Exam Questions 70-744

Securing Windows Server 2016

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

NEW QUESTION 1
Note: The question is part of a series of questions th« 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 2,000 client computers that run Windows 10. All client computers are deployed from 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 them as PAWs. You deploy 10 additional computers and configure them by using the customized Windows image.
Does this meet the goal?

A. Yes
B. No

Answer: A

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 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

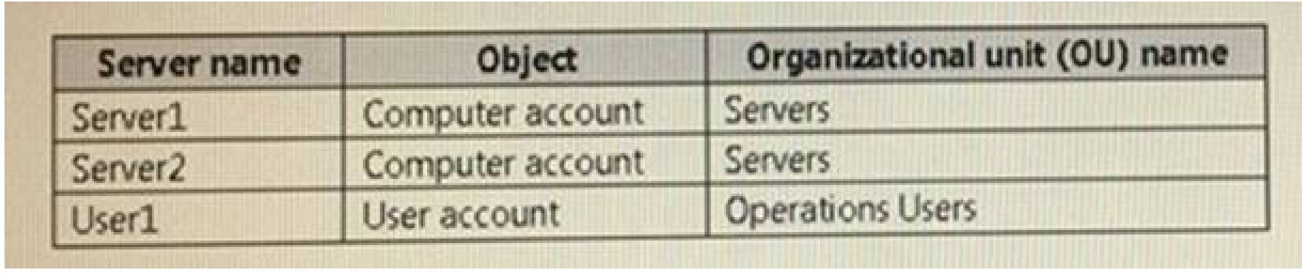
NEW QUESTION 3
Note: This question is part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question In this section, you will NOT be able to return to It. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains 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 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. All servers run Windows Server 2016. All client computers run Windows 10.
The relevant objects in the domain are configured as shown in the following table.



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

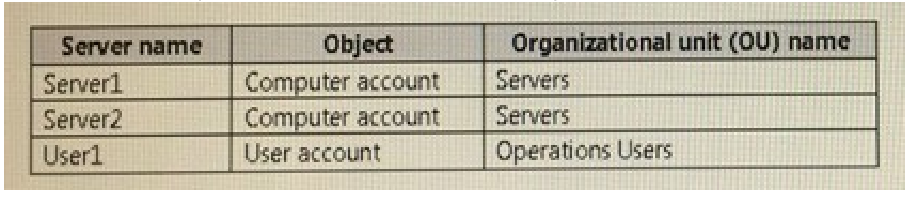
You need to assign User1 the right to restore files and folders on Server1 and Server2.
Solution: You create a Group Policy object (GPO), you link the GPO to the Servers OU, and then you modify the Users Rights Assignment in the GPO.
Does this meet the goat?

A. Yes
B. No

Answer: B

Explanation:
References:
https://technet.microsoft.com/en-us/library/cc771990(v=ws.11).aspx

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 sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. All servers run Windows
Server 2016. All client computers run Windows 10.
The relevant objects in the domain are configured as shown in the following table.



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

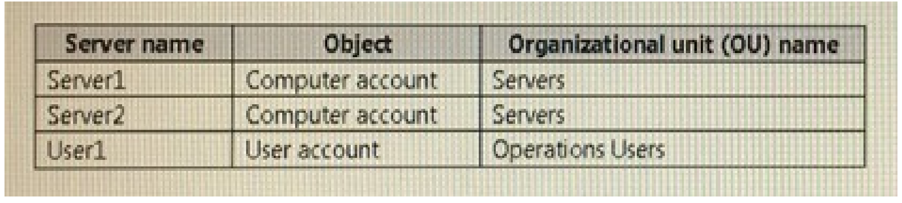
You need to assign User1 the right to restore files and folders on Server1 and Server2. Solution: You add User1 to the Backup Operators group in contoso.com. Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 6
Note: This question b part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear In the review screen.
Your network contains an Active Directory domain named contow.com. All servers run Windows Server 2016. All client computers run Windows 10.
The relevant objects in the domain are configured as shown in the following table.



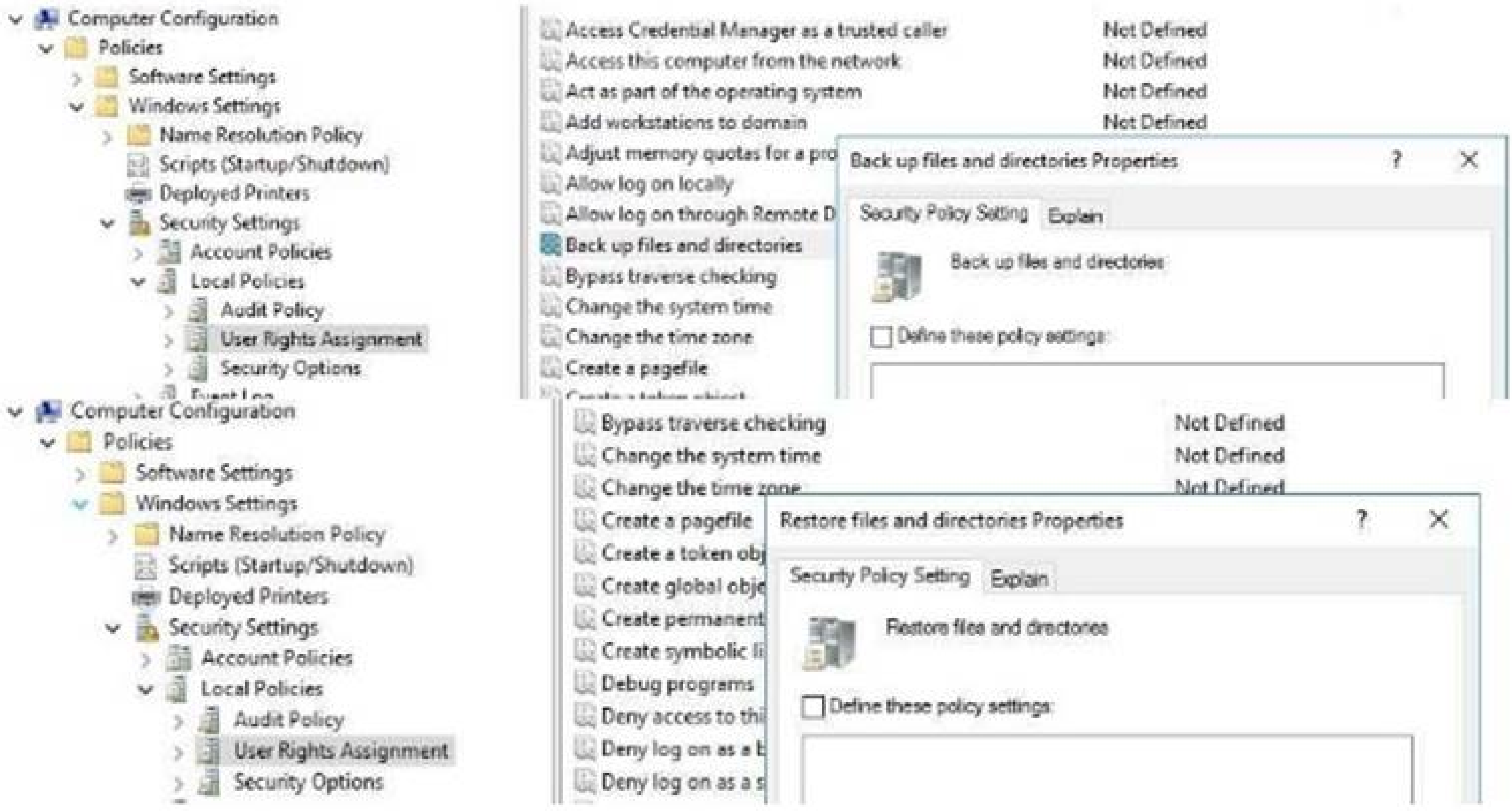
Server name	Object	Organizational unit (OU) name
Server1	Computer account	Servers
Server2	Computer account	Servers
User1	User account	Operations Users

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

A. Yes
B. No

Answer: A

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



Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log

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

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

Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options

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

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

NEW QUESTION 7
Note: This question is part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question In this section, you will NOT be able to return to It. As a result, these questions will not appear In the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains multiple Hyper-V hosts.
You need to deploy several critical line-of-business applications to the network; to meet the following requirements:
*The resources of the applications must be isolated from the physical host.
*Each application must be prevented from accessing the resources of the other applications.
*The configurations of the applications must be accessible only from the operating system that hosts
the application.
Solution: You deploy a separate Windows container for each application. Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 8
Note: Thb question Is part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you willNOTbeabletorrturntoit.Asa result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains multiple Hyper-V hosts.
You need to deploy several critical line-of-business applications to the network to meet the following requirements:
*The resources of the applications must be isolated from the physical host
*Each application must be prevented from accessing the resources of the other applications.
*The configurations of the applications must be accessible only from the operating system that hosts the application.
Solution: You deploy one Windows container to host all of the applications. Does this meet the goal?

A. Yes
B. No

Answer: B

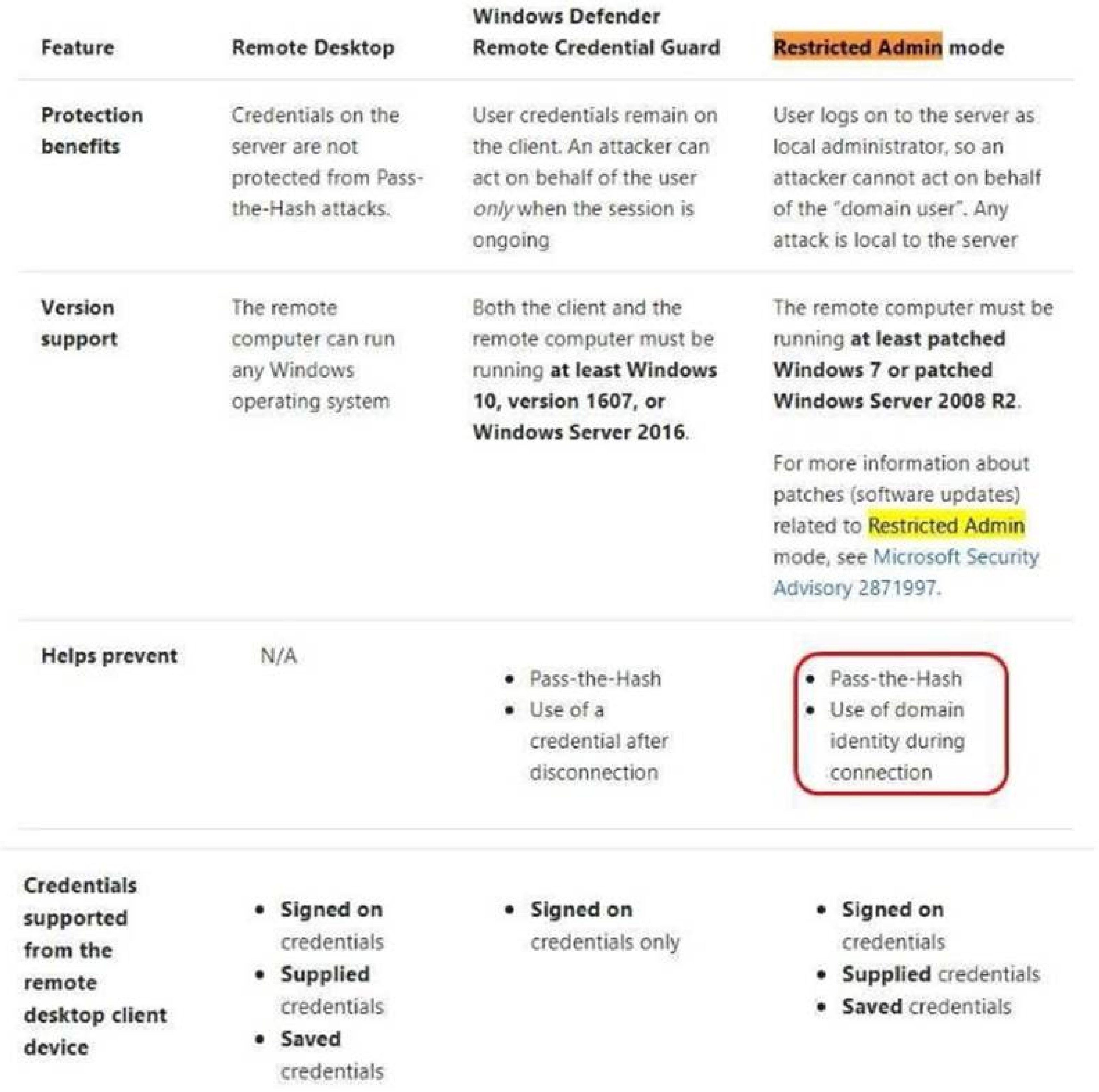
Explanation:
References:
https://docs.microsoft.com/en-us/virtualization/windowscontainers/about/

NEW QUESTION 9
Your network contains an Active Directory domain named contoso.com. The domain contains 1,000 client computers that run Windows 10.
A security audit reveals that the network recently experienced a Pass-the-Hash attack. The attack was initiated from a client computer and accessed Active Directory objects restricted to the members of the Domain Admins group.
You need to minimize the impact of another successful Pass-the-Hash attack on the domain. What should you recommend?

A. Instruct all users to sign in to a client computer by using a Microsoft account.
B. Move the computer accounts of all the client computers to a new organizational unit (OU). Remove the permissions to the new OU from the Domain Admins group.
C. Instruct all administrators to use a local Administrators account when they sign in to a client computer.
D. Move the computer accounts of the domain controllers to a new organizational unit (OU). Remove the permissions to the new OU from the Domain Admins group.

Answer: C

Explanation:
https://docs.microsoft.com/en-us/windows/access-protection/remote-credential-guard



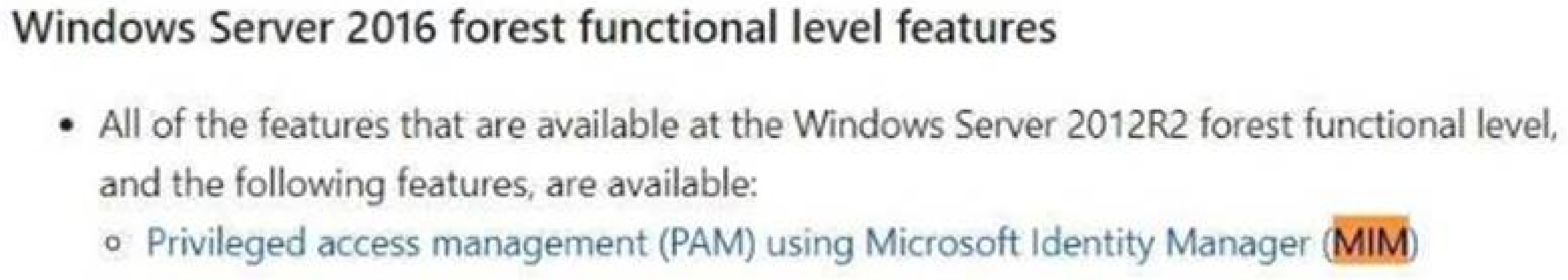
Feature	Remote Desktop	Windows Defender Remote Credential Guard	Restricted Admin mode
Protection benefits	Credentials on the server are not protected from Pass-the-Hash attacks.	User credentials remain on the client. An attacker can act on behalf of the user *only* when the session is ongoing	User logs on to the server as local administrator, so an attacker cannot act on behalf of the "domain user". Any attack is local to the server
Version support	The remote computer can run any Windows operating system	Both the client and the remote computer must be running **at least Windows 10, version 1607, or Windows Server 2016**.	The remote computer must be running **at least patched Windows 7 or patched Windows Server 2008 R2**. For more information about patches (software updates) related to Restricted Admin mode, see Microsoft Security Advisory 2871997.
Helps prevent	N/A	• Pass-the-Hash • Use of a credential after disconnection	• Pass-the-Hash • Use of domain identity during connection
Credentials supported from the remote desktop client device	• **Signed on** credentials • **Supplied** credentials • **Saved** credentials	• **Signed on** credentials only	• **Signed on** credentials • **Supplied** credentials • **Saved** credentials

NEW QUESTION 10
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?

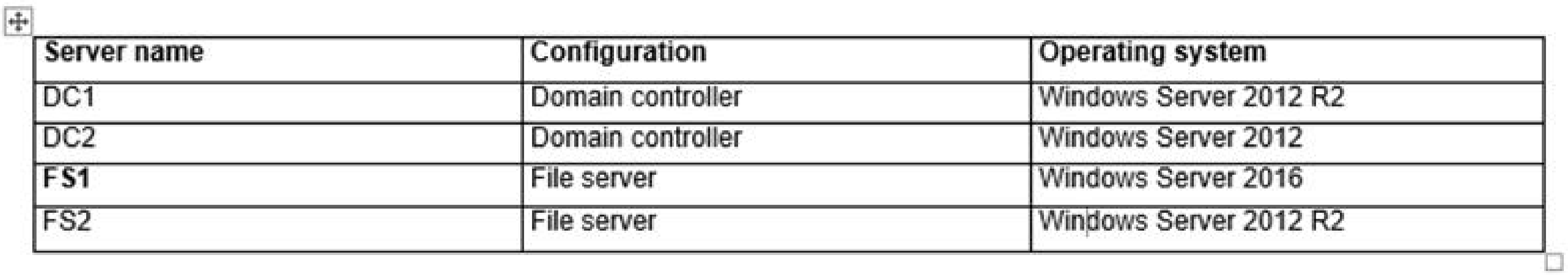
NEW QUESTION 10
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2016. Server1 is configured as a domain controller.
You configure Server1 as a Just Enough Administration (JEA) endpoint You configure the required JEA rights for a user named User1.
You need to tell User1 how to manage Active Directory objects from Server2. What should you tell User1 to do first on Server2?

A. From a command prompt, run ntdsutil.exe.
B. From Windows PowerShell, run the Import-Module cmdlet.
C. From Windows PowerShell run the Enter-PSSession cmdlet.
D. Install the management consoles for Active Directory, and then launch Active Directory Users and Computer.

Answer: C

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

NEW QUESTION 11
Your network contains an Active Directory domain named contoso.com. The domain contains four servers. The servers are configured as shown in the following table.



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

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

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

Answer: C

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

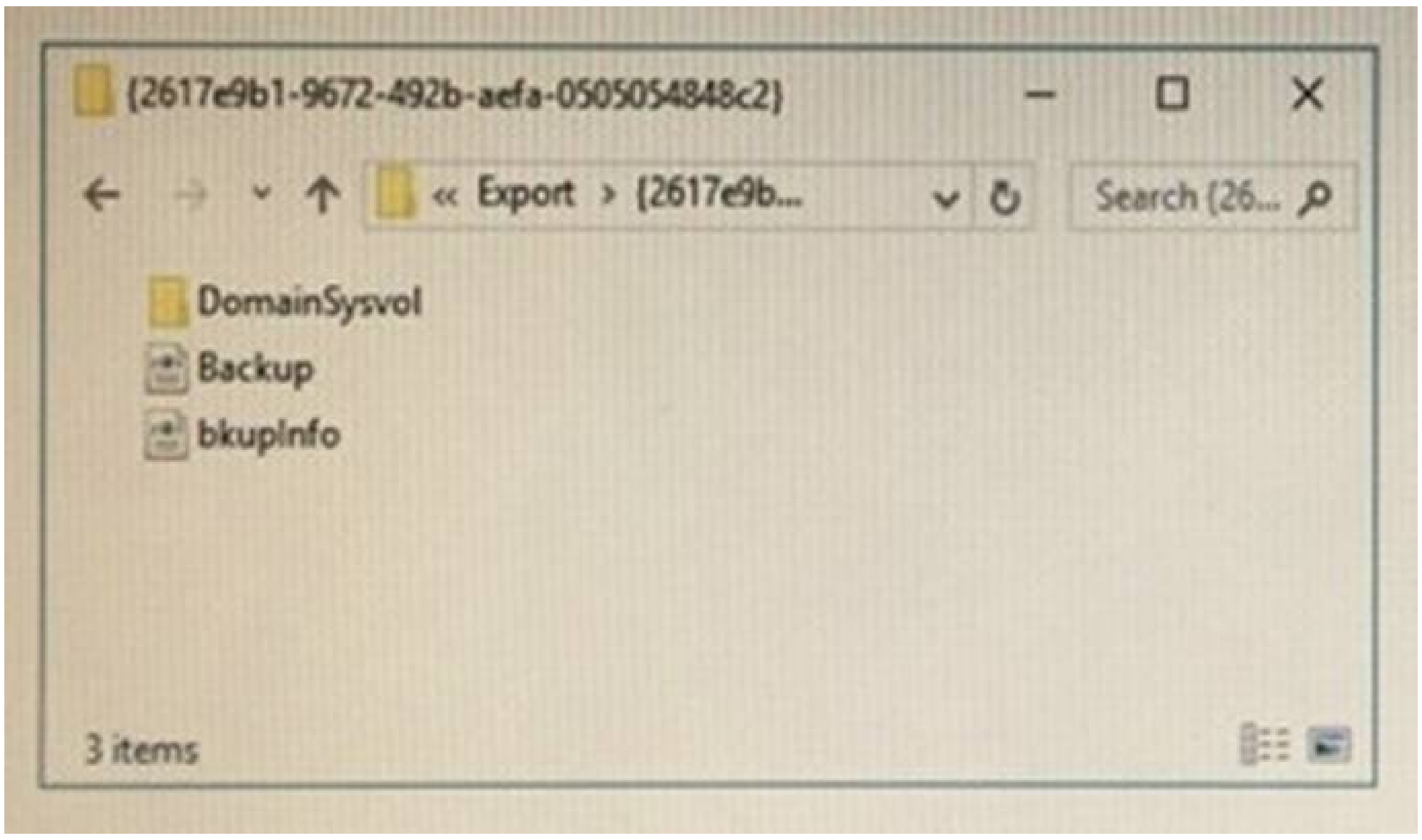
NEW QUESTION 12
Your network contains an Active Directory domain named contoso.com. The domain contains five servers. All servers run Windows Server 2016.
A new secunty policy states that you must modify the infrastructure to meet the following requirements:
*Limit the nghts of administrators.
*Minimize 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 13
Vout network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2016.
The domain contains a server named Serverl that has Microsoft Security Compliance Manager (SCM)
4.0 installed.
You export the baseline shown in the following exhibit.



{2617e9b1-9672-492b-aefa-0505054848c2}

« Export › {2617e9b...

Search (26...

DomainSysvol
Backup
bkupInfo

3 items

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

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

Answer: D

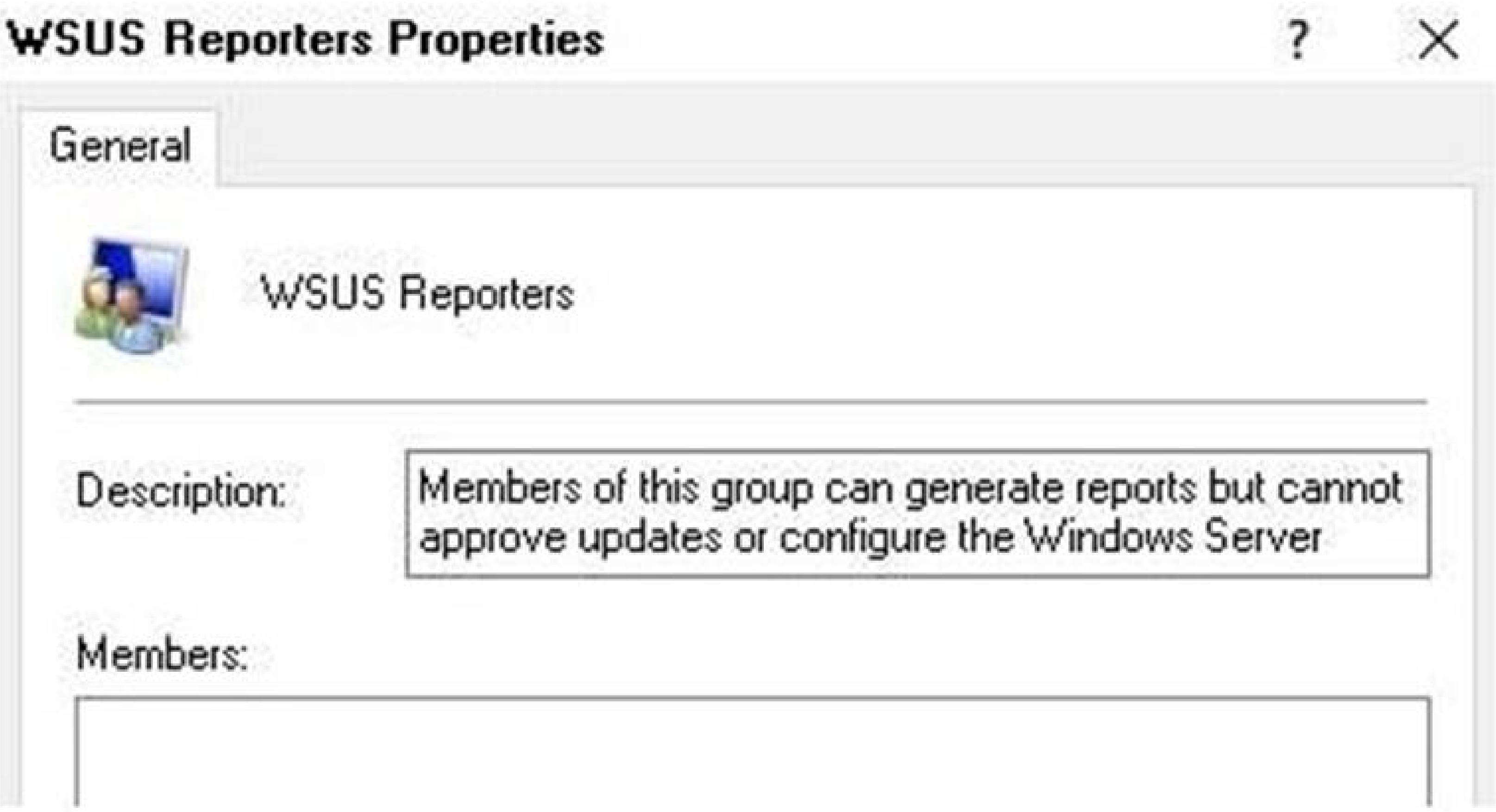
Explanation:
References:
https://anytecho.wordpress.com/2015/05/22/importing-group-policies-using-powershell-almost/

NEW QUESTION 16
Your network contains an Active Directory domain named contoso.com.
You install the Windows Server Update Services server role on a member server named Server1. Server1 runs Windows Server 2016.
You need to ensure that a user named Used can perform the following tasks:
*View the Windows Server Update Services (WSUS) configuration.
*Generate WSUS update reports.
The solution must use the principle of least privilege. What should you do on Server1?

