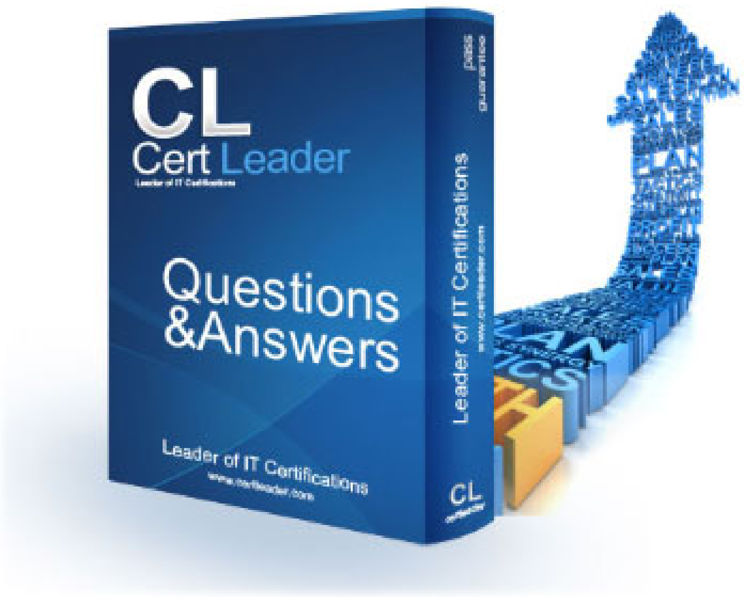
70-744 Dumps

Securing Windows Server 2016

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



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

A. Yes
B. No

Answer: B

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

NEW QUESTION 2
Note: 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 3
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2016. Server1 is configured as a domain controller.
You configure Server1 as a Just Enough Administration (JEA) endpoint You configure the required JEA rights for a user named User1.
You need to tell User1 how to manage Active Directory objects from Server2. What should you tell User1 to do first on Server2?

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

Answer: C

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

NEW QUESTION 4
Your network contains an Active Directory domain named contoso.com. The domain contains five servers. All servers run Windows Server 2016.
A new secunty policy states that you must modify the infrastructure to meet the following requirements:
*Limit the nghts of administrators.
*Minimize the attack surface of the forest
*Support Multi-Factor authentication for administrators.
You need to recommend a solution that meets the new secunty policy requirements. What should you recommend deploying?

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

Answer: A

Explanation:
You have to “-Minimize the attack surface of the forest”, then you must create another forest for administrators.
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securingprivilegedaccess- reference-material#ESAE_BM
This section contains an approach for an administrative forest based on the Enhanced Security Administrative
Environment (ESAE) reference architecture deployed

by Microsoft's cybersecurity professional services teams to protect customers against cybersecurity attacks.
Dedicated administrative forests allow organizations to host administrative accounts, workstations, and groups in an environment that has stronger security controls than the production environment.

NEW QUESTION 5
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

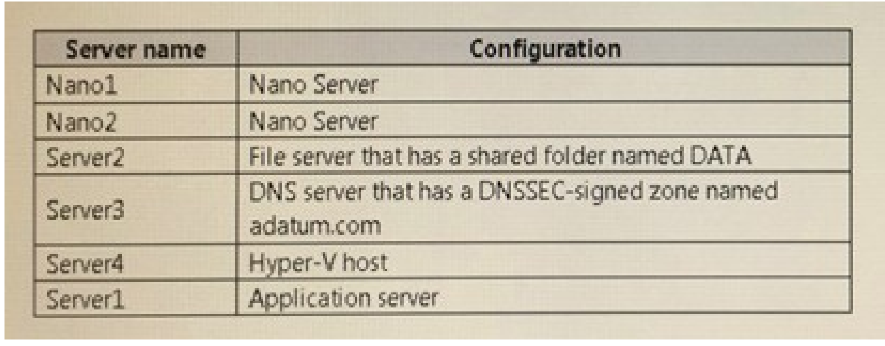
Answer: AB

NEW QUESTION 6
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question Is independent of the other questions in this series. Information and details provided in a question apply only to that question.
Your network contains an Active Directory domain named contoso.com The domain contains a file server named Server1 that runs Windows Server 2016.
You need to create Work Folders on Server1. Which tool should you use?

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

Answer: C

NEW QUESTION 7
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario b repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.
Start of repeated scenario
Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.
The domain contains the servers configured as shown m the following table.



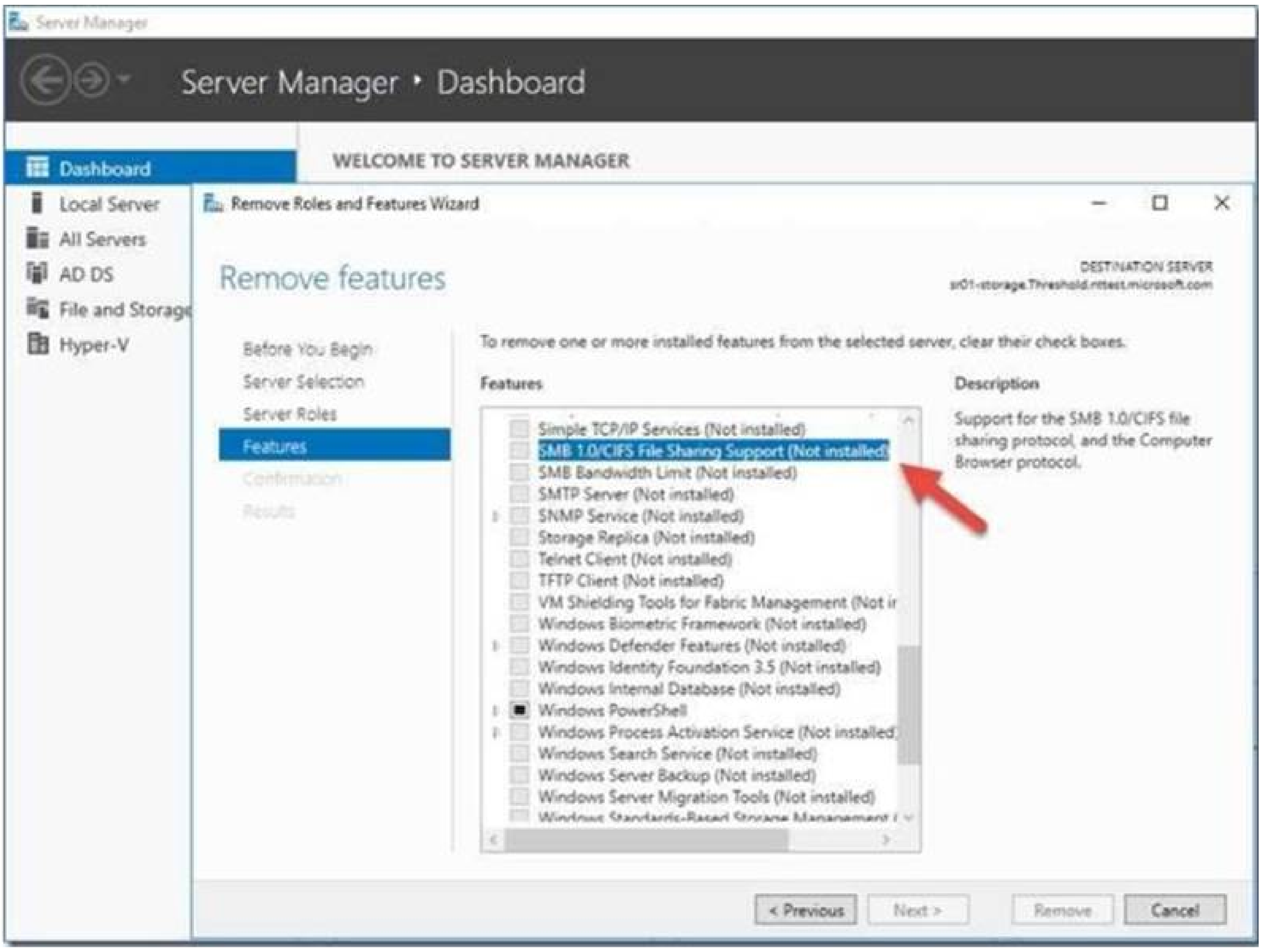
Server name	Configuration
Nano1	Nano Server
Nano2	Nano Server
Server2	File server that has a shared folder named DATA
Server3	DNS server that has a DNSSEC-signed zone named adatum.com
Server4	Hyper-V host
Server1	Application server

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

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

Answer: D

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



Remove features

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

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

Features

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

Description

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

NEW QUESTION 8
Your network contains an Active Directory domain named contoso.com. You create a Microsoft Operations Management Suite (OMS) workspace. You need to connect several computers directly to the workspace.
Which two pieces of information do you require? Each correct answer presents part of the solution.

A. the ID of the workspace
B. the name of the workspace
C. the URL of the workspace
D. the key of the workspace

Answer: A

NEW QUESTION 9
____ 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 10
This question relates to Windows Firewall and related technologies. These rules use IPsec to secure traffic while it crosses the network.
You use these rules to specify that connections between two computers must be authenticated or encrypted.
What is the name for these rules?

A. Connection Security Rules
B. Firewall Rules
C. TCP Rules
D. DHP Rules

Answer: A

NEW QUESTION 10

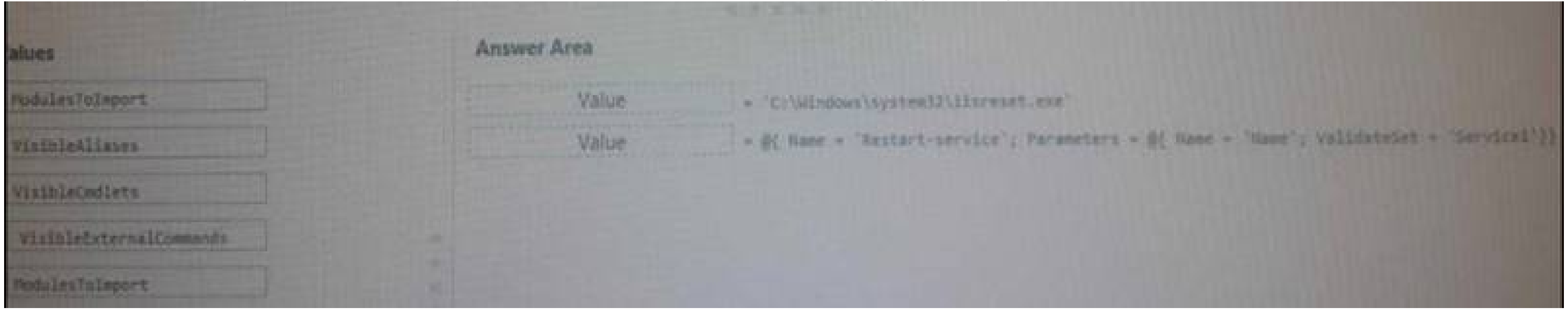
Windows Firewall rules can be configured using PowerShell.
The “Set-NetFirewallProfile” cmdlet configures settings that apply to the per-profile configurations of the Windows Firewall with Advanced Security.
What is the default setting for the AllowInboundRules parameter when managing a GPO?

