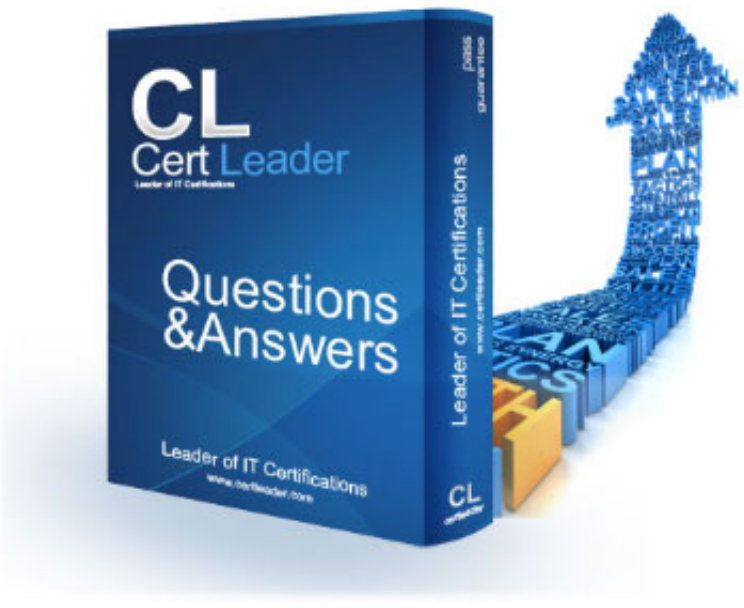
70-744 Dumps

Securing Windows Server 2016

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



NEW QUESTION 1
Note: The question is part of a series of questions th« present the same scenario. Each question In the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to It. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory forest named contoso.com. All servers run Windows Server 2016. The forest contains 2,000 client computers that run Windows 10. All client computers are deployed from a customized Windows image.
You need to deploy 10 Privileged Access Workstations (PAWs). The solution must ensure that administrators can access several client applications used by all users.
Solution: You deploy 10 physical computers and configure them as PAWs. You deploy 10 additional computers and configure them by using the customized Windows image.
Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 2
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory forest named contoso.com. All servers run Windows Server 2016. The forest contains 2,000 client computers that run Windows 10. All client computers are deployed from a customized Windows image.
You need to deploy 10 Privileged Access Workstations (PAWs). The solution must ensure that administrators can access several client applications used by all users.
Solution: You deploy one physical computer and configure it as a Hyper-V host that runs Windows Server 2016. You create 10 virtual machines and configure each one as a PAW.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 3
Note: This question is part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question In this section, you will NOT be able to return to It. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. Computer1 connects to a home network and a corporate network.
The corporate network uses the 172.16.0.0/24 address space internally. Computer1 runs an application named App1 that listens to port 8080.
You need to prevent connections to App1 when Computer1 is connected to the home network. Solution: From Group Policy Management, You create an Applocker rule.

A. Yes
B. No

Answer: B

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

NEW QUESTION 4
Note: This question It part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the stated goats. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to It. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. Computer1 connects to a home network and a corporate network.
The corporate network uses the 17216.0.0/24 address space internally. Computer1 runs an application named App1 that listens to port 8080.
You need to prevent connections to App1 when Computer1 is connected to the home network. Solution: From Group Policy Management you create a software restriction policy.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

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

NEW QUESTION 5
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question In this section, you will NOT be able to return to It. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. Computer1 connects to a home network and a corporate network.
The corporate network uses the 172.16.0.0/24 address space internally. Computer1 runs an application named App1 that listens to port 8080.
You need to prevent connections to App1 when Computer1 is connected to the home network. Solution: From Windows Firewall in the Control Panel, you add an application and allow the application to communicate through the firewall on a Private network.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

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

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

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

A. Yes
B. No

Answer: B

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

NEW QUESTION 7
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. All servers run Windows
Server 2016. All client computers run Windows 10.
The relevant objects in the domain are configured as shown in the following table.

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

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

A. Yes
B. No

Answer: A

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

NEW QUESTION 8
Note: Thb question Is part of a series of questions that present the same scenario. Each question In the series contains a unique solution that might meet the

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

A. Yes
B. No

Answer: B

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

NEW QUESTION 9
Your network contains an Active Directory domain named contoso.com. The domain contains two
servers named Server1 and Server2 that run Windows Server 2016. Server1 is configured as a domain controller.
You configure Server1 as a Just Enough Administration (JEA) endpoint You configure the required JEA rights for a user named User1.
You need to tell User1 how to manage Active Directory objects from Server2. What should you tell User1 to do first on Server2?

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

Answer: C

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

NEW QUESTION 10
Your network contains an Active Directory domain named contoso.com. The domain contains 100 servers.
You deploy the Local Administrator Password Solution (LAPS) to the network.
You deploy a new server named FinanceServer5, and join FinanceServerS to the domain.
You need to ensure that the passwords of the local administrators of FinanceServer5 are available to the LAPS administrators.
What should you do?

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

Answer: A

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

NEW QUESTION 10
Your network contains an Active Directory domain named contoso.com. The domain contains four servers. The servers are configured as shown in the following table.

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

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

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

Answer: C

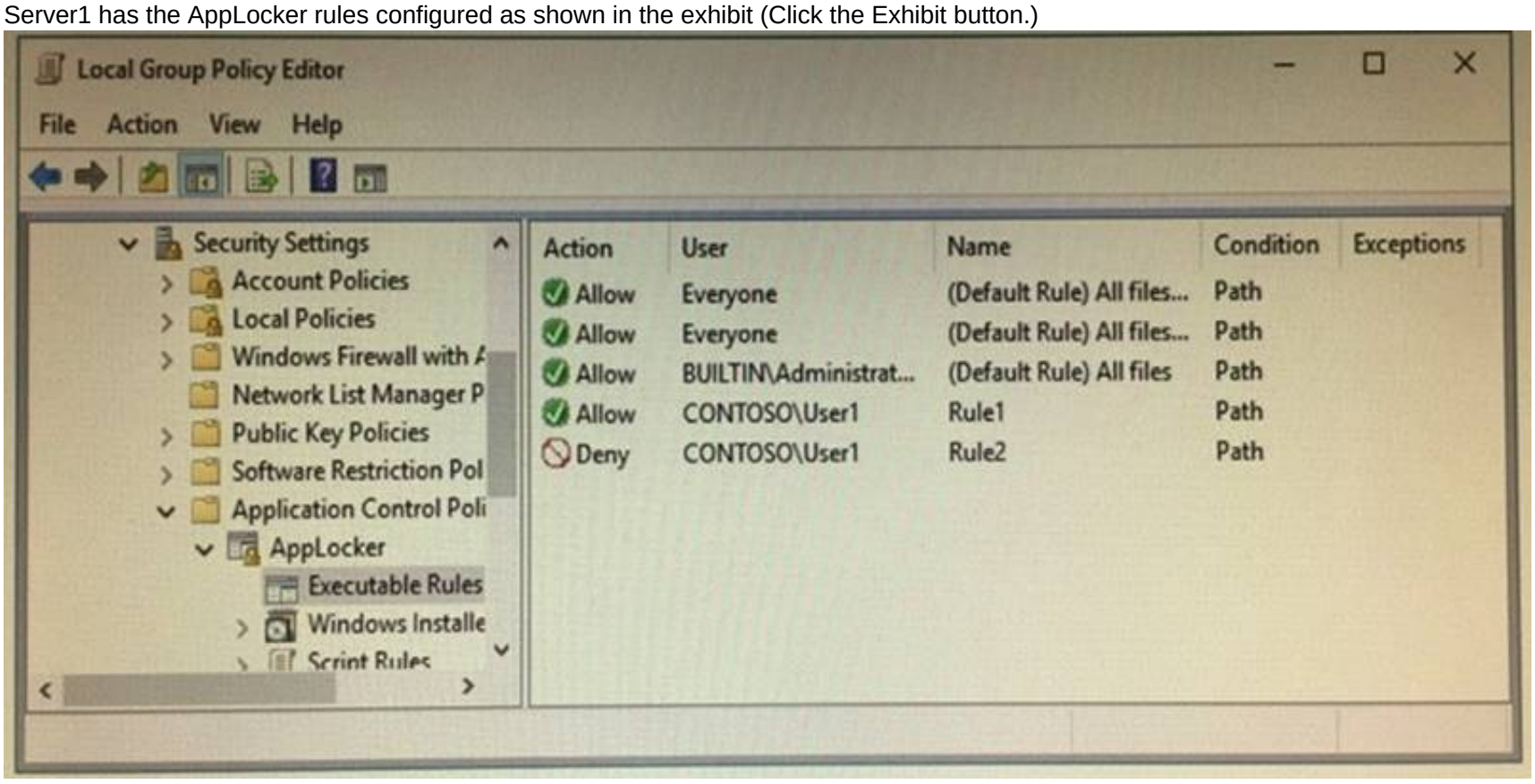
Explanation:
https://msdn.microsoft.com/en-us/library/dn896648.aspx
The current release of JEA is available on the following platforms:
-Windows Server 2016 Technical Preview 5 and higher
-Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2* with Windows Management Framework 5.0 installed FS1 is ready to be

managed by JEA, but FS2 need some extra work to do, either upgrade it to Windows Server 2016 or install Windows Management Framework 5.0 installed,

NEW QUESTION 11
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.
The services on Server1 are shown in the following output.