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

Answer: B

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



WSUS Reporters Properties

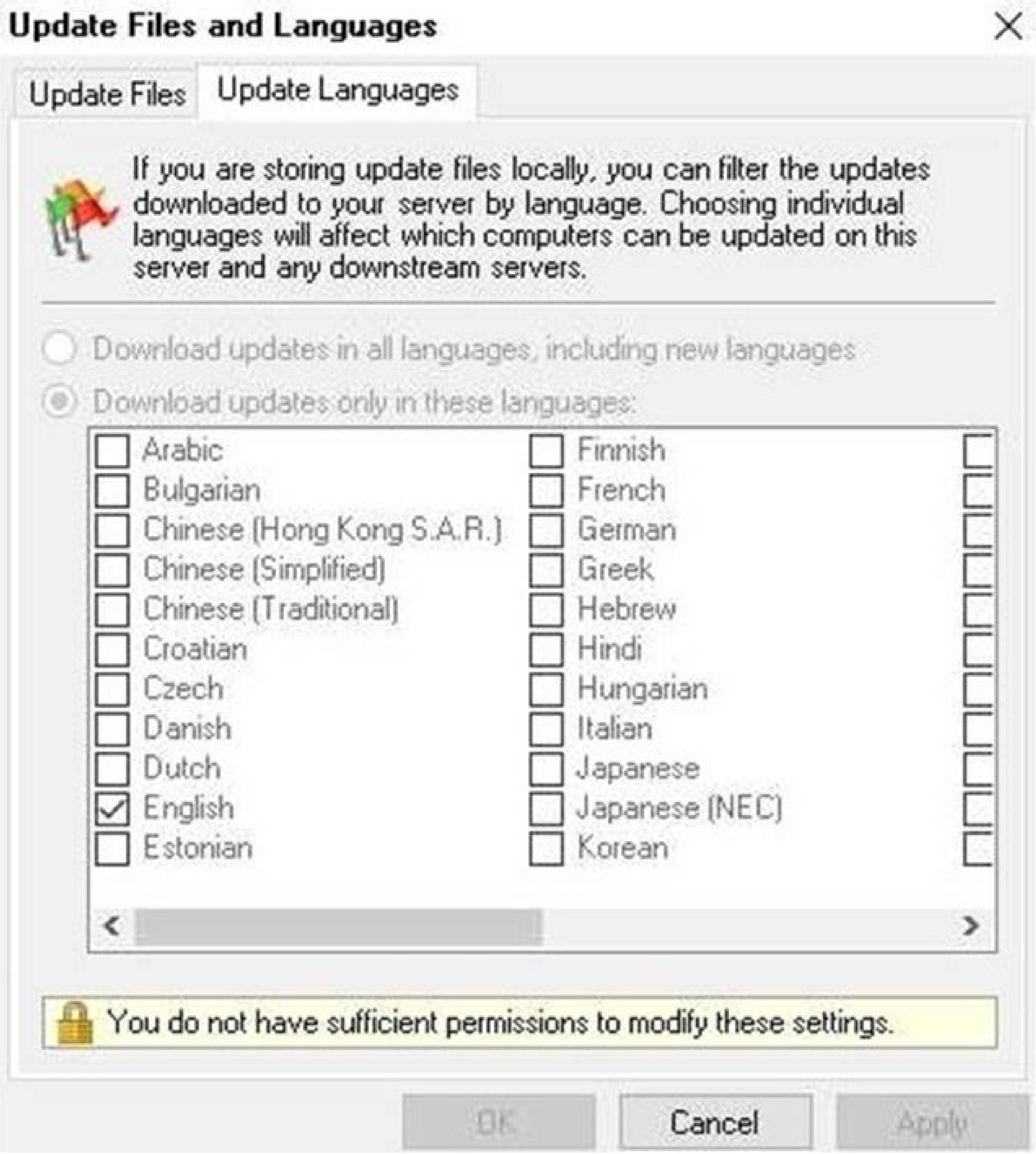
General

WSUS Reporters

Description: Members of this group can generate reports but cannot approve updates or configure the Windows Server

Members:

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



Update Files and Languages

Update Files | Update Languages

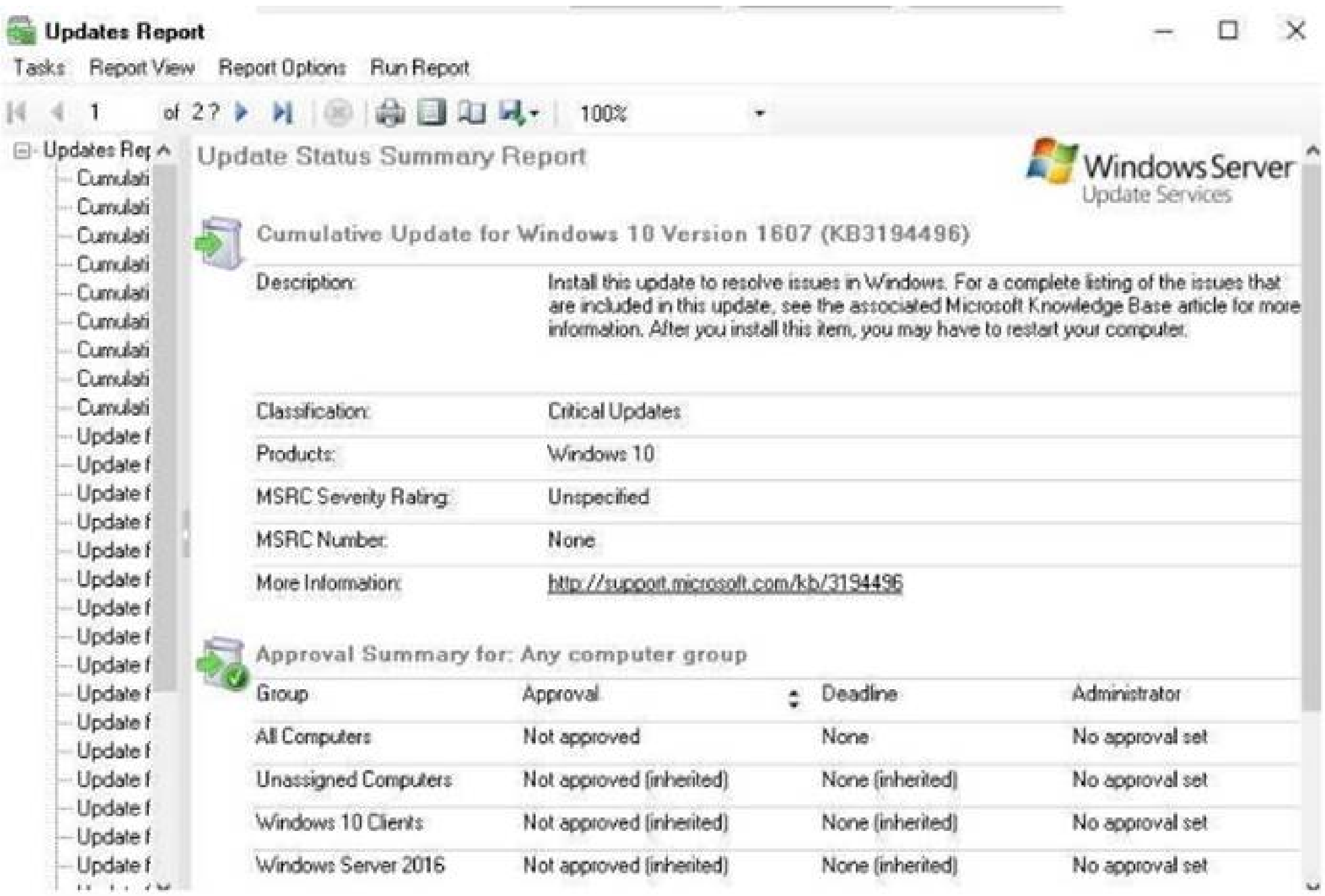
If you are storing update files locally, you can filter the updates downloaded to your server by language. Choosing individual languages will affect which computers can be updated on this server and any downstream servers.

○ Download updates in all languages, including new languages

● Download updates only in these languages:

- □ Arabic
- □ Bulgarian
- □ Chinese (Hong Kong S.A.R.)
- □ Chinese (Simplified)
- □ Chinese (Traditional)
- □ Croatian
- □ Czech
- □ Danish
- □ Dutch
- ☑ English
- □ Estonian
- □ Finnish
- □ French
- □ German
- □ Greek
- □ Hebrew
- □ Hindi
- □ Hungarian
- □ Italian
- □ Japanese
- □ Japanese (NEC)
- □ Korean

You do not have sufficient permissions to modify these settings.



Update Status Summary Report

Cumulative Update for Windows 10 Version 1607 (KB3194496)

Description:	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.
Classification:	Critical Updates
Products:	Windows 10
MSRC Severity Rating:	Unspecified
MSRC Number:	None
More Information:	http://support.microsoft.com/kb/3194496

Approval Summary for: Any computer group

Group	Approval	Deadline	Administrator
All Computers	Not approved	None	No approval set
Unassigned Computers	Not approved (inherited)	None (inherited)	No approval set
Windows 10 Clients	Not approved (inherited)	None (inherited)	No approval set
Windows Server 2016	Not approved (inherited)	None (inherited)	No approval set

NEW QUESTION 18
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 20
Note: This question Is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.
Server1 has a volume named Volume1.
A central access policy named Policy1 is deployed to the domain. You need to apply Policy1 to Volume1.
Which tool should you use?

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

Answer: A

Explanation:

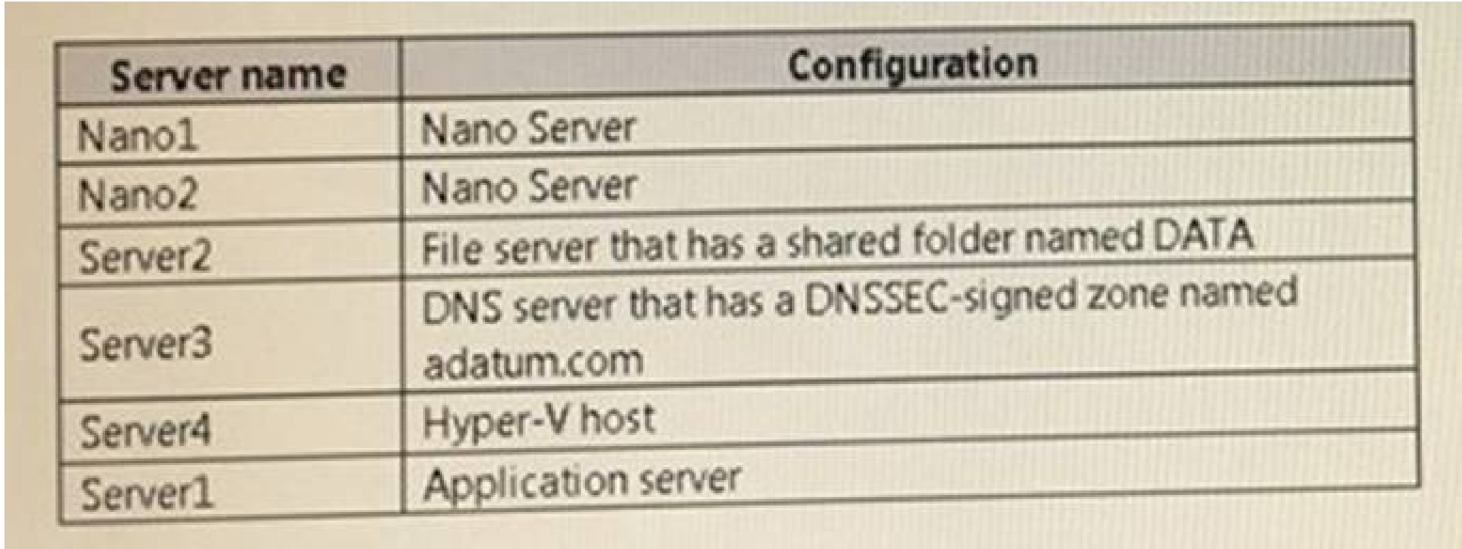
“File Explorer” = “Windows Explorer”.
https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/deploy-a-centralaccess- policy–demonstration-steps-#BKMK_1.4

NEW QUESTION 24
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 file server named Server1 that runs Windows Server 2016.
You need to create Work Folders on Server1. 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)

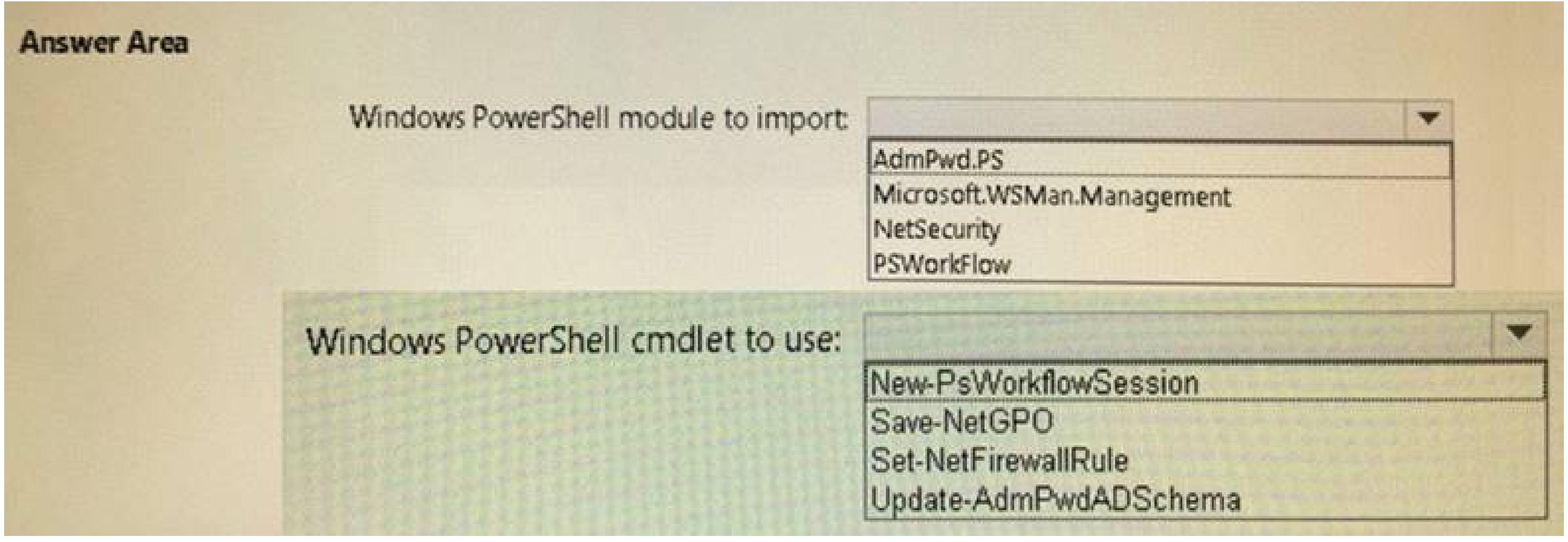
Answer: C

NEW QUESTION 27
HOTSPOT
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.
Start of repeated scenario
Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.
The domain contains the servers configured as shown in the following table.



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

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



Answer Area

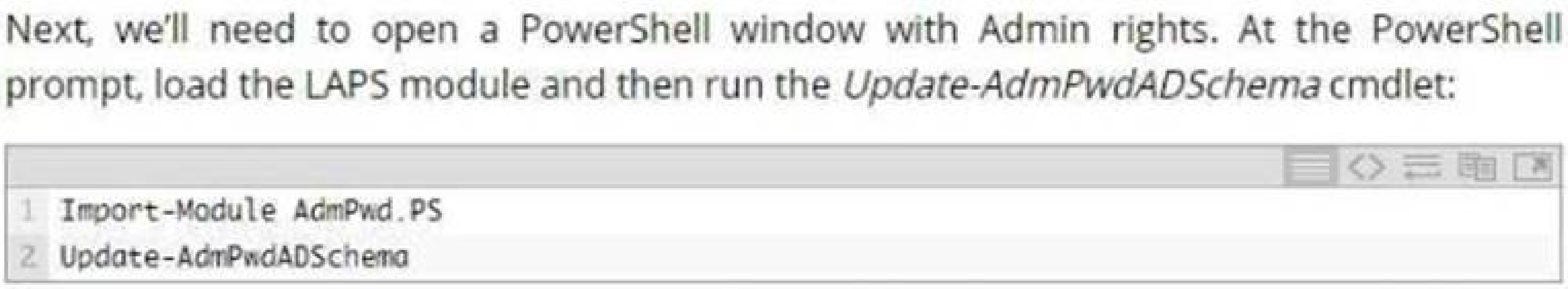
Windows PowerShell module to import:
AdmPwd.PS
Microsoft.WSMan.Management
NetSecurity
PSWorkFlow

