Securing Windows Server 2016

Number: 70-744
Passing Score: 900
Time Limit: 150 min
File Version: 1.0

Exam A

QUESTION 1
You network contains an Active Directory forest named contoso.com.
All domain controllers run Windows Server 2016 Member servers run either Windows Server 2012 R2 or Windows Server 2016.
Client computers run either Windows 8.1 or Windows 10.
You need to ensure that when users access files in shared folders on the network, the files are encrypted when they are transferred over the network.
Solution: You enable access-based enumeration on all the file shares. Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Access-Based Enumeration does not help encrypting network file transfer.

QUESTION 2
You network contains an Active Directory forest named contoso.com.
All domain controllers run Windows Server 2016 Member servers run either Windows Server 2012 R2 or Windows Server 2016.
Client computers run either Windows 8.1 or Windows 10.
You need to ensure that when users access files in shared folders on the network, the files are encrypted when they are transferred over the network.
Solution: You enable SMB encryption on all the computers in domain. Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

SMB Encryption could be enabled on a per-computer wide basis, after you have enabled SMB encryption on a server-level basis, you could not disable encryption for any specific shared folder.
To enable Global level encryption on the server:
Set-SmbServerConfiguration -EncryptData 1

QUESTION 3
Your network contains an Active Directory domain named contoso.com.
The domain contains a computer named Computer1 that runs Windows 10.
Computer1 connects to a home network and a corporate network.
The corporate network uses the 172.16.0.0/24 address space internally.
Computer1 runs an application named App1 that listens to port 8080.
You need to prevent connections to App1 when Computer1 is connected to the home network. Solution: From Group Policy Management, you create a software restriction policy.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Software Restriction Policy does not filter incoming network traffic, what you actually need is Windows Firewall Inbound Rule on the Private profile

QUESTION 4
Your network contains an Active Directory domain named contoso.com.
The domain contains a computer named Computer1 that runs Windows 10.
Computer1 connects to a home network and a corporate network.
The corporate network uses the 172.16.0.0/24 address space internally.
Computer1 runs an application named App1 that listens to port 8080.
You need to prevent connections to App1 when Computer1 is connected to the home network. Solution: From Group Policy Management, you create an AppLocker rule. Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
AppLocker does not filter incoming network traffic, what you actually need is Windows Firewall Inbound Rule on the Private profile.

QUESTION 5
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
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

Correct Answer: B
Section: (none)
Explanation

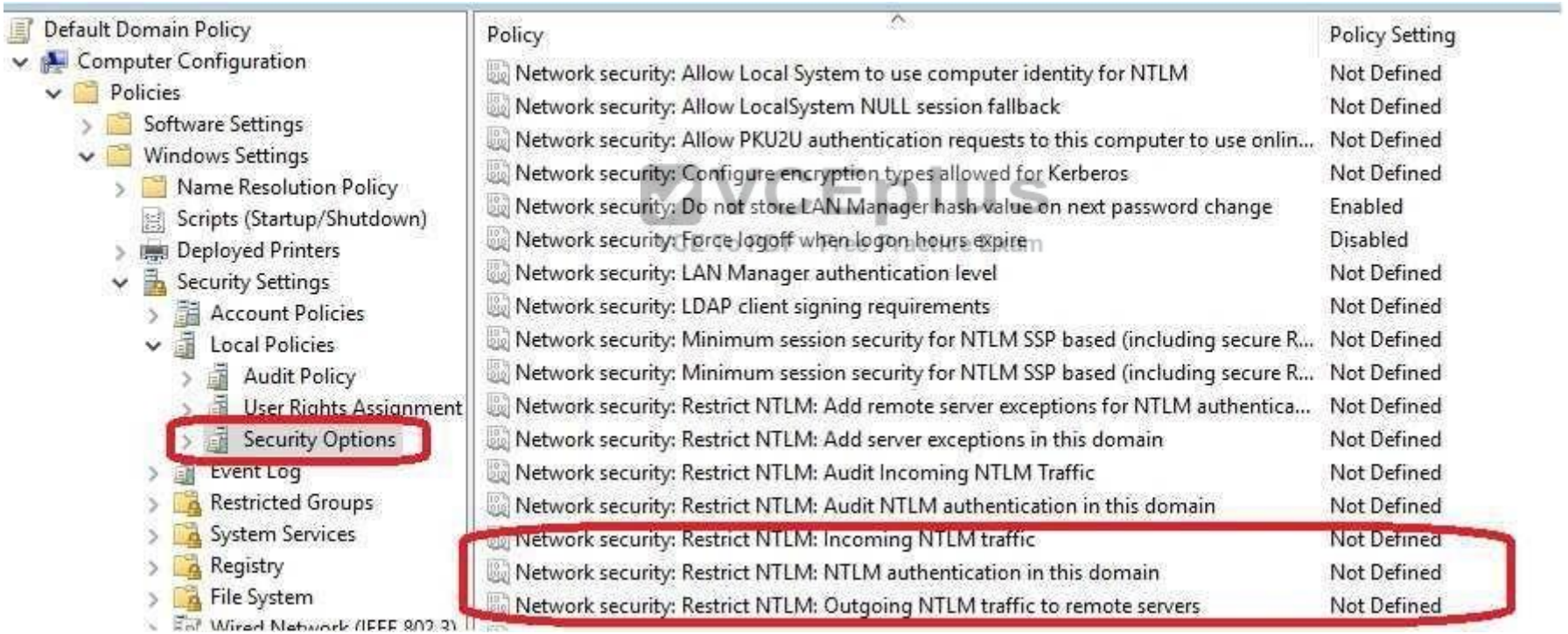
Explanation/Reference:
ADDS Authentication Policy does not provide ability to prevent the use of NTLM authentication.
QUESTION 7
Your network contains an Active Directory domain named contoso.com.
The domain contains a server named Server1 that runs Windows Server 2016.

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:



QUESTION 8
Your network contains an Active Directory domain named contoso.com.
The domain contains two DNS servers that run Windows Server 2016.
The servers host two zones named contoso.com and admin.contoso.com.
You sign both zones.

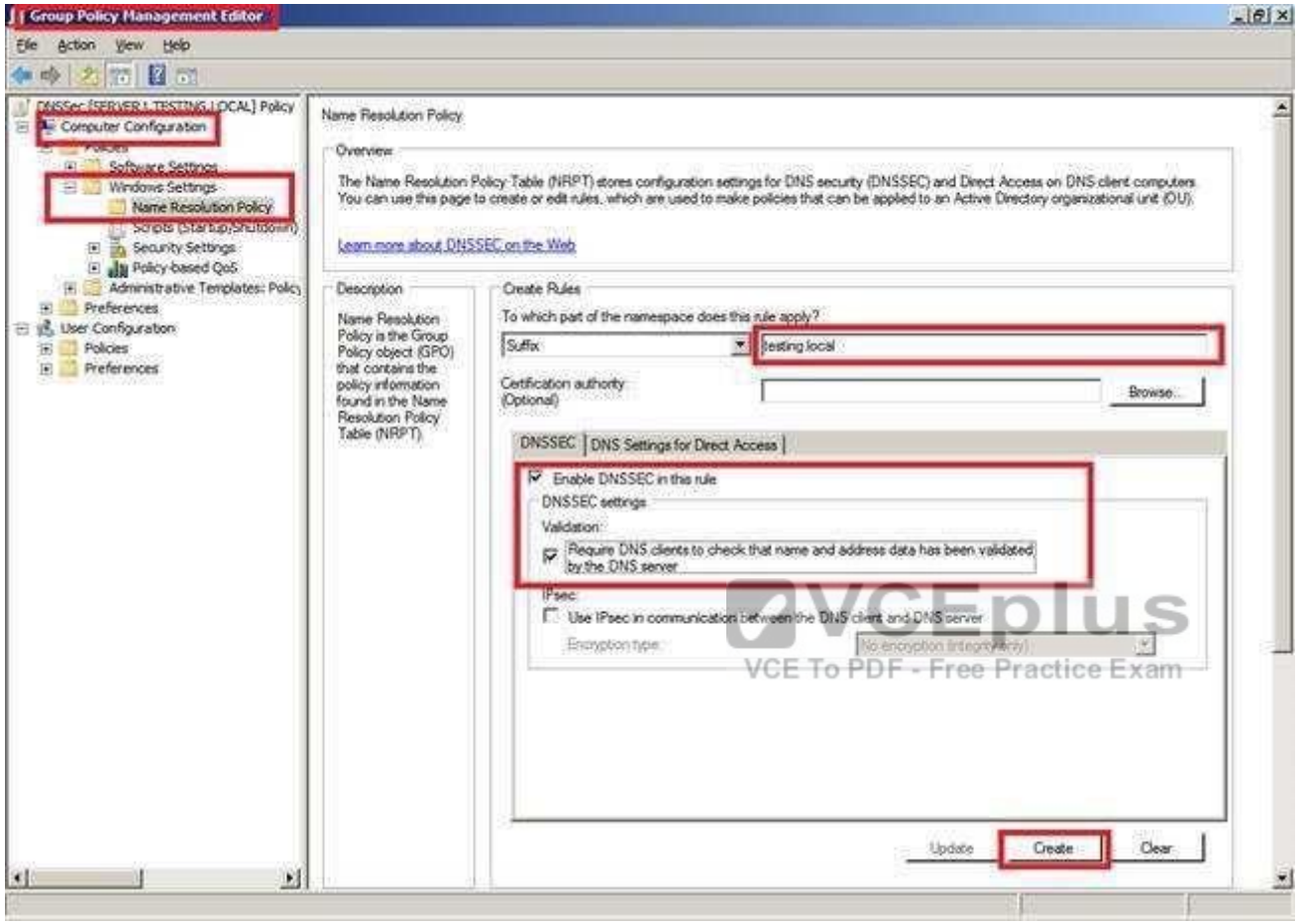
You need to ensure that all client computers in the domain validate the zone records when they query the zone.
What should you deploy?

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

Correct Answer: C
Section: (none)

Explanation

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



QUESTION 9

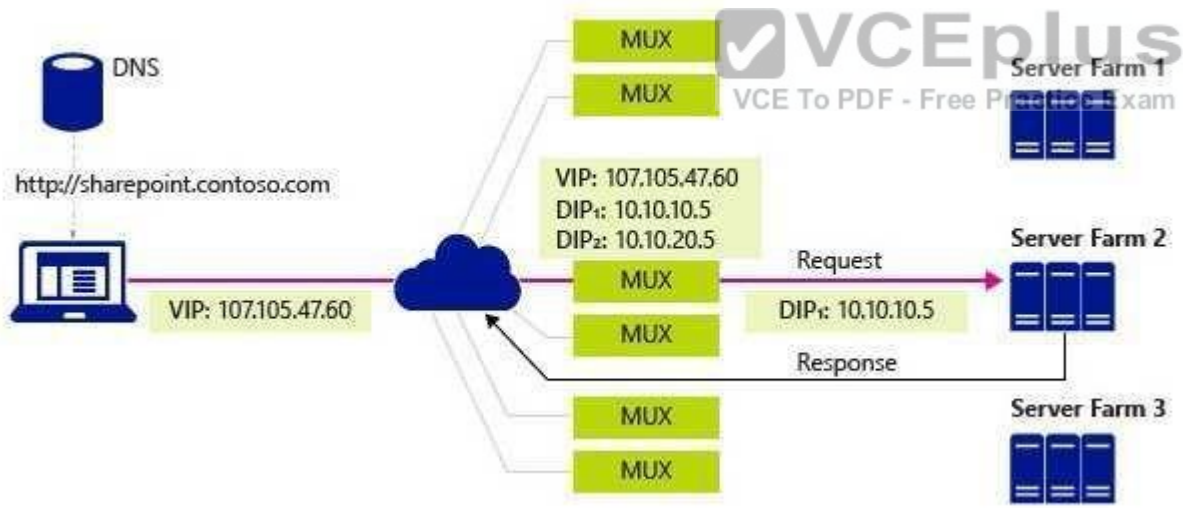
You have 10 Hyper-V hosts that run Windows Server 2016.
Each Hyper-V host has eight virtual machines that run a distributed web application named App1.
You plan to implement a Software Load Balancing (SLB) solution for client access to App1.
You deploy two new virtual machines named SLB1 and SLB2.
You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

A. Component to install on SLB1 and SLB2: SLB Host Agent
B. Component to install on SLB1 and SLB2: Network Load Balancing (NLB)
C. Component to install on SLB1 and SLB2: SLB Multiplexer (MUX)
D. Component to install on each Hyper-V host:SLB Host Agent

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

Correct Answer: CD
Section: (none)
Explanation

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



QUESTION 10
You have the Windows Server 2016 operating system images as described in the answer choices.
Your company's security policy states that you must minimize the attack surface when provisioning new servers.
You need to deploy a Host Guardian Service cluster. Which image should you use for the deployment?

A. A Nano Server that runs the Standard edition of Windows Server
B. A Server Core installation that runs the Datacenter edition of Windows Server

C. A Full installation that runs the Standard edition of Windows Server
D. A Nano Server that runs the Datacenter edition of Windows Server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabric-prepare-for-hgs Prerequisites
Hardware: HGS can be run on physical or virtual machines, but physical machines are recommended.
If you want to run HGS as a three-node physical cluster (for availability), you must have three physical servers. (As a best practice for clustering, the three servers should have very similar hardware.)
Operating system: Windows Server 2016, Standard or Datacenter edition. <---- so you cannot use Server Core or Nano Server for running Host Guardian Service.
Server Roles: Host Guardian Service and supporting server roles.
Configuration permissions/privileges for the fabric (host) domain: You will need to configure DNS forwarding between the fabric (host) domain and the HGS domain. If you are using Admin-trusted attestation (AD mode), you will need to configure an Active Directory trust between the fabric domain and the HGS domain.

QUESTION 11
Your network contains an Active Directory forest named contoso.com.
The forest functional level is Windows Server 2012. The forest contains a single domain. The domain contains multiple Hyper-V hosts.
You plan to deploy guarded hosts.
You deploy a new server named Server22 to a workgroup.
You need to configure Server22 as a Host Guardian Service server.
What should you do before you initialize the Host Guardian Service on Server22?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 14

QUESTION 12
You are implementing Privileged Access Management (PAM) for an Active Directory forest named contoso.com.

You install a bastion forest named adatum.com, and you establish a trust between the forests.
You need to create a group in contoso.com that will be used by Microsoft Identity Manager to create groups in adatum.com.
How should you configure the group? Choose Two.

A. Group name: ADATUM$$$
B. Group name: CONTOSO$$$
C. Group name: CONTOSO_Adatum$
D. Group name: MIM$
E. Group type: a domain local distribution group
F. Group type: a domain local security group
G. Group type: a global distribution group
H. Group type: a universal distribution group
I. Group type: a universal security group

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:
Production forest is contoso.com
Bastion forest is adatum.com
https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/planning-bastion-environment
A security group on the local domain (contoso.com)
There must be a group in the existing domain, whose name is the NetBIOS domain name followed by three dollar signs, e.g., CONTOSO$$$.
The group scope must be domain local and the group type must be Security.
This is needed for groups to be created in the dedicated administrative forest (adatum.com) with the same Security identifier as groups in this domain (contoso.com).
Create this group with the following
New-ADGroup -name 'CONTOSO$$$' -GroupCategory Security -GroupScope DomainLocal -SamAccountName 'CONTOSO$$$'
After this, MIM could create "Shadow Group" in bastion adatum.com forest.

QUESTION 13
You have 100 computers that run Windows 10 and are members of a workgroup.

You need to configure Windows Defender to meet the following requirements:
-Exclude a C:\Sales\Salesdb from malware scans.
-Configure a full scan to occur daily.
What should you run to meet each requirement?

A. Exclude C:\Sales\Salesdb from malware scans: Add-MpPreference
B. Exclude C:\Sales\Salesdb from malware scans: Get-MpThreat
C. Exclude C:\Sales\Salesdb from malware scans: Set-MpPreference
D. Exclude C:\Sales\Salesdb from malware scans: Start-MpScan
E. Exclude C:\Sales\Salesdb from malware scans: Start-MpWDOScan
F. Configure a full scan to occur daily: Add-MpPreference
G. Configure a full scan to occur daily: Get-MpThreat
H. Configure a full scan to occur daily: Set-MpPreference
I. Configure a full scan to occur daily: Start-MpScan
J. Configure a full scan to occur daily: Start-MpWDOScan

Correct Answer: CH
Section: (none)
Explanation

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

QUESTION 14
You have a Hyper-V host named Server1 that runs Windows Server 2016.
Server1 hosts the virtual machines configured as shown in the following table.

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

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

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

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

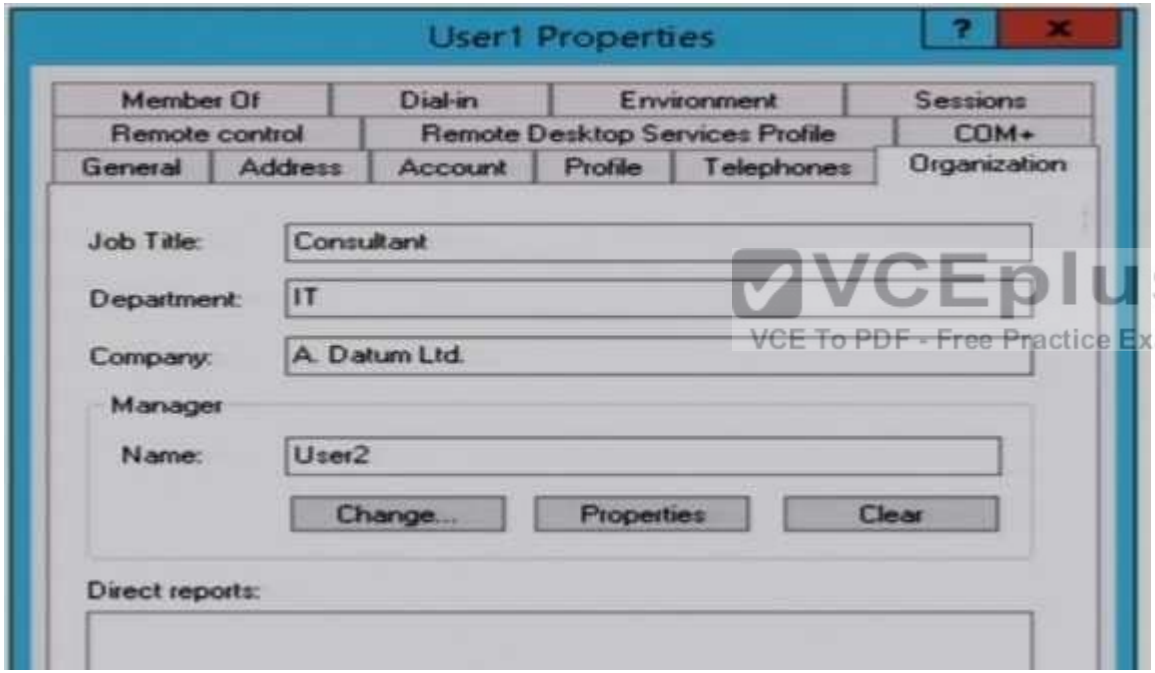
Correct Answer: AL
Section: (none)
Explanation

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

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

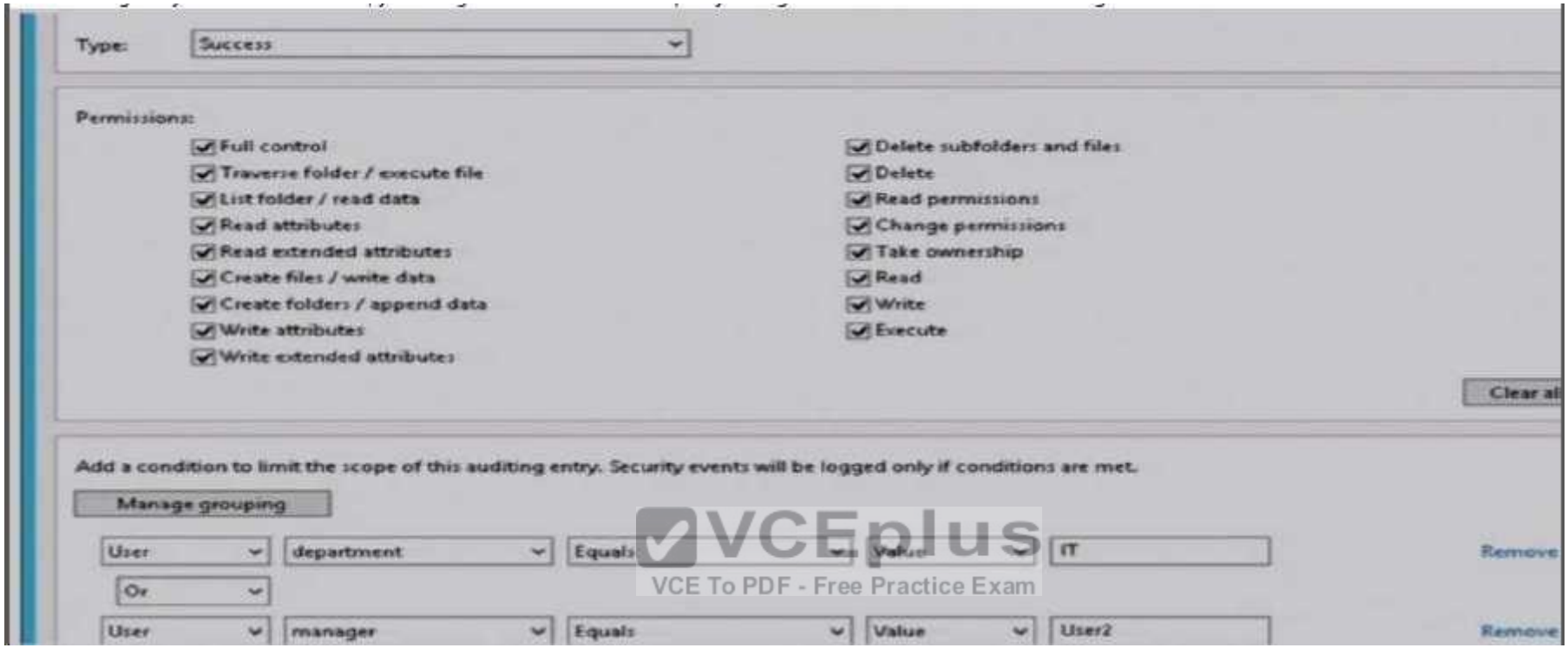
https://www.howtogeek.com/howto/6229/how-to-use-bitlocker-on-drives-without-tpm/
If you don't use TPM for protecting a drive, there is no such Virtual TPM or VM Generation, or VM Configuration version requirement, you can even use Bitlocker without TPM Protector with earlier versions of Windows.

QUESTION 15
Your network contains an Active Directory domain named adatum.com.
The domain contains a file server named Server1 that runs Windows Server 2016.
You have an organizational unit (OU) named OU1 that contains Server1.
You create a Group Policy object (GPO) named GPO1 and link GPO1 to OU1.
A user named User1 is a member of group named Group1. The properties of User1 are shown in follow:-



User1 has permissions to two files on Server1 configured as shown in the following table.
File name Permission
File1.doc Allow Read
File2.doc Deny Modify

From Auditing Entry for Global File SACL, you configure the advanced audit policy settings in GPO1 as shown in the SACL figure:-



Which of the following statements are true? Choose Three.

A. From File Explorer, when User1 double-clicks File1.doc. an event will be logged: Yes
B. From File Explorer, when User1 double-clicks File1.doc. an event will be logged: No
C. From File Explorer, when User1 double-clicks File2.doc. an event will be logged: Yes
D. From File Explorer, when User1 double-clicks File2.doc. an event will be logged: No
E. From Microsoft Word, when User1 attempts to save changes to File1.doc, an event will be logged: Yes
F. From Microsoft Word, when User1 attempts to save changes to File1.doc, an event will be logged: No

Correct Answer: ADF
Section: (none)
Explanation
Explanation/Reference:
From the SACL, only Successful operations by User1 will be logged "Type: Success".

QUESTION 16
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.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 17
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.
You have an organizational unit (OU) named Administration that contains the computer account of Server1.
You import the Active Directory module to Server1.
You create a Group Policy object (GPO) named GPO1. You link GPO1 to the Administration OU.
You need to log an event each time an Active Directory cmdlet executed successfully from Server1.
What should you do?

A. From Advanced Audit Policy in GPO1. configure auditing for other privilege use events.
B. Run the Add-NetEventProvider -Name "Microsoft-Active-Directory" -MatchAnyKeyword PowerShell command.
C. From Advanced Audit Policy in GPO1, configure auditing for directory service changes.
D. From Administrative Templates in GPO1, configure a Windows PowerShell policy.

Correct Answer: D
Section: (none)
Explanation

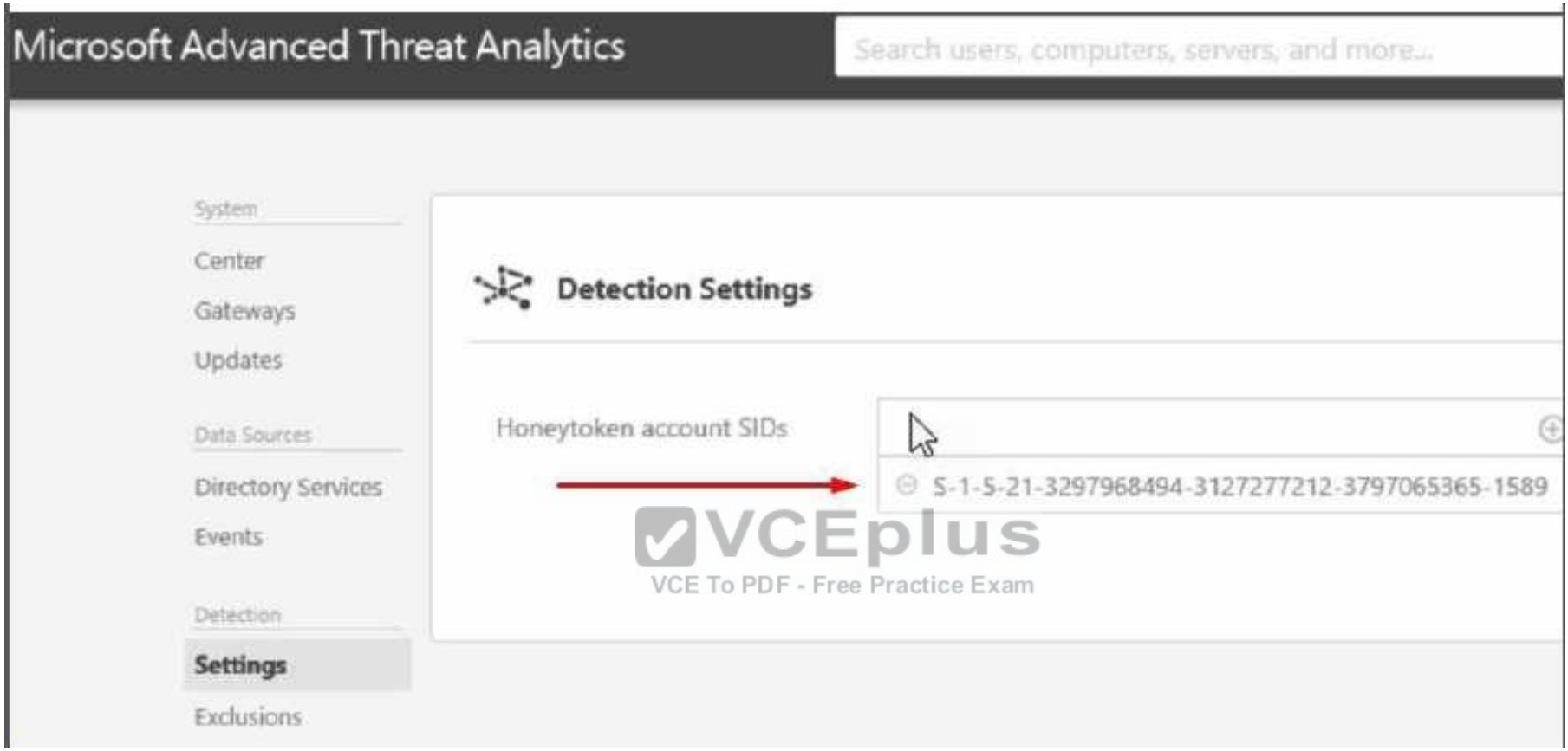
Explanation/Reference:
In the following GPO location, you can enable the setting "Turn on Module Logging" to record an event each time the PowerShell executes a cmdlet of a specific PowerShell module, for example "ActiveDirectory".
"Computer Configuration\Administrative Templates\Windows Components\Windows PowerShell"

QUESTION 18
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 SID of User1
B. the UPN of User1
C. the Globally Unique Identifier (GUID) of User1
D. the SAM account name of User1

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 19
You have a file server named Server1 that runs Windows Server 2016.
A new policy states that ZIP files must not be stored on Server1.
An administrator creates a file screen filter as shown in the following
output Active : False Description:
IncludeGroup: {Compressed Files}
MatchesTemplate: False
Notification {MSFT FSRMAction, MSFT FSRMAction}
Path : C:\

Template :
PSComputerName:
You need to prevent users from storing ZIP files on Server1, what should you do?