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

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

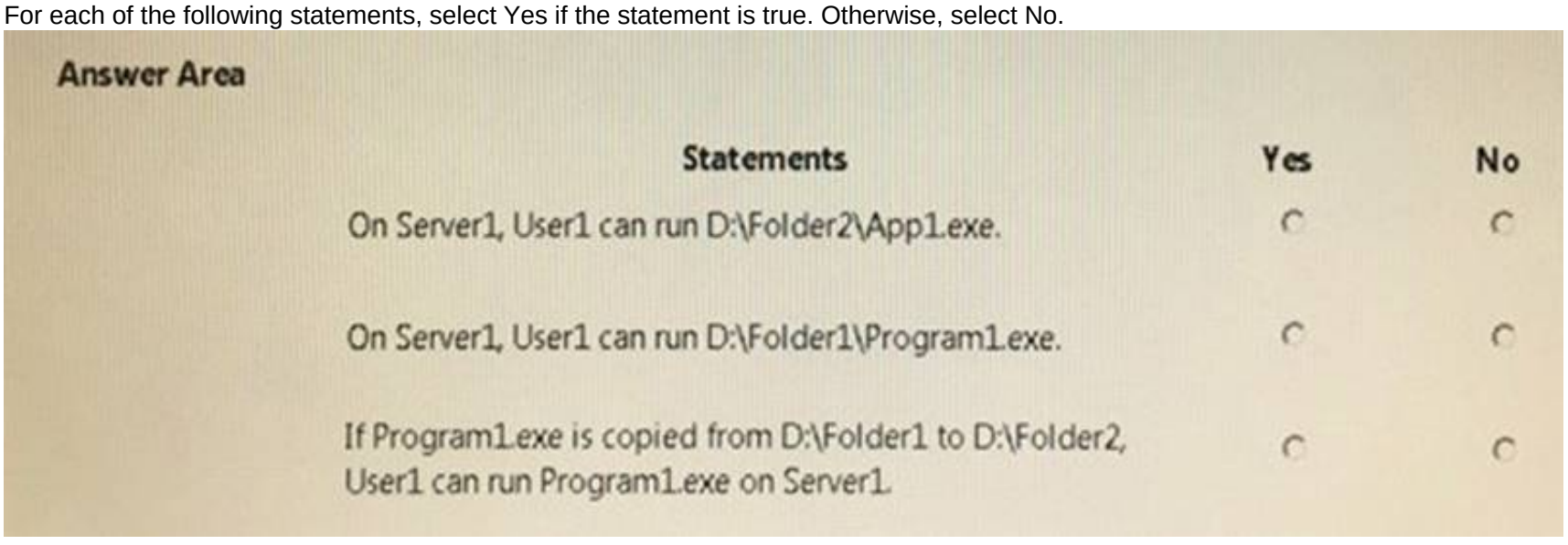
Server1 has the AppLocker rules configured as shown in the exhibit (Click the Exhibit button.)



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

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

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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 13
Your network contains an Active Directory domain named contoso.com. The domain contains a
server named Server5 that has the Windows Server Update Services server role installed. You need to configure Windows Server Update Services (WSUS) on Server5 to use SSI. You install a certificate in the local Computer store.
Which two tools should you use? Each correct answer presents part of the solution.

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

Answer: AC

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

NEW QUESTION 14
Your network contains an Active Directory domain named conioso.com. The domain contains 1,000 client computers that run Windows 8.1 and 1,000 client computers that run Windows 10.
You deploy a Windows Server Update Services (WSUS) server. You create a computer group tor each organizational unit (OU) that contains client computers.
You configure all of the client computers to receive updates from WSUS.
You discover that all of the client computers appear m the Unassigned Computers computer group in the Update Services console.
You need to ensure that the client computers are added automatically to the computer group that corresponds to the location of the computer account in Active Directory.
Which two actions should you perform? Each correct answer presents part of the solution.

A. From Group Policy objects (GPOs), configure the Enable client-side targeting setting.
B. From the Update Services console, configure the Computers option.
C. From Active Directory Users and Computers, create a domain local distribution group for each WSUS computer group.
D. From Active Directory Users and Computers, modify the flags attnbute of each OU.
E. From the Update Services console, run the WSUS Server Configuration Wizar

Answer: AB

NEW QUESTION 18
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

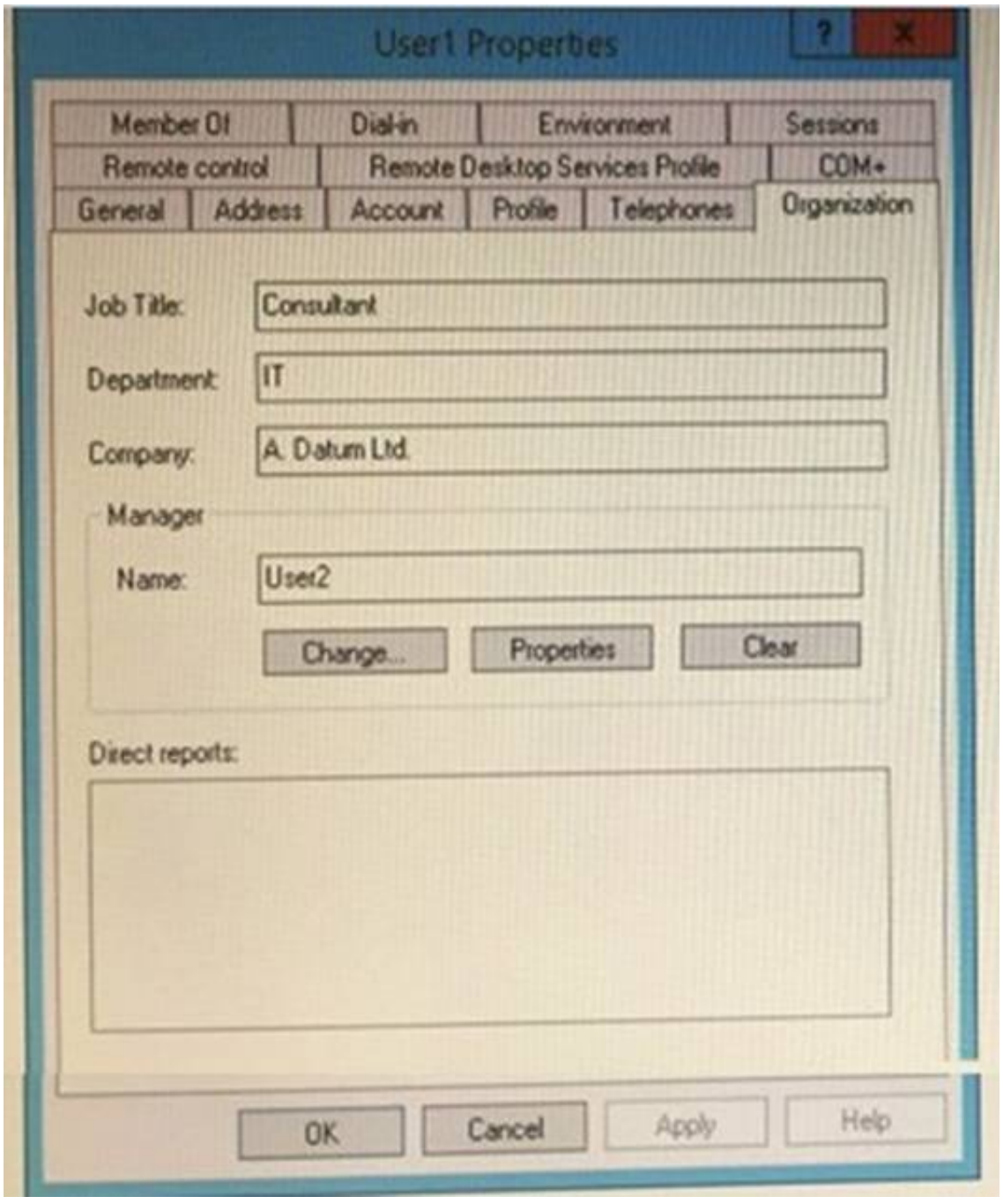
To assign a central access policy to a file server

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**.

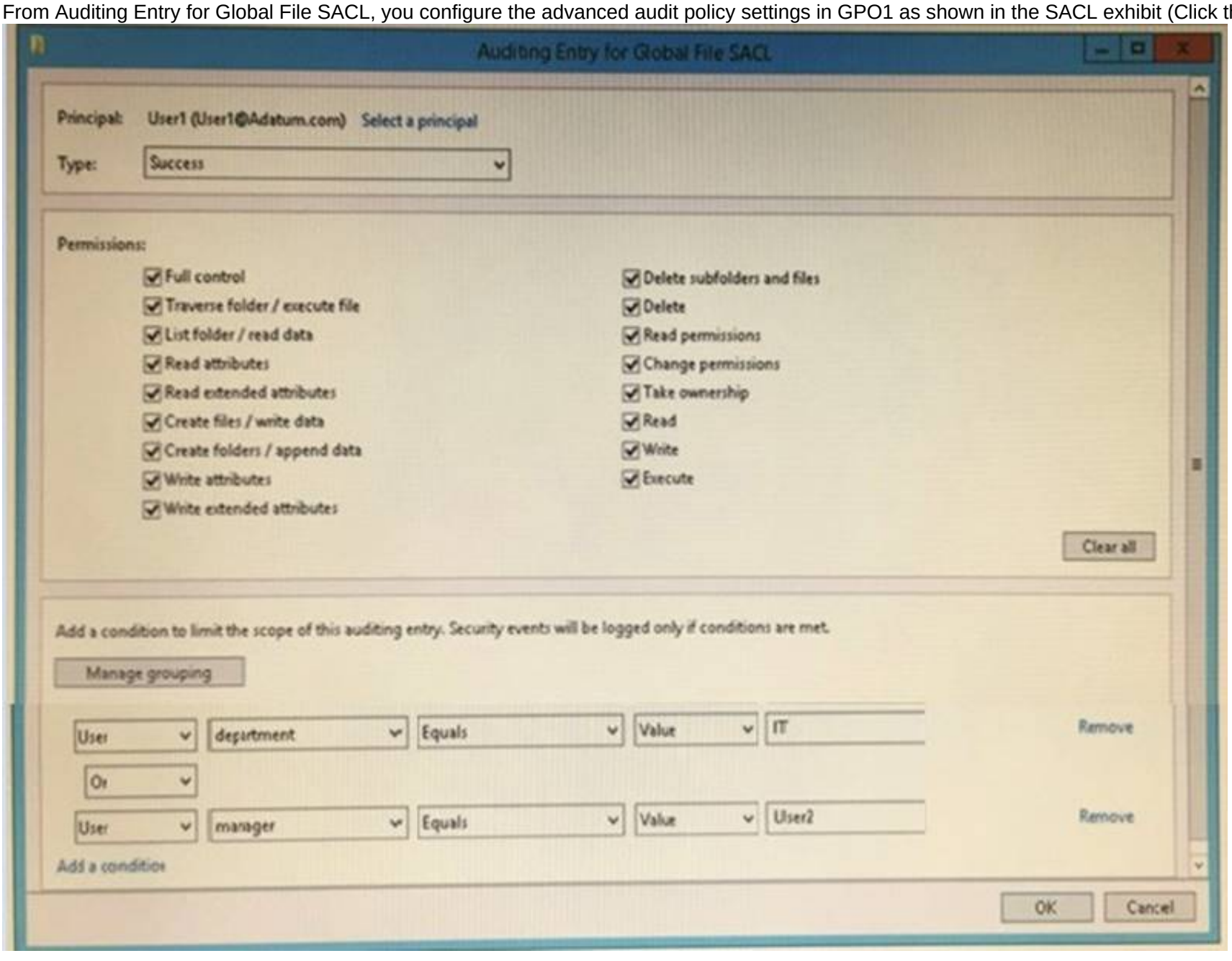
NEW QUESTION 23
HOTSPOT
Your network contains an Active Directory domain named adatum.com. The domain contains a file server named Server1 that runs Windows Server 2016.
You have an organizational unit (OU) named OU1 that contains Server1. You create a Group Policy object (GPO) named GPO1 and link GPO1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



