Microsoft

Exam Questions 70-744

Securing Windows Server 2016

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 2,000 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 2
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 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. 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 4
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this 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

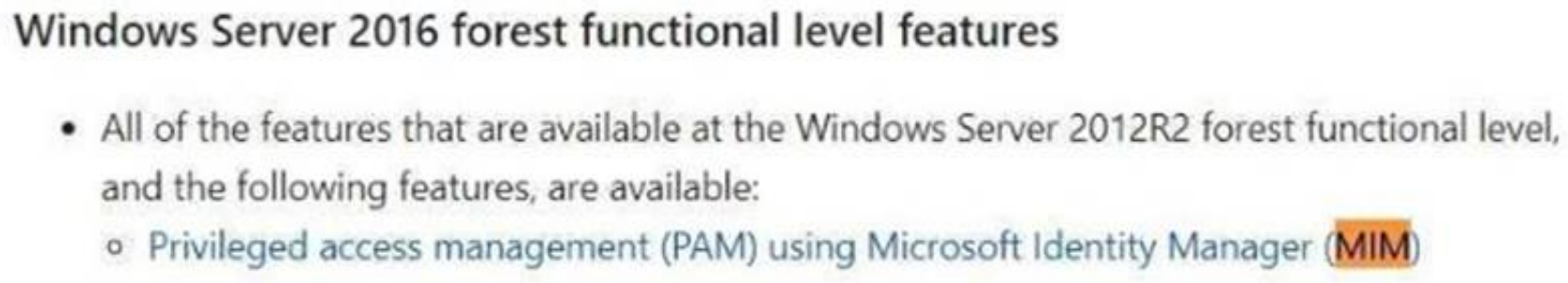
Answer: A

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 5
Your network contains an Active Directory forest named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2016.
You create a new bastion forest named admin.contoso.com. The forest functional level of admin.contoso.com is Windows Server 2012 R2.
You need to implement a Privileged Access Management (PAM) solution.
Which two actions should you perform? Each correct answer presents part of the solution.
A. Raise the forest functional level of admm.contoso.com.
B. Deploy Microsoft Identify Management (MIM) 2016 to admin.contoso.com.
C. Configure contoso.com to trust admin.contoso.com.
D. Deploy Microsoft Identity Management (MIM) 2016 to contoso.com.
E. Raise the forest functional level of contoso.com.
F. Configure admin.contoso.com to trust contoso.co

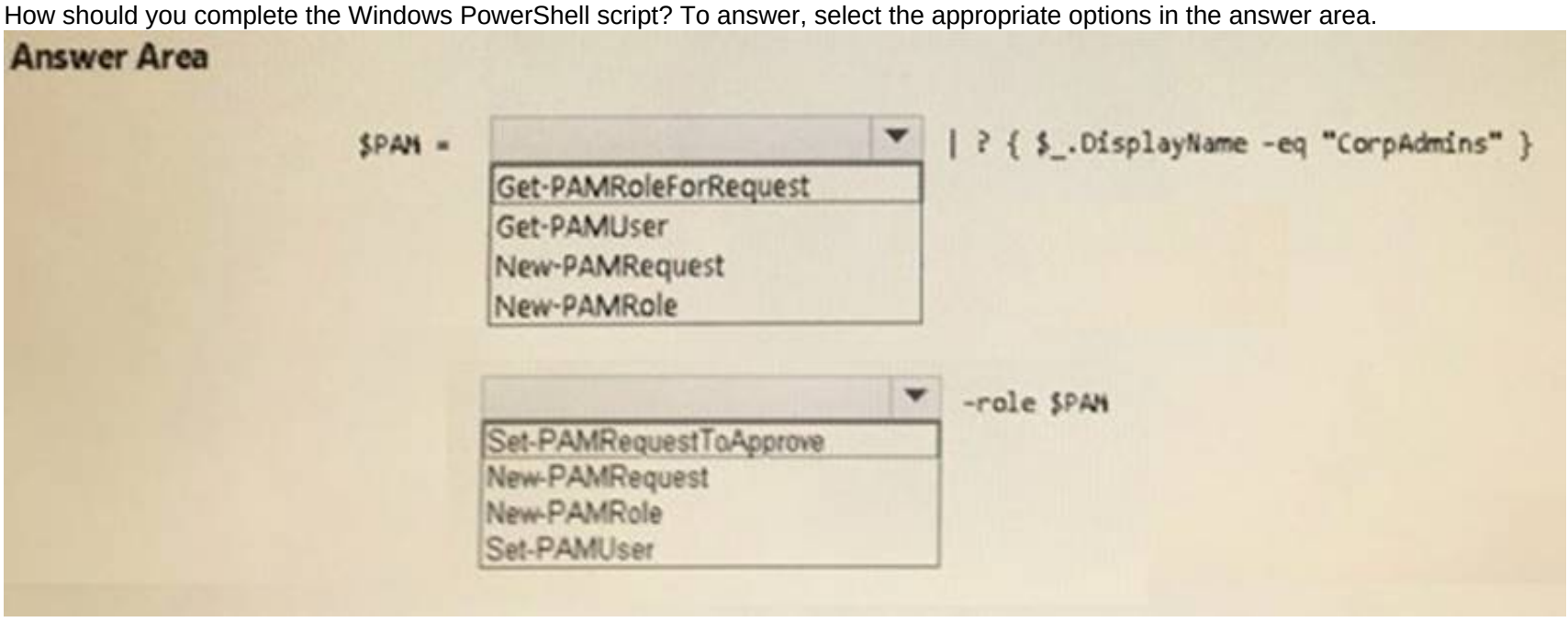
Answer: DE

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



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

NEW QUESTION 6
HOTSPOT
Your network contains an Active Directory forest named contoso.com. The forest has Microsoft Identity Manager (MIM) 2016 deployed. You implement Privileged Access Management (PAM).
You need to request privileged access from a client computer in contoso.com by using PAM.
How should you complete the Windows PowerShell script? To answer, select the appropriate options in the answer area.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

$PAM = Get-PAMRoleForRequest | ? {$_,DisplayName -eq “CorpAdmins” } New-PAMRequest -role $PAM
References:
https://technet.microsoft.com/en-us/library/mt604089.aspx https://technet.microsoft.com/en-us/library/mt604084.aspx

NEW QUESTION 7
Your network contains an Active Directory domain named contoso.com. The domain contains five servers. All servers run Windows Server 2016.
A new secunty policy states that you must modify the infrastructure to meet the following requirements:
*Limit the nghts of administrators.
*Minimize the attack surface of the forest
*Support Multi-Factor authentication for administrators.
You need to recommend a solution that meets the new secunty policy requirements. What should you recommend deploying?

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

Answer: A

Explanation:
You have to “-Minimize the attack surface of the forest”, then you must create another forest for administrators.
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securingprivilegedaccess- reference-material#ESAE_BM
This section contains an approach for an administrative forest based on the Enhanced Security Administrative
Environment (ESAE) reference architecture deployed
by Microsoft’s cybersecurity professional services teams to protect customers against cybersecurity attacks.
Dedicated administrative forests allow organizations to host administrative accounts, workstations, and groups in an environment that has stronger security controls than the production environment.

NEW QUESTION 8
Your network contains two single-domain Active Directory forests named contoso.com and contosoadmin.com. Contosoadmin.com contains all of the user accounts used to manage the servers in contoso.com.
You need to recommend a workstation solution that provides the highest level of protection from vulnerabilities and attacks.
What should you include in the recommendation?

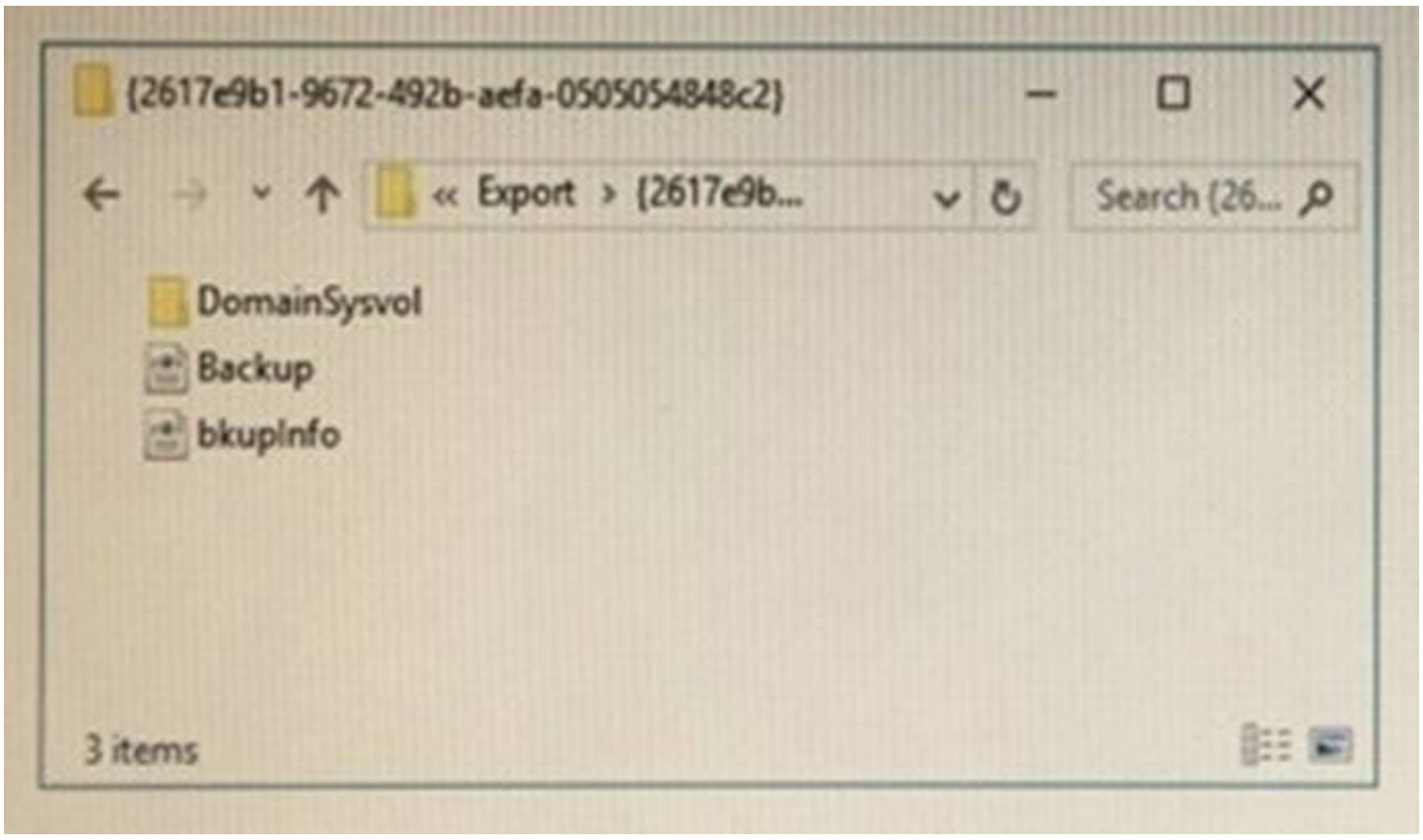
A. Provide a Privileged Access Workstation (PAW) for each user account in both forest
B. Join each PAW to the contoso.com domain.
C. Provide a Pnvileged Access Workstation (PAW) for each user in the contoso.com forest Join each PAW to the contoso.com domain.
D. Provide a Pnvileged Access Workstation (PAW) for each administrato
E. Join each PAW to the contoso.com domain.
F. Provide a Pnvileged Access Workstation (PAW) for each administrato
G. Join each PAW to the contosoadmin.com domain.

Answer: D

Explanation:
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securingprivilegedaccess- reference-material

- **Workstation Hardening** - Build the administrative workstations using the Privileged Access Workstations (through Phase 3), but change the domain membership to the administrative forest instead of the production environment.

NEW QUESTION 9
Vout network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2016.
The domain contains a server named Serverl that has Microsoft Security Compliance Manager (SCM)
4.0 installed.
You export the baseline shown in the following exhibit.



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

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

Answer: D

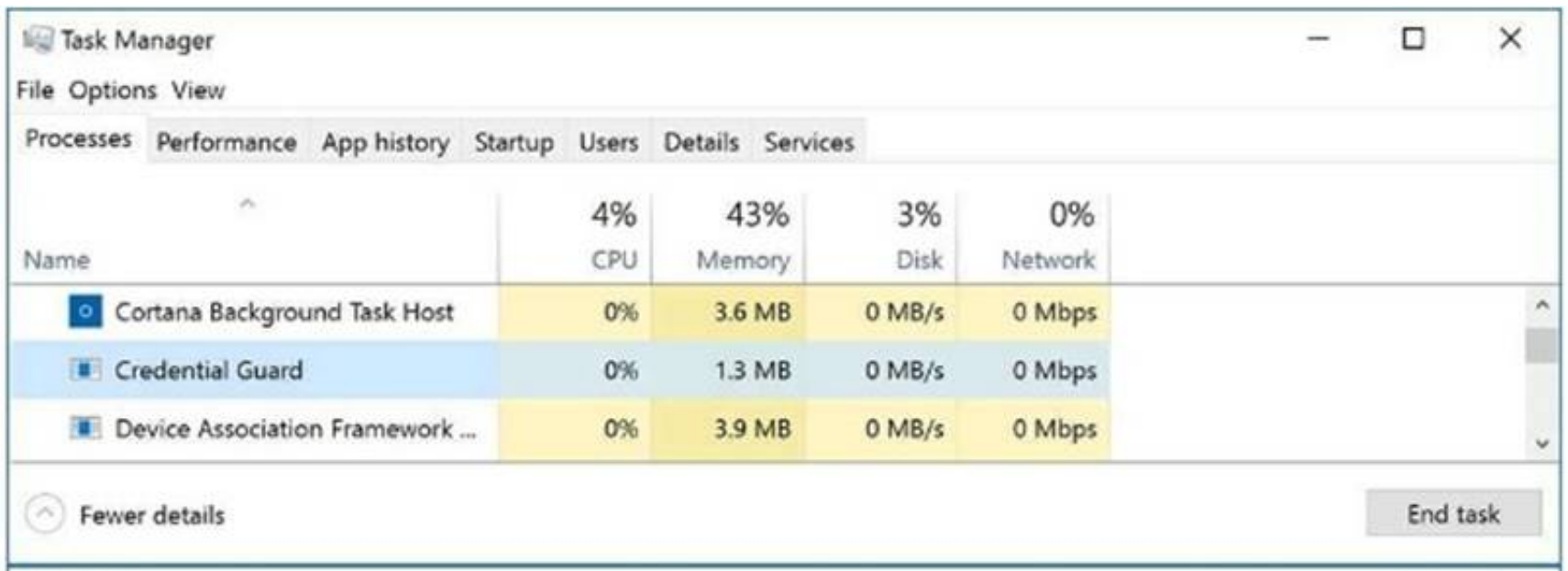
Explanation:
References:
https://anytecho.wordpress.com/2015/05/22/importing-group-policies-using-powershell-almost/

