

## 70-744 Dumps

### Securing Windows Server 2016

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



**NEW QUESTION 1**

Note: This question is part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question In this section, you will NOT be able to return to It. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory 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](https://technet.microsoft.com/en-us/library/dd759068(v=ws.11).aspx)

**NEW QUESTION 2**

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to It. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. 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](https://technet.microsoft.com/en-us/library/cc771990(v=ws.11).aspx)

**NEW QUESTION 3**

Note: This question is part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question In this section, you will NOT be able to return to It. As a result, these questions will not appear In the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains multiple Hyper-V hosts.

You need to deploy several critical line-of-business applications to the network; to meet the following requirements:

\*The resources of the applications must be isolated from the physical host.

\*Each application must be prevented from accessing the resources of the other applications.

\*The configurations of the applications must be accessible only from the operating system that hosts the application.

Solution: You deploy a separate Windows container for each application. Does this meet the goal?

A. Yes

B. No

**Answer: A**

**Explanation:**

References:

<https://docs.microsoft.com/en-us/virtualization/windowscontainers/about/>

**NEW QUESTION 4**

Note: This question Is part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to It, As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains multiple Hyper-V hosts.

You need to deploy several critical line-to-business applications to the network to meet the following requirements:

\*The resources of the applications must be isolated (rom the physical host.

\*Each application must be prevented from accessing the resources of the other applications.

\*The configurations of the applications must be accessible only from the operating system that hosts the application.

Solution: You deploy a separate Hyper-V container for each application. Does this meet the goal?

- A. Yes  
B. No

**Answer:** A

**Explanation:**

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

**NEW QUESTION 5**

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

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

**Answer:** C

**Explanation:**

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

Feature	Remote Desktop	Windows Defender Remote Credential Guard	Restricted Admin mode
<b>Protection benefits</b>	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 <i>only</i> 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
<b>Version support</b>	The remote computer can run any Windows operating system	Both the client and the remote computer must be running <b>at least Windows 10, version 1607, or Windows Server 2016.</b>	The remote computer must be running <b>at least patched Windows 7 or patched Windows Server 2008 R2.</b>  For more information about patches (software updates) related to <b>Restricted Admin</b> mode, see <a href="#">Microsoft Security Advisory 2871997</a> .
<b>Helps prevent</b>	N/A	<ul style="list-style-type: none"> <li>• Pass-the-Hash</li> <li>• Use of a credential after disconnection</li> </ul>	<ul style="list-style-type: none"> <li>• Pass-the-Hash</li> <li>• Use of domain identity during connection</li> </ul>
<b>Credentials supported from the remote desktop client device</b>	<ul style="list-style-type: none"> <li>• <b>Signed on</b> credentials</li> <li>• <b>Supplied</b> credentials</li> <li>• <b>Saved</b> credentials</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Signed on</b> credentials only</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Signed on</b> credentials</li> <li>• <b>Supplied</b> credentials</li> <li>• <b>Saved</b> credentials</li> </ul>

**NEW QUESTION 6**

HOTSPOT

Your network contains an Active Directory forest named contoso.com. The forest has Microsoft Identity Manager (MIM) 2016 deployed. You implement Privileged Access Management (PAM).

You need to request privileged access from a client computer in contoso.com by using PAM.

How should you complete the Windows PowerShell script? To answer, select the appropriate options in the answer area.

**Answer Area**

\$PAM =  | ? { \$\_.DisplayName -eq "CorpAdmins" }

-role \$PAM

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

\$PAM = Get-PAMRoleForRequest | ? { \$\_.DisplayName -eq "CorpAdmins" } New-PAMRequest -role \$PAM

References:

<https://technet.microsoft.com/en-us/library/mt604089.aspx> <https://technet.microsoft.com/en-us/library/mt604084.aspx>

**NEW QUESTION 7**

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Serve1, that runs Windows Server 2016.

A technician is testing the deployment of Credential Guard on Server1. You need to verify whether Credential Guard is enabled on Server1. What should you do?

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

**Answer:** B

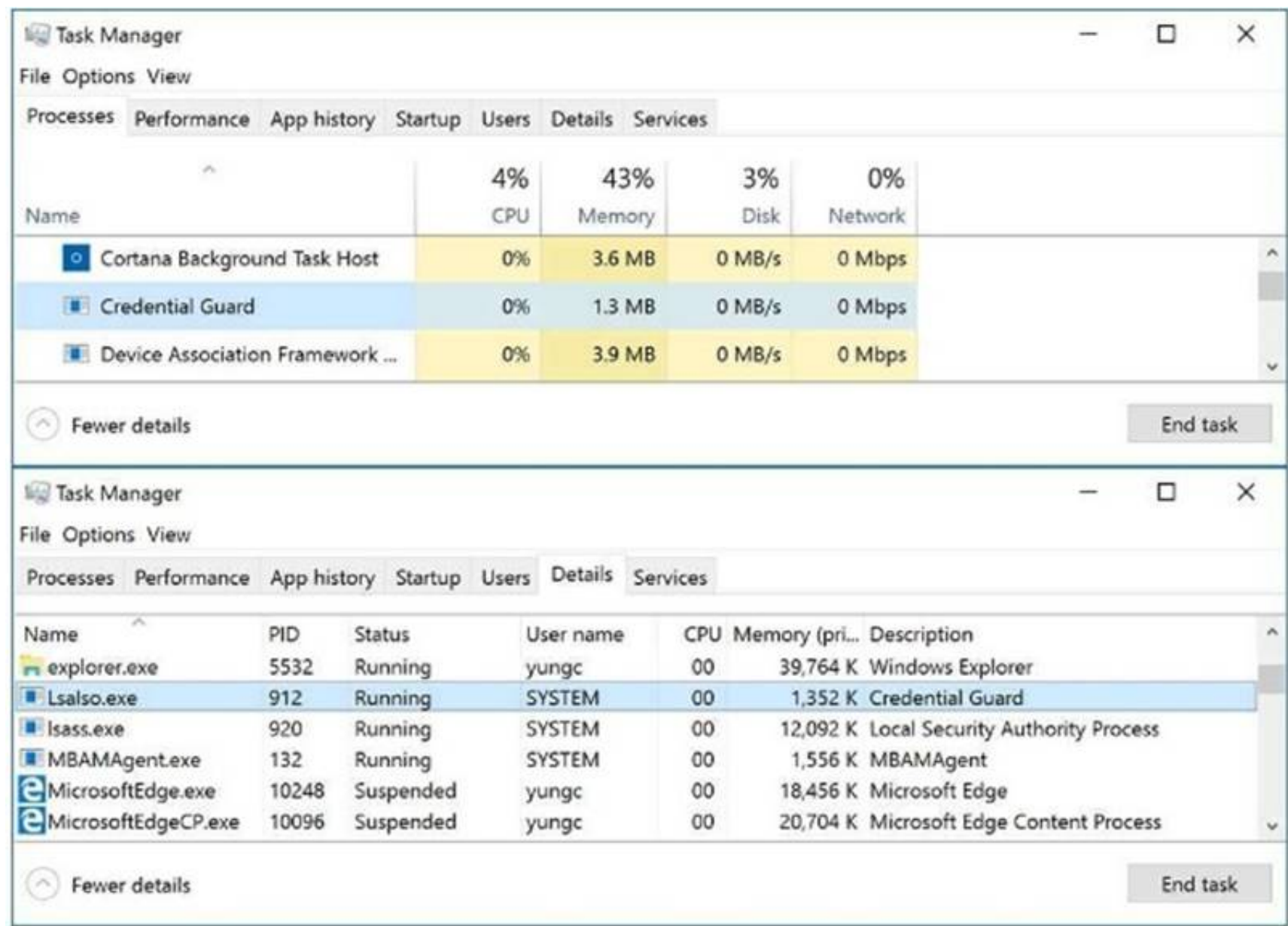
**Explanation:**

<https://yungchou.wordpress.com/2016/10/10/credential-guard-made-easy-in-windows-10-version-1607/>

The same as before, once Credential Guard is properly configured, up and running.

You should find in Task Manager the 'Credential Guard' process and 'Isaiso.exe' listed in the Details page as below.





### NEW QUESTION 8

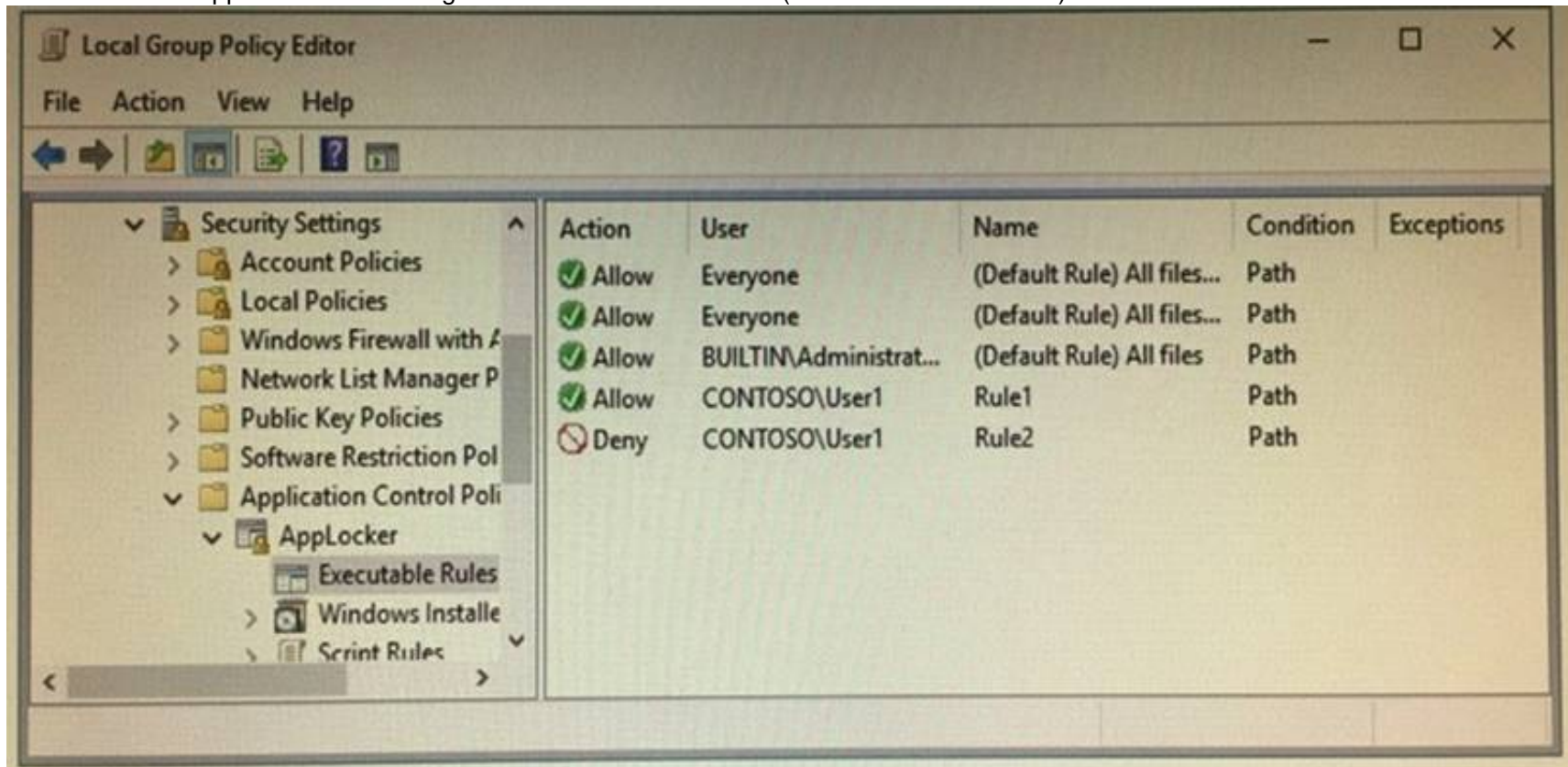
#### HOTSPOT

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

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

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

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



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

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

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

Statements	Yes	No
On Server1, User1 can run D:\Folder2\App1.exe.	<input type="radio"/>	<input type="radio"/>
On Server1, User1 can run D:\Folder1\Program1.exe.	<input type="radio"/>	<input type="radio"/>
If Program1.exe is copied from D:\Folder1 to D:\Folder2, User1 can run Program1.exe on Server1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 9**