A. Enable Quota Management on all the drives.
B. Add a template to the filter.
C. Change the filter to active.
D. Configure File System (Global Object Access Auditing).

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"Active : False", then it is a Passive Filescreen filther which will not block unwanted file types.

QUESTION 20
Your network contains an Active Directory forest named corp.contoso.com.
You are implementing Privileged Access Management (PAM) by using a bastion forest named priv.contoso.com. You need to create shadow groups in priv.contoso.com. Which cmdlet should you use?

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

Correct Answer: D
Section: (none)
Explanation

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

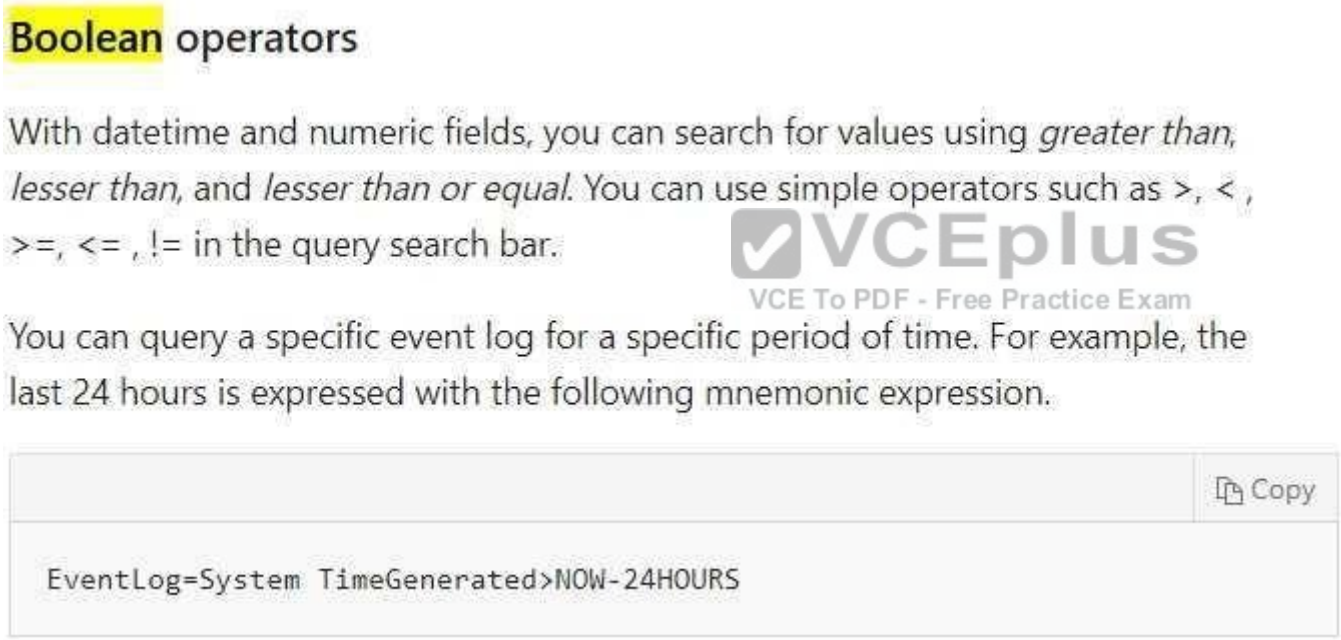
QUESTION 21
You implement Log Analytics in Microsoft Operations Management Suite (OMS) on all servers that run Windows Server 2016.
You need to generate a daily report that identifies which servers restarted during the last 24 hours.
Which query should you use?

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

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

Correct Answer: C
Section: (none)
Explanation

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



QUESTION 22
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      String  "US"
```

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 23
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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 24
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2016.
The Microsoft Advanced Threat Analytics (ATA) Center service is installed on Server1.
The domain contains the users shown in the following table.

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

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

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

Correct Answer: F
Section: (none)
Explanation

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

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

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

QUESTION 25
You are building a guarded fabric.You need to configure Admin-trusted attestation.
Which cmdlet should you use?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Authorize Hyper-V hosts using Admin-trusted attestation https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabric-add-host-information-for-admin-trusted-attestation

QUESTION 26
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. To create the EFS data recovery certificate: Certreq
B. To create the EFS data recovery certificate: Certutil
C. To create the EFS data recovery certificate: Cipher
D. To create the EFS data recovery certificate: Efsui
E. To add the certificate as an EFS data recovery agent: File Explorer
F. To add the certificate as an EFS data recovery agent: File Server Resource Manager
G. To add the certificate as an EFS data recovery agent: Local Group Policy Editor
H. To add the certificate as an EFS data recovery agent: Server Manager

Correct Answer: CG
Section: (none)
Explanation

Explanation/Reference:
https://docs.microsoft.com/en-us/windows/threat-protection/windows-information-protection/create-and-verify-an-efs-dra-certificate
cipher /R

QUESTION 27
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.

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

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.
All laptops are protected by using BitLocker Drive Encryption (BitLocker).
You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.
An OU named OU2 contains the computer accounts of the computers in the marketing department.
A Group Policy object (GPO) named GP1 is linked to OU1.
A GPO named GP2 is linked to OU2.

All computers receive updates from Server1.
You create an update rule named Update1.
You need to implement BitLocker Network Unlock for all of the laptops.
Which server role should you deploy to the network?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-how-to-enable-network-unlock
Network Unlock core requirements
Network Unlock must meet mandatory hardware and software requirements before the feature can automatically unlock domain joined systems. These requirements include:
You must be running at least Windows 8 or Windows Server 2012.
Any supported operating system with UEFI DHCP drivers can be Network Unlock clients.
A server running the Windows Deployment Services (WDS) role on any supported server operating system.
BitLocker Network Unlock optional feature installed on any supported server operating system.
A DHCP server, separate from the WDS server.
Properly configured public/private key pairing.
Network Unlock Group Policy settings configured.

QUESTION 28
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.

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

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

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 29
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.

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

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.
All laptops are protected by using BitLocker Drive Encryption (BitLocker).
You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.

An OU named OU2 contains the computer accounts of the computers in the marketing department.
A Group Policy object (GPO) named GP1 is linked to OU1.
A GPO named GP2 is linked to OU2.
All computers receive updates from Server1.
You create an update rule named Update1.
You need to ensure that AppLocker rules will apply to the marketing department computers. What should you do?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 30
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.

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

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members.
All laptops are protected by using BitLocker Drive Encryption (BitLocker).
You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.
An OU named OU2 contains the computer accounts of the computers in the marketing department.
A Group Policy object (GPO) named GP1 is linked to OU1.
A GPO named GP2 is linked to OU2.
All computers receive updates from Server1.
You create an update rule named Update1.
You need to create a Role Capability file on Server3. Which file should you create?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Your network contains an Active Directory domain named contoso.com.
The domain contains two servers named Server1 and Server2 that run Windows Server 2016.
Server1 is configured as a domain controller.
You configure Server1 as a Just Enough Administration (JEA) endpoint. You configure the required JEA rights for a user named User1. You need to tell User1 how to manage Active Directory objects from Server2. What should you tell User1 to do first on Server2?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Your network contains an Active Directory domain named contoso.com. The domain contains 100 servers.
You deploy the Local Administrator Password Solution (LAPS) to the network.
You discover that the members of a group named FinanceAdministrators can view the password of the local Administrator accounts on the servers in an organizational unit (OU) named FinanceServers.
You need to prevent the FinanceAdministrators members from viewing the local administrators' passwords on the servers in FinanceServers.
Which permission should you remove from FinanceAdministrators?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: https://blogs.technet.microsoft.com/askpfeplat/2015/12/28/local-administrator-password-solution-laps-implementation-hints-and-security-nerd-commentaryincludingmini-threat-model/
Access to the password is granted via the “Control Access” right on the attribute.
Control Access is an “Extended Right” in Active Directory, which means if a user has been granted the “All Extended Rights” permission they’ll be able to see passwords even if you didn’t give them permission.

QUESTION 33
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 Settings.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
-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-service-password-reset#prepare-mim-to-work-with-multi-factor-authentication

QUESTION 34
Your network contains an Active Directory forest named contoso.com. The forest functional level is Windows Server 2012.
The forest contains 20 member servers that are configured as file servers. All domain controllers run Windows Server 2016.
You create a new forest named contosoadmin.com.
You need to use the Enhanced Security Administrative Environment (ESAE) approach for the administration of the resources in contoso.com.
Which two actions should you perform? Each correct answer presents part of the solution.

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material#ESAE_BM
Trust configurations - Configure trust from managed forests(s) or domain(s) to the administrative forest
A one-way trust is required from production environment to the admin forest. This can be a domain trust or a forest trust.

The admin forest/domain (contosoadmin.com) does not need to trust the managed domains/forests (contoso.com) to manage Active Directory, though additional applications may require a two-way trust relationship, security validation, and testing.
Selective authentication should be used to restrict accounts in the admin forest to only logging on to the appropriate production hosts.

QUESTION 35
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

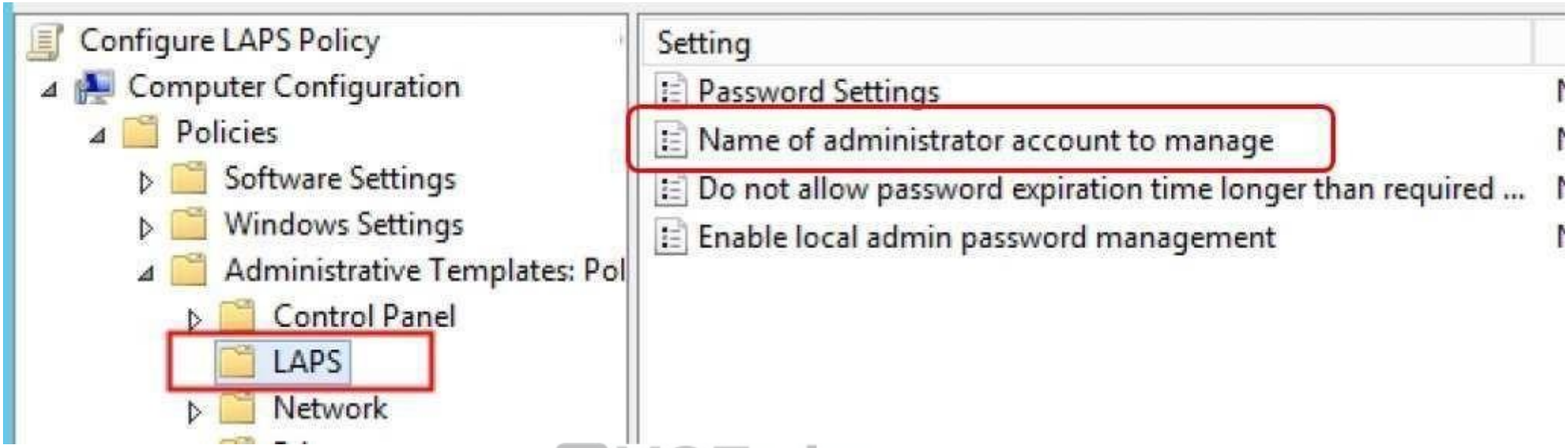
QUESTION 36
Your network contains an Active Directory domain named contoso.com. All servers in the domain run Windows Server 2016.
All client computers run Windows 10.

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 Reset-AdmPwdPassword 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 computers. rename the FinAdmin accounts to Administrator.

Correct Answer: C
Section: (none)
Explanation

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



QUESTION 37

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

Which of the following statements are true? Choose Three.

A. You can configure VM1 as an encryption-supported virtual machine: Yes

B. You can configure VM1 as an encryption-supported virtual machine: No

C. You can configure VM2 as an encryption-supported virtual machine: Yes

D. You can configure VM2 as an encryption-supported virtual machine: No E. You can configure VM3 as an encryption-supported virtual machine: Yes

F. You can configure VM3 as an encryption-supported virtual machine: No

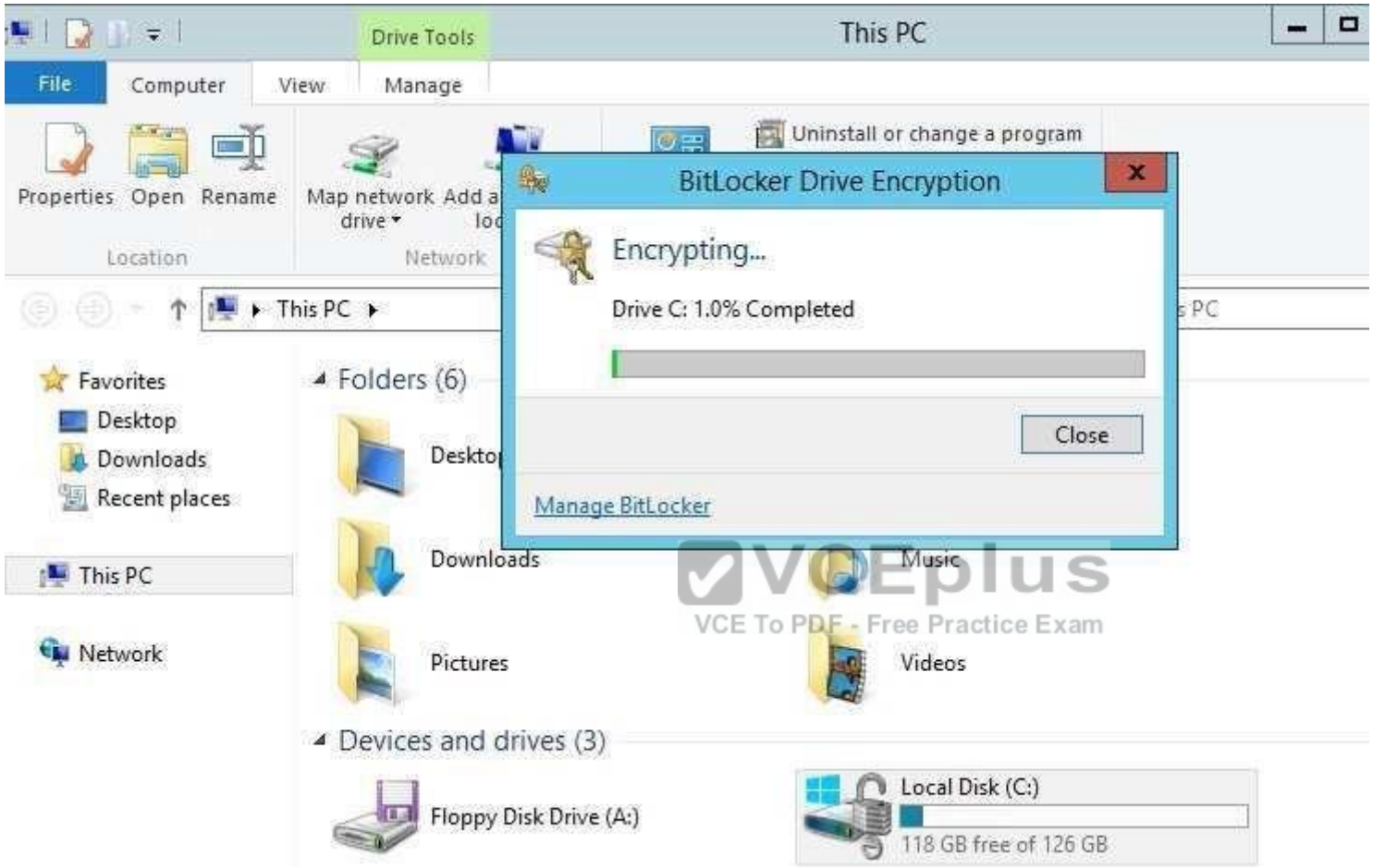
Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
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:-

QUESTION 38
Your network contains an Active Directory domain.
Microsoft Advanced Threat Analytics (ATA) is deployed to the domain.
A database administrator named DBA1 suspects that her user account was compromised.
Which three events can you identify by using ATA? Each correct answer presents a complete solution.

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

Correct Answer: CDE
Section: (none)
Explanation

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

QUESTION 39
You have a server named Server1 that runs Windows Server 2016.
You need to identify whether any inbound rules on Server1 require that users be authenticated before they can connect to the server.
Which cmdlet should you use?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
The complete cmdlet to perform the required action:-

```
PS C:\> Get-NetFirewallRule -DisplayName TEST | Get-NetFirewallSecurityFilter


Authentication     : Required
Encryption         : NotRequired
OverrideBlockRules : False
LocalUser          : Any
RemoteUser         : Any
RemoteMachine      : Any


PS C:\>
```

QUESTION 40
You have a server named Server1 that runs Windows Server 2016.
You need to identify the default action for the inbound traffic when Server1 connects to the domain.
Which cmdlet should you use?

A. Get-NetIPSecRule
B. Get-NetFirewallRule
C. Get-NetFirewallProfile
D. Get-NetFirewallSetting
E. Get-NetFirewallPortFilter

F. Get-NetFirewallAddressFilter
G. Get-NetFirewallApplicationFilter

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

