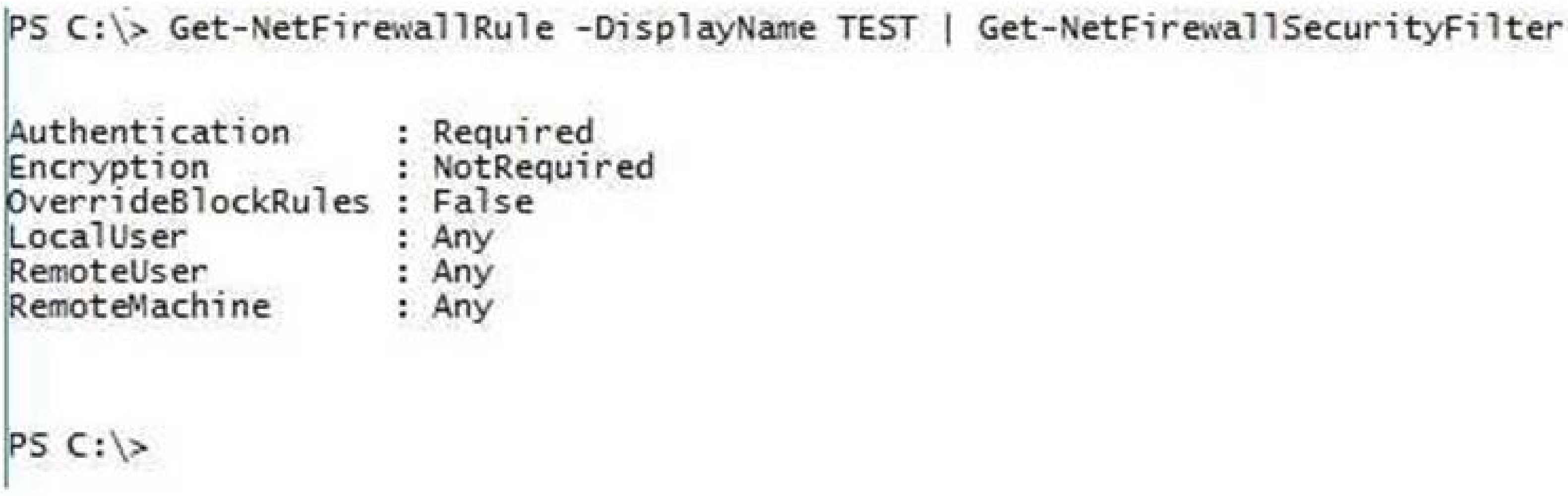
Answer: C

NEW QUESTION 108
You have a server named Server1 that runs Windows Server 2016.
You need to identify whether any inbound rules on Server1 require that users be authenticated before they can connect to the server. Which cmdlet should you use?

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

Answer: B

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



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


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



PS C:\>
```

NEW QUESTION 109
Your network contains an Active Directory forest named contoso.com. The forest functional level is Windows Server 2012.
The forest contains 20 member servers that are configured as file servers. All domain controllers run Windows Server 2016.
You create a new forest named contosoadmin.com.
You need to use the Enhanced Security Administrative Environment (ESAE) approach for the administration of the resources in contoso.com.
Which two actions should you perform? Each correct answer presents part of the solution.

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

Answer: AC

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

NEW QUESTION 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.