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

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

**Answer:** A

**Explanation:**

“File Explorer” = “Windows Explorer”.  
[https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/deploy-a-centralaccess- policy– demonstration-steps-#BKMK\\_1.4](https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/deploy-a-centralaccess- policy– demonstration-steps-#BKMK_1.4)

**NEW QUESTION 10**

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

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

**Answer:** A



#### NEW QUESTION 10

Note: This question is port of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question In the series. Each question is Independent of the other questions In this series. Information and details provided in a question apply only to that question.  
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016 and a Nano Server named Nano1. Nano1 has two volumes named C and D.  
You are signed in to Server1.  
You need to configure Data Deduplication on Nano1. Which tool should you use?

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

**Answer: C**

#### Explanation:

Either use PowerShell Remoting to Nano1 and use "Enable-DedupVolume" cmdlet, however ,there is no such choice for this question; or From Server1, connect it's server manager to remotely manage Nano1 and enable Data Deduplication for volumes on Nano1  
<https://channel9.msdn.com/Series/Nano-Server-Team/Server-Manager-managing-Nano-Server>

#### To assign a central access policy to a file server

1. In Hyper-V Manager, connect to server FILE1. Log on to the server by using contoso\administrator with the password: **pass@word1**.
2. Open an elevated command prompt and type: **gpupdate /force**. This ensures that your Group Policy changes take effect on your server.
3. You also need to refresh the Global Resource Properties from Active Directory. Open an elevated Windows PowerShell window and type `Update-FSRMClassificationpropertyDefinition` . Click ENTER, and then close Windows PowerShell.

#### Tip

You can also refresh the Global Resource Properties by logging on to the file server. To refresh the Global Resource Properties from the file server, do the following

- a. Logon to File Server FILE1 as contoso\administrator, using the password **pass@word1**.
- b. Open File Server Resource Manager. To open File Server Resource Manager, click **Start**, type **file server resource manager**, and then click **File Server Resource Manager**.
- c. In the File Server Resource Manager, click **File Classification Management** , right-click **Classification Properties** and then click **Refresh**.

4. Open **Windows Explorer**, and in the left pane, click drive D. Right-click the **Finance Documents** folder, and click **Properties**.
5. Click the **Classification** tab, click **Country**, and then select **US** in the **Value** field.
6. Click **Department**, then select **Finance** in the **Value** field and then click **Apply**.

#### NEW QUESTION 12

##### 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:

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

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

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

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

PS C:\windows\system32>
```

#### NEW QUESTION 15

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



Start of repeated scenario

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

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

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

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

End of repeated scenario

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

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

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

**Answer: D**

**Explanation:**

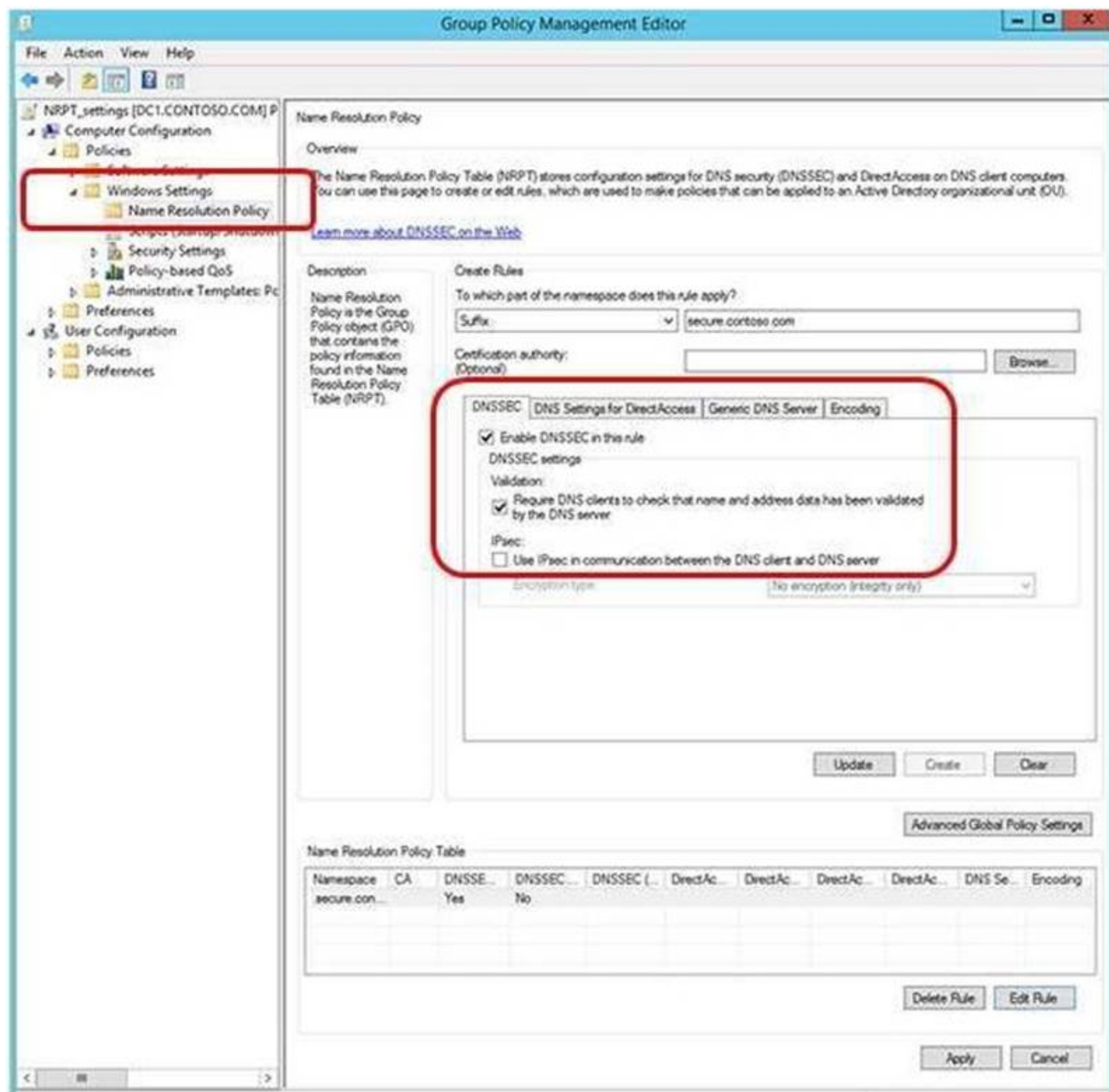
The NRPT is a table that contains rules that you can configure to specify DNS settings or special behavior for names or namespaces.

The NRPT can be configured using the Group Policy Management Editor under Computer Configuration

\\Policies\\Windows Settings\\Name Resolution Policy, or with Windows PowerShell.

If a DNS query matches an entry in the NRPT, it is handled according to settings in the policy. Queries that do not match an NRPT entry are processed normally.

You can use the NRPT to require that DNSSEC validation is performed on DNS responses for queries in the namespaces that you specify.



#### NEW QUESTION 19

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 BitLocker 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&MSPPErrors=2147217396#BKMK\\_rec1](https://technet.microsoft.com/en-us/library/jj679890%28v=ws.11%29.aspx?f=255&MSPPErrors=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.

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

### Reference

This policy setting is applied when you turn on BitLocker.

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

For more information about adding data recovery agents, see [BitLocker Basic Deployment](#).

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

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

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

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

### NEW QUESTION 22

Your network contains an Active Directory domain named 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 25

#### HOTSPOT

Your network contains an Active Directory domain named adatum.com. The domain contains a file server named Server1 that runs Windows Server 2016.

You have an organizational unit (OU) named OU1 that contains Server1. You create a Group Policy object (GPO) named GPO1 and link GPO1 to OU1.

A user named User1 is a member of group named Group1. The properties of User1 are shown in the User1 exhibit (Click the Exhibit button.)



**User1 Properties**

Member Of: Dialin Environment Sessions

Remote control Remote Desktop Services Profile COM+

General Address Account Profile Telephones Organization

Job Title: Consultant

Department: IT

Company: A. Datum Ltd.

Manager:

Name: User2

Change... Properties Clear

Direct reports:

OK Cancel Apply Help

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

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

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

**Auditing Entry for Global File SACL**

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

Type: Success

Permissions:

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

Clear all

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

Manage grouping

User department Equals Value IT Remove

Or

User manager Equals Value User2 Remove

Add a condition

OK Cancel

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

Statements	Yes	No
From File Explorer, when User1 double-clicks <b>File1.doc</b> , an event will be logged.	<input type="radio"/>	<input type="radio"/>
From File Explorer, when User1 double-clicks <b>File2.doc</b> , an event will be logged.	<input type="radio"/>	<input type="radio"/>
From Microsoft Word, when User1 attempts to save changes to File1.doc, an event will be logged.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 27**

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 31**

**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:	<input type="checkbox"/> An encryption-supported virtual machine <input type="checkbox"/> A shielded virtual machine
VM2:	<input type="checkbox"/> An encryption-supported virtual machine <input type="checkbox"/> A shielded virtual machine
VM3:	<input type="checkbox"/> An encryption-supported virtual machine <input type="checkbox"/> 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) <sup>1</sup>	Supported	Disabled (cannot be enabled)

### NEW QUESTION 35

#### 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

#### ① 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:

Copy

```
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 37

Your network contains an Active Directory forest named contoso.com. The forest functional level is Windows Server 2012. The forest contains a single domain. The domain contains multiple Hyper-V hosts.

You plan to deploy guarded hosts.

You deploy a new server named Server22 to a workgroup.

You need to configure Server22 as a Host Guardian Service server.

What should you do before you initialize the Host Guardian Service on Server22?

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

**Answer:** D

#### Explanation:

<https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shieldedvm/guarded-fabricchoose-where-to-install-hgs>

The only technical requirement for installing HGS in an existing forest is that it be added to the root domain; non-root domains are not supported.