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

A. Mastered
B. Not Mastered

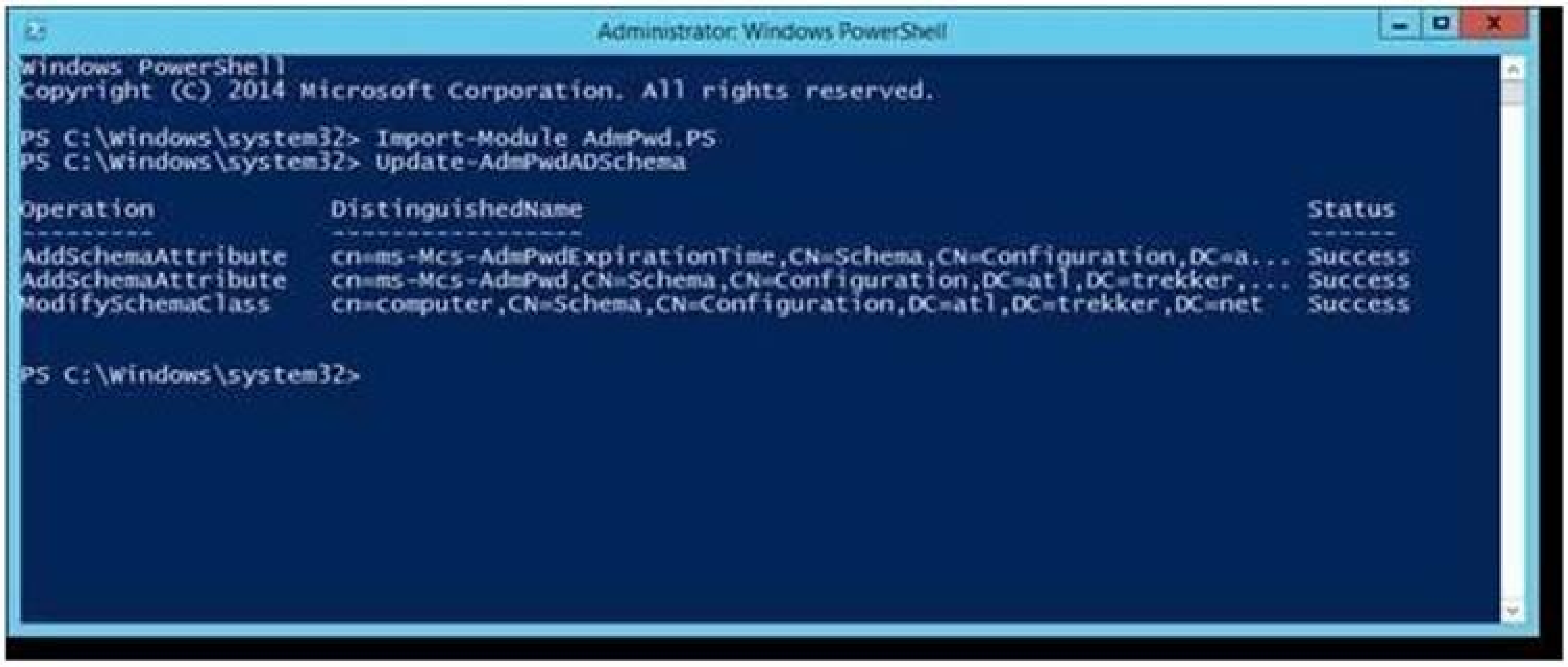
Answer: A

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



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

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



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

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

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


PS C:\Windows\system32>
```

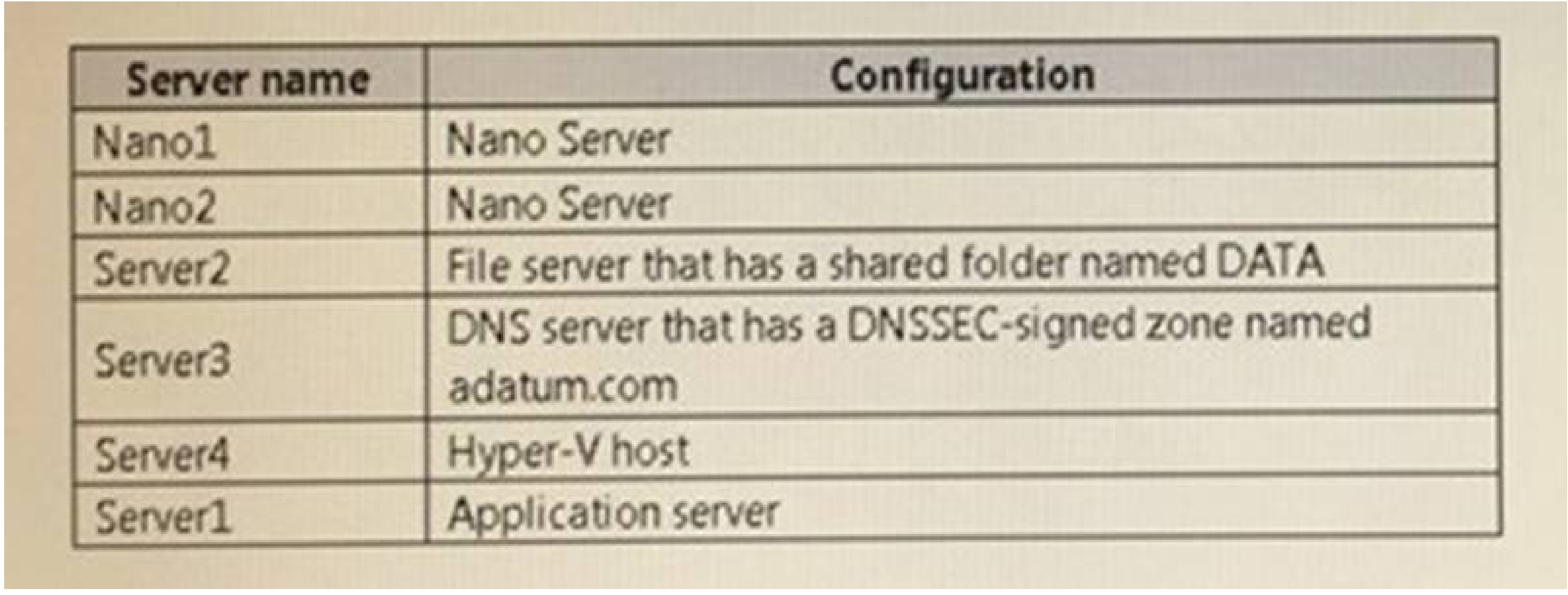
NEW QUESTION 32

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario

Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.

The domain contains the servers configured as shown in the following table.



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

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

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

End of repeated scenario

You need to ensure that the marketing department computers validate DNS responses from adatum.com.

Which setting should you configure in the Computer Configuration node of GP1?

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

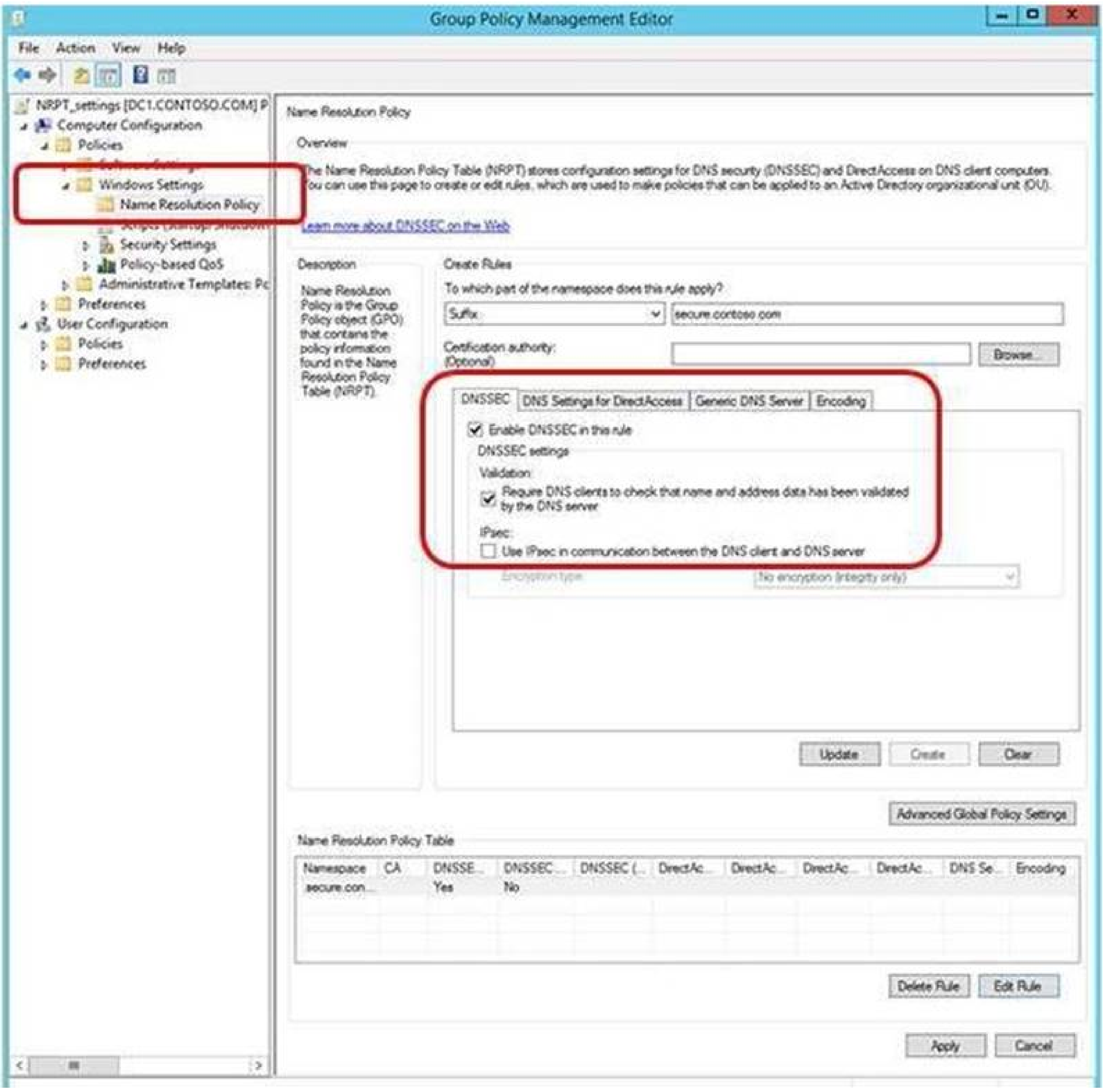
Answer: D

Explanation:

The NRPT is a table that contains rules that you can configure to specify DNS settings or special behavior for names or namespaces.

The NRPT can be configured using the Group Policy Management Editor under Computer Configuration \\Policies\\Windows Settings\\Name Resolution Policy, or with Windows PowerShell.

If a DNS query matches an entry in the NRPT, it is handled according to settings in the policy. Queries that do not match an NRPT entry are processed normally. You can use the NRPT to require that DNSSEC validation is performed on DNS responses for queries in the namespaces that you specify.



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

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

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

Certification authority: (Optional)

☑ Enable DNSSEC in this rule

DNSSEC settings

Validation:

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

IPsec:

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

Encryption type: No encryption (integrity only)

Name Resolution Policy Table

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

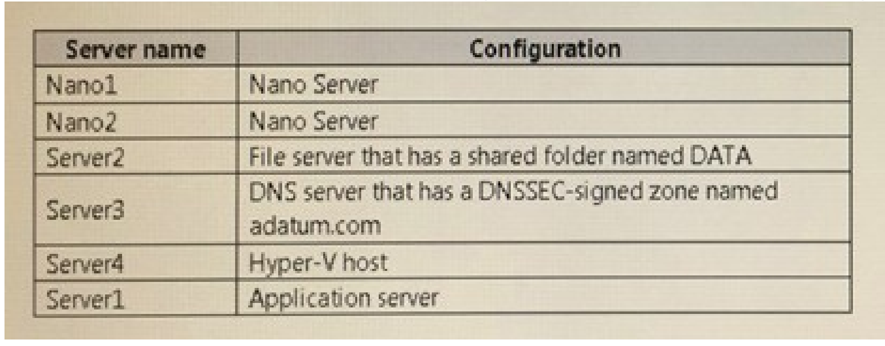
NEW QUESTION 37

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario b repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario

Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.

The domain contains the servers configured as shown m the following table.



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

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

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

End of repeated scenario

You need to disable SMB 1.0 on Server2. What should you do?

A. From File Server Resource Manager, create a classification rule.

B. From the properties of each network adapter on Server2. modify the bindings.

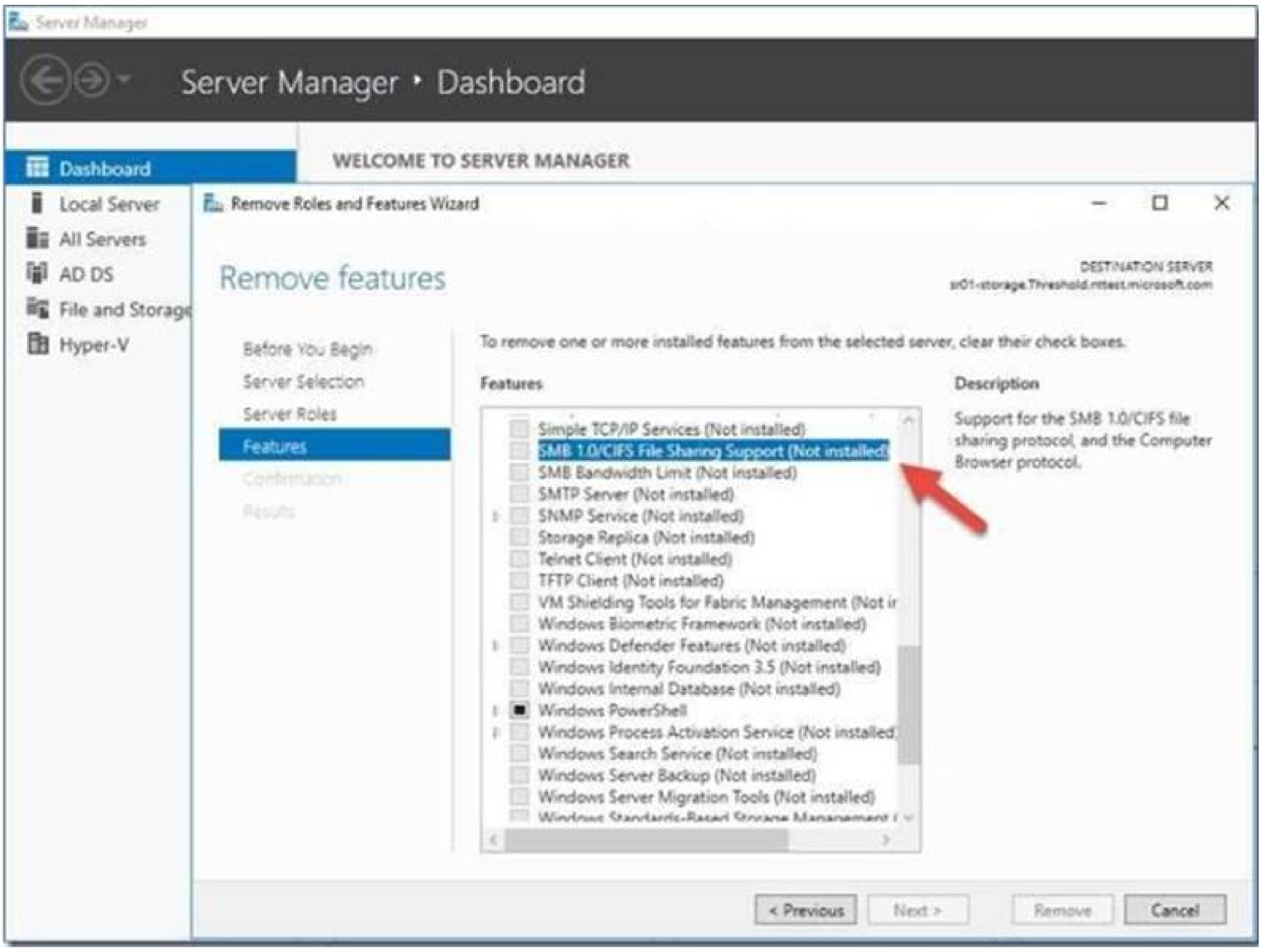
C. From Windows PowerShell, run the Set -SmbClientConfiguration cmdlet.

D. From Server Manager, remove a Windows feature.

Answer: D

Explanation:

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



Remove features

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

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

Features

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

Description

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

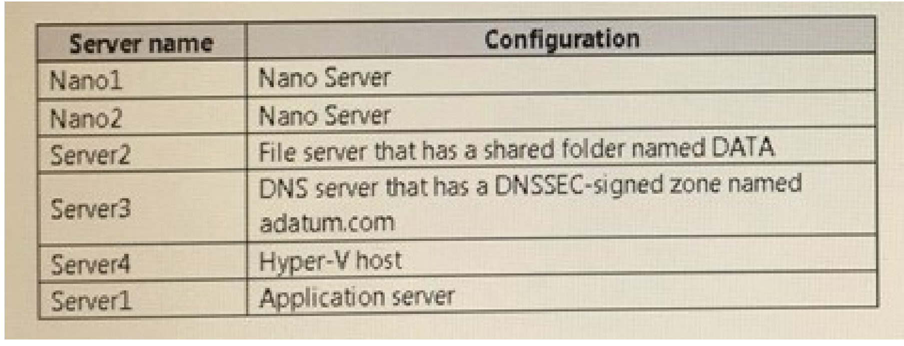
NEW QUESTION 40

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)

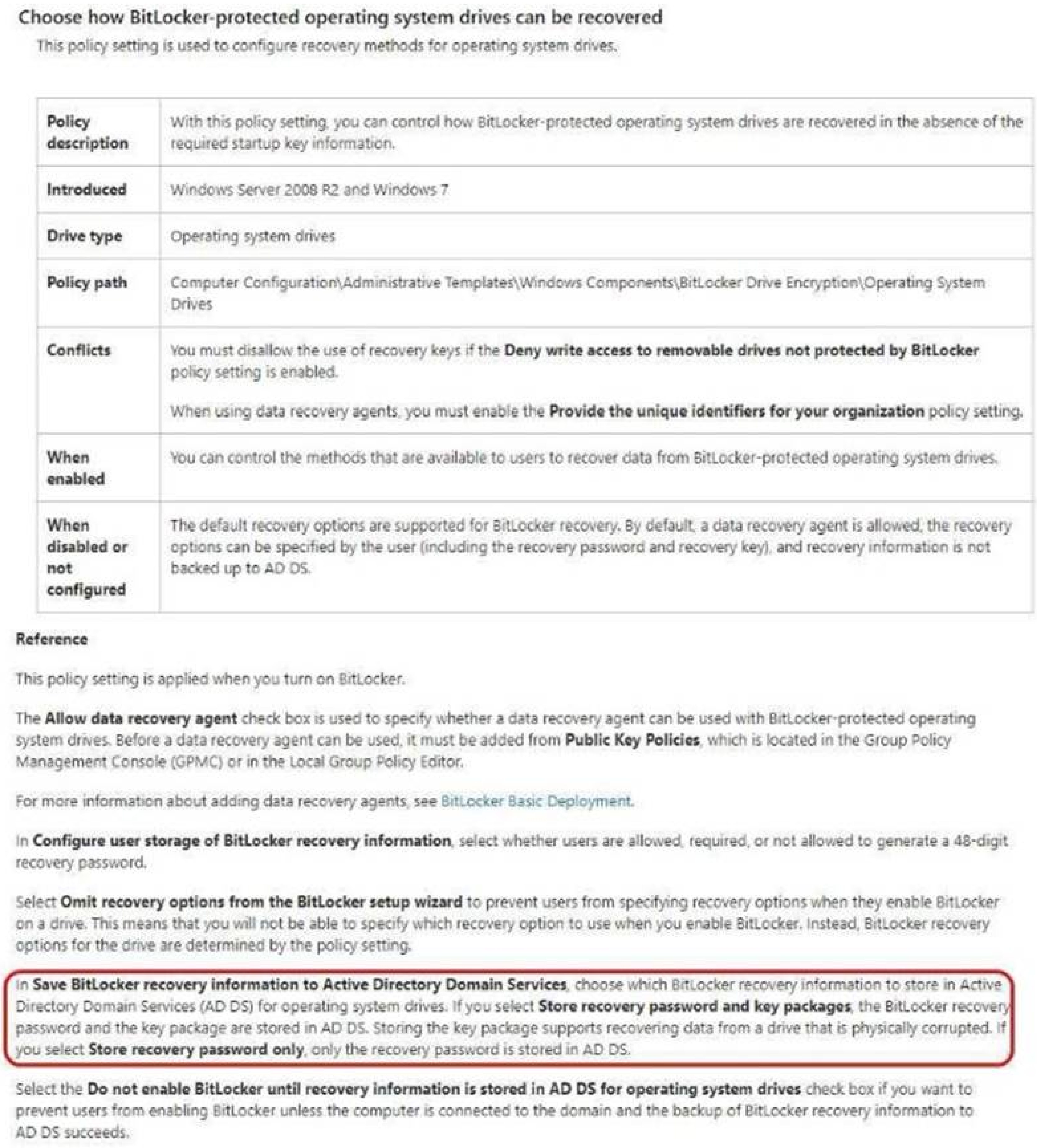
C. System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing

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.

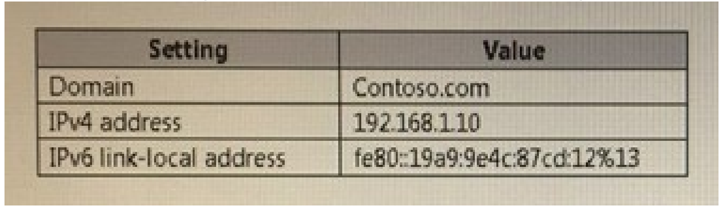
In **Configure user storage of BitLocker recovery information**, select whether users are allowed, required, or not allowed to generate a 48-digit recovery password.

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 43
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1.
Server1 is configured as shown in the following table.



Setting	Value
Domain	Contoso.com
IPv4 address	192.168.1.10
IPv6 link-local address	fe80::19a9:9e4c:87cd:12%13

You plan to create a pilot deployment of Microsoft Advanced Threat Analytics (ATA). You need to install the ATA Center on Server1.
What should you do first?

A. Install Microsoft Security Compliance Manager (SCM).
B. Obtain an SSL certificate.
C. Assign an additional IPv4 address.
D. Remove Server1 from the domai

Answer: B

Explanation:
https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-prerequisites
ATA Center which is the first component to be deployed on Server1, requires the use of SSL protocol to communicate with ATA Gateway
To ease the installation of ATA, you can install self-signed certificates during installation.
Post deployment you should replace the self-signed with a certificate from an internal Certification Authority tobe used by the ATA Center.
Make sure the ATA Center and ATA Gateways have access to your CRL distribution point.
If the they don’t have Internet access, follow the procedure to manually import a CRL, taking care to install the all the CRL distribution points for the whole chain.

NEW QUESTION 44
Your network contains an Active Directory domain named contoso.com The domain contains five file servers that run Windows Server 2016.
You have an organizational unit (OU) named Finance that contains all of the servers. You create a Group Policy object (GPO) and link the GPO to the Finance OU.
You need to ensure that when a user in the finance department deletes a file from a file server, the event is logged. The solution must log only users who have a manager attribute of Ben Smith. Which audit policy setting should you configure in the GPO?

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

Answer: C

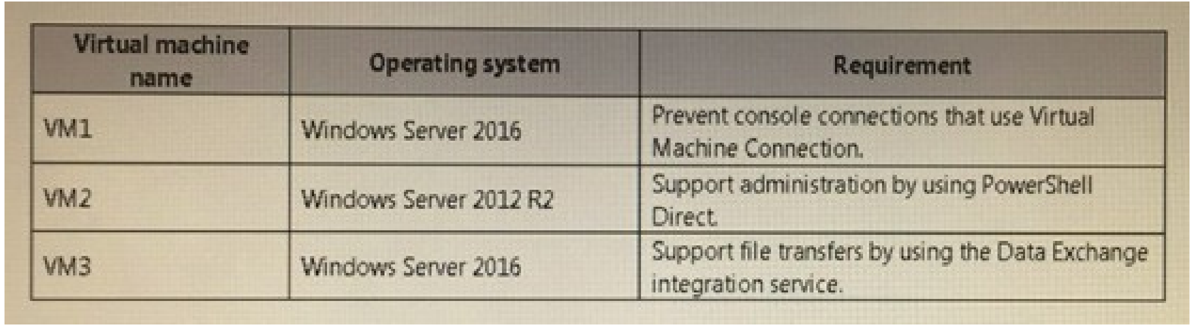
NEW QUESTION 49
Your network contains an Active Directory forest named conloso.com. The network is connected to the Internet.
You have 100 point-of-sale (POS) devices that run Windows 10. The devices cannot access the Internet.
You deploy Microsoft Operations Management Suite (OMS).
You need to use OMS to collect and analyze data from the POS devices. What should you do first?

A. Deploy Windows Server Gateway to the network.
B. Install the OMS Log Analytics Forwarder on the network.
C. Install Microsoft Data Management Gateway on the network.
D. Install the Simple Network Management Protocol (SNMP) feature on the devices.
E. Add the Microsoft NDJS Capture service to the network adapter of the devices.

Answer: B

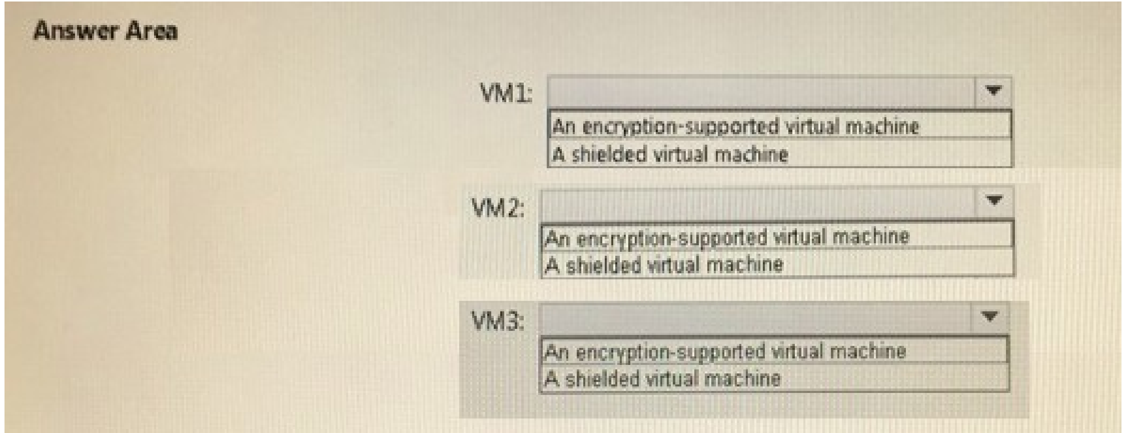
Explanation:
https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-oms-gateway OMS Log Analytics Forwarder = OMS Gateway
If your IT security policies do not allow computers on your network to connect to the Internet, such as point of sale (POS) devices, or servers supporting IT services,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

NEW QUESTION 52
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

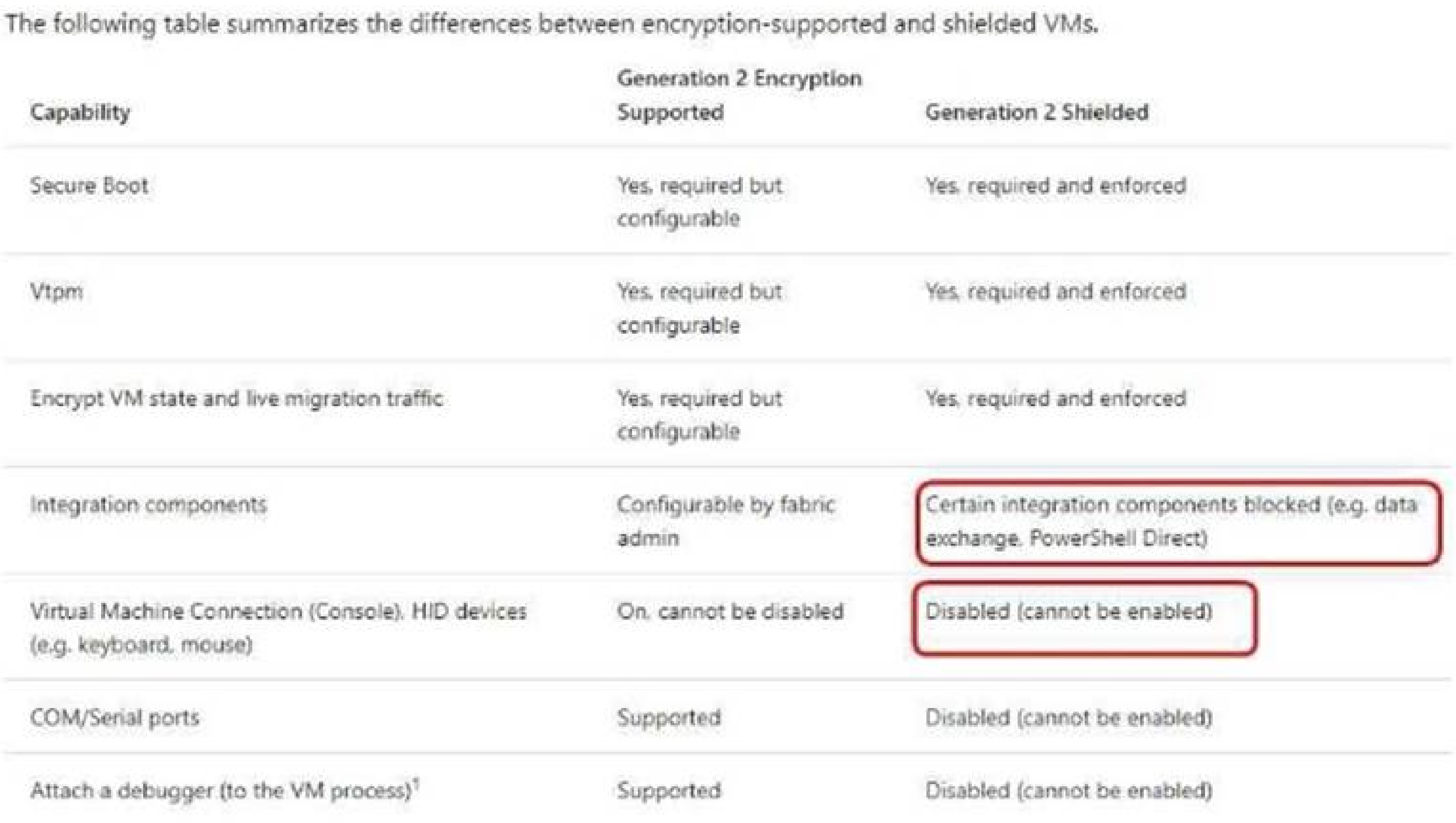
VM2: ▼
An encryption-supported virtual machine
A shielded virtual machine

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 53

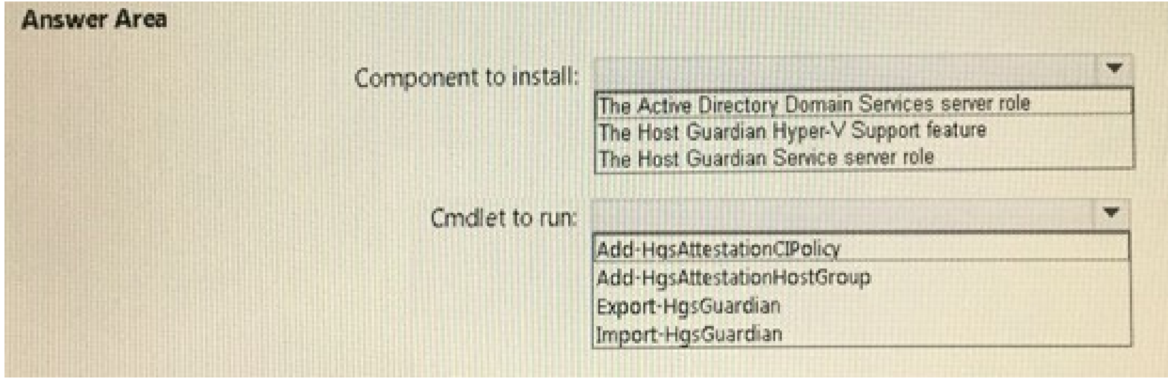
HOTSPOT

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

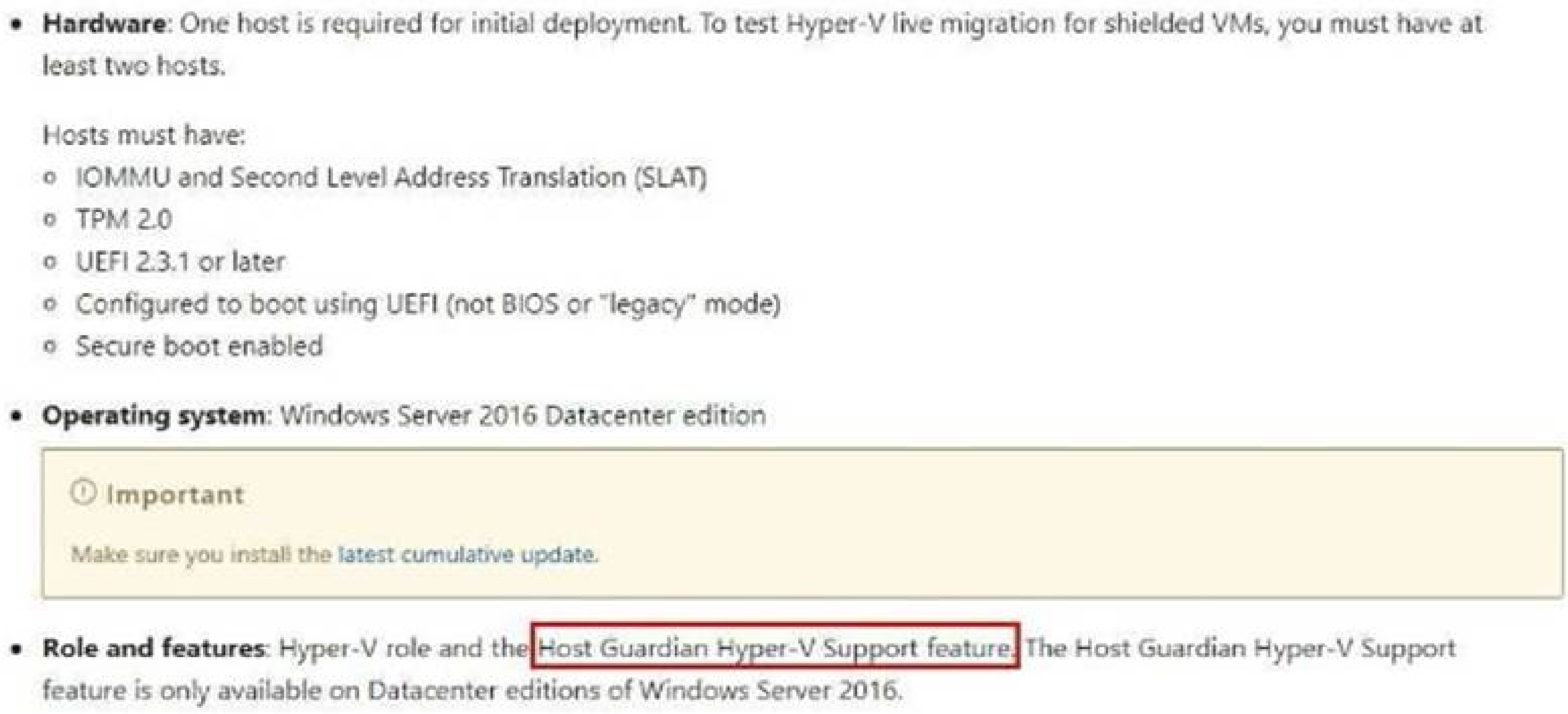
A. Mastered

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.

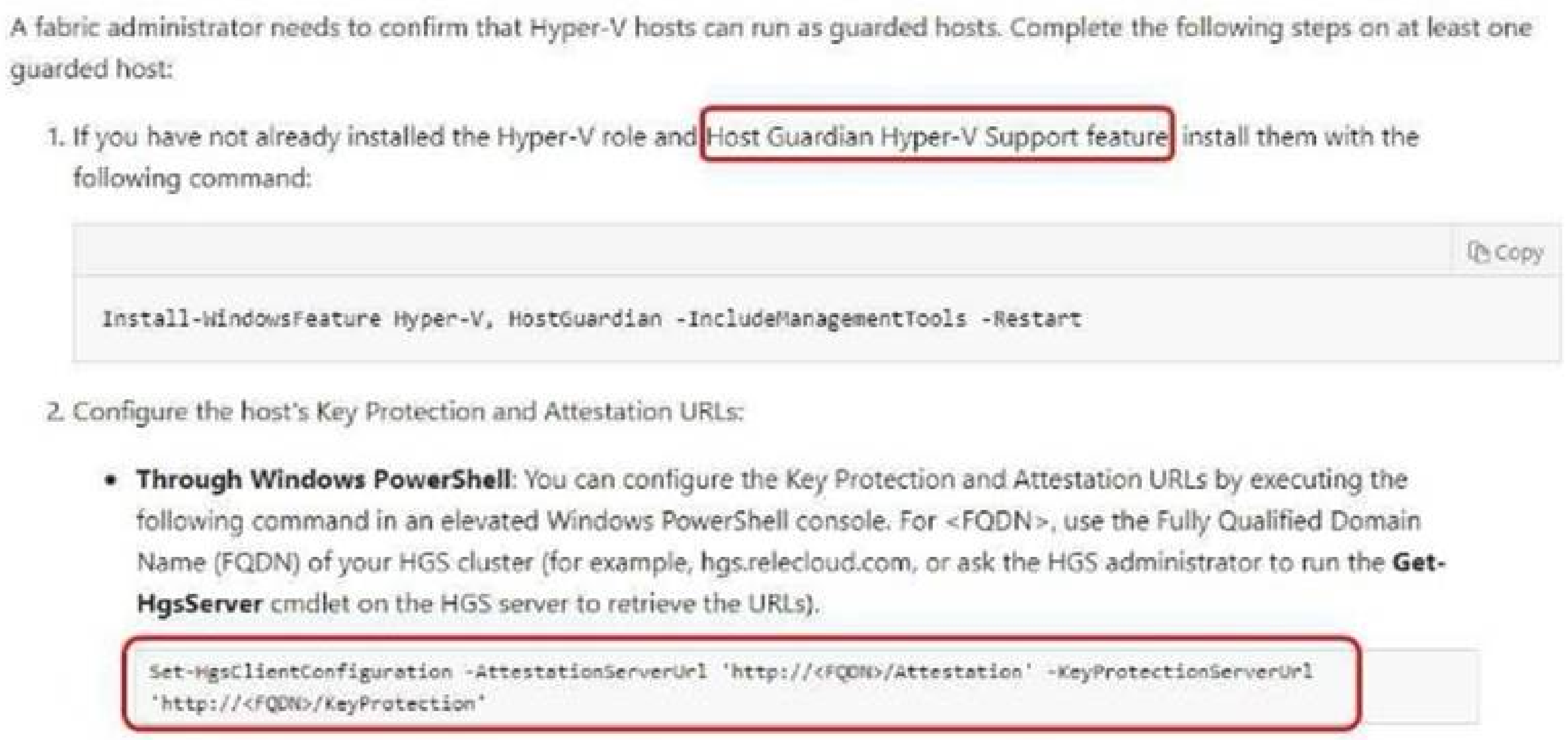


- **Hardware**: One host is required for initial deployment. To test Hyper-V live migration for shielded VMs, you must have at least two hosts.

  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 57
Windows PowerShell is a task-based command-line shell and scripting language designed especially for system administration.
Windows Defender comes with a number of different Defender-specific cmdlets that you can run through PowerShell to automate common tasks.
Which Cmdlet would you run first if you wanted to perform an offline scan?

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

Answer: A

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

NEW QUESTION 58
____ enables easier management for BitLocker enabled desktops and servers in a domain environment by providing automatic unlock of operating system volumes at system reboot when connected to a wired corporate network. This feature requires the client hardware to have a DHCP driver implemented in its UEFI firmware.

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

Answer: A

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

NEW QUESTION 59
The “Network Security: Restrict NTLM: NTLM authentication in this domain” policy setting allows you to deny or allow NTLM authentication within a domain from this domain controller.
Which value would you choose so that the domain controller will deny all NTLM authentication logon attempts using accounts from this domain to all servers in the domain.
The NTLM authentication attempts will be blocked and will return an NTLM blocked error unless the server name is on the exception list in the Network security: Restrict NTLM: Add server exceptions in this domain policy setting.

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

Answer: B

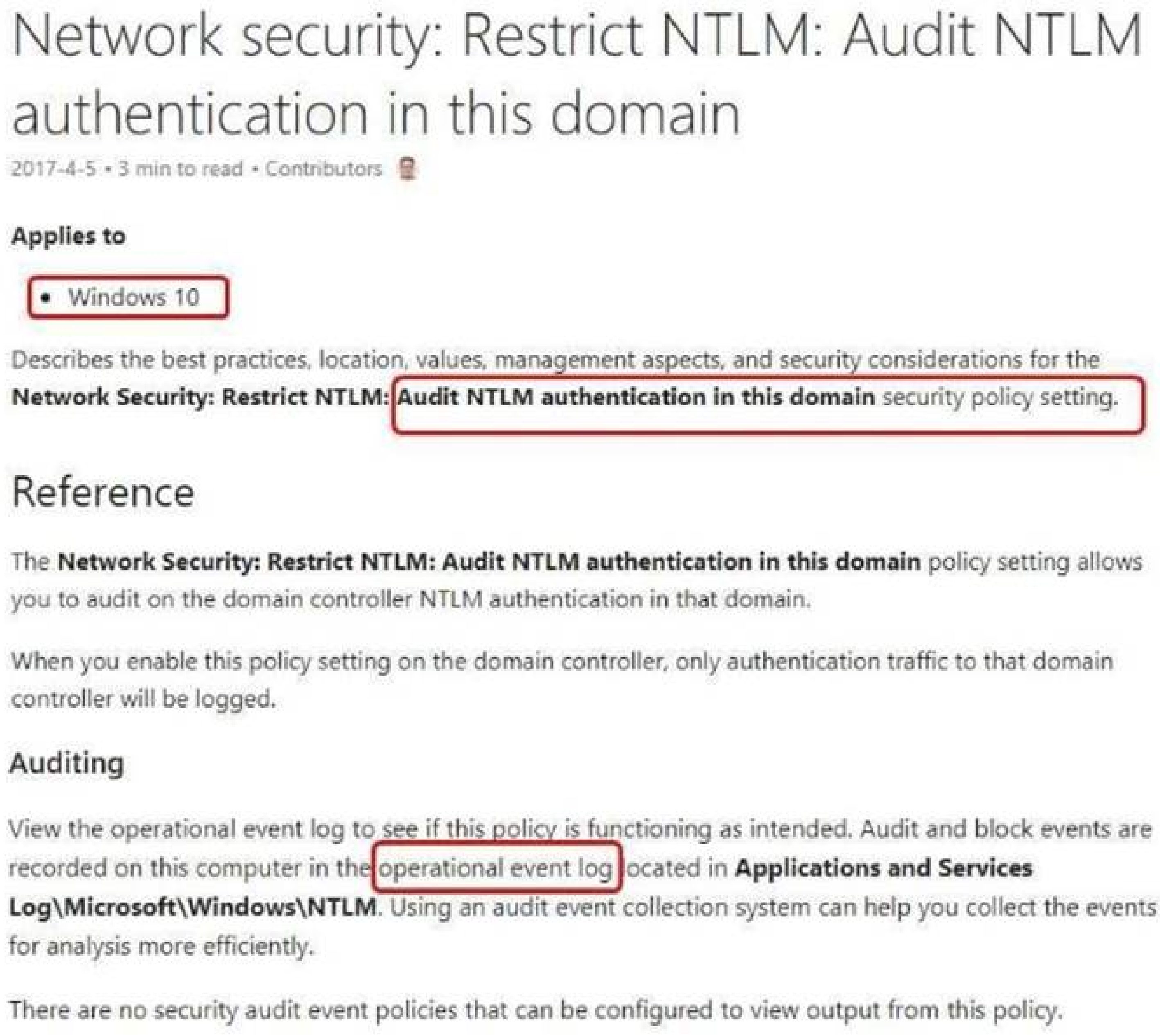
NEW QUESTION 64
Your network contains an Active Directory domain named contoso.com. The domain contains multiple servers that run multiple applications.
Domain user accounts are used to authenticate access requests to the servers. You plan to prevent NTLM from being used to authenticate to the servers. You start to audit NTLM authentication events for the domain.
You need to view all of the NTLM authentication events and to identify which applications authenticate by using NTLM.
On which computers should you review the event logs and which logs should you review?

A. Computers on which to review the event logs: Only client computers

B. Computers on which to review the event logs: Only domain controllers
C. Computers on which to review the event logs: Only member servers
D. Event logs to review: Applications and Services Logs\\Microsoft\\Windows\\Diagnostics- Networking\\Operational
E. Event logs to review: Applications and Services Logs\\Microsoft\\Windows\\NTLM\\Operational
F. Event logs to review: Applications and Services Logs\\Microsoft\\Windows\\SMBClient\\Security
G. Event logs to review: Windows Logs\\Security
H. Event logs to review: Windows Logs\\System

Answer: AE

Explanation:
Do not confuse this with event ID 4776 recorded on domain controller's security event log!!!
This question asks for implementing NTLM auditing when domain clients is connecting to member servers! See below for further information.
https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/networksecurity- restrict-ntlmaudit-ntlm-authentication-in-this-domain
Via lab testing, most of the NTLM audit logs are created on Windows 10 clients, except that you use Windows
Server 2016 OS as clients (but this is unusual)



Network security: Restrict NTLM: Audit NTLM authentication in this domain

2017-4-5 • 3 min to read • Contributors

Applies to

- Windows 10

Describes the best practices, location, values, management aspects, and security considerations for the **Network Security: Restrict NTLM: Audit NTLM authentication in this domain** security policy setting.

Reference

The **Network Security: Restrict NTLM: Audit NTLM authentication in this domain** policy setting allows you to audit on the domain controller NTLM authentication in that domain.

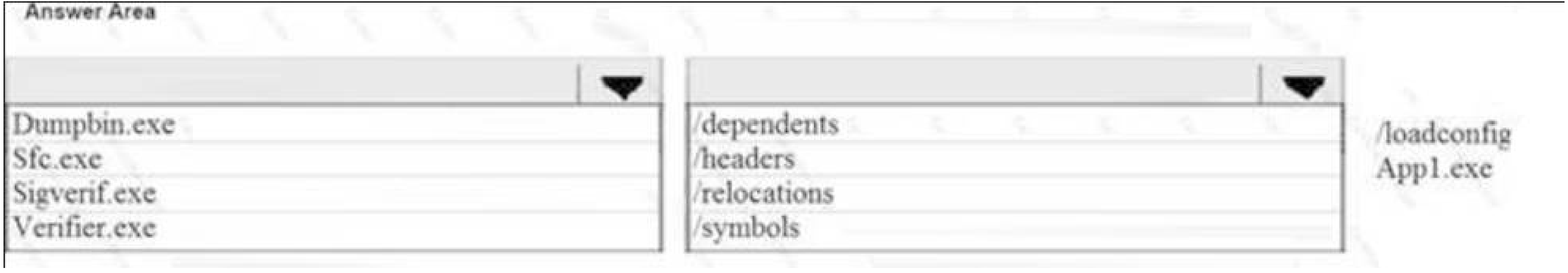
When you enable this policy setting on the domain controller, only authentication traffic to that domain controller will be logged.

Auditing

View the operational event log to see if this policy is functioning as intended. Audit and block events are recorded on this computer in the operational event log located in **Applications and Services Log\Microsoft\Windows\NTLM**. Using an audit event collection system can help you collect the events for analysis more efficiently.

There are no security audit event policies that can be configured to view output from this policy.

NEW QUESTION 65
HOTSPOT
Your network contains an Active Directory domain named contoso.com. You plan to deploy an application named App1.exe.
You need to verify whether Control Flow Guard is enabled for App1.exe.
Which command should you run? To answer, select the appropriate options in the answer area.



Answer Area

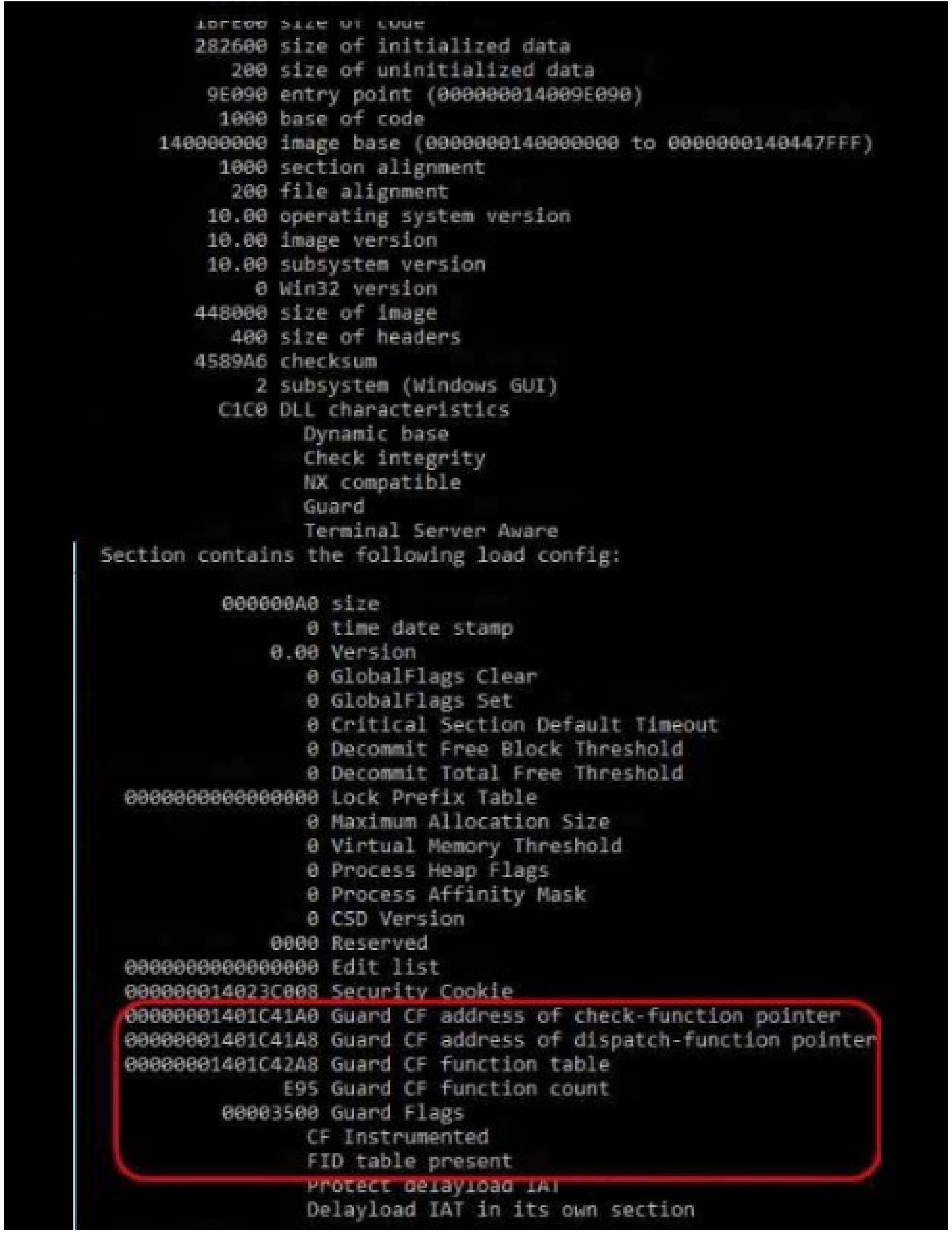
Dumpbin.exe Sfc.exe Sigverif.exe Verifier.exe	/dependents /headers /relocations /symbols	/loadconfig App1.exe

A. Mastered
B. Not Mastered

Answer: A

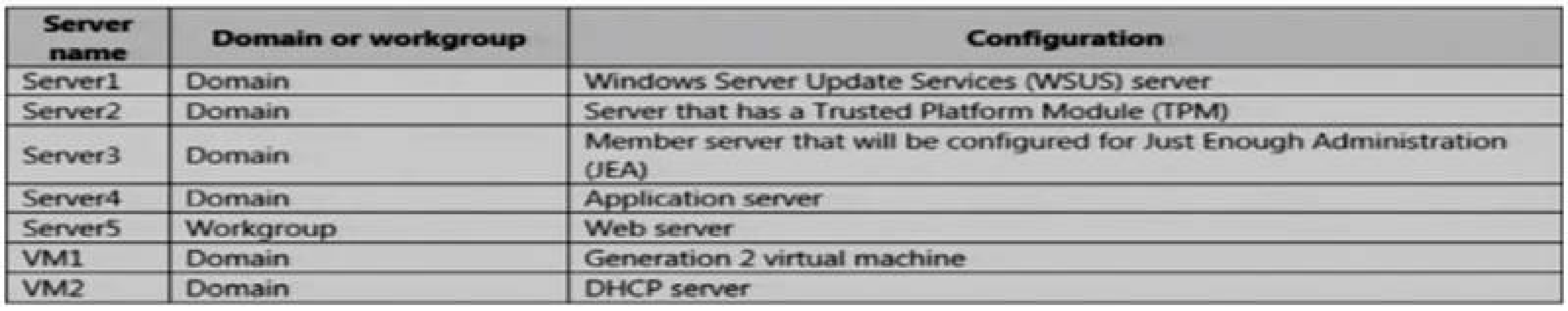
Explanation:
https://msdn.microsoft.com/en-us/library/windows/desktop/mt637065(v=vs.85).aspx
Control Flow Guard (CFG) is a highly-optimized platform security feature that was created to combat memory corruption vulnerabilities.
By placing tight restrictions on where an application can execute code from, it makes it much harder for explogts to execute arbitrary code through vulnerabilities such as buffer overflows.To verify if Control Flow Guard is enable for a certain application executable:-
Run the dumpbin.exe tool (included in the Visual Studio 2015 installation) from the Visual Studio command

prompt with the /headers and /loadconfig options: dumpbin.exe /headers /loadconfig test.exe.
The output for a binary under CFG should show that the header values include “Guard”, and that the load
config values include “CF Instrumented” and “FID table present”.1