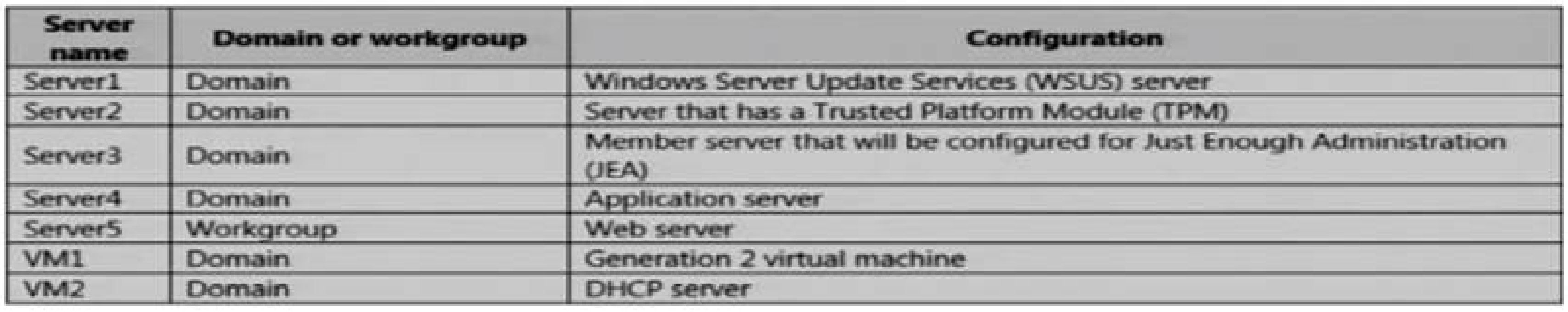
A. From a Group Policy object (GPO), configure Public Key Policies
B. Deploy a Multi-Factor Authentication provider and copy the required certificates to the MIM server.
C. From the MIM Portal, configure the Password Reset AuthN Workflow.
D. Deploy a Multi-Factor Authentication provider and copy the 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 115
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.



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

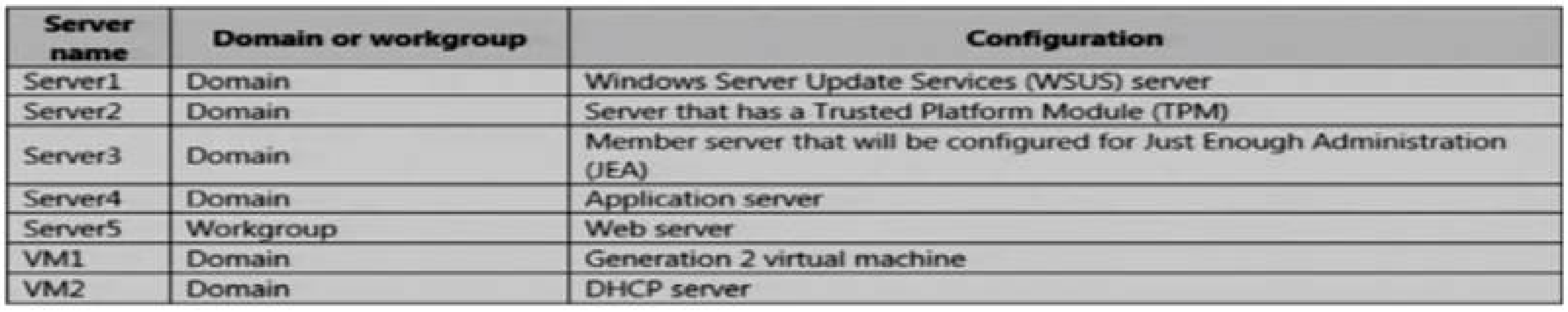
All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.
All laptops are protected by using BitLocker Drive Encryption (BitLocker).You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.
An OU named OU2 contains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

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

Answer: B

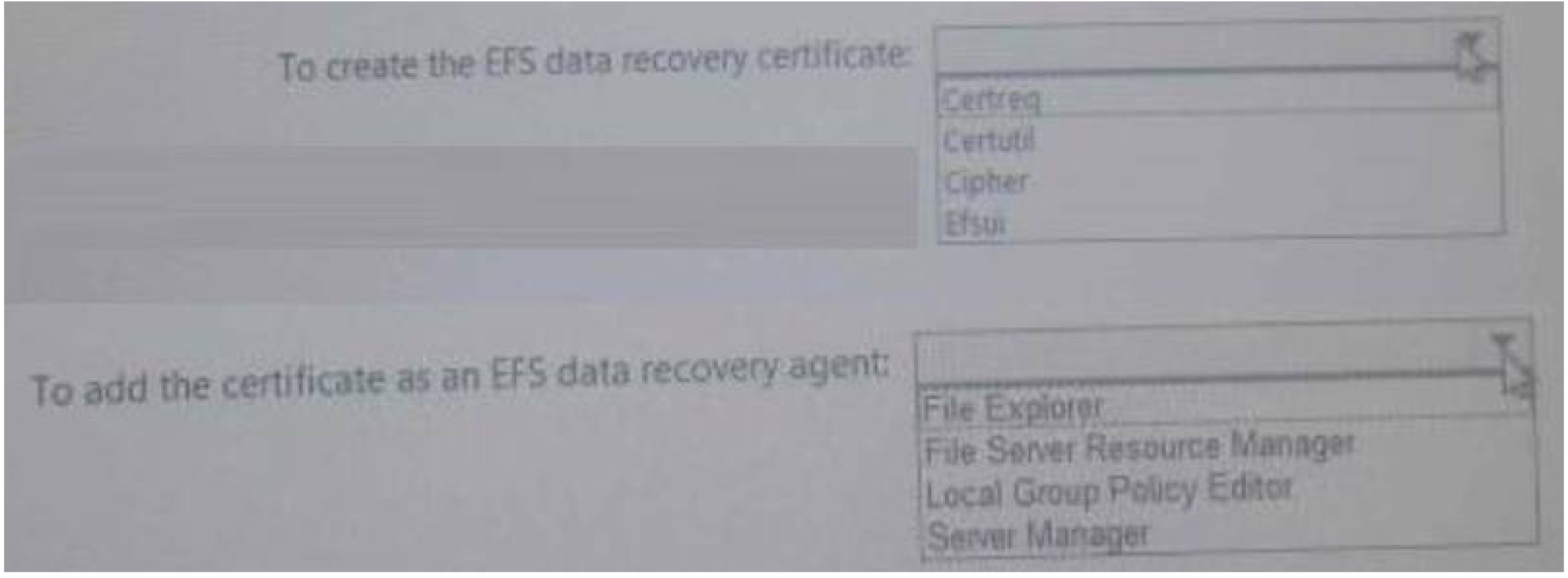
Explanation:
https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-how-to-enablenetwork- unlock Network Unlock core requirements
Network Unlock must meet mandatory hardware and software requirements before the feature can automatically unlock domain joined systems. These requirements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

NEW QUESTION 117
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:
- Certreq
- Certutil
- Cipher
- Efsui

To add the certificate as an EFS data recovery agent:
- File Explorer
- File Server Resource Manager
- Local Group Policy Editor
- Server Manager

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 118
You deploy the Host Guardian Service (HGS).
You have several Hyper-V hosts that have older hardware and Trusted Platform Modules (TPMs) version 1.2.
You discover that the Hyper-V hosts cannot start shielded virtual machines.
You need to configure HGS to ensure that the older Hyper-V hosts can host shielded virtual machines. What should you do?