```
PS C:\> Get-NetFirewallProfile Domain


Name                            : Domain
Enabled                         : False
DefaultInboundAction            : NotConfigured
DefaultOutboundAction           : NotConfigured
AllowInboundRules               : NotConfigured
AllowLocalFirewallRules         : NotConfigured
AllowLocalIPsecRules            : NotConfigured
AllowUserApps                   : NotConfigured
AllowUserPorts                  : NotConfigured
AllowUnicastResponseToMulticast : NotConfigured
NotifyOnListen                  : False
EnableStealthModeForIPsec       : NotConfigured
LogFileName                     : %systemroot%\system32\LogFiles\Firewall\pfirewall.log
LogMaxSizeKilobytes             : 4096
LogAllowed                      : False
LogBlocked                      : False
LogIgnored                      : NotConfigured
DisabledInterfaceAliases        : {NotConfigured}
```


QUESTION 41
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Serverl that has Microsoft Security Compliance Manager (SCM) 4.0 installed. The domain contains domain controllers that run Windows Server 2016.
A Group Policy object (GPO) named GPO1 is applied to all of the domain controllers.
GPO1 has a Globally Unique Identifier (GUID) of 7ABCDEFG-1234-5678-90AB-005056123456.
You need to create a new baseline that contains the settings from GPO1. What should you do first?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 42
Your network contains an Active Directory domain named contoso.com.
The domain contains a server named Servers that has the Windows Server Update Services server role installed.
You need to configure Windows Server Update Services (WSUS) on Servers to use SSL.
You install a certificate in the local Computer store. Which two tools should you use? Each correct answer presents part of the solution.

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

Correct Answer: AC
Section: (none)
Explanation

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

QUESTION 43
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 settings.

Correct Answer: C
Section: (none)
Explanation

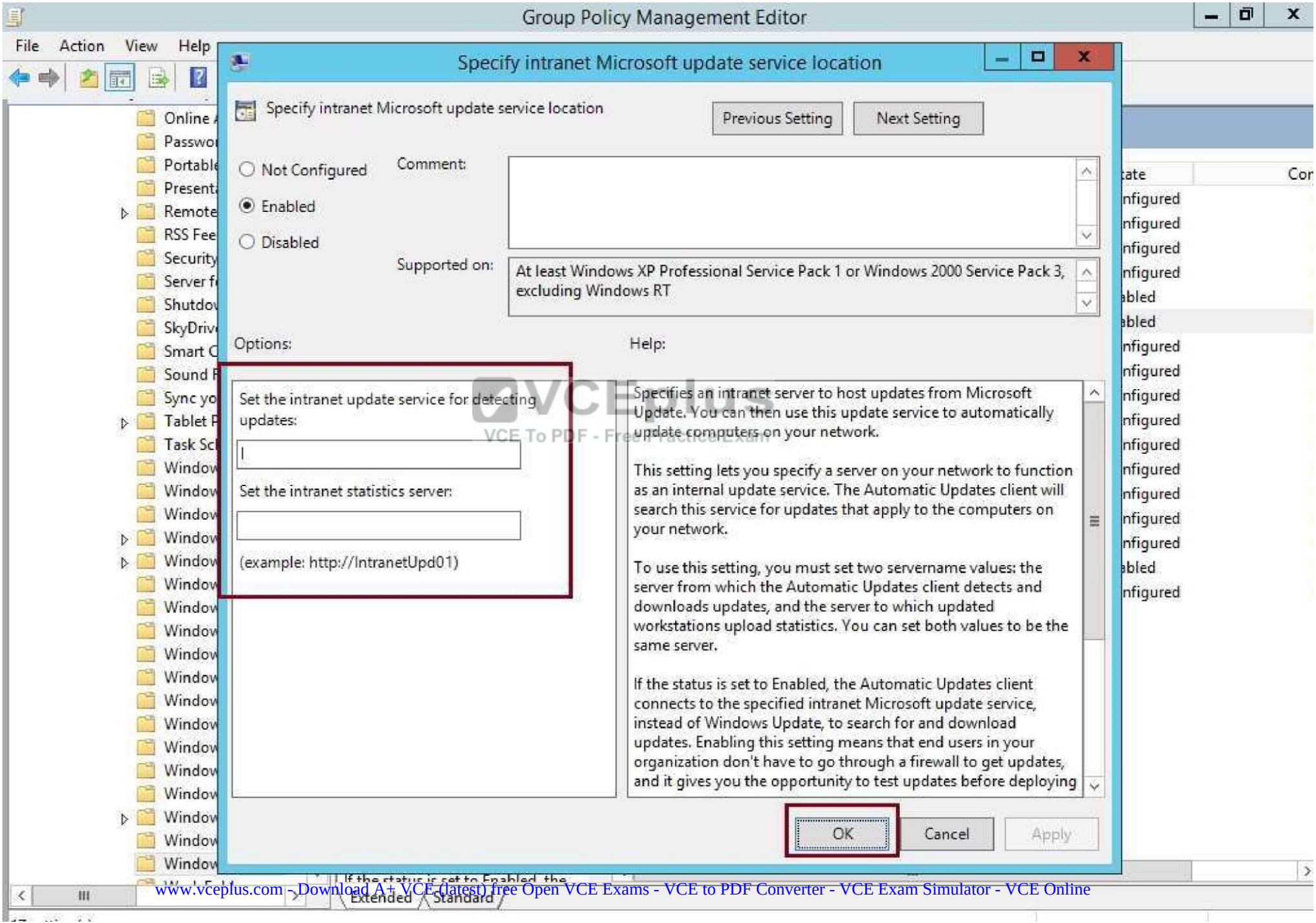
Explanation/Reference:
The most accurate way to do so is to configure a PowerShell execution policy, however, answers of this question do not provide this choice.
As Answer A,B and D are completely irrelevant, only answer C could achieve what the question requires. Answer C prevents all interactive remote PowerShell sessions.

QUESTION 44
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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

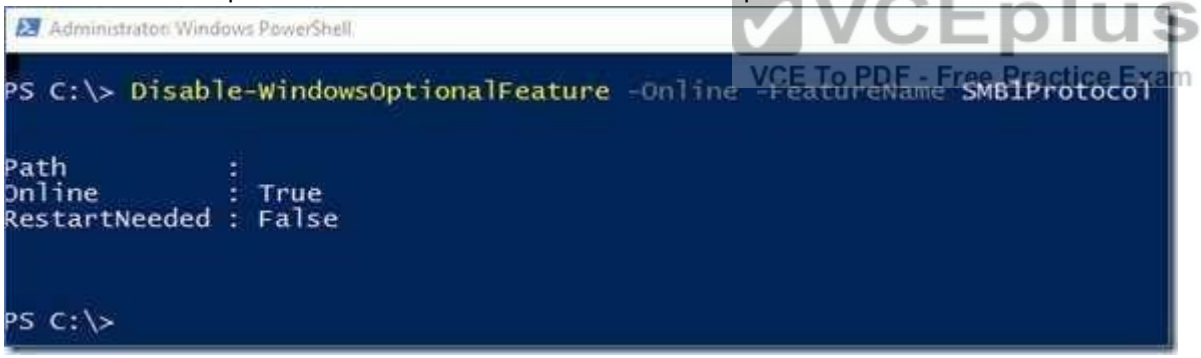


QUESTION 45
Your network contains an Active Directory domain named contoso.com.
The domain contains a server named Server1 that runs Windows Server 2016.
You need to prevent NTLM authentication on Server1.
Solution: From Windows PowerShell, you run the Disable-WindowsOptionalFeature cmdlet.
Does this meet the goal?

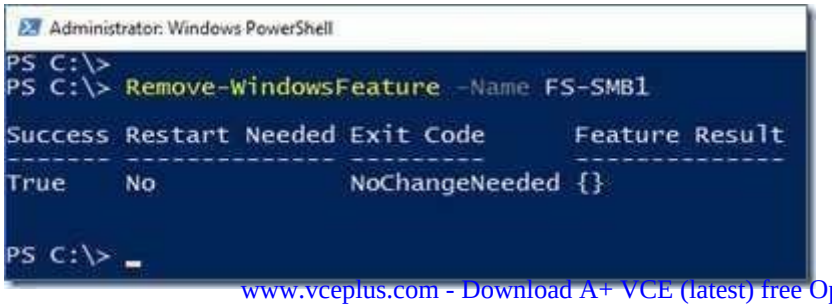
A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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".

QUESTION 46
Your network contains an Active Directory domain named contoso.com.
The domain contains a computer named Computer1 that runs Windows 10.
The network uses the 172.16.0.0/16 address space.
Computer1 has an application named App1.exe that is located in D:\Apps\.
App1.exe is configured to accept connections on TCP port 8080.
You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.
Solution: You configure an inbound rule that allows the TCP protocol on port 8080, uses a scope of 172.16.0.0/16 for local IP addresses, and applies to a private profile.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

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

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

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

QUESTION 47
Your network contains an Active Directory domain named contoso.com.
The domain contains a computer named Computer1 that runs Windows 10.
The network uses the 172.16.0.0/16 address space.
Computer1 has an application named App1.exe that is located in D:\Apps\.
App1.exe is configured to accept connections on TCP port 8080.
You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network. Solution: You configure an inbound rule that allows the TCP protocol on port 8080 and applies to all profiles
Does this meet the goal?

A. Yes
B. No
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
You need to ensure that App1.exe can accept connections **only** when Computer1 is connected to the corporate network."
Therefore, you should not create firewall rule for all three profiles.

QUESTION 48
Your network contains an Active Directory domain named contoso.com. All client computers run Windows 10.
You plan to deploy a Remote Desktop connection solution for the client computers.
You have four available servers in the domain that can be configured as Remote Desktop servers. The servers are configured as shown in the following table.

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

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

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

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

Must allow the client's domain user to access Remote Desktop connections.
Must allow delegation of non-exportable credentials.

QUESTION 49
Your network contains an Active Directory domain named contoso.com. All client computers run Windows 10.
You plan to deploy a Remote Desktop connection solution for the client computers.
You have four available servers in the domain that can be configured as Remote Desktop servers. The servers are configured as shown in the following table.

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

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

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

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

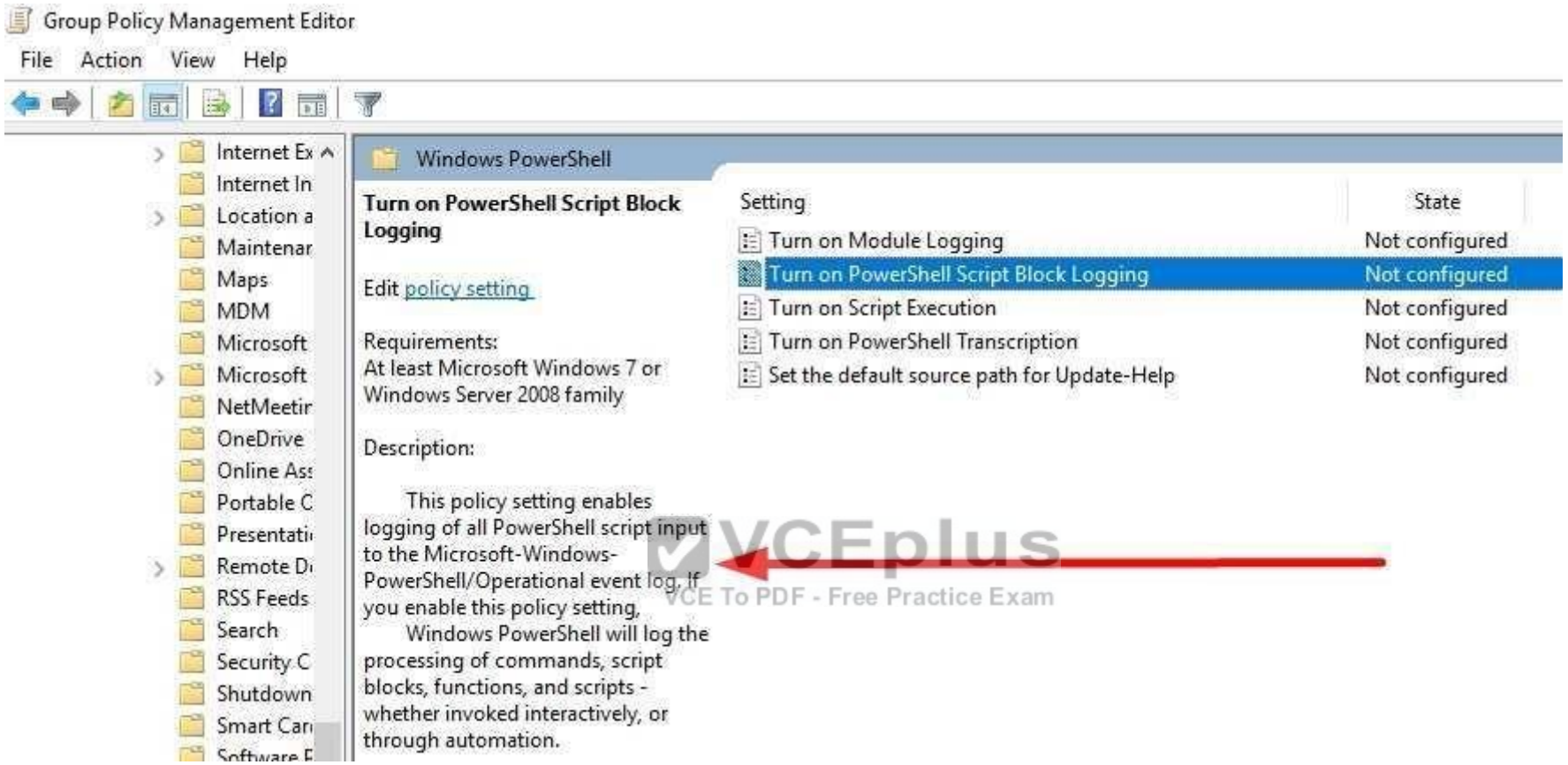
Must allow the client's domain user to access Remote Desktop connections.
Must allow delegation of non-exportable credentials.

QUESTION 50
You enable and configure PowerShell Script Block Logging.
You need to view which script blocks were executed by using Windows PowerShell scripts.
What should you do?

A. View the Microsoft-Windows-PowerShell/Operational event log.
B. Open the log files in %LocalAppData%\Microsoft\Windows\PowerShell.
C. View the Windows PowerShell event log.
D. Open the log files in %SYSTEMROOT%\Logs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit_script
After you enable detailed script tracing, Windows PowerShell logs all script blocks to the event log, **Microsoft-Windows-PowerShell/Operational.**



QUESTION 51
You have a server named Server1 that runs Windows Server 2016.
You configure Just Enough Administration (JEA) on Server1.
You need to view a list of commands that will be available to a user named User1 when User1 establishes a JEA session to Server1.
Which cmdlet should you use?

A. Trace-Command
B. Get-PSSessionCapability
C. Get-PSSessionConfiguration
D. Show-Command

Correct Answer: B
Section: (none)
Explanation

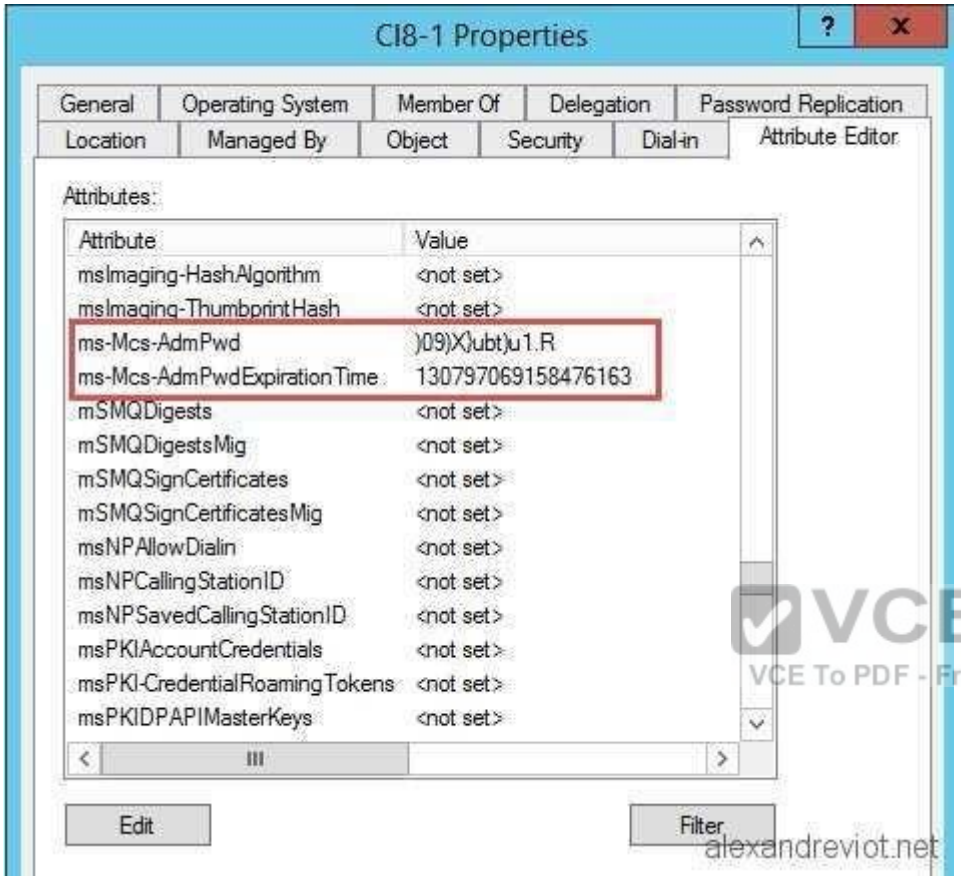
Explanation/Reference:
https://docs.microsoft.com/en-us/powershell/module/Microsoft.PowerShell.Core/get-pssessioncapability?view=powershell-5.0.
The Get-PSSessionCapability cmdlet gets the capabilities of a specific user on a constrained session configuration.
Use this cmdlet to audit customized session configurations for users.
Starting in Windows PowerShell 5.0, you can use the RoleDefinitions property in a session configuration (.pssc) file.
Using this property lets you grant users different capabilities on a single constrained endpoint based on group membership.
The Get-PSSessionCapability cmdlet reduces complexity when auditing these endpoints by letting you determine the exact capabilities granted to a user.
This command is used by I.T. Administrator (The "You" mention in the question) to verify configuration for a User.

QUESTION 52
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 Active Directory Users and Computers, open the properties of Server1 and view the value of the ms-Mcs-AdmPwd attribute.
B. From Active Directory Users and Computers, open the properties of Administrator and view the value of the userPassword attribute.
C. From Windows PovverShell on Server1, run the Get-ADUser cmdlet and specify the -Credential parameter.
D. From Windows PowerShell on Server1, run the Get-ADFineGrainedPasswordPolicy cmdlet and specify the -Credential parameter.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.



QUESTION 53
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1.
On Server1, administrators plan to use several scripts that have the .ps1 extension.
You need to ensure that when code is generated from the scripts, an event containing the details of the code is logged in the Operational log.
Which Group Policy setting or settings should you configure?

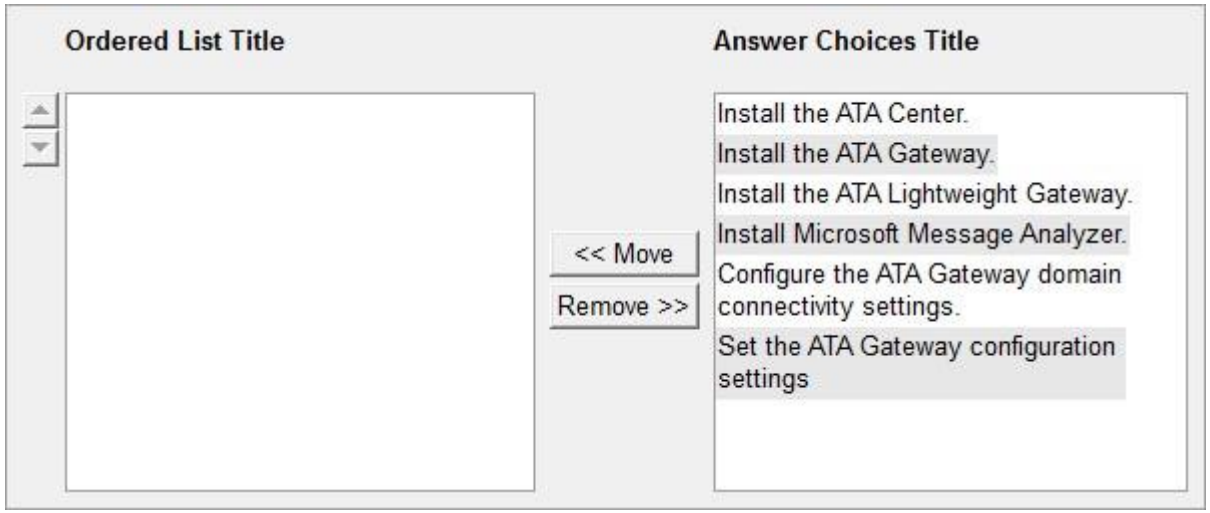
A. Enable Protected Event Logging
B. Audit Process Creation and Audit Process Termination
C. Turn on PovverShell Script Block Logging
D. Turn on PowerShell Transcription

Correct Answer: C
Section: (none)
Explanation

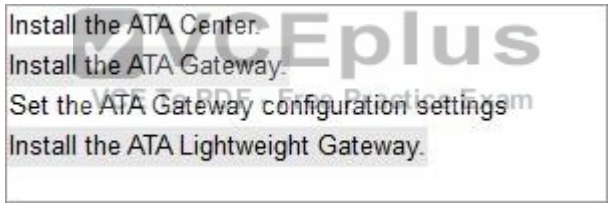
Explanation/Reference:
https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit_script
The new Detailed Script Tracing feature lets you enable detailed tracking and analysis of Windows PowerShell scripting use on a system.
After you enable detailed script tracing, Windows PowerShell logs all script blocks to the ETW event log, Microsoft-Windows-PowerShell/Operational.
If a script block creates another script block (for example, a script that calls the Invoke-Expression cmdlet on a string), that resulting script block is logged as well. Logging of these events can be enabled through the **Turn on PowerShell Script Block Logging Group Policy setting** (in GPO Administrative Templates -> Windows Components -> Windows PowerShell).
Answer D is incorrect, since Transcription (Start-Transcript -path <FilePath>) uses a custom output location instead of Event Viewer \ Operational Log

QUESTION 55
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?

Build List and Reorder:

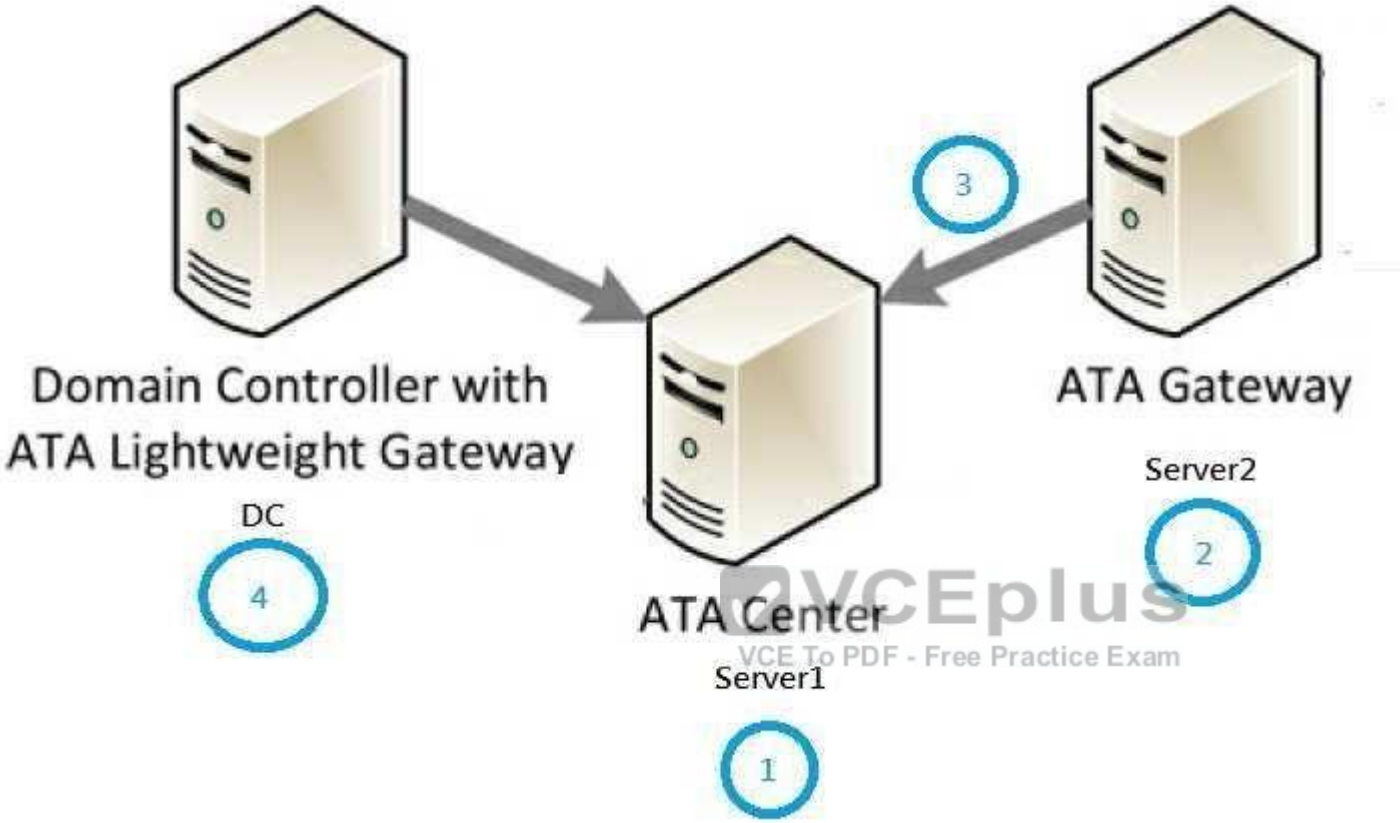


Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
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.



QUESTION 56
Your network contains an Active Directory forest named contoso.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. Add the Microsoft NDIS Capture service to the network adapter of the devices.
E. Install the Simple Network Management Protocol (SNMP) feature on the devices.

Correct Answer: B
Section: (none)
Explanation

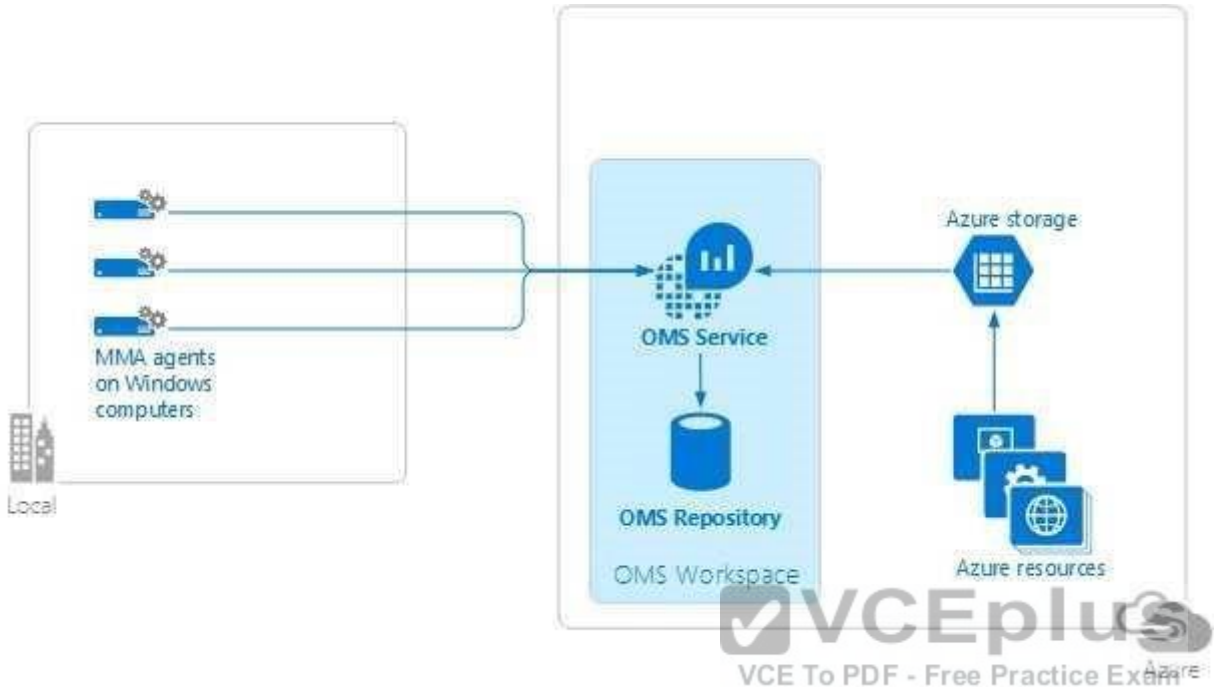
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-oms-gateway
OMS Log Analytics Forwarder = OMS Gateway
If your IT security policies do not allow computers on your network to connect to the Internet, such as point of sale (POS) devices, or servers supporting IT 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.

QUESTION 57
Your network contains an Active Directory domain named contoso.com.
You deploy a server named Server1 that runs Windows Server 2016. Server1 is in a workgroup.
You need to collect the logs from Server1 by using Log Analytics in Microsoft Operations Management Suite (OMS).
What should you do first?

A. Join Server1 to the domain.
B. Create a Data Collector Set.
C. Install Microsoft Monitoring Agent on Server1.
D. Create an event subscription.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-windows-agents
You need to install and connect Microsoft Monitoring Agent for all of the computers that you



You can install the OMS MMA on **stand-alone computers**, servers, and virtual machines.

QUESTION 58
Your network contains an Active Directory domain named contoso.com.
The domain contains 10 computers that are in an organizational unit (OU) named OU1.

You deploy the Local Administrator Password Solution (LAPS) client to the computers.
You link a Group Policy object (GPO) named GPO1 to OU1, and you configure the LAPS password policy settings in GPO1.
You need to ensure that the administrator passwords on the computers in OU1 are managed by using LAPS.
Which two actions should you perform? Each correct answer presents part of the solution.

A. Restart the domain controller that hosts the PDC emulator role.
B. Update the Active Directory Schema.
C. Enable LDAP encryption on the domain controllers.
D. Restart the computers.
E. Modify the permissions on OU1.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
https://blogs.technet.microsoft.com/datacentersecurity/2016/06/06/step-by-step-creating-shielded-vms-without-vmm/
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
```

QUESTION 60
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)

Correct Answer: H
Section: (none)
Explanation

Explanation/Reference:

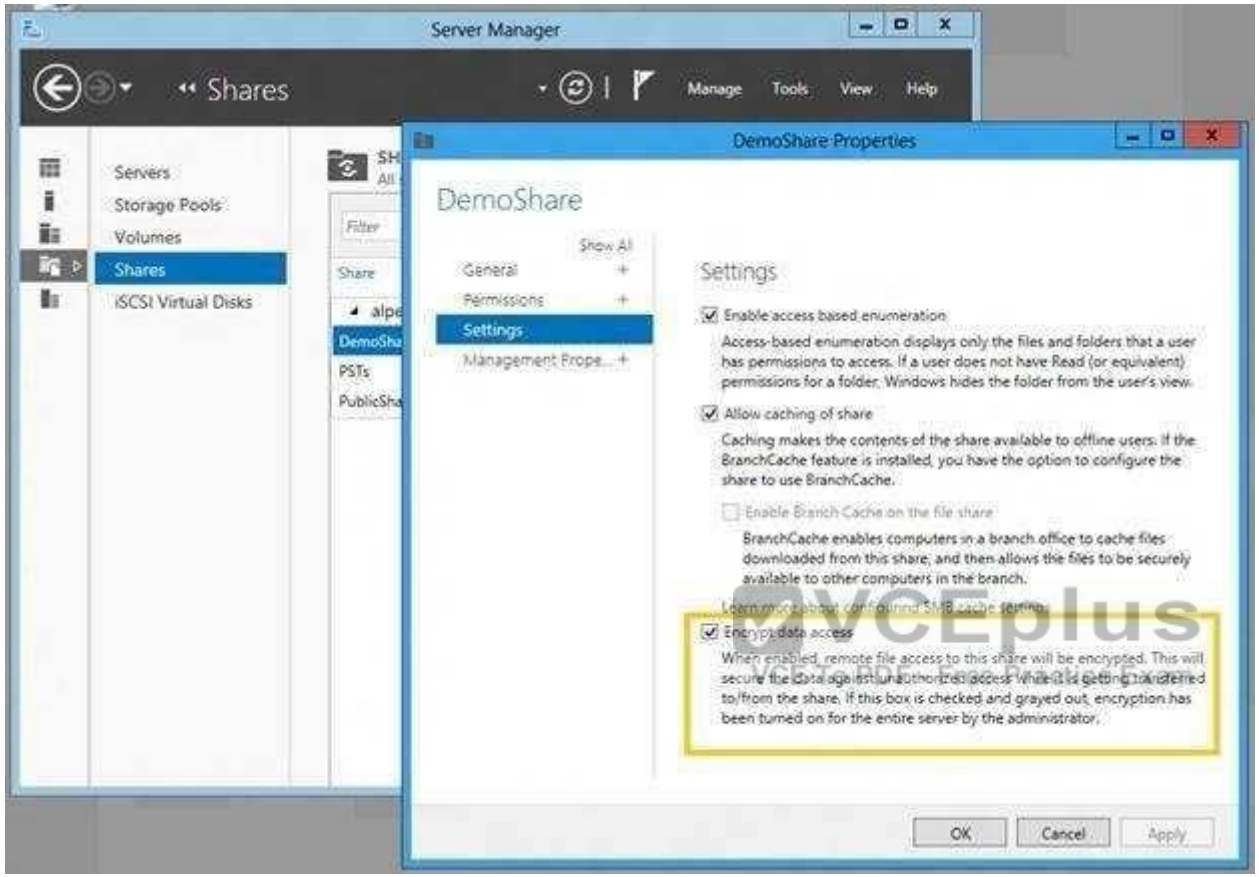
QUESTION 61
Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1 that runs Windows Server 2016. Server1 has a shared folder named Share1.
You need to ensure that all access to Share1 uses SMB Encryption.
Which tool should you use?

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)

Correct Answer: C
Section: (none)
Explanation

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



QUESTION 62
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 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)

Correct Answer: C
Section: (none)
Explanation

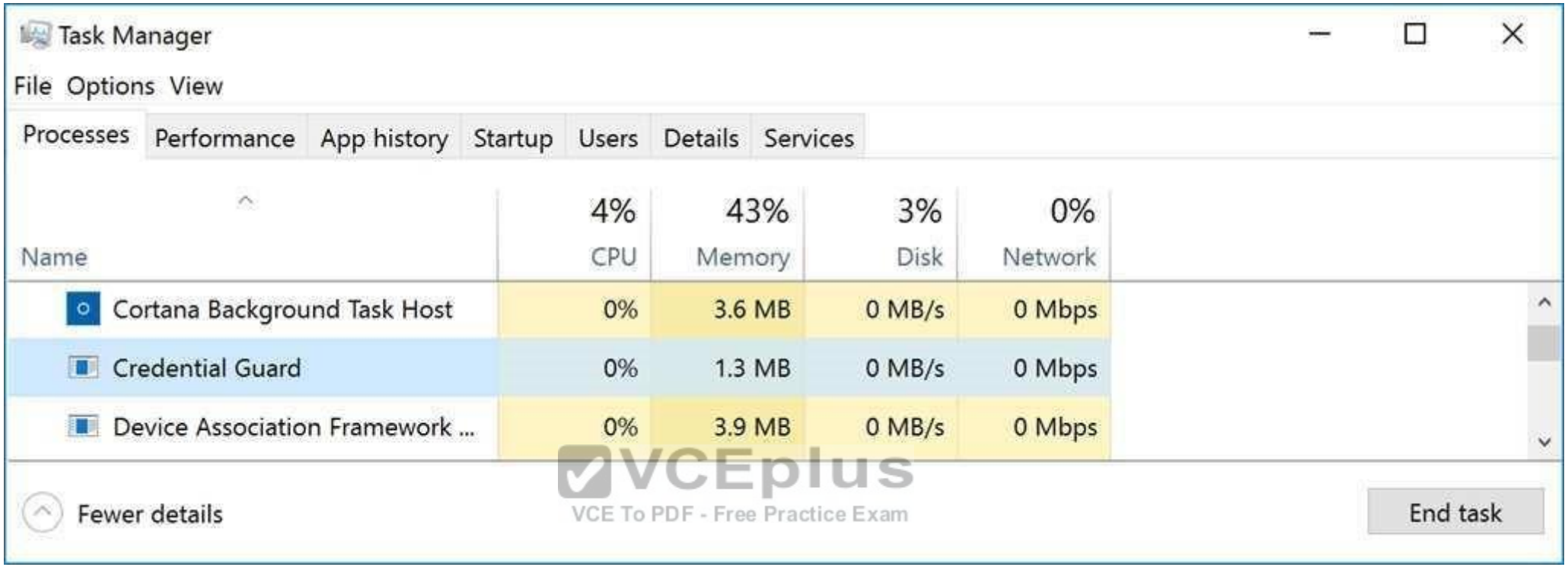
Explanation/Reference:

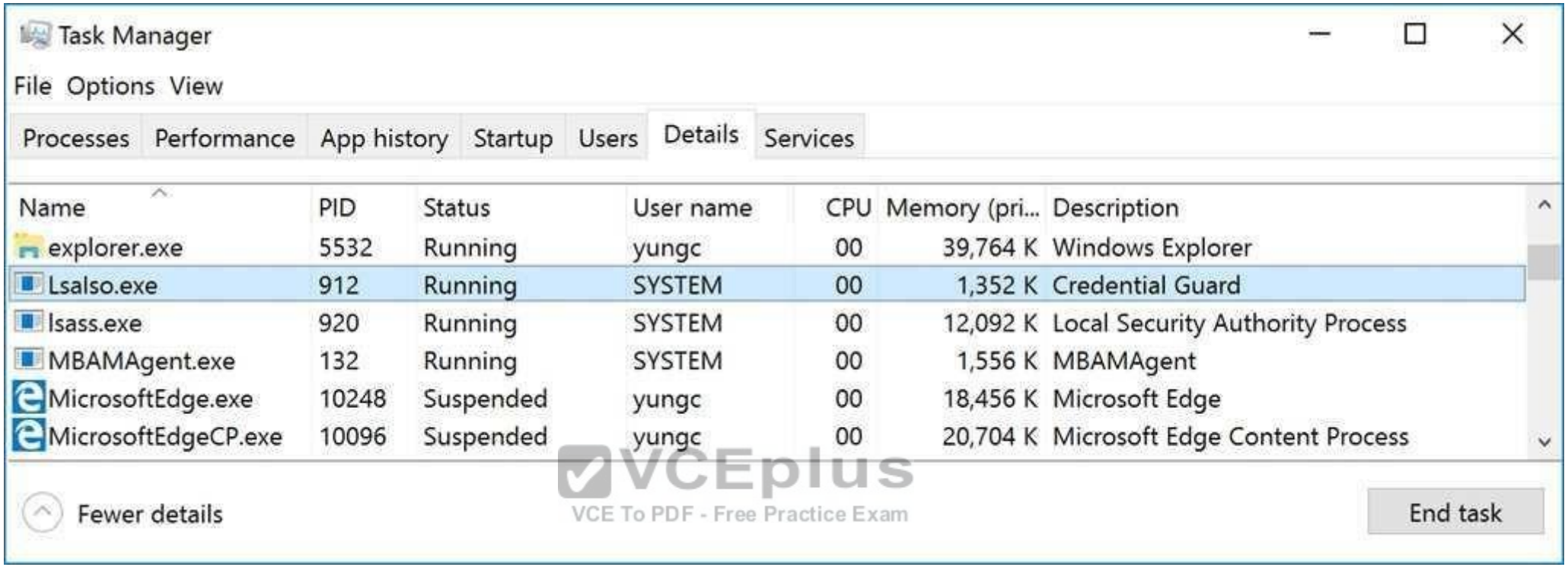
QUESTION 63
Your network contains an Active Directory domain named contoso.com.
The domain contains a server named Server1 that runs Windows Server 2016.
A technician is testing the deployment of Credential Guard on Server1.
You need to verify whether Credential Guard is enabled on Server1. What should you do?