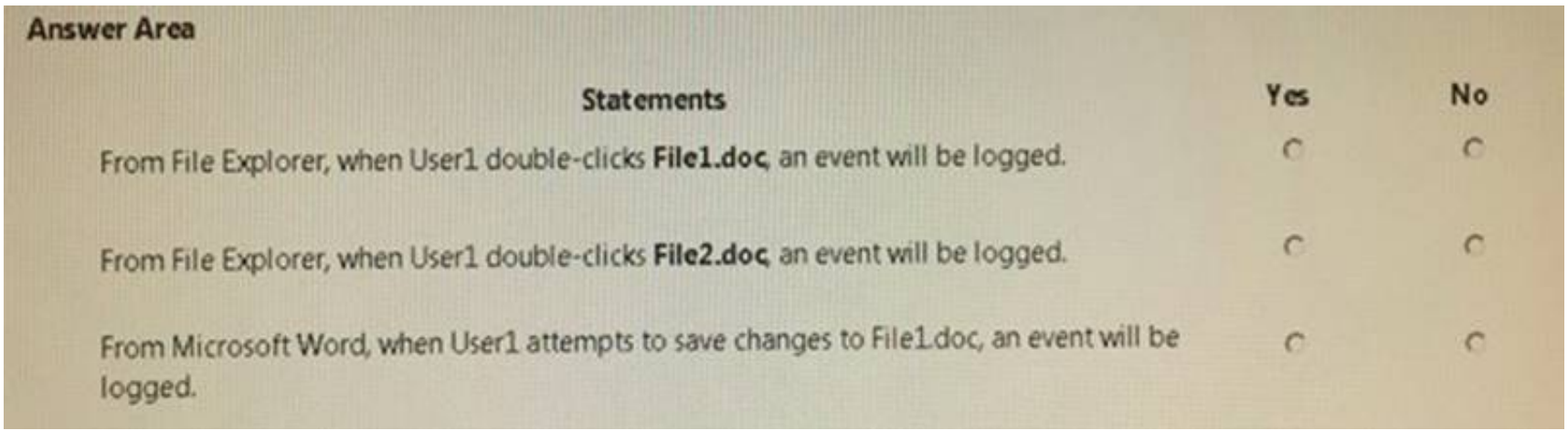
User1 has permissions to two files on Server1 configured as shown in the following table.

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.)



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

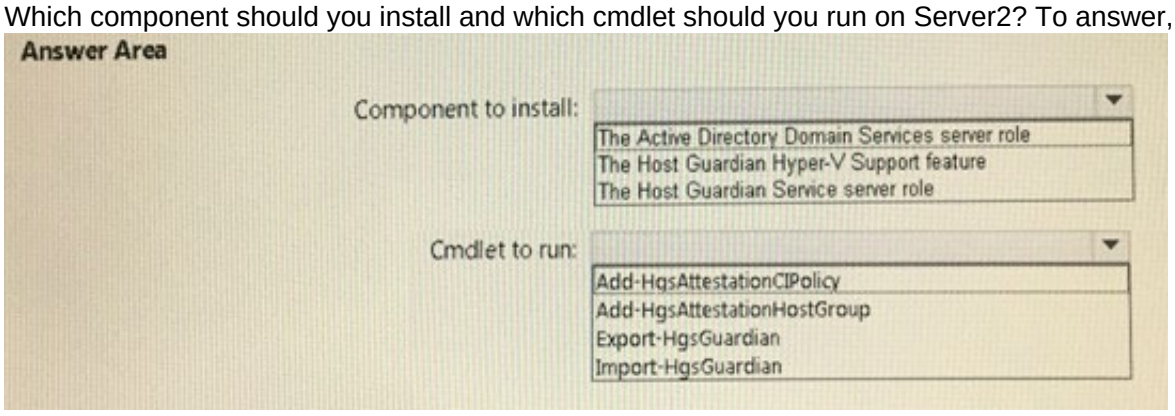


A. Mastered
B. Not Mastered

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
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.



A. Mastered
B. Not Mastered

Answer: A

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

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

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

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

  > ⓘ Important
  >
  > Make sure you install the latest cumulative update.

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

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

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

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

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

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

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

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

NEW QUESTION 30
Your network contains an Active Directory forest named contoso.com. The forest functional level is Windows Server 2012. The forest contains a single domain.
The domain contains multiple Hyper-V hosts.
You plan to deploy guarded hosts.
You deploy a new server named Server22 to a workgroup.
You need to configure Server22 as a Host Guardian Service server.
What should you do before you initialize the Host Guardian Service on Server22?

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

Answer: D

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

NEW QUESTION 33
____ enables easier management for BitLocker enabled desktops and servers in a domain environment by providing automatic unlock of operating system volumes at system reboot when connected to a wired corporate network. This feature requires the client hardware to have a DHCP driver implemented in its UEFI firmware.

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

Answer: A

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

NEW QUESTION 34
The "Network Security: Restrict NTLM: NTLM authentication in this domain" policy setting allows you to deny or allow NTLM authentication within a domain from this domain controller.
Which value would you choose so that the domain controller will deny all NTLM authentication logon attempts using accounts from this domain to all servers in the domain.
The NTLM authentication attempts will be blocked and will return an NTLM blocked error unless the server name is on the exception list in the Network security: Restrict NTLM: Add server exceptions in this domain policy setting.

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

Answer: B

NEW QUESTION 37
Encryption-supported VMs are intended for use where the fabric administrators are fully trusted. For example, an enterprise might deploy a guarded fabric in order to ensure VM disks are encrypted at-rest for compliance purposes.
Shielded VMs are intended for use in fabrics where the data and state of the VM must be protected from both fabric administrators and untrusted software that

might be running on the Hyper-V hosts. Is the Virtual Machine Connection (Console), HID devices (e.g. keyboard, mouse) ON or OFF for Encryption Supported VM's?

A. Off
B. On

Answer: B

NEW QUESTION 42
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.

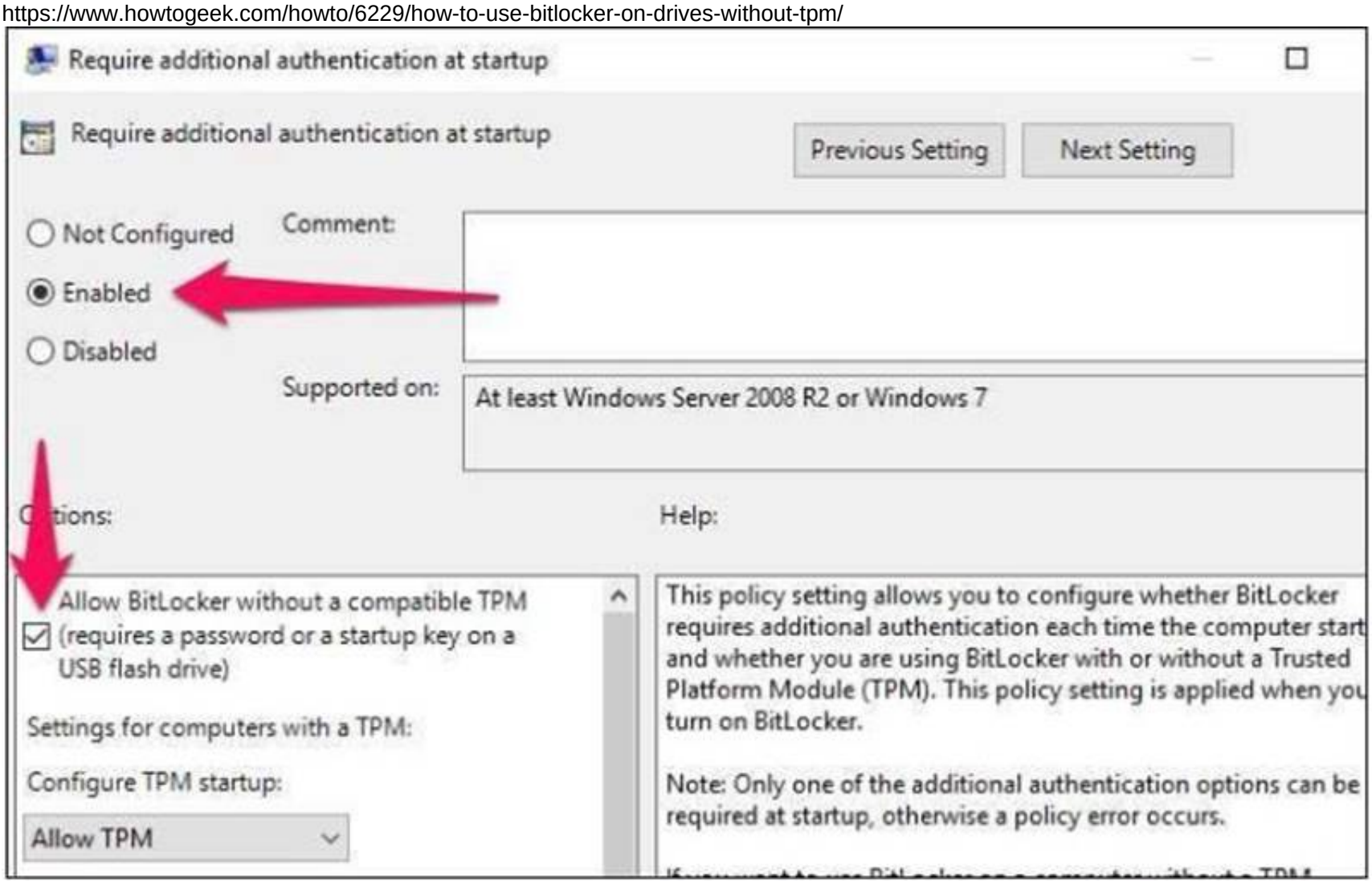
Server name	Domain or workgroup	Configuration
Server1	Domain	Windows Server Update Services (WSUS) server
Server2	Domain	Server that has a Trusted Platform Module (TPM)
Server3	Domain	Member server that will be configured for Just Enough Administration (JEA)
Server4	Domain	Application server
Server5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