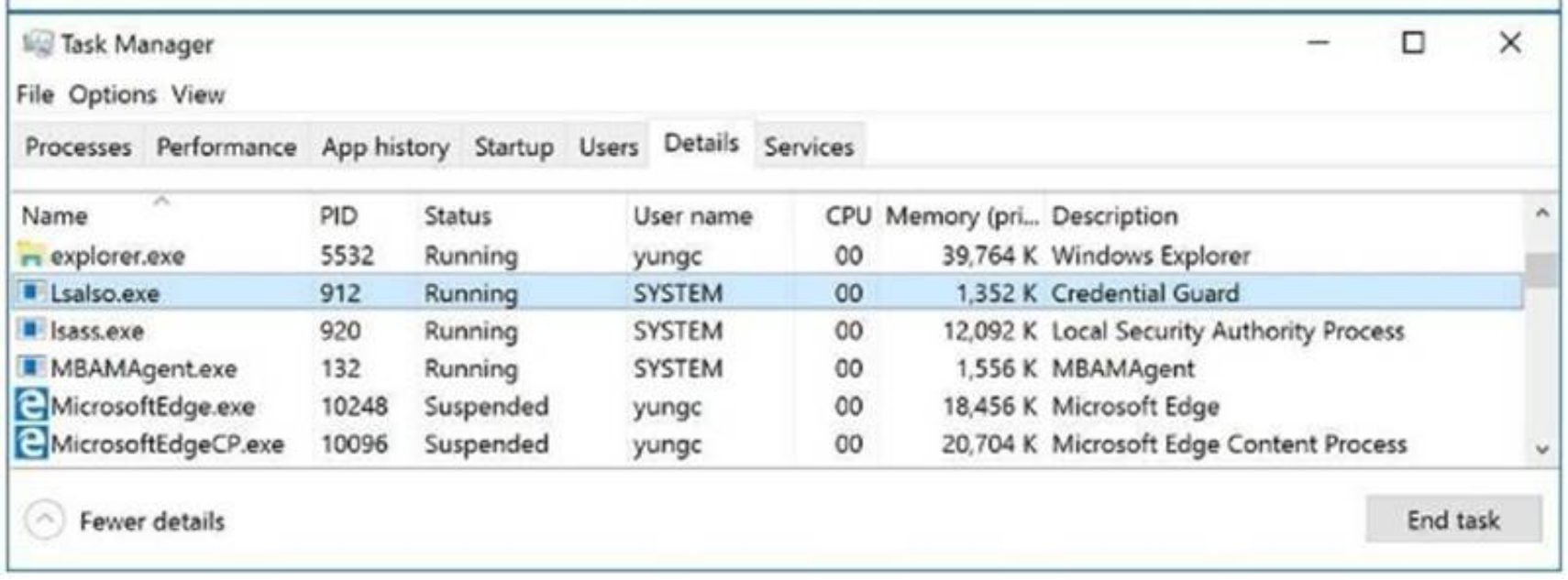
NEW QUESTION 10
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Serve1, that runs Windows Server 2016.
A technician is testing the deployment of Credential Guard on Server1. You need to verify whether Credential Guard is enabled on Server1. What should you do?

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

Answer: B

Explanation:
https://yungchou.wordpress.com/2016/10/10/credential-guard-made-easy-in-windows-10-version- 1607/
The same as before, once Credential Guard is properly configured, up and running.
You should find in Task Manager the ‘Credential Guard’ process and ‘lsaiso.exe’ listed in the Details page as below.



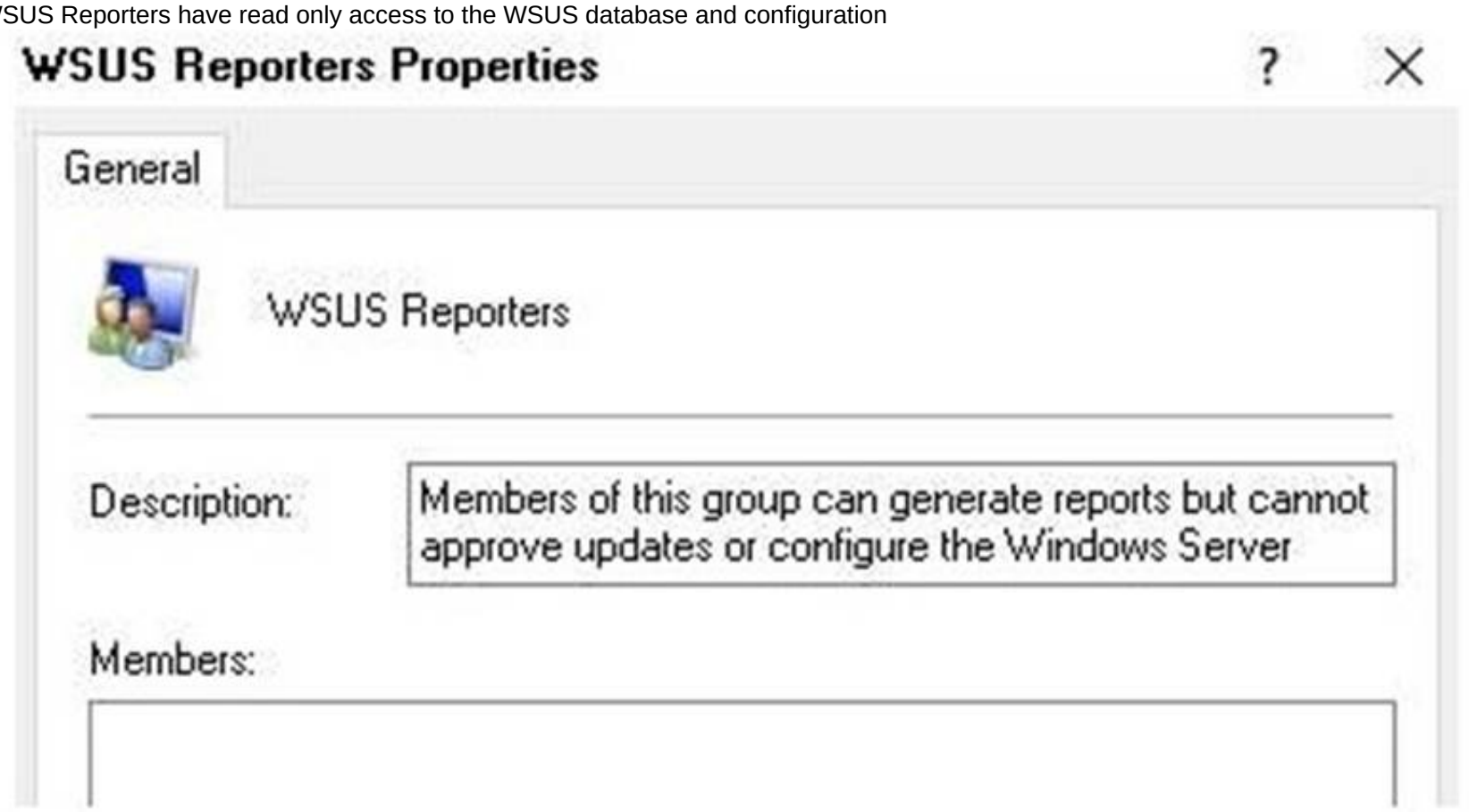


NEW QUESTION 10
Your network contains an Active Directory domain named contoso.com.
You install the Windows Server Update Services server role on a member server named Server1. Server1 runs Windows Server 2016.
You need to ensure that a user named Used can perform the following tasks:
*View the Windows Server Update Services (WSUS) configuration.
*Generate WSUS update reports.
The solution must use the principle of least privilege. What should you do on Server1?

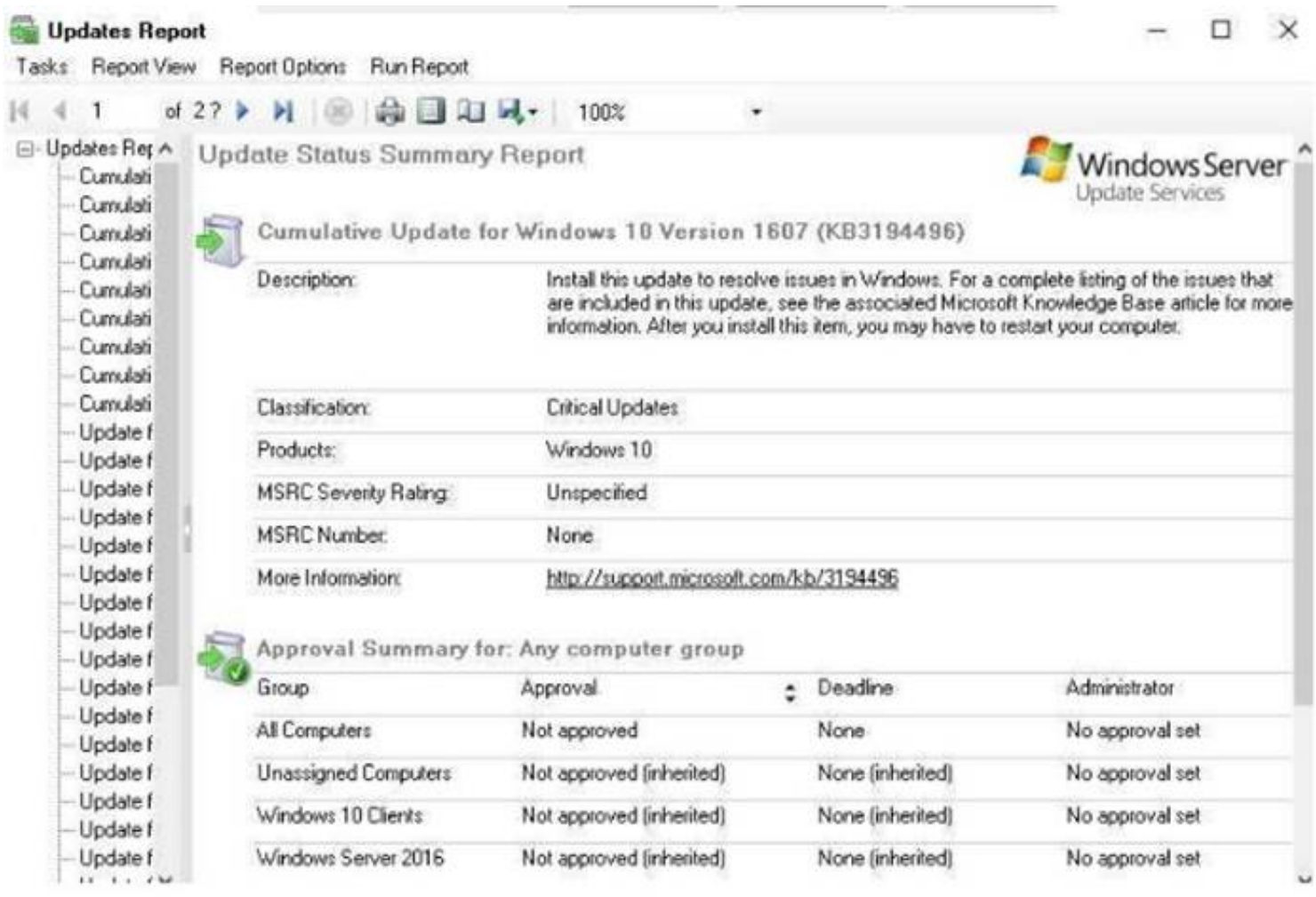
A. Modify the permissions of the ReportWebService virtual folder from the WSUS Administration website.
B. Add User1 to the WSUS Reporters local group.
C. Add User1 to the WSUS Administrators local group.
D. Run wsusutil.exe and specify the postinstall paramete

Answer: B

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



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



NEW QUESTION 12
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 17
Note: This question Is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.
Server1 has a volume named Volume1.
A central access policy named Policy1 is deployed to the domain. You need to apply Policy1 to Volume1.
Which tool should you use?

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

Answer: A

Explanation:

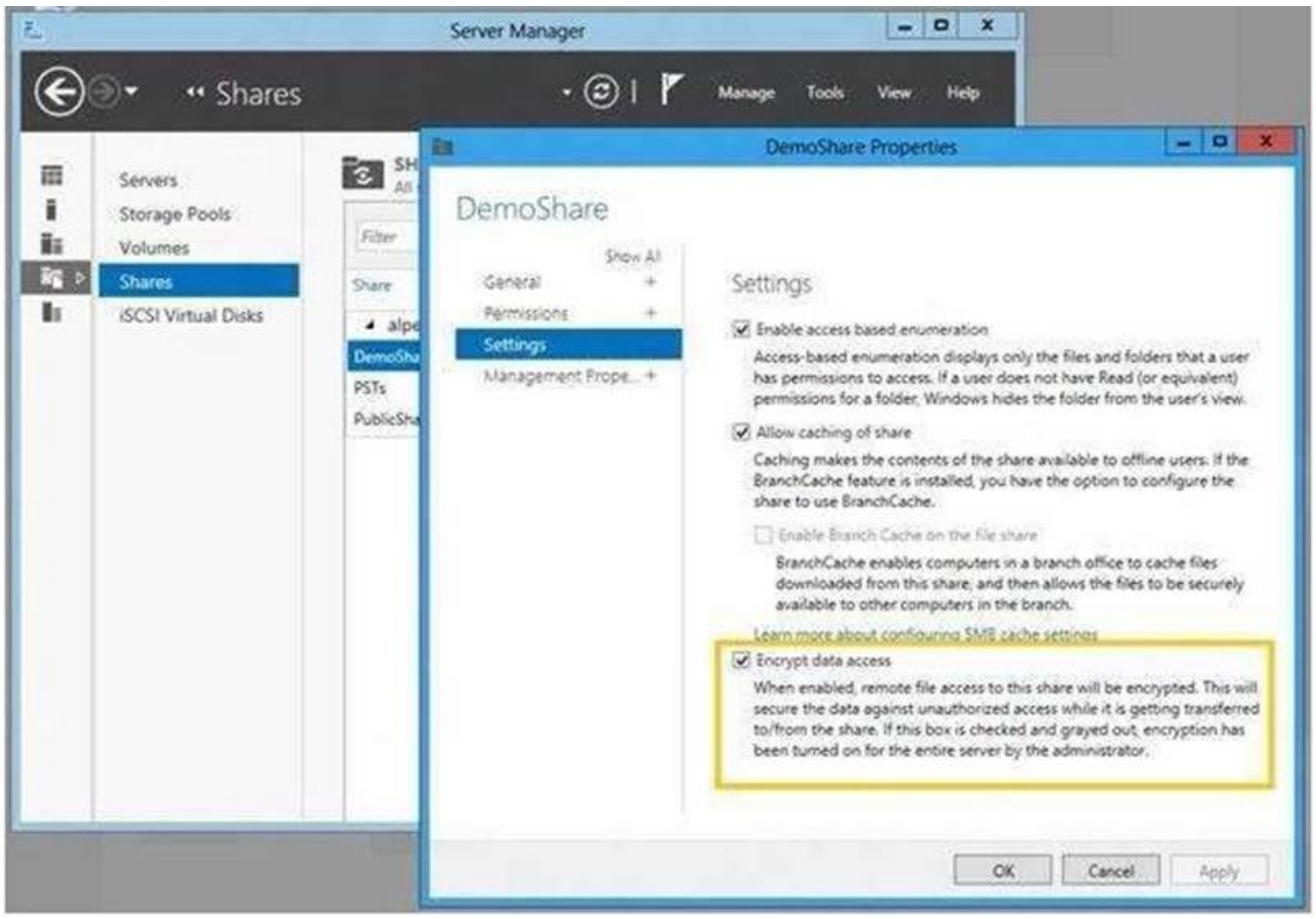
“File Explorer” = “Windows Explorer”.
https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/deploy-a-centralaccess- policy–demonstration-steps-#BKMK_1.4

NEW QUESTION 19
Note: This question b part of a series of questions that use the same or simitar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.
Your network contains an Active Directory domain named contoso.com The domain contains a server named Server1 that runs Windows Server 2016.
Server1 has a shared folder named Share1.
You need to ensure that all access to Share1 uses SMB Encryption. Which tool should you use?