### NEW QUESTION 40

Windows Firewall rules can be configured using PowerShell.

The "Set-NetFirewallProfile" cmdlet configures settings that apply to the per-profile configurations of the Windows Firewall with Advanced Security.

What is the default setting for the AllowInboundRules parameter when managing a GPO?

- A. FALSE
- B. NotConfigured

**Answer:** B

#### Explanation:

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

### NEW QUESTION 44

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

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

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

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

You verify that User1 is unable to run App2.exe on Server1.

Which changes will allow User1 to run D:\Folder1\Program.exe and D:\Folder2\App2.exe? Choose Two.

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

**Answer:** AF

**Explanation:**

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

**Important**

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

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

For “D:\Folder1\Program.exe”, it is originally explicitly denied due to Rule1, when moving the “Program.exe” out of “D:\Folder1\”, it does not match Rule1.

Assume that “Program.exe” is moved to “D:\Folder2”, it matches an Explicit Allow rule for group “BUILTIN

\Administrators” which User1 is a member of, therefore A is correct.

For “App2”.exe, it matches a Explicit Deny rule using its File Hash (created File content), no matter where you move it to, or how you rename it, it would still match Rule2.

Only changing the file content of App2.exe would let it no longer match the explicit deny hash-based rule

“Rule2”.

By upgrading its version and content, it will generate a new hash. so F is correct.

**NEW QUESTION 48**

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](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 52**

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



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

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.

All laptops are protected by using BitLocker Drive Encryption (BitLocker).

You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.

An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1.

A GPO named GP2 is linked to OU2.

All computers receive updates from Server1. You create an update rule named Update1.

You need to prepare the environment to support applying Update1 to the laptops only. What should you do? Choose Two.

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

**Answer:** DE

**Explanation:**

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

## Automatically Approving Updates for Detection


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

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

### To automatically approve updates for detection

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

Add Rule ✕

 Select which updates to approve and the groups for which to approve them.

Step 1: Select properties

☒ When an update is in a specific classification  
☐ When an update is in a specific product  
☐ Set a deadline for the approval

Step 2: Edit the properties (click an underlined value)

When an update is in any classification

Approve the update for all computers



#### NEW QUESTION 57

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

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

You purchase a Microsoft Azure subscription, and you create three Microsoft Operations

Management Suite (OMS) workspaces named Workspace1, Workspace2, and Workspace3

You need to deploy Microsoft Monitoring Agent to the servers to meet the following requirements:

- Antimalware data from all the servers must be visible in Workspace1.
- Security and audit data from the domain controllers and the virtualization hosts must be visible in Workspace2.
- System update data from all the servers in all the workgroups must be visible in Workspace& How many OMS agents should you deploy?

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

**Answer:** C

#### Explanation:

-Antimalware data from all the servers must be visible in Workspace1.

-Security and audit data from the domain controllers and the virtualization hosts must be visible in Workspace2.

-System update data from all the servers in all the workgroups must be visible in Workspace& "All the servers" mean all 5 domain controllers, plus all member servers (physical and virtual, domain and workgroup) and virtualization hosts, so there are no exemptions.

All servers in the above table mentioned must install OMS Microsoft Monitoring agents

#### NEW QUESTION 58

You have two computers configured as shown in the following table.

Computer name	Operating system	Workgroup/domain
Client1	Windows 10 Pro, version 1607	Workgroup
Server1	Windows Server 2016 Standard	Domain named adatum.com

You need to ensure that the credentials that you use to establish Remote Desktop sessions from Client1 to Server1 are protected by using Remote CredentialGuard.

- A. Join Client1 to the domain.
- B. Remove Server1 from the domain.
- C. Upgrade Server1 to Windows Server 2016 Datacenter.
- D. Upgrade Client1 to Windows 10 Enterpris

**Answer:** A

#### Explanation:

<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.

#### NEW QUESTION 59

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:

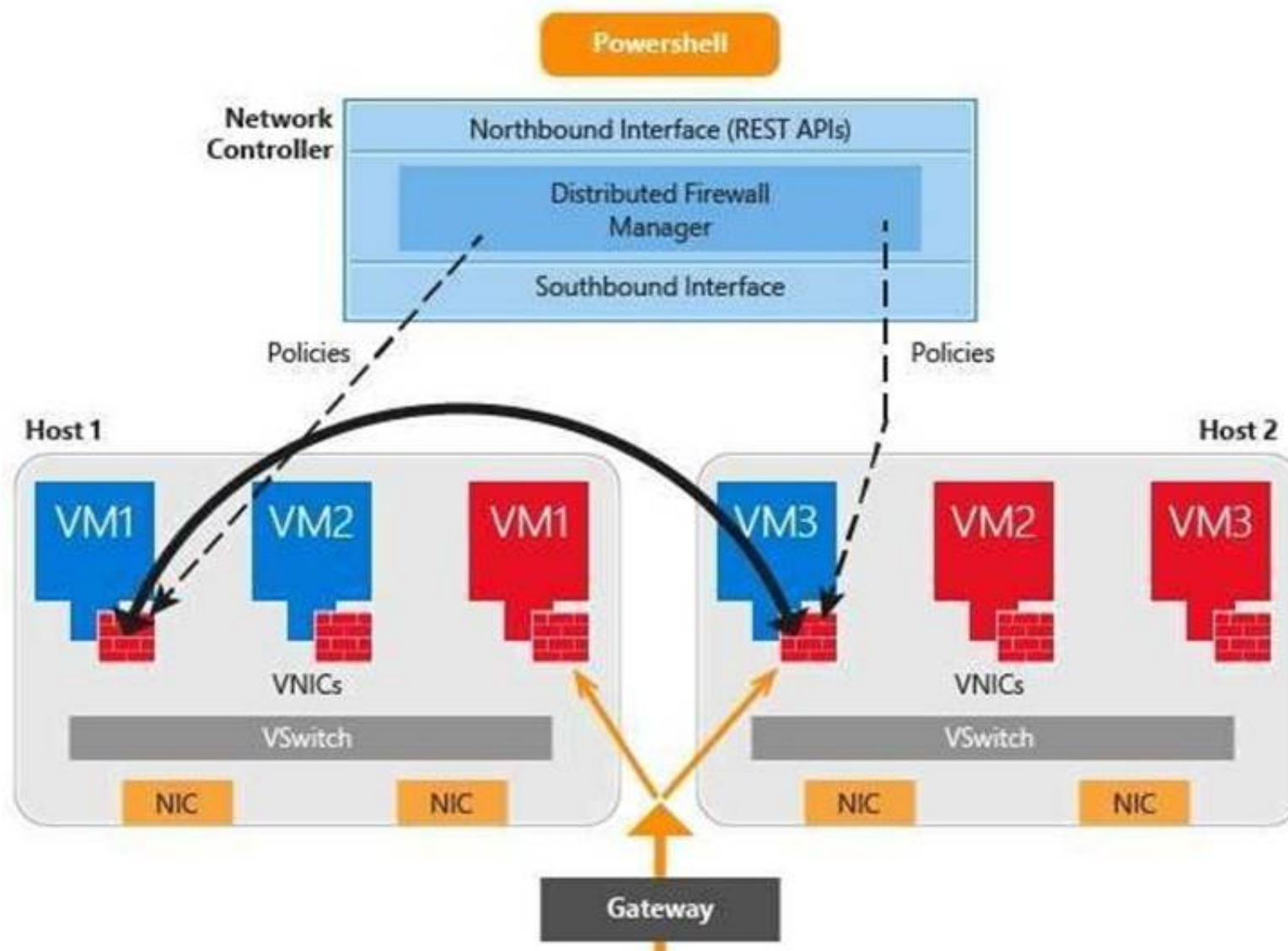
Datacenter Firewall is a new service included with Windows Server 2016. It is a network layer, 5- tuple (protocol, source and destination port numbers, source and destination IP addresses), stateful, multitenant firewall. When deployed and offered as a service by the serviceprovider, tenant administrators 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 64

You are creating a Nano Server image for the deployment of 10 servers.

You need to configure the servers as guarded hosts that use Trusted Platform Module (TPM) attestation.

Which three packages should you include in the Nano Server image? Each correct answer presents part of the solution.

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



**Answer:** ABF

**Explanation:**

<https://docs.microsoft.com/en-us/system-center/vmm/guarded-deploy-host?toc=/windowsserver/virtualization/toc.json>

For an SCVMM Managed Nano Server Hyper-V case:

If your host is running Nano Server Hyper-V host, it should have the Compute, SCVMM-Package, SCVMMCompute, SecureStartup, and ShieldedVM packages installed.

<https://docs.microsoft.com/en-us/windows-server/get-started/deploy-nano-server>

For an standalone Nano Server Hyper-V host, no SCVMM related packages are required, only Compute, SecureStartup, and ShieldedVM packages are required.

This table shows the roles and features that are available in this release of Nano Server, along with the Windows PowerShell options that will install the packages for them.

Some packages are installed directly with their own Windows PowerShell switches (such as -

Compute); others you install by passing package names to the -

Package parameter, which you can combine in a comma-separated list. You can dynamically list available packages using the Get-NanoServerPackage cmdlet.

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

**NEW QUESTION 68**

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

The relevant objects in the domain are configured as shown in the following table.

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

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

- A. Yes
- B. No

**Answer:** A

**Explanation:**

[https://technet.microsoft.com/en-us/library/cc771990\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc771990(v=ws.11).aspx) Backup Operators



Members of this group can back up and restore files on a computer, regardless of any permissions that protect those files.  
This is because the right to perform a backup takes precedence over all file permissions. Members of this group cannot change security settings.

**NEW QUESTION 70**

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 74**

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 76**

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 79**

You have a server named Server1 that runs Windows Server 2016.

You need to identify whether IPsec tunnel authorization is configured on Server1. Which cmdlet should you use?