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

A. Configure use of hardware-based encryption for operating system drives
B. Configure TPM platform validation profile for native UEFI firmware configurations
C. Require additional authentication at startup
D. Configure TPM platform validation profile for BIOS-based firmware configurations

Answer: C

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



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

A. Enable BitLocker Drive Encryption (BitLocker) for all the volumes on FS1
B. Disable the virtualization extensions for FS1

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

Answer: AE

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

NEW QUESTION 50
Your network contains an Active Directory domain named contoso.com. The domain contains several shielded virtual machines.
You deploy a new server named Server1 that runs Windows Server 2016. You install the Hyper-V server role on Server1.
You need to ensure that you can host shielded virtual machines on Server1. What should you install on Server1?

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

Answer: A

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

NEW QUESTION 51
You are creating a Nano Server image for the deployment of 10 servers.
You need to configure the servers as guarded hosts that use Trusted Platform Module (TPM) attestation.
Which three packages should you include in the Nano Server image? Each correct answer presents part of the solution.

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

Answer: ABF

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

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

NEW QUESTION 53
Your network contains an Active Directory domain named contoso.com. The domain contains several Hyper-V hosts.
You deploy a server named Server22 to a workgroup. Server22 runs Windows Server 2016. You need to configure Server22 as the primary Host Guardian Service server.
Which three cmdlets should you run in sequence?

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

Answer: AEF

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

NEW QUESTION 55
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 57
You have a server named Server1 that runs Windows Server 2016.
You need to identify whether IPsec tunnel authorization is configured on Server1. Which cmdlet should you use?

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

Answer: A

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

```
PS C:\> Get-NetIPsecRule

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

NEW QUESTION 62
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 65
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 machin

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 66
You have a server named Server1 that runs Windows Server 2016. Server1 has the Windows Server Update Services server role installed.
Windows Server Update Services (WSUS) updates for Server1 are stored on a volume named D. The hard disk that contains volume D fails.
You replace the hard disk. You recreate volume D and the WSUS folder hierarchy in the volume. You need to ensure that the updates listed in the WSUS console are available in the WSUS folder. What should you run?

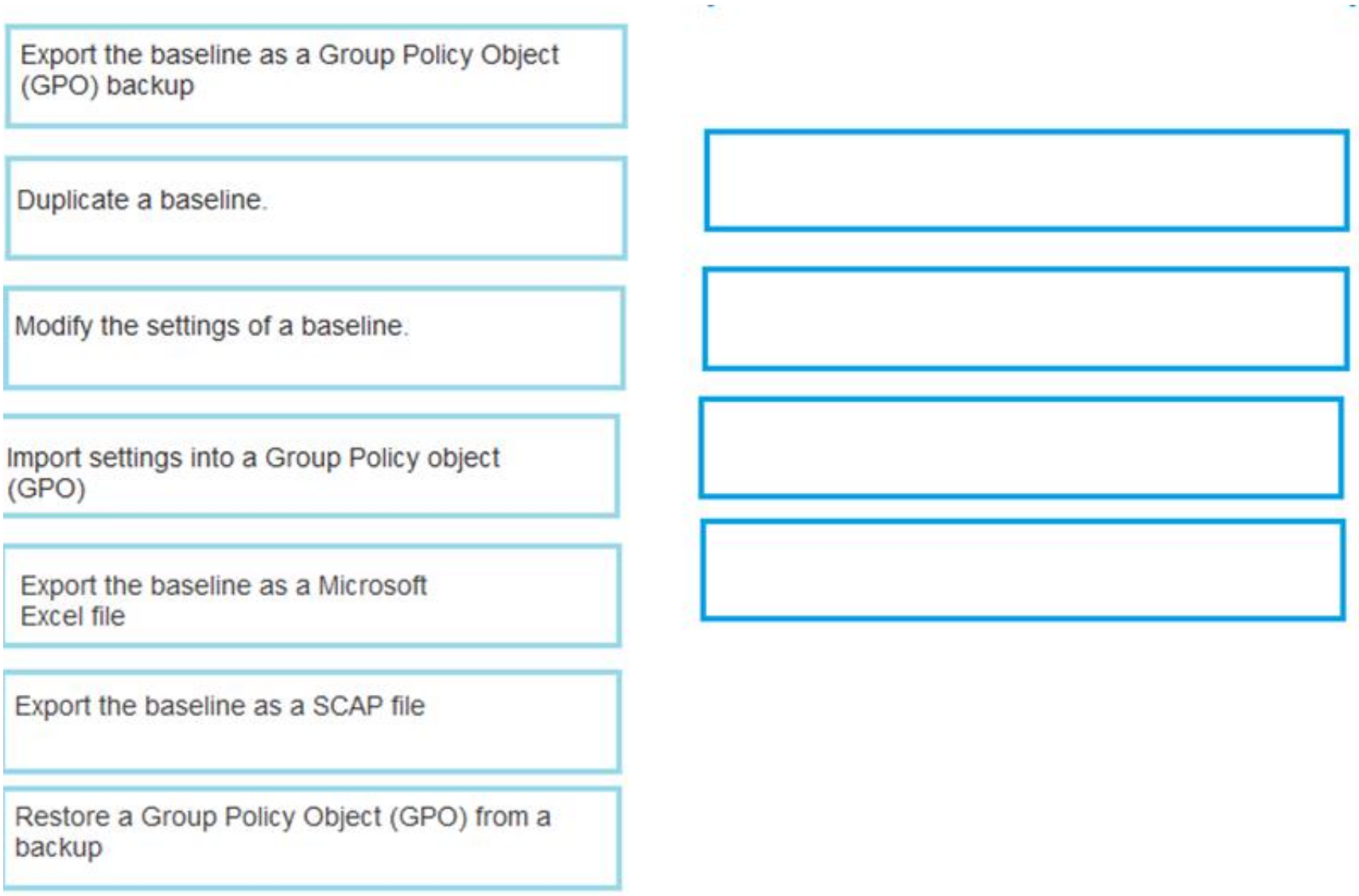
A. wsusutil.exe /import
B. wsusutil.exe /reset
C. Set-WsusServerSynchronization
D. Invoke-WsusServerCleanup

Answer: B

Explanation:
https://technet.microsoft.com/en-us/library/cc720466%28v=ws.10%29.aspx?f=255&MSPPError=- 2147217396
WSUSutil.exe is a tool that you can use to manage your WSUS server from the command line.
WSUSutil.exe
is located in the %drive%\\Program Files\\Update Services\\Tools folder on your WSUS server.
You can run specific commands with WSUSutil.exe to perform specific functions, as summarized in the following table.
The syntax you would use to run WSUSutil.exe with specific commands follows the table.

Command	What it enables you to do	When you might use it
export	The first of the two parts that make up the export / import process. The **export** command enables you to export update metadata to an export package file. You cannot use this parameter to export update files, update approvals, or server settings.	• On an ongoing basis, if you are running a network with limited or restricted internet connectivity
import	The second of the two parts that make up the export/import process. The **import** command imports update metadata to a server from an export package file created on another WSUS server. This synchronizes the destination WSUS server without using a network connection.	• On an ongoing basis, if you are running a network with limited or restricted connectivity
migratesus	This command migrates update approvals from a SUS 1.0 server to a WSUS server.	• If you are upgrading your implementation SUS 1.0 to WSUS.
movecontent	Changes the file system location where the WSUS server stores update files, and optionally copies any update files from the old location to the new location	• Hard drive is full • Disk fails
reset	Checks that every update metadata row in the database has corresponding update files stored in the file system. If update files are missing or have been corrupted, WSUS downloads the update files again.	• After restoring the WSUS database. • When troubleshooting

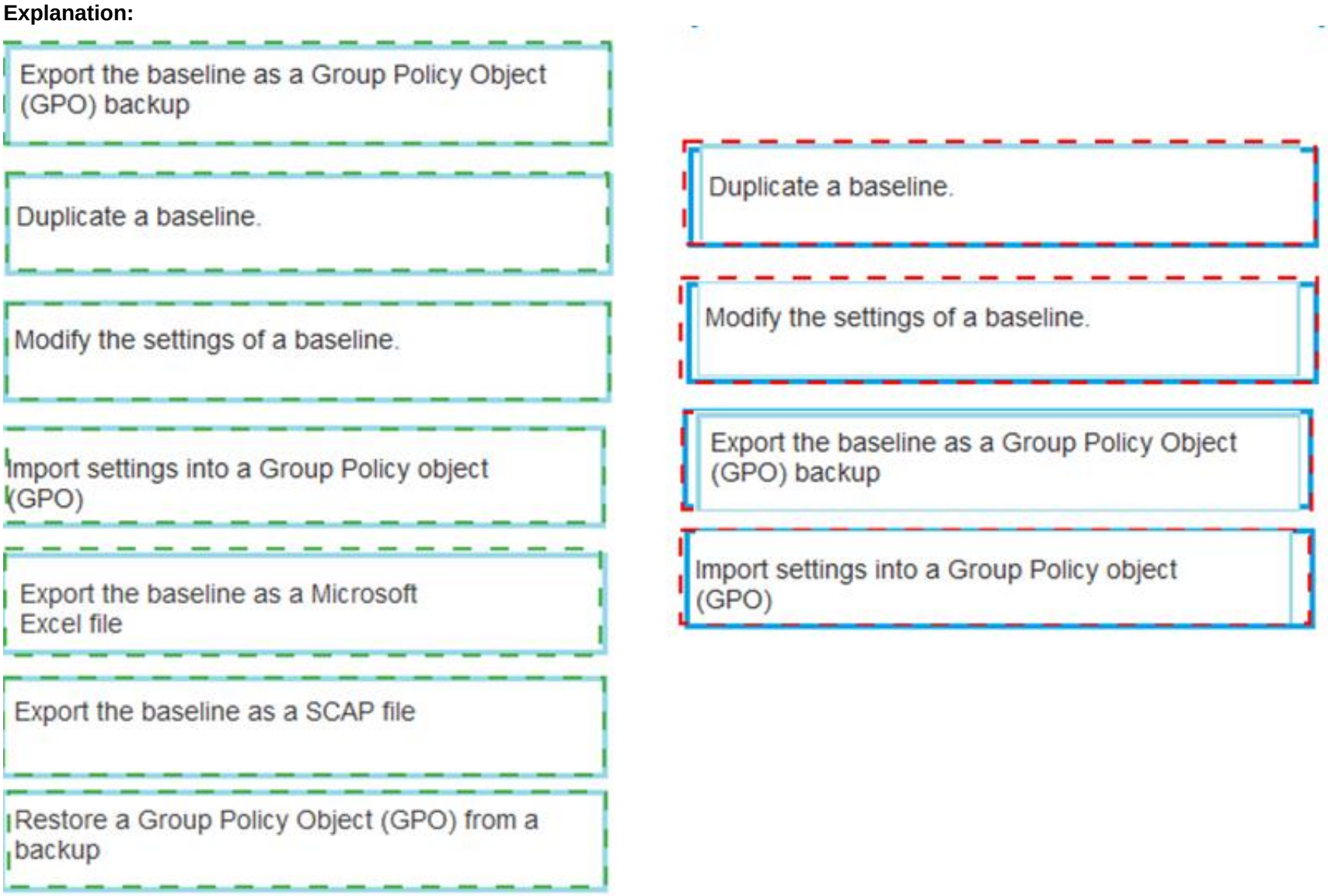
NEW QUESTION 70
DRAG DROP
Your network contains an Active Directory domain.
You install Security Compliance Manager (SCM) 4.0 on a server that runs Windows Server 2016. You need to modify a baseline, and then make the baseline available as a domain policy.
Which four actions should you perform in sequence?



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 73
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.

Copy