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

Answer: C

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



NEW QUESTION 20
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question Is independent of the other questions in this series. Information and details provided in a question apply only to that question.
Your network contains an Active Directory domain named contoso.com The domain contains a 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)

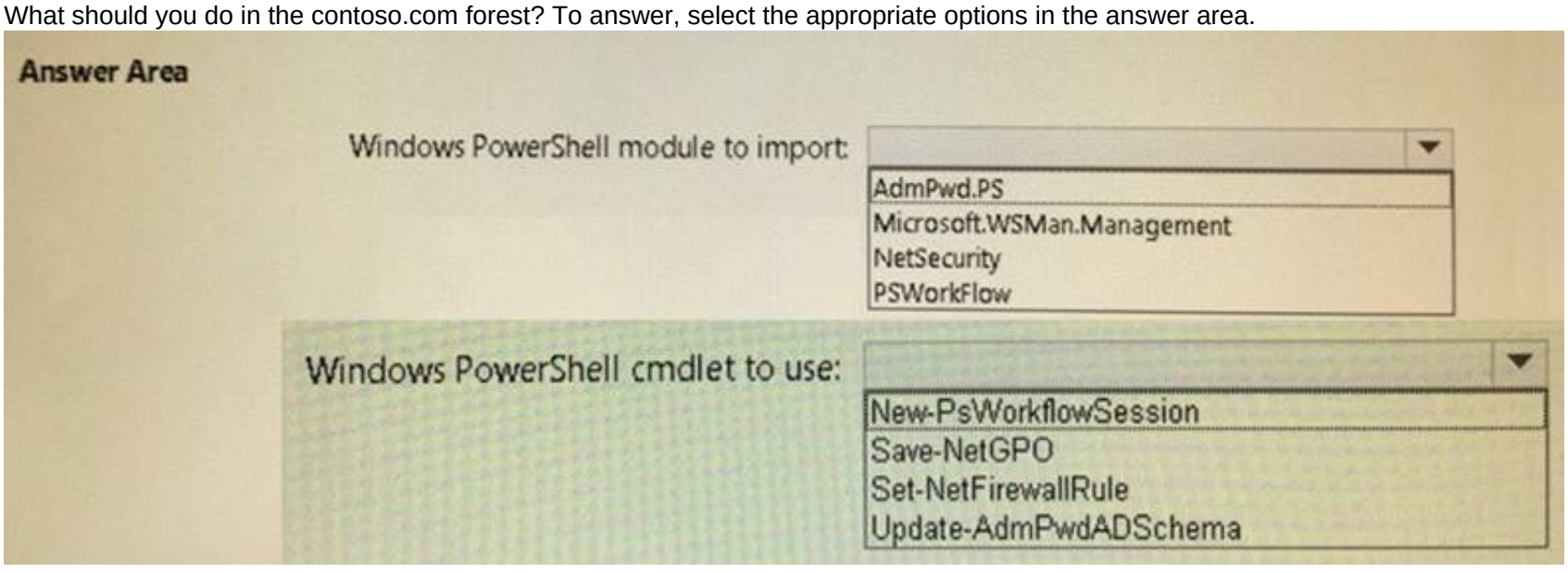
Answer: C

NEW QUESTION 24
HOTSPOT
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.
Start of repeated scenario
Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.
The domain contains the servers configured as shown in the following table.

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

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

You need to ensure that you can implement the Local Administrator Password Solution (LAPS) (or the finance department computers.
What should you do in the contoso.com forest? To answer, select the appropriate options in the answer area.



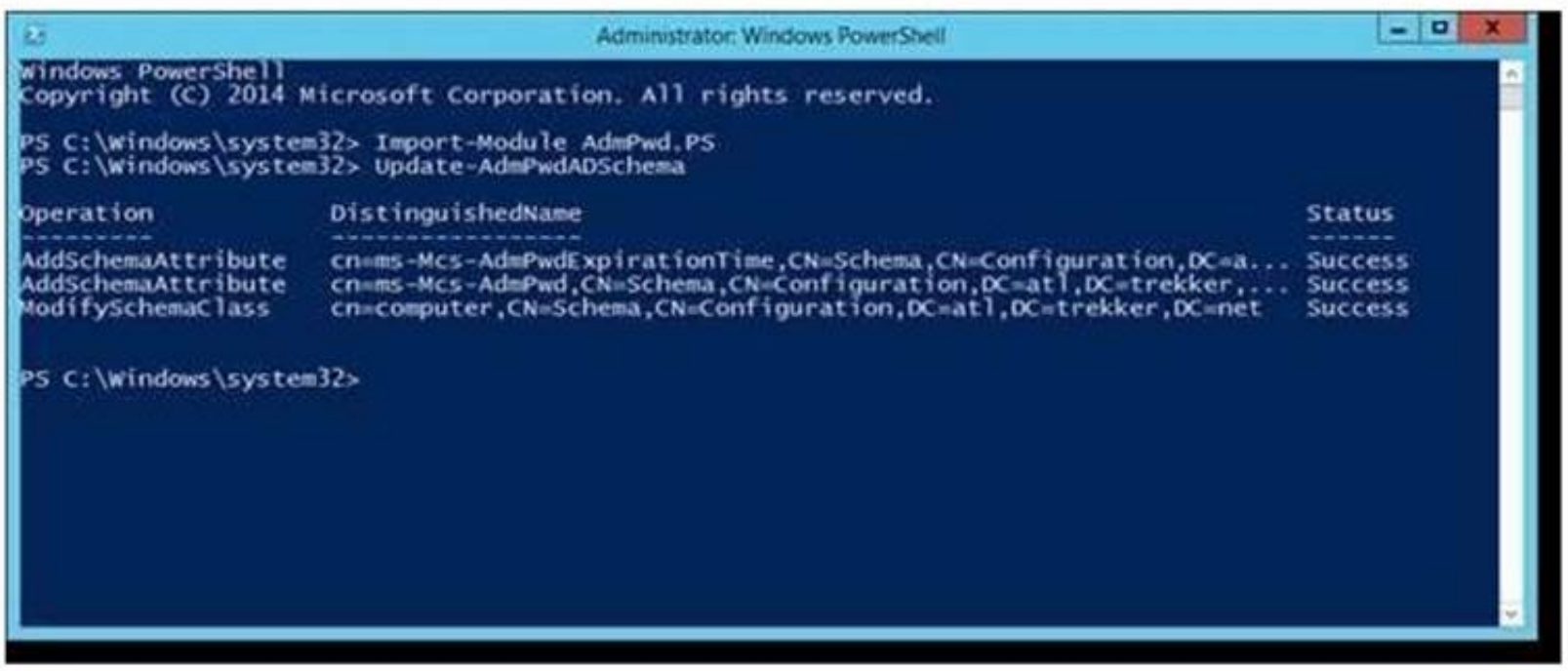
A. Mastered
B. Not Mastered

Answer: A

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

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

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



NEW QUESTION 28
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

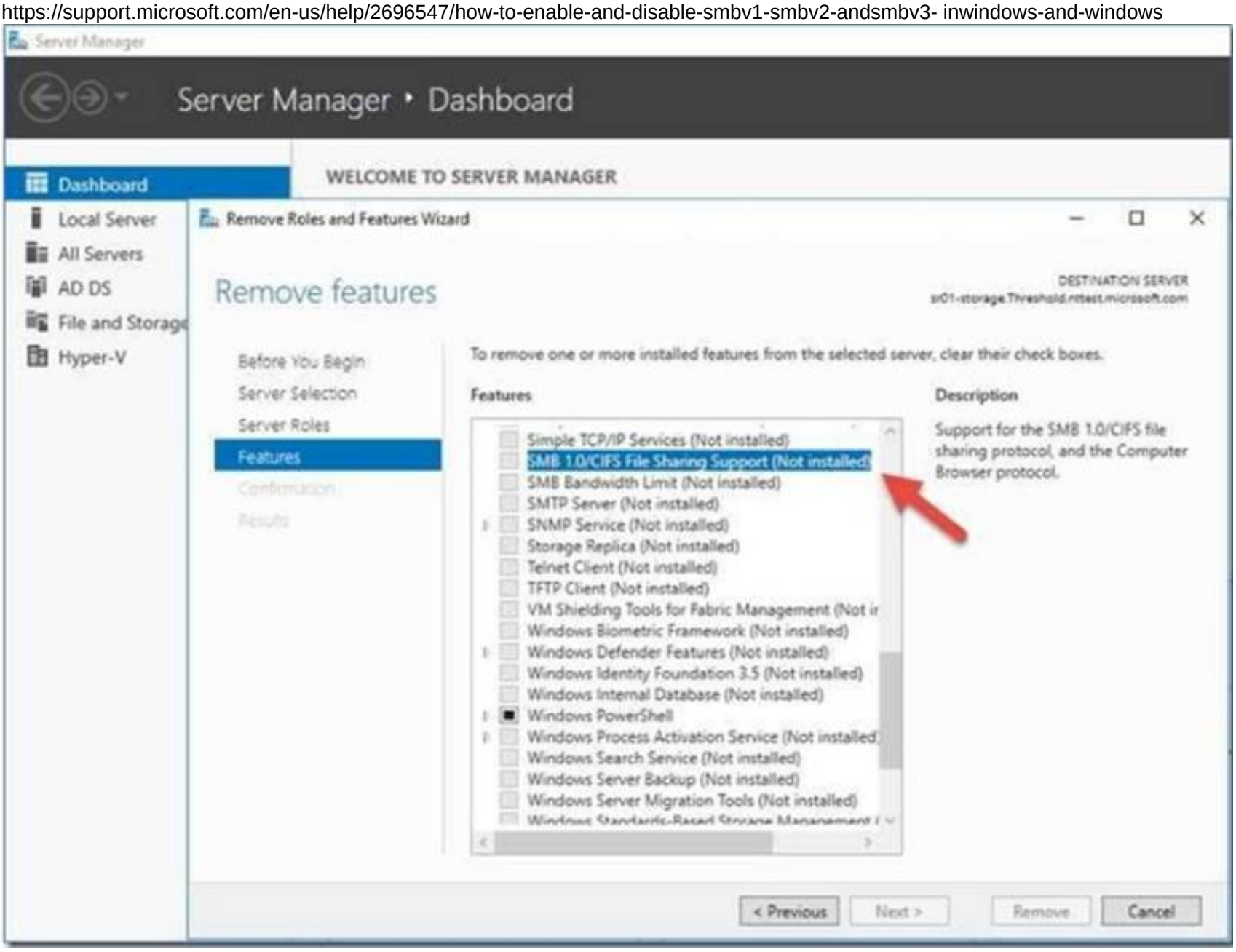
All servers run Windows Server 2016. All client computers run Windows 10.
You have an organizational unit (OU) named Marketing that contains the computers in the marketing department You have an OU named Finance that contains the computers in the finance department You have an OU named AppServers that 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

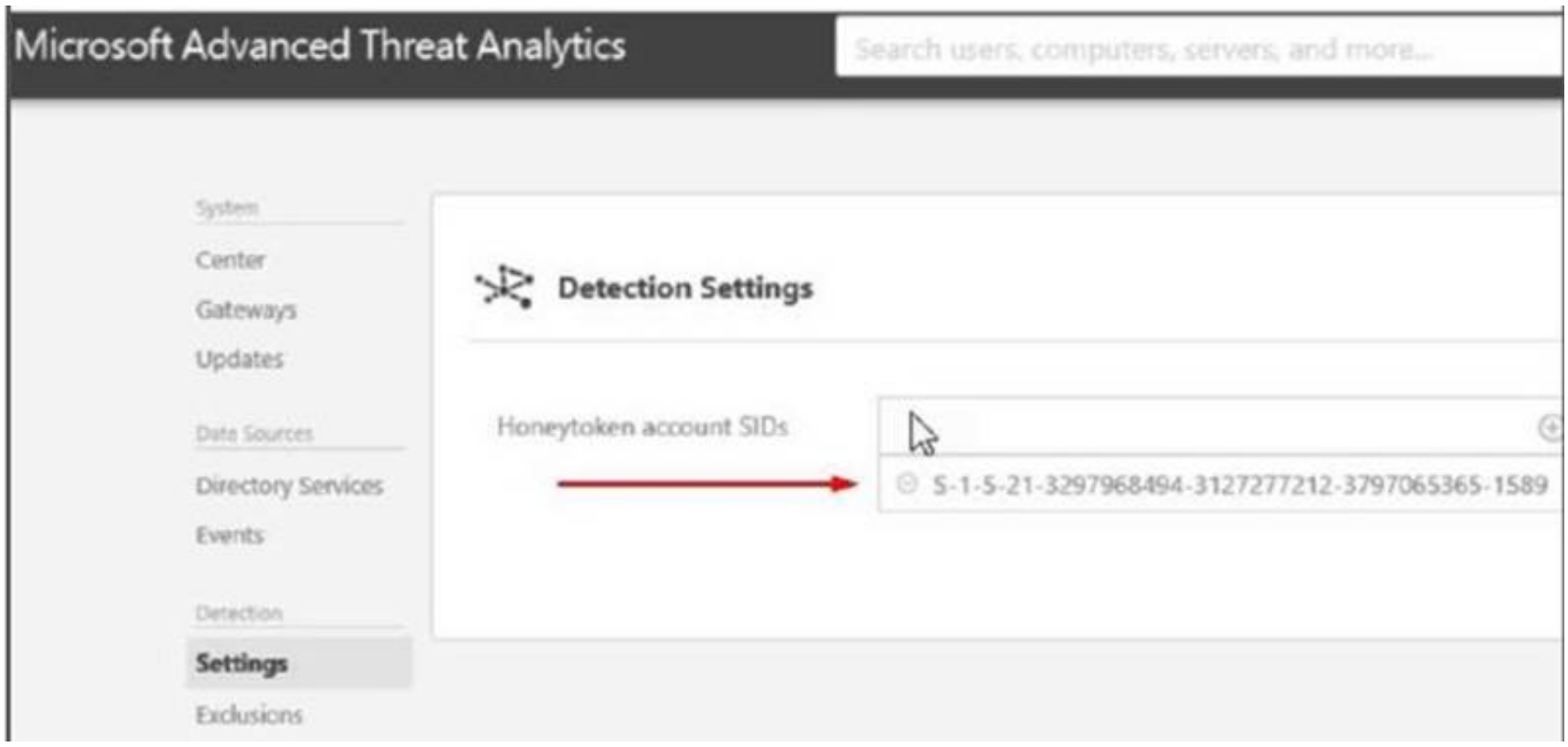


NEW QUESTION 32
Your network contains an Active Directory domain named contoso.com. You are deploying Microsoft Advanced Threat Analytics (ATA).
You create a user named User1.
You need to configure the user account of User1 as a Honeytoken account. Which information must you use to configure the Honeytoken account?

A. the SAM account name of User1
B. the Globally Unique Identifier (GUID) of User1
C. the SID of User1
D. the UPN of User1

Answer: C

Explanation:
https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-prerequisites A user account of a user who has no network activities.
This account is configured as the ATA Honeytoken user.
To configure the Honeytoken user you need the SID of the user account, not the username.



https://docs.microsoft.com/en-us/advanced-threat-analytics/install-ata-step7
ATA also enables the configuration of a Honeytoken user, which is used as a trap for malicious actors – any authentication associated with this (normally dormant) account will trigger an alert.

NEW QUESTION 36
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 40
Your network contains an Active Directory domain named contoso.com The domain contains five file servers that run Windows Server 2016.
You have an organizational unit (OU) named Finance that contains all of the servers. You create a Group Policy object (GPO) and link the GPO to the Finance OU.
You need to ensure that when a user in the finance department deletes a file from a file server, the event is logged. The solution must log only users who have a manager attribute of Ben Smith. Which audit policy setting should you configure in the GPO?