A. From Control Panel, open Credential Manager, and review the list of Windows Credentials.
B. From Task Manager, review the processes listed on the Details tab.
C. From a command prompt, run the tsecimp.exe command.
D. From Server Manager, click Local Server. and review the properties of Server1.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.**





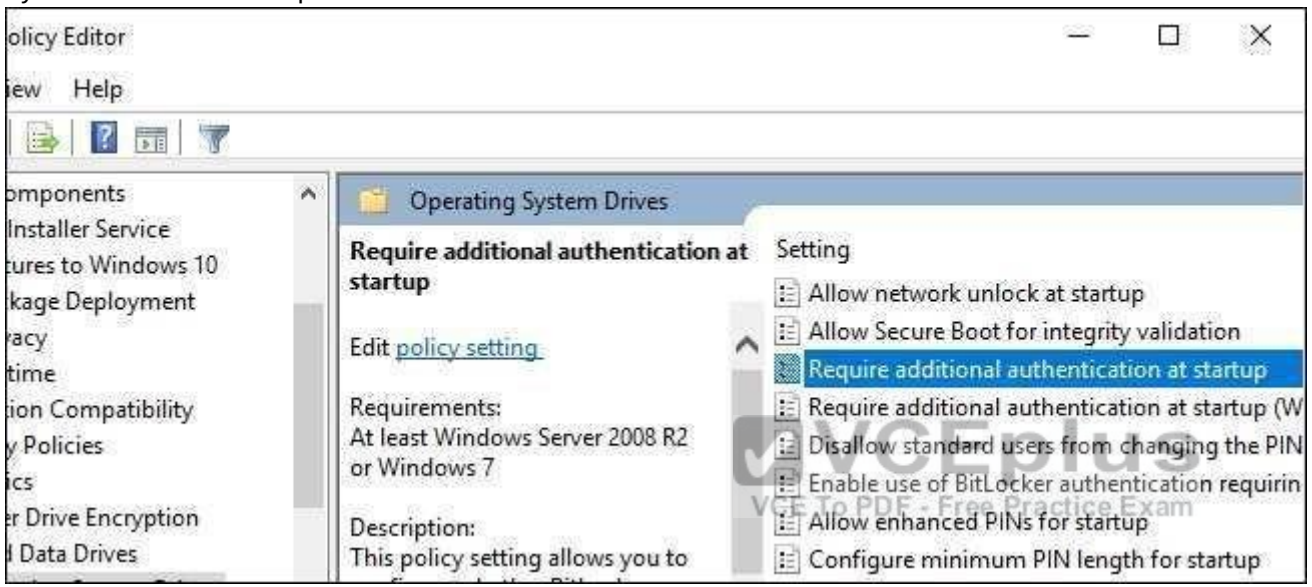
QUESTION 64
You have a Hyper-V host named Server1 that runs Windows Server 2016.
Server1 has a generation 2 virtual machine named VM1 that runs Windows 10.
You need to ensure that you can turn on BitLocker Drive Encryption (BitLocker) for drive C: on VM1. What should you do?

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

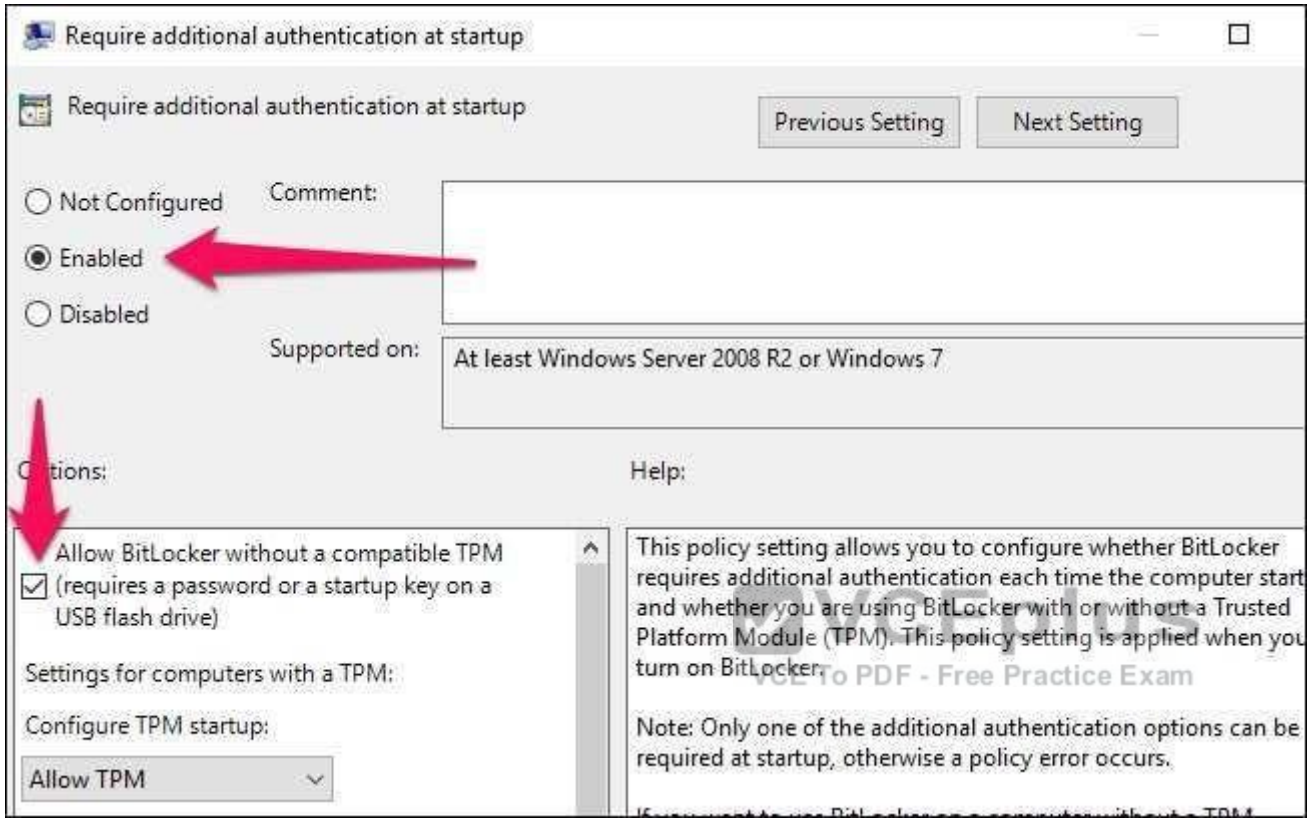
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

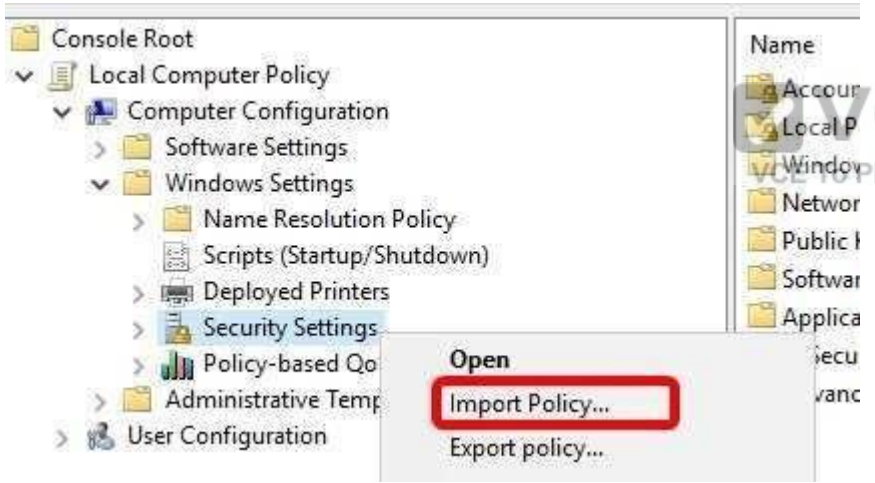
QUESTION 65
Your network contains an internal network and a perimeter network.
The internal network contains an Active Directory forest named contoso.com.
You deploy five servers to the perimeter network.
All of the servers run Windows Server 2016 and are the members of a workgroup.
You need to apply a security baseline named Perimeter.inf to the servers in the perimeter network.

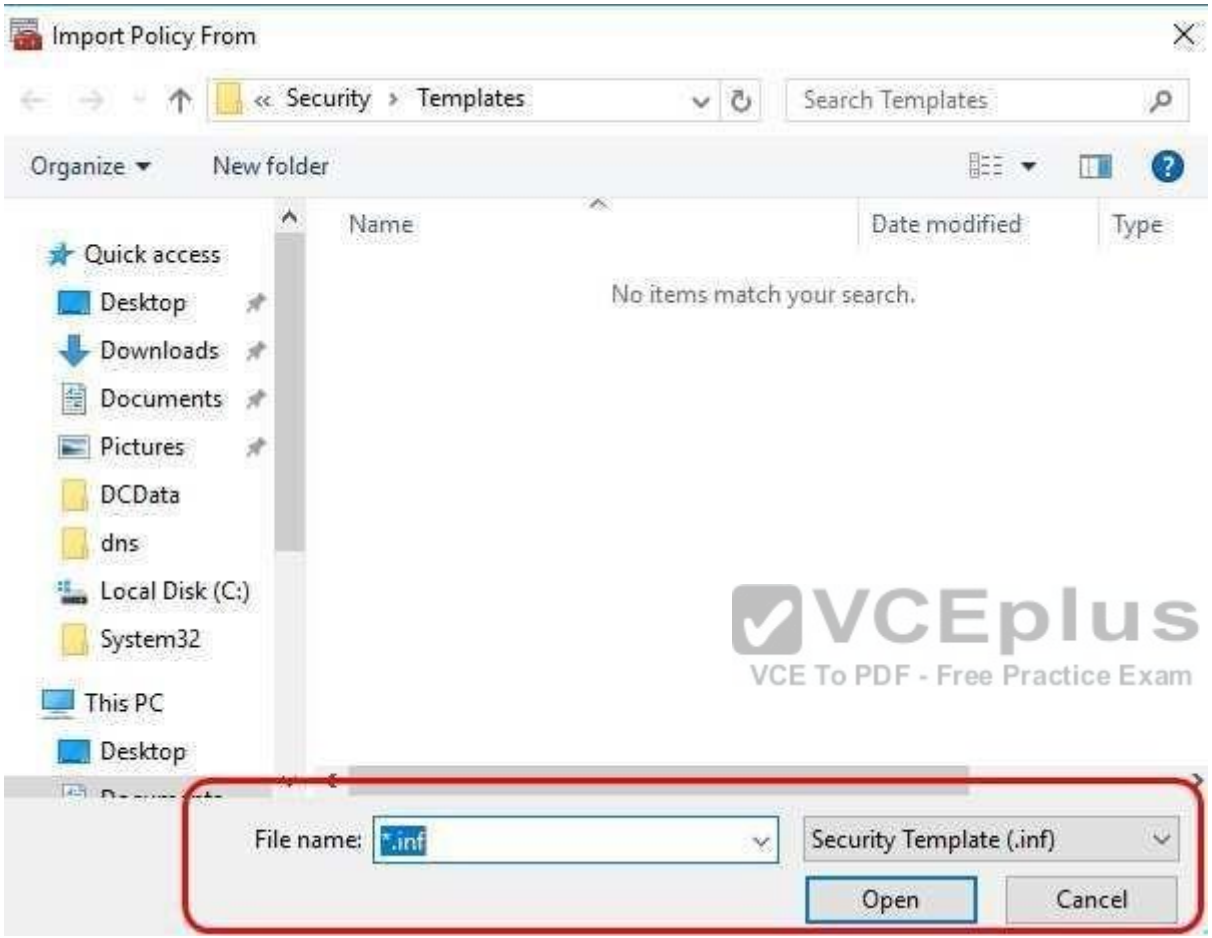
What should you use to apply Perimeter.inf?
A. Local Computer Policy
B. Security Configuration Wizard (SCW)
C. Group Policy Management

D. Server Manager

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
https://docs.microsoft.com/en-us/windows-server/get-started/deprecated-features
The "Security Configuration Wizard (SCW)" is removed since Windows Server 2016, therefore Answer B is incorrect.
The question mentioned that all servers are NOT joint to a domain, therefore, you could not deploy GPO on them, Answer C is incorrect.
Answer D is totally irrelevant.
You can import a .INF file with security settings (exported from another computer) to a Local Computer Policy by using either "GPEdit.msc" the local policy snap in or LGPO.exe
https://blogs.technet.microsoft.com/secguide/2016/01/21/lgpo-exe-local-group-policy-object-utility-v1-0/ https://msdn.microsoft.com/en-us/library/bb742512.aspx





QUESTION 66

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 ensure that you can deploy a shielded virtual machine to Server4. Which server role should you deploy?

A. Network Controller
B. Device Health Attestation
C. Hyper-V
D. Host Guardian Service

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference: https://blogs.technet.microsoft.com/datacentersecurity/2016/06/06/step-by-step-creating-shielded-vms-without-vmm/ Shielding an existing VM
Let's start with the simpler approach. This requires you to have a running VM on a host which is not the guarded host.
This is important to distinguish, because you are simulating the scenario where a tenant wants to take an existing, unprotected VM and shield it before moving it to a guarded host.
For clarity, the host machine which is not the guarded host will be referred as the tenant host below.
A shielded VM can only run on a trusted guarded host.
The trust is established by the adding the Host Guardian Service server role (retrieved from the HGS server) to the Key Protector which is used to shield the VM.
That way, the shielded VM can only be started after the guarded host successfully attest against the HGS server.
In this example, the running VM is named SVM. This VM must be generation 2 and have a supported OS installed with remote desktop enabled.
You should verify the VM can be connected through RDP first, as it will almost certainly be the primary way to access the VM once it is shielded (unless you have installed other remoting capabilities).
QUESTION 67
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-WindowsFeature Microsoft-NanoServer-Guest-Package
K. Install-WindowsFeature Microsoft-NanoServer-Host-Package
L. Install-WindowsFeature Microsoft-NanoServer-ShieldedVM-Package

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 68
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 plan to implement BitLocker Drive Encryption (BitLocker) on the operating system volumes of the application servers.
You need to ensure that the BitLocker recovery keys are stored in Active Directory. Which Group Policy setting should you configure?

A. Store BitLocker recovery information in Active Directory Domain Services (Windows Server 2008 and Windows Vista)
B. Choose how BitLocker-protected operating system drives can be recovered
C. System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing
D. System cryptography: Force strong key protection for user keys stored on the computer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
https://technet.microsoft.com/en-us/library/jj679890%28v=ws.11%29.aspx?f=255&MSPPError=-2147217396#BKMK_rec1

Choose how BitLocker-protected operating system drives can be recovered

This policy setting is used to configure recovery methods for operating system drives.

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

Reference

This policy setting is applied when you turn on BitLocker.

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

For more information about adding data recovery agents, see BitLocker Basic Deployment.

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

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

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

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

QUESTION 69

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 ensure that you can implement the Local Administrator Password Solution (LAPS) for the finance department computers.
What should you do in the contoso.com forest? Choose Two.

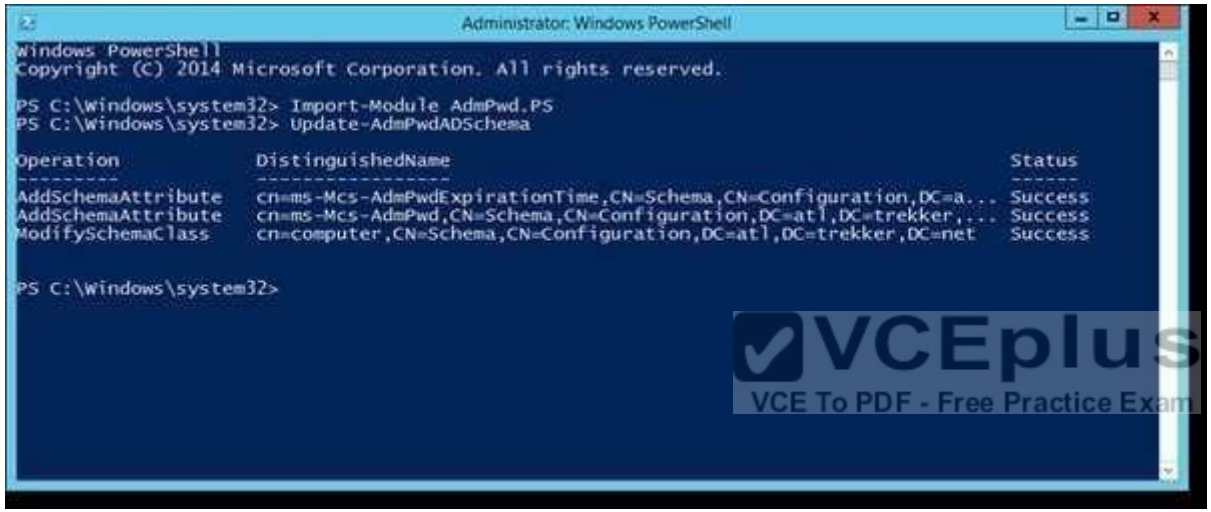
A. Windows PowerShell module to import: AdmPwd.PS
B. Windows PowerShell module to import: Microsoft.WSMAN.Management
C. Windows PowerShell module to import: NetSecurity
D. Windows PowerShell module to import: PSWorkFlow
E. Windows PowerShell cmdlet to use: New-PsWorkflowSession
F. Windows PowerShell cmdlet to use: Save-NetGPO
G. Windows PowerShell cmdlet to use: Set-NetFirewallRule
H. Windows PowerShell cmdlet to use: Update-AdmPwdADSchema

Correct Answer: AH
Section: (none)
Explanation

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

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
```



QUESTION 70

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.

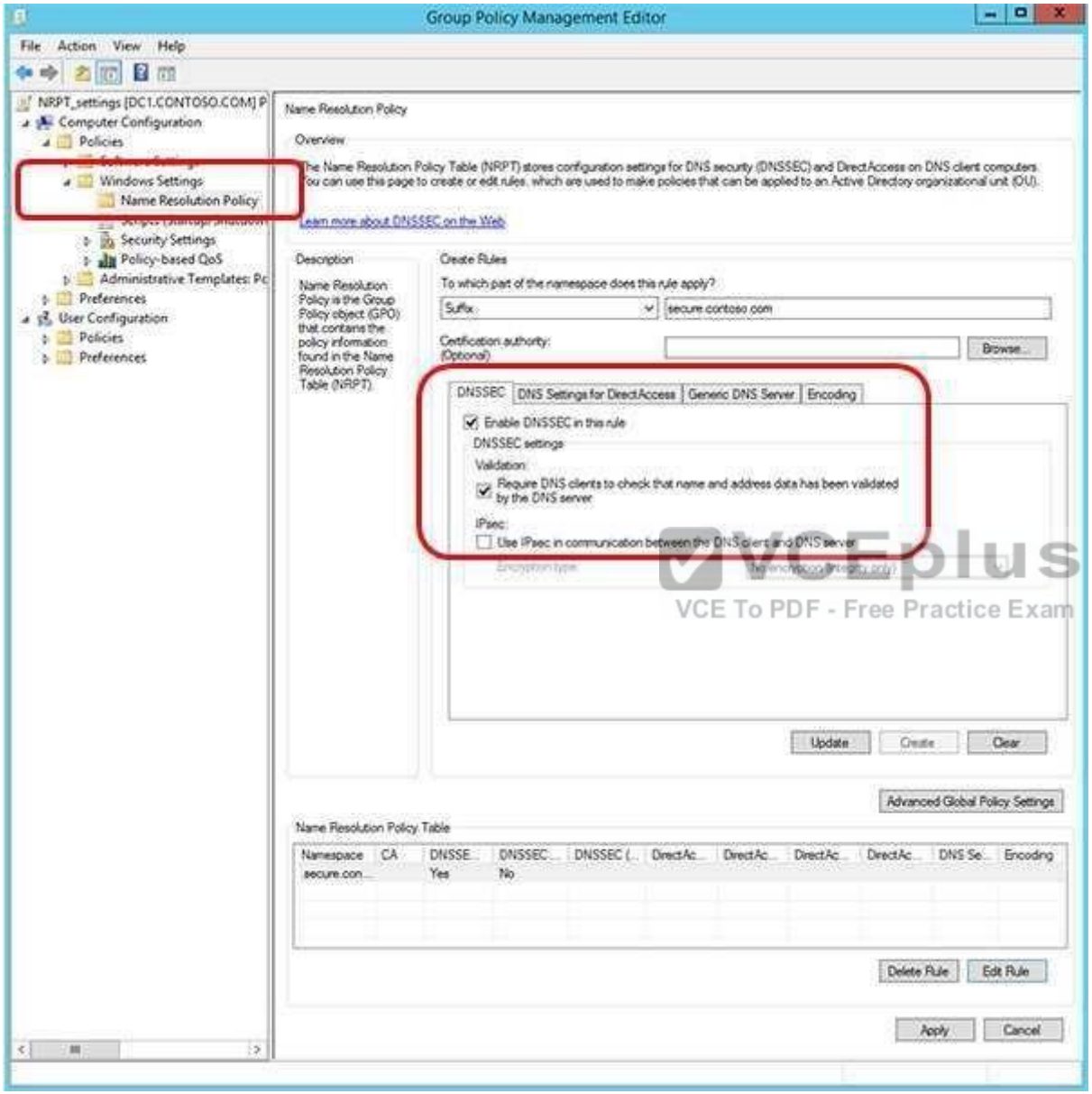
A Group Policy object (GPO) named GP1 is linked to the Marketing OU. A GPO named GP2 is linked to the AppServers OU.

You install Windows Defender on Nano1.
You need to ensure that the marketing department computers validate DNS responses from adatum.com.
Which setting should you configure in the Computer Configuration node of GP1?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
The NRPT is a table that contains rules that you can configure to specify DNS settings or special behavior for names or namespaces.
The NRPT can be configured using the Group Policy Management Editor under Computer Configuration\Policies\Windows Settings\Name Resolution Policy, or with Windows PowerShell.
If a DNS query matches an entry in the NRPT, it is handled according to settings in the policy.
Queries that do not match an NRPT entry are processed normally.
You can use the NRPT to require that DNSSEC validation is performed on DNS responses for queries in the namespaces that you specify.



QUESTION 71

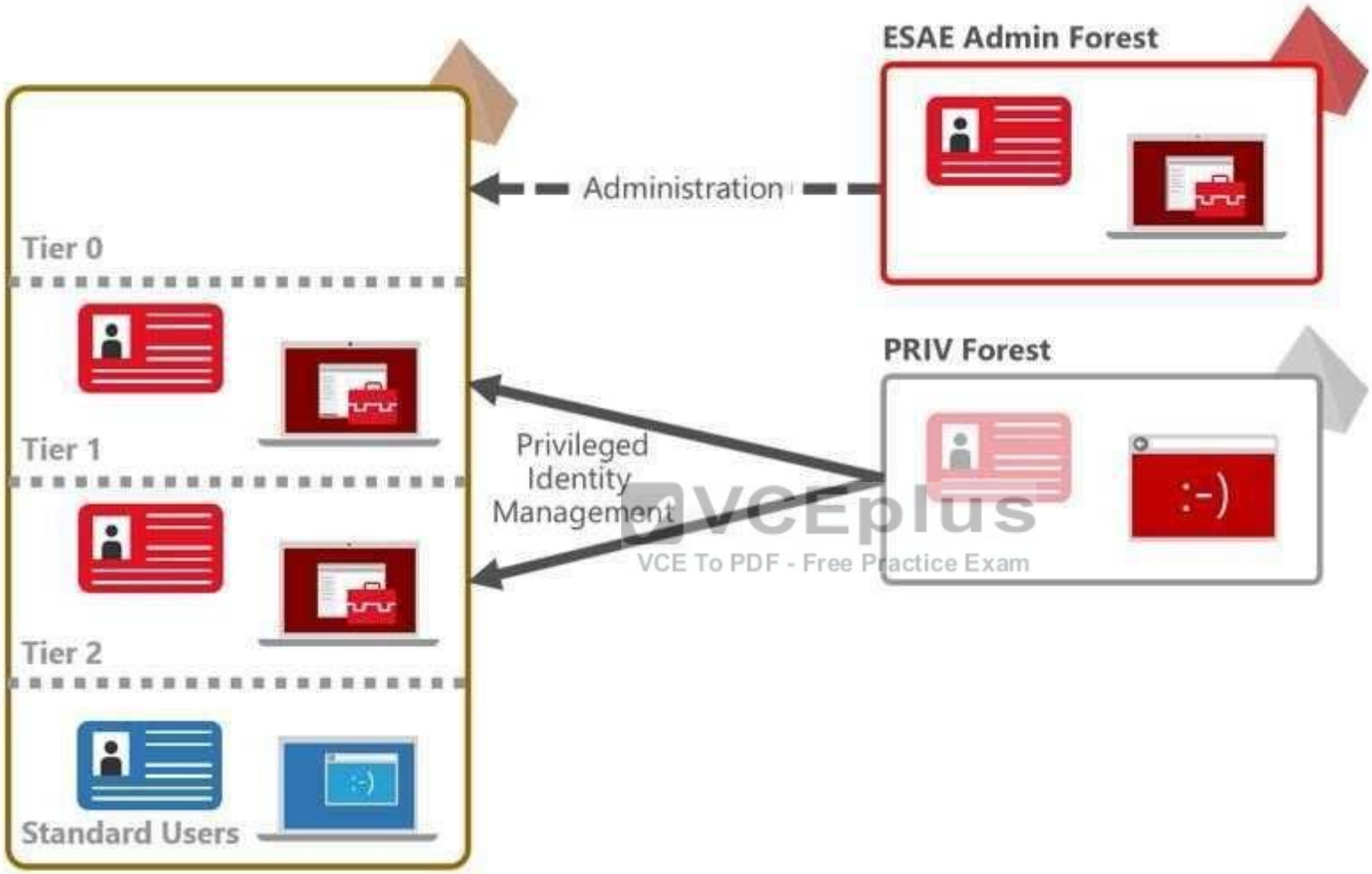
Your network contains an Active Directory domain named contoso.com. The domain contains five servers. All servers run Windows Server 2016. A new security policy states that you must modify the infrastructure to meet the following requirements: -Limit the rights of administrators.
-Minimize the attack surface of the forest
-Support Multi-Factor authentication for administrators

You need to recommend a solution that meets the new security policy requirements. What should you recommend deploying?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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/securing-privileged-access-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.



QUESTION 72
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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-solution-laps-implementation-hints-and-security-nerd-commentaryincludingmini-threat-model/

QUESTION 73
Your network contains an Active Directory domain named contoso.com. The domain contains servers that run Windows Server 2016.
You enable Remote Credential Guard on a server named Server1.
You have an administrative computer named Computer1 that runs Windows 10.
Computer1 is configured to require Remote Credential Guard.
You sign in to Computer1 as Contoso\User1.
You need to establish a Remote Desktop session to Server1 as Contoso\ServerAdmin1.
What should you do first?

A. Install the Universal Windows Platform (UWP) Remote Desktop application
B. Turn on virtualization based security
C. Run the mstsc.exe /remoteGuard
D. Sign in to Computer1 as Contoso\ServerAdmin1

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

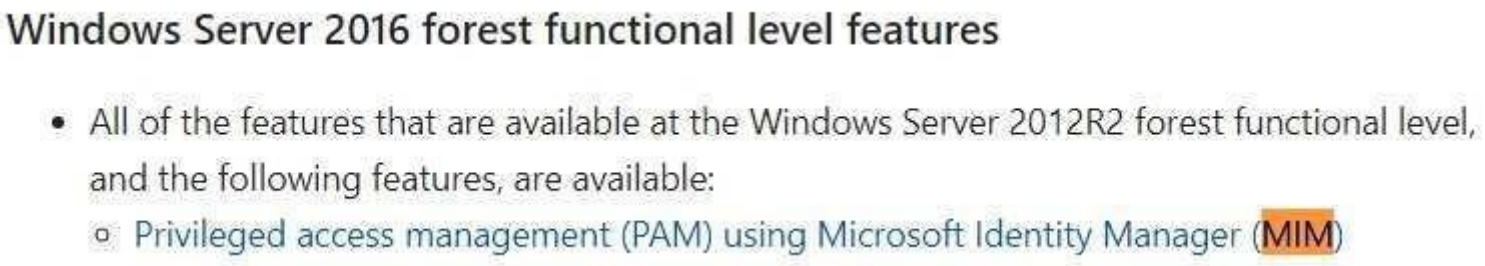
When Computer1 is configured to require Remote Credential Guard, you cannot use NTLM authentication to specify (or impersonate) another user account when connecting to Server1.
Therefore, you have to sign in to Computer1 as "ServerAdmin1" and use Kerberos for authenticating to RDP server "Server1" when Remote Credential Guard is required.

QUESTION 74
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 contoso.com.
B. Deploy Microsoft Identity Management (MIM) 2016 to contoso.com.
C. Configure contoso.com to trust admin.contoso.com.
D. Deploy Microsoft Identify Management (MIM) 2016 to admin.contoso.com.
E. Raise the forest functional level of admin.contoso.com.
F. Configure admin.contoso.com to trust contoso.com.

Correct Answer: DE
Section: (none)
Explanation

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



For the bastion forest which deploys MIM, you should raise the Forest Functional Level to "Windows Server 2016", E is correct.
QUESTION 75
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.
Which of the following PowerShell script should you use?

A. $PAM = Get-PAMRoleForRequest | ? {$_,DisplayName -eq "CorpAdmins" } Set-PAMRequestToApprove -role $PAM
B. $PAM = Get-PAMRoleForRequest | ? {$_,DisplayName -eq "CorpAdmins" } New-PAMRequest -role $PAM
C. $PAM = Get-PAMRoleForRequest | ? {$_,DisplayName -eq "CorpAdmins" } New-PAMRole -role $PAM
D. $PAM = Get-PAMRoleForRequest | ? {$_,DisplayName -eq "CorpAdmins" } Set-PAMUser -role $PAM
E. $PAM = Get-PAMUser | ? {$_,DisplayName -eq "CorpAdmins" } Set-PAMRequestToApprove -role $PAM
F. $PAM = Get-PAMUser | ? {$_,DisplayName -eq "CorpAdmins" } New-PAMRequest -role $PAM
G. $PAM = Get-PAMUser | ? {$_,DisplayName -eq "CorpAdmins" } New-PAMRole -role $PAM
H. $PAM = Get-PAMUser | ? {$_,DisplayName -eq "CorpAdmins" } Set-PAMUser -role $PAM
I. $PAM = New-PAMRequest | ? {$_,DisplayName -eq "CorpAdmins" } Set-PAMRequestToApprove -role $PAM
J. $PAM = New-PAMRequest | ? {$_,DisplayName -eq "CorpAdmins" } New-PAMRequest -role $PAM
K. $PAM = New-PAMRequest | ? {$_,DisplayName -eq "CorpAdmins" } New-PAMRole -role $PAM
L. $PAM = New-PAMRequest | ? {$_,DisplayName -eq "CorpAdmins" } Set-PAMUser -role $PAM
M. $PAM = New-PAMRole | ? {$_,DisplayName -eq "CorpAdmins" } Set-PAMRequestToApprove -role $PAM
N. $PAM = New-PAMRole | ? {$_,DisplayName -eq "CorpAdmins" } New-PAMRequest -role $PAM
O. $PAM = New-PAMRole | ? {$_,DisplayName -eq "CorpAdmins" } New-PAMRole -role $PAM
P. $PAM = New-PAMRole | ? {$_,DisplayName -eq "CorpAdmins" } Set-PAMUser -role $PAM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
https://docs.microsoft.com/en-us/powershell/identitymanager/mimpam/vlatest/get-pamroleforrequest

Example 2: Get a list of roles and select a role by name

PowerShell Copy