```
$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.

Copy

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

NEW QUESTION 76
Your network contains an Active Directory domain named contoso.com. The domain contains 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

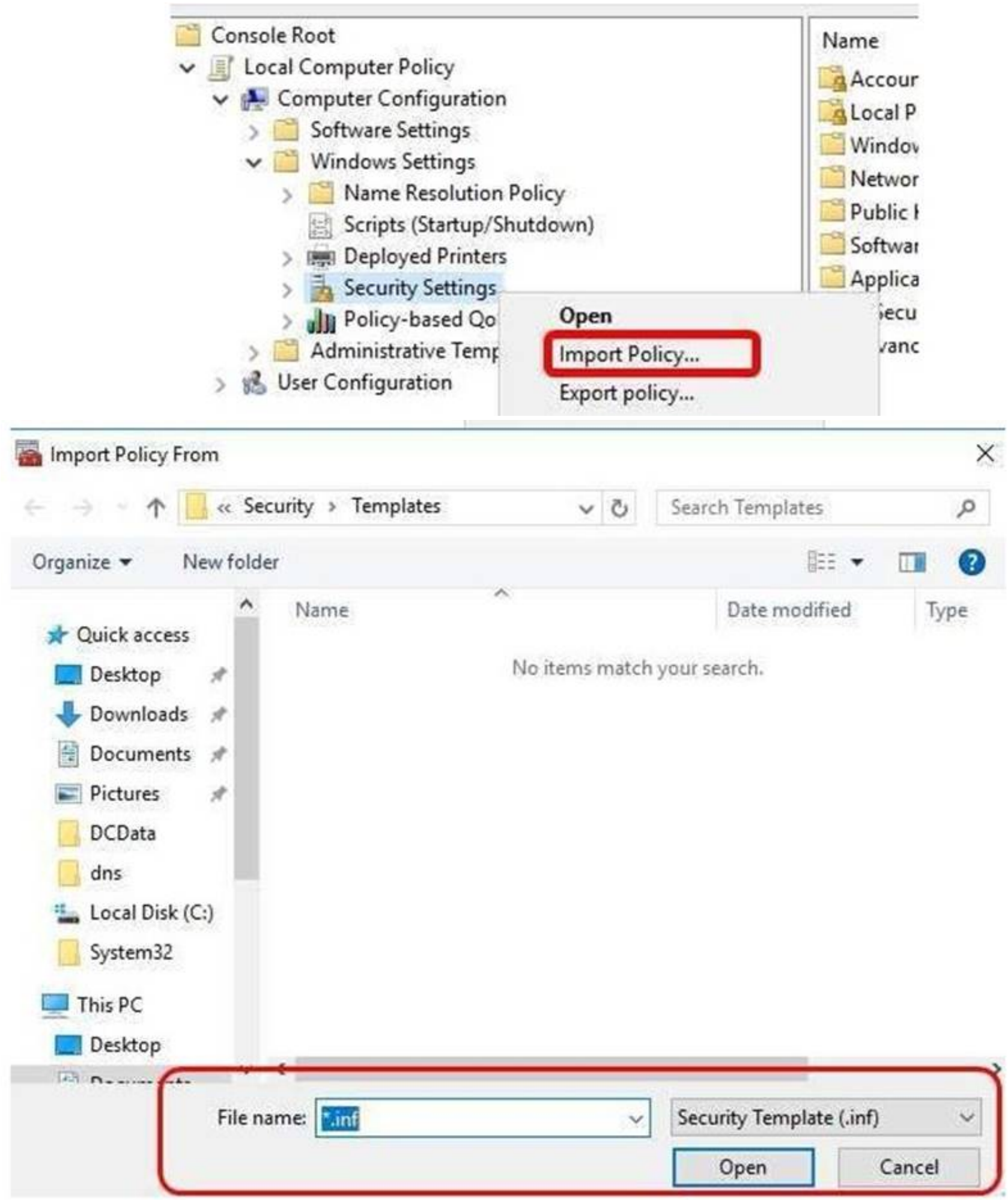
Explanation:
Use “Active Directory Users and Computers” to view the attribute value of “ms-MCS-adminpwd” of the Server5 computer account
https://blogs.technet.microsoft.com/askpfeplat/2015/12/28/local-administrator-password-solutionlapsimplementation- hints-and-security-nerd-commentaryincludingmini-threat-model/

NEW QUESTION 79
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 81
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 83
Your network contains an Active Directory domain named contoso.com. All client computers run Windows 10.
You plan to deploy a Remote Desktop connection solution for the client computers.
You have four available servers in the domain that can be configured as Remote Desktop servers. The servers are configured as shown in the following table.

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

You need to ensure that all Remote Desktop connections can be protected by using Remote Credential Guard.
Solution: You deploy the Remote Desktop connection solution by using Server3. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Yes, since all client computers run Windows 10, and Server2 is Windows Server 2016 which fulfills the following requirements of using Remote Credential Guard. https://docs.microsoft.com/en-us/windows/access-protection/remote-credential-guard Remote Credential Guard requirements
To use Windows Defender Remote Credential Guard, the Remote Desktop client and remote host must meet the following requirements:
The Remote Desktop client device:
Must be running at least Windows 10, version 1703 to be able to supply credentials.
Must be running at least Windows 10, version 1607 or Windows Server 2016 to use the user's signed-in credentials. This requires the user's account be able to sign in to both the client device and the remote host.
Must be running the Remote Desktop Classic Windows application. The Remote Desktop Universal Windows Platform application doesn't support Windows Defender Remote Credential Guard.
Must use Kerberos authentication to connect to the remote host. If the client cannot connect to a domain controller, then RDP attempts to fall back to NTLM.
Windows Defender Remote Credential Guard does not allow NTLM fallback because this would expose credentials to risk.
The Remote Desktop remote host:
Must be running at least Windows 10, version 1607 or Windows Server 2016. Must allow Restricted Admin connections.
Must allow the client's domain user to access Remote Desktop connections. Must allow delegation of non-exportable credentials.

NEW QUESTION 88
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 90
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. The network uses the 172.16.0.0/16 address space.
Computer1 has an application named App1.exe that is located in D:\\Apps\\. App1.exe is configured to accept connections on TCP port 8080.
You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.
Solution: You configure an inbound rule that allows the TCP protocol on port 8080, uses a scope of 172.16.0.0/16 for local IP addresses, and applies to a private profile.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
"You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.", you should create the firewall rule for "Domain" profile instead, not the "Private" profile.
https://technet.microsoft.com/en-us/library/getting-started-wfas-firewall-profilesipsec(v=ws.10).aspx

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

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

NEW QUESTION 93
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that has Microsoft Security Compliance Manager (SCM) 4.0 installed. The domain contains domain controllers that run Windows Server 2016.
A Group Policy object (GPO) named GPO1 is applied to all of the domain controllers.
GPO1 has a Globally Unique Identifier (GUID) of 7ABCDEFG-1234-5678-90AB-005056123456. You need to create a new baseline that contains the settings from GPO1. What should you do first?

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

Answer: B

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

NEW QUESTION 94
You have a server named Server1 that runs Windows Server 2016.
You need to identify the default action for the inbound traffic when Server1 connects to the domain. Which cmdlet should you use?

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

Answer: C

NEW QUESTION 95
Your network contains an Active Directory domain.
Microsoft Advanced Threat Analytics (ATA) is deployed to the domain.
A database administrator named DBA1 suspects that her user account was compromised.
Which three events can you identify by using ATA? Each correct answer presents a complete solution.

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

Answer: CDE

Explanation:
https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-threats Suspicious authentication failures (Behavioral brute force)

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

NEW QUESTION 99
HOTSPOT
You have a Hyper-V host named Server1 that runs Windows Server 2016. A new security policy states that all the virtual machines must be encrypted.
Server1 hosts the virtual machines configured as shown in the following table.