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

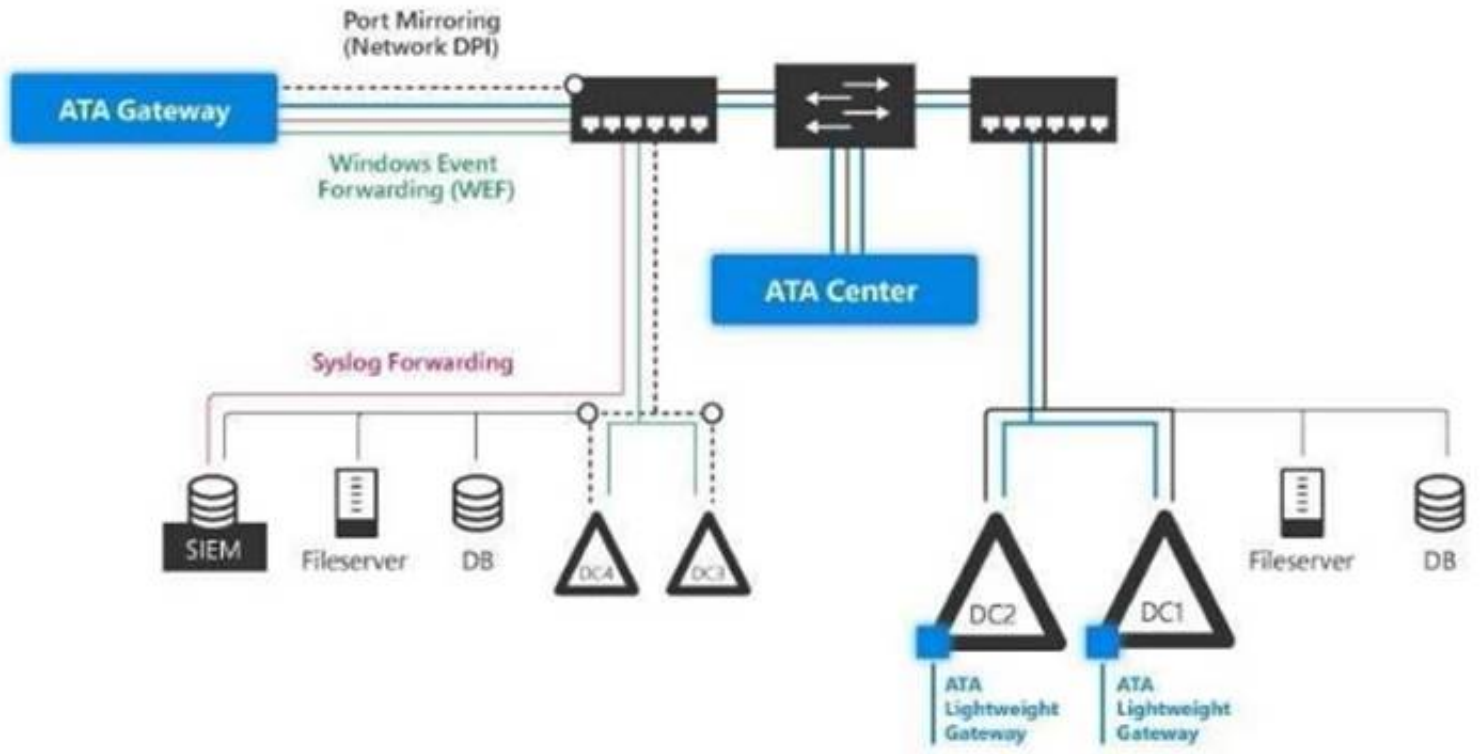
Answer: C

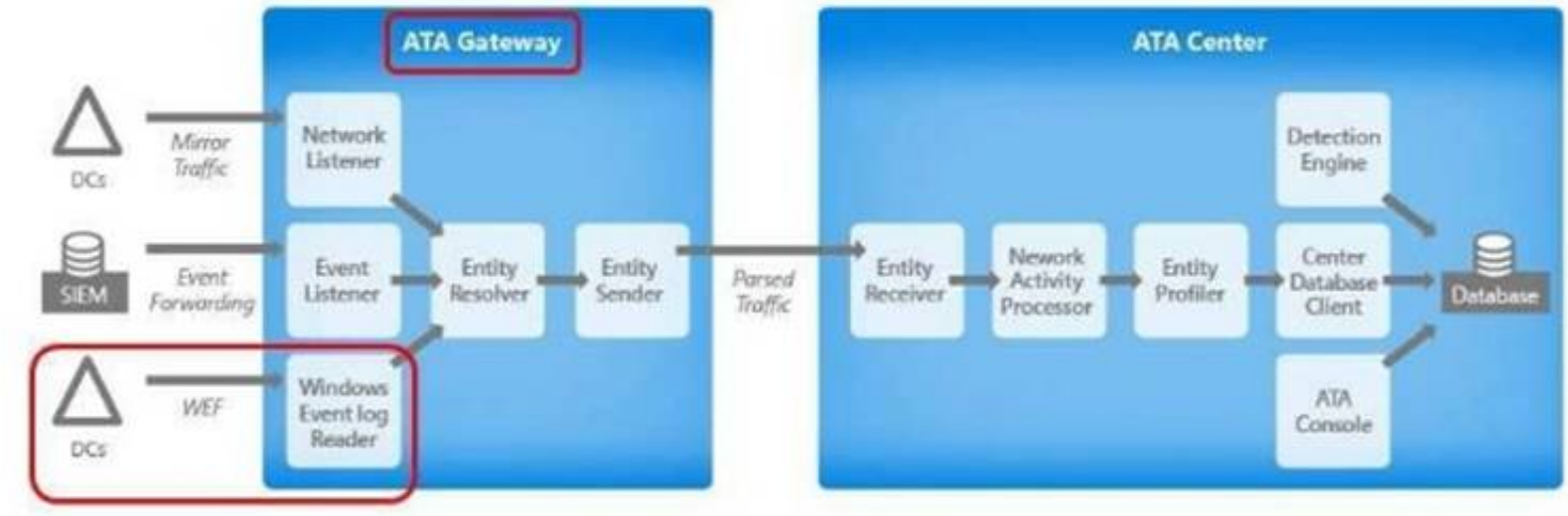
NEW QUESTION 41
Your network contains an Active Directory domain named contoso.com.
You are deploying Microsoft Advanced Threat Analytics (ATA) to the domain.
You install the ATA Center on server named Server1 and the ATA Gateway on a server named Served. You need to ensure that Server2 can collect NTLM authentication events.
What should you configure?

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

Answer: A

Explanation:
https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-architecture
ATA monitors your domain controller network traffic by utilizing port mirroring to an ATA Gateway using physical or virtual switches.
If you deploy the ATA Lightweight Gateway directly on your domain controllers, it removes the requirement for port mirroring.
In addition, ATA can leverage Windows events (forwarded directly from your domain controllers or from a SIEM server) and analyze the data for attacks and threats.
See the GREEN line in the following figure, forward event ID 4776 which indicates NTLM authentication is being used to ATA Gateway Server2.





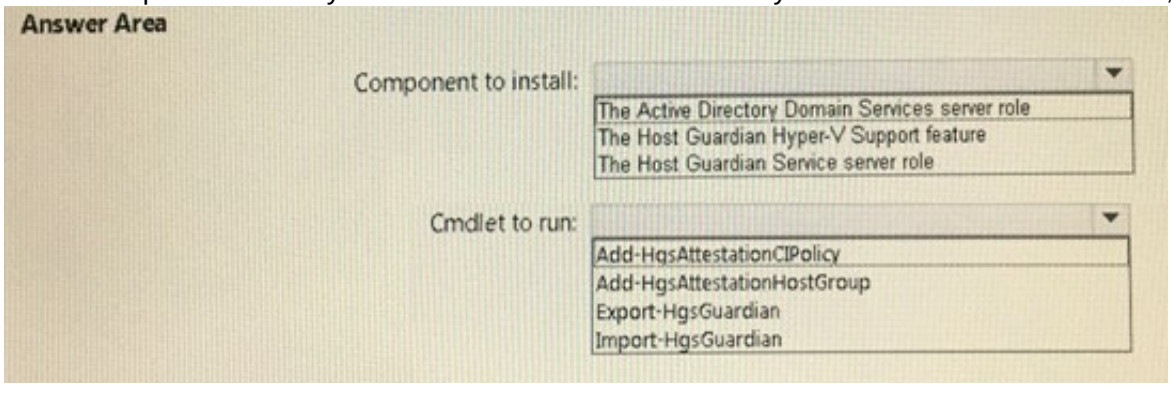
NEW QUESTION 46
Your network contains an Active Directory forest named conloso.com. The network is connected to the Internet.
You have 100 point-of-sale (POS) devices that run Windows 10. The devices cannot access the Internet.
You deploy Microsoft Operations Management Suite (OMS).
You need to use OMS to collect and analyze data from the POS devices. What should you do first?

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

Answer: B

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

NEW QUESTION 50
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 54
A shielding data file (also called a provisioning data file or PDK file) is an encrypted file that a tenant or VM owner creates to protect important VM configuration information.
A fabric administrator uses the shielding data file when creating a shielded VM, but is unable to view or use the information contained in the file.
Which information can be stored in the shielding data file?

A. Administrator credentials
B. All of these
C. A Key Protector
D. Unattend.xml

Answer: B

NEW QUESTION 55
____ 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 56
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 60
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 65
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.

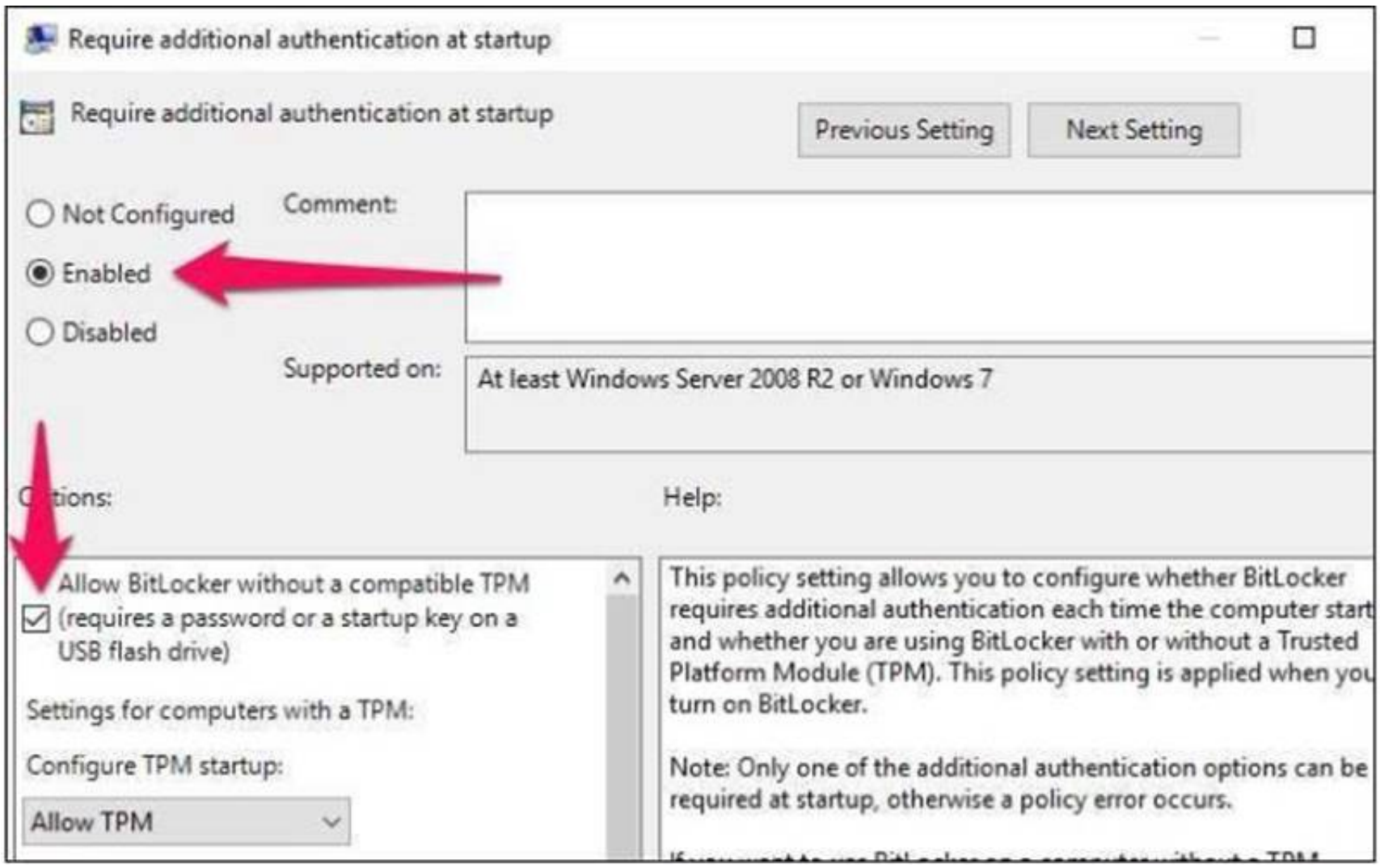
Server name	Domain or workgroup	Configuration
Server1	Domain	Windows Server Update Services (WSUS) server
Server2	Domain	Server that has a Trusted Platform Module (TPM)
Server3	Domain	Member server that will be configured for Just Enough Administration (JEA)
Server4	Domain	Application server
Server5	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 68
Your network contains an Active Directory domain named contoso.com. The domain contains a DNS server named Server1 that runs Windows Server 2016.
A domain-based Group Policy object (GPO) is used to configure the security policy of Server1.
You plan to use Security Compliance Manager (SCM) 4.0 to compare the security policy of Server1 to the WS2012 DNS Server Security 1.0 baseline.
You need to import the security policy into SCM. What should you do first?

A. From Security Configuration and Analysis, use the Export Template option.
B. Run the Copy-GPO cmdlet and specify the -TargetName parameter.
C. Run the Backup-GPO cmdlet and specify the -Path parameter.
D. Run the secedit.exe command and specify the/export paramete

Answer: C

Explanation:
https://technet.microsoft.com/en-us/library/ee461052.aspx
Backup-GPO cmdlet and specify the -Path parameter creates a GPO backup folder with GUID name and is
suitable to import to SCM 4.0

NEW QUESTION 71
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 74
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 75
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 78
You have two computers configured as shown in the following table.

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

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

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

Answer: A

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

Remote Credential Guard requirements

To use Windows Defender Remote Credential Guard, the Remote Desktop client and remote host must meet the following requirements:

The Remote Desktop client device:

- Must be running at least Windows 10, version 1703 to be able to supply credentials.
- Must be running at least Windows 10, version 1607 or Windows Server 2016 to use the user's signed-in credentials. This requires the user's account be able to sign in to both the client device and the remote host.
- Must be running the Remote Desktop Classic Windows application. The Remote Desktop Universal Windows Platform application doesn't support Windows Defender Remote Credential Guard.
- Must use Kerberos authentication to connect to the remote host. If the client cannot connect to a domain controller, then RDP attempts to fall back to NTLM. Windows Defender Remote Credential Guard does not allow NTLM fallback because this would expose credentials to risk.

NEW QUESTION 80
Your data center contains 10 Hyper-V hosts that host 100 virtual machines.
You plan to secure access to the virtual machines by using the Datacenter Firewall service.
You have four servers available for the Datacenter Firewall service. The servers are configured as shown in the following table.