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 11
DRAG DROP
You configure Just Enough Administration (JEA).
You need to ensure that a non-administrator user can perform the following actions:
-Restart Internet Information Services (IIS)
-Restart a custom service named Service1.
How should you complete the role configuration file? To answer, select the appropriate options in the answer area.



alues

ModulesToImport

VisibleAliases

VisibleCmdlets

VisibleExternalCommands

ModulesToImport

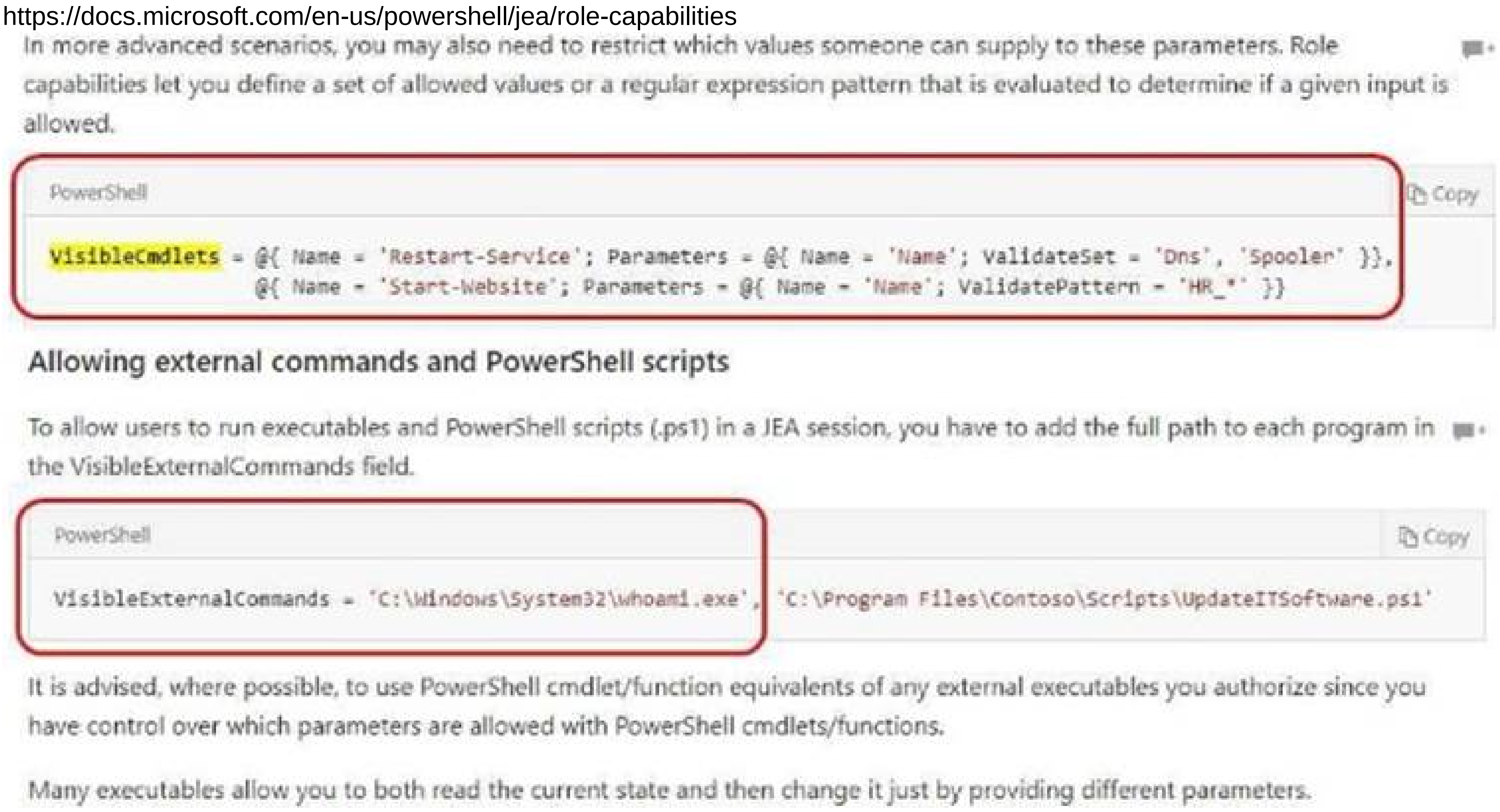
Answer Area

```
Value = 'C:\Windows\system32\iisreset.exe'
Value = @{ Name = 'Restart-service'; Parameters = @{ Name = 'Name'; ValidateSet = 'Service1'}}
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
VisibleExternalCommands = ‘C:\\Windows\\system32\\iisreset.exe’
VisibleCmdlets = @{ Name ‘Restart-service’ ; Parameters @{ Name = ‘Name’; ValidateSet = ‘Service1’}}
https://docs.microsoft.com/en-us/powershell/jea/role-capabilities



In more advanced scenarios, you may also need to restrict which values someone can supply to these parameters. Role capabilities let you define a set of allowed values or a regular expression pattern that is evaluated to determine if a given input is allowed.

PowerShell

```
VisibleCmdlets = @{ Name = 'Restart-Service'; Parameters = @{ Name = 'Name'; ValidateSet = 'Dns', 'Spooler' }},
                 @{ Name = 'Start-Website'; Parameters = @{ Name = 'Name'; ValidatePattern = 'HR_*' }}
```

Allowing external commands and PowerShell scripts

To allow users to run executables and PowerShell scripts (.ps1) in a JEA session, you have to add the full path to each program in the VisibleExternalCommands field.

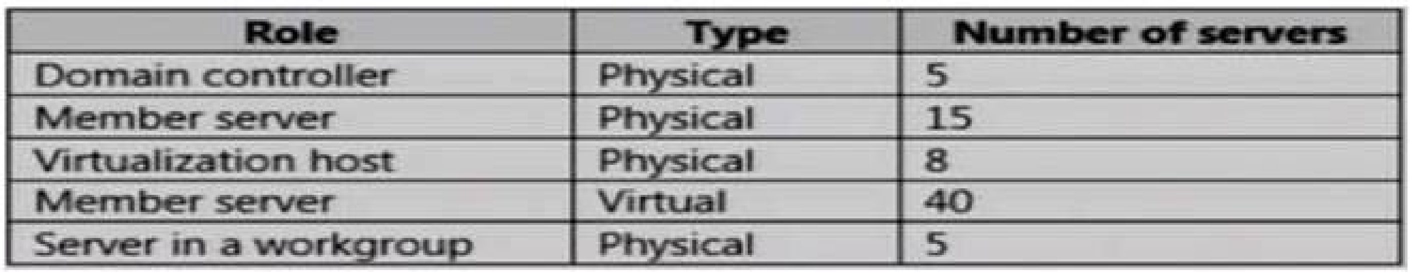
PowerShell