```
          1BFE00 size of code
          282600 size of initialized data
             200 size of uninitialized data
           9E090 entry point (000000014009E090)
            1000 base of code
       140000000 image base (0000000140000000 to 0000000140447FFF)
            1000 section alignment
             200 file alignment
           10.00 operating system version
           10.00 image version
           10.00 subsystem version
               0 Win32 version
          448000 size of image
             400 size of headers
          4589A6 checksum
               2 subsystem (Windows GUI)
            C1C0 DLL characteristics
                   Dynamic base
                   Check integrity
                   NX compatible
                   Guard
                   Terminal Server Aware
 Section contains the following load config:

          000000A0 size
                 0 time date stamp
              0.00 Version
                 0 GlobalFlags Clear
                 0 GlobalFlags Set
                 0 Critical Section Default Timeout
                 0 Decommit Free Block Threshold
                 0 Decommit Total Free Threshold
  0000000000000000 Lock Prefix Table
                 0 Maximum Allocation Size
                 0 Virtual Memory Threshold
                 0 Process Heap Flags
                 0 Process Affinity Mask
                 0 CSD Version
              0000 Reserved
  0000000000000000 Edit list
  000000014023C008 Security Cookie
  00000001401C41A0 Guard CF address of check-function pointer
  00000001401C41A8 Guard CF address of dispatch-function pointer
  00000001401C42A8 Guard CF function table
               E95 Guard CF function count
          00003500 Guard Flags
                     CF Instrumented
                     FID table present
                     Protect delayload IAT
                     Delayload IAT in its own section
```

NEW QUESTION 68
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.



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

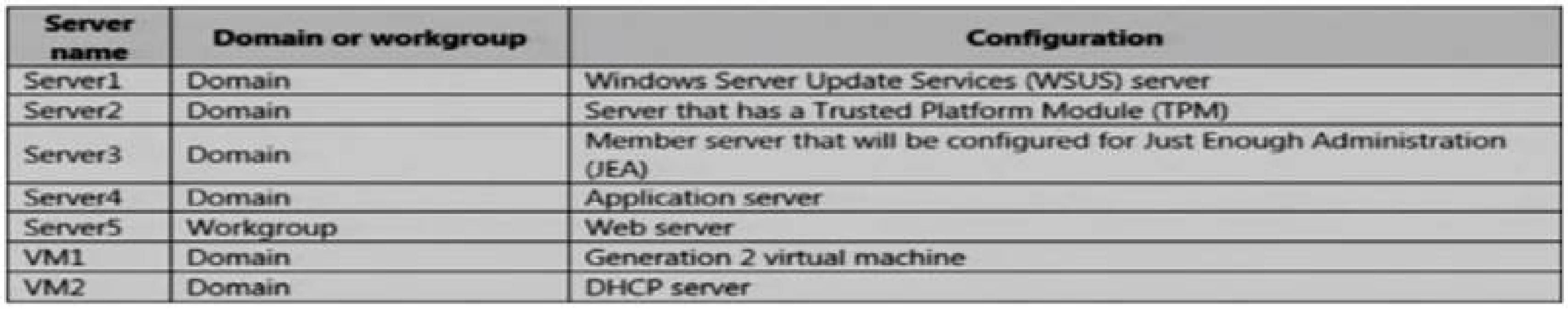
All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.
All laptops are protected by using BitLocker Drive Encryption (BitLocker).
You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.
An OU named OU2 contains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

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

Answer: A

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

NEW QUESTION 73
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.



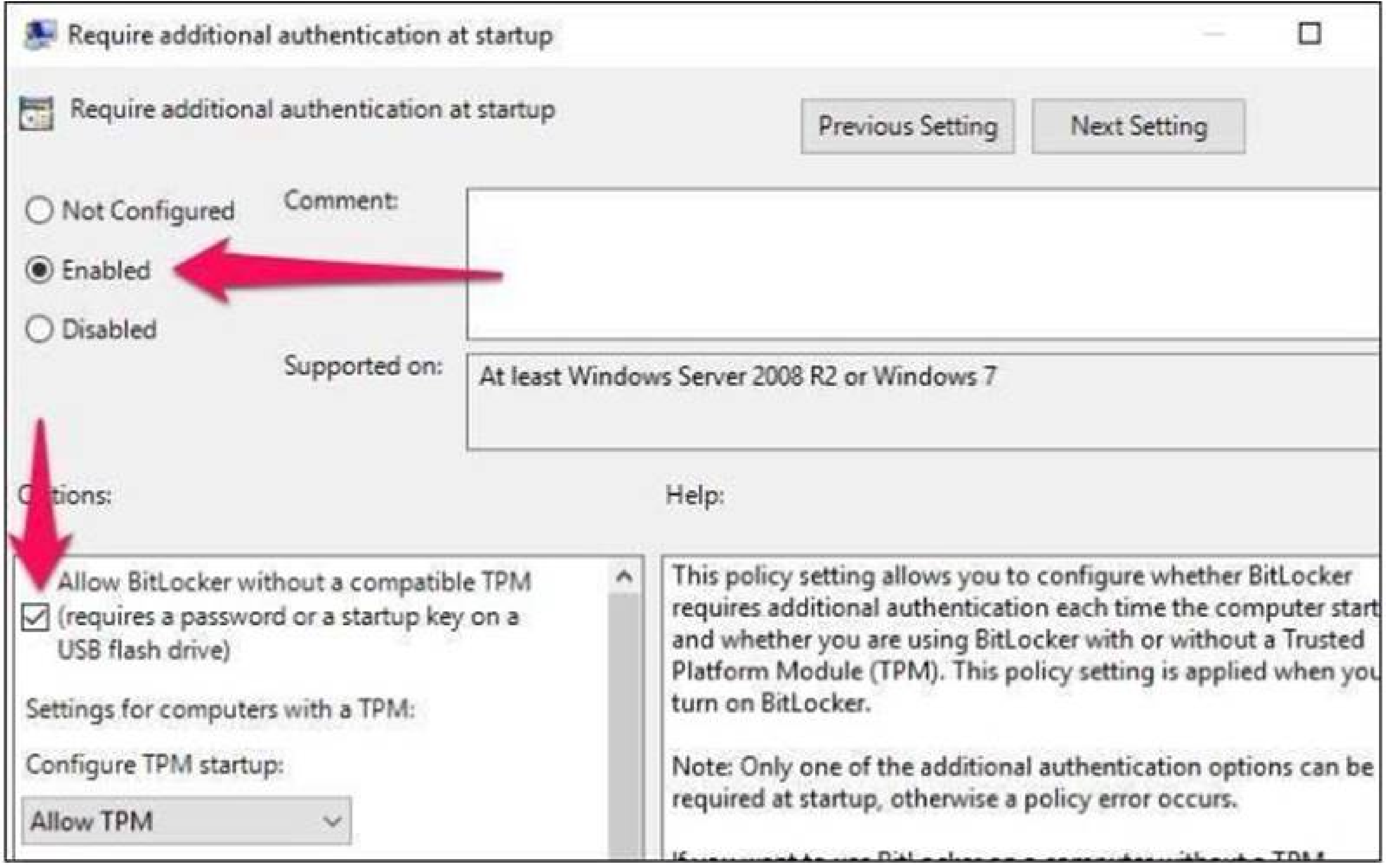
Server name	Domain or workgroup	Configuration
Server1	Domain	Windows Server Update Services (WSUS) server
Server2	Domain	Server that has a Trusted Platform Module (TPM)
Server3	Domain	Member server that will be configured for Just Enough Administration (JEA)
Server4	Domain	Application server
Server5	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 75
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

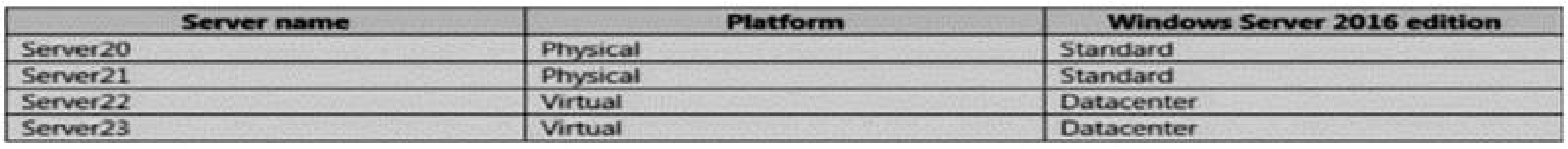
Answer: AE

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 78

Your data center contains 10 Hyper-V hosts that host 100 virtual machines.
You plan to secure access to the virtual machines by using the Datacenter Firewall service.
You have four servers available for the Datacenter Firewall service. The servers are configured as shown in the following table.



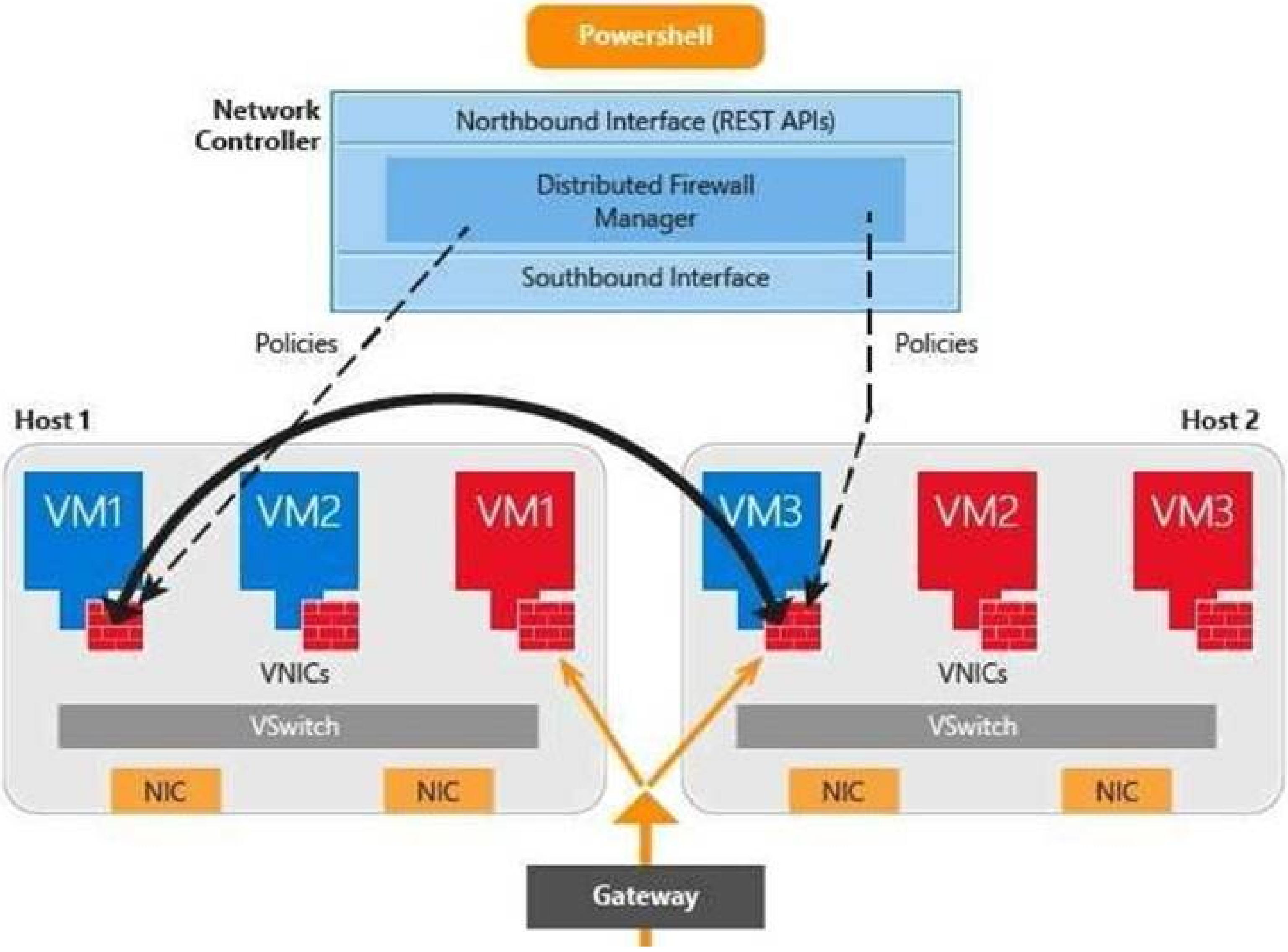
Server name	Platform	Windows Server 2016 edition
Server20	Physical	Standard
Server21	Physical	Standard
Server22	Virtual	Datacenter
Server23	Virtual	Datacenter

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

A. Server role to deploy: Multipoint Services
B. Server role to deploy: Network Controller
C. Server role to deploy: Network Policy and Access Services
D. Servers on which to deploy the server role: Server20 and Server21
E. Servers on which to deploy the server role: Server22 and Server23

Answer: BE

Explanation:
Datacenter Firewall is a new service included with Windows Server 2016. It is a network layer, 5- tuple (protocol, source and destination port numbers, source and destination IP addresses), stateful, multitenant firewall. When deployed and offered as a service by the serviceprovider, tenant administrators can install and configure firewall policies to help protect their virtual networks from unwanted traffic originating from Internet and intranet networks.
https://docs.microsoft.com/en-us/windows-server/networking/sdn/technologies/networkcontroller/ networkcontroller
Network Controller Features
The following Network Controller features allow you to configure and manage virtual and physical network devices and services.
i) Firewall Management (Datacenter Firewall)
ii) Software Load Balancer Management
iii) Virtual Network Management
iv) RAS Gateway Management



https://docs.microsoft.com/en-us/windows-server/networking/sdn/plan/installation-andpreparationrequirements- for-deploying-network-controller
Installation requirements
Following are the installation requirements for Network Controller.
For Windows Server 2016 deployments, you can deploy Network Controller on one or more computers, one or more VMs, or a combination of computers and VMs.
All VMs and computers planned as Network Controller nodes must be running Windows Server 2016 Datacenter edition.

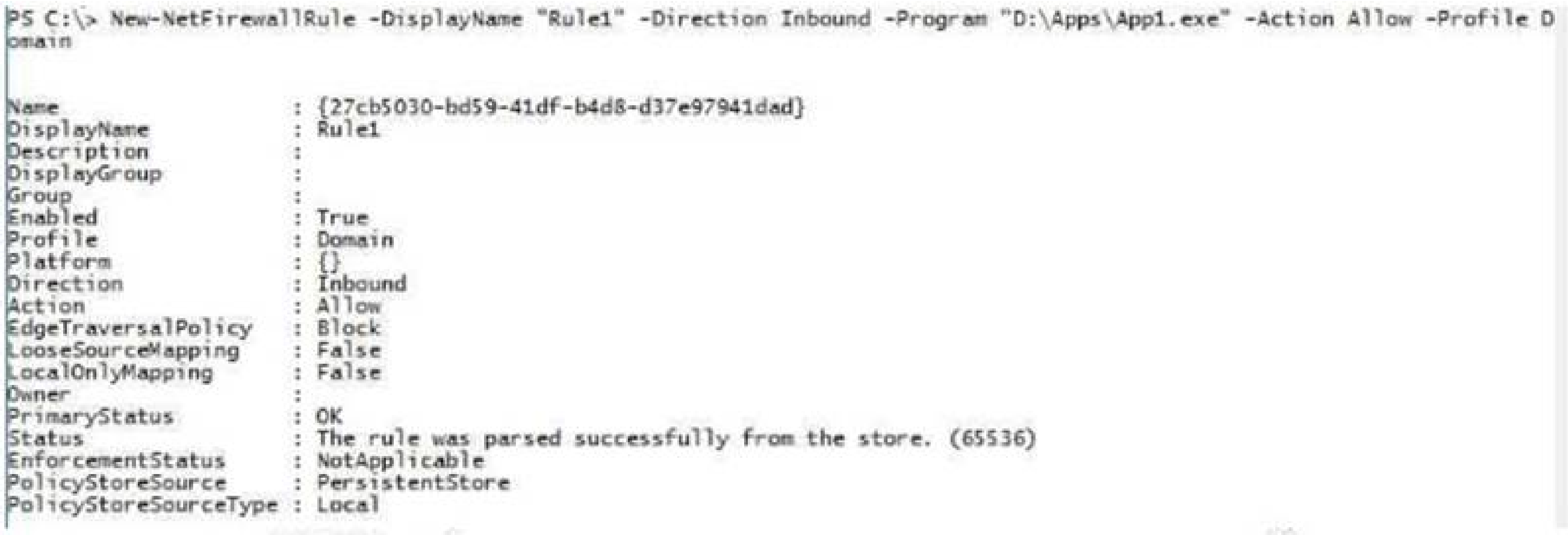
NEW QUESTION 80

Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. Computer1 connects to a home network and a corporate network.
The corporate network uses the 172.16.0.0/24 address space internally. Computer1 runs an application named App1 that listens to port 8080.
You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.
Solution: You run the command New-NetFirewallRule -DisplayName “Rule1” -Direction Inbound - Program “D:\\Apps\\App1.exe” –Action Allow -Profile Domain
Does this meet the goal?

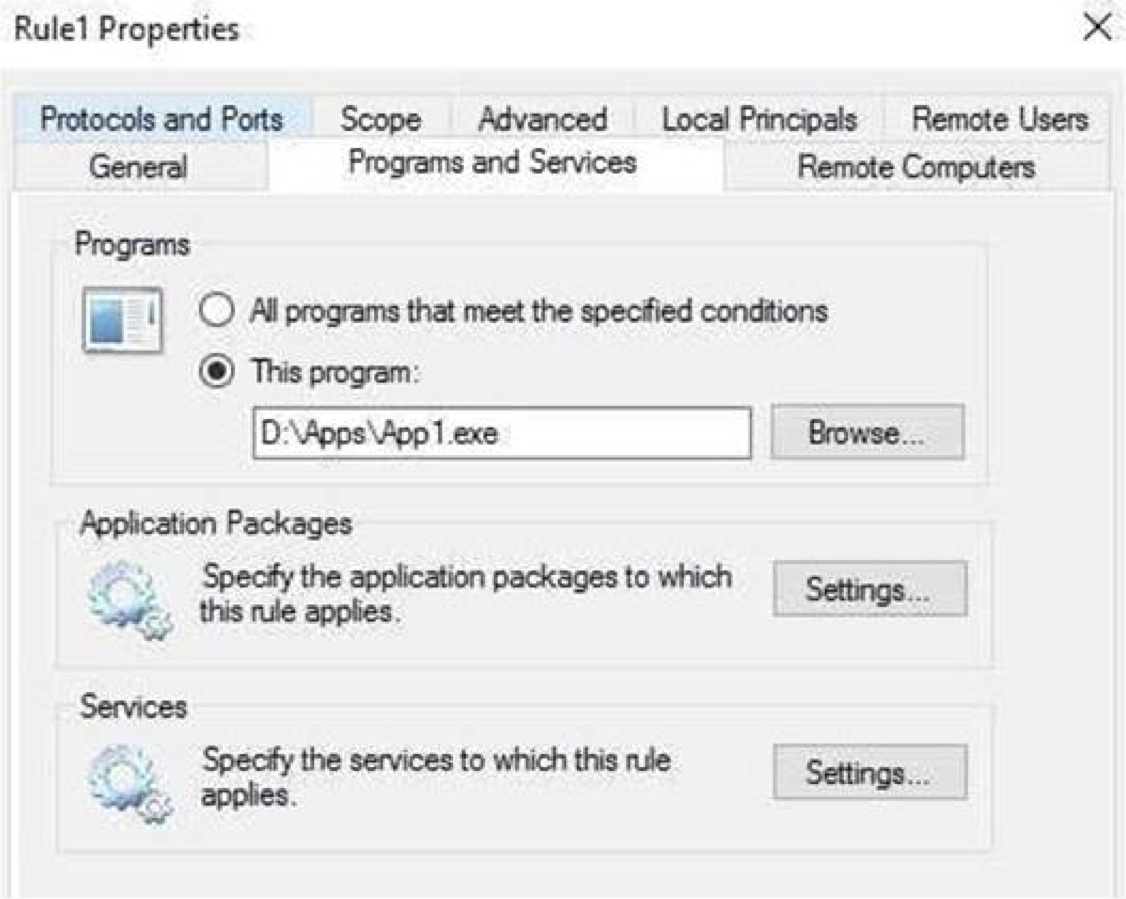
A. Yes
B. No

Answer: A

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



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


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



Rule1 Properties

Programs

○ All programs that meet the specified conditions

● This program:

D:\Apps\App1.exe

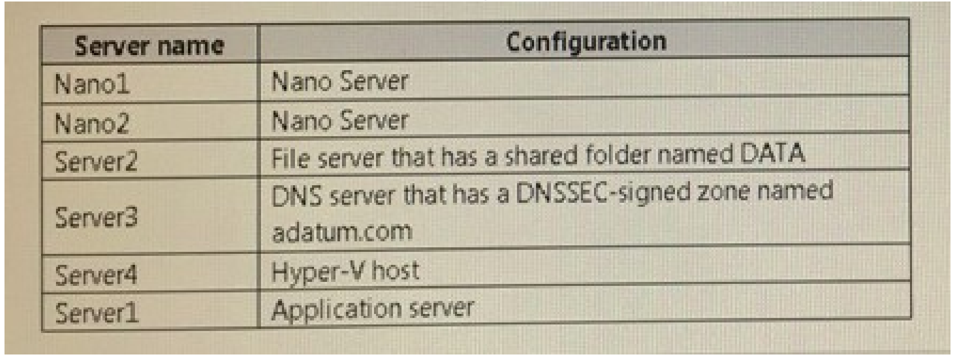
Application Packages

Specify the application packages to which this rule applies.

Services

Specify the services to which this rule applies.

NEW QUESTION 83
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.
Start of repeated scenario
Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.
The domain contains the servers configured as shown in the following table.



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

All servers run Windows Server 2016. All client computers run Windows 10.
You have an organizational unit (OU) named Marketing that contains the computers in the marketing department You have an OU named finance that contains the computers in the finance department You have an OU named AppServers that contains application servers. A Group Policy object (GPO) named GP1 is linked to the Marketing OU. A GPO named GP2 is linked to the AppServers OU. You install Windows Defender on Nano1.
End of repeated scenario
You need to ensure that when a configuration change is made on Nano2, Nano2 will revert back to the original configuration automatically.
What should you do first?

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

Answer: B

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

NEW QUESTION 84
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

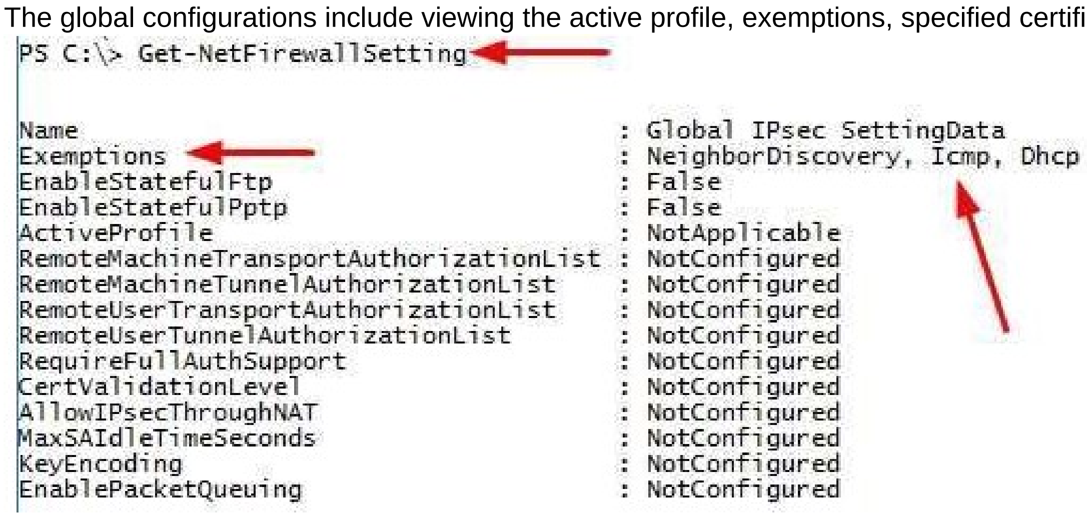
Explanation:
In IPsec connection security rule, the IPsec protocol verifies the sending host IP address by utilize integrity
functions like Digitally signing all packets.
If unsigned packets arrives Server11, those are possible source address spoofed packets, when using connection security rule in-conjunction 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 88
You have a server named Server1 that runs Windows Server 2016.
You need to identify whether ICMP traffic is exempt from IPsec 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: D

Explanation:
The Get-NetFirewallSetting cmdlet retrieves the global firewall settings of the target computer. The NetFirewallSetting object specifies properties that apply to the firewall and IPsec settings, no matter which
network profile is currently in use.
The global configurations include viewing the active profile, exemptions, specified certification validation levels, and user and computer authorization lists.