A. Run the Set-HgsServer cmdlet and specify the -TrustTpm parameter.
B. Run the Set-HgsServer cmdlet and specify the -TrustActiveDirectory parameter.
C. Run the Clear-HgsServer cmdlet and specify the -Clustername parameter
D. Run the Clear-HgsServer cmdlet and specify the -Force parameter.
E. It is not possible to enable older Hyper-V hosts to run Shielded virtual machines

Answer: E

Explanation:
Requirements and Limitations
There are several requirements for using Shielded VMs and the HGS:
One bare metal host: You can deploy the Shielded VMs and the HGS with just one host. However,
Microsoft
recommends that you cluster HGS for high availability.
Windows Server 2016 Datacenter Edition: The ability to create and run Shielded VMs and the HGS is only
supported by Windows Server 2016 Datacenter Edition.
For Admin-trusted attestation mode: You only need to have server hardware capable of running Hyper-V in
Windows Server 2016 TP5 or higher.
For TPM-trusted attestation: Your servers must have TPM 2.0 and UEFI 2.3.1 and they must boot in UEFI
mode. The hosts must also have secure boot enabled. Hyper-V role: Must be installed on the guarded host. HGS Role: Must be added to a physical host.
Generation 2 VMs.
A fabric AD domain.
An HGS AD, which in Windows Server 2016 TP5 is a separate AD infrastructure from your fabric AD.

NEW QUESTION 122
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 123
Your network contains several secured subnets that are disconnected from the Internet.
One of the secured subnets contains a server named Server1 that runs Windows Server 2016.
You implement Log Analytics in Microsoft Operations Management Suite (OMS) for the servers that connect to the Internet.
You need to ensure that Log Analytics can collect logs from Server1.
Which two actions should you perform? Each correct answer presents part of the solution.