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

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

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

A. Mastered
B. Not Mastered

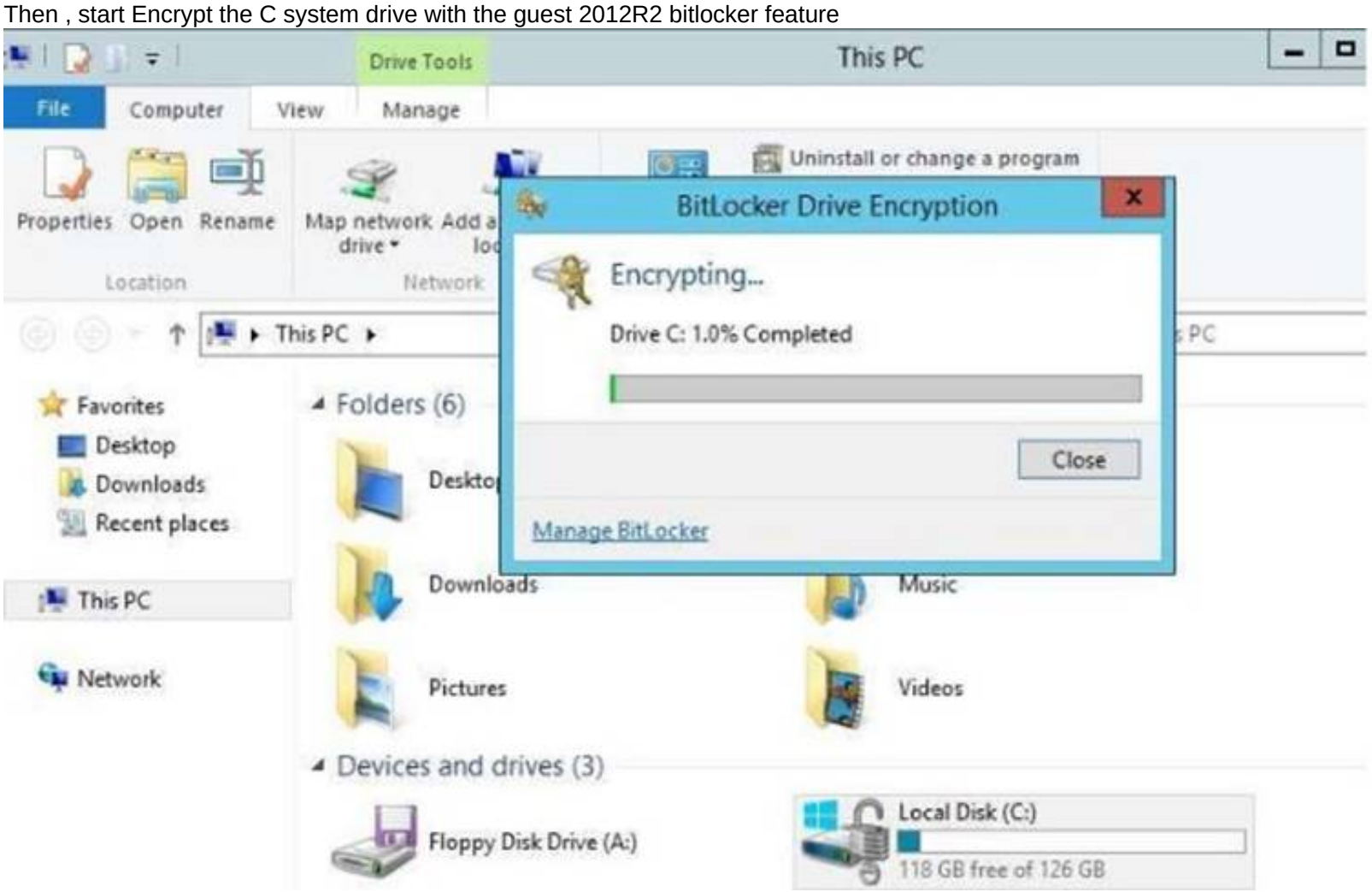
Answer: A

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

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

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


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


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


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

Within the guest, there is no Virtual TPM

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



After the encryption is completed:-

NEW QUESTION 100
Your network contains an Active Directory domain named contoso.com. All servers in the domain run Windows Server 2016.All client computers run Windows 10.
Your company has deployed the Local Administrator Password Solution (LAPS).
Client computers in the finance department are located in an organizational unit (OU) named Finance.
Each finance computer has a custom administrative account named FinAdmin. You discover that the FinAdmin accounts are not managed by LAPS.
You need to ensure that the FinAdmin accounts are managed by LAPS. What should you do?

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

Answer: C

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

NEW QUESTION 105
Your network contains an Active Directory forest named contoso.com. The forest functional level is Windows Server 2012.
The forest contains 20 member servers that are configured as file servers. All domain controllers run Windows Server 2016.
You create a new forest named contosoadmin.com.
You need to use the Enhanced Security Administrative Environment (ESAE) approach for the administration of the resources in contoso.com.
Which two actions should you perform? Each correct answer presents part of the solution.

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

Answer: AC

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

NEW QUESTION 110
Your network contains an Active Directory domain named contoso.com. The domain contains 100 servers.
You deploy the Local Administrator Password Solution (LAPS) to the network.
You discover that the members of a group named FinanceAdministrators can view the password of the local Administrator accounts on the servers in an organizational unit (OU) named FinanceServers. You need to prevent the FinanceAdministrators members from viewing the local administrators' passwords on the servers in FinanceServers.
Which permission should you remove from FinanceAdministrators?

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

Answer: B

Explanation:
https://blogs.technet.microsoft.com/askpfeplat/2015/12/28/local-administrator-password-solutionQuestions
& Answers PDF P-123
lapsimplementation-hints-and-security-nerd-commentaryincludingmini-threat-model/ Access to the password is granted via the "Control Access" right on the attribute.
Control Access is an "Extended Right" in Active Directory, which means if a user has been granted the "All
Extended Rights" permission they'll be able to see passwords even if you didn't give them permission.

NEW QUESTION 112
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 116
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.

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

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

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

Answer: B

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

NEW QUESTION 118
Your network contains an Active Directory forest named corp.contoso.com.
You are implementing Privileged Access Management (PAM) by using a bastion forest named priv.contoso.com.
You need to create shadow groups in priv.contoso.com. Which cmdlet should you use?

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

Answer: D

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

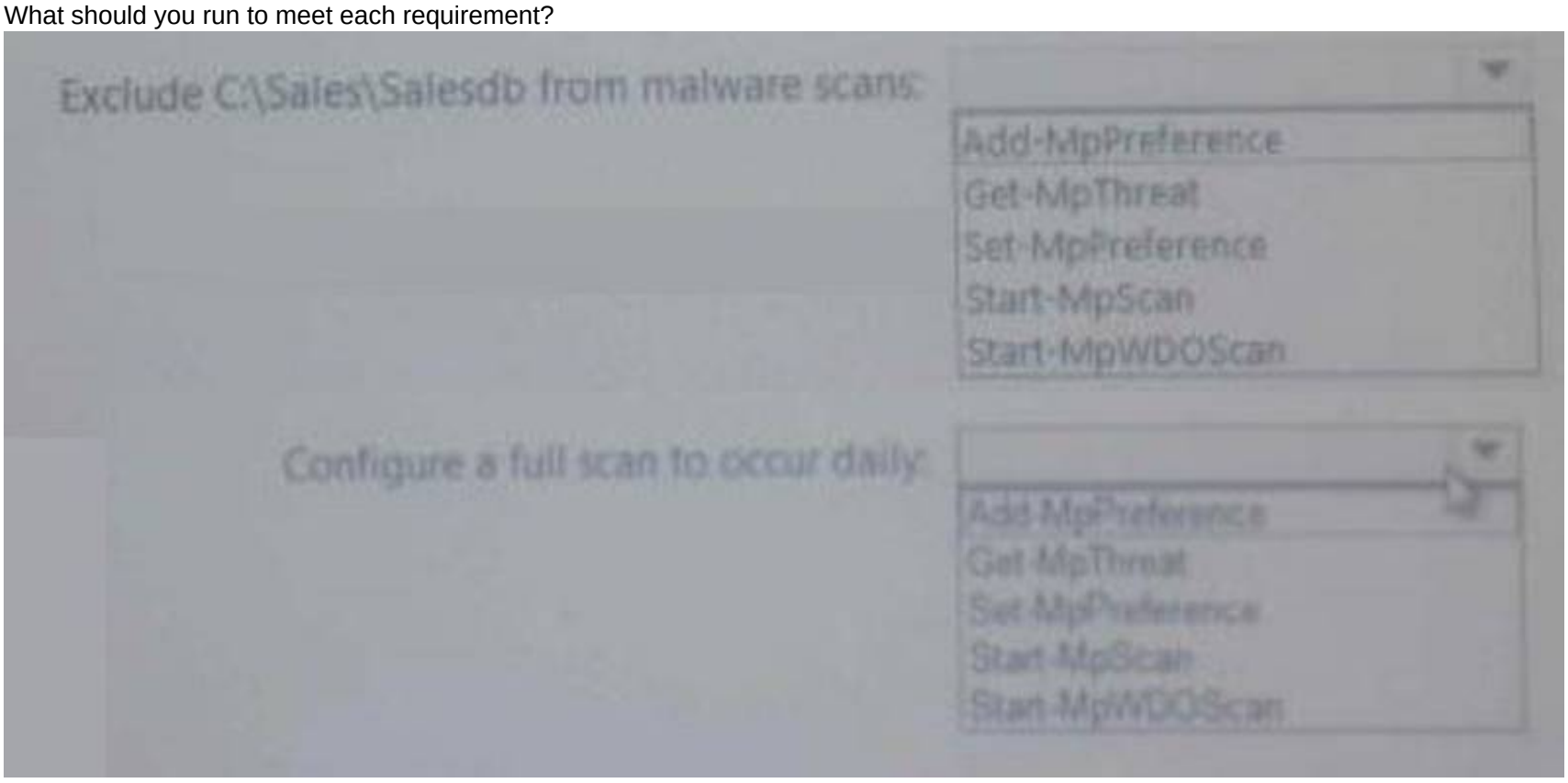
NEW QUESTION 120
Your network contains several secured subnets that are disconnected from the Internet.
One of the secured subnets contains a server named Server1 that runs Windows Server 2016.
You implement Log Analytics in Microsoft Operations Management Suite (OMS) for the servers that connect to the Internet.
You need to ensure that Log Analytics can collect logs from Server1.
Which two actions should you perform? Each correct answer presents part of the solution.