```
VisibleExternalCommands = 'C:\Windows\System32\whoami.exe', 'C:\Program Files\Contoso\Scripts\UpdateITSoftware.ps1'
```

It is advised, where possible, to use PowerShell cmdlet/function equivalents of any external executables you authorize since you have control over which parameters are allowed with PowerShell cmdlets/functions.

Many executables allow you to both read the current state and then change it just by providing different parameters.

NEW QUESTION 16
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

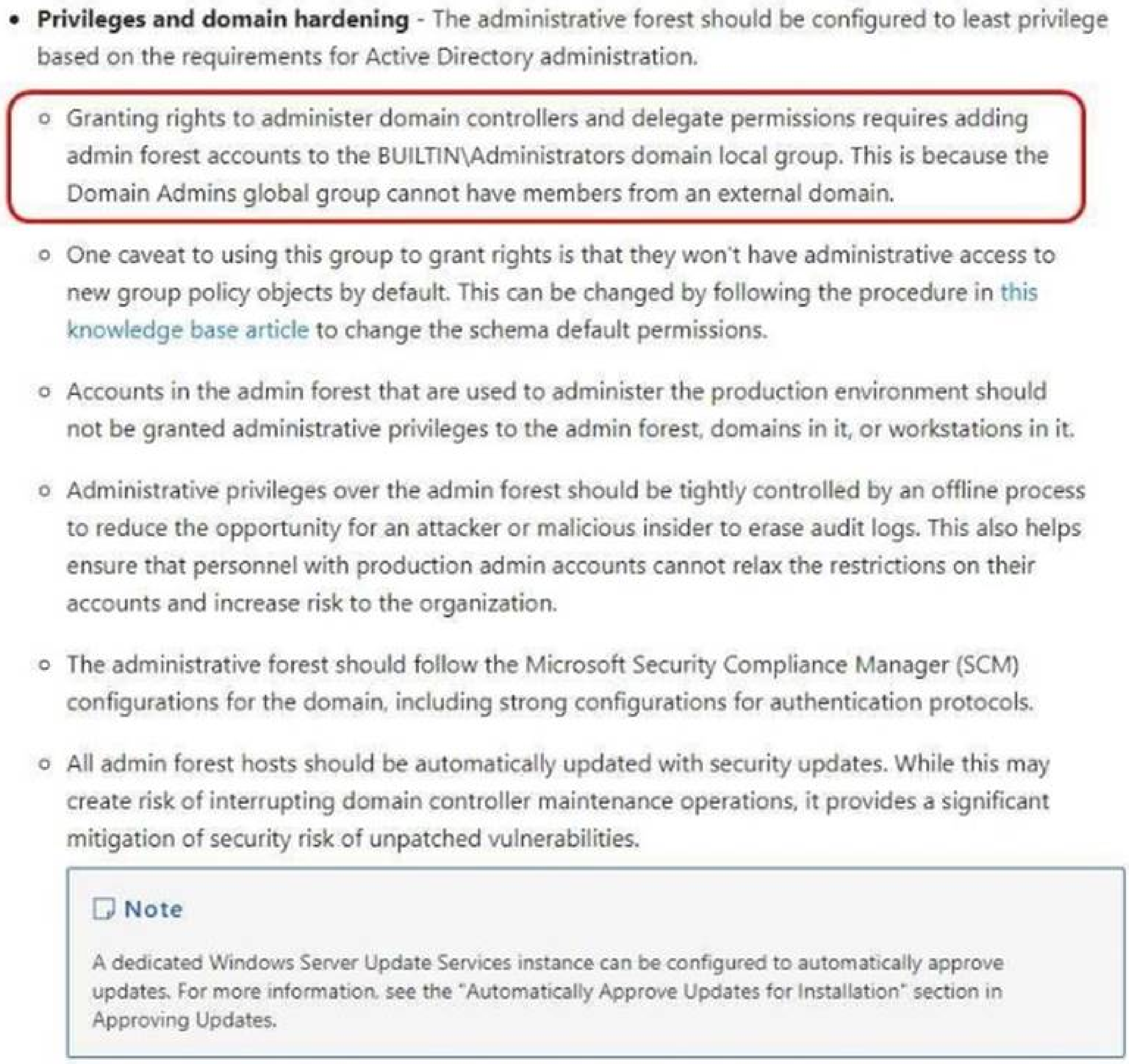
Explanation:
-Antimalware data from all the servers must be visible in Workspace1.
-Security and audit data from the domain controllers and the virtualization hosts must be visible in Workspace2.
-System update data from all the servers in all the workgroups must be visible in Workspace& "All the servers" 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 18
Your network contains an Active Directory forest named contoso.com. All servers run Windows Server 2016.
You implement a single-domain administrative forest named admin.contoso.com that has Enhanced Security Administrative Environment (ESAE) deployed.
You have an administrative user named Admin1 in admin.contoso.com.
You need to ensure that Admin1 can manage the domain controllers in contoso.com. To which group should you add Admin1?

A. Contoso\\Domain Admins
B. Admin\\Administrators
C. Admin\\Domain Admins
D. Contoso\\Administrators

Answer: D

Explanation:
admin.contoso.com (NetBIOS domain name "ADMIN\\") is the administrative domain. contoso.com (NetBIOS domain name "CONTOSO\\") is the corporate resource domain. See below.
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securingprivilegedaccess- reference-material



- **Privileges and domain hardening** - The administrative forest should be configured to least privilege based on the requirements for Active Directory administration.
  - Granting rights to administer domain controllers and delegate permissions requires adding admin forest accounts to the BUILTIN\Administrators domain local group. This is because the Domain Admins global group cannot have members from an external domain.
  - One caveat to using this group to grant rights is that they won't have administrative access to new group policy objects by default. This can be changed by following the procedure in this knowledge base article to change the schema default permissions.
  - Accounts in the admin forest that are used to administer the production environment should not be granted administrative privileges to the admin forest, domains in it, or workstations in it.
  - Administrative privileges over the admin forest should be tightly controlled by an offline process to reduce the opportunity for an attacker or malicious insider to erase audit logs. This also helps ensure that personnel with production admin accounts cannot relax the restrictions on their accounts and increase risk to the organization.
  - The administrative forest should follow the Microsoft Security Compliance Manager (SCM) configurations for the domain, including strong configurations for authentication protocols.