```
PS C:\> Get-NetFirewallSetting


Name                                  : Global IPsec SettingData
Exemptions                            : NeighborDiscovery, Icmp, Dhcp
EnableStatefulFtp                     : False
EnableStatefulPptp                    : False
ActiveProfile                         : NotApplicable
RemoteMachineTransportAuthorizationList : NotConfigured
RemoteMachineTunnelAuthorizationList  : NotConfigured
RemoteUserTransportAuthorizationList  : NotConfigured
RemoteUserTunnelAuthorizationList     : NotConfigured
RequireFullAuthSupport                : NotConfigured
CertValidationLevel                   : NotConfigured
AllowIPsecThroughNAT                  : NotConfigured
MaxSAIdleTimeSeconds                  : NotConfigured
KeyEncoding                           : NotConfigured
EnablePacketQueuing                   : NotConfigured
```

NEW QUESTION 92
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

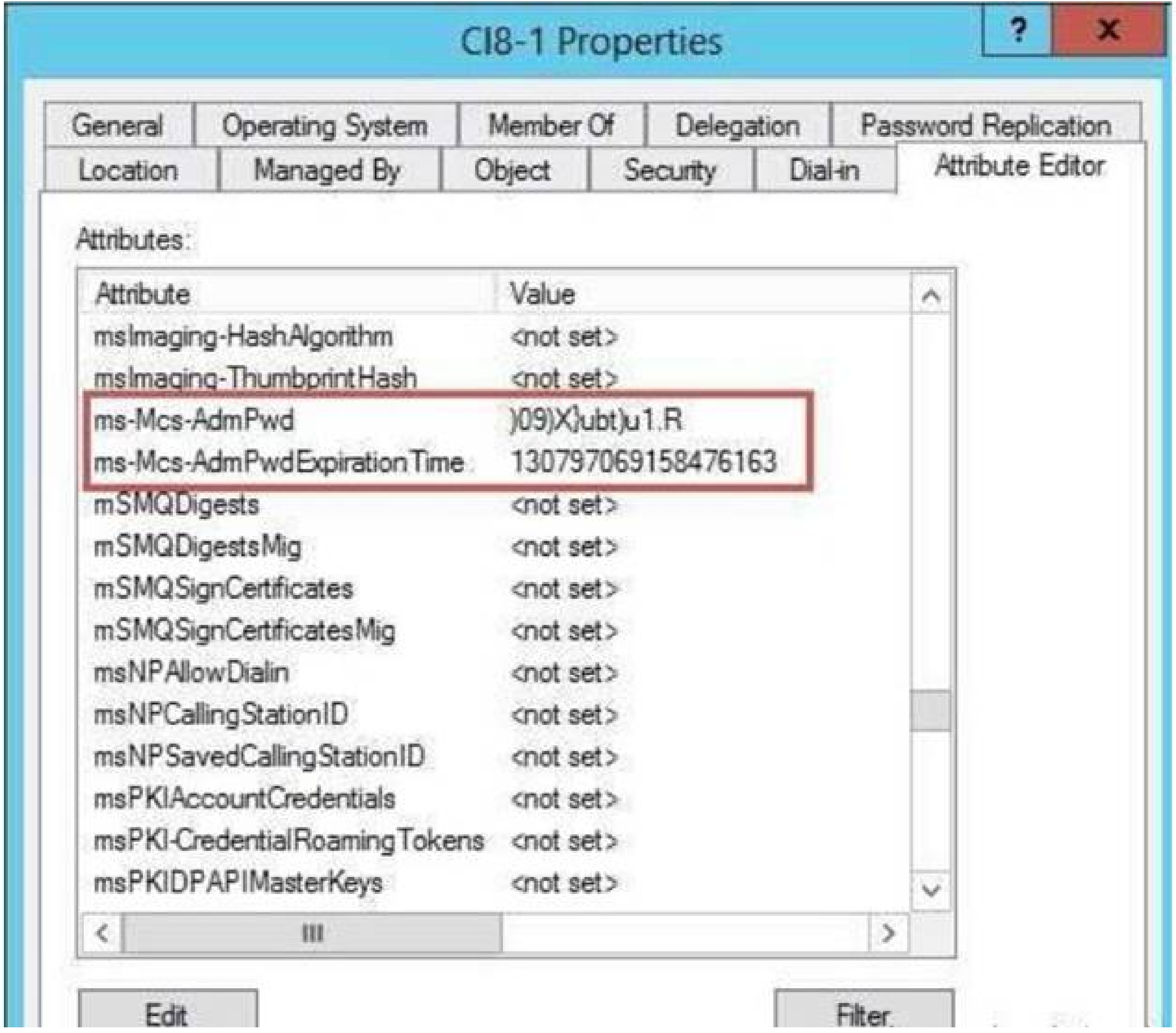
Explanation:
https://docs.microsoft.com/en-us/powershell/jea/role-capabilities https://docs.microsoft.com/en-us/powershell/jea/register-jea

NEW QUESTION 95
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 97
Your network contains an Active Directory domain named contoso.com. The domain contains 100 servers.
You deploy the Local Administrator Password Solution (LAPS) to the network You need to view the password of the local administrator of a server named Server5.
Which tool should you use?

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

Answer: A

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

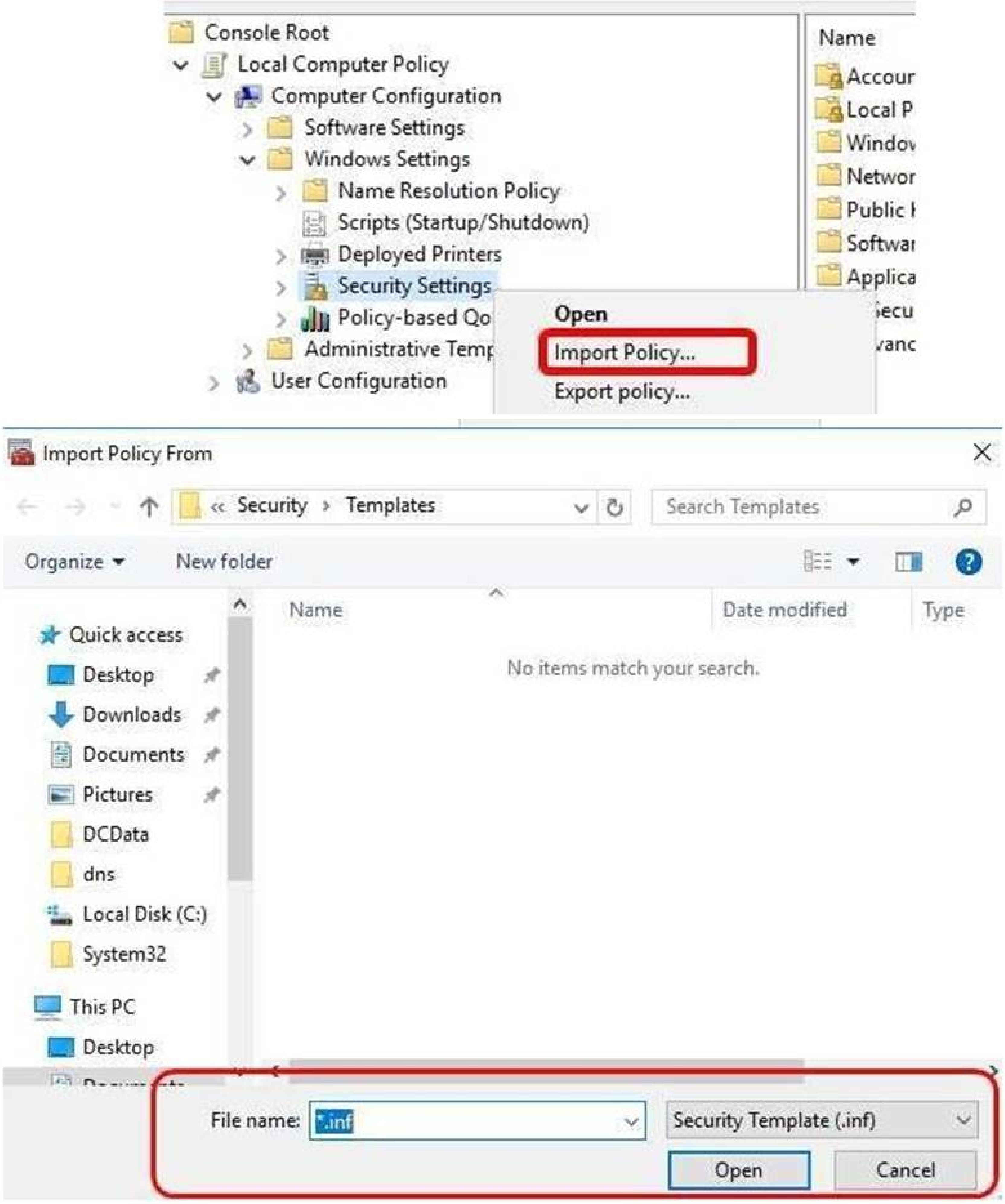
NEW QUESTION 100
Your network contains an internal network and a perimeter network. The internal network contains an Active Directory forest named contoso.com.
You deploy five servers to the perimeter network.

All of the servers run Windows Server 2016 and are the members of a workgroup.
You need to apply a security baseline named Perimeter.inf to the servers in the perimeter network. What should you use to apply Perimeter.inf?

A. Local Computer Policy
B. Security Configuration Wizard (SCW)
C. Group Policy Management
D. Server Manager

Answer: A

Explanation:
https://docs.microsoft.com/en-us/windows-server/get-started/deprecated-features https://blogs.technet.microsoft.com/secguide/2016/01/21/lgpo-exe-local-group-policy-objectutility- v1-0/
https://msdn.microsoft.com/en-us/library/bb742512.aspx



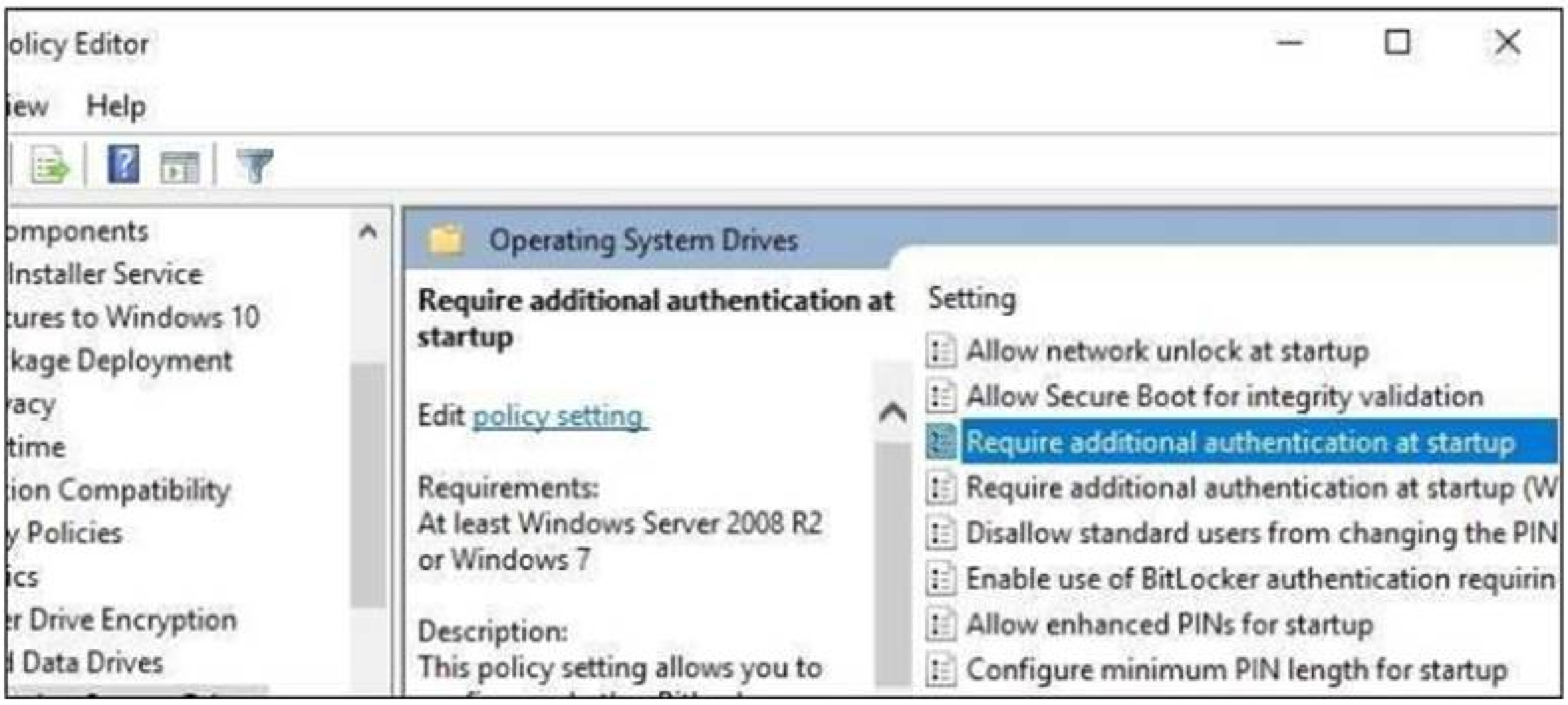
File name: *.inf
Security Template (.inf)

NEW QUESTION 101
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.


olicy Editor

iew Help

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

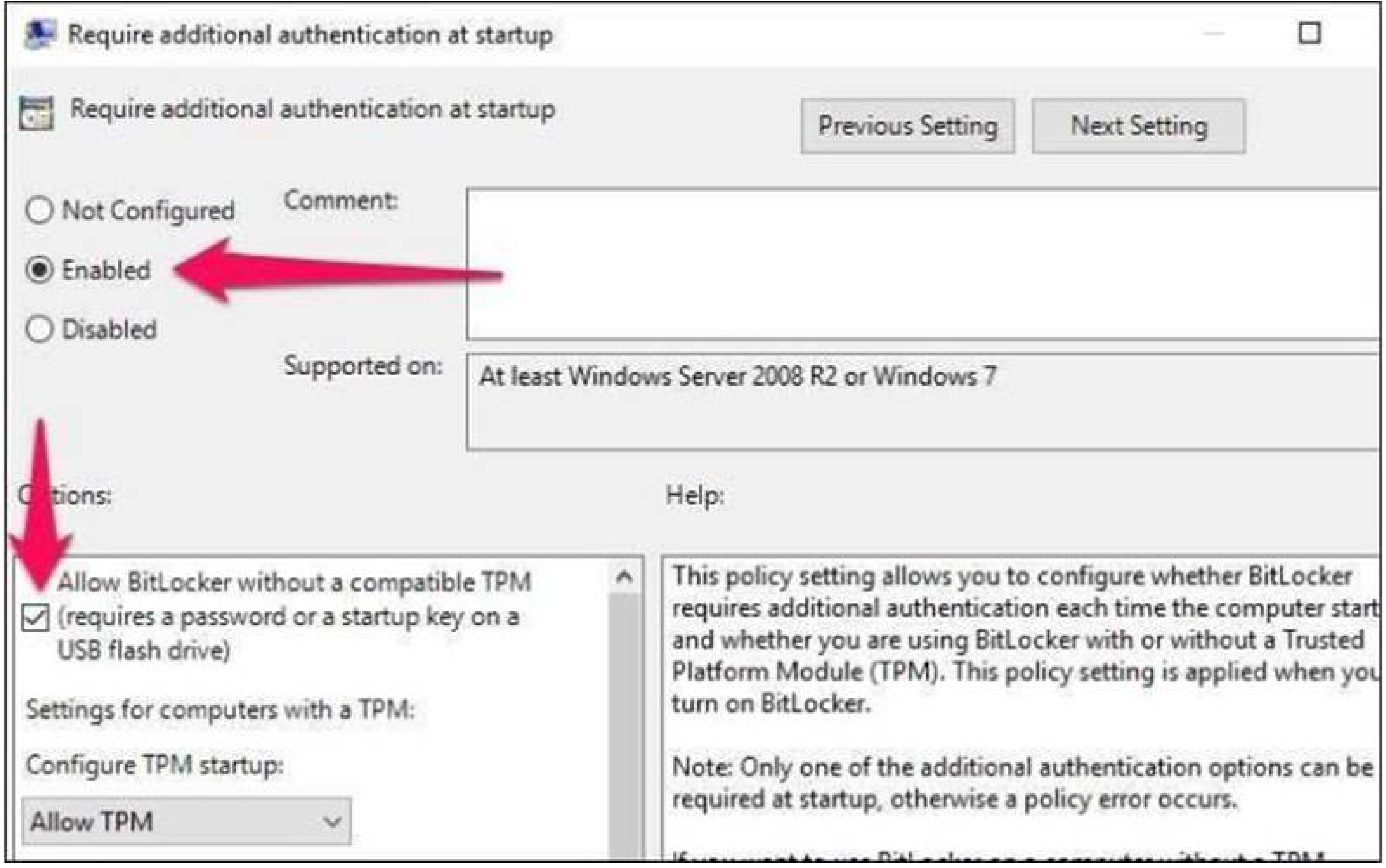
Edit policy setting

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 105
You have a guarded fabric and a Host Guardian Service server named HGS1.
You deploy a Hyper-V host named Hyper1, and configure Hyper1 as part of the guarded fabric. You plan to deploy the first shielded virtual machine. You need to ensure that you can run the virtual machine on Hyper1.
What should you do?

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

Answer: A

Explanation:
https://blogs.technet.microsoft.com/datacentersecurity/2016/06/06/step-by-step-creating-shieldedvms- withoutvmm/
The first step is to get the HGS guardian metadata from the HGS server, and use it to create the Key protector.
To do this, run the following PowerShell command
on a guarded host or any machine that can reach the HGS server:
Invoke-WebRequest http://<HGSServer">FQDN>/KeyProtection/service/metadata/2014- 07/metadata.xml –
OutFile C:\\HGSGuardian.xml Shield the VM
Each shielded VM has a Key Protector which contains one owner guardian, and one or more HGS guardians.
The steps below illustrate the process of getting the guardians, create the Key Protector in order to shield the VM.
Run the following cmdlets on a tenant host "Hyper1":

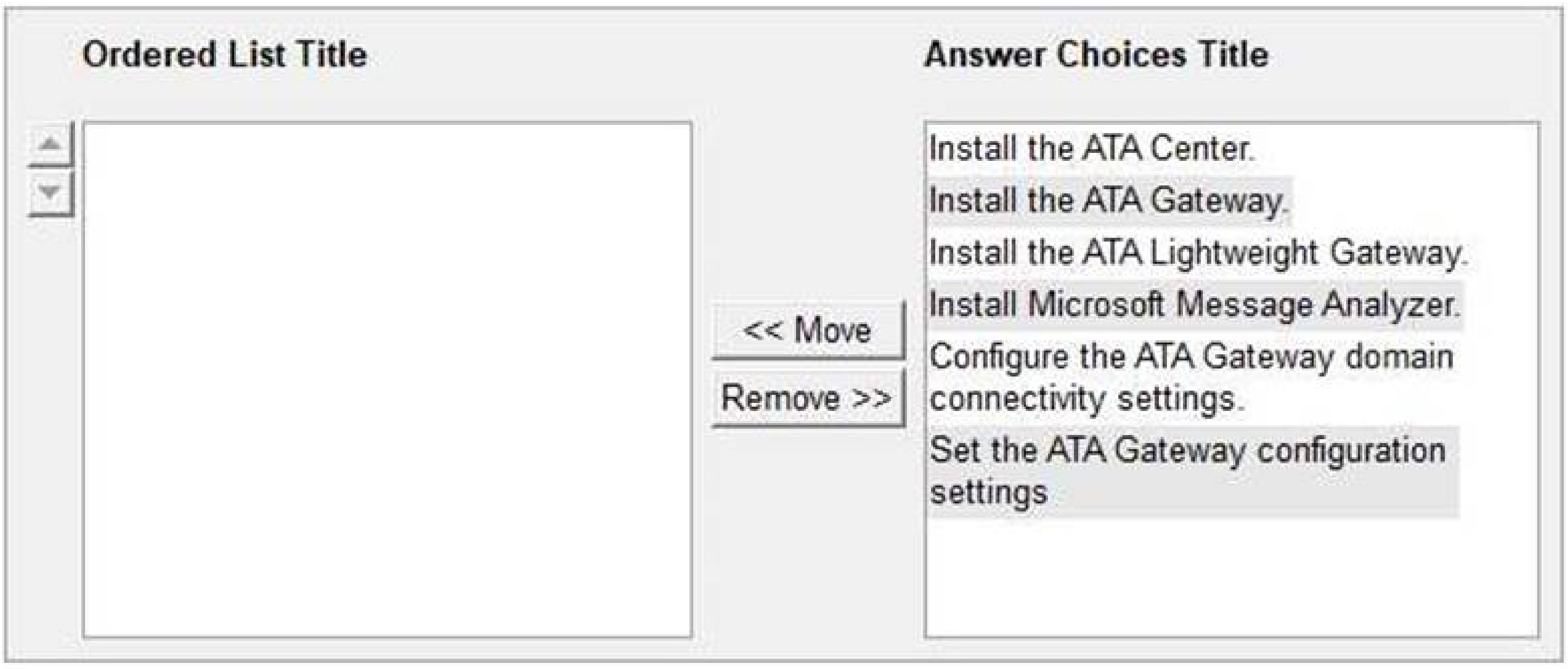
```
# SVM is the VM name which to be shielded
$VMName = 'SVM'
# Turn off the VM first. You can only shield a VM when it is powered off Stop-VM –VMName $VMName
# Create an owner self-signed certificate
$Owner = New-HgsGuardian –Name 'Owner' –GenerateCertificates
# Import the HGS guardian
$Guardian = Import-HgsGuardian -Path 'C:\\HGSGuardian.xml' -Name 'TestFabric' – AllowUntrustedRoot
# Create a Key Protector, which defines which fabric is allowed to run this shielded VM
$KP = New-HgsKeyProtector -Owner $Owner -Guardian $Guardian -AllowUntrustedRoot
# Enable shielding on the VM
Set-VMKeyProtector –VMName $VMName –KeyProtector $KP.RawData
# Set the security policy of the VM to be shielded
Set-VMSecurityPolicy -VMName $VMName -Shielded $true
# Enable vTPM on the VM
Enable-VMTPM -VMName $VMName
```

NEW QUESTION 110
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 114
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

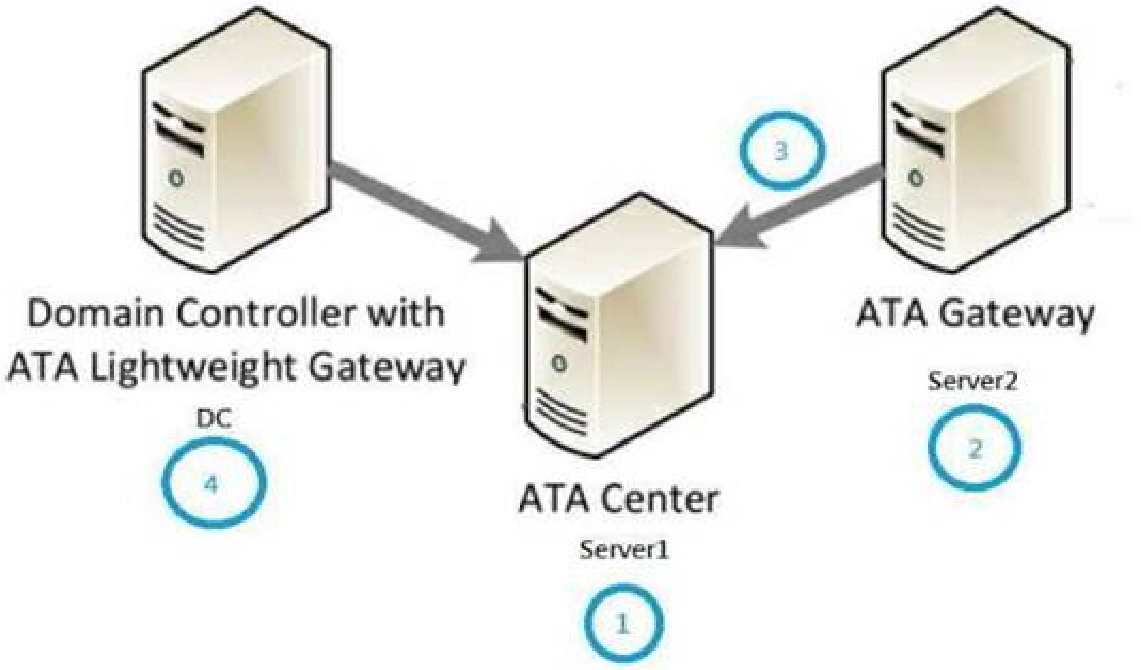
Install the ATA Center.
Install the ATA Gateway.
Install the ATA Lightweight Gateway.
Install Microsoft Message Analyzer.
Configure the ATA Gateway domain connectivity settings.
Set the ATA Gateway configuration settings

A. Mastered
B. Not Mastered

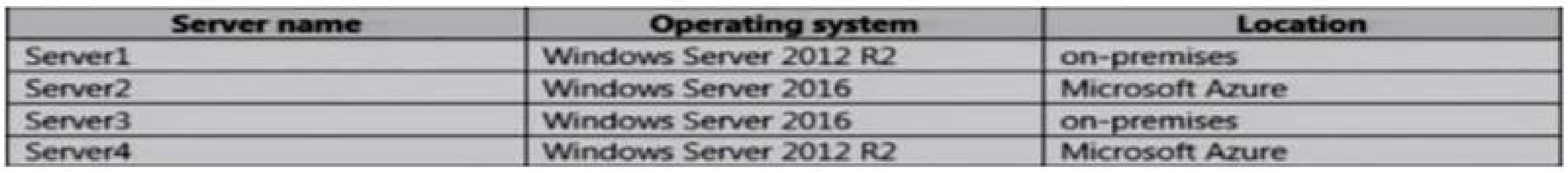
Answer: A

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 119
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.

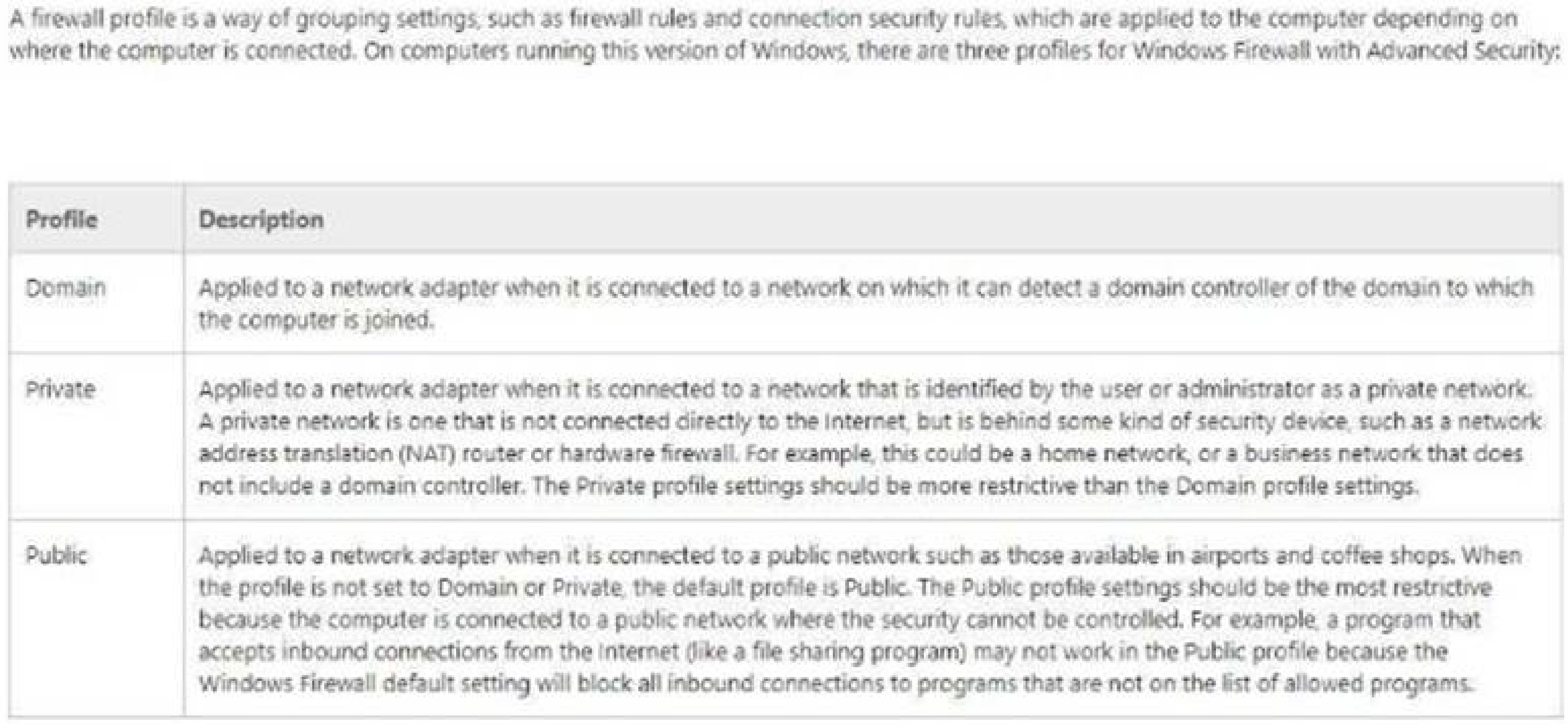
NEW QUESTION 122
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. The network uses the 172.16.0.0/16 address space.
Computer1 has an application named App1.exe that is located in D:\\Apps\\. App1.exe is configured to accept connections on TCP port 8080.
You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.
Solution: You configure an inbound rule that allows the TCP protocol on port 8080, uses a scope of 172.16.0.0/16 for local IP addresses, and applies to a private profile.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
"You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.", you should create the firewall rule for

“Domain” profile instead, not the “Private” profile.
https://technet.microsoft.com/en-us/library/getting-started-wfas-firewall-profilesipsec(v=ws.10).aspx



A firewall profile is a way of grouping settings, such as firewall rules and connection security rules, which are applied to the computer depending on where the computer is connected. On computers running this version of Windows, there are three profiles for Windows Firewall with Advanced Security:

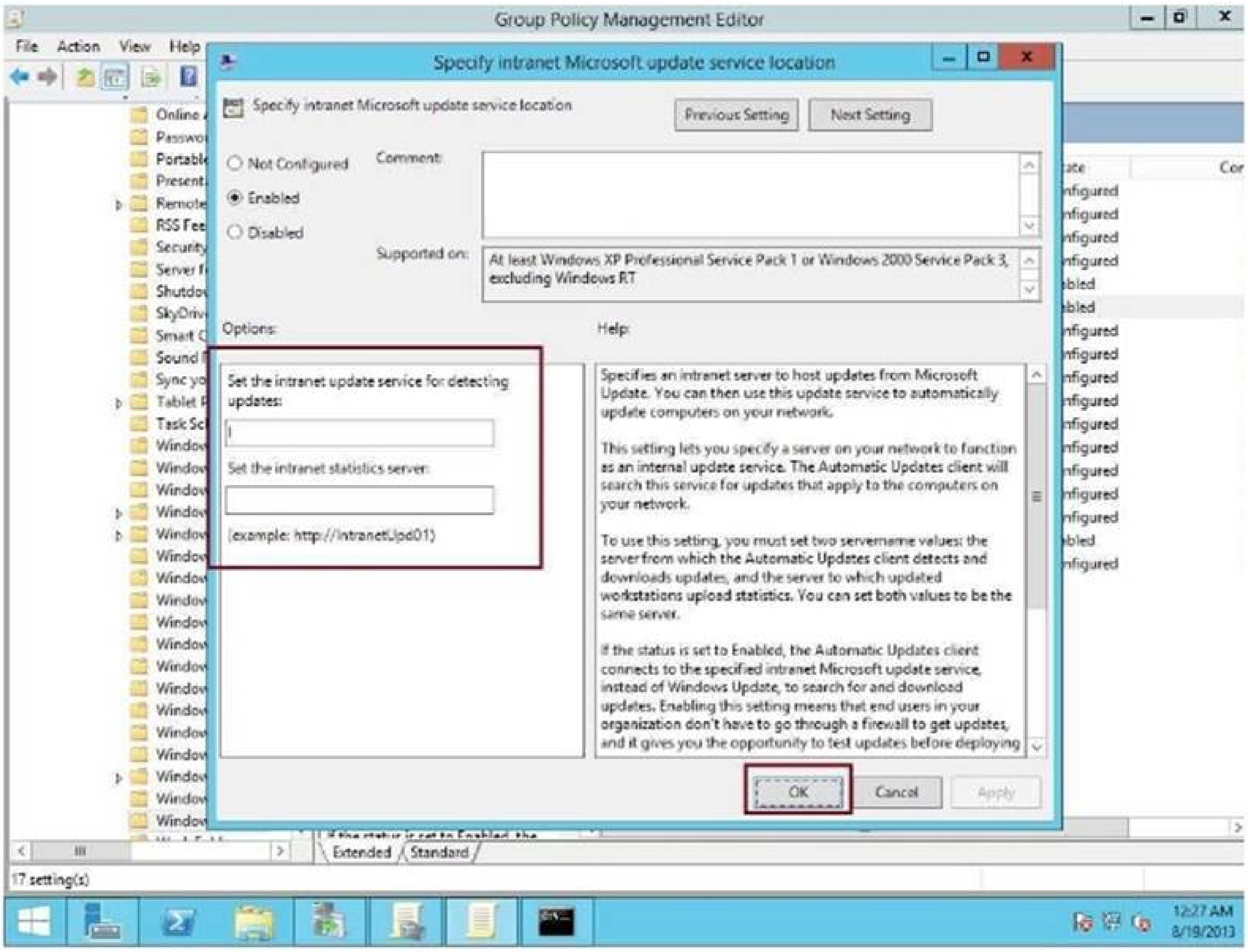
Profile	Description
Domain	Applied to a network adapter when it is connected to a network on which it can detect a domain controller of the domain to which the computer is joined.
Private	Applied to a network adapter when it is connected to a network that is identified by the user or administrator as a private network. A private network is one that is not connected directly to the Internet, but is behind some kind of security device, such as a network address translation (NAT) router or hardware firewall. For example, this could be a home network, or a business network that does not include a domain controller. The Private profile settings should be more restrictive than the Domain profile settings.