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

Answer: AE

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

NEW QUESTION 123
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 124
You have the Windows Server 2016 operating system images as following table.

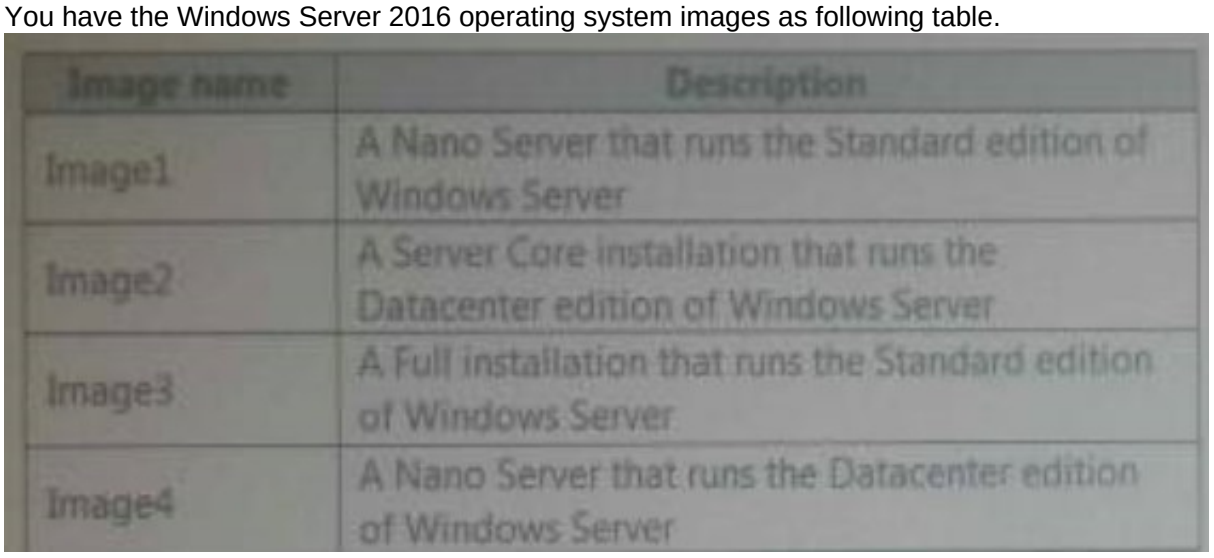


Image name	Description
Image1	A Nano Server that runs the Standard edition of Windows Server
Image2	A Server Core installation that runs the Datacenter edition of Windows Server
Image3	A Full installation that runs the Standard edition of Windows Server
Image4	A Nano Server that runs the Datacenter edition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

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

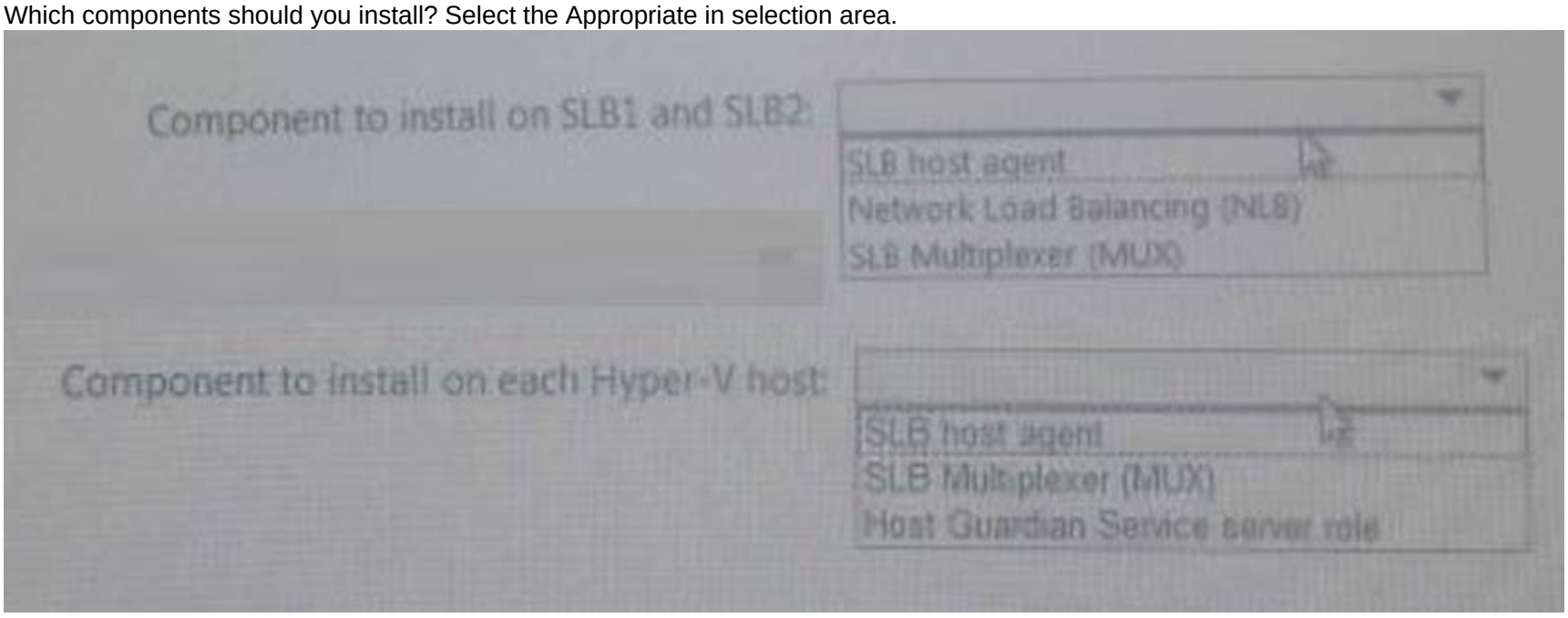
A. image1
B. image2
C. image3
D. image4

Answer: C

Explanation:
https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shieldedvm/ guarded-fabricprepare-for-hgs
Prerequisites
Hardware: HGS can be run on physical or virtual machines, but physical machines are recommended. If you want to run HGS as a three-node physical cluster (for availability), you must have three physical servers.

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

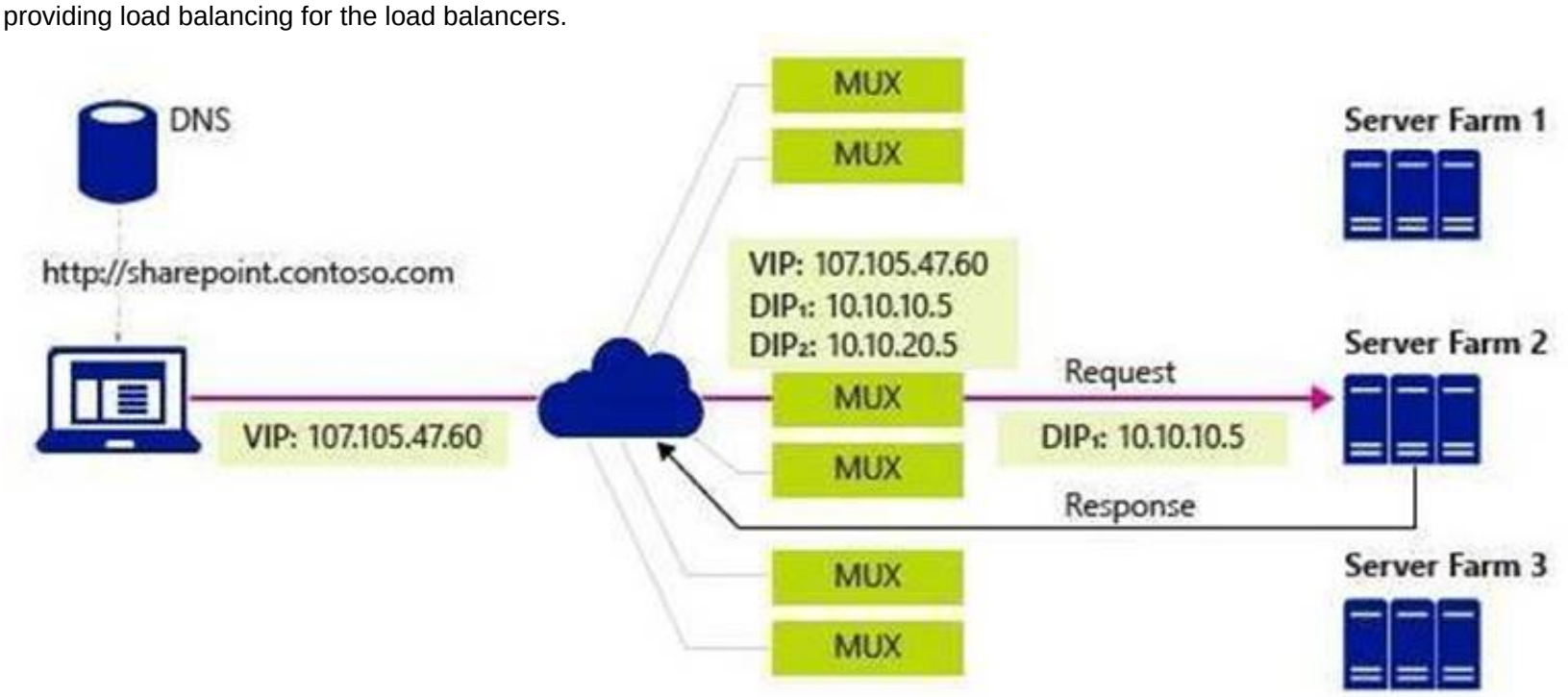
NEW QUESTION 126
HOTSPOT
You have 10 Hyper-V hosts that run Windows Server 2016.
Each Hyper-V host has eight virtual machines that run a distributed web application named App1. You plan to implement a Software Load Balancing (SLB) solution for client access to App1. You deploy two new virtual machines named SLB1 and SLB2.
You need to install the required components on the Hyper-V hosts and the new servers for the planned implementation.
Which components should you install? Select the Appropriate in selection area.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://blogs.technet.microsoft.com/tip_of_the_day/2016/06/28/tip-of-the-day-demystifyingsoftware- definednetworking-terms-the-components/
https://technet.microsoft.com/en-us/library/mt632286.aspx
SLB Host Agent – When you deploy SLB, you must use System Center, Windows PowerShell, or another management application to deploy the SLB Host Agent on every Hyper-V host computer.
You can install the SLB Host Agent on all versions of Windows Server 2016 that provide Hyper-V support, including Nano Server.
SLB MUX – Part of the Software Load Balancer (SLB on Windows Server 2016, the SLB MUX processes inbound network traffic and maps VIPs (virtual IPs) to DIPs (datacenter IPs), then forwards the traffic to the correct DIP. Each MUX also uses BGP to publish VIP routes to edge routers. BGP Keep Alive notifies MUXes when a MUX fails, which allows active MUXes to redistribute the load in case of a MUX failure – essentially providing load balancing for the load balancers.