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

**Answer: A**

**Explanation:**

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

```
PS C:\> Get-NetIPSecRule

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

**NEW QUESTION 84**

You have a server named Server1 that runs Windows Server 2016. You need to view all of the inbound rules on Server1.

Which cmdlet should you use?



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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 85**

You plan to enable Credential Guard on four servers. Credential Guard secrets will be bound to the TPM.  
The servers run Windows Server 2016 and are configured as shown in the following table.

Server name	Trusted Platform Module (TPM) version	UEFI firmware version	Hypervisor installed	Platform
Server1	1.2	2.3.2	Hyper-V	Physical
Server2	2.0	2.3.1	Hyper-V	Physical
Server3	2.0	2.3.2	None	Physical
Server4	2.0	2.3.2	Hyper-V	Generation 2 virtual machine

Which of the above server you could enable Credential Guard?

- A. Server1
- B. Server2
- C. Server3
- D. Server4

**Answer: D**

**Explanation:**

<https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guardrequirements> Hardware and software requirements  
To provide basic protections against OS level attempts to read Credential Manager domain credentials, NTLM and Kerberos derived credentials, Windows Defender Credential Guard uses:  
-Support for Virtualization-based security (required)  
-Secure boot (required)  
-TPM 2.0 either discrete or firmware (preferred – provides binding to hardware)-UEFI lock (preferred – prevents attacker from disabling with a simple registry key change)

**NEW QUESTION 89**

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 91**

Your network contains an Active Directory domain.  
The domain contains two organizational units (OUs) named ProdOU and TestOU.  
All production servers are in ProdOU. All test servers are in TestOU. A server named Server1 is in TestOU.  
You have a Windows Server Update Services (WSUS) server named WSUS1 that runs Windows Server 2016.  
All servers receive updates from WSUS1.  
WSUS is configured to approve updates for computers in the Test computer group automatically. Manual approval is required for updates to the computers in the Production computer group.  
You move Server1 to ProdOU, and you discover that updates continue to be approved and installed automatically on Server1.  
You need to ensure that all the servers in ProdOU only receive updates that are approved manually. What should you do?

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

**Answer: B**

**Explanation:**

Updates in WSUS are approved against “Computer Group” , not AD OUs. For this example, to prevent Server1 to install automatically approved updates, you have to remove Server1 from “Test” computer group and add Server1 into “Production” computer group in WSUS console, manually or use the WSUS GPO Client-Side Targeting feature.

<https://technet.microsoft.com/en-us/library/cc720450%28v=ws.10%29.aspx?f=255&MSPPErr=-2147217396>

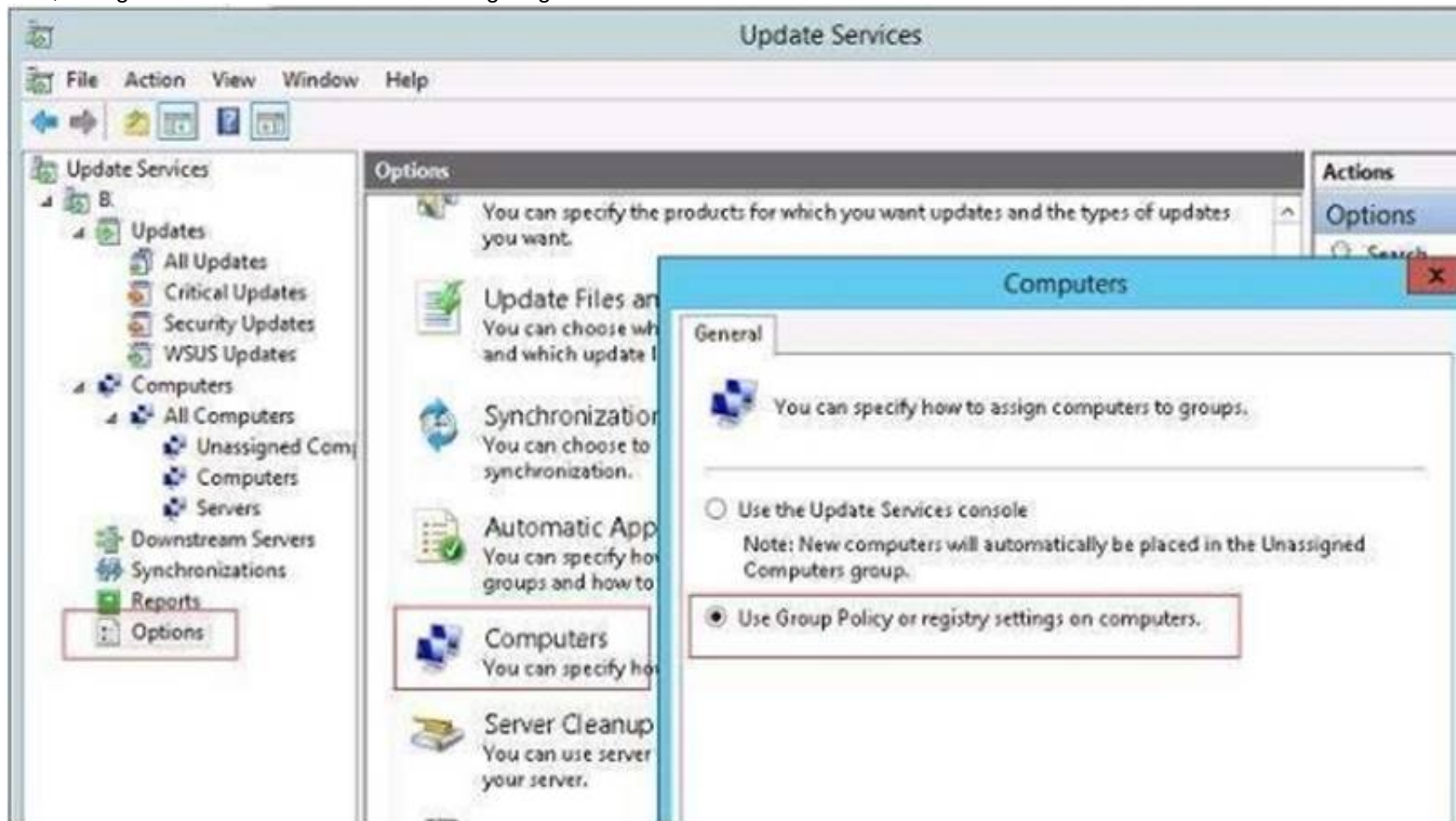
With client-side targeting, you enable client-computers to add themselves to the computer groups you create in the WSUS console.

You can enable client-side targeting through Group Policy (in an Active Directory network environment) or by editing registry entries (in a non-Active Directory network environment) for the client computers.

When the WSUS client computers connect to the WSUS server, they will add themselves into the correct computer group.

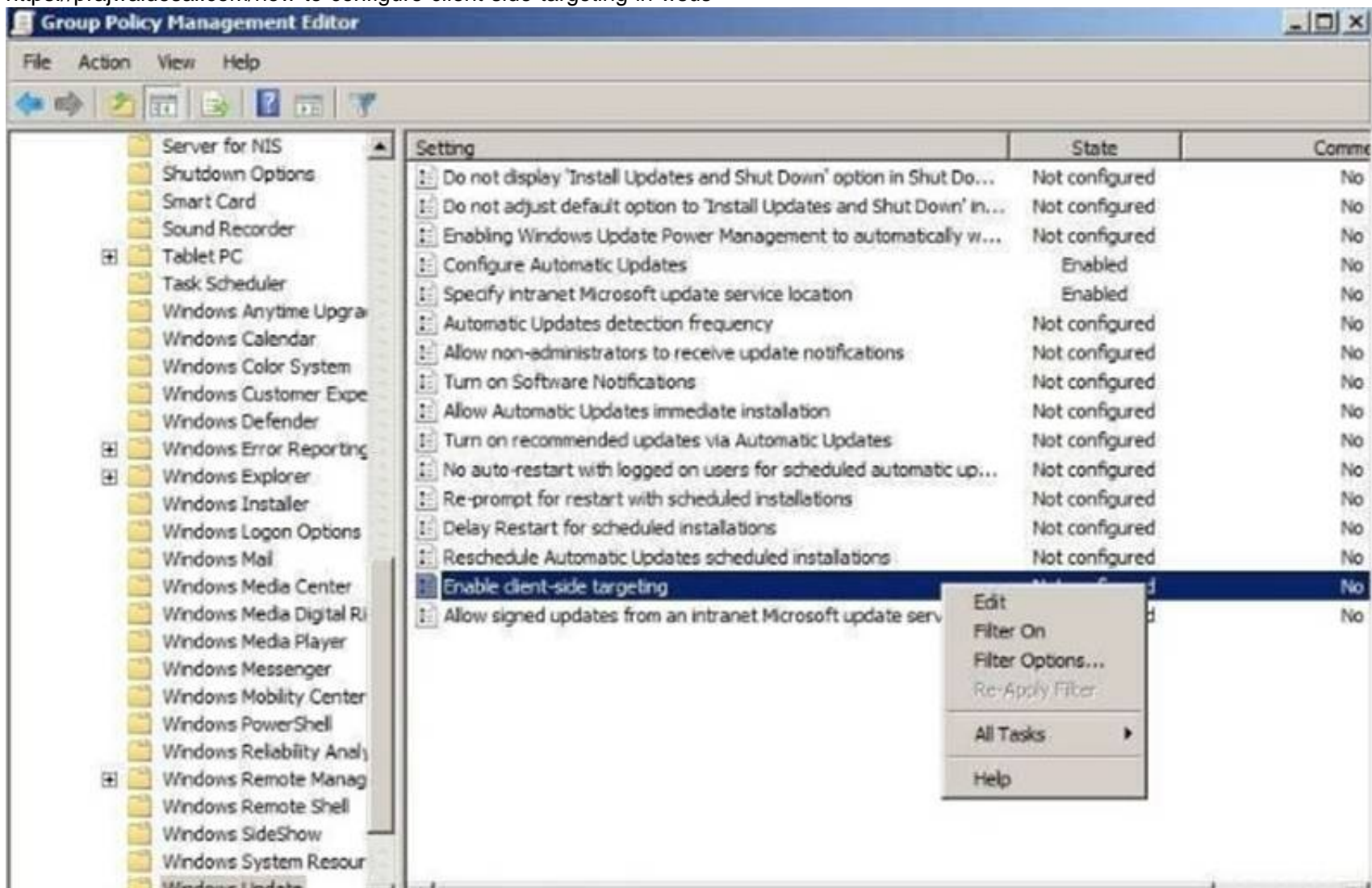