```
PS C:\> $Role = Get-PAMRoleForRequest | ? { $_.DisplayName -eq "CorpAdmins" }
```

This command gets the list of roles and selects a role named CorpAdmins. The returned object result can then be provided to the New-PAMRequest cmdlet.

https://docs.microsoft.com/en-us/powershell/identitymanager/mimpam/vlatest/new-pamrequest
The New-PAMRequest cmdlet creates a Privileged Access Management (PAM) activation request in the Microsoft Identity Manager (MIM) Service.

Examples

Example 1: Create a new request for a PAM role

PowerShell Copy

```
PS C:\> New-PAMRequest -role $Role
```

This command creates a new request for a PAM role. The variable Role is assumed to have been set by a previous use of the cmdlet Get-PAMRoleForRequest.

https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/step-7-elevate-user-access

3. When the PowerShell window appears, type the following commands.

Note

After you run these commands, all the following steps are time-sensitive.

Copy

```
Import-module MIMPAM
$r = Get-PAMRoleForRequest | ? { $_.DisplayName -eq "CorpAdmins" }
New-PAMRequest -role $r
klist purge
```


QUESTION 76
Your network contains an Active Directory domain named contoso.com.
The domain contains two global groups named Group1 and Group2. A user named User1 is a member of Group1
You have an organizational unit (OU) named OU1 that contains the computer accounts of computers that contain sensitive data.
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, Domain Admins
Deny log on locally	Contoso\Group2

You need to prevent User1 from signing in to Computer1. What should you do?

A. From Default Domain Policy, modify the Allow log on locally user right
B. On Computer1, modify the Deny log on locally user right.
C. From Default Domain Policy, modify the Deny log on locally user right
D. Remove User1 to Group2.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
https://technet.microsoft.com/en-us/library/cc957048.aspx
"Deny log on locally"
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment
Determines which users are prevented from logging on at the computer.
This policy setting supercedes the Allow Log on locally policy setting if an account is subject to both policies.
Therefore, adding User1 to Group2 will let User1 to inherit both policy, and then prevent User1 to sign in to Computer1.

QUESTION 77
Your network contains an Active Directory forest named contoso.com. The forest contains three domains.
All domain controllers run Windows Server 2016.
You deploy a second Active Directory forest named admin.contoso.com.
The forest contains a domain member server named Server1. Server1 has Microsoft Identity Manager (MIM) 2016 deployed.
You need to implement Privileged Access Management (PAM) and to use admin.contoso.com as an administrative forest.
Which two actions should you perform? Each correct answers presents part of the solution.

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

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:
https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/configuring-mim-environment-for-pam https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/step-5-establish-trust-between-priv-corp-forests

Establish trust on PAMSRV

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

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

Copy

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

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

Copy

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

QUESTION 78

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

The domain contains a computer named Computer1 that runs Windows 10.
Computer1 connects to a home network and a corporate network.
The corporate network uses the 172.16.0.0/24 address space internally.
Computer1 runs an application named App1 that listens to port 8080.
You need to prevent connections to App1 when Computer1 is connected to the home network.
Solution: From Windows Firewall in the Control Panel, you add an application and allow the application to communicate through the firewall on a Private network.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Objective is "PREVENT", solution is "allow"....

QUESTION 79
Your network contains an Active Directory domain named contoso.com.
The domain contains multiple Hyper-V hosts.
You need to deploy several critical line-of-business applications to the network to meet the following requirements:
-The resources of the applications must be isolated from the physical host
-Each application must be prevented from accessing the resources of the other applications.
-The configurations of the applications must be accessible only from the operating system that hosts the application.
Solution: You deploy a separate Windows container for each application. Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
By using Windows Container
-The resources of the applications must be isolated from the physical host (ACHIEVED, as a single container could only access its own resources, but not others)
-Each application must be prevented from accessing the resources of the other applications. (ACHIEVED, as a single container could only access its own resources, but not others)
-The configurations of the applications must be accessible only from the operating system that hosts the application. (ACHIEVED, you can use DockerFile or DockerRun to push configurations to containers from the Container Host OS)

QUESTION 80
Your network contains an Active Directory domain named contoso.com.
The domain contains multiple Hyper-V hosts.
You need to deploy several critical line-of-business applications to the network to meet the following requirements:
-The resources of the applications must be isolated from the physical host
-Each application must be prevented from accessing the resources of the other applications.
-The configurations of the applications must be accessible only from the operating system that hosts the application.
Solution: You deploy one Windows container to all of the applications. Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

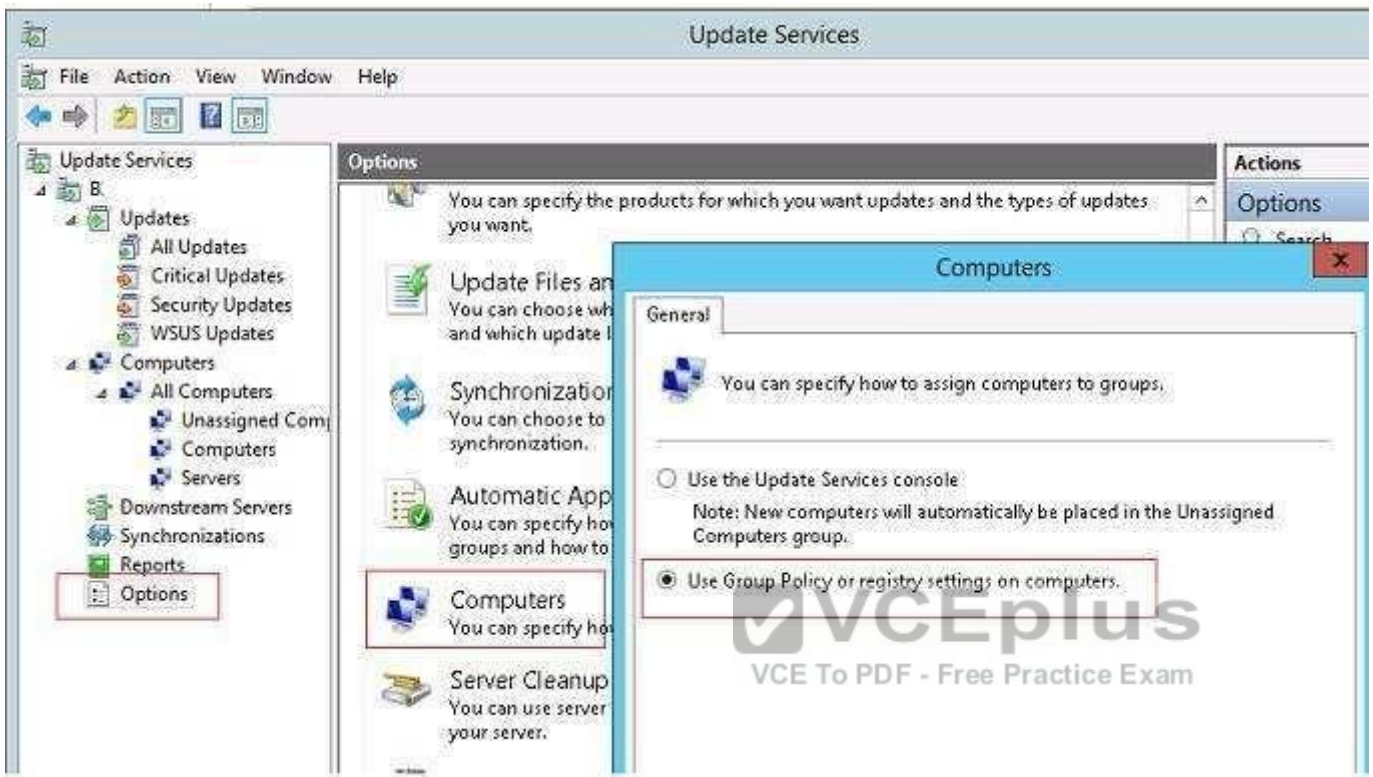
QUESTION 81
Your network contains an Active Directory domain.
The domain contains two organizational units (OUs) named ProdOU and TestOU.
All production servers are in ProdOU. All test servers are in TestOU. A server named Server1 is in TestOU.
You have a Windows Server Update Services (WSUS) server 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 OU.

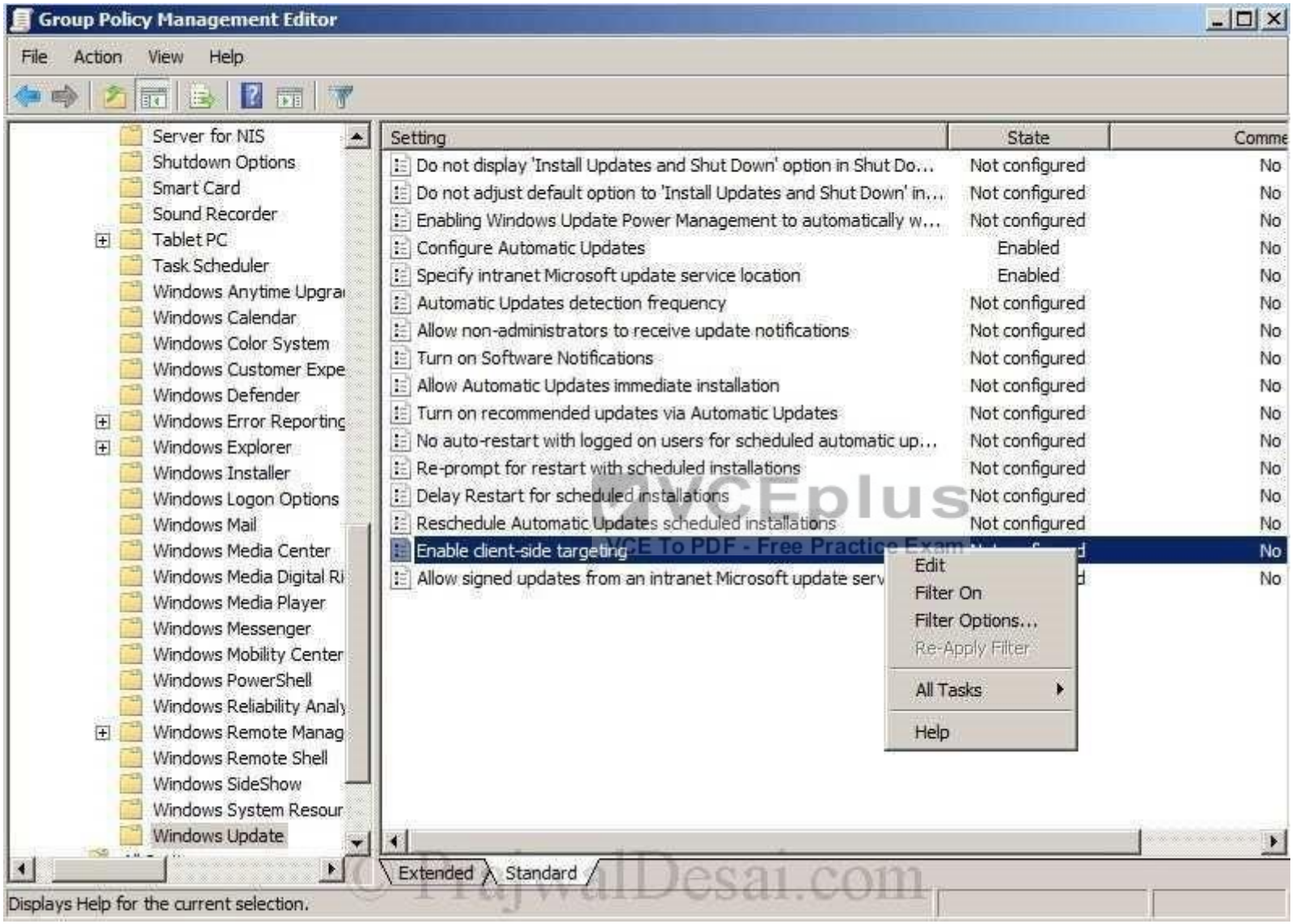
Correct Answer: B
Section: (none)
Explanation

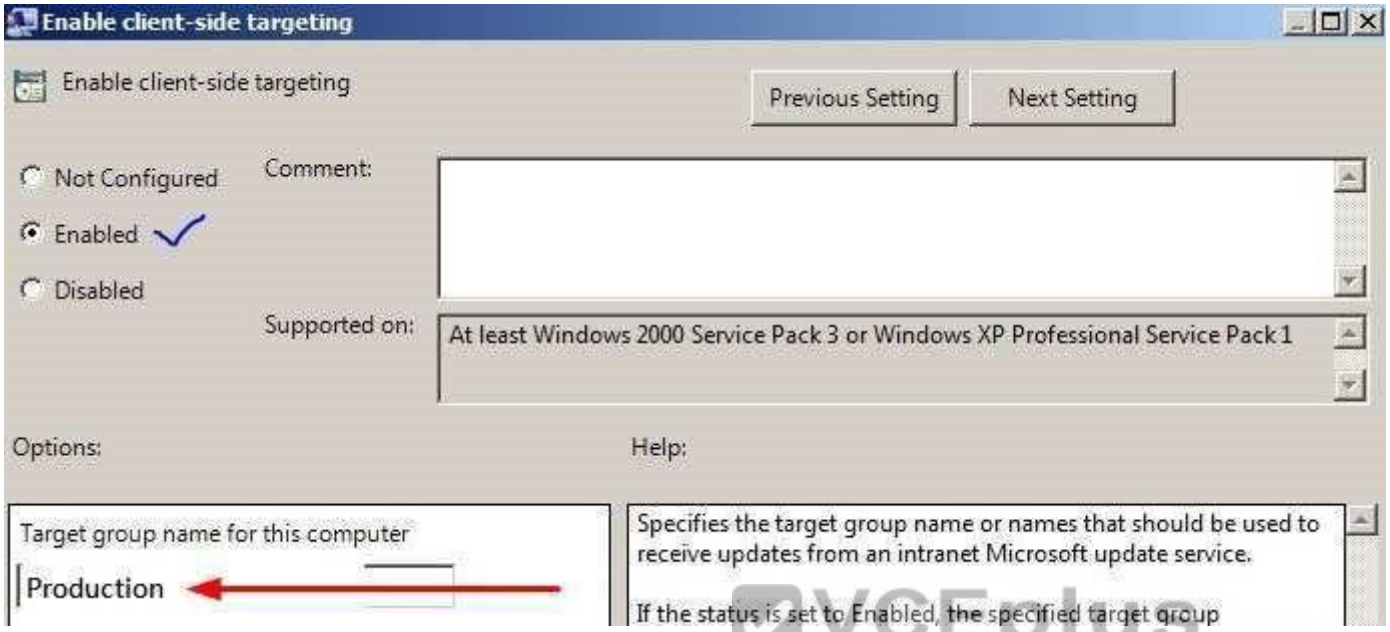
Explanation/Reference:

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





QUESTION 82
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. Run the Save-NetGPO crndlet and specify the -GPOSession parameter
B. Run the secedit.exe command and specify the /export parameter
C. From Group Policy Manager, use the Back up option
D. From Local Group Policy Editor, use the Export policy option

Correct Answer: C
Section: (none)
Explanation

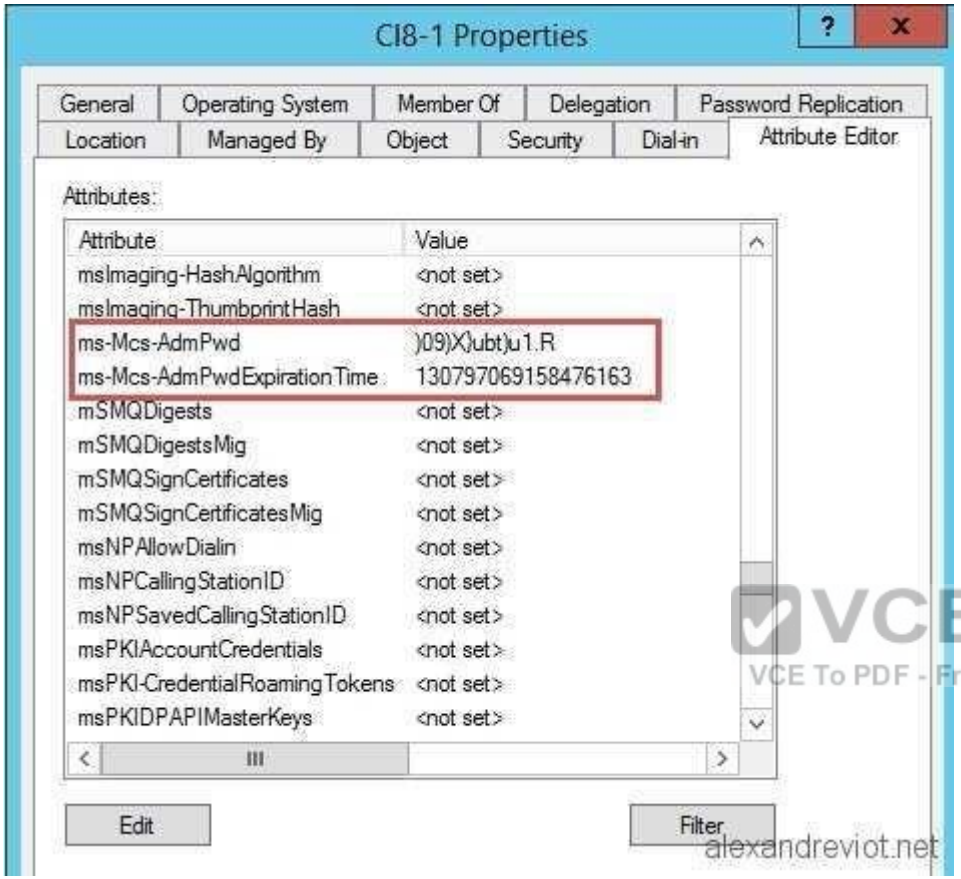
Explanation/Reference:
QUESTION 83
Your network contains an Active Directory domain named contoso.com.
The domain contains a server named Server1 that runs Windows Server 2016.

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 ms-Mcs-AdmPwd attribute
D. From Active Directory Users and Computers, open the properties of Administrator and view the value of the userPassword attribute

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
ms-Mcs-AdmPwd , do you still need explanation!?



QUESTION 84

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

A. Export the baseline as a Group Policy Object (GPO) backup
B. Duplicate a baseline.
C. Modify the settings of a baseline.
D. Import settings into a Group Policy object (GPO)
E. Export the baseline as a Microsoft Excel file
F. Export the baseline as a SCAP file
G. Restore a Group Policy Object (GPO) from a backup

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:
Explanation/Reference:
Correct Order of Actions:1.
Duplicate a baseline.
2. Modify the settings of a baseline.
3. Export the baseline as a Group Policy Object (GPO) backup
4. Import settings into a Group Policy object (GPO)

QUESTION 85
Your network contains an Active Directory domain named contoso.com. The domain contains four servers. The servers are configured as shown in the following table:

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
https://msdn.microsoft.com/en-us/library/dn896648.aspx
The current release of JEA is available on the following platforms: **-**
Windows Server 2016 Technical Preview 5 and higher
-Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2* with **Windows Management Framework 5.0 installed**
FS1 is ready to be managed by JEA, but FS2 need some extra work to do, either upgrade it to Windows Server 2016 or install **Windows Management Framework 5.0 installed, however this choice is not available for this question. So C is correct.**

QUESTION 86
Your network contains an Active Directory domain named contoso.com.
The domain contains a member server named Servers that runs Windows Server 2016.
You need to configure Servers as a Just Enough Administration (JEA) endpoint.
Which two actions should you perform? Each correct answer presents part of the solution.

A. Create and export a Windows PowerShell session.
B. Deploy Microsoft Identity Manager (MIM) 2016
C. Create a maintenance Role Capability file
D. Generate a random Globally Unique Identifier (GUID)
E. Create and register a session configuration file.

Correct Answer: CE
Section: (none)
Explanation

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

QUESTION 87
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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".

QUESTION 88
Your network contains an Active Directory domain named contoso.com. The domain contains 1,000 client computers that run Windows 10.
A security audit reveals that the network recently experienced a Pass-the-Hash attack.
The attack was initiated from a client computer and accessed Active Directory objects restricted to the members of the Domain Admins group.
You need to minimize the impact of another successful Pass-the-Hash attack on the domain. What should you recommend?

A. Move the computer accounts of all the client computers to a new organizational unit (OU). Remove the permissions to the new OU from the Domain Admins group.
B. Configure the Domain Admins group as a restricted group.
C. Instruct all administrators to use a restricted Remote Desktop connection when they sign in to a client computer.
D. Instruct all users to sign in to a client computer by using a Microsoft account

Correct Answer: C
Section: (none)

Explanation

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

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

QUESTION 89
You have a server named Server1 that runs Windows Server 2016. Server1 has the Windows Server Update Services server role installed.
Windows Server Update Services (WSUS) updates for Server1 are stored on a volume named D. The hard disk that contains volume D fails.
You replace the hard disk. You recreate volume D and the WSUS folder hierarchy in the volume.
You need to ensure that the updates listed in the WSUS console are available in the WSUS folder. What should you run?

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

Correct Answer: B
Section: (none)
Explanation

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

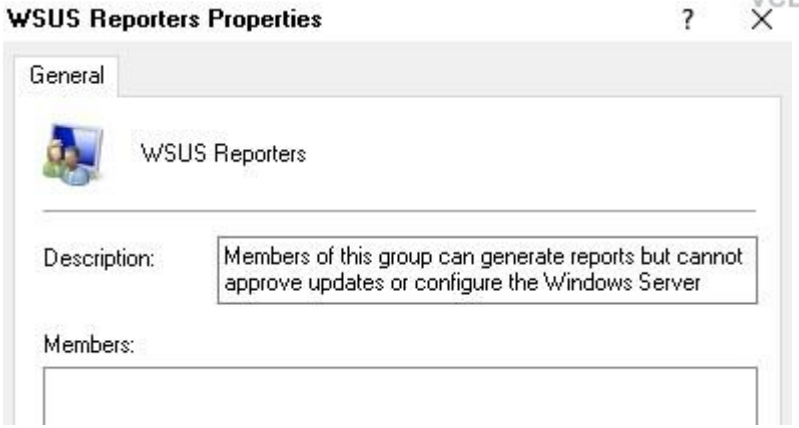
Command	What it enables you to do	When you might use it
export	The first of the two parts that make up the export / import process. The **export** command enables you to export update metadata to an export package file. You cannot use this parameter to export update files, update approvals, or server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

QUESTION 90
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 User1 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?

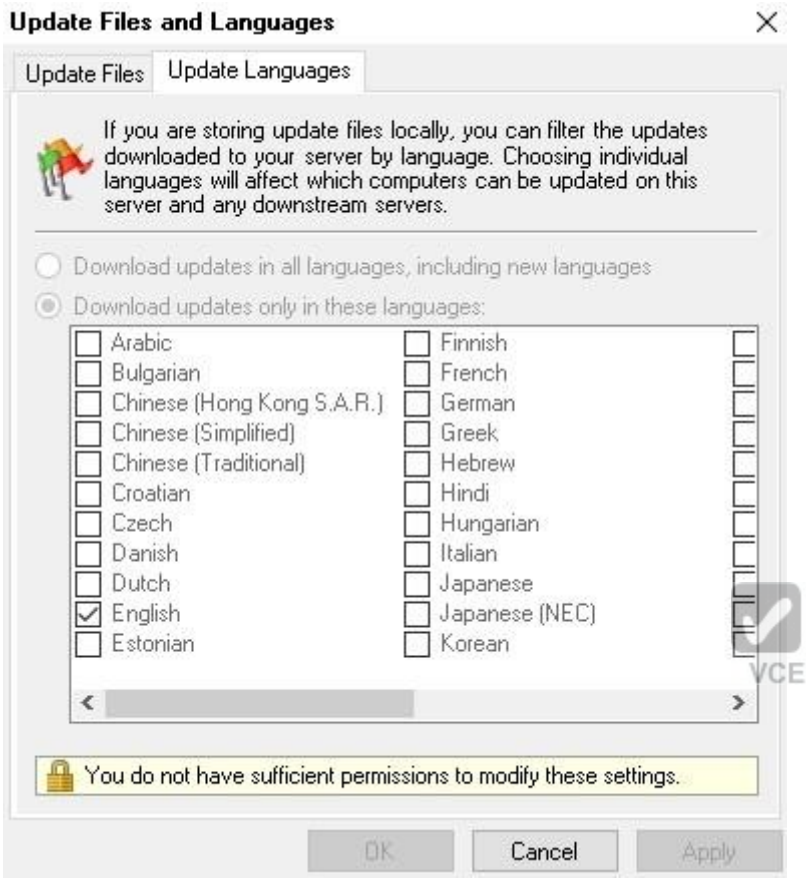
A. Run wsusutil.exe and specify the postinstall parameter.
B. Add User1 to the WSUS Reporters local group
C. Modify the permissions of the ReportWebService virtual folder from the WSUS Administration website.
D. Add User1 to the WSUS Administrators local group.

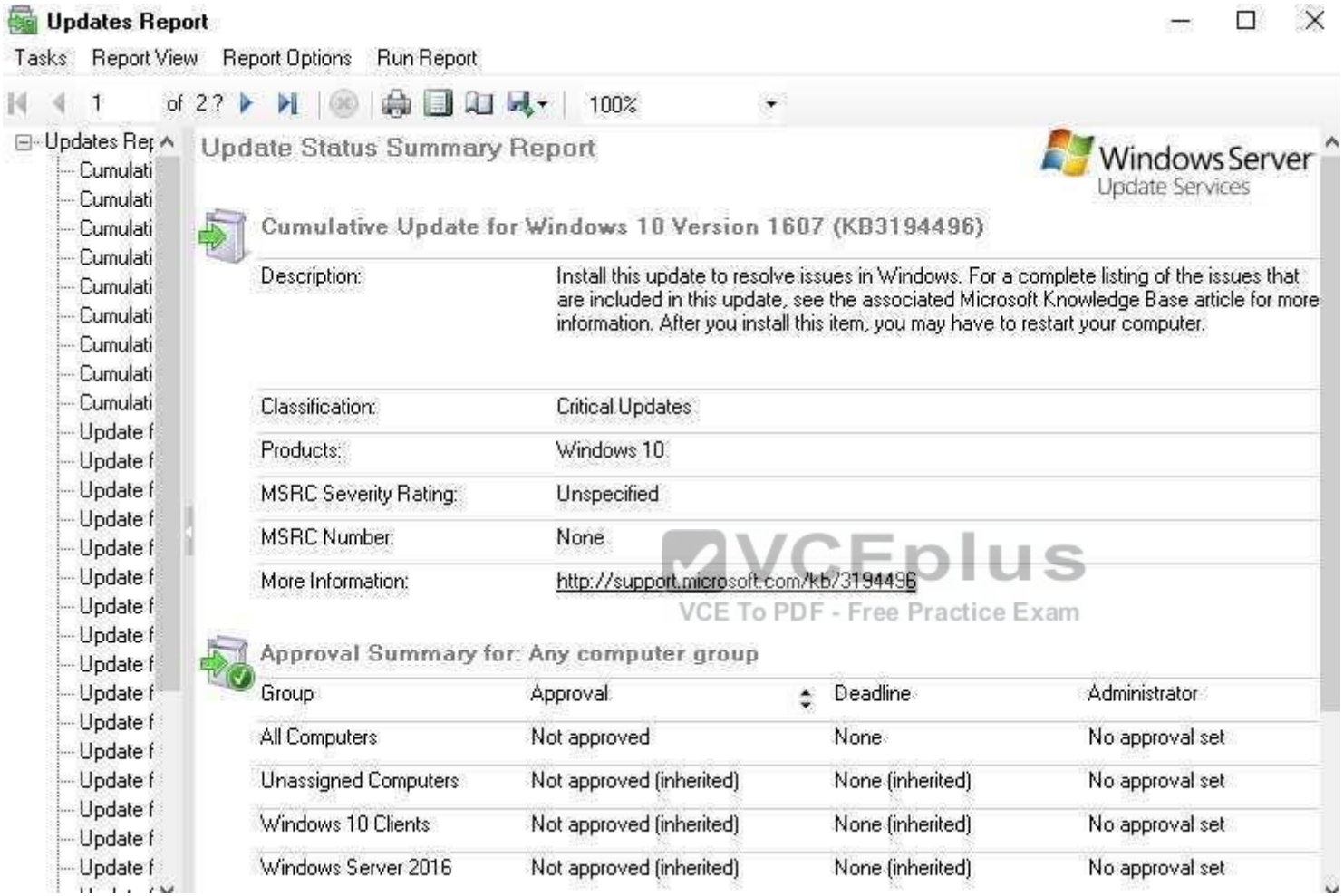
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation/Reference:
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:-





QUESTION 91

Your network contains an Active Directory domain named contoso.com.
The domain contains a server named Server1 that runs Windows Server 2016.
The hardware configuration on Server1 meets the requirements for Credential Guard.
You need to enable Credential Guard on Server. What should you do? Choose Two.

A. Component to install: The Host Guardian Service server role
B. Component to install: The Hyper-V server role
C. Component to install: The VM Shielding Tools for Fabric Management feature
D. Group Policy setting to configure: Access Credential Manager as a trusted provider

E. Group Policy setting to configure: Network Security: Configure encryption types allowed for Kerberos
F. Group Policy setting to configure: Turn on Virtualization Based Security

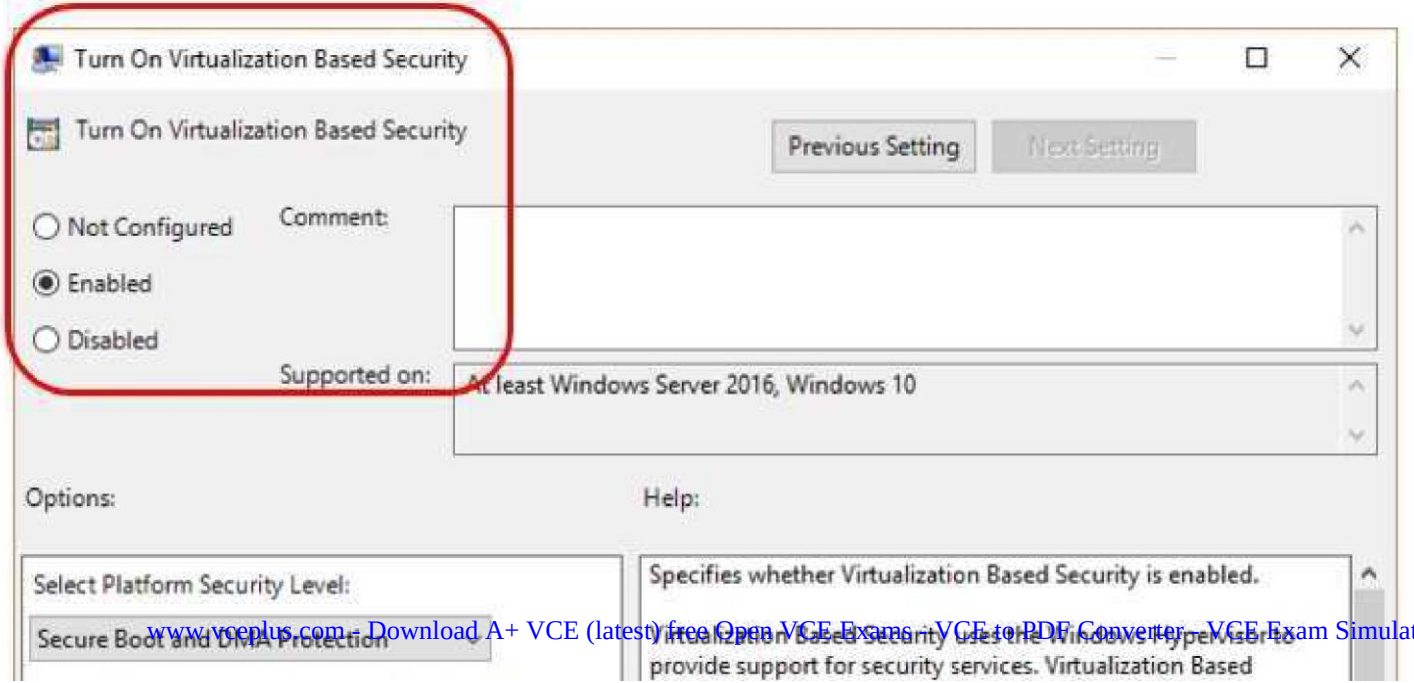
Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:
https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard-requirements
The Virtualization-based security requires:
-64-bit CPU
-CPU virtualization extensions plus extended page tables
-Windows hypervisor
https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard-manage#hardware-readiness-tool

Enable Windows Defender Credential Guard by using Group Policy

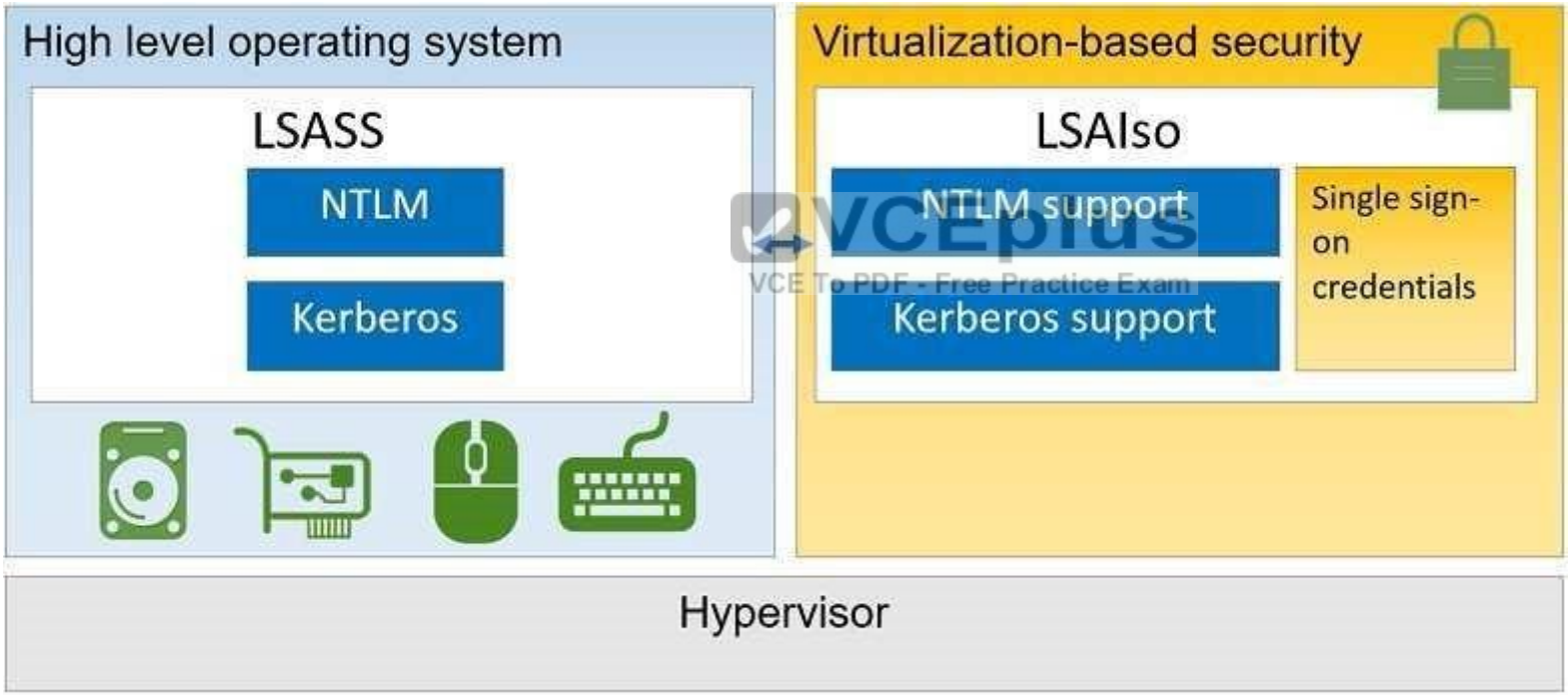
You can use Group Policy to enable Windows Defender Credential Guard. This will add and enable the virtualization-based security features for you if needed.

1. From the Group Policy Management Console, go to **Computer Configuration** -> **Administrative Templates** -> **System** -> **Windows Defender Device Guard**.
2. Double-click **Turn On Virtualization Based Security**, and then click the **Enabled** option.