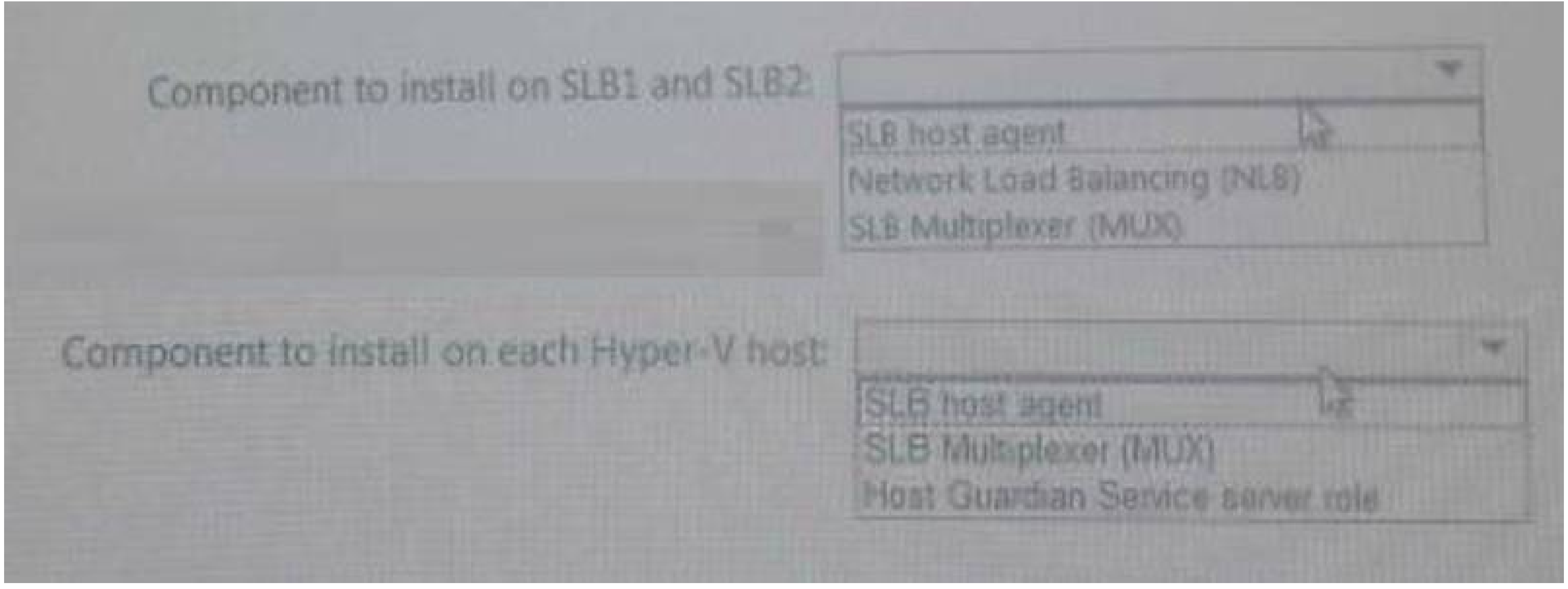
A. Install the OMS Log Analytics Forwarder on a server that has Internet connectivity.
B. Create an event subscription on a server that has Internet connectivity.
C. Create a scheduled task on Server1.
D. Install the OMS Log Analytics Forwarder on Server1.
E. Install Microsoft Monitoring Agent on Server1.

Answer: AE

Explanation:
https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-oms-gateway OMS Log Analytics Forwarder = OMS Gateway
If your IT security policies do not allow computers on your network to connect to the Internet, such as point of sale (POS) devices, or servers supporting IT services, but you need to connect them to OMS to manage and monitor them, they can be configured to communicate directly with the OMS Gateway (previous called “OMS Log Analytics Fowarder”) to receive configuration and forward data on their behalf.
You have to also install Microsoft Monitoring Agent on Server1 to generate and send events to the OMS
Gateway,since Server1 does not have direct Internet connectivity.