Public	Applied to a network adapter when it is connected to a public network such as those available in airports and coffee shops. When the profile is not set to Domain or Private, the default profile is Public. The Public profile settings should be the most restrictive because the computer is connected to a public network where the security cannot be controlled. For example, a program that accepts inbound connections from the Internet (like a file sharing program) may not work in the Public profile because the Windows Firewall default setting will block all inbound connections to programs that are not on the list of allowed programs.

NEW QUESTION 125
Your network contains an Active Directory domain named contoso.com.The domain contains 1,000 client computers that run either Windows 8.1 or Windows 10.
You have a Windows Server Update Services (WSUS) deployment All client computers receive updates from WSUS.
You deploy a new WSUS server named WSUS2.
You need to configure all of the client computers that run Windows 10 to send WSUS reporting data to WSUS2.
What should you configure?

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

Answer: C

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



Specify intranet Microsoft update service location

Specify intranet Microsoft update service location

Previous Setting | Next Setting

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, excluding Windows RT

Options:

Set the intranet update service for detecting updates:

Set the intranet statistics server:

(example: http://IntranetUpd01)

Help:

Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.

This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.

To use this setting, you must set two servername values: the server from which the Automatic Updates client detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server.

If the status is set to Enabled, the Automatic Updates client connects to the specified intranet Microsoft update service, instead of Windows Update, to search for and download updates. Enabling this setting means that end users in your organization don't have to go through a firewall to get updates, and it gives you the opportunity to test updates before deploying

OK | Cancel | Apply

NEW QUESTION 128

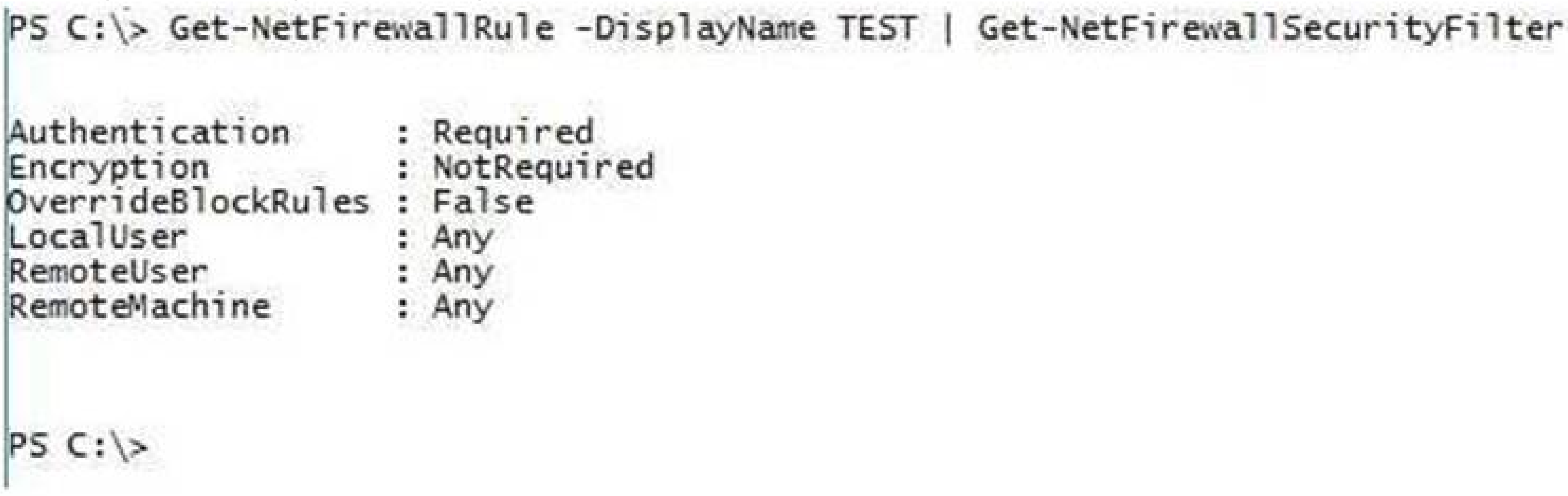
You have a server named Server1 that runs Windows Server 2016.
You need to identify whether any inbound rules on Server1 require that users be authenticated before they can connect to the server. Which cmdlet should you use?

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 132

Your network contains an Active Directory domain.
Microsoft Advanced Threat Analytics (ATA) is deployed to the domain.
A database administrator named DBA1 suspects that her user account was compromised.
Which three events can you identify by using ATA? Each correct answer presents a complete solution.

A. Spam messages received by DBA1.
B. Phishing attempts that targeted DBA1
C. The last time DBA1 experienced a failed logon attempt
D. Domain computers into which DBA1 recently signed.
E. Servers that DBA1 recently accesse

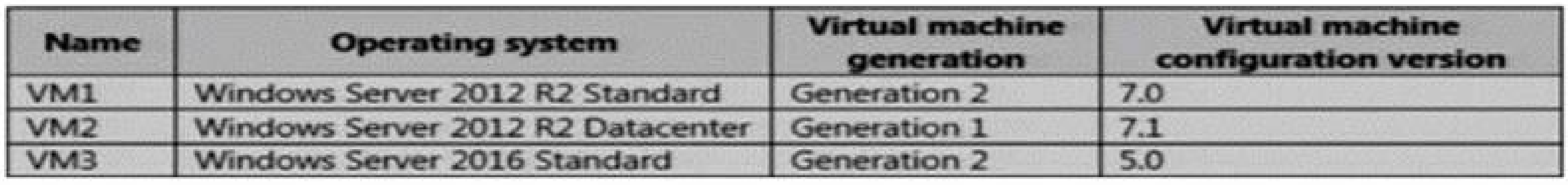
Answer: CDE

Explanation:

https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-threats Suspicious authentication failures (Behavioral brute force)
Attackers attempt to use brute force on credentials to compromise accounts. ATA raises an alert when abnormal failed authentication behavior is detected.
Abnormal behavior
Lateral movement is a technique often used by attackers, to move between devices and areas in the victim's network to gain access to privileged credentials or sensitive information of interest to the attacker. ATA is able to detect lateral movement by analyzing the behavior of users, devices and their relationship inside the corporate network, and detect on any abnormal access patterns which may indicate a lateral movement performed by an attacker.
https://gallery.technet.microsoft.com/ATA-Playbook-ef0a8e38/view/Reviews ATA Suspicious Activity Playbook Page 35 Action: Attempt to authenticate to DC1

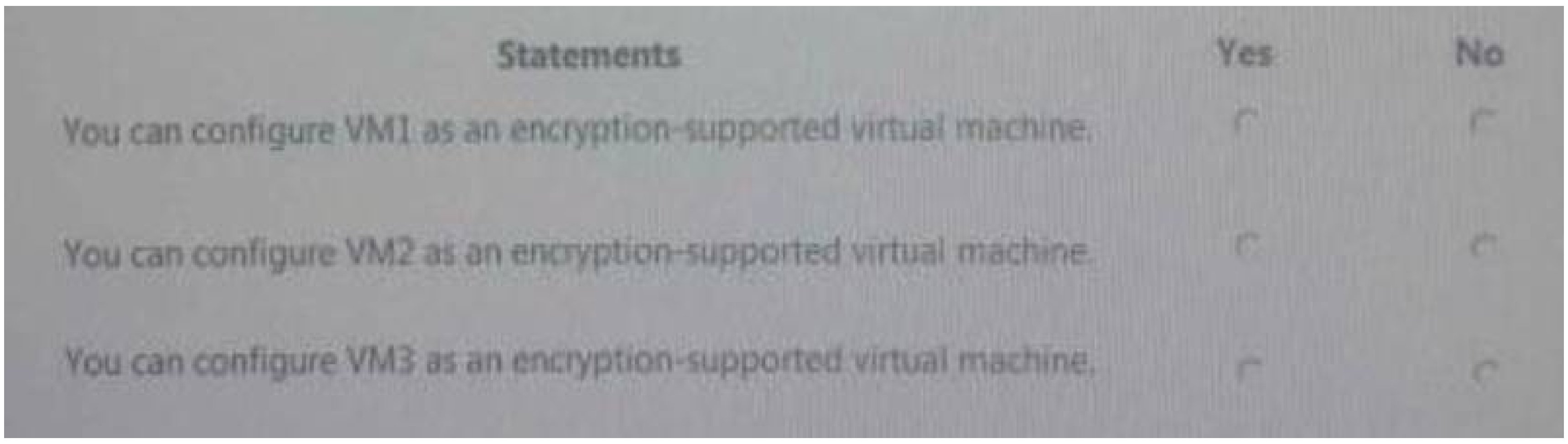
NEW QUESTION 137

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



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

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

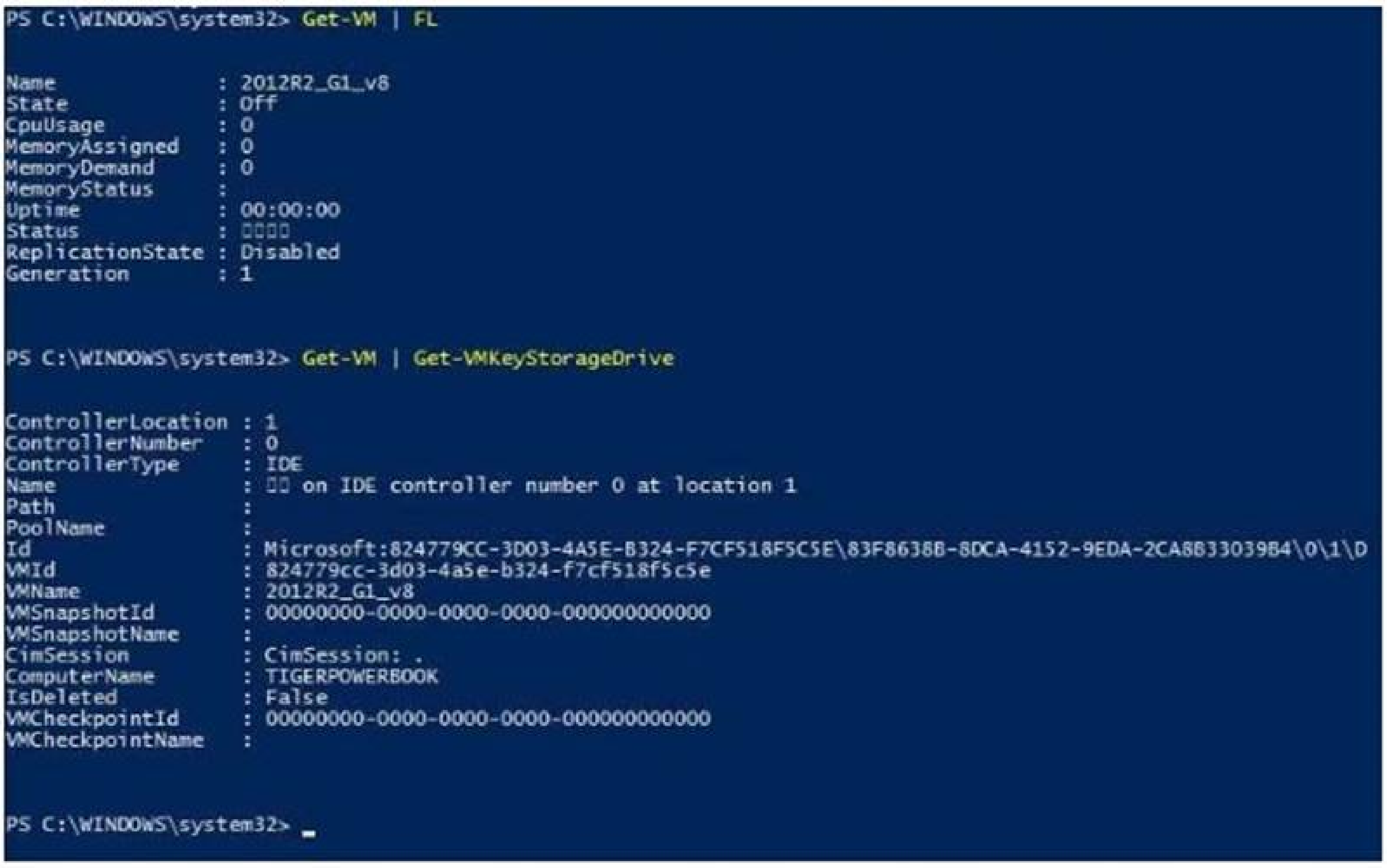


Statements	Yes	No
You can configure VM1 as an encryption-supported virtual machine.	○	○
You can configure VM2 as an encryption-supported virtual machine.	○	○
You can configure VM3 as an encryption-supported virtual machine.	○	○

A. Mastered
B. Not Mastered

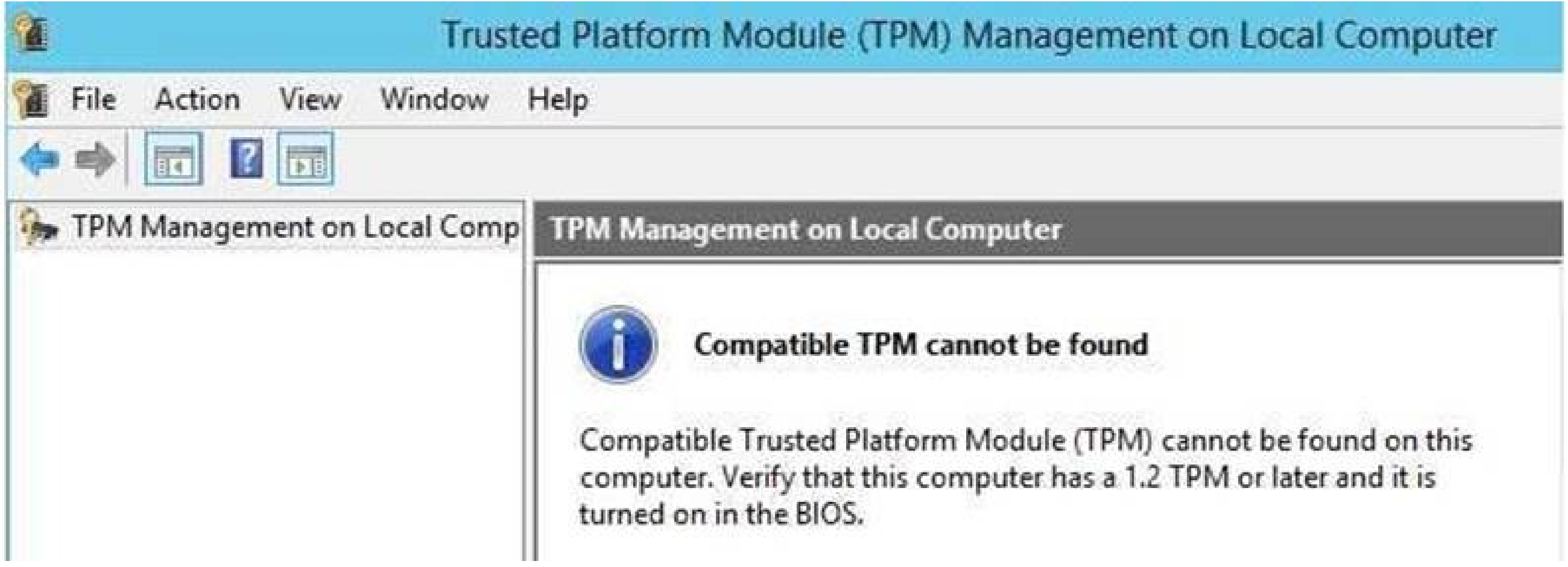
Answer: A

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



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


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


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


ControllerLocation : 1
ControllerNumber   : 0
ControllerType     : IDE
Name               : □□ on IDE controller number 0 at location 1
Path               :
PoolName           :
Id                 : Microsoft:824779CC-3D03-4A5E-B324-F7CF518F5C5E\83F8638B-8DCA-4152-9EDA-2CA8B33039B4\0\1\D
VMId               : 824779cc-3d03-4a5e-b324-f7cf518f5c5e
VMName             : 2012R2_G1_v8
VMSnapshotId       : 00000000-0000-0000-0000-000000000000
VMSnapshotName     :
CimSession         : CimSession: .
ComputerName       : TIGERPOWERBOOK
IsDeleted          : False
VMCheckpointId     : 00000000-0000-0000-0000-000000000000
VMCheckpointName   :


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

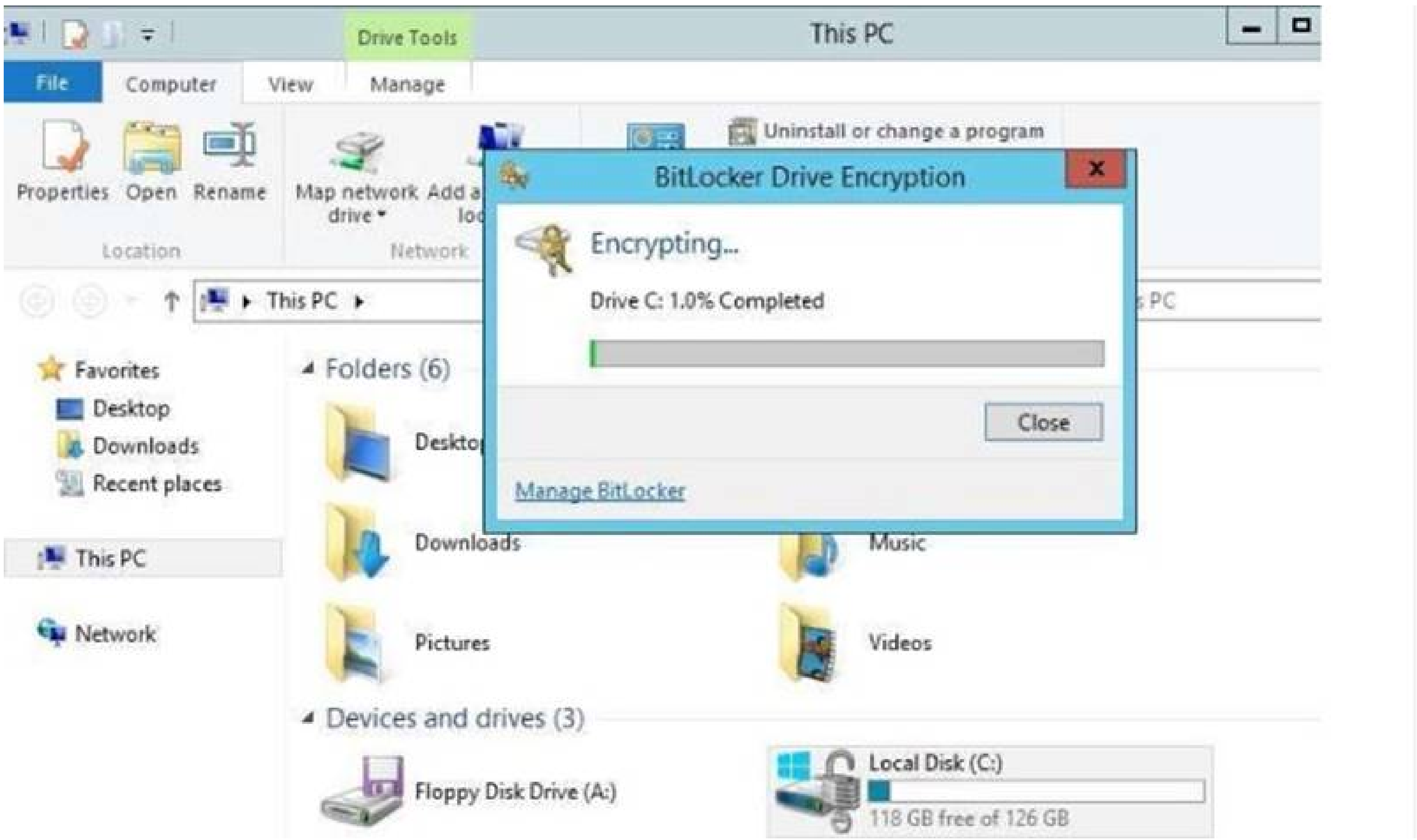
Within the guest, there is no Virtual TPM


Trusted Platform Module (TPM) Management on Local Computer
File
Action
View
Window
Help
TPM Management on Local Comp
TPM Management on Local Computer

Compatible TPM cannot be found

Compatible Trusted Platform Module (TPM) cannot be found on this computer. Verify that this computer has a 1.2 TPM or later and it is turned on in the BIOS.

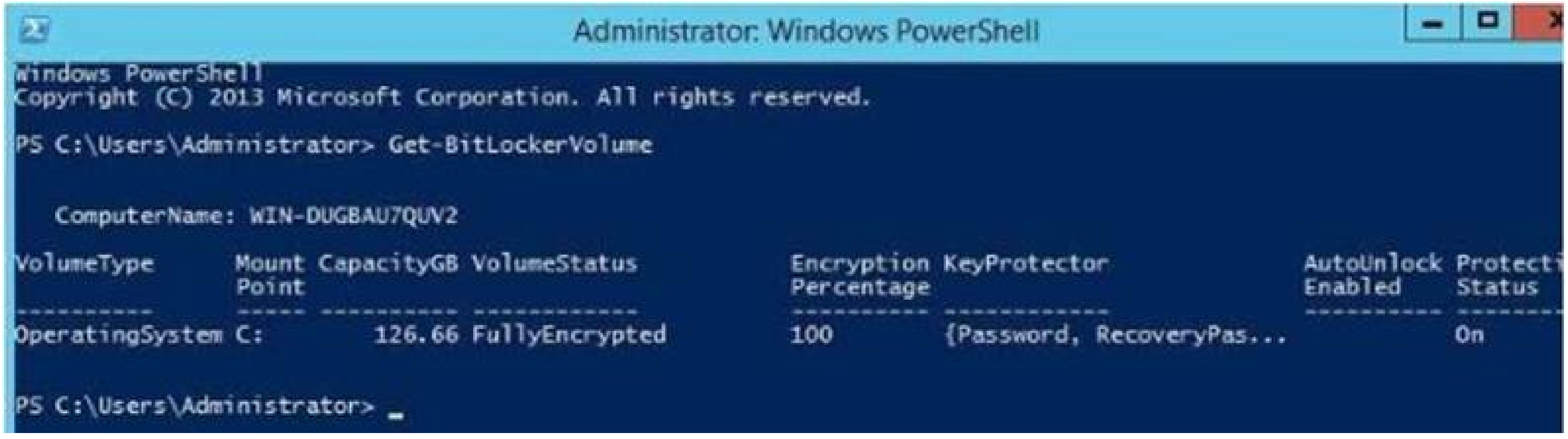
Then , start Encrypt the C system drive with the guest 2012R2 bitlocker feature



Encrypting...

Drive C: 1.0% Completed

After the encryption is completed:-



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-BitLockerVolume


   ComputerName: WIN-DUGBAU7QUV2

VolumeType      Mount CapacityGB VolumeStatus           Encryption KeyProtector              AutoUnlock Protecti
                Point                                   Percentage                           Enabled    Status
----------      ----- ---------- ------------           ---------- ------------              ---------- -------
OperatingSystem C:        126.66 FullyEncrypted         100        {Password, RecoveryPas...            On

PS C:\Users\Administrator> _
```