Client-side targeting is an excellent option if you have many client computers and want to automate the process of assigning them to computer groups.

First, configure WSUS to allow Client Site Targeting.

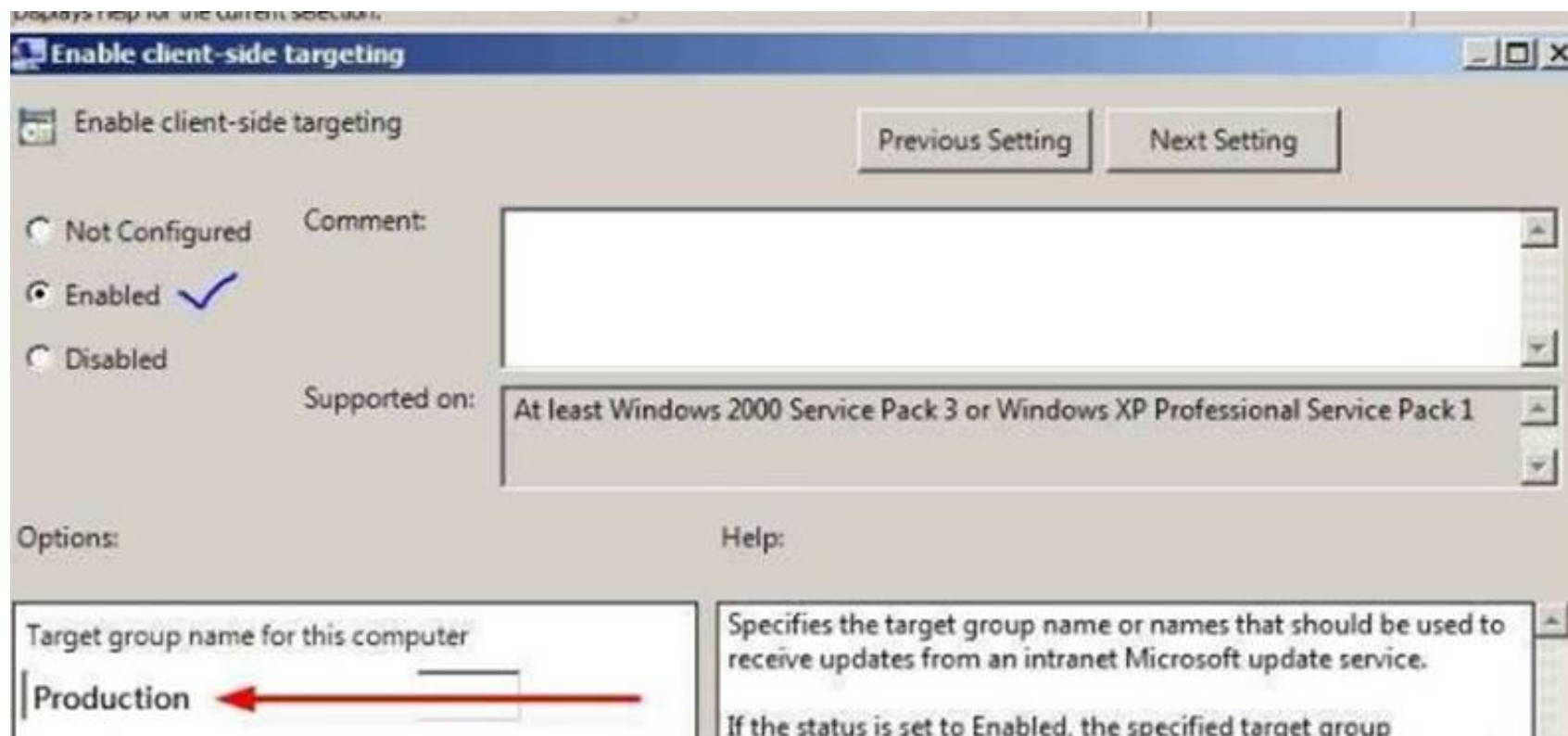


Secondly, configure GPO to affect “ProdOU” , so that Server1 add itself to “Production” computer group.

<https://prajwaldesai.com/how-to-configure-client-side-targeting-in-wsus>







#### NEW QUESTION 95

Your network contains an Active Directory forest named contoso.com. The forest contains three domains. All domain controllers run Windows Server 2016. You deploy a second Active Directory forest named admin.contoso.com. The forest contains a domain member server named Server1. Server1 has Microsoft Identity Manager (MIM) 2016 deployed. You need to implement Privileged Access Management (PAM) and to use admin.contoso.com as an administrative forest. Which two actions should you perform? Each correct answers presents part of the solution.

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

**Answer:** BF

#### Explanation:

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

## Establish trust on PAMSRV

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

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

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

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

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

#### NEW QUESTION 99

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

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

You have an organizational unit (OU) named Marketing that contains the computers in the marketing department.

You have an OU named Finance that contains the computers in the finance department. You have an OU named AppServers that contains application servers.

A Group Policy object (GPO) named GP1 is linked to the Marketing OU. A GPO named GP2 is linked to the AppServers OU.

You install Windows Defender on Nano1.

You need to configure Nano1 as a Hyper-V Host. Which command should you run?

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

**Answer:** E

**Explanation:**

[https://docs.microsoft.com/en-us/windows-server/get-started/deploy-nano-server#BKMK\\_online](https://docs.microsoft.com/en-us/windows-server/get-started/deploy-nano-server#BKMK_online) The Nano Server package “Microsoft-NanoServer-Compute-Package” includes the Hyper-V role for a Nano Server host.

Moreover, the Install-WindowsFeature or Add-WindowsFeature cmdlet are NOT available on a Nano Server.

**NEW QUESTION 101**

Your network contains an internal network and a perimeter network. The internal network contains an Active Directory forest named contoso.com.

You deploy five servers to the perimeter network.

All of the servers run Windows Server 2016 and are the members of a workgroup.

You need to apply a security baseline named Perimeter.inf to the servers in the perimeter network. What should you use to apply Perimeter.inf?

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

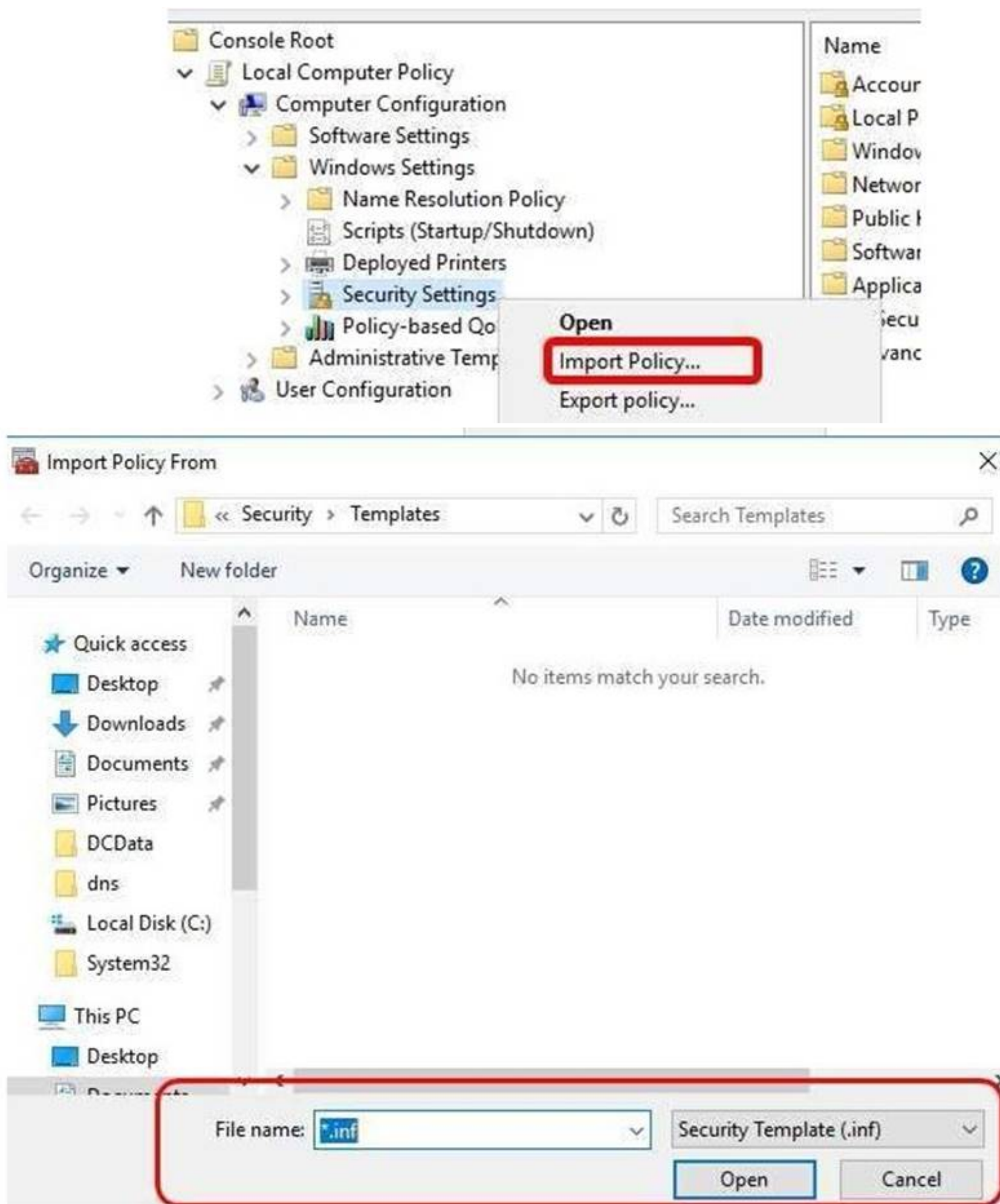
**Answer:** A

**Explanation:**

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

<https://msdn.microsoft.com/en-us/library/bb742512.aspx>





#### NEW QUESTION 105

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?

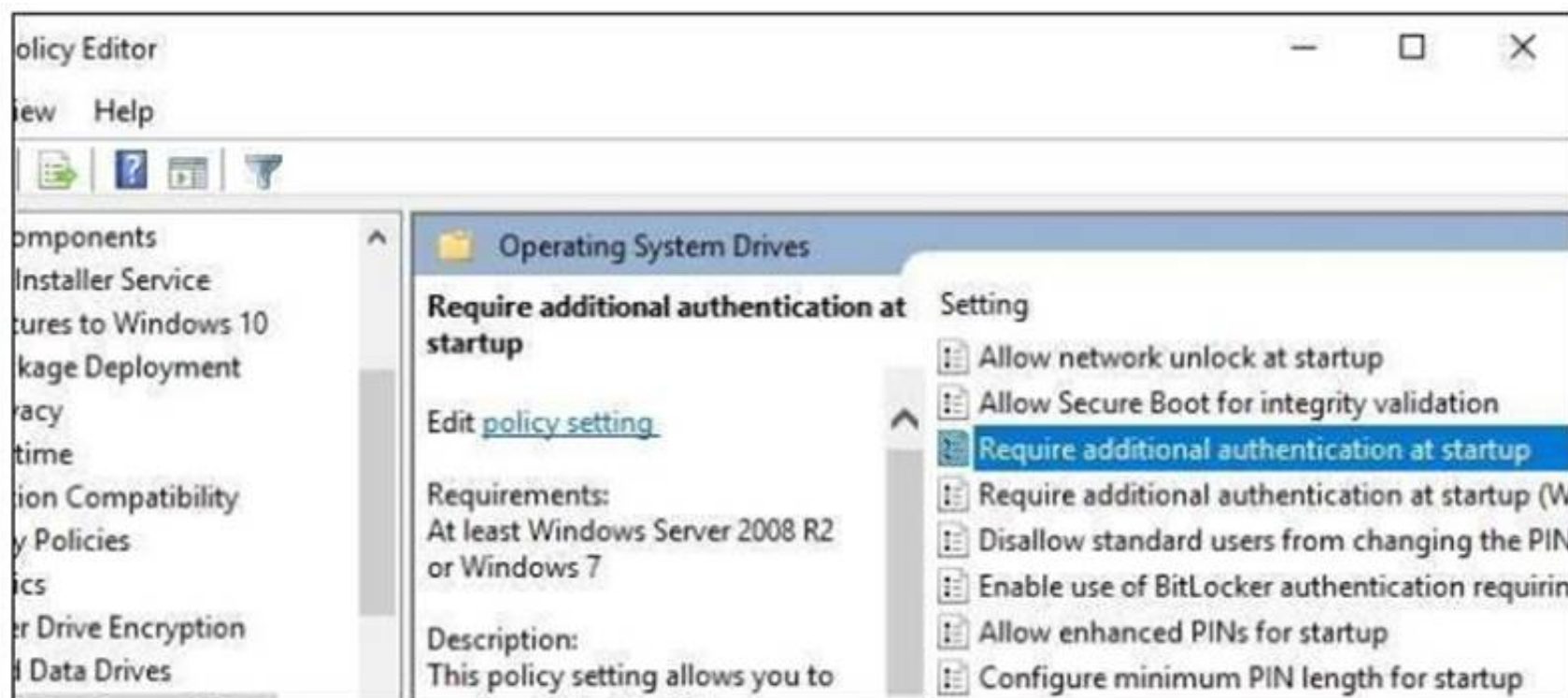
- A. From Server1, install the BitLocker feature.
- B. From Server1, enable nested virtualization for VM1.
- C. From VM1, configure the Require additional authentication at startup Group Policy setting.
- D. From VM1, configure the Enforce drive encryption type on fixed data drives Group Policy setting.

**Answer: C**

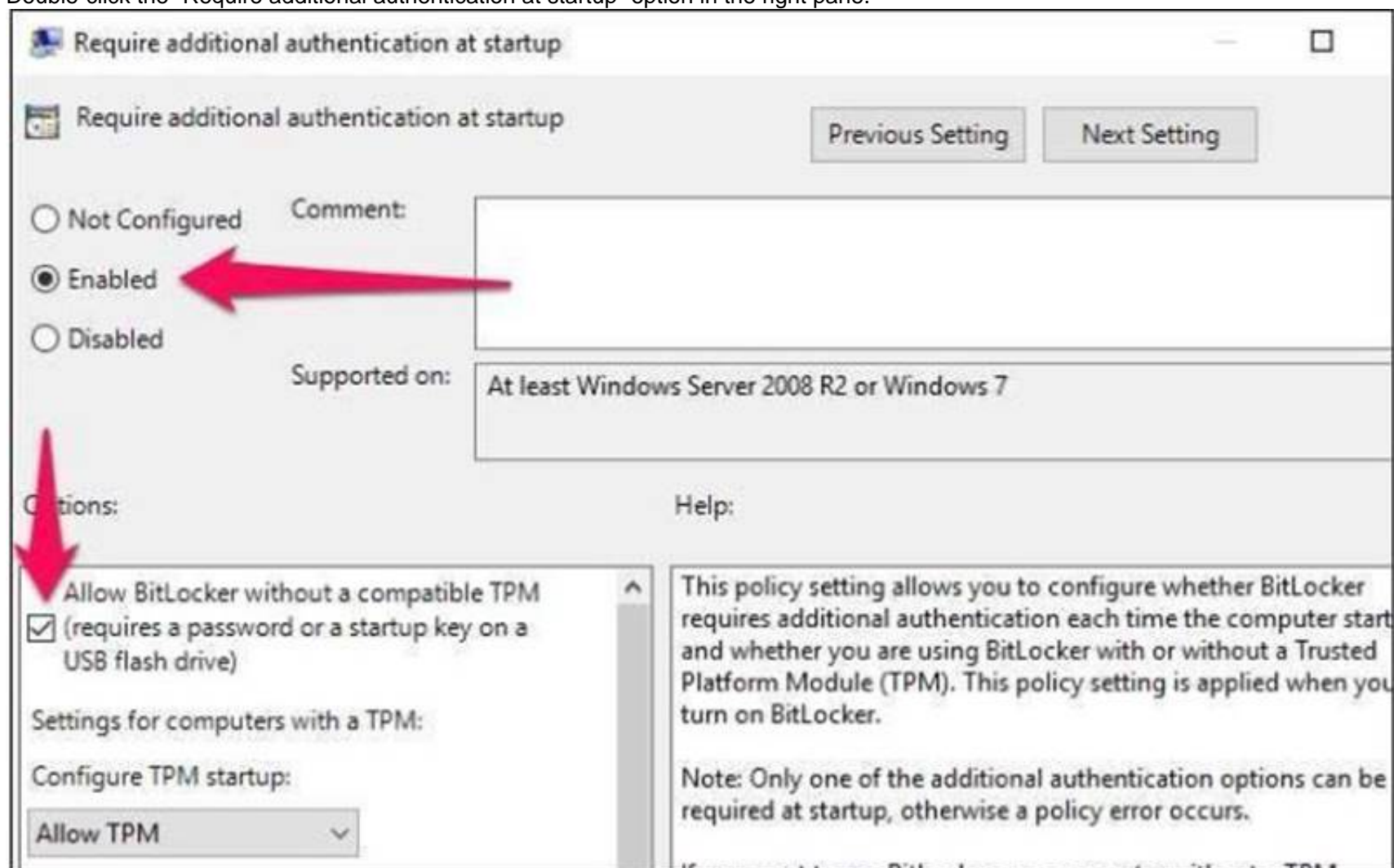