NEW QUESTION 125
HOTSPOT

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



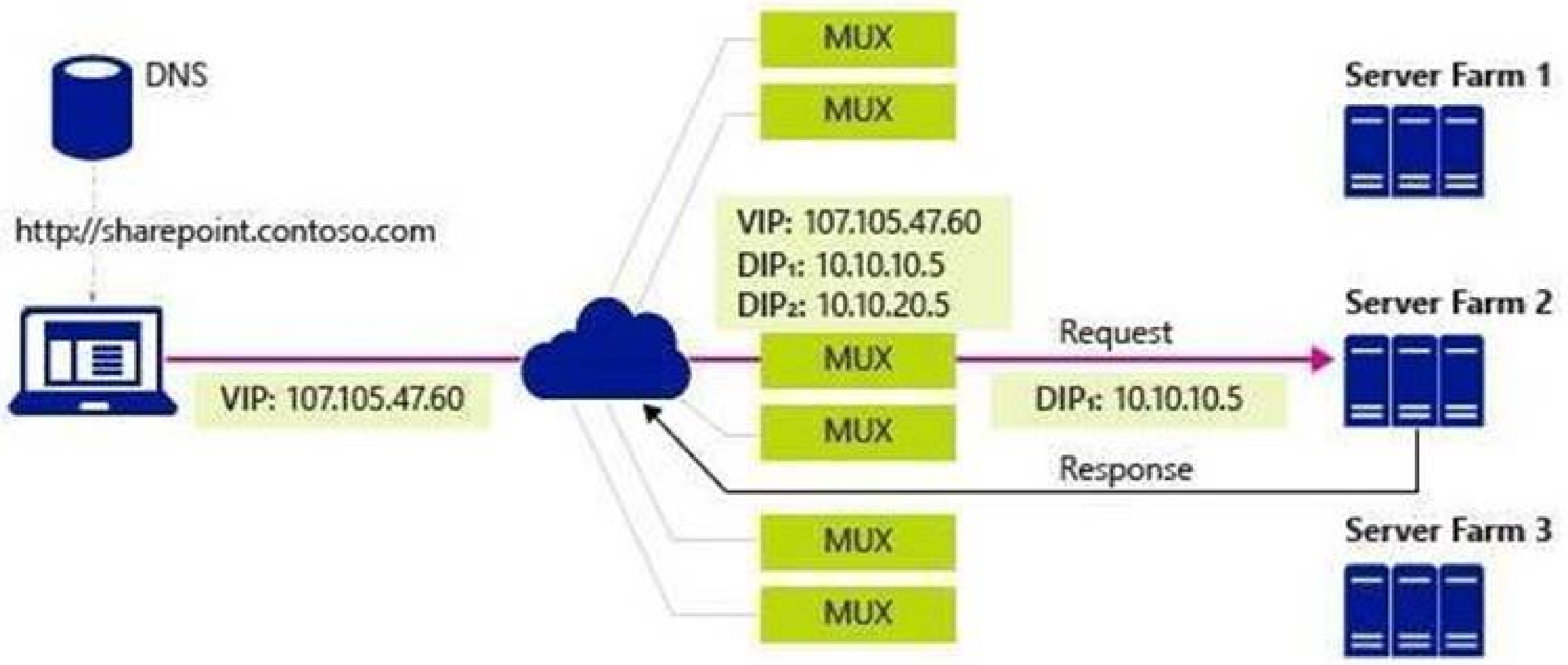
Component to install on SLB1 and SLB2:
- SLB host agent
- Network Load Balancing (NLB)
- SLB Multiplexer (MUX)

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

A. Yes
B. No

Answer: A

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

NEW QUESTION 134
You network contains an Active Directory forest named contoso.com.
All domain controllers run Windows Server 2016 Member servers run either Windows Server 2012 R2 or Windows Server 2016.
Client computers run either Windows 8.1 or Windows 10.
You need to ensure that when users access files in shared folders on the network, the files are encrypted when they are transferred over the network.
Solution: You enable access-based enumeration on all the file shares. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Access-Based Enumeration does not help encrypting network file transfer.

NEW QUESTION 135
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows10.
The network uses the 172.16.0.0/16 address space.
Computer1 has an application named App1.exe that is located in D:\Apps\. App1.exe is configured to accept connections on TCP port 8080.
You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.
Solution: You run the New-NetFirewallRule –DisplayName "Rule1" –Direction Inbound
–Program "D:\Apps\App1.exe" –Action Allow -Profile Domain command. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 139
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. The domain has Dynamic Access Control enabled.
Server1 contains a folder named C:\Folder1. Folder1 is shared as Share1.
You need to audit all access to the contents of Folder1 from Server2. The solution must minimize the number of event log entries.