3. **Select Platform Security Level** box, choose **Secure Boot** or **Secure Boot and DMA Protection**.
4. In the **Windows Defender Credential Guard Configuration** box, click **Enabled with UEFI lock**, and then click **OK**. If you want to be able to turn off Windows Defender Credential Guard remotely, choose **Enabled without lock**.



Add the virtualization-based security features by using Programs and Features

1. Open the Programs and Features control panel.
2. Click **Turn Windows feature on or off**.
3. Go to **Hyper-V** -> **Hyper-V Platform**, and then select the **Hyper-V Hypervisor** check box.
4. Select the **Isolated User Mode** check box at the top level of the feature selection.
5. Click **OK**.

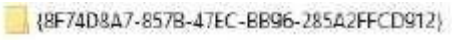


QUESTION 92
Your network contains an Active Directory domain named contoso.com.
You have an organizational unit (OU) named Secure that contains all servers.
You install Microsoft Security Compliance Manager (SCM) 4.0 on a server named Server1.
You need to export the SCM Print Server Security baseline and to deploy the baseline to a server named Server2.
What should you do? Choose Two.

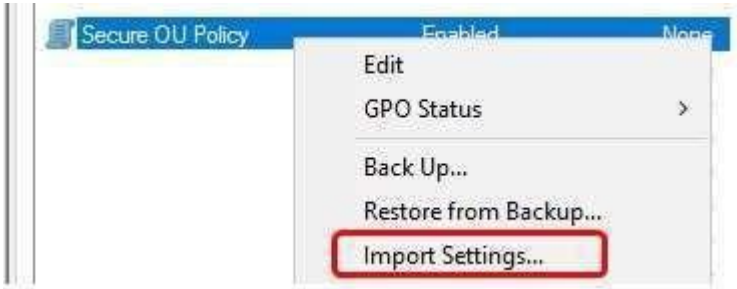
A. Format to use to export the baseline: Excel (.xlsm)
B. Format to use to export the baseline: GPO Backup (folder)
C. Format to use to export the baseline: SCAP v1.0 (.cap)
D. Format to use to export the baseline: SCCM DCM 2007 (.cab)
E. Format to use to export the baseline: SCM (.cab)
F. Tool to use to import the baseline: Group Policy Management
G. Tool to use to import the baseline: Group Policy Object Editor
H. Tool to use to import the baseline: Microsoft Security Compliance Manager (SCM)
I. Tool to use to import the baseline: Resultant Set of Policy
J. Tool to use to import the baseline: Security Configuration and Analysis

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:
When the security settings is exported from SCM 4 in a GPO (folder) format, with a long GUID name



You have to import it to GPO by using "Group Policy Management", right-click the GPO and use "Import Settings" button. F is correct.



Do not confuse with security template .inf files. **Only security template .INF file (which is a single file, not a folder) could be imported to a GPO by Group Policy Object Editor**, so G is incorrect.

QUESTION 93
You plan to enable Credential Guard on four servers. Credential Guard secrets will be bound to the TPM.
The servers run Windows Server 2016 and are configured as shown in the following table

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

Which of the above server you could enable Credential Guard?

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

Correct Answer: D
Section: (none)
Explanation

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

Baseline protections

Baseline Protections	Description	Security benefits
Hardware: **64-bit CPU**	A 64-bit computer is required for the Windows hypervisor to provide VBS.	
Hardware: **CPU virtualization extensions**, plus **extended page tables**	**Requirements**: These hardware features are required for VBS: One of the following virtualization extensions: • VT-x (Intel) or • AMD-V And: • Extended page tables, also called Second Level Address Translation (SLAT).	VBS provides isolation of secure kernel from normal operating system. Vulnerabilities and Day 0s in normal operating system cannot be exploited because of this isolation.
Hardware: **Trusted Platform Module (TPM)**	**Requirement**: TPM 1.2 or TPM 2.0, either discrete or firmware. TPM recommendations	A TPM provides protection for VBS encryption keys that are stored in the firmware. This helps protect against attacks involving a physically present user with BIOS access.
Firmware: **UEFI firmware version 2.3.1.c or higher with UEFI Secure Boot**	**Requirements**: See the following Windows Hardware Compatibility Program requirement: System.Fundamentals.Firmware.UEFISecureBoot	UEFI Secure Boot helps ensure that the device boots only authorized code. This can prevent boot kits and root kits from installing and persisting across reboots.

Background: UEFI 2.3.1 is older that UEFI 2.3.1c
http://www.uefi.org/specifications

UEFI Specification

- UEFI Specification Version 2.7

Previous Versions of the UEFI Specification:

- UEFI Specification Version 2.6 (Errata B)
- UEFI Specification Version 2.6 (Errata A)
- UEFI Specification Version 2.6
- UEFI Specification Version 2.5 (Errata A)
- UEFI Specification Version 2.5
- UEFI Specification Version 2.5 Related Links
- UEFI Specification Version 2.4 (Errata C)
- UEFI Specification Version 2.4 (Errata B)
- UEFI Specification Version 2.4 (Errata A)
- UEFI Specification Version 2.4
- UEFI Specification Version 2.3.1 (Errata D)
- UEFI Specification Version 2.3.1 (Errata C)
- UEFI Specification Version 2.3.1 (Errata B)
- UEFI Specification Version 2.3.1 (Errata A)
- UEFI Specification Version 2.3.1
- UEFI Specification Version 2.3 (Errata E)
- UEFI Specification Version 2.3 (Errata D)
- UEFI Specification Version 2.2 (Errata D)
- UEFI Specification Version 2.1 (Errata D)
- UEFI Specification Version 2.0

When applying these above requirements to Server1, Server2 and Server3,
Server2 is eliminated due to UEFI version is lower than the required 2.3.1c.
Server3 is eliminated due to Hyper-V role is not installed.
Use the following to verify if Server4 virtual machine is eligible for running Credential Guard
Server4

Windows Defender Credential Guard deployment in virtual machines

Credential Guard can protect secrets in a Hyper-V virtual machine, just as it would on a physical machine. When Credential Guard is deployed on a VM, secrets are protected from attacks inside the VM. Credential Guard does not provide additional protection from privileged system attacks originating from the host.

Requirements for running Windows Defender Credential Guard in Hyper-V virtual machines

- The Hyper-V host must have an IOMMU, and run at least Windows Server 2016 or Windows 10 version 1607.
- The Hyper-V virtual machine must be Generation 2, have an enabled virtual TPM, and be running at least Windows Server 2016 or Windows 10.

Server4 looks good and could enable Credential Guard.
So, we have to made a choice between Server1 (A) and Server4-virtual machine (D).
Server4 is a better choice while it uses a newer TPM version 2.0, so D is correct answer for this question as Server4 has no uncertainties.
There are documented uncertainties of Server1 using TPM 1.2, there are possibilities and reasonable doubt that Server1 could not bound Credential Guard secrets to TPM1.2, see below:-
https://docs.microsoft.com/en-us/windows/device-security/tpm/tpm-recommendations

TPM 1.2 vs. 2.0 comparison

From an industry standard, Microsoft has been an industry leader in moving and standardizing on TPM 2.0, which has many key realized benefits across algorithms, crypto, hierarchy, root keys, authorization and NV RAM.

Why TPM 2.0?

TPM 2.0 products and systems have important security advantages over TPM 1.2, including:

- The TPM 1.2 spec only allows for the use of RSA and the SHA-1 hashing algorithm.
- For security reasons, some entities are moving away from SHA-1. Notably, NIST has required many federal agencies to move to SHA-256 as of 2014, and technology leaders, including Microsoft and Google have announced they will remove support for SHA-1 based signing or certificates in 2017.
- TPM 2.0 **enables greater crypto agility** by being more flexible with respect to cryptographic algorithms.
    - TPM 2.0 supports newer algorithms, which can improve drive signing and key generation performance. For the full list of supported algorithms, see the TCG Algorithm Registry. Some TPMs do not support all algorithms.
    - For the list of algorithms that Windows supports in the platform cryptographic storage provider, see CNG Cryptographic Algorithm Providers.
    - TPM 2.0 achieved ISO standardization (ISO/IEC 11889:2015).
    - Use of TPM 2.0 may help eliminate the need for OEMs to make exception to standard

Via lab test, we are unable to bound Credential Guard credentials on an old computer with TPM 1.2 purchased near 8 years ago. So, Server1 (A) is wrong.

QUESTION 94

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

The domain contains a server named Server1 that runs Windows Server 2016.

The services on Server1 are shown in the following output:

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

Server1 has AppLocker rules configured as shown in follow:

Rule1 and Rule2 are configured as shown in follow:

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

Which of the following statements are true? Choose Three.

A. On Server1, User1 can run D:\Folder2\App1.exe : Yes
B. On Server1, User1 can run D:\Folder2\App1.exe : No
C. On Server1, User1 can run D:\Folder1\Program1.exe : Yes
D. On Server1, User1 can run D:\Folder1\Program1.exe : No
E. If Program1 is copied from D:\Folder1 to D:\Folder2, User1 can run Program1.exe on Server1 : Yes
F. If Program1 is copied from D:\Folder1 to D:\Folder2, User1 can run Program1.exe on Server1 : No

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
Explanation/Reference:
https://docs.microsoft.com/en-us/windows/device-security/applocker/configure-the-application-identity-service
The Application Identity service determines and verifies the identity of an app. **Stopping this service will prevent AppLocker policies from being enforced.**
In this question, Server1's Application Identity service is stopped, therefore, no more enforcement on AppLocker rules, everyone could run everything on Server1.

QUESTION 95
Your network contains several Windows container hosts..
You plan to deploy three custom .NET applications.
You need to recommend a deployment solution for the applications.
Each application must:
-be accessible by using a different IP address.
-have access to a unique file system.
-start as quickly as possible.
What should you recommend? Choose Two.

A. Type of container: Hyper-V
B. Type of container: Windows
C. Number of containers: 1D. Number of containers: 2
E. Number of containers: 3

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Both Hyper-V container and Windows container could achieve, you'll need 3 containers to do so. Answer E is correct. -
be accessible by using a different IP address.
-have access to a unique file system.
However, Hyper-V container starts 5 times or more slower than Windows container in our lab, on same computer.
The question demands that each application must "start as quickly as possible.", therefore Answer B is correct
QUESTION 96
You plan to deploy three encrypted virtual machines that use Secure Boot. The virtual machines will be configured as shown in the following table:
How should you protect each virtual machine? Choose Three.

A. VM1: An encryption-supported virtual machine B.
VM1: A shielded virtual machine

Virtual machine name	Operating system	Requirement
VM1	Windows Server 2016	Prevent console connections that use Virtual Machine Connection.
VM2	Windows Server 2012 R2	Support administration by using PowerShell Direct.
VM3	Windows Server 2016	Support file transfers by using the Data Exchange integration service.

C. VM2: An encryption-supported virtual machine
D. VM2: A shielded virtual machine
E. VM3: An encryption-supported virtual machine
F. VM3: A shielded virtual machine

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Shielded VM Prevents Virtual Machine connection and PowerShell Direct, it prevent the Hyper-V host to interact in any means with the Shielded VM.
https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vms

The following table summarizes the differences between encryption-supported and shielded VMs.

Capability	Generation 2 Encryption Supported	Generation 2 Shielded
Secure Boot	Yes, required but configurable	Yes, required and enforced
Vtpm	Yes, required but configurable	Yes, required and enforced
Encrypt VM state and live migration traffic	Yes, required but configurable	Yes, required and enforced
Integration components	Configurable by fabric admin	Certain integration components blocked (e.g. data exchange, PowerShell Direct)
Virtual Machine Connection (Console), HID devices (e.g. keyboard, mouse)	On, cannot be disabled	Disabled (cannot be enabled)
COM/Serial ports	Supported	Disabled (cannot be enabled)
Attach a debugger (to the VM process)[1]	Supported	Disabled (cannot be enabled)

QUESTION 97
Your network contains two Active Directory forests named contoso.com and adatum.com.
Contoso.com contains a Hyper-V host named Server1.
Server1 is the member of a group named HyperHosts.
Adatum.com contains a server named Server2 that is configured for Admin-trusted attestation.
Server1 and Server2 run Windows Server 2016.
Contoso.com trusts adatum.com.
You plan to deploy shielded virtual machines to Server1. Which component should you install and which cmdlet should you run on Server1?

A. Component to install on Server1: The Active Directory Domain Services server role
B. Component to install on Server1: The Host Guardian Hyper-V Support feature
C. Component to install on Server1: The Host Guardian Service server role
D. Cmdlet to run on Server1: Export-HgsGuardian
E. Cmdlet to run on Server1: Get-HgsAttestationBaselinePolicy
F. Cmdlet to run on Server1: Import-HgsGuardian
G. Cmdlet to run on Server1: Set-HgsClientConfiguration

Correct Answer: BG
Section: (none)
Explanation

Explanation/Reference:
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. https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabric-guarded-host-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.

https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabric-confirm-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'
```

QUESTION 98
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1.
Server1 is configured as shown in the following table:

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

You plan to create a pilot deployment of Microsoft Advanced Threat Analytics (ATA). What should you do first?
A. Remove Server1 from the domain. B.
Assign an additional IPv4 address.
C. Obtain an SSL certificate.

