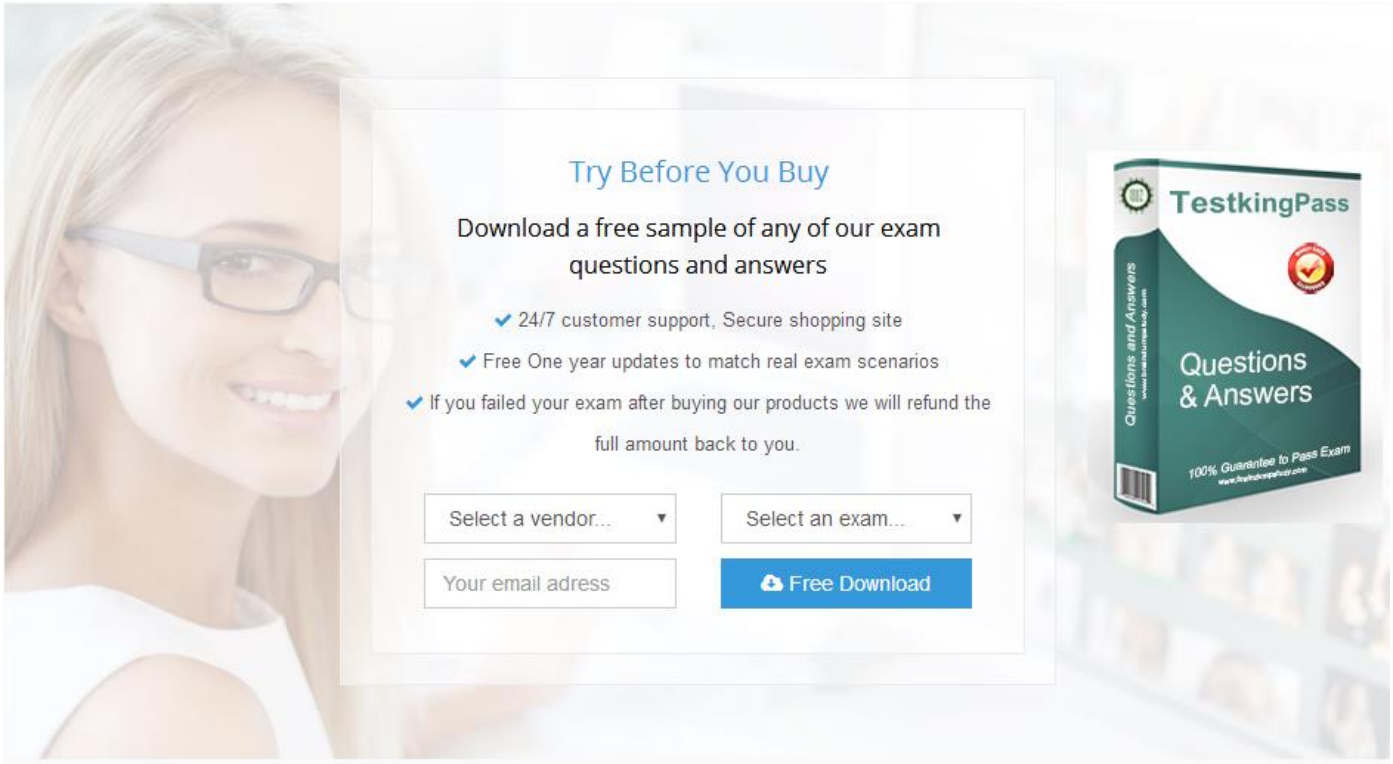
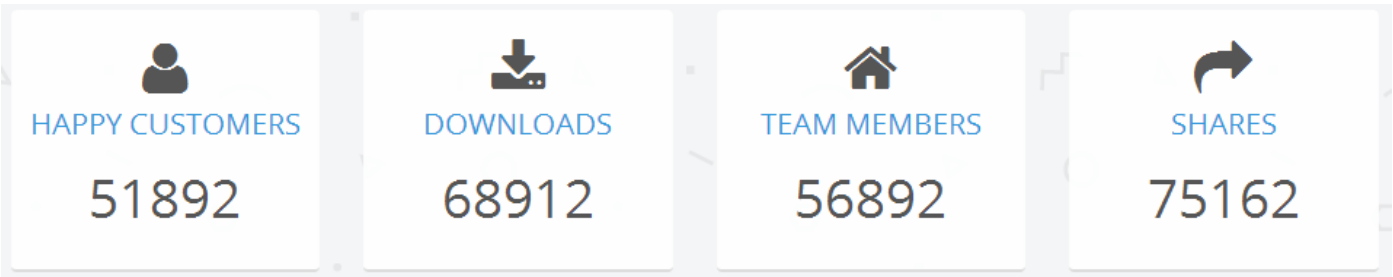
TestkingPass