Which two audit policies should you enable on Server1? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

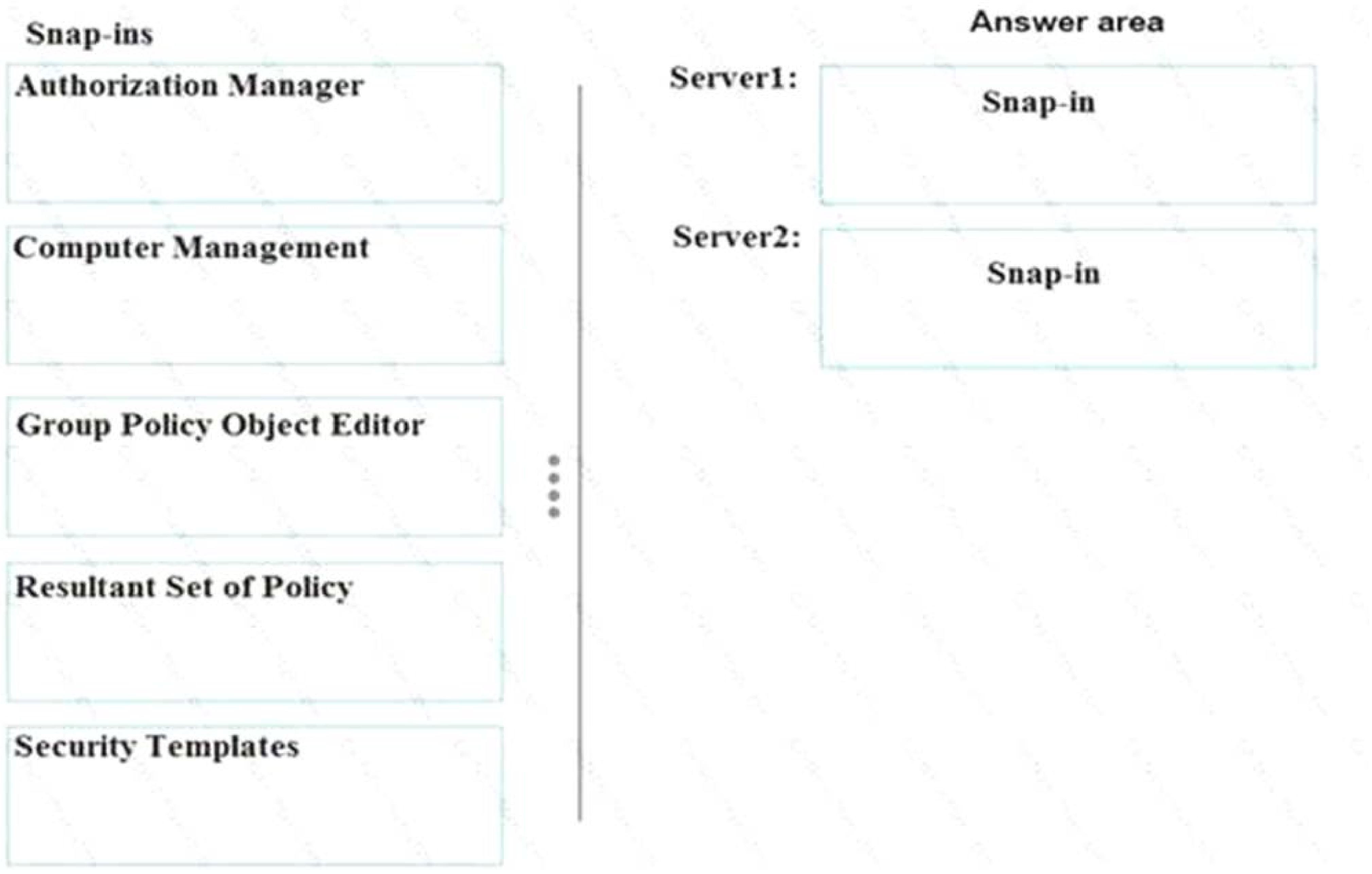
A. Global Object Access- File System
B. Object Access – Audit Detailed File Share
C. Object Access – Audit Other Object Access Events
D. Object Access – Audit File System
E. Object Access – Audit File Share

Answer: BE

Explanation:

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

NEW QUESTION 141
DRAG DROP
You have two servers named Server1 and Server2 that run Windows Server 2016. The servers are in a workgroup.
You need to create a security template that contains the security settings of Server1 and to apply the template to Server2. The solution must minimize administrative effort.
Which snap-in should you use for each server? To answer, drag the appropriate snap-ins to the correct servers. Each snap-in may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Snap-ins

Authorization Manager

Computer Management

Group Policy Object Editor

Resultant Set of Policy

Security Templates

Answer area

Server1: Snap-in

Server2: Snap-in

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 144
......