NEW QUESTION 139

Your network contains an Active Directory domain named contoso.com. All servers in the domain run Windows Server 2016.All client computers run Windows 10.

Your company has deployed the Local Administrator Password Solution (LAPS).

Client computers in the finance department are located in an organizational unit (OU) named Finance.

Each finance computer has a custom administrative account named FinAdmin. You discover that the FinAdmin accounts are not managed by LAPS.

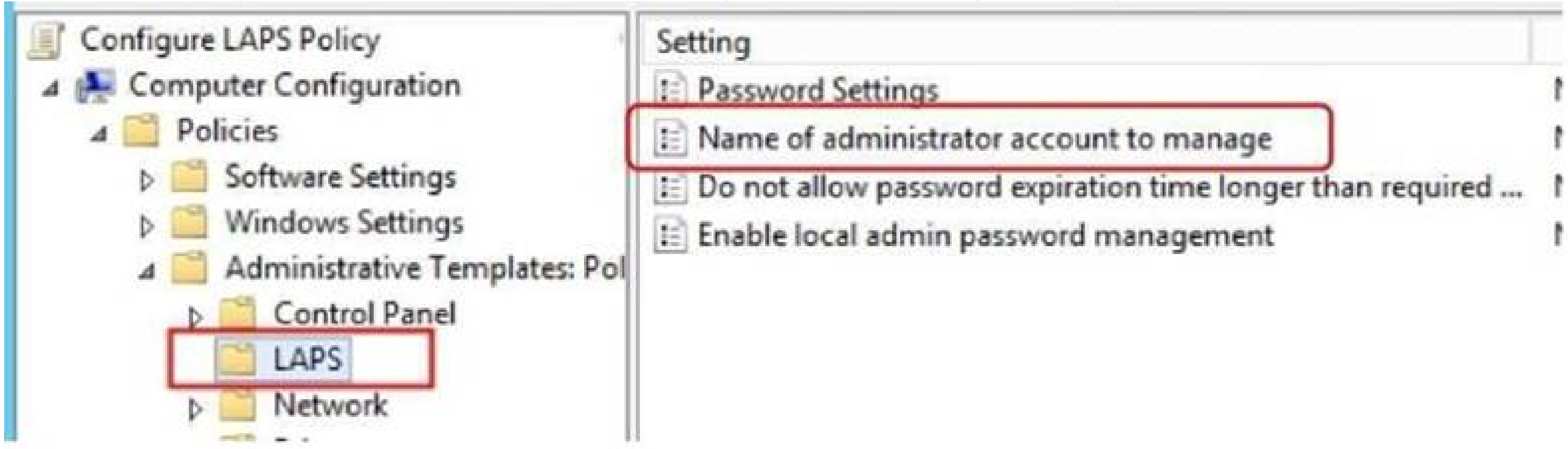
You need to ensure that the FinAdmin accounts are managed by LAPS. What should you do?

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

Answer: C

Explanation:

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


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

NEW QUESTION 143

Your network contains an Active Directory forest named contoso.com. The forest functional level is Windows Server 2012.

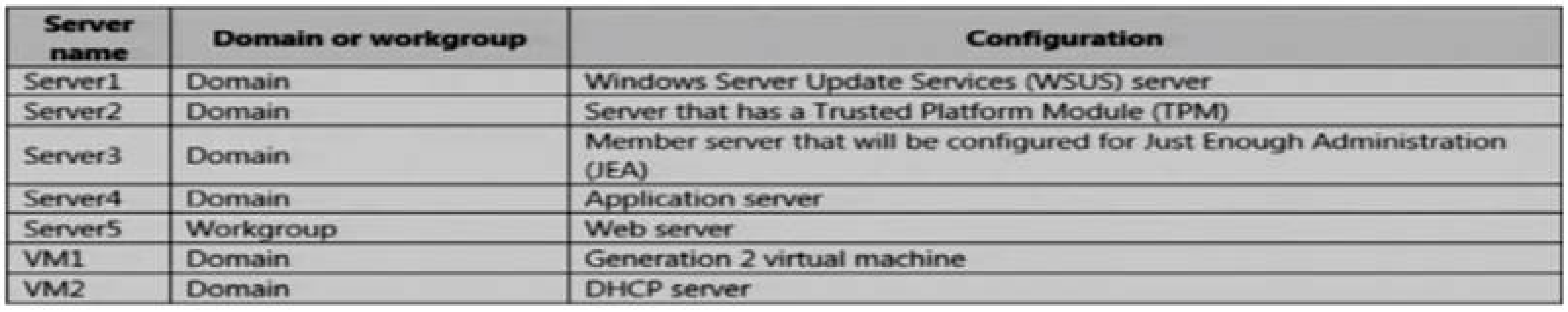
The forest contains 20 member servers that are configured as file servers. All domain controllers run Windows Server 2016.
You create a new forest named contosoadmin.com.
You need to use the Enhanced Security Administrative Environment (ESAE) approach for the administration of the resources in contoso.com.
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 145
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.



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

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.
All laptops are protected by using BitLocker Drive Encryption (BitLocker).You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.
An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1.
A GPO named GP2 is linked to OU2.
All computers receive updates from Server1. You create an update rule named Update1.
You need to ensure that you can view Windows PowerShell code that was generated dynamically and executed on the computers in OU1.
What would you configure in GP1?

A. Object Access\\Audit Application Generated from the advanced audit policy
B. Turn on PowerShell Script Block Logging from the PowerShell settings
C. Turn on Module Logging from the PowerShell settings
D. Object Access\\Audit Other Object Access Events from the advanced audit policy

Answer: B

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

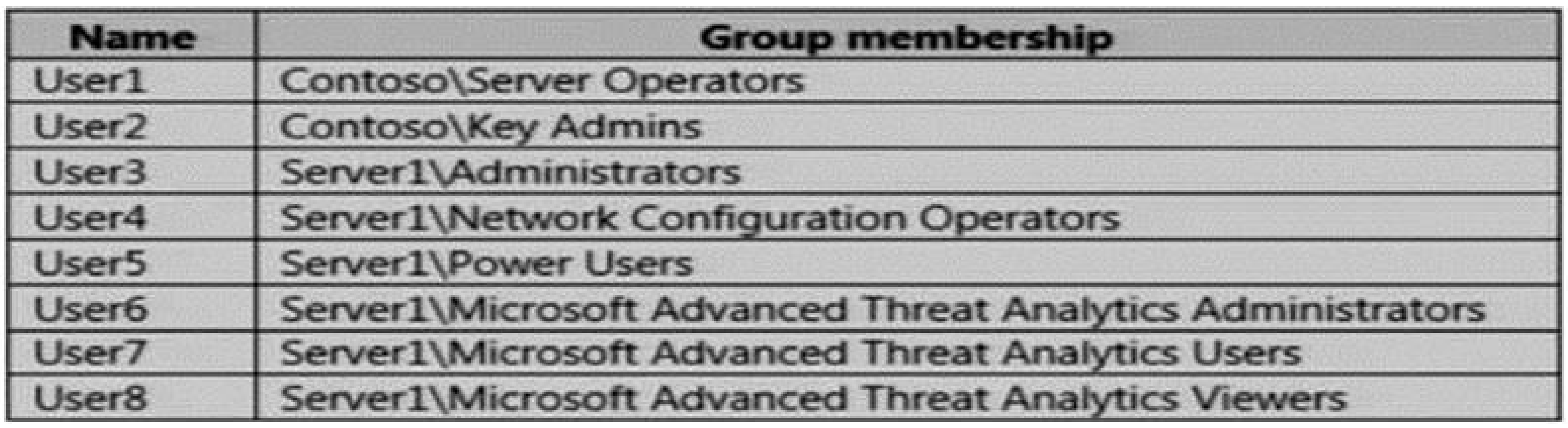
NEW QUESTION 146
You are building a guarded fabric. You need to configure Admin-trusted attestation. Which cmdlet should you use?

A. Add-HgsAttestationHostGroup
B. Add-HgsAttestationTpmHost
C. Add-HgsAttestationCIPolicy
D. Add-HgsAttestationTpmPolicy

Answer: A

Explanation:
Authorize Hyper-V hosts using Admin-trusted attestation
https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shieldedvm/ guarded-fabric-addhost-information-for-admin-trusted-attestation

NEW QUESTION 147
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2016.
The Microsoft Advanced Threat Analytics (ATA) Center service is installed on Server1. The domain contains the users shown in the following table.



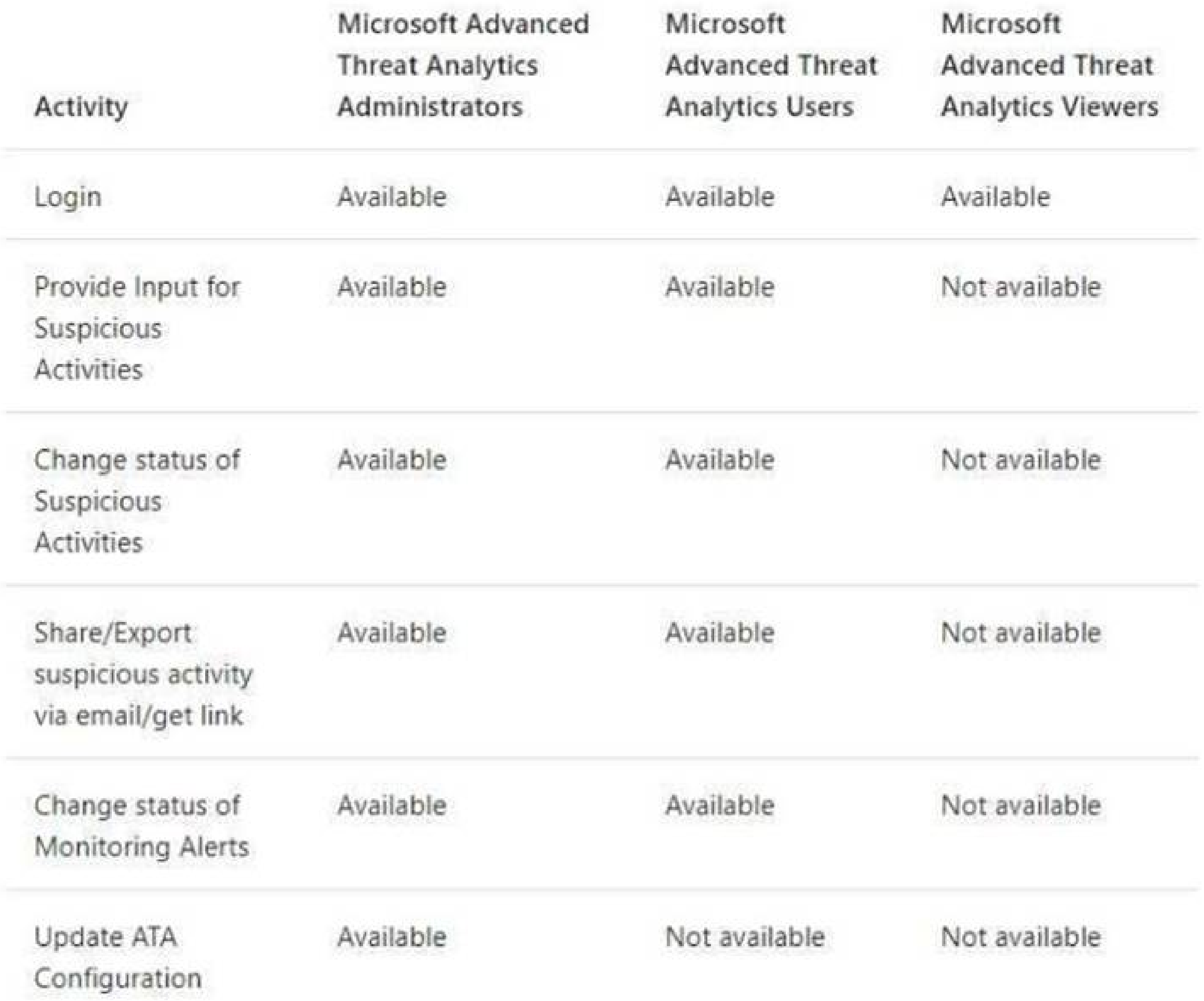
Name	Group membership
User1	Contoso\Server Operators
User2	Contoso\Key Admins
User3	Server1\Administrators
User4	Server1\Network Configuration Operators
User5	Server1\Power Users
User6	Server1\Microsoft Advanced Threat Analytics Administrators
User7	Server1\Microsoft Advanced Threat Analytics Users
User8	Server1\Microsoft Advanced Threat Analytics Viewers

You are installing ATA Gateway on Server2.
You need to specify a Gateway Registration account. Which account should you use?

A. User1
B. User2
C. User3
D. User4
E. User5
F. User6
G. User7
H. User8

Answer: F

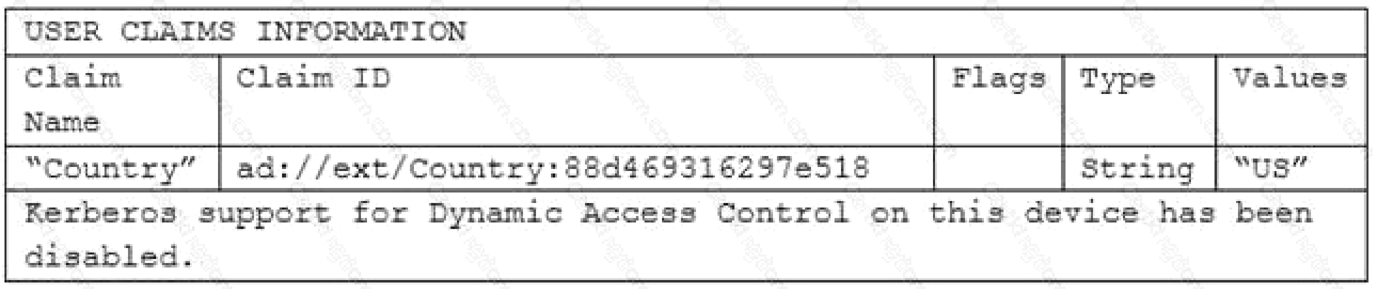
Explanation:
https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-role-groups



Activity	Microsoft Advanced Threat Analytics Administrators	Microsoft Advanced Threat Analytics Users	Microsoft Advanced Threat Analytics Viewers
Login	Available	Available	Available
Provide Input for Suspicious Activities	Available	Available	Not available
Change status of Suspicious Activities	Available	Available	Not available
Share/Export suspicious activity via email/get link	Available	Available	Not available
Change status of Monitoring Alerts	Available	Available	Not available
Update ATA Configuration	Available	Not available	Not available

The user who installed ATA will be able to access the management portal (ATA Center) as members of the “Microsoft Advanced Threat Analytics Administrators” local group on the ATA Center server.

NEW QUESTION 148
The Job Title attribute for a domain user named User1 has a value of Sales Manager. User1 runs whoami /claims and receives the following output:



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

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

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

Answer: C

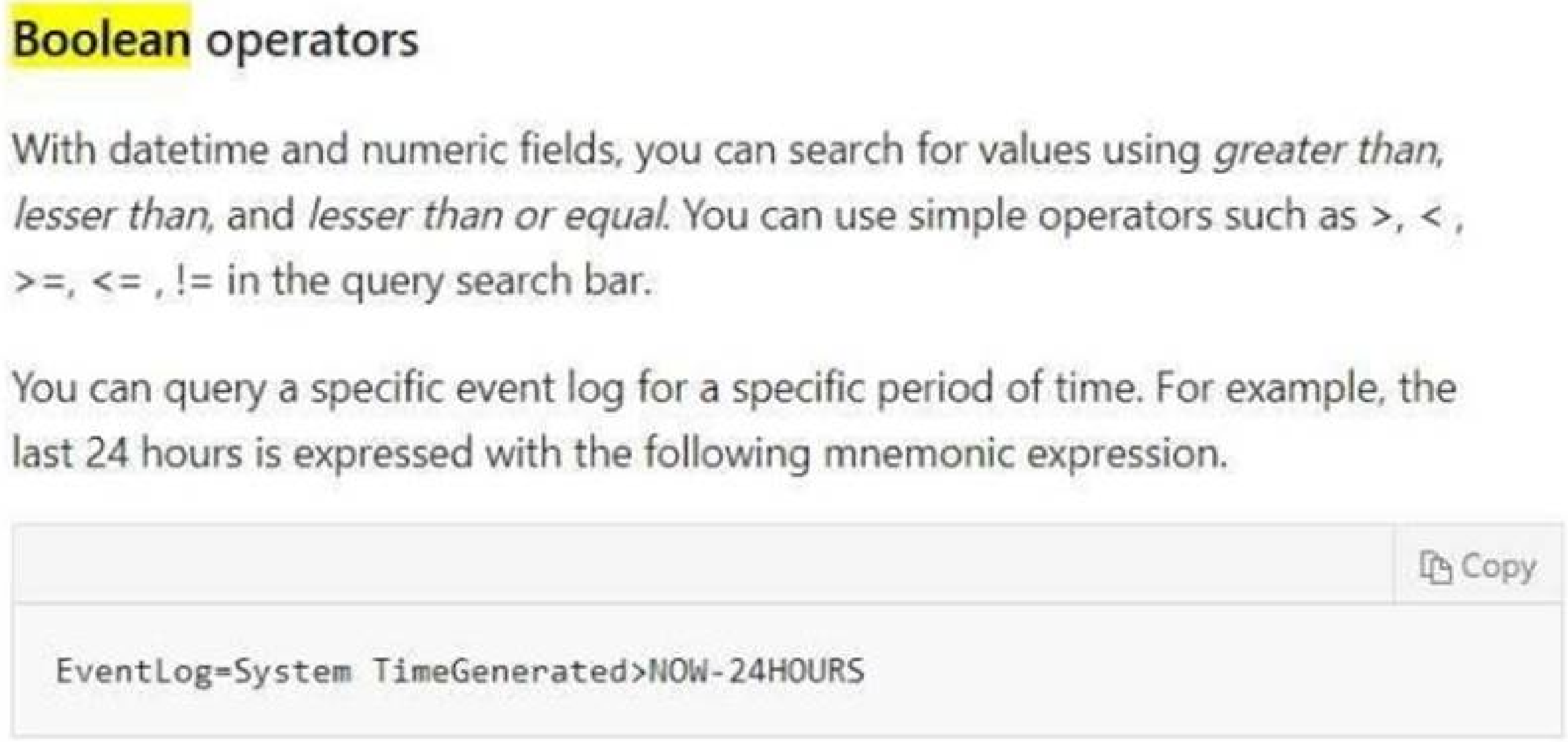
Explanation:
From the output, obviously, a claim type is missing (or disabled) so that the domain controller is not issuing
tickets with the “Job Title” claim type.