  - All admin forest hosts should be automatically updated with security updates. While this may create risk of interrupting domain controller maintenance operations, it provides a significant mitigation of security risk of unpatched vulnerabilities.

> **Note**
>
> A dedicated Windows Server Update Services instance can be configured to automatically approve updates. For more information, see the "Automatically Approve Updates for Installation" section in Approving Updates.

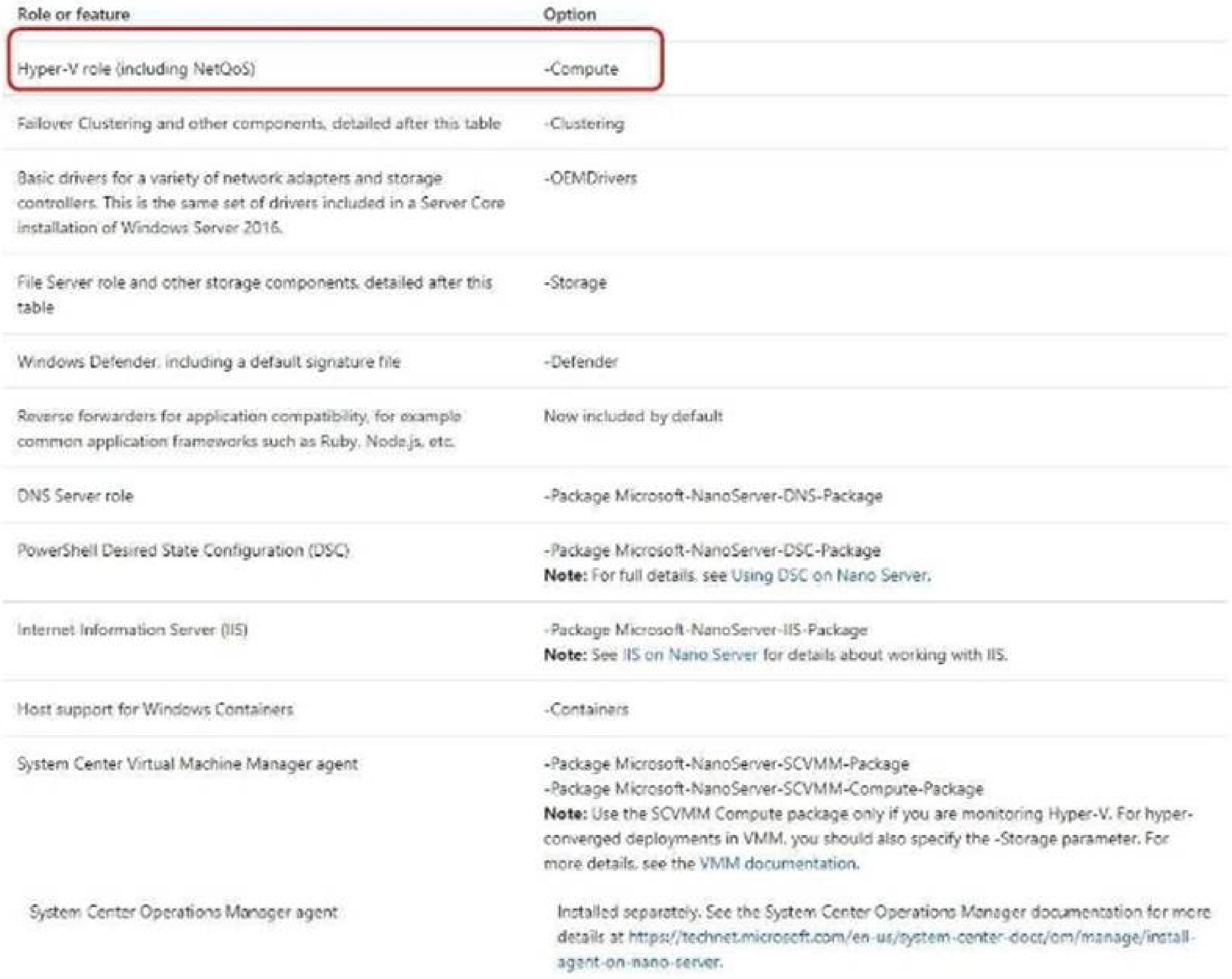
NEW QUESTION 22

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 23

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?

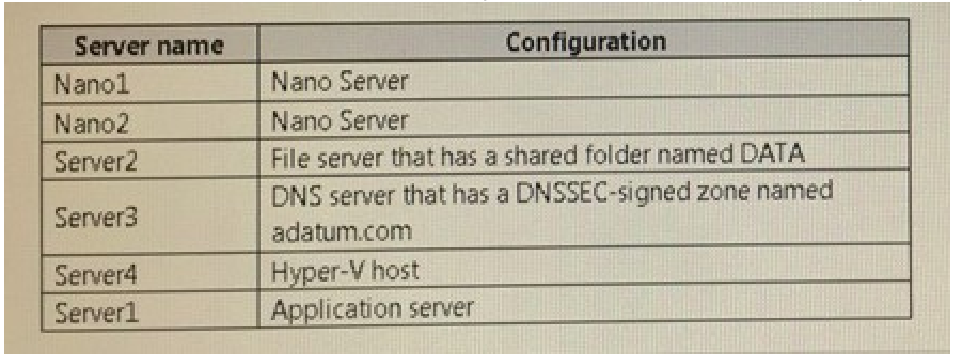
A. Install-HgsServer
B. Install-Module
C. Install-Package
D. Enable-WindowsOptionalFeature
E. Install-ADDSDomainController

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 25
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 26
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

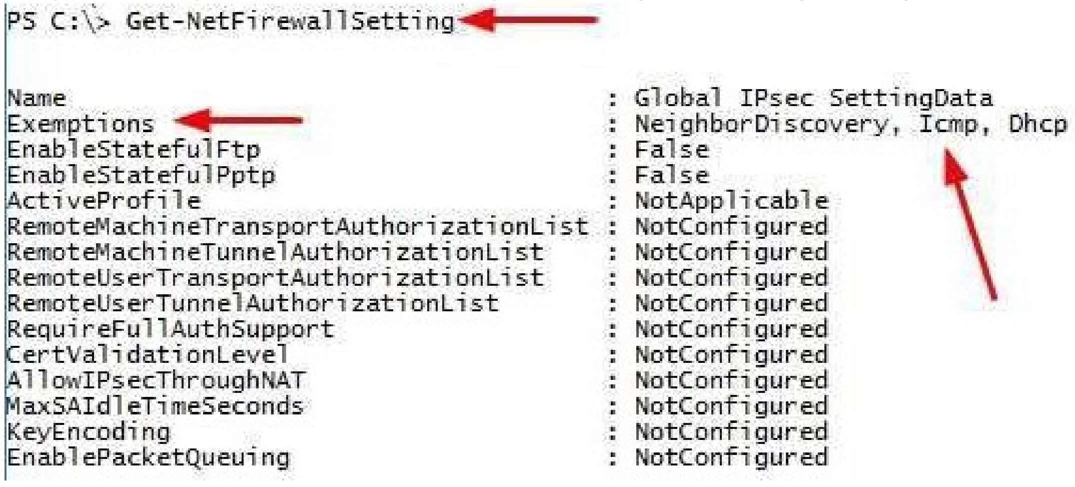
Explanation:
In IPsec connection security rule, the IPsec protocol verifies the sending host IP address by utilize integrity
functions like Digitally signing all packets.
If unsigned packets arrives Server11, those are possible source address spoofed packets, when using connection security rule in-conjunction 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 30
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

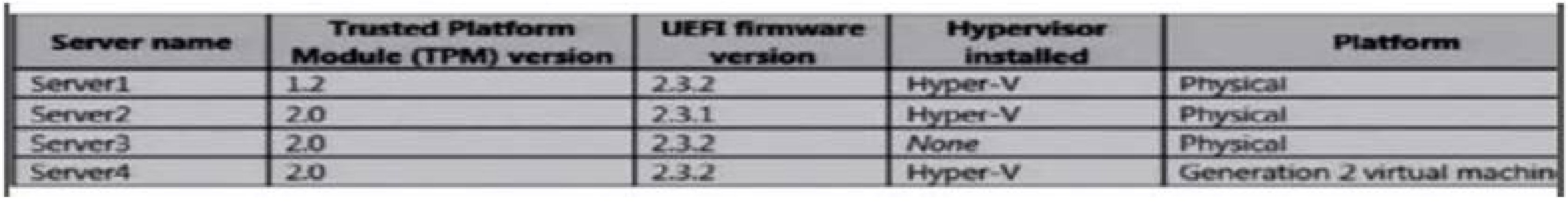
Explanation:
The Get-NetFirewallSetting cmdlet retrieves the global firewall settings of the target computer. The NetFirewallSetting object specifies properties that apply to the firewall and IPsec settings, no matter which
network profile is currently in use.
The global configurations include viewing 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 33
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

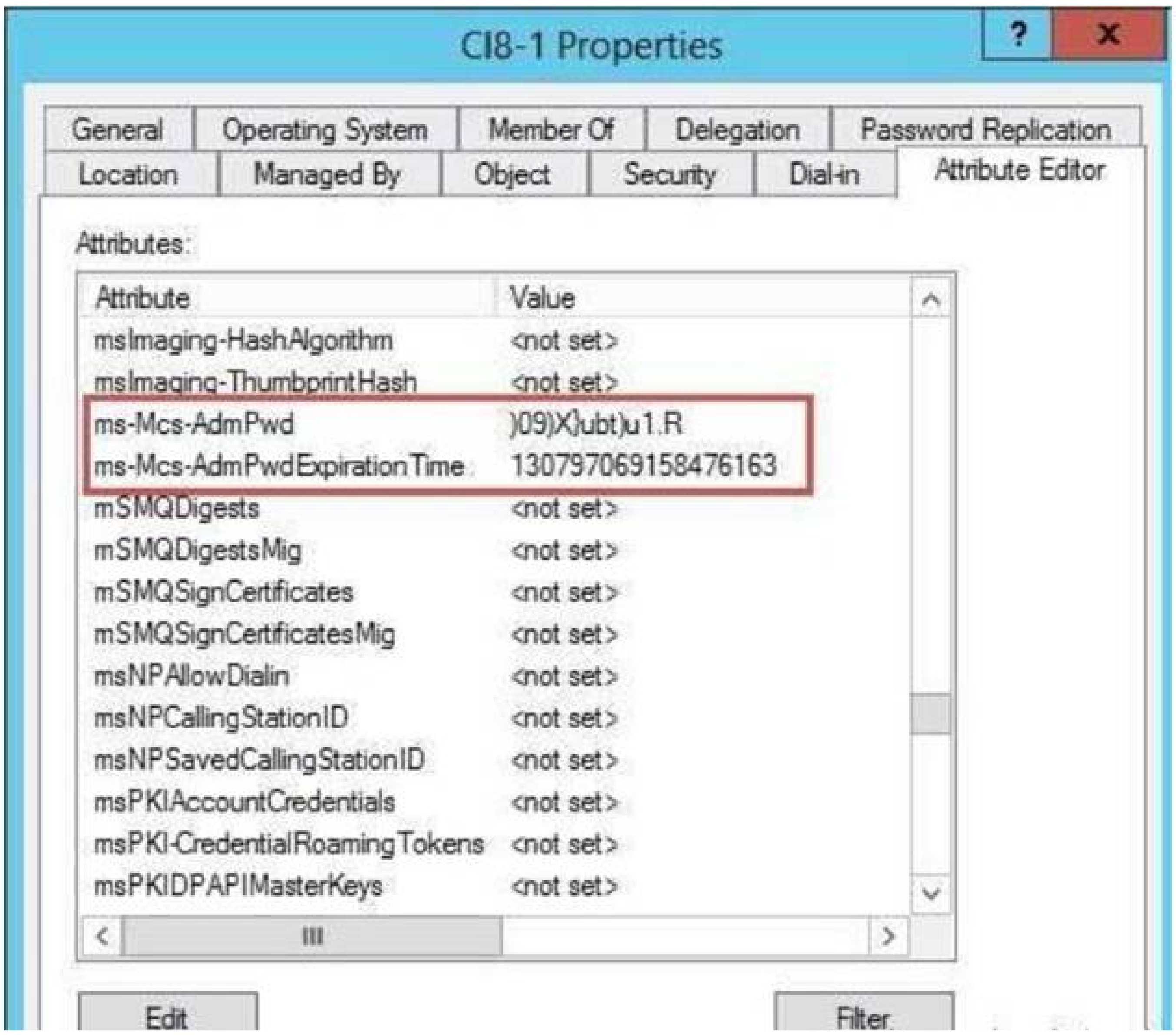
Explanation:
https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guardrequirements Hardware and software requirements
To provide basic protections against OS level attempts to read Credential Manager domain credentials, NTLM
and Kerberos derived credentials, Windows 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 37
Your network contains an Active Directory domain named contoso.com.
The domain contains a server named Server1 that runs Windows Server 2016.
The local administrator credentials of Server1 are managed by using the Local Administrator Password Solution (LAPS).
You need to retrieve the password of the Administrator account on Server1. What should you do?

A. From Windows PowerShell on Server1, run the Get-ADFineGrainedPasswordPolicy cmdlet and specify the -Credential parameter.
B. From Windows PowerShell on Server1, run the Get-ADUser cmdlet and specify the -Credential parameter.
C. From Active Directory Users and Computers, open the properties at Server1 and view the value at the msMcs-AdmPwd attribute
D. From Active Directory Users and Computers, open the properties of Administrator and view the value of the userPassword attribute

Answer: C

Explanation:
The “ms-Mcs-AdmPwd” attribute of a computer account in Active Directory Users and Computers stores the local Administrator password of a computer, which is configured by LAPS.



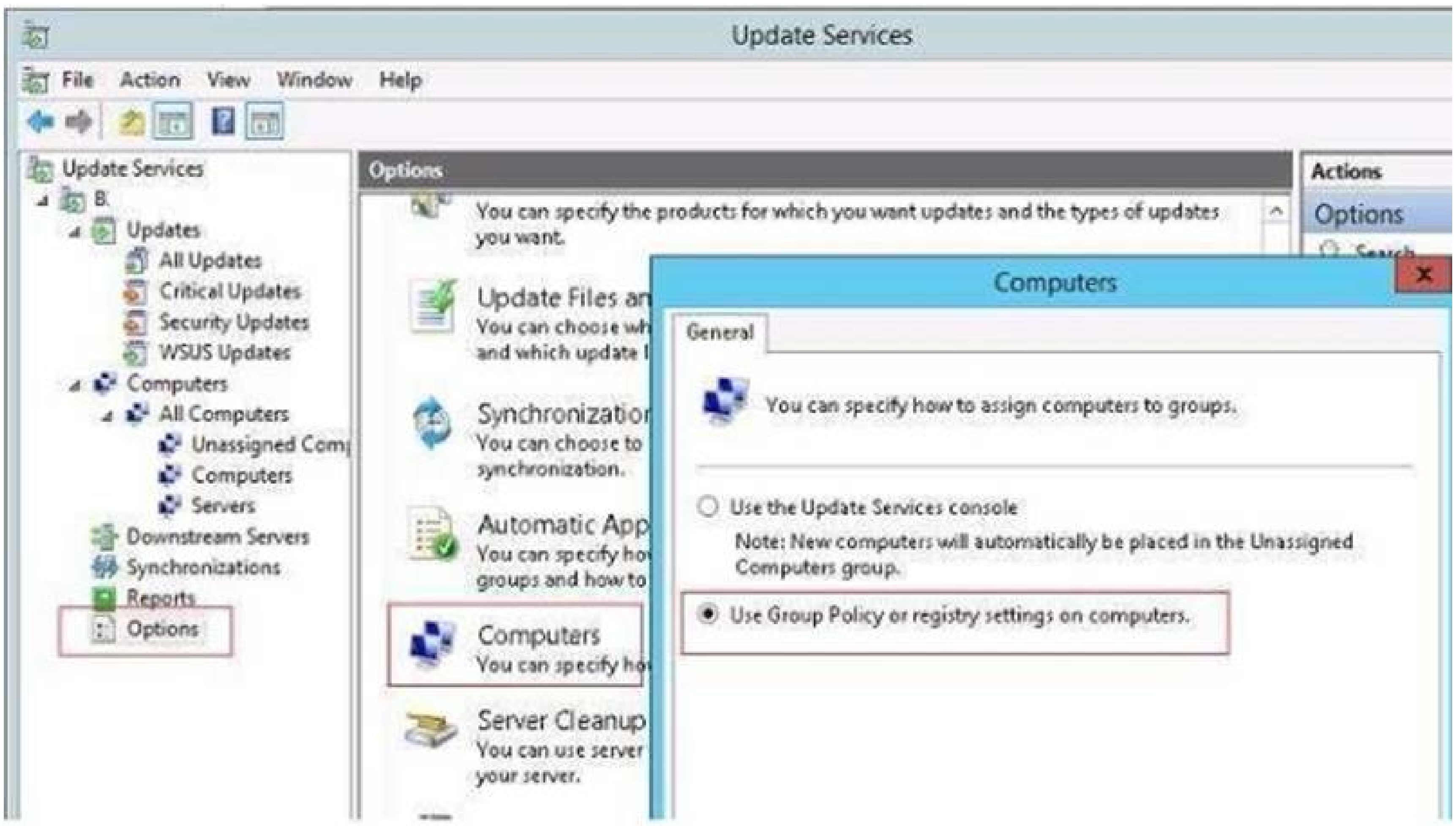
Attribute	Value
msImaging-HashAlgorithm	<not set>