D. Install Microsoft Security Compliance Manager (SCM).

Correct Answer: C
Section: (none)
Explanation

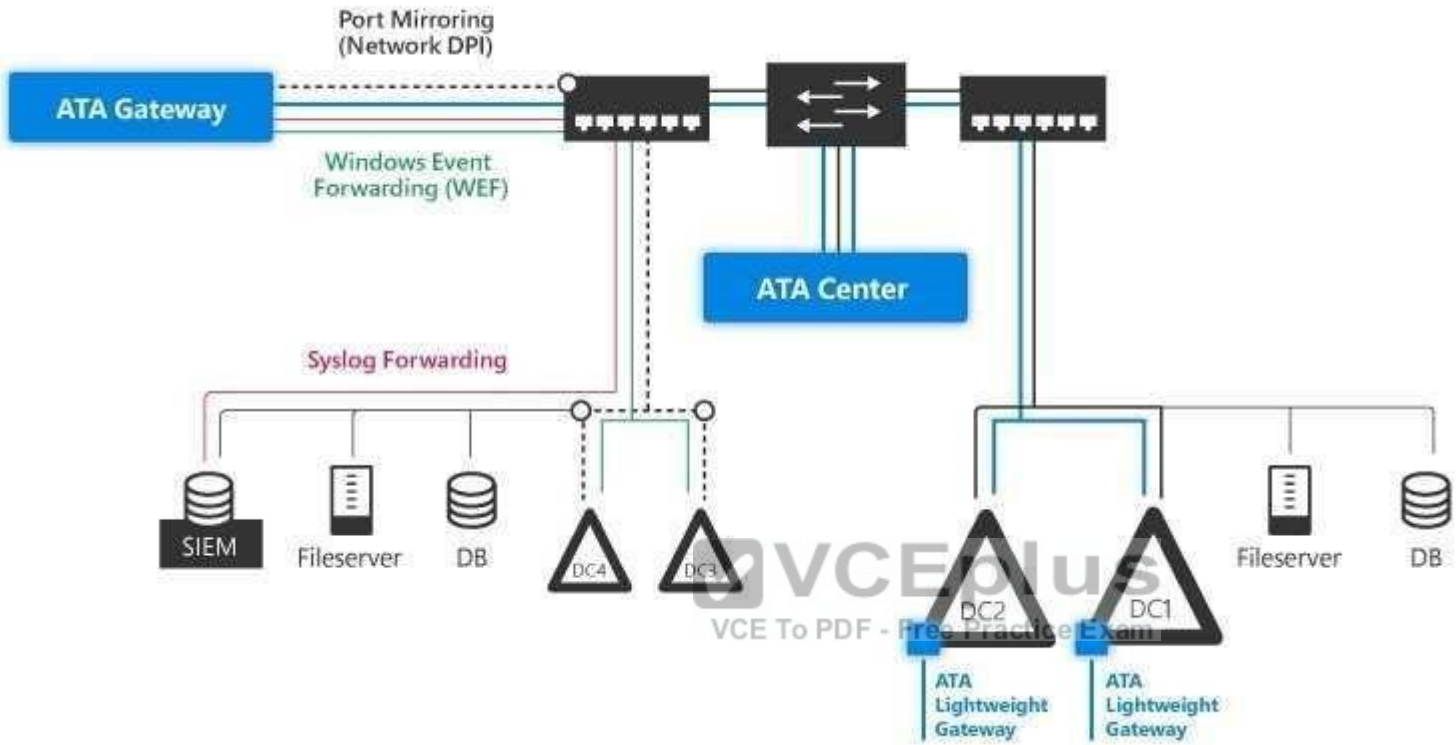
Explanation/Reference:
https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-prerequisites
ATA Center which is the first component to be deployed on Server1, requires the use of SSL protocol to communicate with ATA Gateway
To ease the installation of ATA, you can install self-signed certificates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

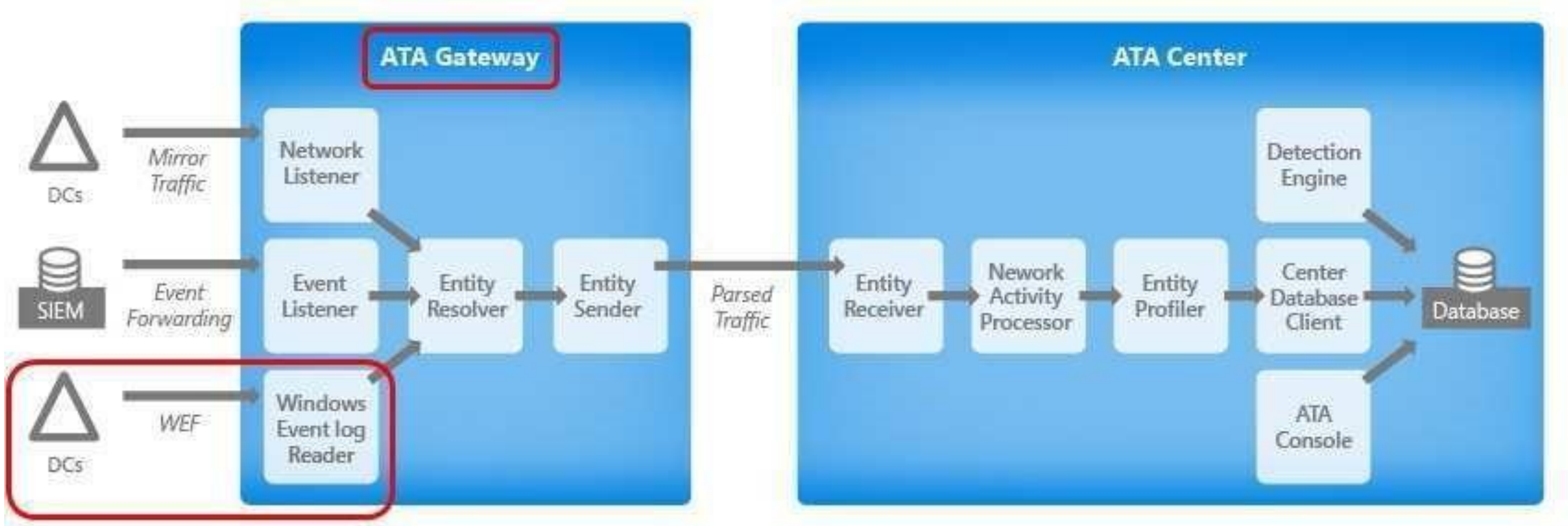
QUESTION 99
Your network contains an Active Directory domain named contoso.com.
You are deploying Microsoft Advanced Threat Analytics (ATA) to the domain.
You install the ATA Center on server named Server1 and the on a server named
Server2. You need to ensure that Server2 can collect NTLM authentication events. What should you configure?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation/Reference:
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.





QUESTION 100
You have a server named Server1 that runs Windows Server 2016.
You need to view all of the inbound rules on Server1.
Which cmdlet should you use?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Examples:-
Get-NetFirewallRule -Direction Inbound <--- view inbound rules for all profiles
The following examples shows inbound rule for specific firewall profile

Get-NetFirewallRule -Direction Inbound | where {$_.Profile -eq "Domain"}
Get-NetFirewallRule -Direction Inbound | where {$_.Profile -eq "Public"}
Get-NetFirewallRule -Direction Inbound | where {$_.Profile -eq "Private"}

QUESTION 101
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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
```


QUESTION 102

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

You need to identify whether ICMP traffic is exempt from IPsec on Server1.

Which cmdlet should you use?

A. Get-NetIPSecRule
B. Get-NetFirewallRule
C. Get-NetFirewallProfile D. Get-NetFirewallSetting

E. Get-NetFirewallPortFilter
F. Get-NetFirewallAddressFilter
G. Get-NetFirewallSecurityFilter
H. Get-NetFirewallApplicationFilter

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 103
You have a server named Server1 that runs Windows Server 2016.
You need to identity whether any connection security rules are 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
https://technet.microsoft.com/en-us/itpro/powershell/windows/netsecurity/get-netipsecrule
Get-NetIPSecRule displays the existence and details of Connection Security Rules, as connection security rules implements IPsec between computers (not using tunnel endpoints) or sites (using tunnel endpoints)

QUESTION 104
Your company has an accounting department.
The network contains an Active Directory domain named contoso.com. The domain contains 10 servers.
You deploy a new server named Server11 that runs Windows Server 2016.
Server11 will host several network applications and network shares used by the accounting department.
You need to recommend a solution for Server11 that meets the following requirements:
-Protects Server11 from address spoofing and session hijacking
-Allows only the computers in We accounting department to connect to Server11
What should you recommend implementing?

A. AppLocker rules
B. Just Enough Administration (JEA)
C. connection security rules
D. Privileged Access Management (PAM)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
In IPsec connection security rule, the IPsec protocol verifies the sending host IP address by utilize integrity functions like Digitally signing all packets.
If unsigned packets arrives Server11, those are possible source address spoofed packets, when using connection security rule in-conjunction with inbound firewall rules, you can kill those un-signed packets with the action "Allow connection if it is secure" to prevent spoofing and session hijacking attacks.
QUESTION 105
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:

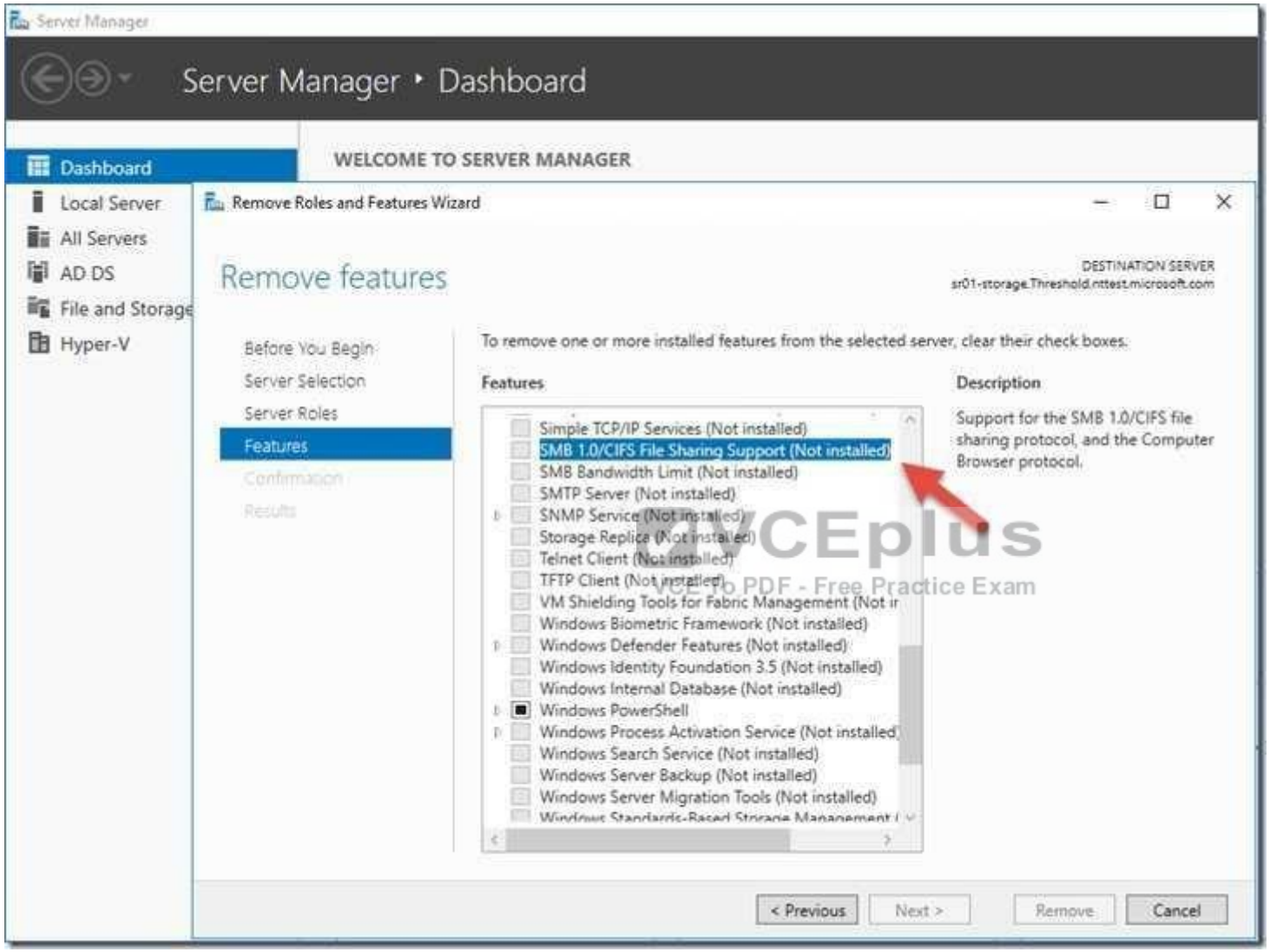
Server name	Configuration
Nano1	Nano Server
Nano2	Nano Server
Server2	File server that has a shared folder named DATA
Server3	DNS server that has a DNSSEC-signed zone named adatum.com
Server4	Hyper-V host
Server1	Application server

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Server2 is a Server, B is incorrect.
Moreover, as there is no such choice for using "Set-SmbServerConfiguration -EnableSMB1Protocol $false" cmdlet, you have to remove the SMB1's supporting server feature instead.
Answer A is correct for this question, see below.
https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows



QUESTION 106
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.
You need to exclude D:\Folder1 on Nano1 from being scanned by Windows Defender.
Which cmdlet should you run?

A. Set-StorageSetting
B. Set-DtcAdvancedSetting
C. Set-FsrmFileScreenException
D. Set-MpPreference

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
https://technet.microsoft.com/en-us/itpro/powershell/windows/defender/set-mppreference

QUESTION 107
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.
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)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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-NanoServer-DSC-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

QUESTION 108
Your network contains an Active Directory domain named contoso.com.

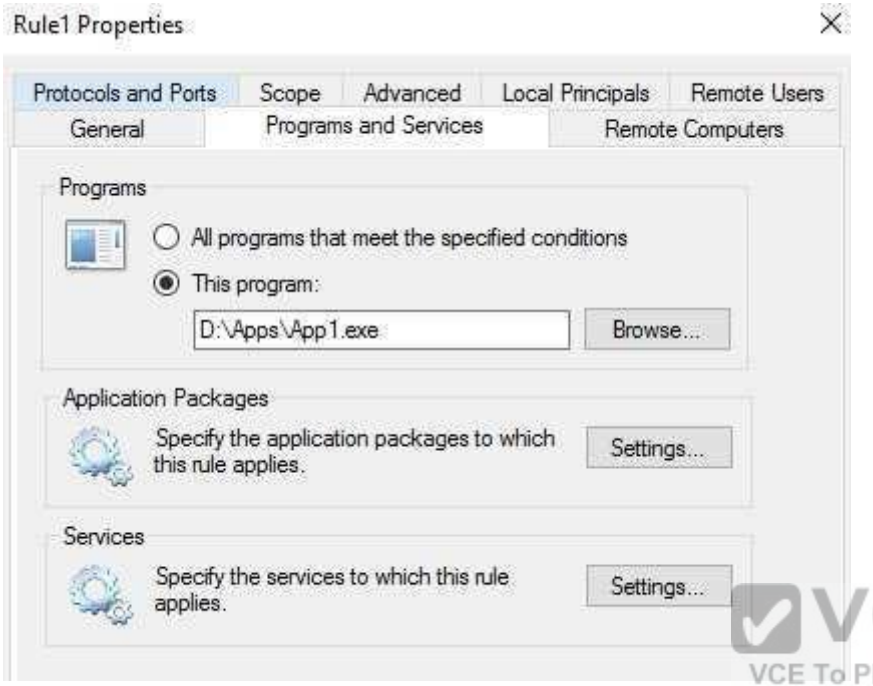
The domain contains a computer named Computer1 that runs Windows 10.
Computer1 connects to a home network and a corporate network.
The corporate network uses the 172.16.0.0/24 address space internally.
Computer1 runs an application named App1 that listens to port 8080.
You need to ensure that App1.exe 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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
```



QUESTION 109
Your network contains an Active Directory domain named contoso.com.
The domain contains multiple Hyper-V hosts.
You need to deploy several critical line-of-business applications to the network to meet the following requirements:
-The resources of the applications must be isolated from the physical host
-Each application must be prevented from accessing the resources of the other applications.
-The configurations of the applications must be accessible only from the operating system that hosts the application.
Solution: You deploy a separate Hyper-V container for each application. Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:
-The resources of the applications must be isolated from the physical host (ACHIEVED)
-Each application must be prevented from accessing the resources of the other applications. (ACHIEVED)
-The configurations of the applications must be accessible only from the operating system that hosts the application. (ACHIEVED)

QUESTION 110
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
No, Server1 and Server2 uses local group "Backup Operators" for granting backup and restore rights to normal users.
The solution would let User1 to backup files and folders on domain controllers for contoso.com instead.

QUESTION 111
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.

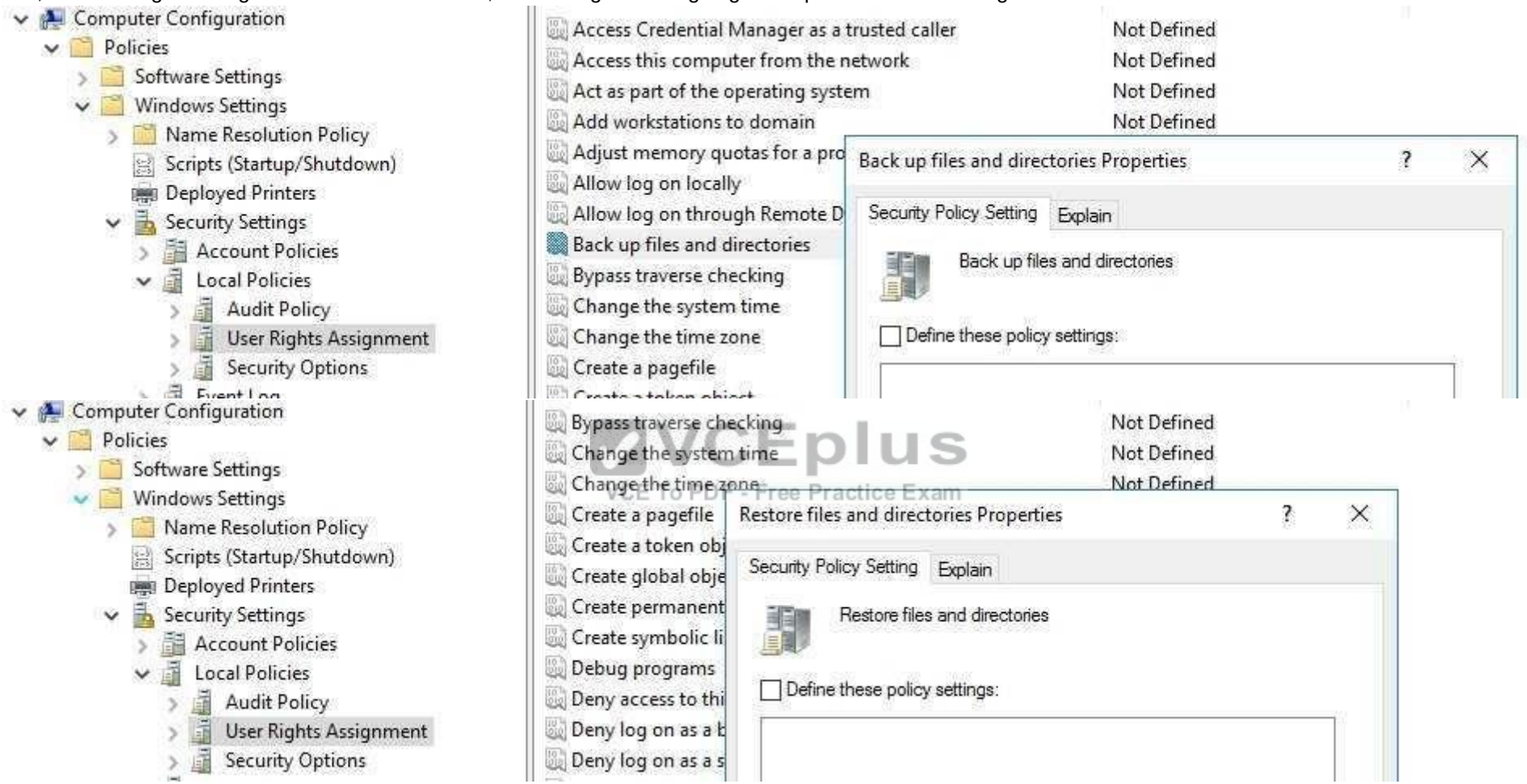
Server name	Object	Organizational unit (OU) name
Server1	Computer account	Servers
Server2	Computer account	Servers
User1	User account	Operations Users

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 goal?
A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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



QUESTION 112

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 113
Your network contains an Active Directory domain named contoso.com. The domain contains several Hyper-V hosts.
You deploy a server named Server22 to a workgroup. Server22 runs Windows Server 2016.
You need to configure Server22 as the primary Host Guardian Service server.
Which three cmdlets should you run in sequence?

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

Correct Answer: AEF
Section: (none)
Explanation

Explanation/Reference:
Correct order of actions:
1. Install-ADDSDomainController , as Server22 is a workgroup computer, create a new domain on it first.
2. Install-HgsServer3. Initialize-HgsServer https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabric-setting-up-the-host-guardian-service-hgs

https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabric-install-hgs-default Install-HgsServer

https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabric-initialize-hgs-tpm-mode-default Initialize-HgsServer

QUESTION 114
You are creating a Nano Server image for the deployment of 10 servers.
You need to configure the servers as guarded hosts that use Trusted Platform Module (TPM) attestation.
Which three packages should you include in the Nano Server image? Each correct answer presents part of the solution.

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

Correct Answer: ABF
Section: (none)
Explanation

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

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

System Center Operations Manager agent	Installed separately. See the System Center Operations Manager documentation for more details at https://technet.microsoft.com/en-us/system-center-docs/om/manage/install-agent-on-nano-server.
Data Center Bridging (including DCBQoS)	-Package Microsoft-NanoServer-DCB-Package
Deploying on a virtual machine	-Package Microsoft-NanoServer-Guest-Package
Deploying on a physical machine	- Package Microsoft-NanoServer-Host-Package
BitLocker, trusted platform module (TPM), volume encryption, platform identification, cryptography providers, and other functionality related to secure startup	-Package Microsoft-NanoServer-SecureStartup-Package
Hyper-V support for Shielded VMs	-Package Microsoft-NanoServer-ShieldedVM-Package **Note:** This package is only available for the Datacenter edition of Nano Server.

QUESTION 115
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

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:
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-shielded-vm/guarded-fabric-guarded-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.

QUESTION 116
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.
You need to install the required server roles for the planned deployment
Which server role should you deploy? Choose Two.

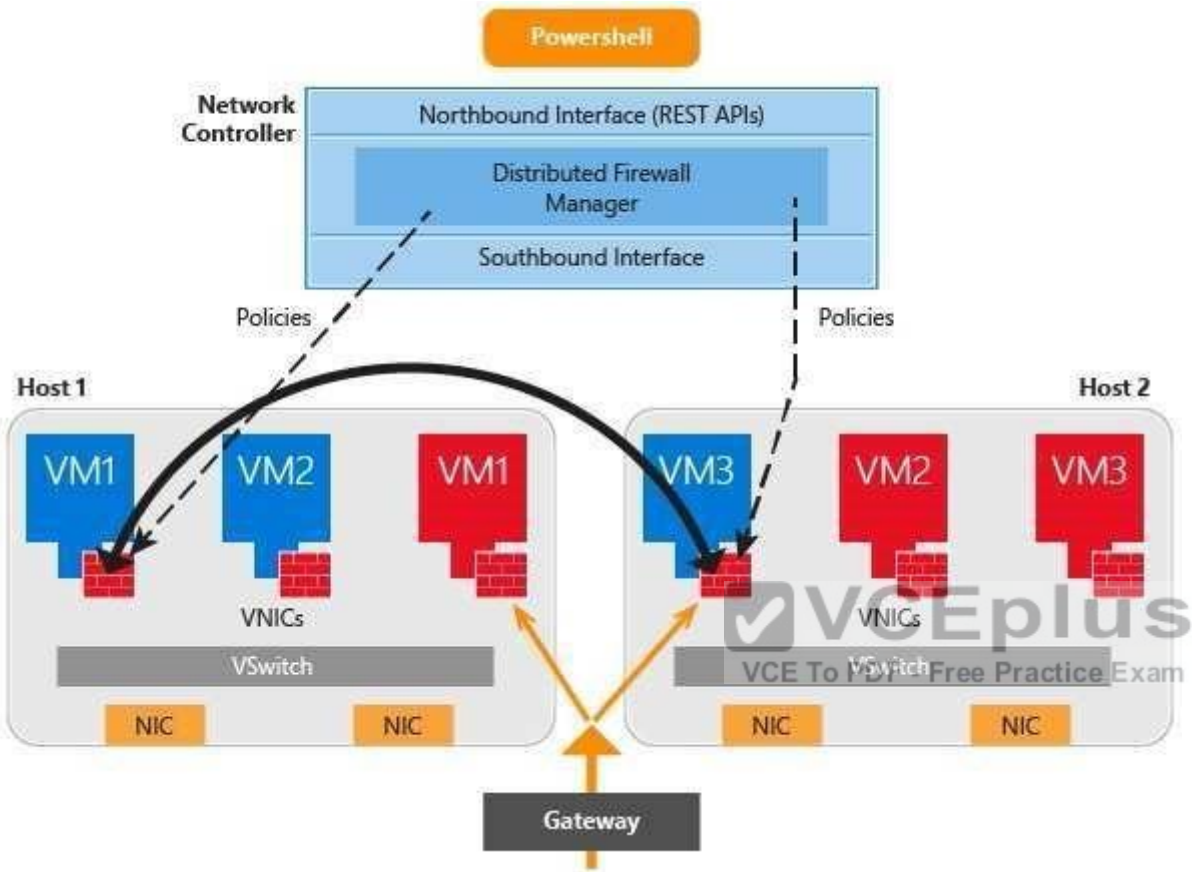
A. Server role to deploy: Multipoint Services
B. Server role to deploy: Network Controller
C. Server role to deploy: Network Policy and Access Services
D. Servers on which to deploy the server role: Server20 and Server21

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

E. Servers on which to deploy the server role: Server22 and Server23

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
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 service provider, 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/network-controller/network-controller
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-and-preparation-requirements-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.

Feature Differentiation: Datacenter and Standard Editions		
Feature	**Datacenter Edition**	**Standard Edition**
Core functionality of Windows Server	●	●
OSEs / Hyper-V Containers	Unlimited	2
Windows Server containers	Unlimited	Unlimited
Host Guardian Service	●	●
Nano Server*	●	●
Storage features including Storage Spaces Direct and Storage Replica	●	
Shielded Virtual Machines	●	
Networking stack	●	
Core-based pricing**	$6,155	$882

QUESTION 117
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 Credential Guard.

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 Enterprise.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 118
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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/securing-privileged-access-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.

QUESTION 119
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 administrator. Join each PAW to the contosoadmin.com domain.
B. Provide a Privileged Access Workstation (PAW) for each user in the contoso.com forest. Join each PAW to the contoso.com domain.
C. Provide a Privileged Access Workstation (PAW) for each administrator. Join each PAW to the contoso.com domain.
D. Provide a Privileged Access Workstation (PAW) for each user account in both forests. Join each PAW to the contoso.com domain.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 120
Your network contains an Active Directory domain named contoso.com. The domain contains multiple servers that run either Windows Server 2012 or Windows Server 2012 R2.
You plan to implement Just Enough Administration (JEA) to manage all of the servers.
What should you install on each server to ensure that the servers can be managed by using JEA?

A. Remote Server Administration Tools (RSAT)
B. Microsoft .NET Framework 3.5 Service Pack 1 (SP1)
C. Management Odata Internet Information Services (IIS) Extension
D. Windows Management Framework 5.0

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:
https://msdn.microsoft.com/en-us/library/dn896648.aspx
Get JEA

The current release of JEA is available on the following platforms:
Windows Server
Windows Server 2016 Technical Preview 5 and higher
Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2* with Windows Management Framework 5.0 installed

QUESTION 121
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

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:
-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

QUESTION 122
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

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
-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

QUESTION 123
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?1

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 parameter.