NEW QUESTION 127
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 132
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You manage a file server that runs Windows Server 2016. The file server contains the volumes configured as shown in the following table.

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

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

A. Yes
B. No

Answer: A

Explanation:

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

NEW QUESTION 133
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 138
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.

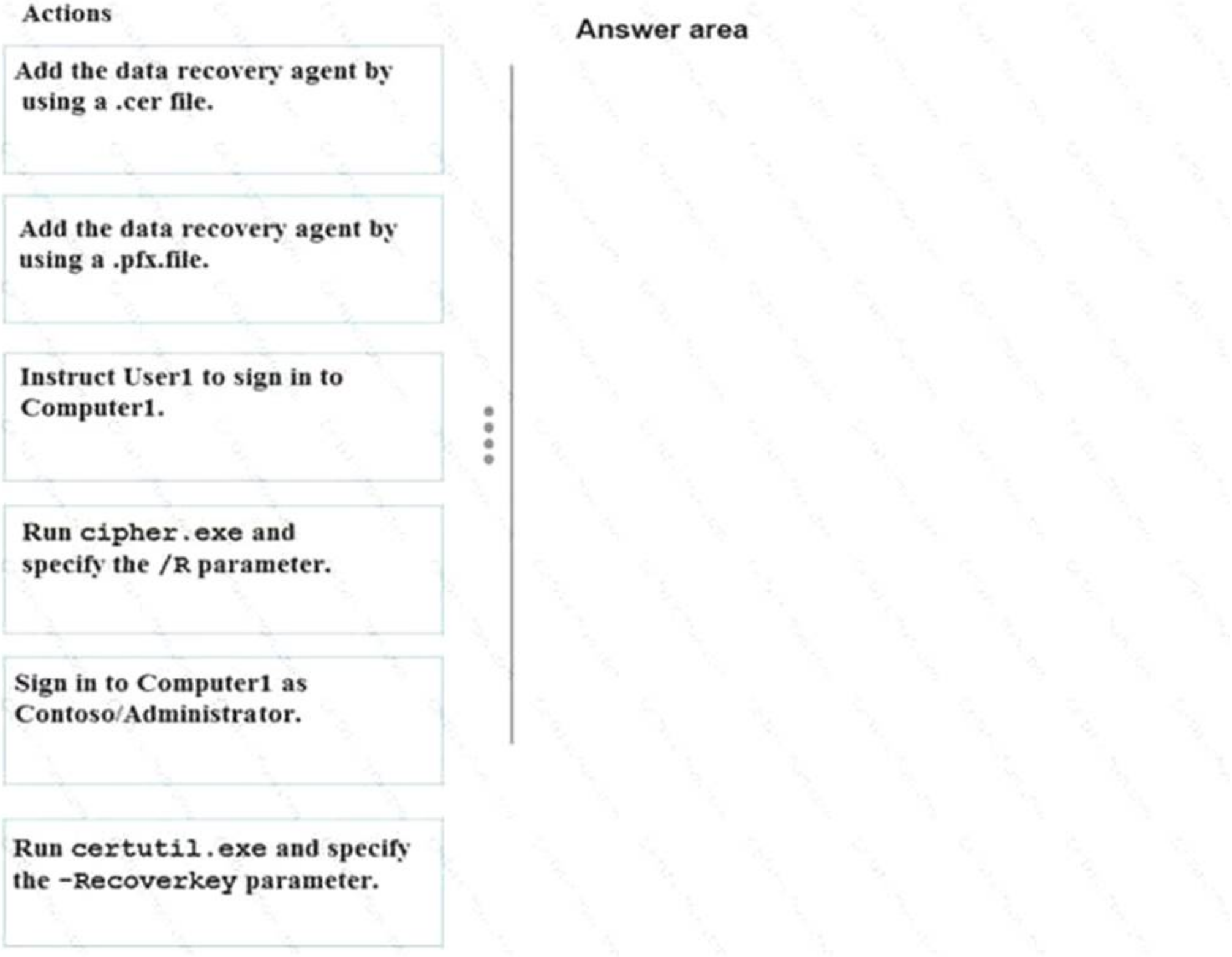
Answer: B

NEW QUESTION 140
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 145
DRAG DROP
Your network contains an Active Directory domain named contoso.com. The domain contains a user named User1 and a computer named Computer1. Remote Server Administration Tools (RSAT) is installed on Computer1.
You need to add User1 as a data recovery agent in the domain.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

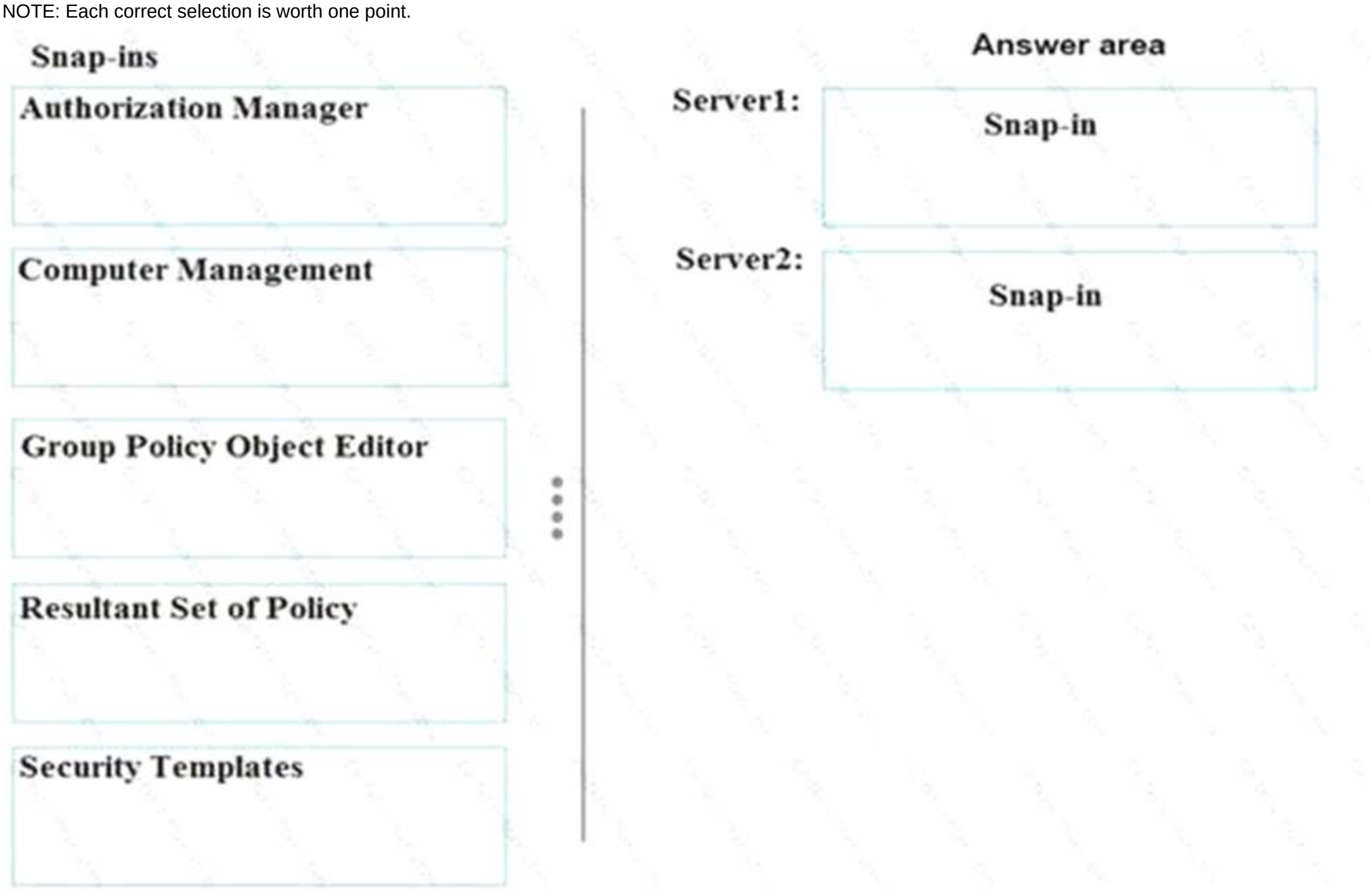
References:
https://msdn.microsoft.com/library/cc875821.aspx#EJAA
https://www.serverbrain.org/managing-security-2003/using-the-cipher-command-to-add-datarecovery- agent.html

NEW QUESTION 149
Your network contains an Active Directory domain named contoso.com. The domain contains a certification authority (CA).
You need to implement code integrity policies and sign them by using certificates issued by the CA. You plan to use the same certificate to sign policies on multiple computers.
You duplicate the Code Signing certificate template and name the new template CodeIntegrity. How should you configure the CodeIntegrity template?

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

Answer: D

NEW QUESTION 150
DRAG DROP
You have two servers named Server1 and Server2 that run Windows Server 2016. The servers are in a workgroup.
You need to create a security template that contains the security settings of Server1 and to apply the template to Server2. The solution must minimize administrative effort.
Which snap-in should you use for each server? To answer, drag the appropriate snap-ins to the correct servers. Each snap-in may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 153
.....

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