msImaging-ThumbprintHash	<not set>
ms-Mcs-AdmPwd	)09)X}ubt)u1.R
ms-Mcs-AdmPwdExpirationTime	130797069158476163
mSMQDigests	<not set>
mSMQDigestsMig	<not set>
mSMQSignCertificates	<not set>
mSMQSignCertificatesMig	<not set>
msNPAllowDialin	<not set>
msNPCallingStationID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

NEW QUESTION 39
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 wuauclt.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&MSPPError=- 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.



You can specify the products for which you want updates and the types of updates you want.

Computers

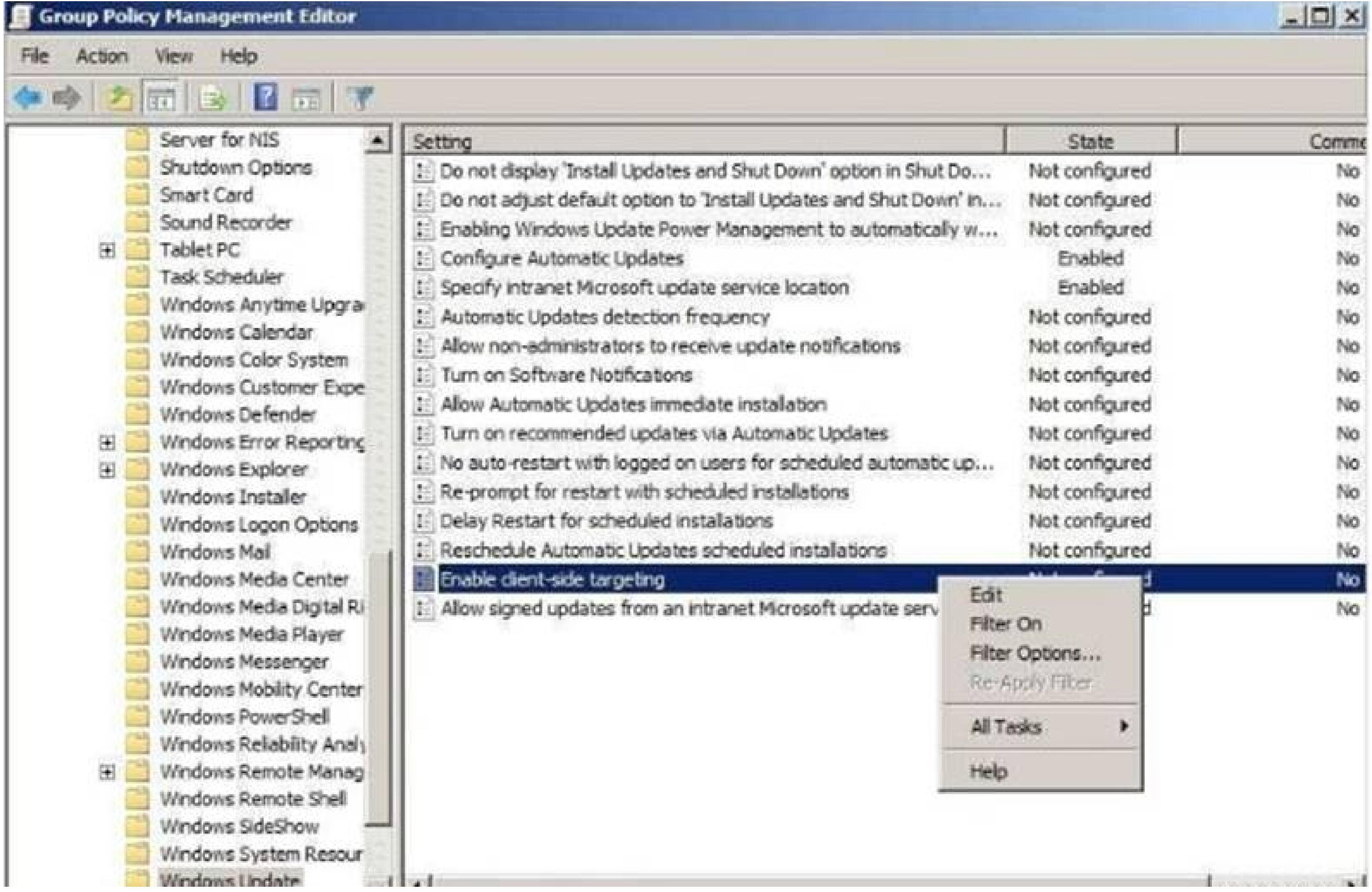
You can specify how to assign computers to groups.

○ Use the Update Services console

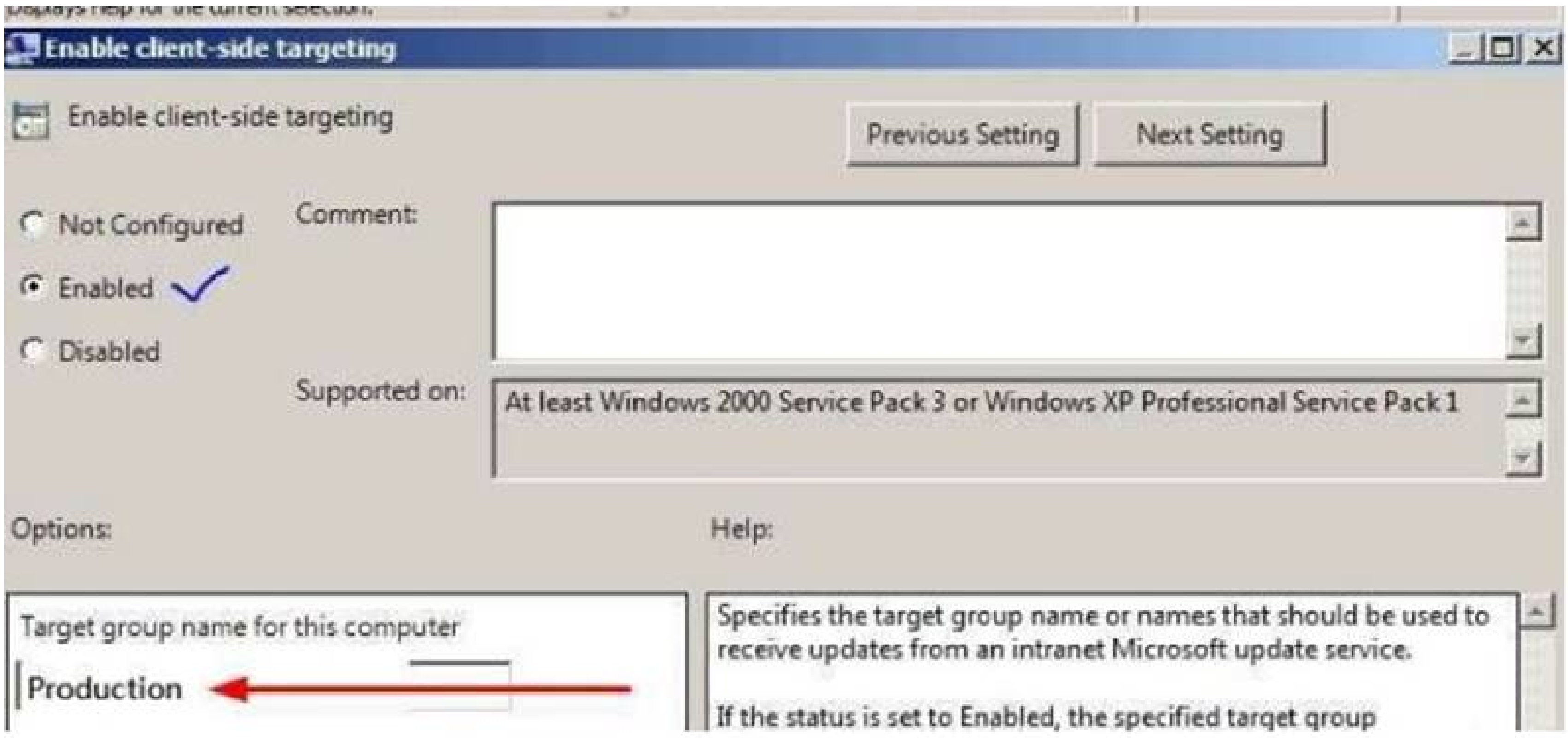
Note: New computers will automatically be placed in the Unassigned Computers group.

● Use Group Policy or registry settings on computers.

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



Setting	State	Comme
Do not display 'Install Updates and Shut Down' option in Shut Do...	Not configured	No
Do not adjust default option to 'Install Updates and Shut Down' in...	Not configured	No
Enabling Windows Update Power Management to automatically w...	Not configured	No
Configure Automatic Updates	Enabled	No
Specify intranet Microsoft update service location	Enabled	No
Automatic Updates detection frequency	Not configured	No
Allow non-administrators to receive update notifications	Not configured	No
Turn on Software Notifications	Not configured	No
Allow Automatic Updates immediate installation	Not configured	No
Turn on recommended updates via Automatic Updates	Not configured	No
No auto-restart with logged on users for scheduled automatic up...	Not configured	No
Re-prompt for restart with scheduled installations	Not configured	No
Delay Restart for scheduled installations	Not configured	No
Reschedule Automatic Updates scheduled installations	Not configured	No
Enable client-side targeting	N[illegible]d	No
Allow signed updates from an intranet Microsoft update serv	[illegible]d	No



Enable client-side targeting

Enable client-side targeting

○ Not Configured
● Enabled ✓
○ Disabled

Comment:

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

Options:

Target group name for this computer

Production

Help:

Specifies the target group name or names that should be used to receive updates from an intranet Microsoft update service.

If the status is set to Enabled, the specified target group

NEW QUESTION 43
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

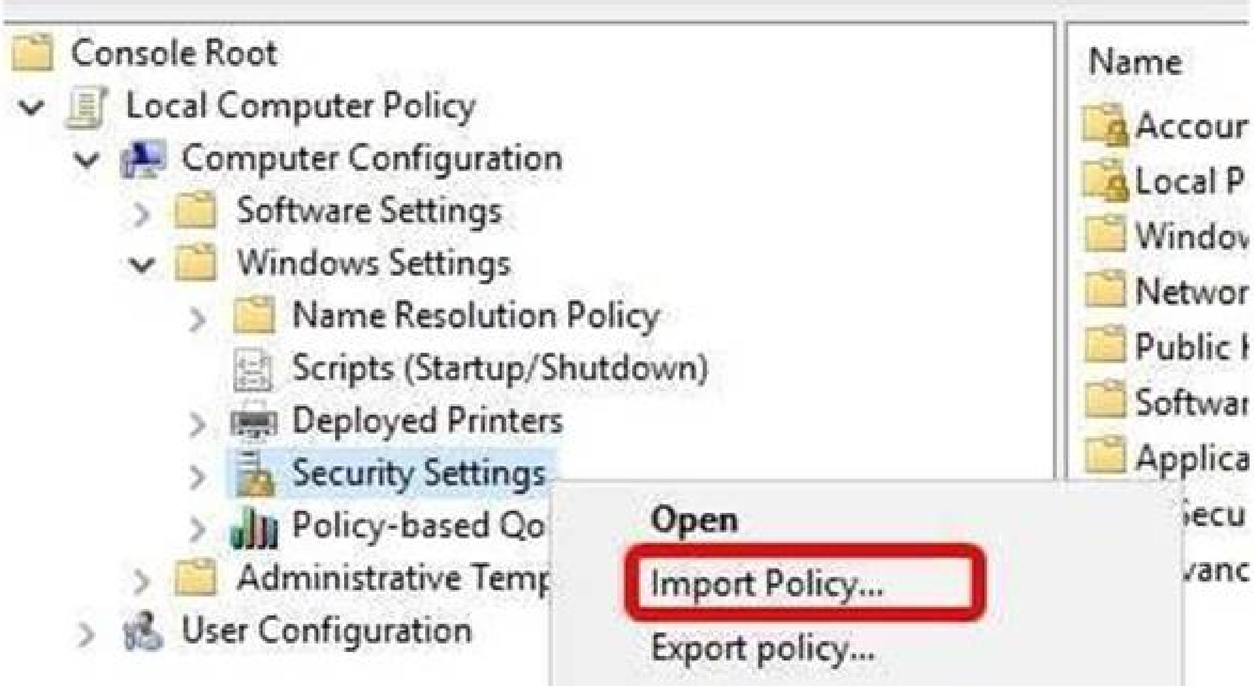
Explanation:
Use “Active Directory Users and Computers” to view the attribute value of “ms-MCS-adminpwd” of the Server5 computer account https://blogs.technet.microsoft.com/askpfeplat/2015/12/28/local-administrator-password-solutionlapsimplementation- hints-and-security-nerd-commentaryincludingmini-threat-model/

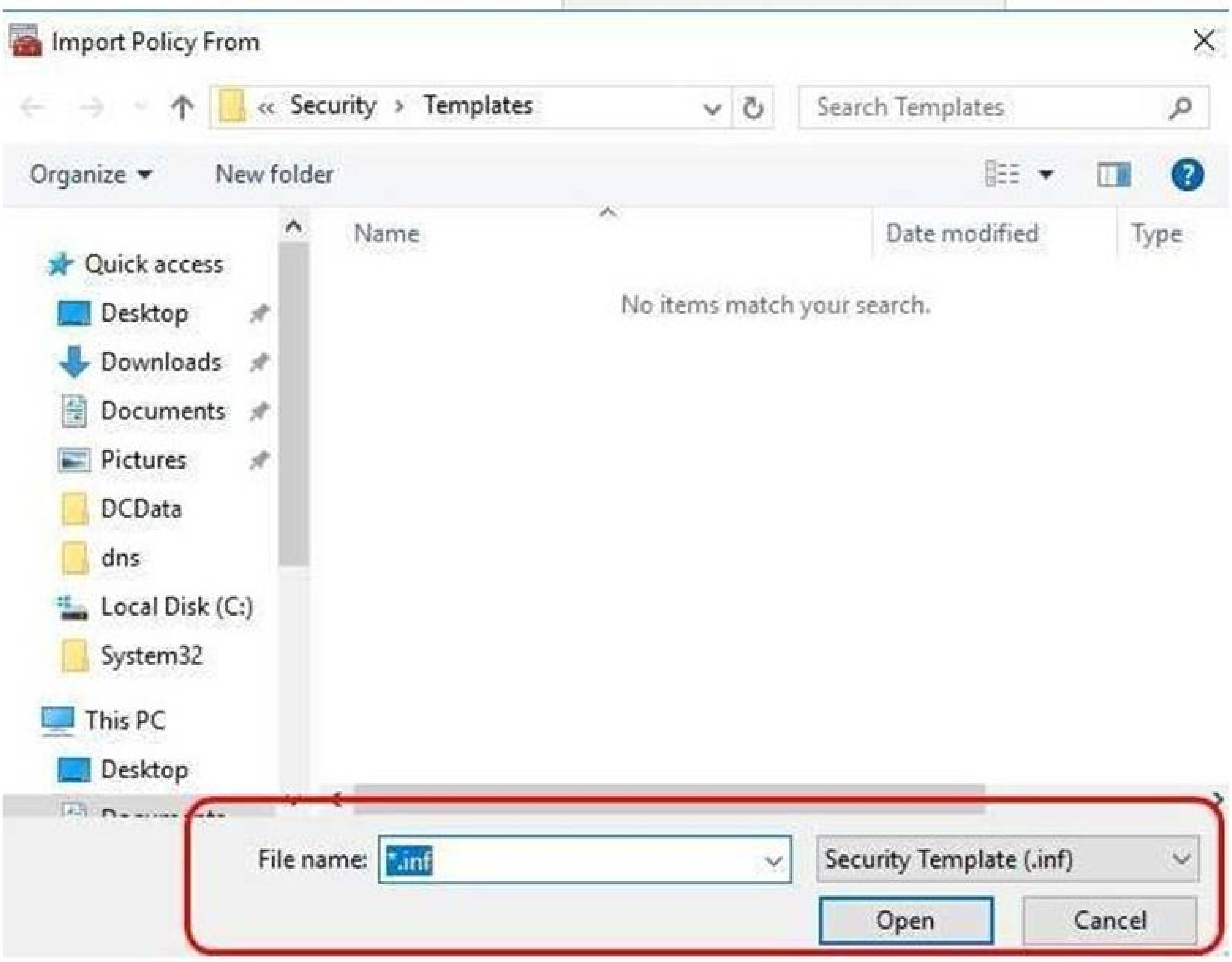
NEW QUESTION 45
Your network contains an internal network and a perimeter network. The internal network contains an Active Directory forest named contoso.com.
You deploy five servers to the perimeter network.
All of the servers run Windows Server 2016 and are the members of a workgroup.
You need to apply 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 49