#### Explanation:

<https://www.howtogeek.com/howto/6229/how-to-use-bitlocker-on-drives-without-tpm/>

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



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



Select "Enabled" at the top of the window, and ensure the "Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)" checkbox is enabled here.

Click "OK" to save your changes. You can now close the Group Policy Editor window. Your change takes effect immediately—you don't even need to reboot.

#### NEW QUESTION 108

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 111

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
<div style="border: 1px solid #ccc; min-height: 100px;"></div>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">                     &lt;&lt; Move                 </div> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block; margin-top: 5px;">                     Remove &gt;&gt;                 </div>	<div style="border: 1px solid #ccc; padding: 5px;">                     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                 </div>

- A. Mastered
- B. Not Mastered

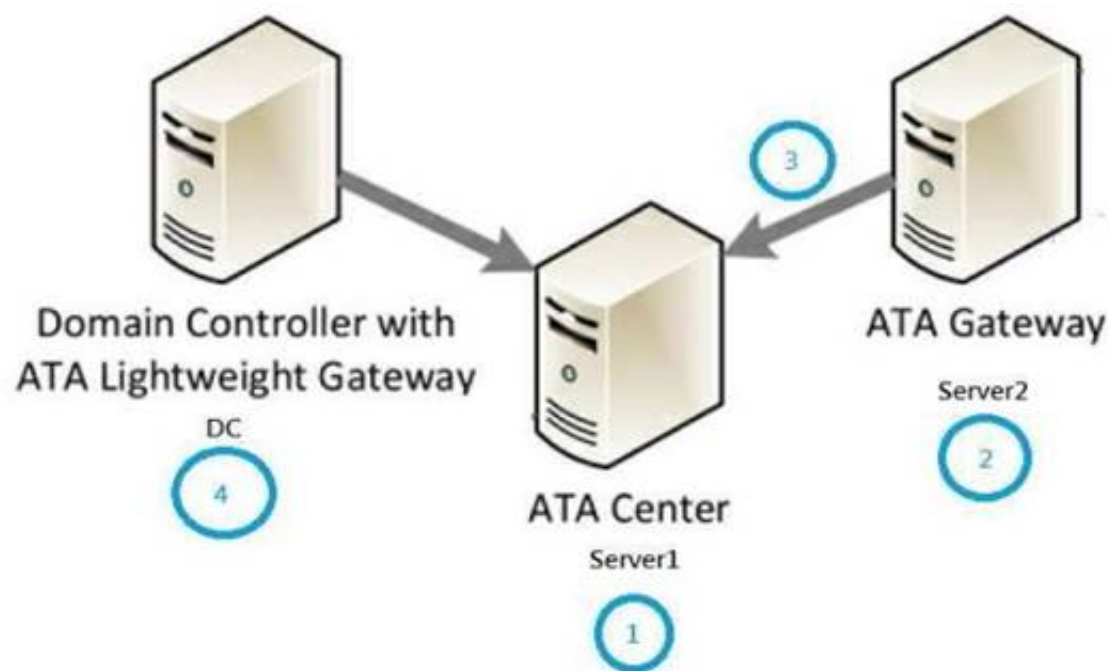
**Answer:** A

#### 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 112

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

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

**Answer: C**

#### Explanation:

[https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit\\_script](https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit_script)

The new Detailed Script Tracing feature lets you enable detailed tracking and analysis of Windows PowerShell scripting use on a system.

After you enable detailed script tracing, Windows PowerShell logs all script blocks to the ETW event log, Microsoft-Windows-PowerShell/Operational.

If a script block creates another script block (for example, a script that calls the Invoke-Expression cmdlet on a string), that resulting script block is logged as well. Logging of these events can be enabled through the Turn on PowerShell Script Block Logging Group Policy setting (in GPO Administrative Templates -> Windows Components -> Windows PowerShell).

Answer D is incorrect, since Transcription (Start-Transcript -path <FilePath>) uses a custom output location instead of Event Viewer \ Operational Log

#### NEW QUESTION 116

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

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

**Answer: A**

#### NEW QUESTION 119

Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. The network uses the 172.16.0.0/16 address space.

Computer1 has an application named App1.exe that is located in D:\Apps\. App1.exe is configured to accept connections on TCP port 8080.

You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.

Solution: You configure an inbound rule that allows the TCP protocol on port 8080 and applies to all profiles

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

#### Explanation:

You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.”

Therefore, you should not create firewall rule for all three profiles.

#### NEW QUESTION 120

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. You need to prevent NTLM authentication on Server1.



Solution: From Windows PowerShell, you run the Disable-WindowsOptionalFeature cmdlet. Does this meet the goal?

- A. Yes
- B. No

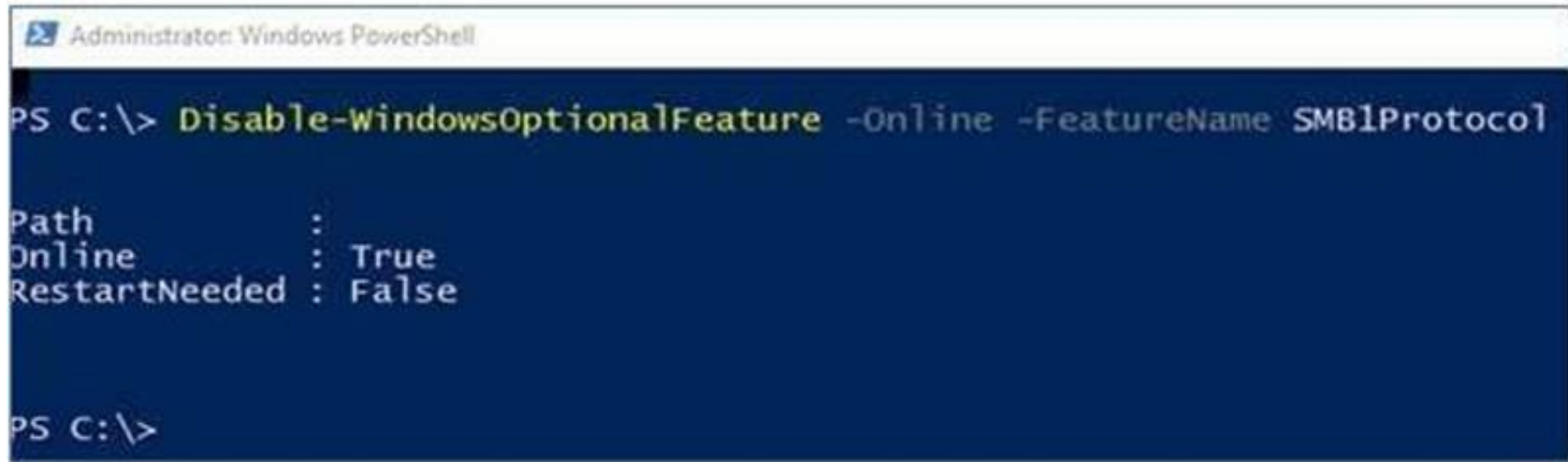
**Answer: B**

**Explanation:**

<https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>

On Client, the PowerShell approach (Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol)

Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol