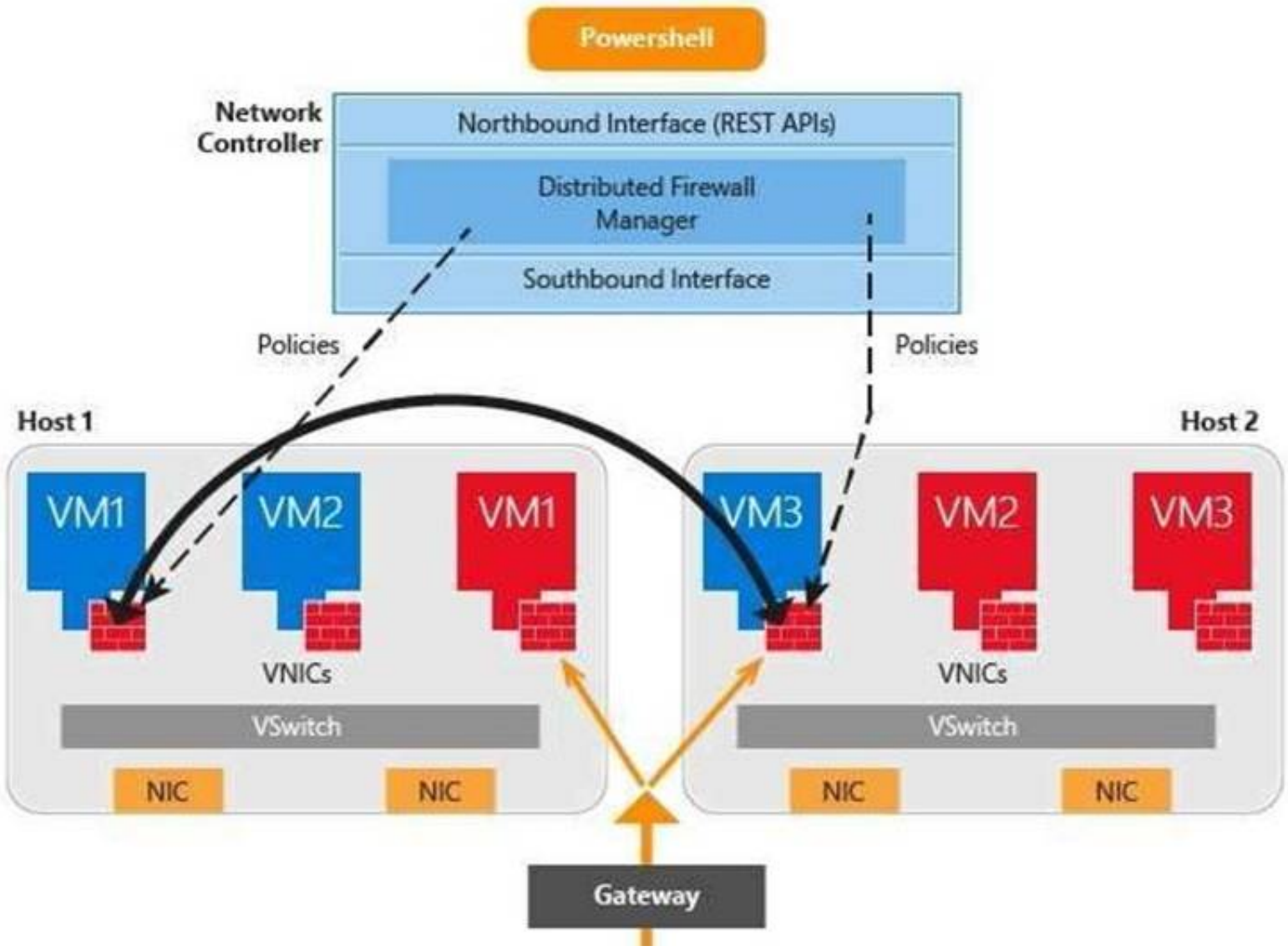
Server name	Platform	Windows Server 2016 edition
Server20	Physical	Standard
Server21	Physical	Standard
Server22	Virtual	Datacenter
Server23	Virtual	Datacenter

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

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

Answer: BE

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



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

NEW QUESTION 84
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”.

Guarded hosts using TPM mode must meet the following prerequisites:

- **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.

NEW QUESTION 88

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

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

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

A. Yes
B. No

Answer: A

Explanation:
https://technet.microsoft.com/en-us/library/cc771990(v=ws.11).aspx Backup Operators
Members of this group can back up and restore files on a computer, regardless of any permissions that protect those files.
This is because the right to perform a backup takes precedence over all file permissions. Members of this group cannot change security settings.

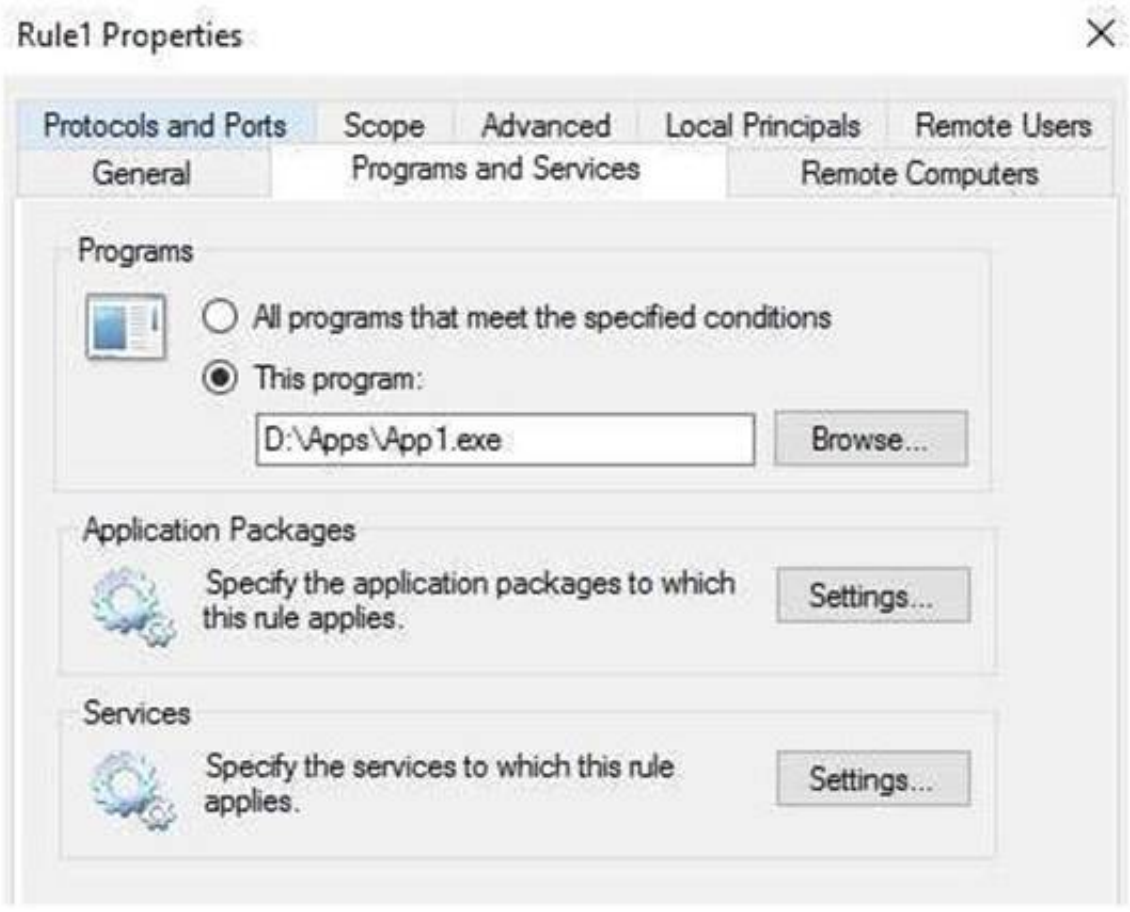
NEW QUESTION 92
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. Computer1 connects to a home network and a corporate network.
The corporate network uses the 172.16.0.0/24 address space internally. Computer1 runs an application named App1 that listens to port 8080.
You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.
Solution: You run the command New-NetFirewallRule -DisplayName “Rule1” -Direction Inbound - Program “D:\\Apps\\App1.exe” –Action Allow -Profile Domain
Does this meet the goal?

A. Yes
B. No

Answer: A

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

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


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



NEW QUESTION 96
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 99
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 103
Your network contains an Active Directory domain named contoso.com.
The domain contains four global groups named Group].., Group2, Group3, and Group4.A user named User1 is a member of Group3.
You have an organizational unit (OU) named OU1 that contains computer accounts.
A Group Policy object (GPO) named GPO1 is linked to OU1. OU1 contains a computer account named Computer1.
GPO1 has the User Rights Assignment configured as shown in the following table:

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

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

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

Answer: B

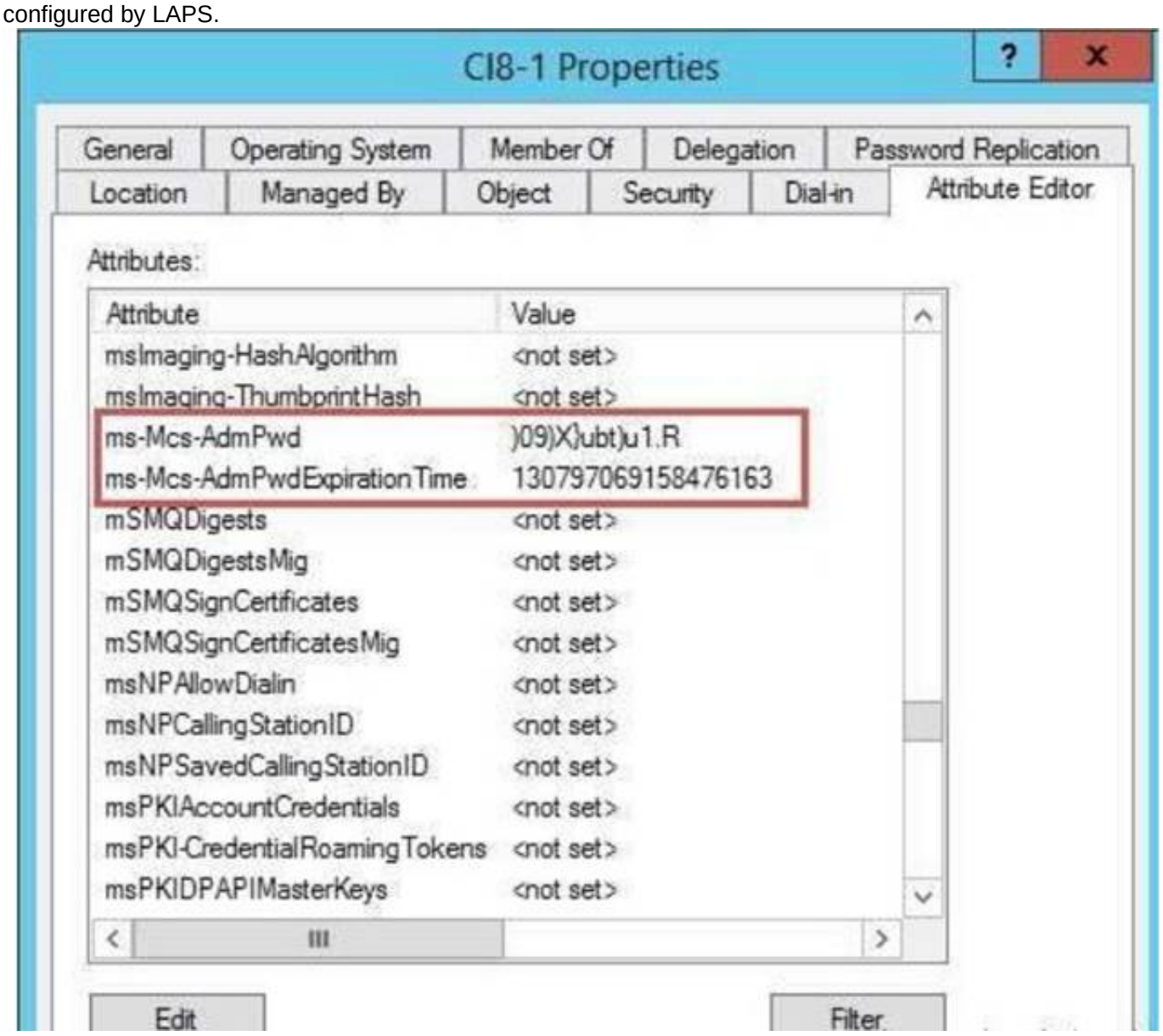
Explanation:
You need to ensure that User1 can access the shares on Computer1, from network.
If not from network, where would you access a shared folder from? from Mars? from Space? from toilet?
Moreover, this question has explicitly state User1 is a member of Group3, and hence it is not possible for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

NEW QUESTION 108
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.



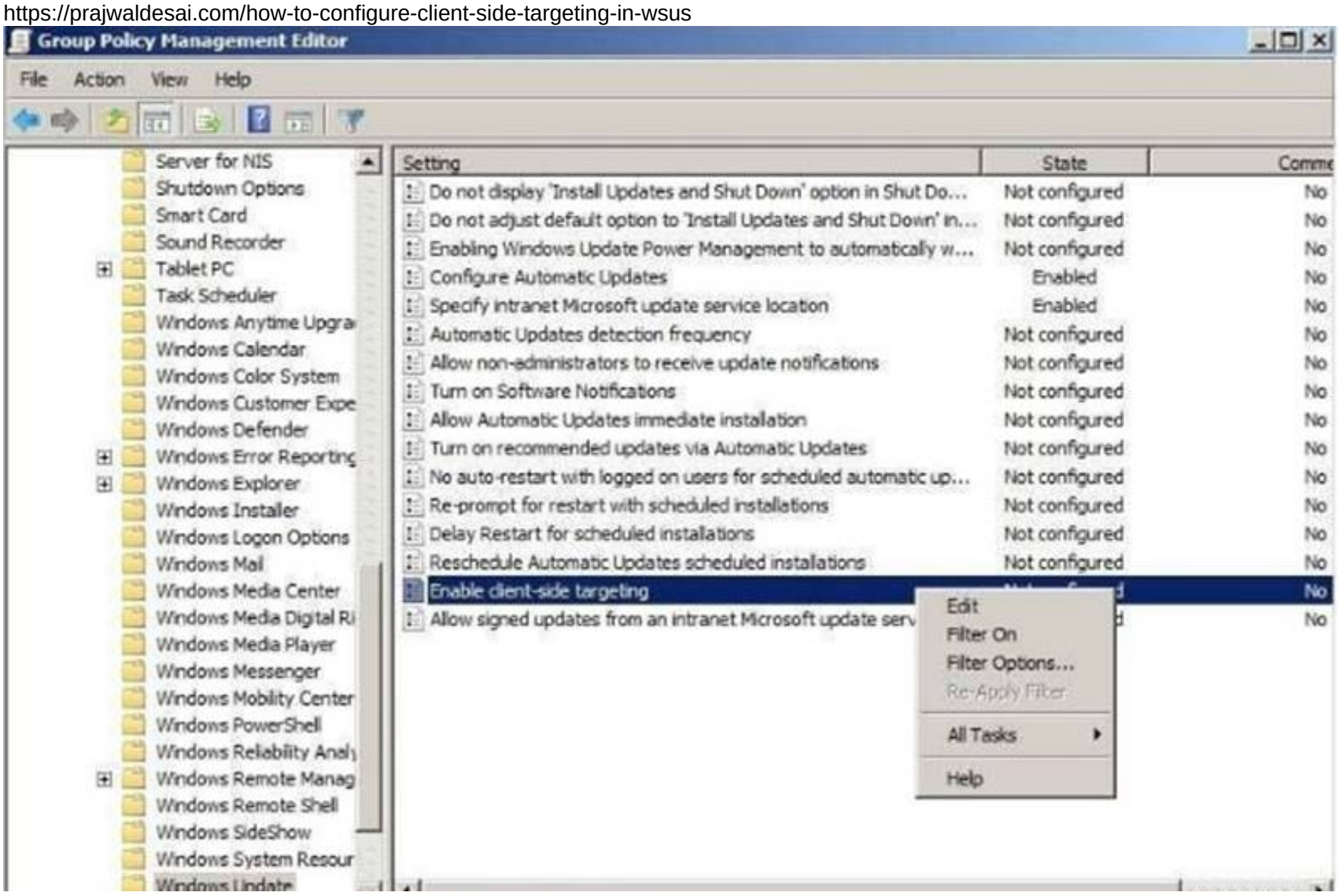
NEW QUESTION 111
Your network contains an Active Directory domain.
The domain contains two organizational units (OUs) named ProdOU and TestOU.
All production servers are in ProdOU. All test servers are in TestOU. A server named Server1 is in TestOU.
You have a Windows Server Update Services (WSUS) server 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?