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 53

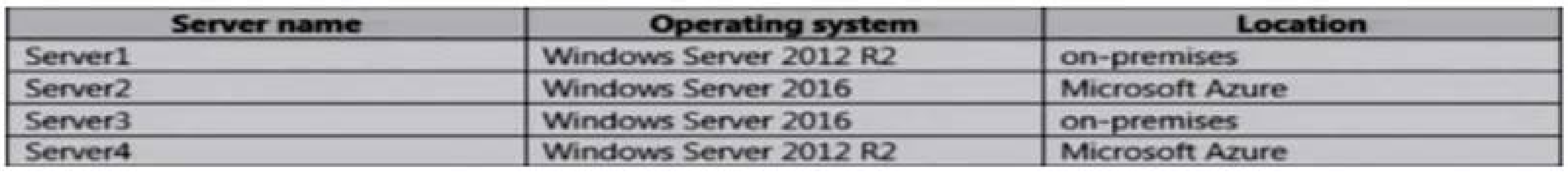
Your network contains an Active Directory domain named contoso.com.

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 57
Your network contains an Active Directory domain named contoso.com. All client computers run Windows 10.
You plan to deploy a Remote Desktop connection solution for the client computers.
You have four available servers in the domain that can be configured as Remote Desktop servers. The servers are configured as shown in the following table.



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

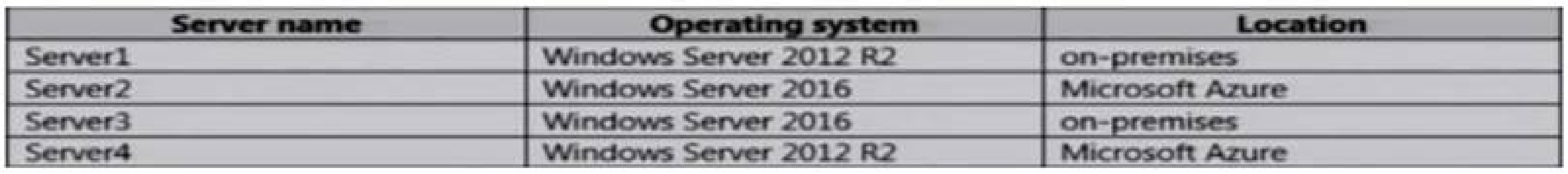
You need to ensure that all Remote Desktop connections can be protected by using Remote Credential Guard.
Solution: You deploy the Remote Desktop connection solution by using Server4. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
No, as Server4 is a Windows Server 2012R2 which does not meet the requirements of Remote Credential Guard.
https://docs.microsoft.com/en-us/windows/access-protection/remote-credential-guard Remote Credential Guard requirements
To use Windows Defender Remote Credential Guard, the Remote Desktop client and remote host must meet the following requirements:
The Remote Desktop client device:
Must be running at least Windows 10, version 1703 to be able to supply credentials.
Must be running at least Windows 10, version 1607 or Windows Server 2016 to use the user's signed-in credentials. This requires the user's account be able to sign in to both the client device and the remote host.
Must be running the Remote Desktop Classic Windows application. The Remote Desktop Universal Windows Platform application doesn't support Windows Defender Remote Credential Guard.
Must use Kerberos authentication to connect to the remote host. If the client cannot connect to a domain controller, then RDP attempts to fall back to NTLM.
Windows Defender Remote Credential Guard does not allow NTLM fallback because this would expose credentials to risk.
The Remote Desktop remote host:
Must be running at least Windows 10, version 1607 or Windows Server 2016. Must allow Restricted Admin connections.
Must allow the client's domain user to access Remote Desktop connections. Must allow delegation of non-exportable credentials.

NEW QUESTION 58
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

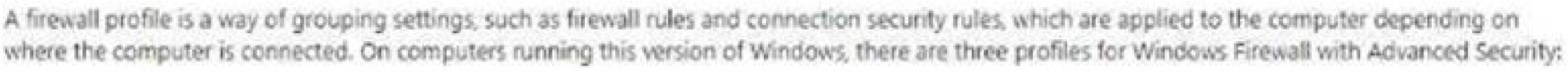
Platform application doesn't support Windows Defender Remote Credential Guard.
Must use Kerberos authentication to connect to the remote host. If the client cannot connect to a domain controller, then RDP attempts to fall back to NTLM.
Windows Defender Remote Credential Guard does not allow NTLM fallback 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.

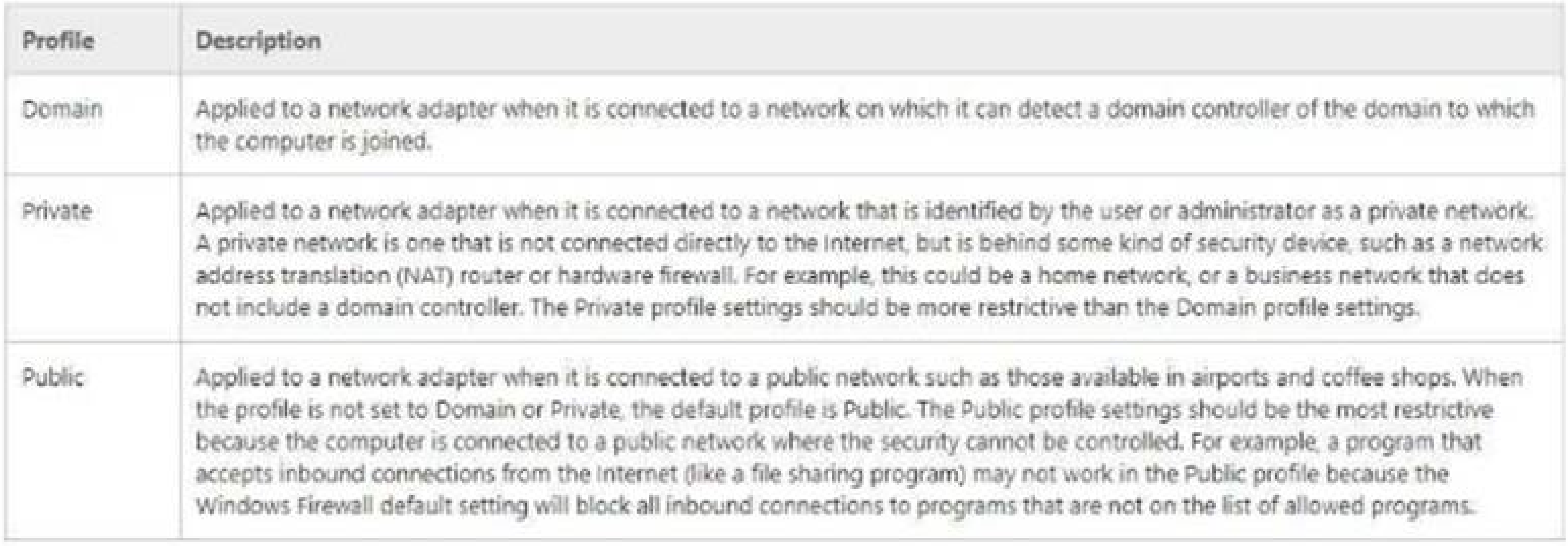
NEW QUESTION 59
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. The network uses the 172.16.0.0/16 address space.
Computer1 has an application named App1.exe that is located in D:\\Apps\\. App1.exe is configured 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 60
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 62
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.

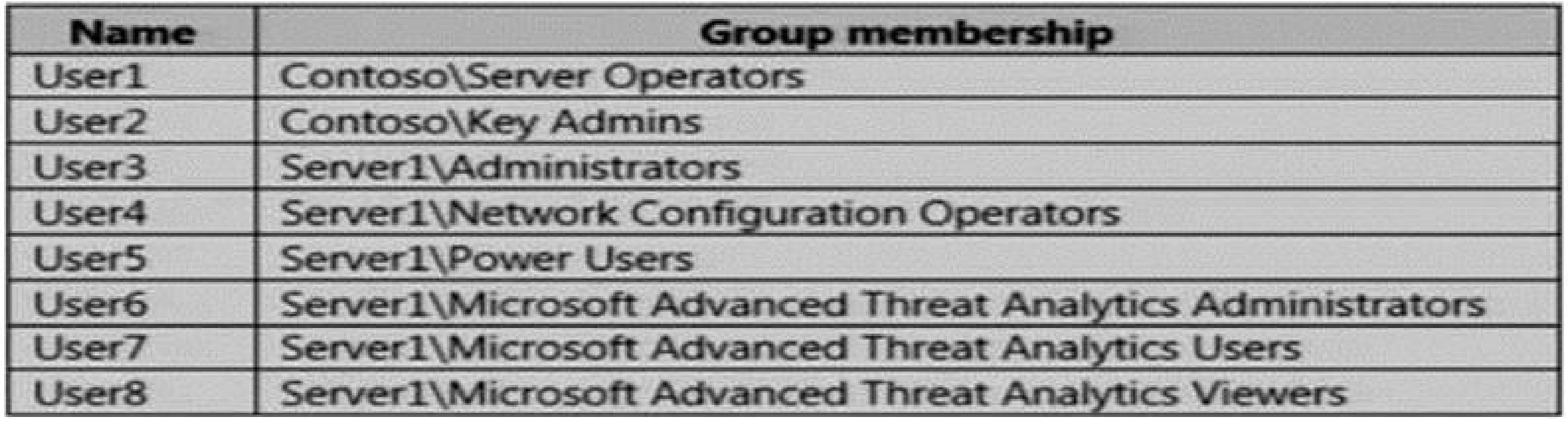