Correct Answer: C
Section: (none)
Explanation

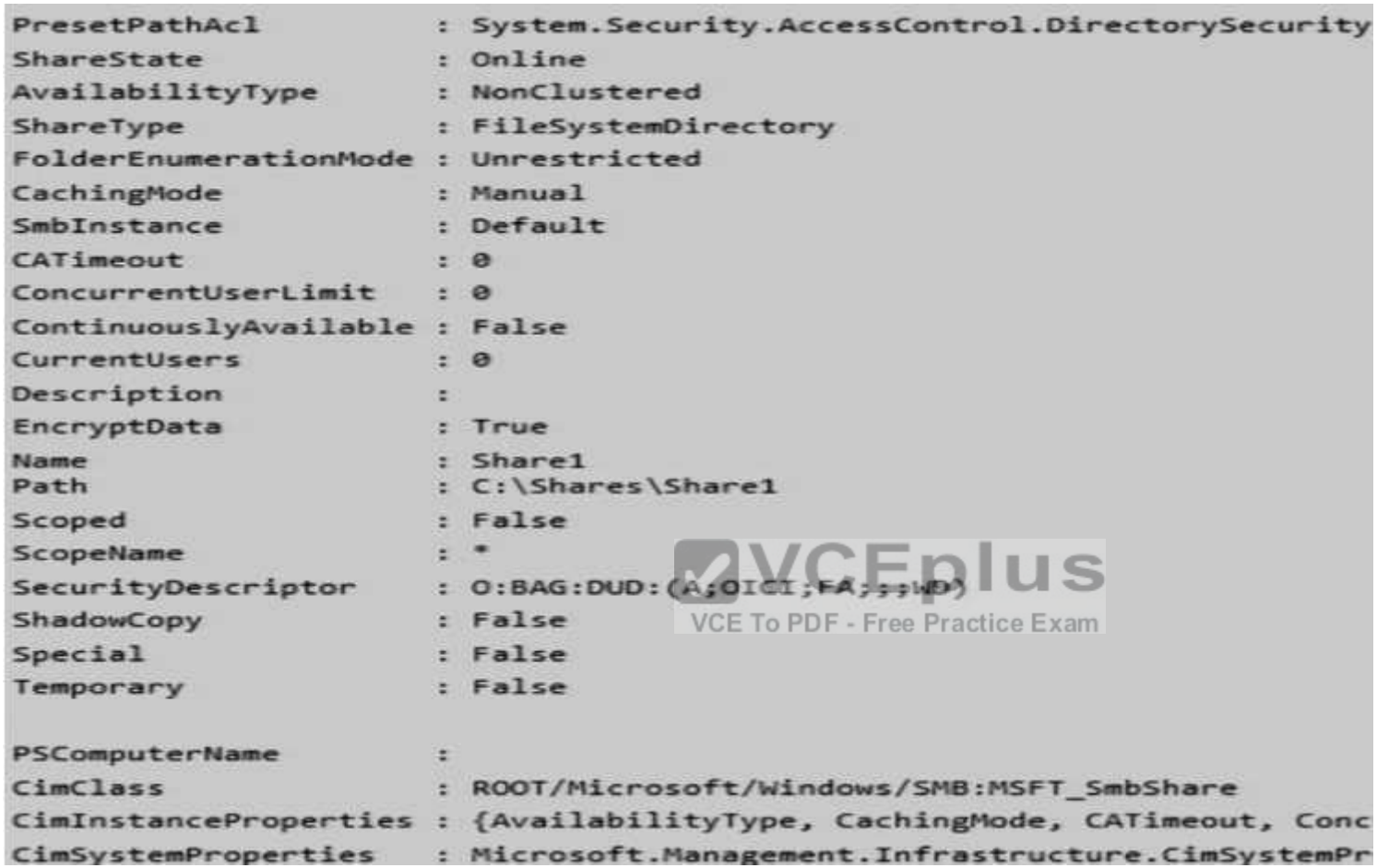
Explanation/Reference:

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

QUESTION 124
Your network contains an Active Directory named contoso.com.
The domain contains the computers configured as shown in the following table.

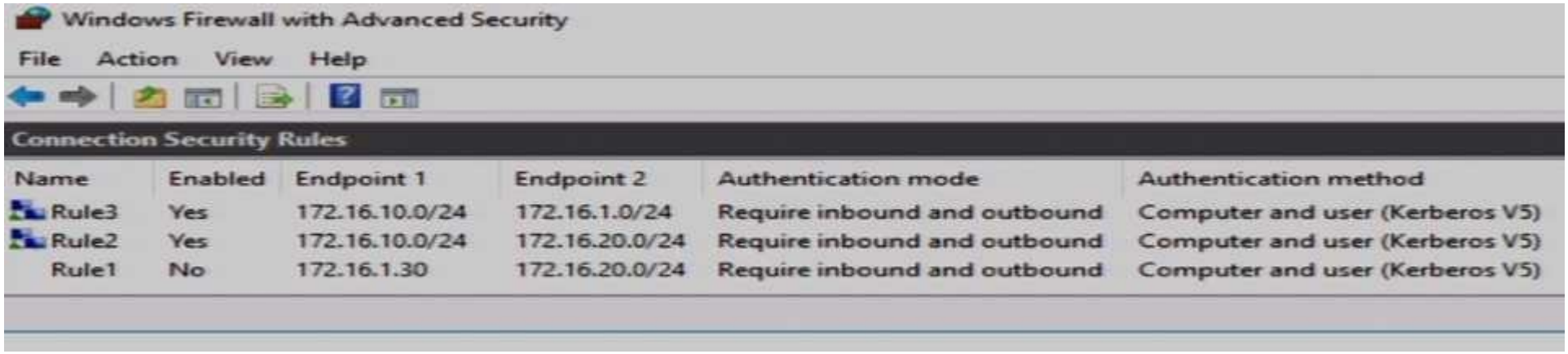
Name	IP address
Server1	172.16.1.30
Computer1	172.16.10.60
Computer2	172.16.20.50

Server1 has a share named Share1 with the following configurations:-



```
PresetPathAcl          : System.Security.AccessControl.DirectorySecurity
ShareState             : Online
AvailabilityType       : NonClustered
ShareType              : FileSystemDirectory
FolderEnumerationMode  : Unrestricted
CachingMode            : Manual
SmbInstance            : Default
CATimeout              : 0
ConcurrentUserLimit    : 0
ContinuouslyAvailable  : False
CurrentUsers           : 0
Description            :
EncryptData            : True
Name                   : Share1
Path                   : C:\Shares\Share1
Scoped                 : False
ScopeName              : *
SecurityDescriptor     : O:BAG:DUD:(A;OICI;FA;;;WD)
ShadowCopy             : False
Special                : False
Temporary              : False

PSComputerName         :
CimClass               : ROOT/Microsoft/Windows/SMB:MSFT_SmbShare
CimInstanceProperties  : {AvailabilityType, CachingMode, CATimeout, Conc
CimSystemProperties    : Microsoft.Management.Infrastructure.CimSystemPr
```


Server1, Computer1, and Computer2 have the connection security rules configured as shown in follow:-



For each of the following statements are true? Choose Three.

A. When Computer1 accesses Share1, SMB encryption will be used: YES
B. When Computer1 accesses Share1, SMB encryption will be used: NO
C. When Computer2 accesses Share1, SMB encryption will be used: YES
D. When Computer2 accesses Share1, SMB encryption will be used: NO
E. When Server1 accesses a shared folder on Computer1, IPsec encryption will be used: YES
F. When Server1 accesses a shared folder on Computer1, IPsec encryption will be used: NO

Correct Answer: ACF
Section: (none)
Explanation

Explanation/Reference:
A and C are correct.
The shared folder "Share1" is configured with "EncryptData : True", no matter which network the client resides, SMB 3 communication will be encrypted.
When Server1 access Computer1 over network, the original packet L3 IP Header is as follow:-
172.16.1.30 --> 172.16.10.60
These traffic does not match the enabled IPSec rule "Rule2" nor "Rule3", and the only matching rule "Rule1" is disabled. So, no IPsec encryption will be achieved.
F is correct.

QUESTION 125
The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.

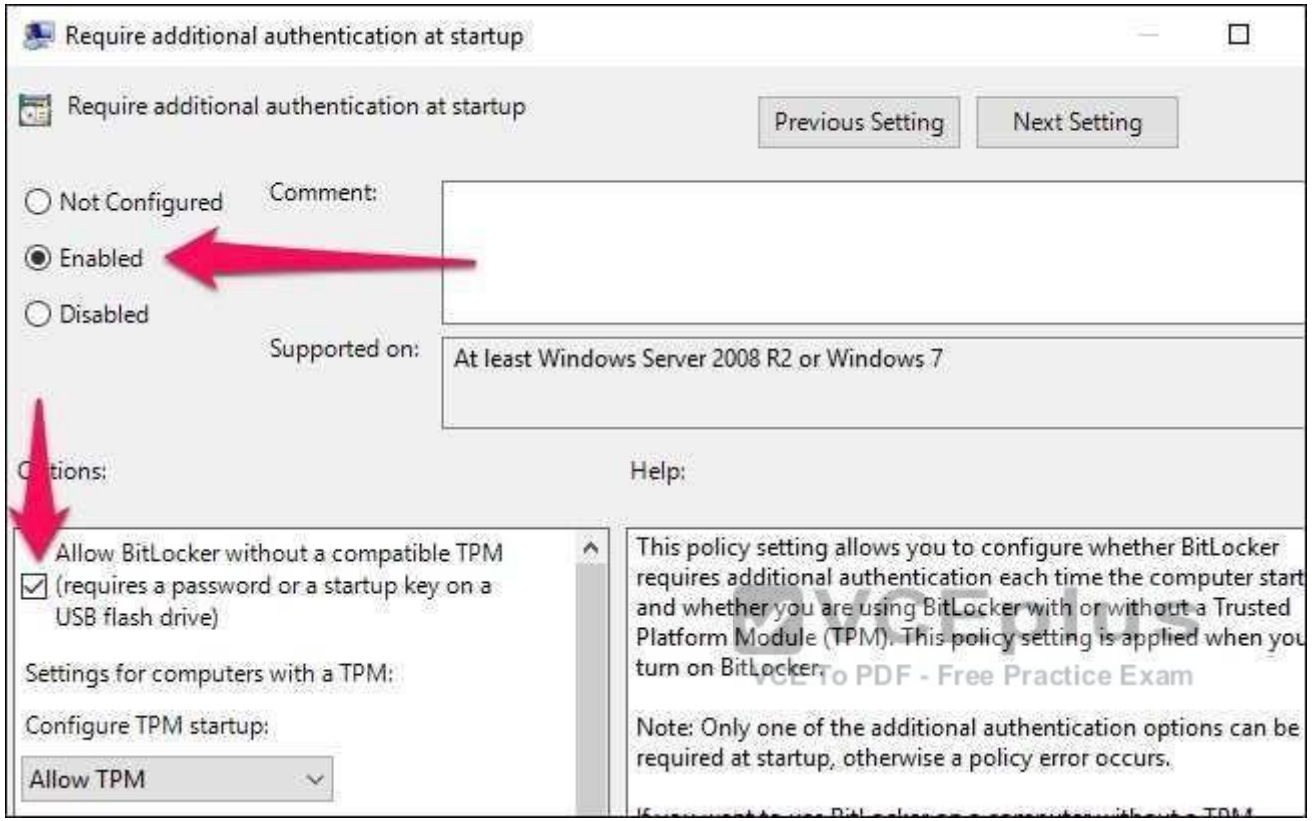
Server name	Domain or workgroup	Configuration
Server1	Domain	Windows Server Update Services (WSUS) server
Server2	Domain	Server that has a Trusted Platform Module (TPM)
Server3	Domain	Member server that will be configured for Just Enough Administration (JEA)
Server4	Domain	Application server
Server5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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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/



QUESTION 126

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

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

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

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

You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers.
An OU named OU2 contains the computer accounts of the computers in the marketing department.
A Group Policy object (GPO) named GP1 is linked to OU1.
A GPO named GP2 is linked to OU2.
All computers receive updates from Server1.
You create an update rule named Update1.
You need to prepare the environment to support applying Update1 to the laptops only.
What should you do? Choose Two.

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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
https://technet.microsoft.com/en-us/library/cc708458(v=ws.10).aspx

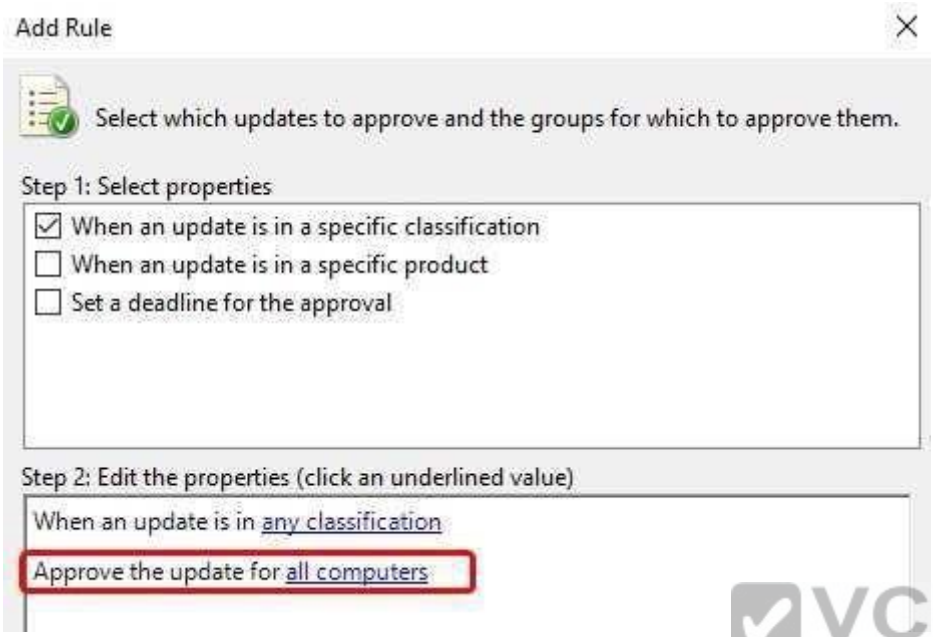
Automatically Approving Updates for Detection

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

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

To automatically approve updates for detection

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



QUESTION 127

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

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

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

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

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

An OU named OU2 contains the computer accounts of the computers in the marketing department.

A Group Policy object (GPO) named GP1 is linked to OU1.

A GPO named GP2 is linked to OU2.

All computers receive updates from Server1.

You create an update rule named Update1.
You enable deep script block logging for Windows PowerShell.
In which event log will PowerShell code that is generated dynamically appear?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 128
You configure Just Enough Administration (JEA).
You need to ensure that a non-administrator user can perform the following actions:
-Restart Internet Information Services (IIS)
-Restart a custom service named Service1
How should you complete the role configuration file? Choose Two

A. VisibleAliases = 'C:\Windows\system32\iisreset.exe'
B. VisibleCmdlets = 'C:\Windows\system32\iisreset.exe'
C. VisibleExternalCommands = 'C:\Windows\system32\iisreset.exe'
D. VisibleAliases = @{ Name 'Restart-service' ; Parameters @{ Name = 'Name'; ValidateSet = 'Service1'}}
E. VisibleCmdlets = @{ Name 'Restart-service' ; Parameters @{ Name = 'Name'; ValidateSet = 'Service1'}}
F. VisibleExternalCommands = @{ Name 'Restart-service' ; Parameters @{ Name = 'Name'; ValidateSet = 'Service1'}}

Correct Answer: CE
Section: (none)
Explanation

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

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

```
PowerShell                                                                    Copy

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

Allowing external commands and PowerShell scripts

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


```
PowerShell                                                                    Copy

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

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

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

QUESTION 129
Your network contains an Active Directory domain named contoso.com.
You plan to deploy an application named App1.exe.
You need to verify whether Control Flow Guard is enabled for App1.exe. Which command should you run?

A. Dumpbin.exe /dependents /locadconfig App1.exe
B. Dumpbin.exe /headers /locadconfig App1.exe
C. Dumpbin.exe /relocations /locadconfig App1.exe

D. Dumpbin.exe /symbols /locadconfig App1.exe
E. Sfc.exe /dependents /locadconfig App1.exe
F. Sfc.exe /headers /locadconfig App1.exe
G. Sfc.exe /relocations /locadconfig App1.exe
H. Sfc.exe /symbols /locadconfig App1.exe
I. Sigverif.exe /dependents /locadconfig App1.exe
J. Sigverif.exe /headers /locadconfig App1.exe
K. Sigverif.exe /relocations /locadconfig App1.exe
L. Sigverif.exe /symbols /locadconfig App1.exe
M. Verifier.exe /dependents /locadconfig App1.exe
N. Verifier.exe /headers /locadconfig App1.exe
O. Verifier.exe /relocations /locadconfig App1.exe
P. Verifier.exe /symbols /locadconfig App1.exe

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
https://msdn.microsoft.com/en-us/library/windows/desktop/mt637065(v=vs.85).aspx
Control Flow Guard (CFG) is a highly-optimized platform security feature that was created to combat memory corruption vulnerabilities.
By placing tight restrictions on where an application can execute code from, it makes it much harder for exploits to execute arbitrary code through vulnerabilities

such as buffer overflows.
To verify if Control Flow Guard is enable for a certain application executable:-
Run the dumpbin.exe tool (included in the Visual Studio 2015 installation) from the Visual Studio command prompt with the /headers and /loadconfig options:
dumpbin.exe /headers /loadconfig test.exe.
The output for a binary under CFG should show that the header values include "Guard", and that the load config values include "CF Instrumented" and "FID table present".1

```
OPTIONAL HEADER VALUES
             20B magic # (PE32+)
           12.10 linker version
          1BFE00 size of code
          282600 size of initialized data
             200 size of uninitialized data
           9E090 entry point (0000000140090E090)
            1000 base of code
       140000000 image base (0000000140000000 to 0000000140447FFF)
            1000 section alignment
             200 file alignment
           10.00 operating system version
           10.00 image version
           10.00 subsystem version
               0 Win32 version
          448000 size of image
             400 size of headers
          4589A6 checksum
               2 subsystem (Windows GUI)
            C1C0 DLL characteristics
                   Dynamic base
                   Check integrity
                   NX compatible
                   Guard
                   Terminal Server Aware
  Section contains the following load config:

            000000A0 size
                   0 time date stamp
                0.00 Version
                   0 GlobalFlags Clear
                   0 GlobalFlags Set
                   0 Critical Section Default Timeout
                   0 Decommit Free Block Threshold
                   0 Decommit Total Free Threshold
    0000000000000000 Lock Prefix Table
                   0 Maximum Allocation Size
                   0 Virtual Memory Threshold
                   0 Process Heap Flags
                   0 Process Affinity Mask
                   0 CSD Version
                0000 Reserved
    0000000000000000 Edit list
    000000014023C008 Security Cookie
```

QUESTION 130

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.1
A user named User1 is a member of the local Administrators group. Server1 has the AppLocker rules configured as shown in follow:

Rule1 and Rule2 are configured as shown in the following table:1

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

You verify that User1 is unable to run App2.exe on Server1.
Which changes will allow User1 to run D:\Folder1\Program.exe and D:\Folder2\App2.exe? Choose Two.

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

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference: https://technet.microsoft.com/en-us/library/ee449492(v=ws.11).aspx

For "D:\Folder1\Program.exe", it is originally explicitly denied due to Rule1, when moving the "Program,exe" out of "D:\Folder1\", it does not match Rule1.
Assume that "Program.exe" is moved to "D:\Folder2", it matches an Explicit Allow rule for group "BUILTIN\Administrators" which User1 is a member of, therefore A is correct.
For "App2",exe, it matches a Explicit Deny rule using its File Hash (created File content), no matter where you move it to, or how you rename it, it would still match Rule2.
Only changing the file content of App2.exe would let it no longer match the explicit deny hash-based rule "Rule2".
By upgrading its version and content, it will generate a new hash. so F is correct.

QUESTION 131
Your network contains an Active Directory domain named contoso.com. The domain contains multiple servers that run multiple applications.
Domain user accounts are used to authenticate access requests to the servers.
You plan to prevent NTLM from being used to authenticate to the servers.
You start to audit NTLM authentication events for the domain.
You need to view all of the NTLM authentication events and to identify which applications authenticate by using NTLM.
On which computers should you review the event logs and which logs should you review?

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

Correct Answer: AE
Section: (none)
Explanation

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

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

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

Applies to

- Windows 10

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

Reference

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

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

Auditing

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

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

QUESTION 132
Your network contains an Active Directory domain named contoso.com.
The domain contains a server named Server1 that runs Windows Server 2016 and a Nano Server named Nano1.
Nano1 has two volumes named C and D.
You are signed in to Server1.
You need to configure Data Deduplication on Nano1.
Which tool should you use?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 133
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)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
I think I don't have to remind you that "File Explorer" = "Windows Explorer".
https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/deploy-a-central-access-policy--demonstration-steps-#BKMK_1.4

To assign a central access policy to a file server

1. In Hyper-V Manager, connect to server FILE1. Log on to the server by using contoso\administrator with the password: **pass@word1**.

2. Open an elevated command prompt and type: **gpupdate /force**. This ensures that your Group Policy changes take effect on your server.

3. You also need to refresh the Global Resource Properties from Active Directory. Open an elevated Windows PowerShell window and type `Update-FSRMClassificationpropertyDefinition`. Click ENTER, and then close Windows PowerShell.

   > **Tip**
   >
   > You can also refresh the Global Resource Properties by logging on to the file server. To refresh the Global Resource Properties from the file server, do the following
   >
   > a. Logon to File Server FILE1 as contoso\administrator, using the password **pass@word1**.
   >
   > b. Open File Server Resource Manager. To open File Server Resource Manager, click **Start**, type **file server resource manager**, and then click **File Server Resource Manager**.
   >
   > c. In the File Server Resource Manager, click **File Classification Management** , right-click **Classification Properties** and then click **Refresh**.

4. Open Windows Explorer, and in the left pane, click drive D. Right-click the **Finance Documents** folder, and click **Properties**.

5. Click the **Classification** tab, click **Country**, and then select **US** in the **Value** field.

6. Click **Department**, then select **Finance** in the **Value** field and then click **Apply**.

   > **Note**
   >
   > Remember that the central access policy was configured to target files for the Department of Finance. The

QUESTION 134
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.
Dynamic Access Control is configured. A resource property named Property1 was created in the domain.
You need to ensure that Property1 is set to a value of Big for all of the files in Volume1 that are larger than 10 MB.
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)

Correct Answer: H
Section: (none)
Explanation

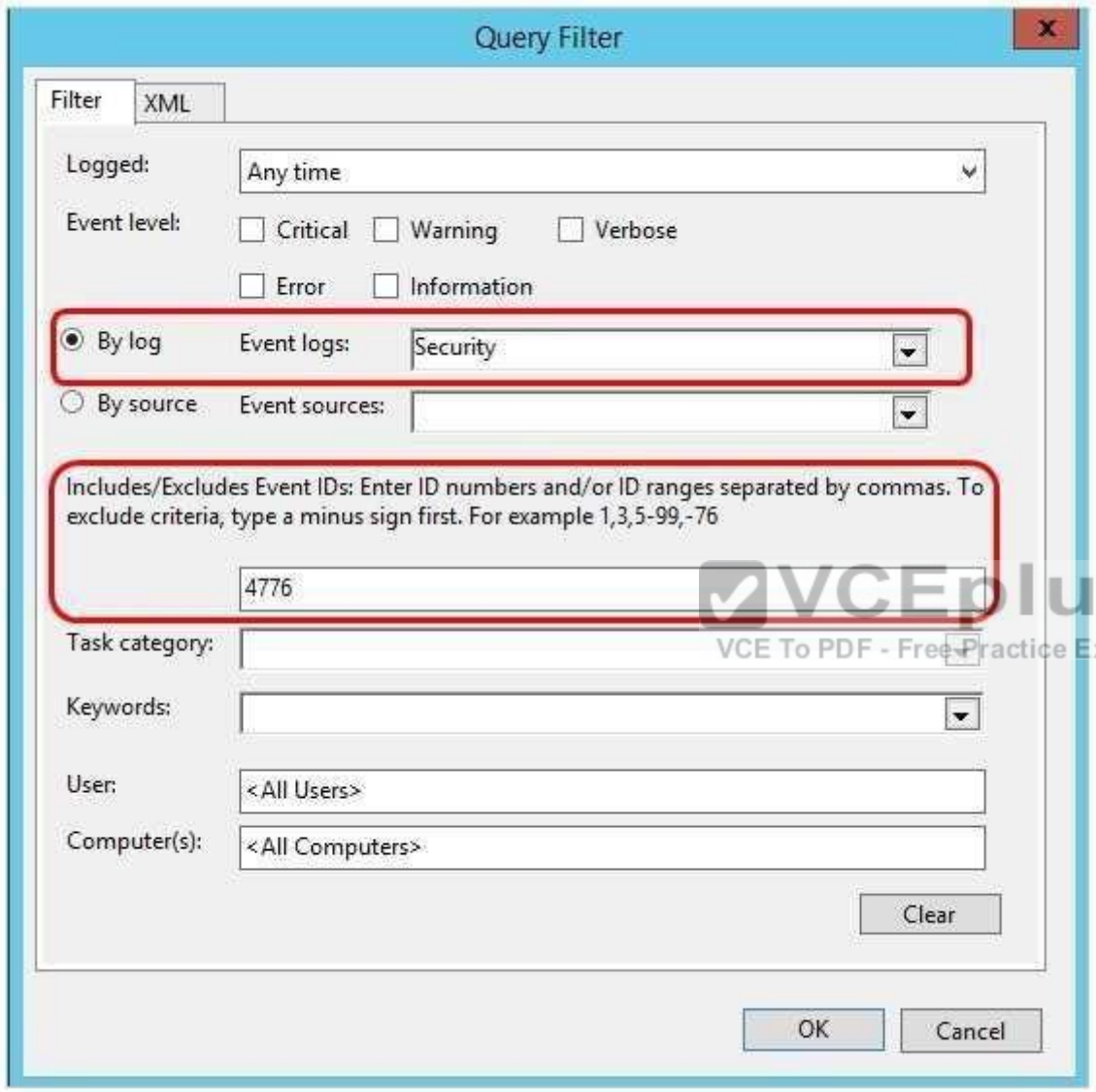
Explanation/Reference:
Automatic File Classification of FSRM
https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/deploy-automatic-file-classification--demonstration-stepshttps://
blogs.technet.microsoft.com/filecab/2009/08/13/using-windows-powershell-scripts-for-file-classification/

QUESTION 135
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 Gateway on a server named Server1.
To assist in detecting Pass-the-Hash attacks, you plan to configure ATA Gateway to collect events.
You need to configure the query filter for event subscriptions on Server1.
How should you configure the query filter?

A. Event log to configure: Application
B. Event log to configure: Directory Services
C. Event log to configure: Security
D. Event log to configure: System
E. Event ID to include: 1000 F. Event ID to include: 1009 G. Event ID to include: 1025 H. Event ID to include: 4776
I. Event ID to include: 4997

Correct Answer: CH
Section: (none)
Explanation

Explanation/Reference:
https://docs.microsoft.com/en-us/advanced-threat-analytics/configure-event-collection
To enhance detection capabilities, ATA needs the following Windows events: **4776**, 4732, 4733, 4728, 4729, 4756, 4757. These can either be read automatically by the ATA Lightweight Gateway or in case the ATA Lightweight Gateway is not deployed, it can be forwarded to the ATA Gateway in one of two ways, by configuring the ATA Gateway to listen for SIEM events or by configuring Windows Event Forwarding.



Event ID: 4776 NTLM authentication is being used against domain controller
Event ID: 4732 A User is Added to Security-Enabled DOMAIN LOCAL Group,
Event ID: 4733 A User is removed from Security-Enabled DOMAIN LOCAL Group Event ID: 4728 A User is Added or Removed from Security-Enabled Global Group
Event ID: 4729 A User is Removed from Security-Enabled GLOBAL Group

Event ID: 4756 A User is Added or Removed From Security-Enabled Universal Group
Event ID: 4757 A User is Removed From Security-Enabled Universal Group