http://www.testkingpass.com

Reliable test dumps & stable pass king & valid test questions

Exam : **70-744**

Title : Securing Windows Server 2016

Vendor : Microsoft

Version : DEMO

NO.1 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. 33
B. 45
C. 73
D. 10

Answer: C
Explanation
-Antimalware data from all the servers must be visible in Workspace1.-Security and audit data from the domain controllers and the virtualization hosts must be visible in Workspace2.-System update data from all the servers in all the workgroups must be visible in Workspace&"All the servers" mean all 5 domain controllers, plus all member servers (physical and virtual, domain andworkgroup) and virtualization hosts, so there are noexemptions.All servers in the above table mentioned must install OMS Microsoft Monitoring agents

NO.2 Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario b repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.
Start of repeated scenario
Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.
The domain contains the servers configured as shown m the following table.

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

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

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

A. From Server Manager, remove a Windows feature.

B. From Windows PowerShell, run the Set -SmbClientConfiguration cmdlet.

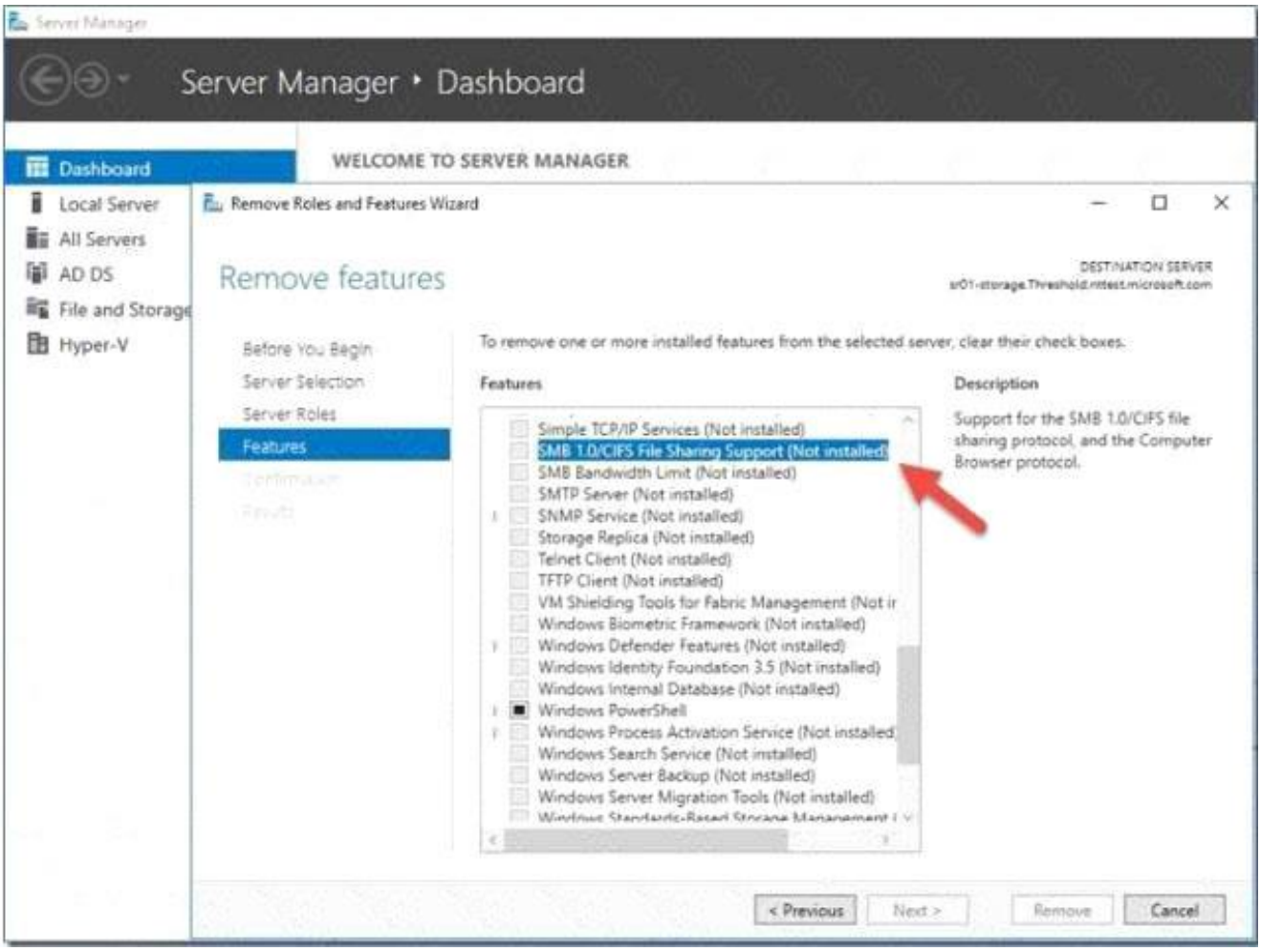
C. From File Server Resource Manager, create a classification rule.