```
Administrator: Windows PowerShell

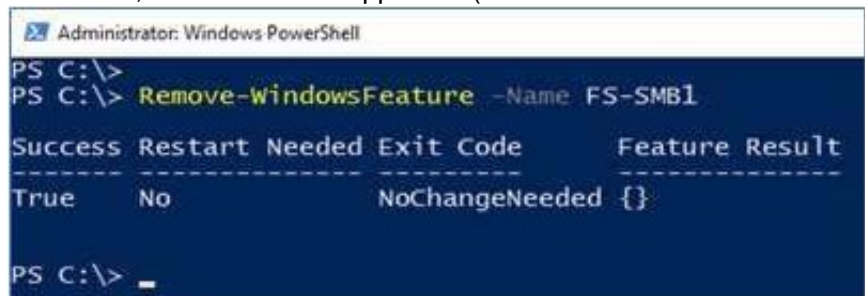
PS C:\> Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

Path           :
Online          : True
RestartNeeded  : False

PS C:\>
```

However, the question asks about Server!

On Server, the PowerShell approach (Remove-WindowsFeature FS-SMB1): Remove-WindowsFeature FS-SMB1



```
Administrator: Windows PowerShell

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

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

PS C:\> _
```

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

**NEW QUESTION 123**

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?

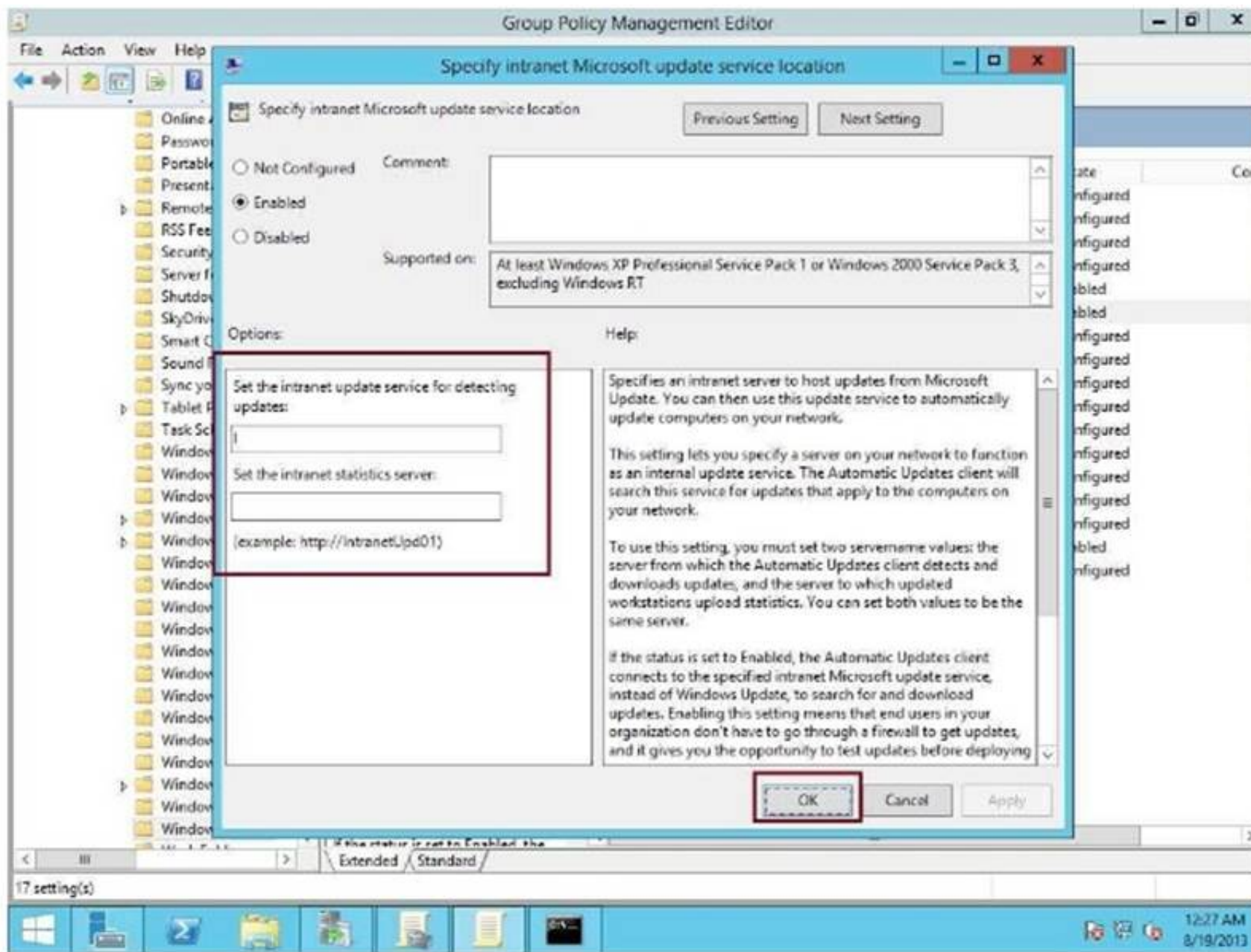
- A. an approval rule
- B. a computer group
- C. a Group Policy object (GPO)
- D. a synchronization rule

**Answer: C**

**Explanation:**

[https://technet.microsoft.com/en-us/library/cc708574\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc708574(v=ws.10).aspx)

Under “Set the intranet update service for detecting updates”, type <http://wsus:8530> Under “Set the intranet statistics server”, type <http://wsus2:8531>



#### NEW QUESTION 125

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

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

**Answer: C**

#### NEW QUESTION 127

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 128

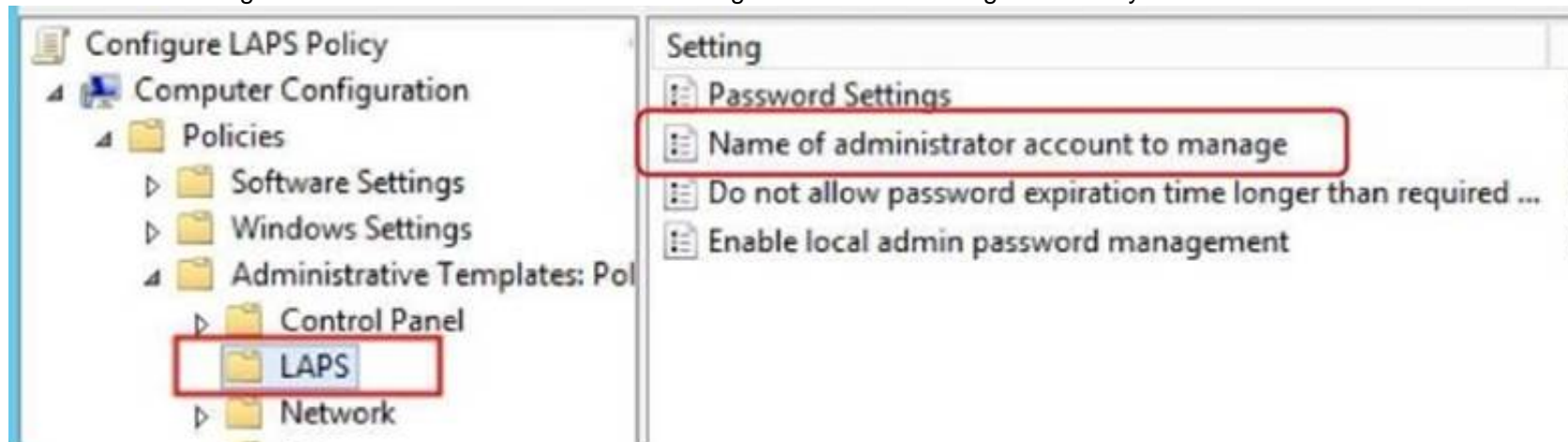
Your network contains an Active Directory domain named contoso.com. All servers in the domain run Windows Server 2016. All client computers run Windows 10. Your company has deployed the Local Administrator Password Solution (LAPS). Client computers in the finance department are located in an organizational 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 Administrator

**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"



#### NEW QUESTION 129

You implement Just Enough Administration (JEA) on several file servers that run Windows Server 2016. The Role Capability file from a server named Server5 contains the following code.

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

Which action can be performed by a user who connects to Server5?

- A. Create a new file share.
- B. Modify the properties of any share.
- C. Stop any process.
- D. View the NTFS permissions of any folder.

**Answer: B**

#### Explanation:

<https://docs.microsoft.com/en-us/powershell/jea/role-capabilities> Focus on the 3rd Visible Cmdlets in this question 'SmbShare\\Set-\*' The PowerShell "SmbShare" module has the following "Set-\*" cmdlets, as reported by "Get- Command -Module SmbShare" command:-