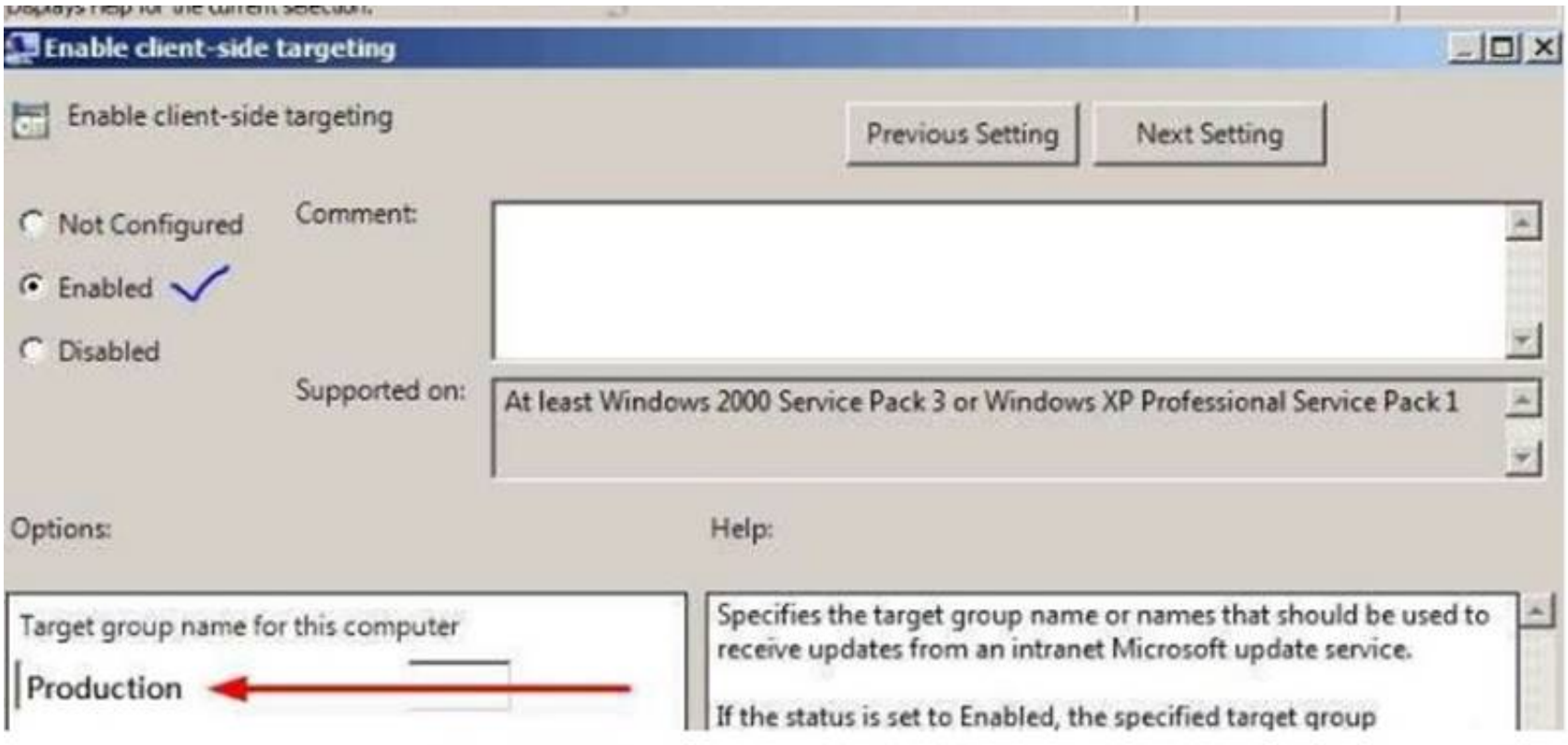
A. Turn off auto-restart for updates during active hours by using Group Policy objects (GPOs).
B. Configure client-side targeting by using Group Policy objects (GPOs).
C. Create computer groups by using the Update Services console.
D. Run wuauclt.exe /detectnow on each server after the server is moved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

Secondly, configure GPO to affect “ProdOU” , so that Server1 add itself to “Production” computer group.
https://prajwaldesai.com/how-to-configure-client-side-targeting-in-wsus





NEW QUESTION 116
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 119
Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2. The domain contains the servers configured as shown in the following table.

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

You have an organizational unit (OU) named Marketing that contains the computers in the marketing department.
You have an OU named Finance that contains the computers in the finance department. You have an OU named AppServers that contains application servers.
A Group Policy object (GPO) named GP1 is linked to the Marketing OU. A GPO named GP2 is linked to the AppServers OU.
You install Windows Defender on Nano1.
You need to configure Nano1 as a Hyper-V Host. Which command should you run?

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

Answer: E

Explanation:
https://docs.microsoft.com/en-us/windows-server/get-started/deploy-nano-server#BKMK_online The Nano Server package “Microsoft-NanoServer-Compute-Package” includes the Hyper-V role for a Nano

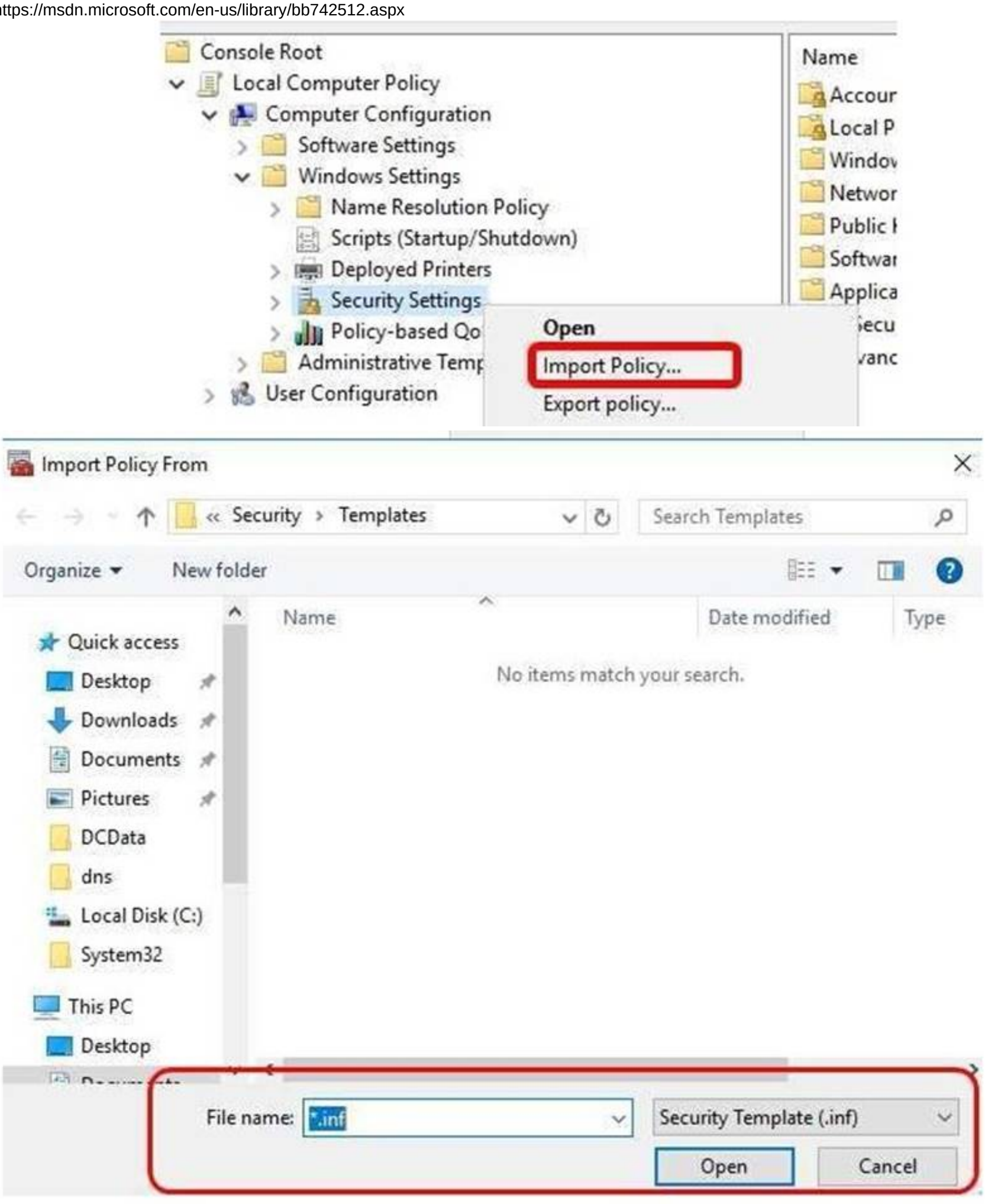
Server host.
Moreover, the Install-WindowsFeature or Add-WindowsFeature cmdlet are NOT available on a Nano Server.

NEW QUESTION 122
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



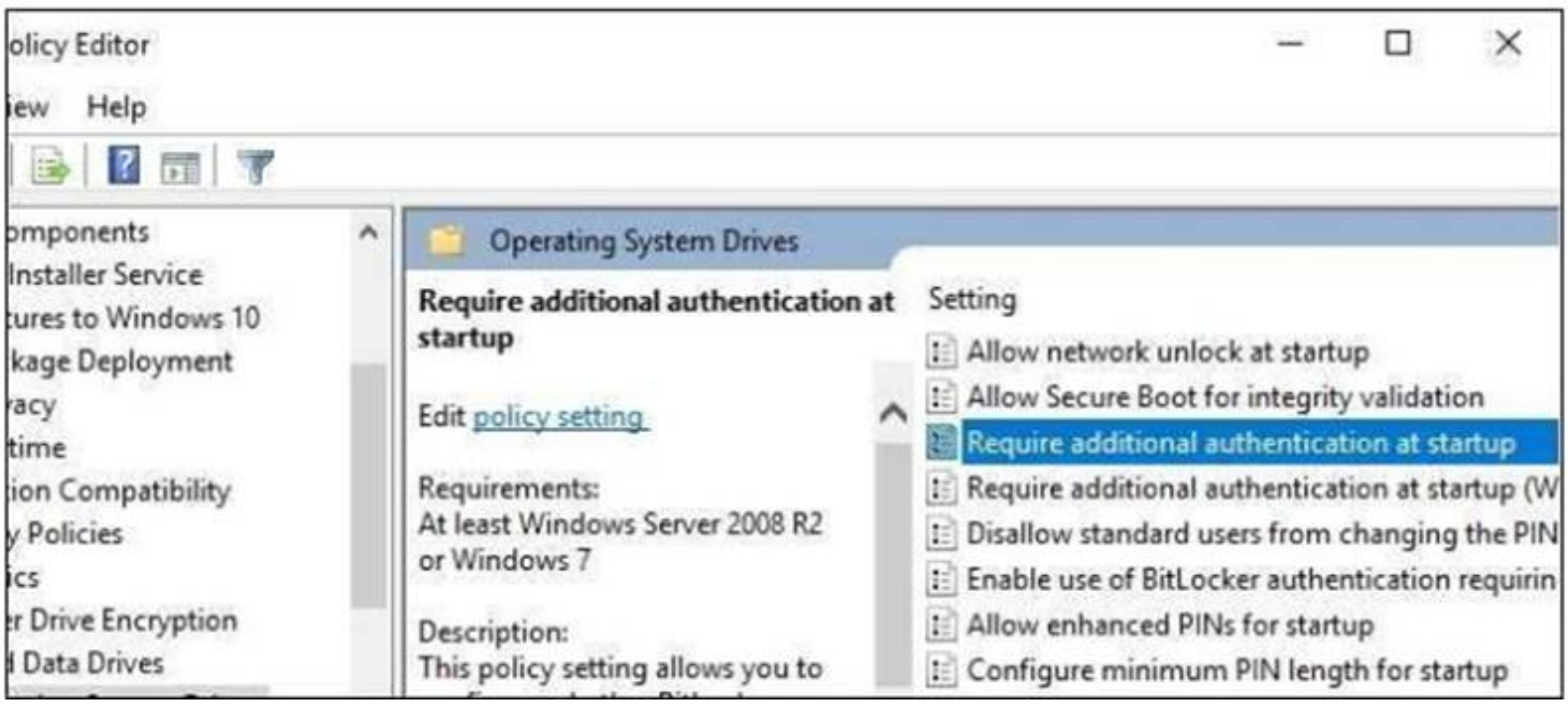
NEW QUESTION 124

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

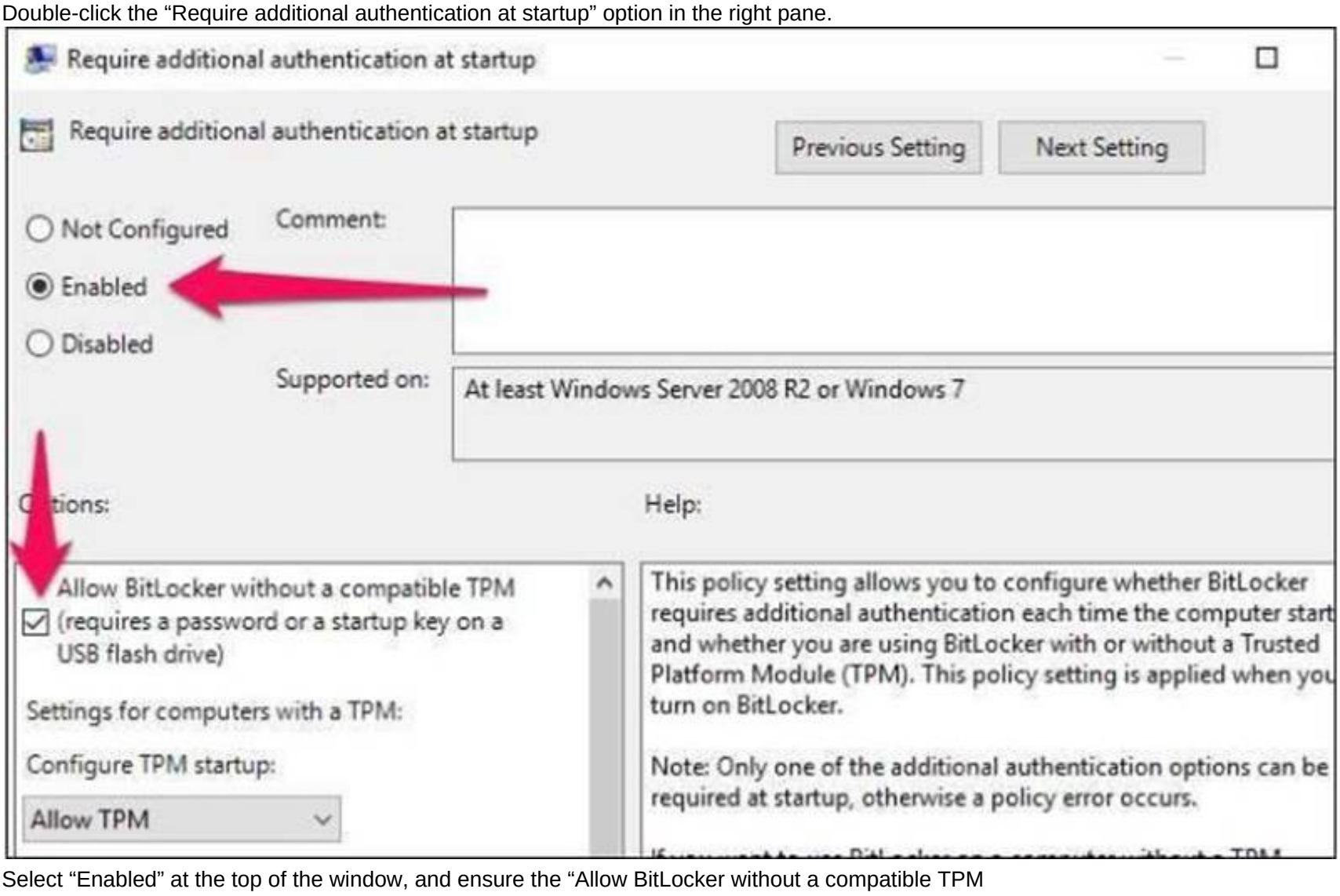
A. From Server1, install the BitLocker feature.
B. From Server1, enable nested virtualization for VM1.
C. From VM1, configure the Require additional authentication at startup Group Policy setting.
D. From VM1, configure the Enforce drive encryption type on fixed data drives Group Policy settin

Answer: C

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



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



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

NEW QUESTION 126
Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1 that runs Windows Server 2016.Server1 has a shared folder named Share1. You plan to create a subfolder in Share1 for each domain user.