NEW QUESTION 66
You are building a guarded fabric. You need to configure Admin-trusted attestation. Which cmdlet should you use?

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

Answer: A

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

NEW QUESTION 71
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2016.
The Microsoft Advanced Threat Analytics (ATA) Center service is installed on Server1. The domain contains the users shown in the following table.



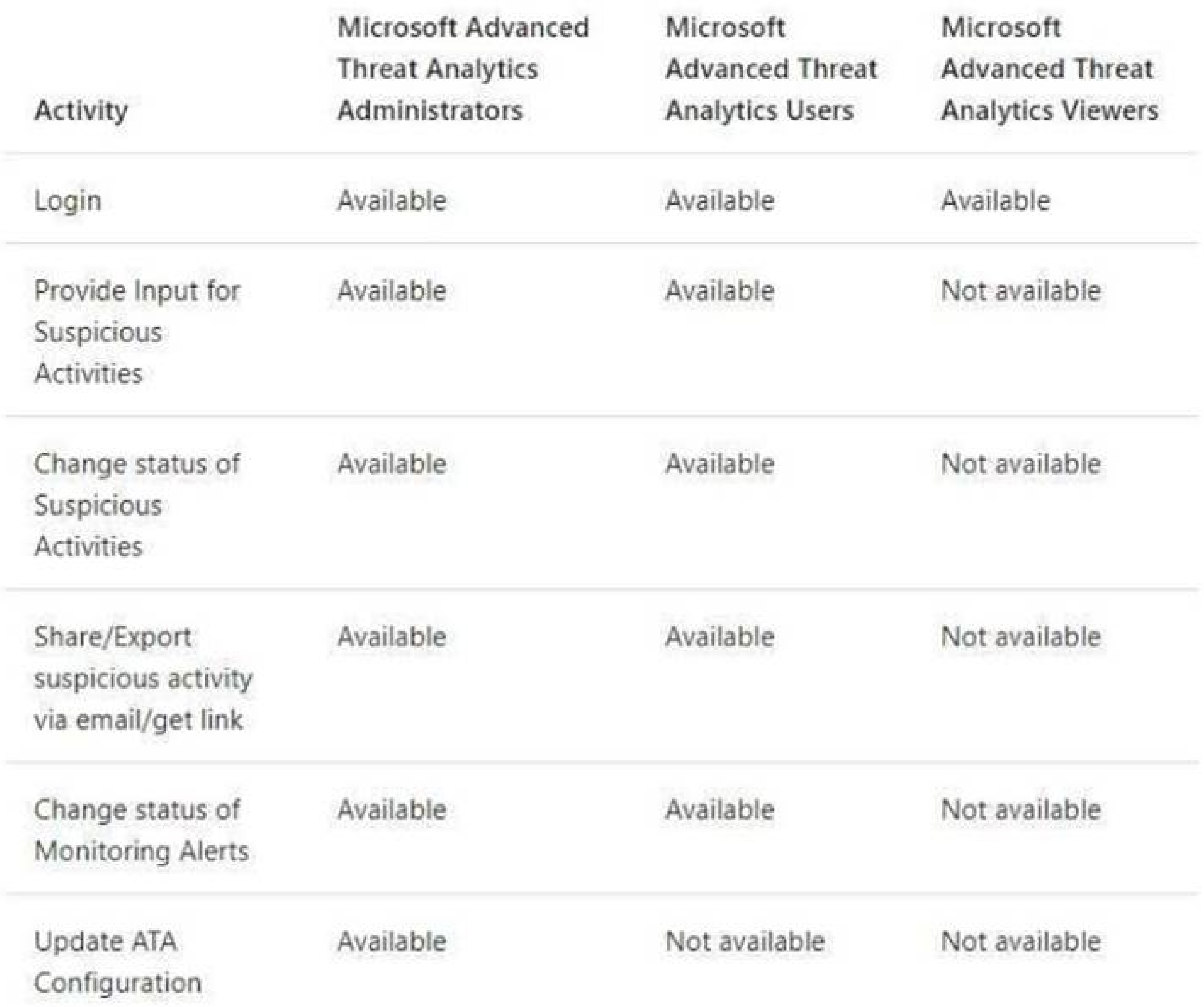
Name	Group membership
User1	Contoso\Server Operators
User2	Contoso\Key Admins
User3	Server1\Administrators
User4	Server1\Network Configuration Operators
User5	Server1\Power Users
User6	Server1\Microsoft Advanced Threat Analytics Administrators
User7	Server1\Microsoft Advanced Threat Analytics Users
User8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

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

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

Answer: F

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



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

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

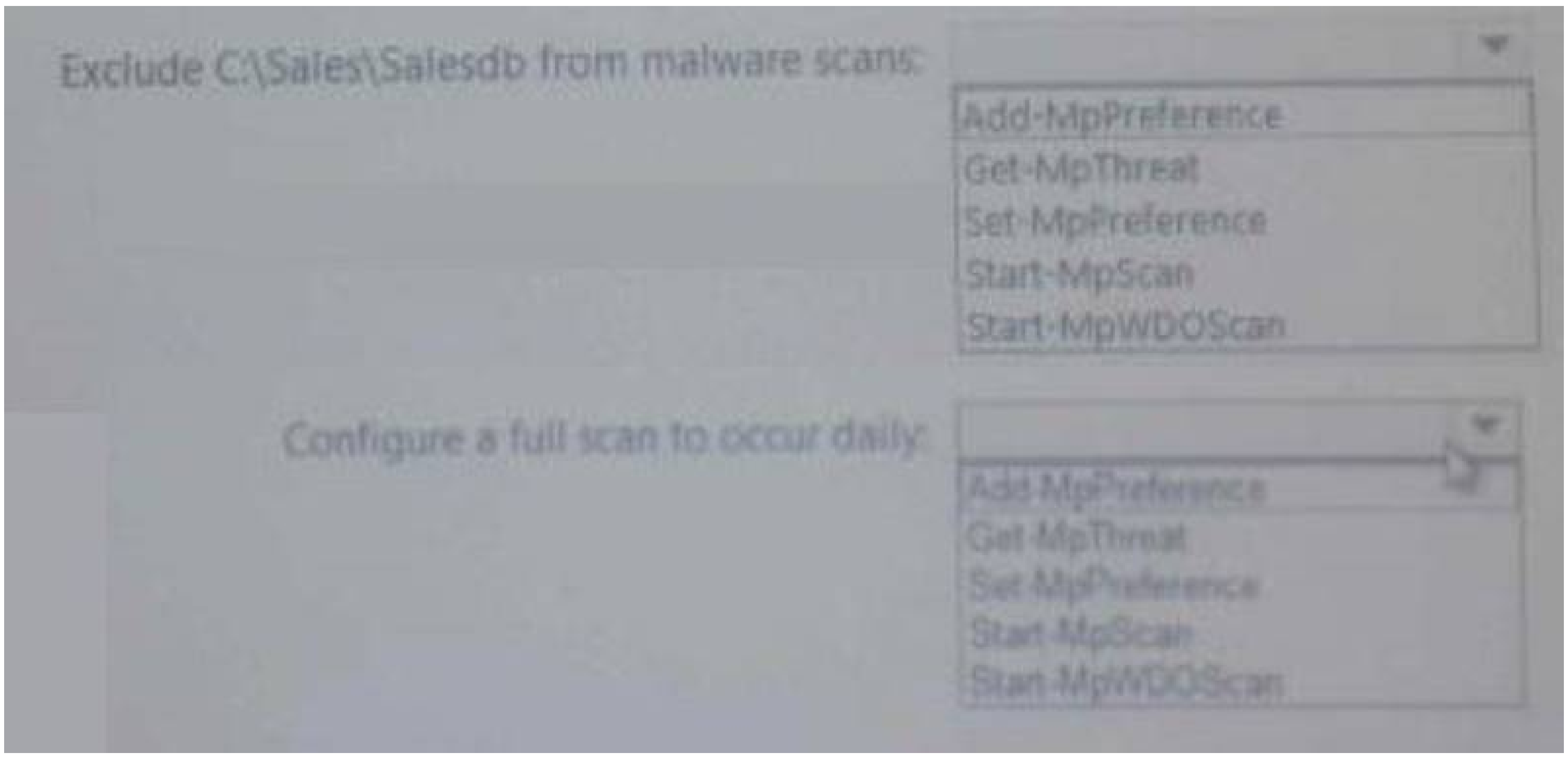
NEW QUESTION 76
Your network contains an Active Directory forest named corp.contoso.com.
You are implementing Privileged Access Management (PAM) by using a bastion forest named priv.contoso.com.
You need to create shadow groups in priv.contoso.com. Which cmdlet should you use?

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 81
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?



Exclude C:\Sales\Salesdb from malware scans:

- Add-MpPreference
- Get-MpThreat
- Set-MpPreference
- Start-MpScan
- Start-MpWDOScan

Configure a full scan to occur daily:

- Add-MpPreference
- Get-MpThreat
- Set-MpPreference
- Start-MpScan
- Start-MpWDOScan

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 83
You have the Windows Server 2016 operating system images as following table.

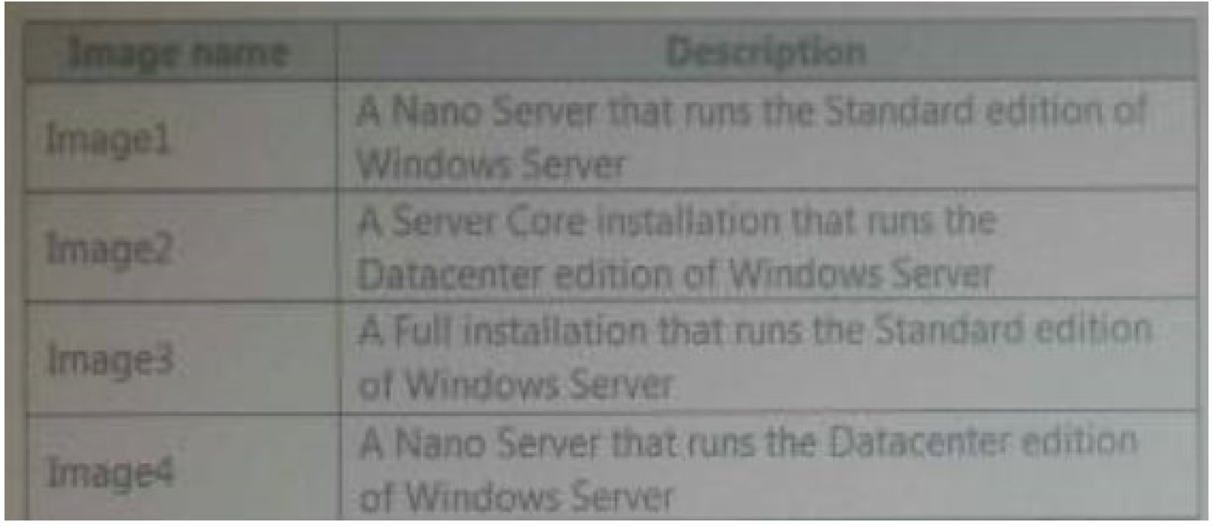


Image name	Description
Image1	A Nano Server that runs the Standard edition of Windows Server
Image2	A Server Core installation that runs the Datacenter edition of Windows Server
Image3	A Full installation that runs the Standard edition of Windows Server
Image4	A Nano Server that runs the Datacenter edition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

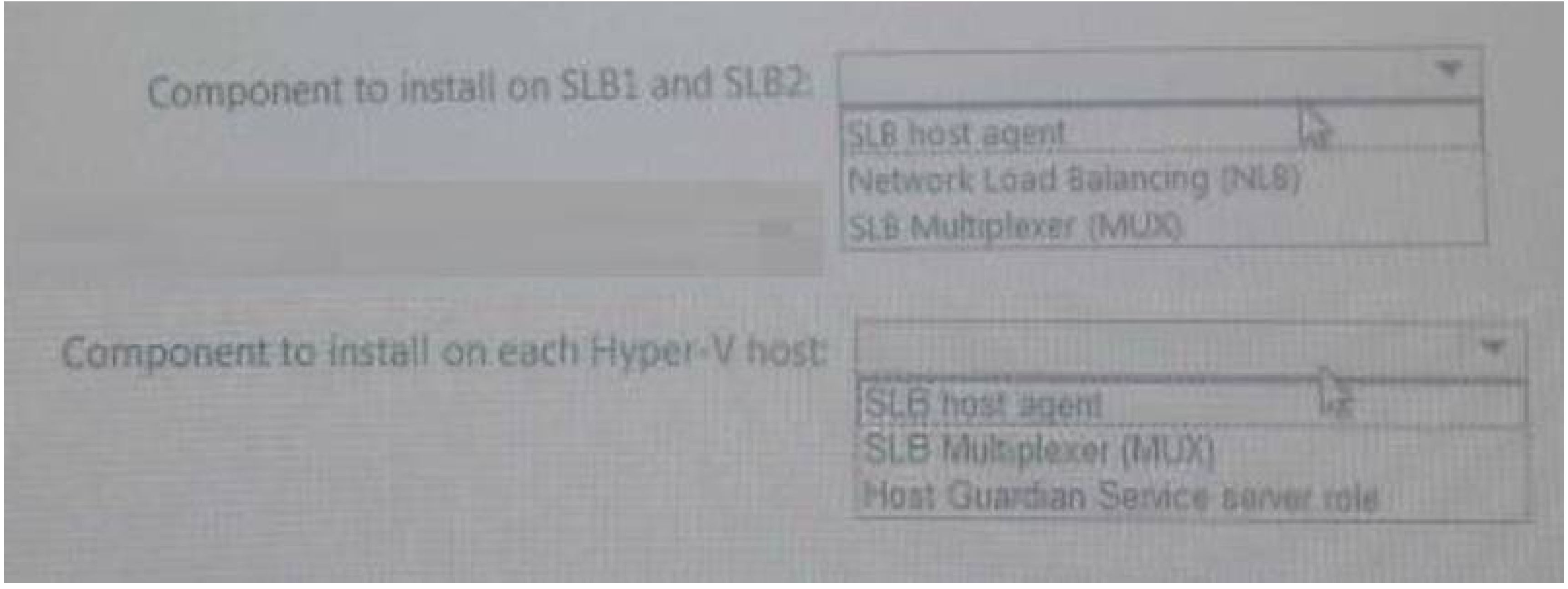
A. image1
B. image2
C. image3
D. image4

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 85
HOTSPOT
You have 10 Hyper-V hosts that run Windows Server 2016.
Each Hyper-V host has eight virtual machines that run a distributed web application named App1. You plan to implement a Software Load Balancing (SLB) solution for client access to App1. You deploy two new virtual machines named SLB1 and SLB2.

You need to install the required components on the Hyper-V hosts and the new servers for the planned implementation.
Which components should you install? Select the Appropriate in selection area.



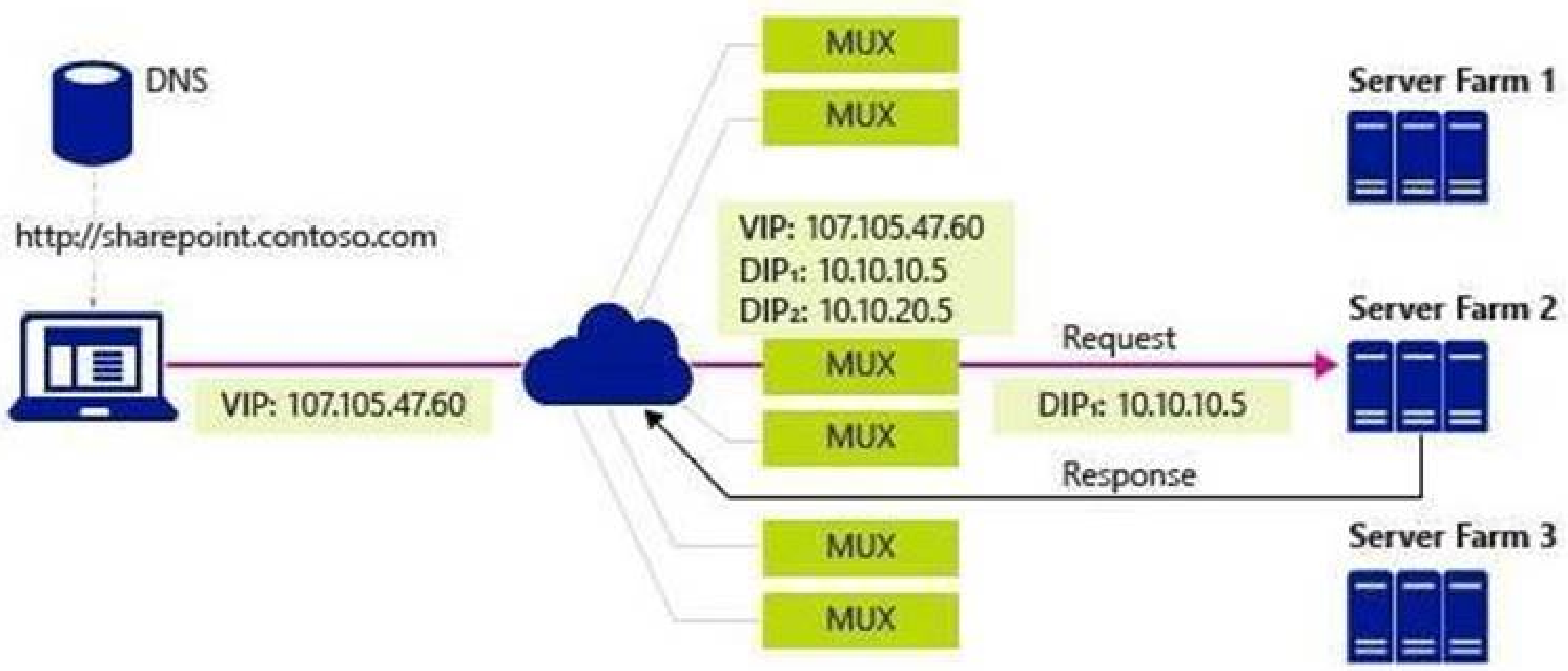
Component to install on SLB1 and SLB2:
- SLB host agent
- Network Load Balancing (NLB)
- SLB Multiplexer (MUX)

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

A. Mastered
B. Not Mastered

Answer: A