```
Set-SmbBandwidthLimit
Set-SmbClientConfiguration
Set-SmbPathAcl
Set-SmbServerConfiguration
Set-SmbShare
```

The “Set-SmbShare” cmdlet is then visible on Server5’s JEA endpoint, and allows JEA users to modify the properties of any file share.

<https://technet.microsoft.com/en-us/itpro/powershell/windows/smbshare/set-smbshare>

#### NEW QUESTION 132

Your network contains an Active Directory domain named contoso.com. The domain contains 100 servers.

You deploy the Local Administrator Password Solution (LAPS) to the network.

You discover that the members of a group named FinanceAdministrators can view the password of the local Administrator accounts on the servers in an organizational unit (OU) named FinanceServers. You need to prevent the FinanceAdministrators members from viewing the local administrators’ passwords on the servers in FinanceServers.

Which permission should you remove from FinanceAdministrators?

- A. List contents
- B. All extended rights
- C. Read all properties
- D. Read permissions

**Answer: B**

#### Explanation:

[https://blogs.technet.microsoft.com/askpfeplat/2015/12/28/local-administrator-password-solutionQuestions](https://blogs.technet.microsoft.com/askpfeplat/2015/12/28/local-administrator-password-solutionQuestions&AnswersPDFP-123)  
& Answers PDF P-123

lapsimplementation-hints-and-security-nerd-commentaryincludingmini-threat-model/ Access to the password is granted via the “Control Access” right on the attribute.

Control Access is an “Extended Right” in Active Directory, which means if a user has been granted the “All Extended Rights” permission they’ll be able to see passwords even if you didn’t give them permission.

#### NEW QUESTION 133

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

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

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.

All laptops are protected by using BitLocker Drive Encryption (BitLocker). You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.

An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1.

A GPO named GP2 is linked to OU2.

All computers receive updates from Server1. You create an update rule named Update1.

You need to create a Role Capability file on Server3. Which file should you create?

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

**Answer: D**

#### NEW QUESTION 138

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

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

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.

All laptops are protected by using BitLocker Drive Encryption (BitLocker). You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.

An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1.

A GPO named GP2 is linked to OU2.

All computers receive updates from Server1. You create an update rule named Update1.



You need to ensure that AppLocker rules will apply to the marketing department computers. What should you do?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 142**

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

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

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.

All laptops are protected by using BitLocker Drive Encryption (BitLocker). You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.

An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1.

A GPO named GP2 is linked to OU2.

All computers receive updates from Server1. You create an update rule named Update1.

You need to implement BitLocker Network Unlock for all of the laptops. Which server role should you deploy to the network?

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

**Answer: B**

**Explanation:**

<https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-how-to-enablenetwork-unlock> Network Unlock core requirements  
Network Unlock must meet mandatory hardware and software requirements before the feature can automatically unlock domain joined systems. These requirements include:

You must be running at least Windows 8 or Windows Server 2012.

Any supported operating system with UEFI DHCP drivers can be Network Unlock clients.

A server running the Windows Deployment Services (WDS) role on any supported server operating system.

BitLocker Network Unlock optional feature installed on any supported server operating system. A DHCP server, separate from the WDS server.

Properly configured public/private key pairing. Network Unlock Group Policy settings configured.

**NEW QUESTION 144**

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  $>$ ,  $<$ ,  $>=$ ,  $<=$ ,  $\neq$  in the query search bar.

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

	Copy
EventLog=System TimeGenerated>NOW-24HOURS	

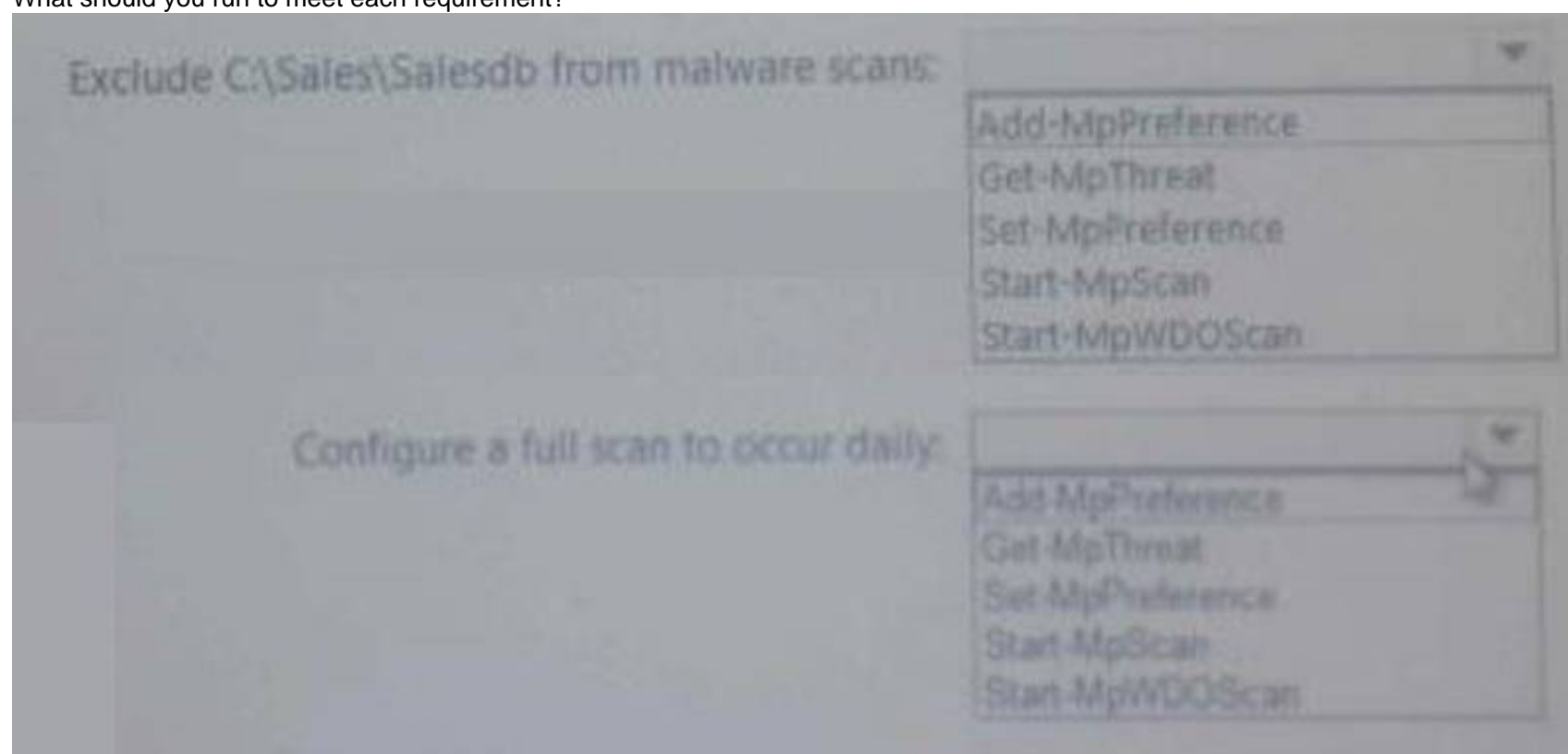
### NEW QUESTION 149

#### HOTSPOT

You have 100 computers that run Windows 10 and are members of a workgroup. You need to configure Windows Defender to meet the following requirements:

- Exclude a C:\Sales\Salesdb from malware scans.
- Configure a full scan to occur daily.

What should you run to meet each requirement?



- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

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

### NEW QUESTION 153

Your network contains an Active Directory domain named contoso.com. The domain contains two DNS servers that run Windows Server 2016. The servers host two zones named contoso.com and admin.contoso.com. You sign both zones.

You need to ensure that all client computers in the domain validate the zone records when they query the zone.

What should you deploy?

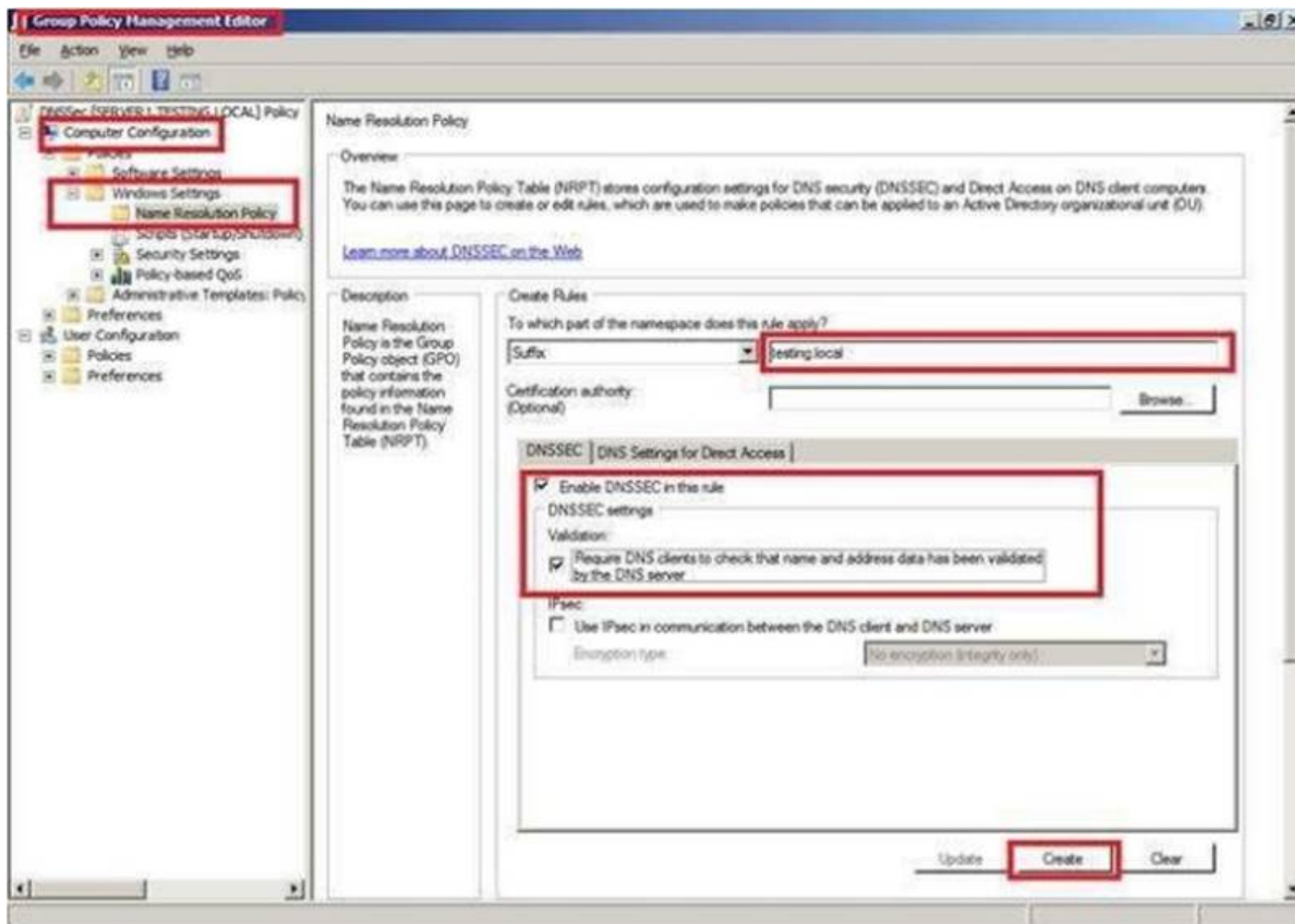
- A. a Microsoft Security Compliance Manager (SCM) policy
- B. a zone transfer policy
- C. a Name Resolution Policy Table (NRPT)
- D. a connection security rule

**Answer:** C

#### Explanation:

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





#### NEW QUESTION 154

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 157

You network contains an Active Directory forest named contoso.com.

All domain controllers run Windows Server 2016 Member servers run either Windows Server 2012 R2 or Windows Server 2016.

Client computers run either Windows 8.1 or Windows 10.

You need to ensure that when users access files in shared folders on the network, the files are encrypted when they are transferred over the network.

Solution: You enable access-based enumeration on all the file shares. Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 160

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

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

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

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

**Answer:** D

**Explanation:**

References:

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

#### NEW QUESTION 165

Your network contains an Active Directory domain named contoso.com.

You download Microsoft Security Compliance Toolkit 1.0 and all the security baselines.

You need to deploy one of the security baselines to all the computers in an organizational unit (OU) named OU1.

What should you do?

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 168

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

You need to prevent NTLM authentication on Server1.

Solution: From a Group Policy, you configure the Kerberos Policy. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

References:

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

#### NEW QUESTION 173

Your network contains an Active Directory domain named contoso.com.

The domain contains four global groups named Group1, Group2, Group3, and Group4. A user named User1 is a member of Group3.

You have an organizational unit (OU) named OU1 that contains computer accounts. A Group Policy object (GPO) named GPO1 is linked to OU1. OU1 contains a computer account named Computer1. GPO1 has the User Rights Assignment configured as shown in the following table.

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

**Answer:** B

#### NEW QUESTION 177

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 182

.....



## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your 70-744 Exam with Our Prep Materials Via below:**

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