NEW QUESTION 150
You implement Log Analytics in Microsoft Operations Management Suite (OMS) on all servers that run Windows Server 2016.
You need to generate a daily report that identifies which servers restarted during the last 24 hours. Which query should you use?

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

Answer: C

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



Boolean operators

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

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

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

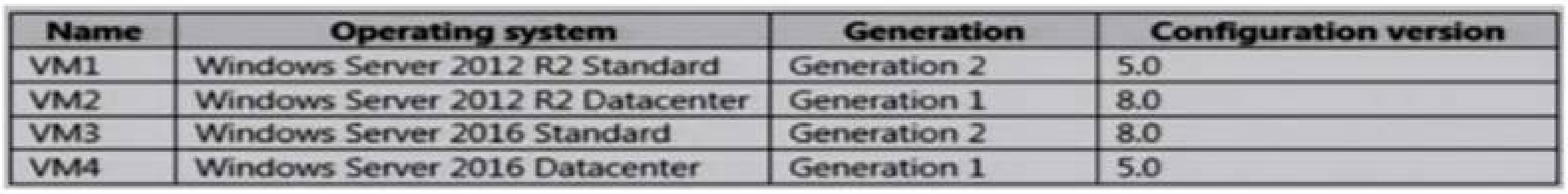
NEW QUESTION 152
Your network contains an Active Directory forest named corp.contoso.com.
You are implementing Privileged Access Management (PAM) by using a bastion forest named priv.contoso.com.
You need to create shadow groups in priv.contoso.com. Which cmdlet should you use?

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 154
You have a Hyper-V host named Server1 that runs Windows Server 2016. Server1 hosts the virtual machines configured as shown in the following table.



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

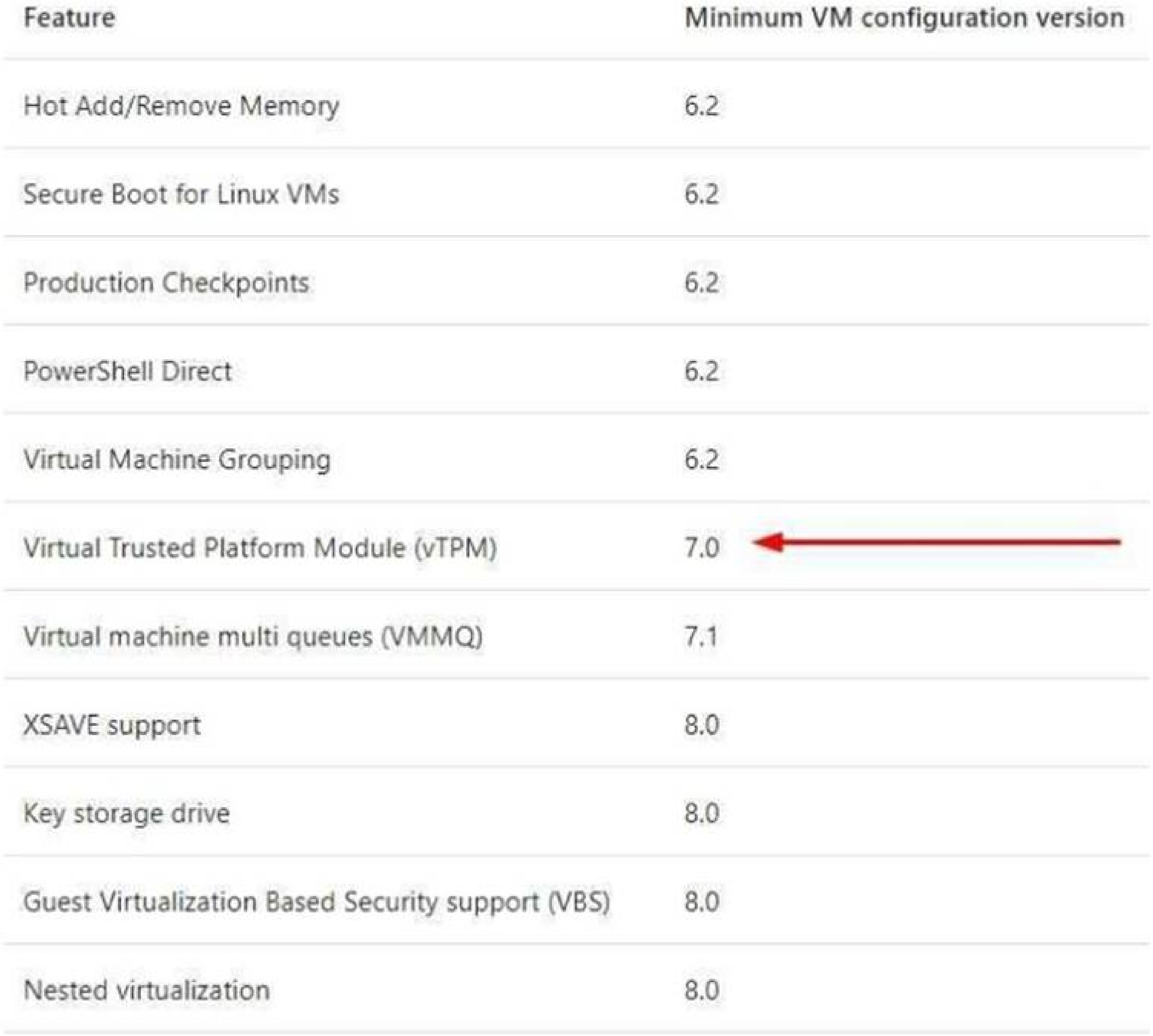
All the virtual machines have two volumes named C and D.
You plan to implement BitLocker Drive Encryption (BitLocker) on the virtual machines. Which virtual machines can have their volumes protected by using BitLocker? Choose Two.

A. Virtual machines that can have volume C protected by using BitLocker and a Trusted Platform Module (TPM) protector: VM3 only

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

Answer: AG

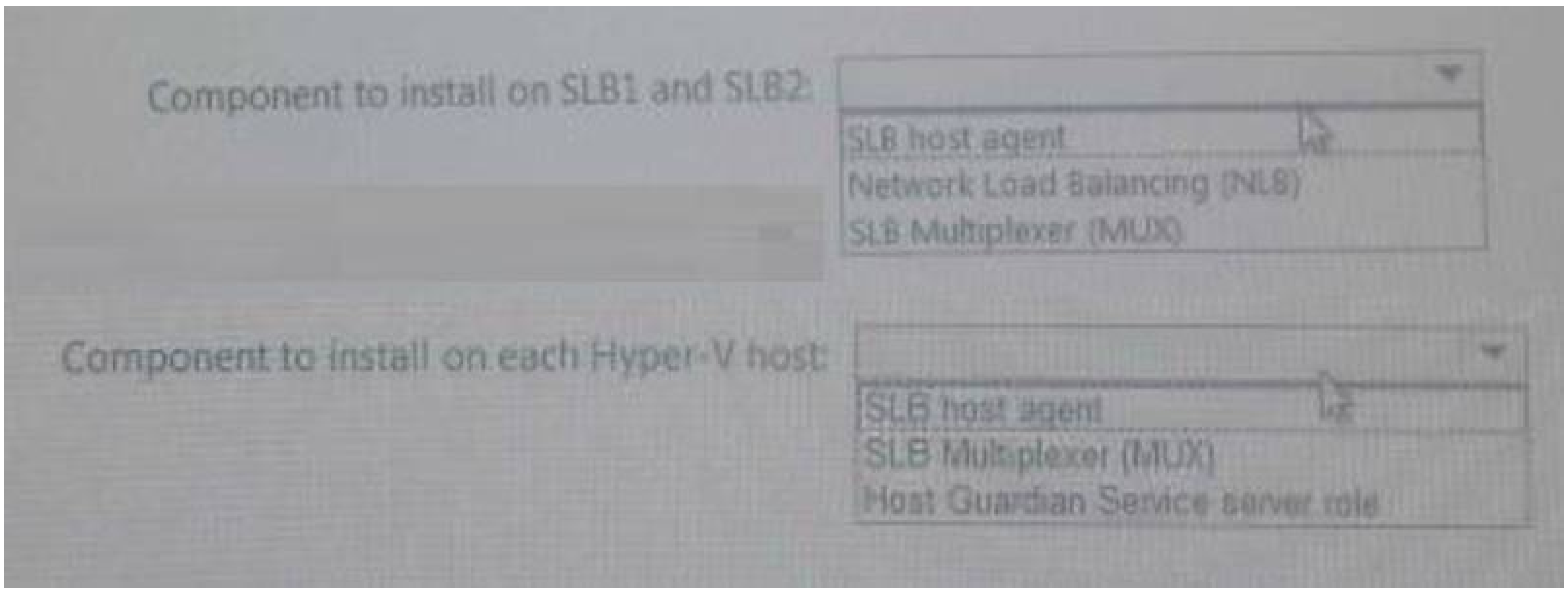
Explanation:
https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/deploy/upgrade-virtualmachine- versionin-hyper-v-on-windows-or-windows-server
To use Virtual TPM protector for encrypting C: drive, you have to use at least VM Configuration Version 7.0 and Generation 2 Virtual machines.



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

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

NEW QUESTION 156
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)

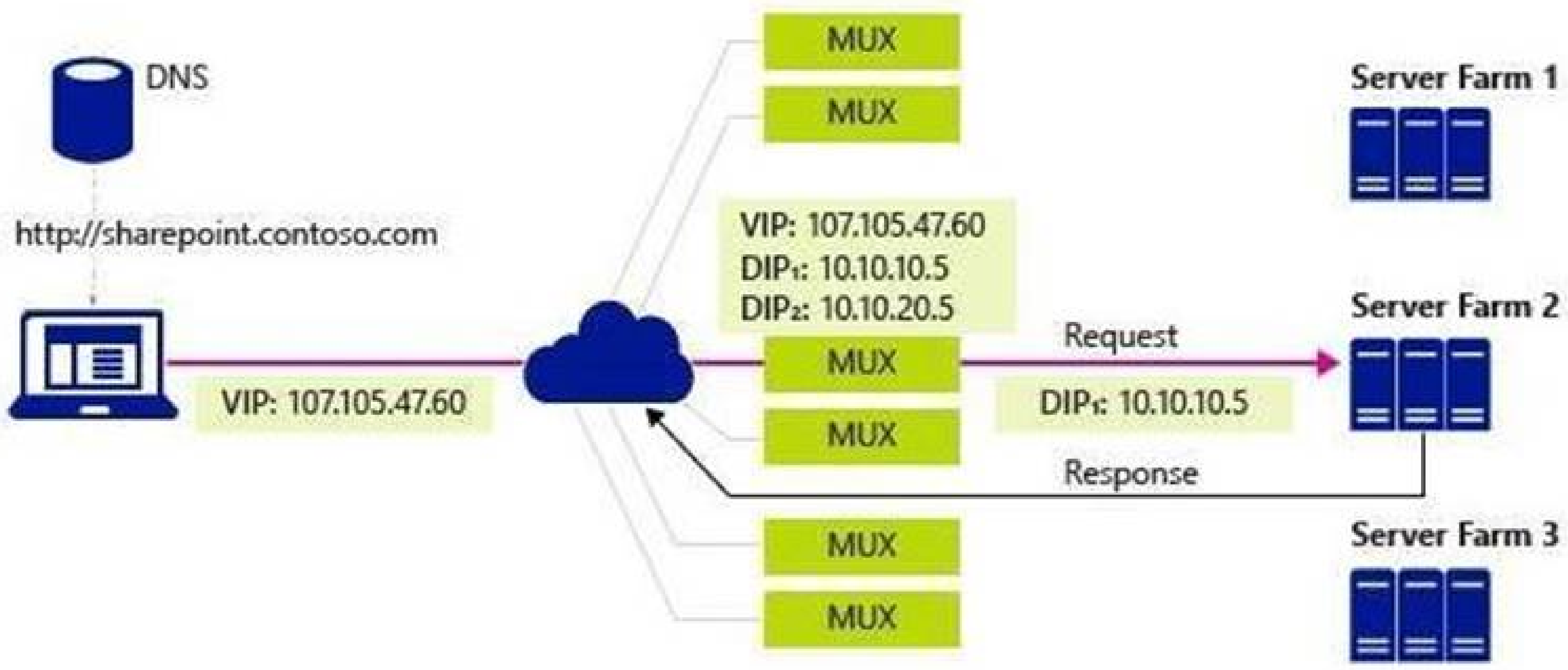
Component to install on each Hyper-V host:

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.

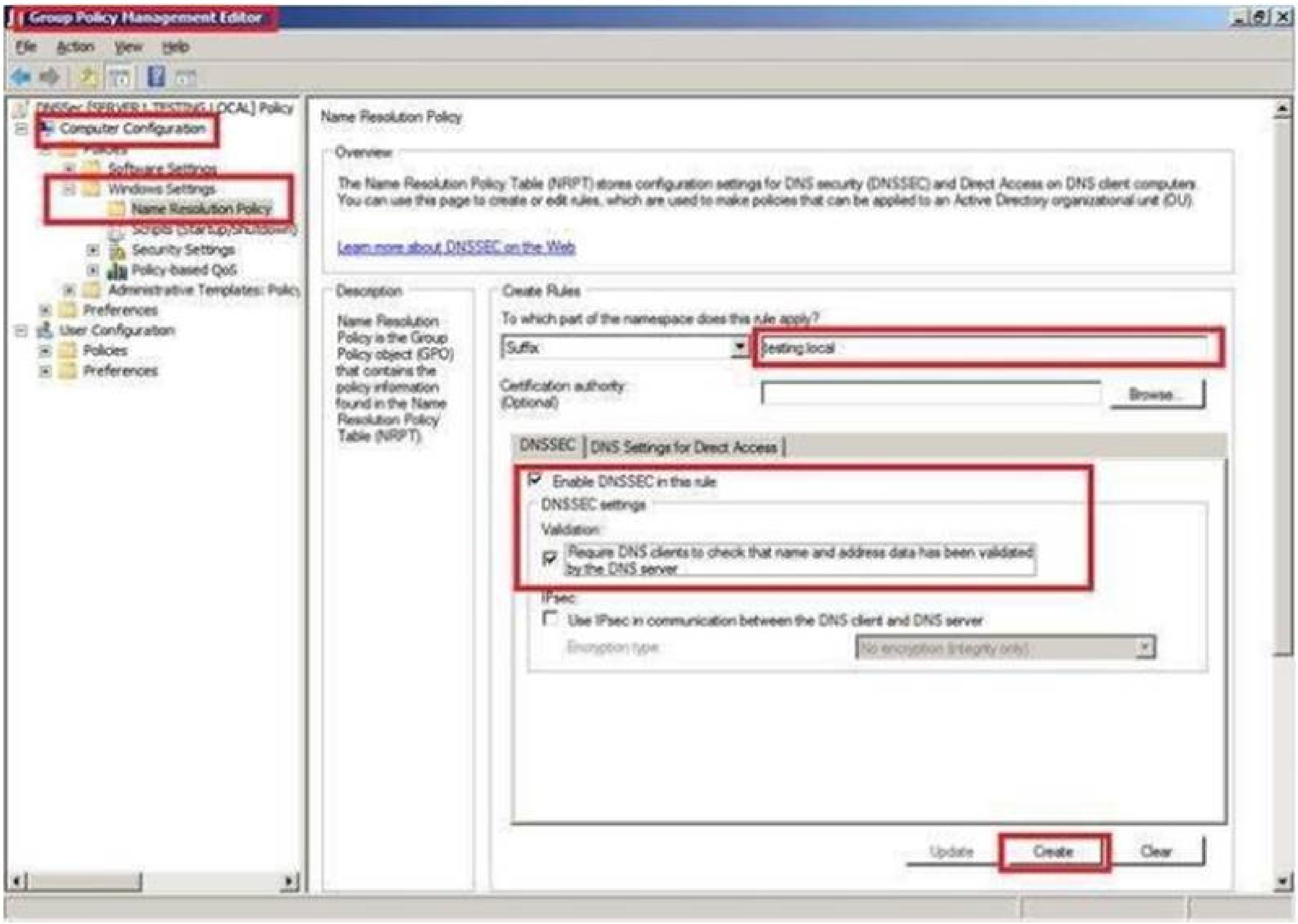


NEW QUESTION 160
Your network contains an Active Directory domain named contoso.com. The domain contains two DNS servers that run Windows Server 2016. The servers host two zones named contoso.com and admin.contoso.com. You sign both zones.
You need to ensure that all client computers in the domain validate the zone records when they query the zone.
What should you deploy?

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

Answer: C

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



Name Resolution Policy

Overview

The Name Resolution Policy Table (NRPT) stores configuration settings for DNS security (DNSSEC) and Direct Access 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).

Learn more about DNSSEC on the Web

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 testing.local

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)

NEW QUESTION 164
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. You need to prevent NTLM authentication on Server1.
Solution: From a Group Policy, you configure the Security Options. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 166
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. You need to prevent NTLM authentication on Server1.
Solution: From Windows PowerShell, you run the New-ADAuthenticationPolicy cmdlet. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 168
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 with Advanced Security, you create an inbound rule. Does this meet the goal?

A. Yes
B. No

Answer: A

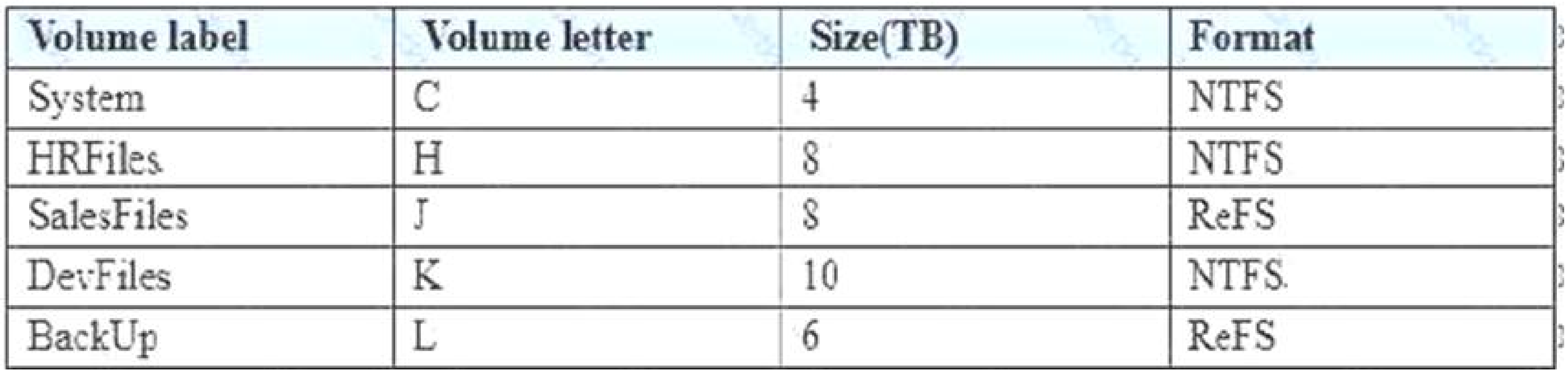
NEW QUESTION 170
You network contains an Active Directory forest named contoso.com.
All domain controllers run Windows Server 2016 Member servers run either Windows Server 2012 R2 or Windows Server 2016.
Client computers run either Windows 8.1 or Windows 10.
You need to ensure that when users access 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 171
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You manage a file server that runs Windows Server 2016. The file server contains the volumes configured as shown in the following table.



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

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

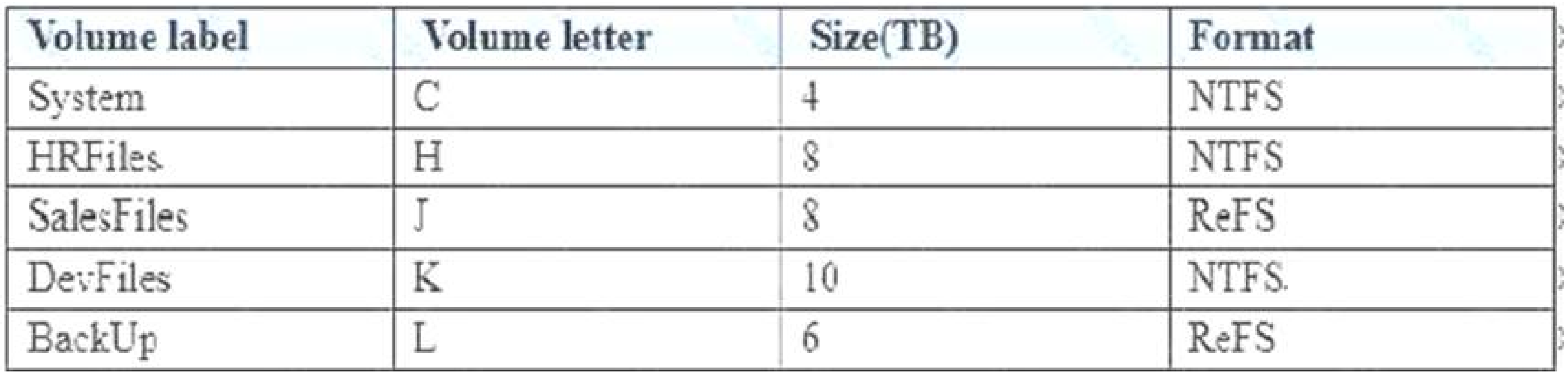
A. Yes
B. No

Answer: A

Explanation:

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

NEW QUESTION 174
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You manage a file server that runs Windows Server 2016. The file server contains the volumes configured as shown in the following table.



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

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

A. Yes
B. No

Answer: A

Explanation:

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

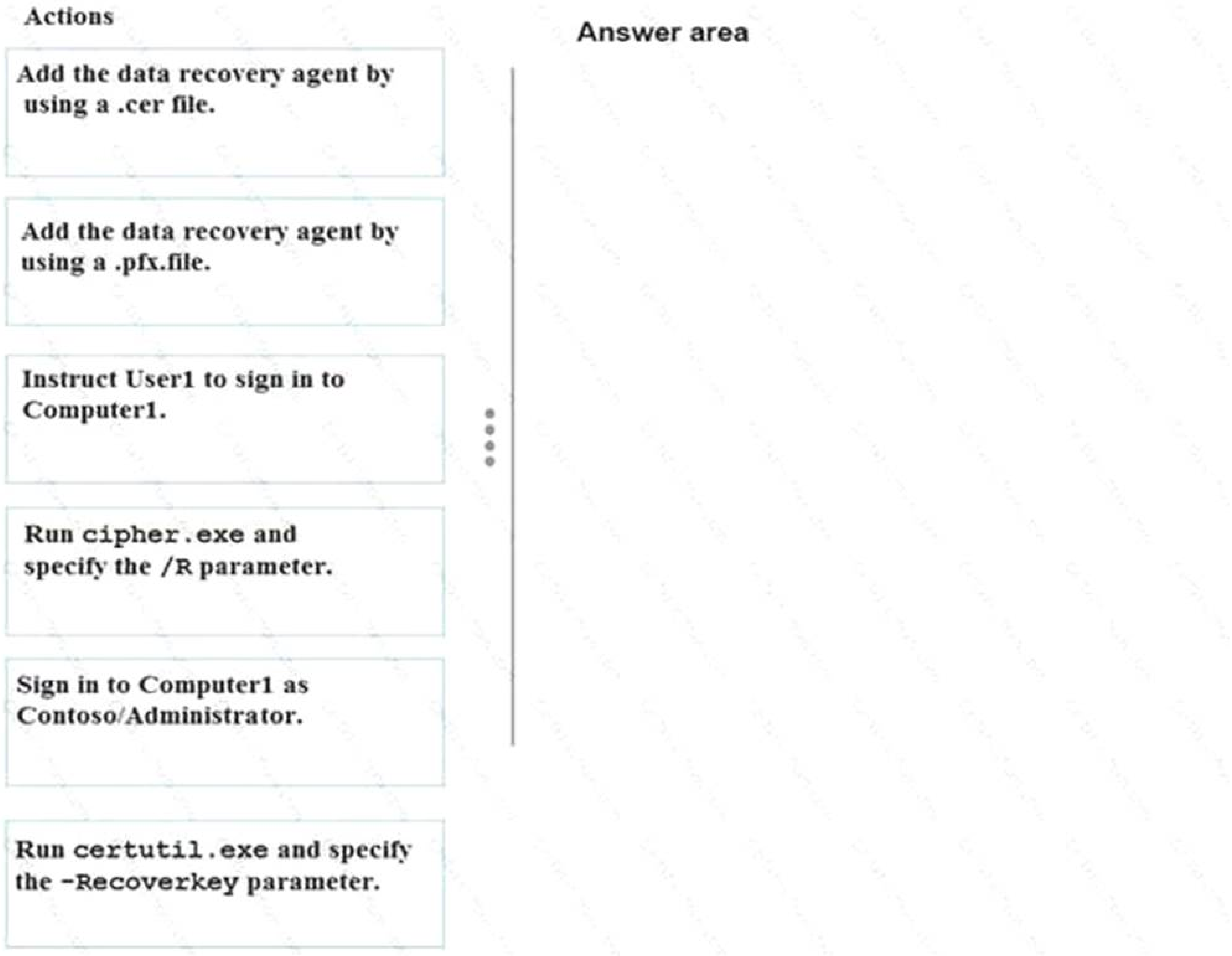
NEW QUESTION 176
You have a file server named FS1 that runs Windows Server 2016. You plan to disable SMB 1.0 on the server.
You need to verify which computers access FS1 by using SMB 1.0. What should you run first?

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

E. Set-SmbClientConfiguration

Answer: D

NEW QUESTION 181
DRAG DROP
Your network contains an Active Directory domain named contoso.com. The domain contains a user named User1 and a computer named Computer1. Remote Server Administration Tools (RSAT) is installed on Computer1.
You need to add User1 as a data recovery agent in the domain.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

Answer area

Add the data recovery agent by using a .cer file.

Add the data recovery agent by using a .pfx.file.

Instruct User1 to sign in to Computer1.

Run cipher.exe and specify the /R parameter.

Sign in to Computer1 as Contoso/Administrator.

Run certutil.exe and specify the -Recoverkey parameter.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 184
Your network contains an Active Directory domain named contoso.com. The domain contains a certification authority (CA).
You need to implement code integrity policies and sign them by using certificates issued by the CA. You plan to use the same certificate to sign policies on multiple computers.
You duplicate the Code Signing certificate template and name the new template CodeIntegrity. How should you configure the CodeIntegrity template?

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

Answer: D

NEW QUESTION 188
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

70-744 Practice Exam Features:

* 70-744 Questions and Answers Updated Frequently

* 70-744 Practice Questions Verified by Expert Senior Certified Staff

* 70-744 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 70-744 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year