D. From the properties of each network adapter on Server2. modify the bindings.

Answer: A

Explanation

https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-inwindows-and-windows



NO.3 Your network contains an Active Directory forest named contoso.com.
You deploy another Active Directory forest named admin.contoso.com.
You create a trust relationship between the two forests. The trust relationship has the following configurations:

* SID history is disabled. SID filtering is disabled.
You need to implement Privileged Access Management (PAM) and to specify admin.contoso.com as an administrative forest.
What should you do?

A. Run netdom.exe and specify the /transitive switch.

B. Run netdom.exe and specify the /quarantine switch.

C. Enable SID history on the trust

D. Enable SID filtering on the trust.

Answer: A

NO.4 Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.
You deploy Advanced Threat Analytics (ATA) to Server1.
You need to move the ATA database to a different folder.
Which configuration file should you modify?

A. Mongod.cfg

B. Config.xml

C. Config.json

D. Web.config

Answer: A
Explanation
References:
https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-database-management

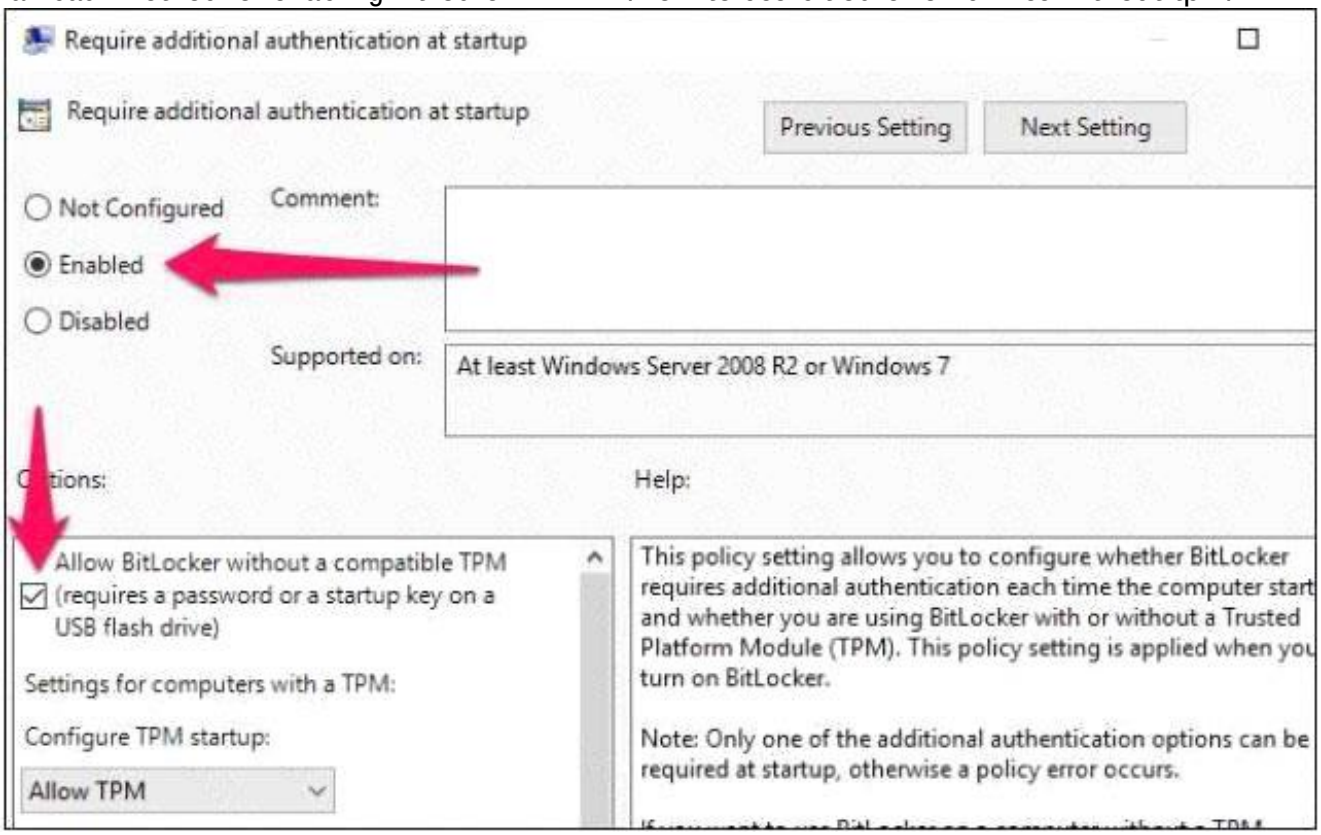
NO.5 The network contains an Active Directory domain named contoso.com. The domain contains the servers configured as shown in the following table.

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. Require additional authentication at startup
C. Configure TPM platform validation profile for native UEFI firmware configurations
D. Configure TPM platform validation profile for BIOS-based firmware configurations
Answer: B
Explanation
As there is not a choice "Enabling Virtual TPM for the virtual machine VM1", then we have to use a fall-back method for enabling BitLocker in VM1. /how-to-use-bitlocker-on-d rives-without-tpm/