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



NEW QUESTION 90
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. Computer1 connects to a home network and a corporate network.
The corporate network uses the 172.16.0.0/24 address space internally. Computer1 runs an application named App1 that listens to port 8080.
You need to prevent connections to App1 when Computer1 is connected to the home network. Solution: From Windows Firewall with Advanced Security, you create an inbound rule. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 93
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 run the New-NetFirewallRule –DisplayName “Rule1” –Direction Inbound –LocalPort 8080 –Protocol TCP –Action allow –Profile Domain Command.

Does this meet the goal?

A. Yes
B. No

Answer: B

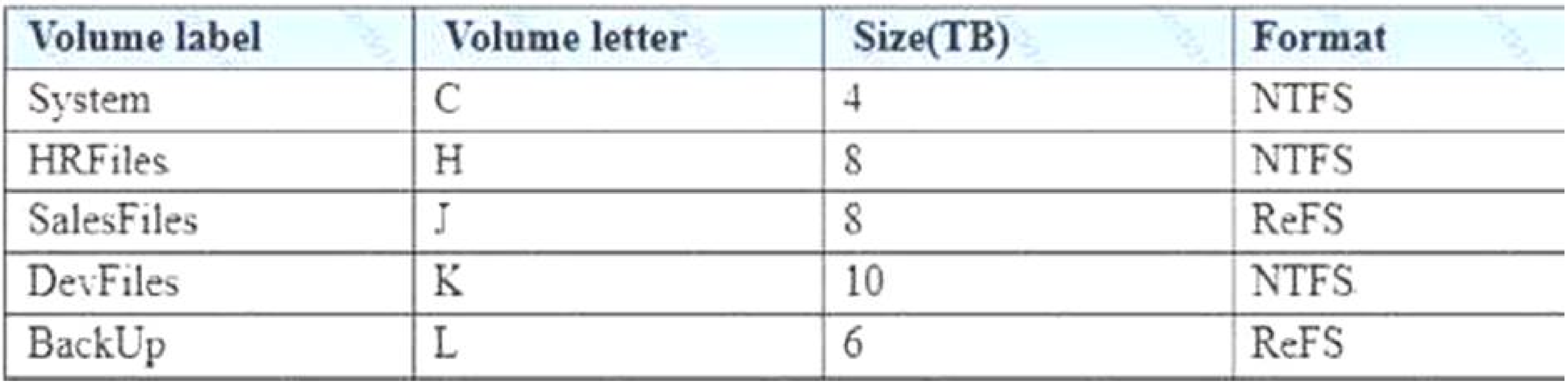
NEW QUESTION 95
Your network has an internal network and a perimeter network. Only the servers on the perimeter network can access the Internet. You create a Microsoft Operations Management Suite (OMS) instance in Microsoft Azure.
You deploy Microsoft Monitoring Agent to all the servers on both the networks. You discover that only the servers on the perimeter network report to OMS. You need to ensure that all the servers report to OMS.
What should you do?

A. Install a Web Application Proxy on the perimeter network and install an OMS Gateway on the internal networ
B. Publish the OMS Gateway from the Web Application Proxy.
C. Install a Web Application Proxy and an OMS Gateway on the perimeter networ
D. Publish the OMS Gateway from the Web Application Proxy.
E. Configure the network firewalls to allow the internal servers to access the IP addresses of the Azure OMS instance by using TCP port 443.
F. On the internal servers, run the Add-AzureRmUsageConnect cmdlet and specify the –AdminUri parameter.

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-oms-gateway

NEW QUESTION 96
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You manage a file server that runs Windows Server 2016. The file server contains the volumes configured as shown in the following table.



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

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

A. Yes
B. No

Answer: B

Explanation:

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

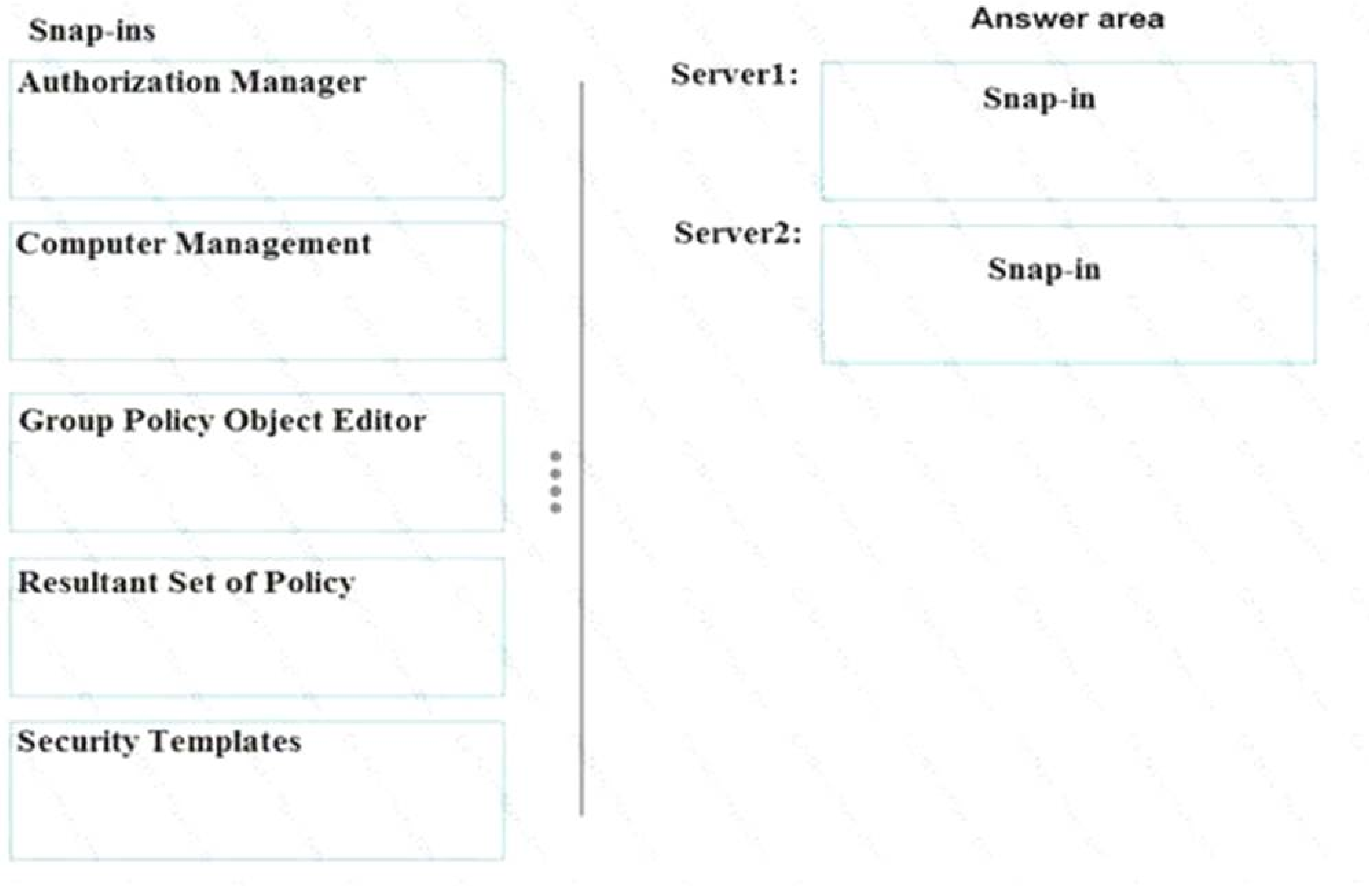
NEW QUESTION 97
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows10.
The network uses the 172.16.0.0/16 address space.
Computer1 has an application named App1.exe that is located in D:\Apps\. App1.exe is configured to accept connections on TCP port 8080.
You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.
Solution: You run the New-NetFirewallRule –DisplayName "Rule1" –Direction Inbound
–Program "D:\Apps\App1.exe" –Action Allow -Profile Domain command. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 99
DRAG DROP
You have two servers named Server1 and Server2 that run Windows Server 2016. The servers are in a workgroup.

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



Snap-ins

Authorization Manager

Computer Management

Group Policy Object Editor

Resultant Set of Policy

Security Templates

Answer area

Server1: Snap-in

Server2: Snap-in

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 100
......