You need to limit each user to using 100 MB of data in their respective subfolder.
The solution must enable the users to be notified when they use 80 percent of the available space in the subfolder.
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: H

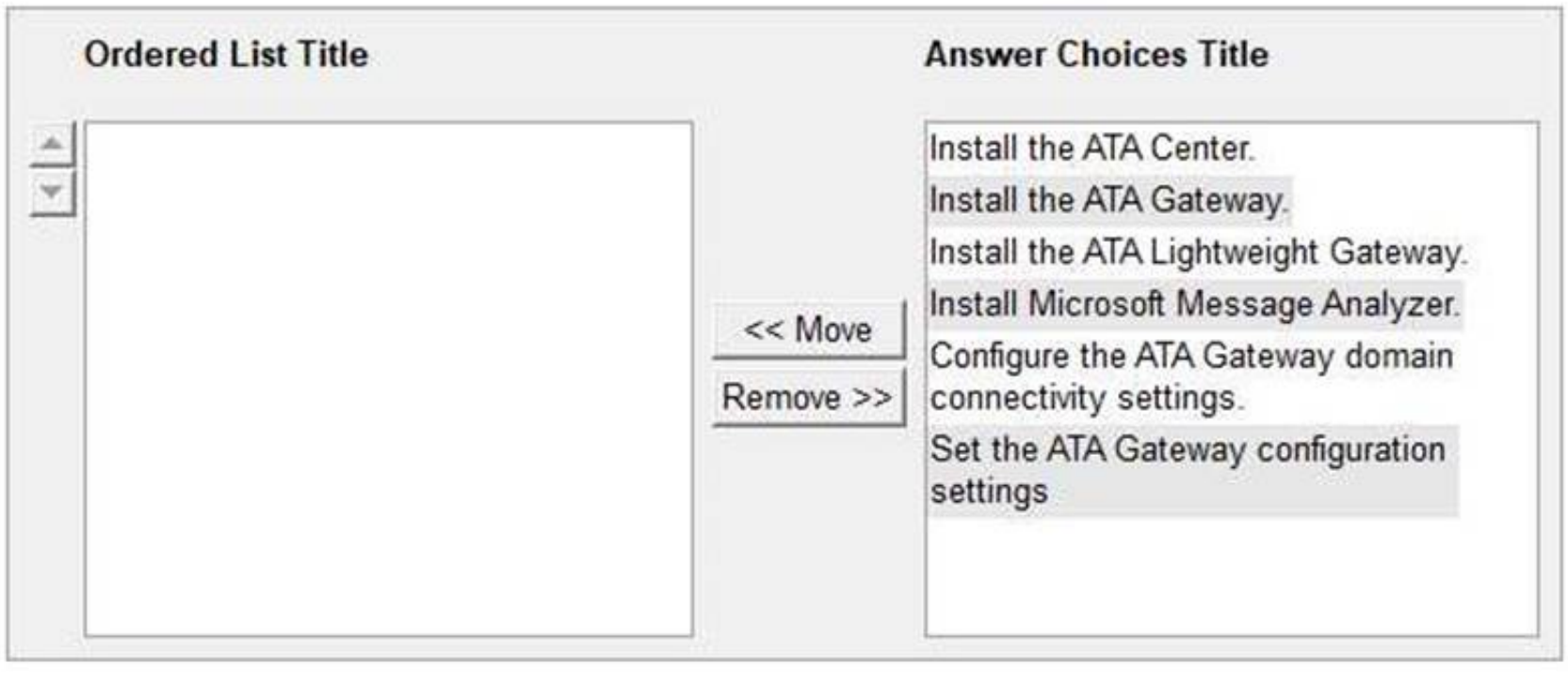
NEW QUESTION 130
You have a guarded fabric and a Host Guardian Service server named HGS1.
You deploy a Hyper-V host named Hyper1, and configure Hyper1 as part of the guarded fabric. You plan to deploy the first shielded virtual machine. You need to ensure that you can run the virtual machine on Hyper1.
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

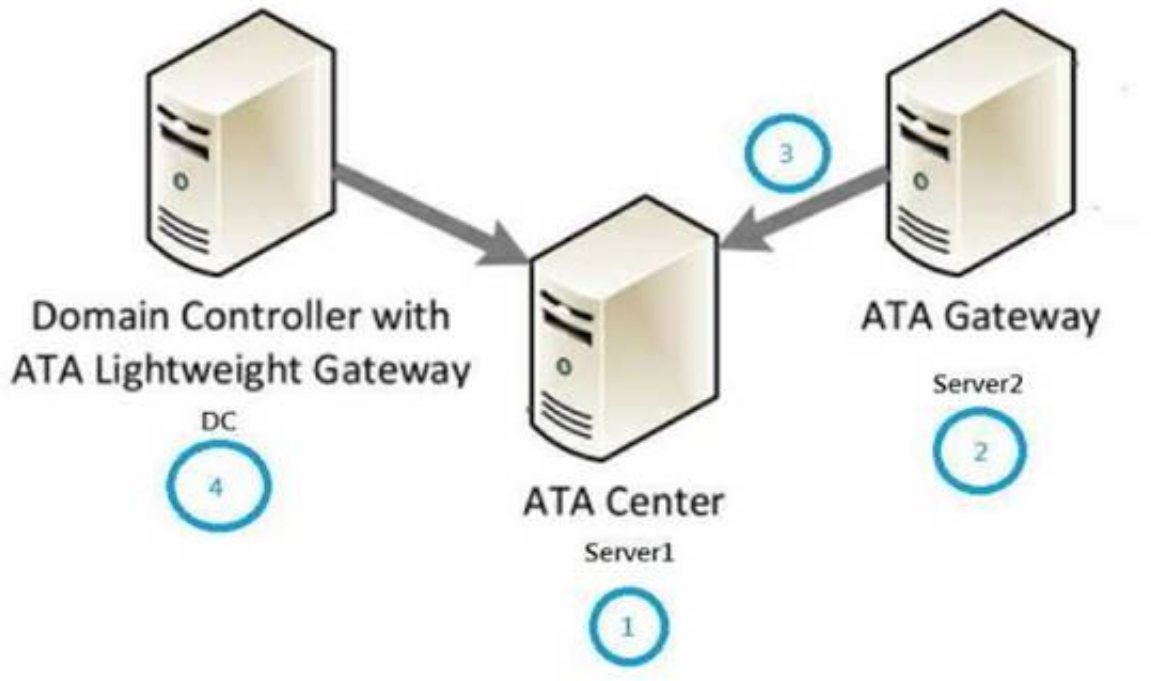
NEW QUESTION 131
DRAG DROP
Your network contains an Active Directory domain named contoso.com.
The domain contains two servers named Server1 and Server2 that run Windows Server 2016. You need to install Microsoft Advanced Threat Analytics (ATA) on Server1 and Server2. Which four actions should you perform in sequence?



A. Mastered
B. Not Mastered

Answer: A

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



NEW QUESTION 135
You have a server named Server1 that runs Windows Server 2016.
You need to install Security Compliance Manager (SCM) 4.0 on Server1. What should you install on Server1 first?

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

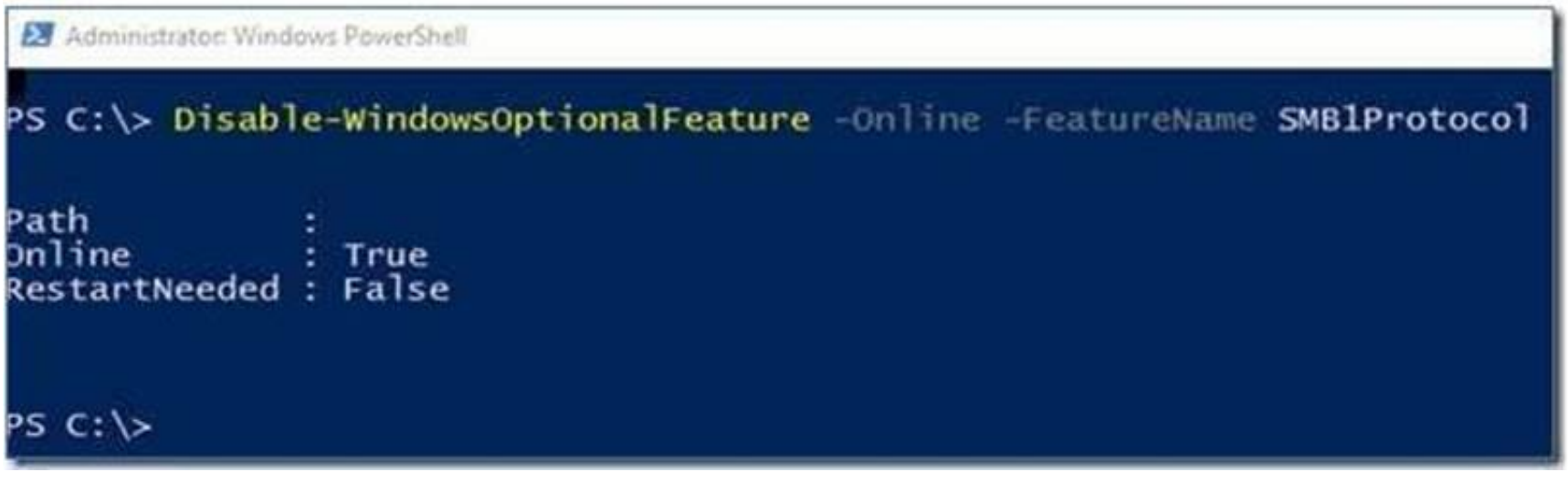
Answer: A

NEW QUESTION 140
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. You need to prevent NTLM authentication on Server1.
Solution: From Windows PowerShell, you run the Disable-WindowsOptionalFeature cmdlet. Does this meet the goal?

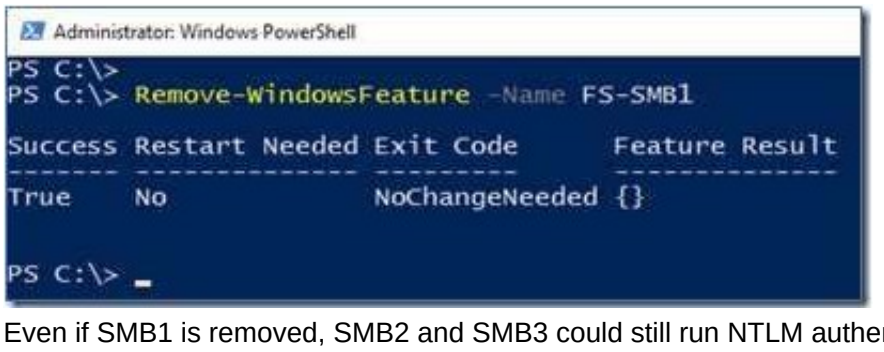
A. Yes
B. No

Answer: B

Explanation:
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
On Client, the PowerShell approach (Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol)
Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol



However, the question asks about Server!
On Server, the PowerShell approach (Remove-WindowsFeature FS-SMB1): Remove-WindowsFeature FS-SMB1



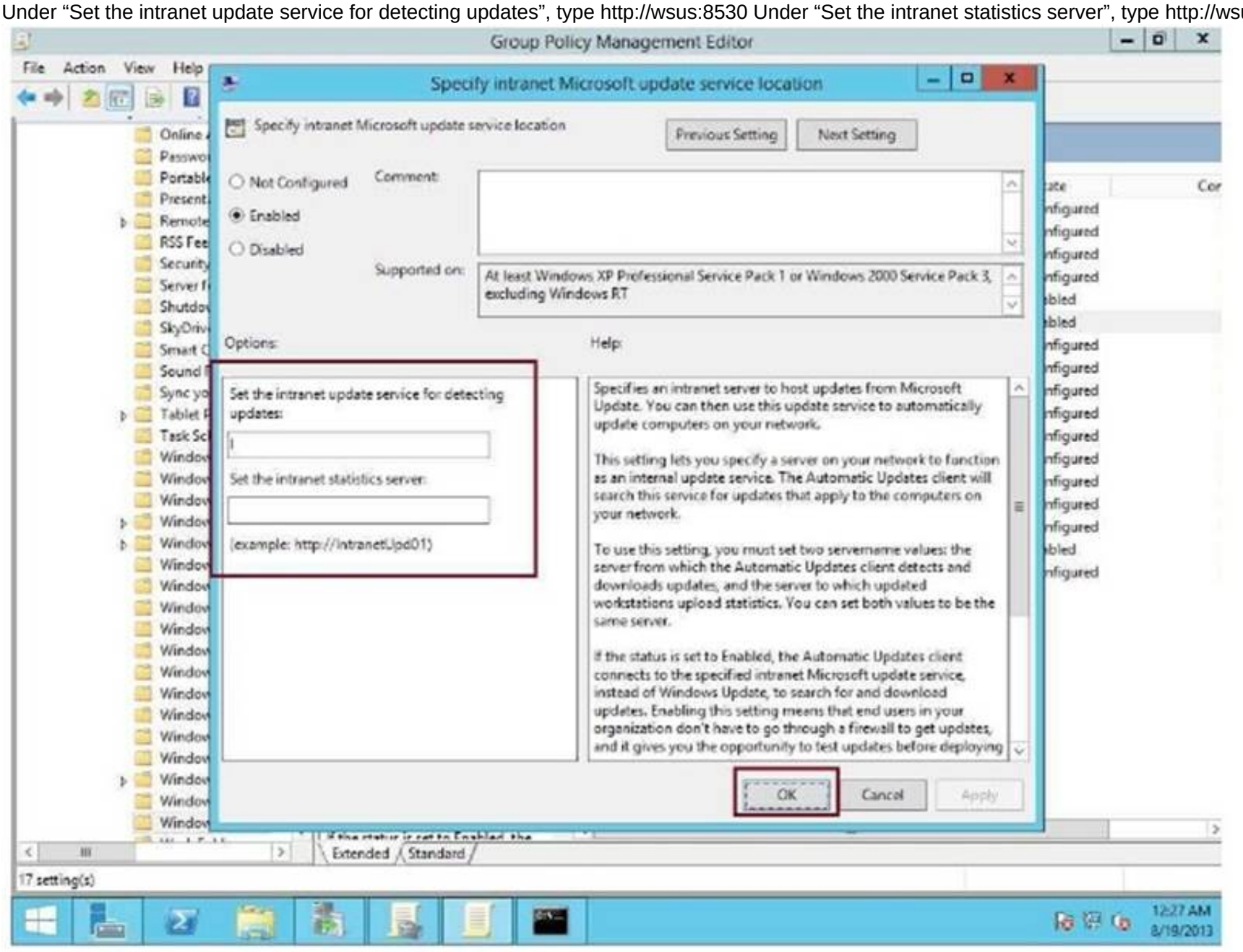
Even if SMB1 is removed, SMB2 and SMB3 could still run NTLM authentication! Therefore, answer is a“NO”.

NEW QUESTION 143
Your network contains an Active Directory domain named contoso.com.The domain contains 1,000 client computers that run either Windows 8.1 or Windows 10.
You have a Windows Server Update Services (WSUS) deployment All client computers receive updates from WSUS.
You deploy a new WSUS server named WSUS2.
You need to configure all of the client computers that run Windows 10 to send WSUS reporting data to WSUS2.
What should you configure?

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

Answer: C

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



NEW QUESTION 146
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2016.
You need to prevent direct .NET scripts invoked by interactive Windows PowerShell sessions from running on the servers.
What should you do for each server?

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

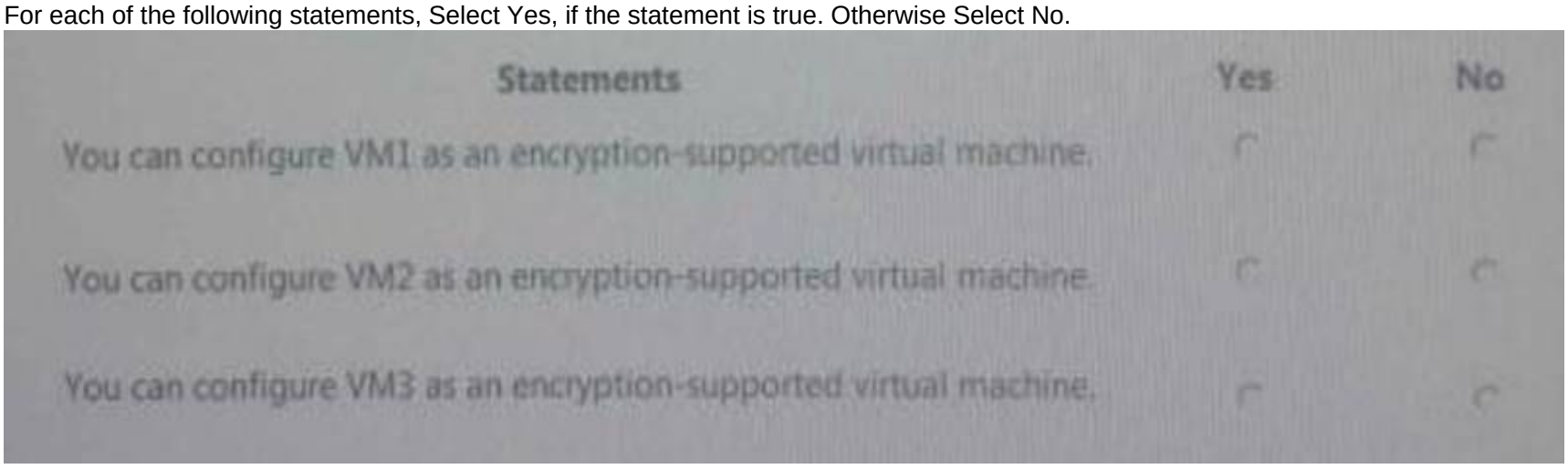
Answer: C

NEW QUESTION 147

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.



A. Mastered
B. Not Mastered

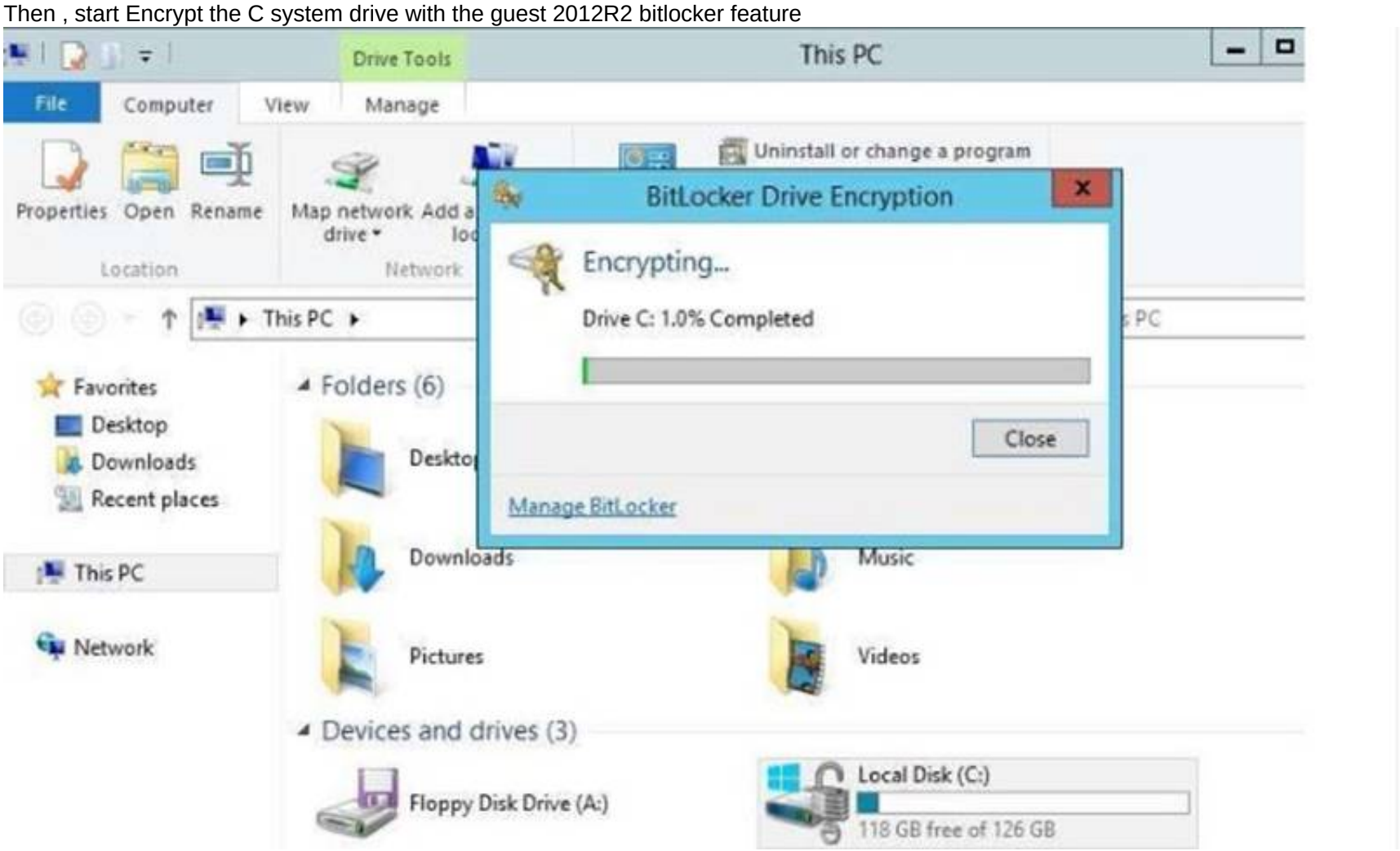
Answer: A

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 151
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 153
You implement Just Enough Administration (JEA) on several file servers that run Windows Server 2016.
The Role Capability file from a server named Server5 contains the following code.

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

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

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

Answer: B

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

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

The "Set-SmbShare" cmdlet is then visible on Server5's JEA endpoint, and allows JEA users to modify the properties of any file share.
https://technet.microsoft.com/en-us/itpro/powershell/windows/smbshare/set-smbshare

NEW QUESTION 157
Your network contains an Active Directory domain named contoso.com.
The domain contains 10 servers that run Windows Server 2016 and 800 client computers that run Windows 10.
You need to configure the domain to meet the following requirements:
-Users must be locked out from their computer if they enter an incorrect password twice.
-Users must only be able to unlock a locked account by using a one-time password that is sent to their mobile phone.
You deploy all the components of Microsoft Identity Manager (MIM) 2016.
Which three actions should you perform before you deploy the MIM add-ins and extensions? Each correct answer presents part of the solution.

A. From a Group Policy object (GPO), configure Public Key Policies
B. Deploy a Multi-Factor Authentication provider and copy the required certificates to the MIM server.
C. From the MIM Portal, configure the Password Reset AuthN Workflow.
D. Deploy a Multi-Factor Authentication provider and copy the required certificates to the client computers.
E. From a Group Policy object (GPO), configure Security Setting

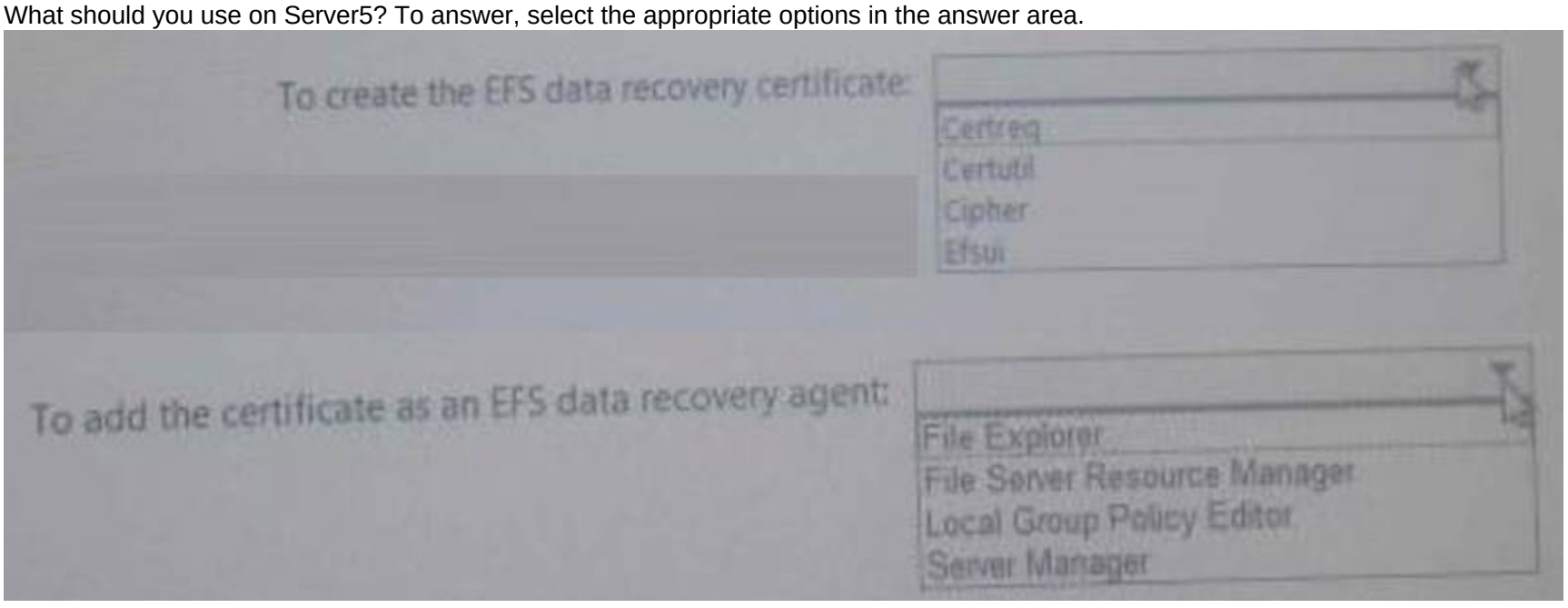
Answer: BCE

Explanation:
-Users must be locked out from their computer if they enter an incorrect password twice. (E)
-Users must only be able to unlock a locked account by using a one-time password that is sent to their mobile phone. (B and C), detailed configuration process in the following web page.
https://docs.microsoft.com/en-us/microsoft-identity-manager/working-with-self-servicepasswordreset# prepare-mim-to-work-with-multi-factor-authentication

NEW QUESTION 159
HOTSPOT
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.

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

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.
All laptops are protected by using BitLocker Drive Encryption (BitLocker).You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.
An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1.
A GPO named GP2 is linked to OU2.
All computers receive updates from Server1. You create an update rule named Update1.
You need to create an Encrypting File System (EFS) data recovery certificate and then add the certificate as an EFS data recovery agent on Server5.
What should you use on Server5? To answer, select the appropriate options in the answer area.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://docs.microsoft.com/en-us/windows/threat-protection/windows-informationprotection/ create-and-verifyan-efs-dra-certificatecipher /R

NEW QUESTION 162
You deploy the Host Guardian Service (HGS).
You have several Hyper-V hosts that have older hardware and Trusted Platform Modules (TPMs) version 1.2.
You discover that the Hyper-V hosts cannot start shielded virtual machines.
You need to configure HGS to ensure that the older Hyper-V hosts can host shielded virtual machines. What should you do?

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

Answer: E

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

NEW QUESTION 163
The Job Title attribute for a domain user named User1 has a value of Sales Manager. User1 runs whoami /claims and receives the following output:

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

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

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

Answer: C

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

NEW QUESTION 167
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 171
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. You need to prevent NTLM authentication on Server1.
Solution: From a Group Policy, you configure the Security Options. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 175
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. You need to prevent NTLM authentication on Server1.
Solution: From Windows PowerShell, you run the New-ADAuthenticationPolicy cmdlet. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 176
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 181
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 allow network administrators to use Just Enough Administration (JEA) to change the
TCP/IP settings on Server1. The solution must use the principle of least privilege. How should you configure the session configuration file?

A. Set RunAsVirtualAccount to $false and set RunAsVirtualAccountGroups to Contoso\Network Configuration Operators.
B. Set RunAsVirtualAccount to $true and set RunAsVirtualAccountGroups to Contoso\Network Configuration Operators.
C. Set RunAsVirtualAccount to $false and set RunAsVirtualAccountGroups to Network Configuration Operators.
D. Set RunAsVirtualAccount to $true and set RunAsVirtualAccountGroups to Network Configuration Operators.

Answer: D

Explanation:

References:
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/newpssessionconfigurationfile? view=powershell-6

NEW QUESTION 183
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You manage a file server that runs Windows Server 2016. The file server contains the volumes configured as shown in the following table.

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

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

A. Yes
B. No

Answer: A

Explanation:

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

NEW QUESTION 188
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 192
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

70-744 Practice Exam Features:

* 70-744 Questions and Answers Updated Frequently

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

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

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