NO.6 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You manage a file server that runs Windows Server 2016. The file server contains the volumes configured as shown in the following table.

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

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

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

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

NO.7 Your network contains an Active Directory domain The domain contains the computers shown in the following table.

Name	Operating system
Computer1	Windows 8.1
Computer2	Windows 10
Server1	Windows Server 2016
Server2	Windows Server 2016

server 1 is a file server that has two shared folders named Share1 and Share2. Share1 has encryption enabled.

Share2 has encryption disabled. Domain users have read access to both shares.

From PowerShell, you run set-smbServerConfiguration -EncryptData $true -Force.

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

Statements	Yes	No
If you connect to Share1 from Server2, network traffic will be encrypted.	○	○
If a user attempts to connect to Share1 from Computer1, the user will be prevented from accessing Share1.	○	○
If you connect to Share2 from Computer2, network traffic will be encrypted.	○	○

Answer:

Statements	Yes	No
If you connect to Share1 from Server2, network traffic will be encrypted.	○	○
If a user attempts to connect to Share1 from Computer1, the user will be prevented from accessing Share1.	○	○
If you connect to Share2 from Computer2, network traffic will be encrypted.	○	○

NO.8 Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario.

Your company has a marketing department.
The network contains an Active Directory domain named constoso.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.
End of repeated scenario.
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.

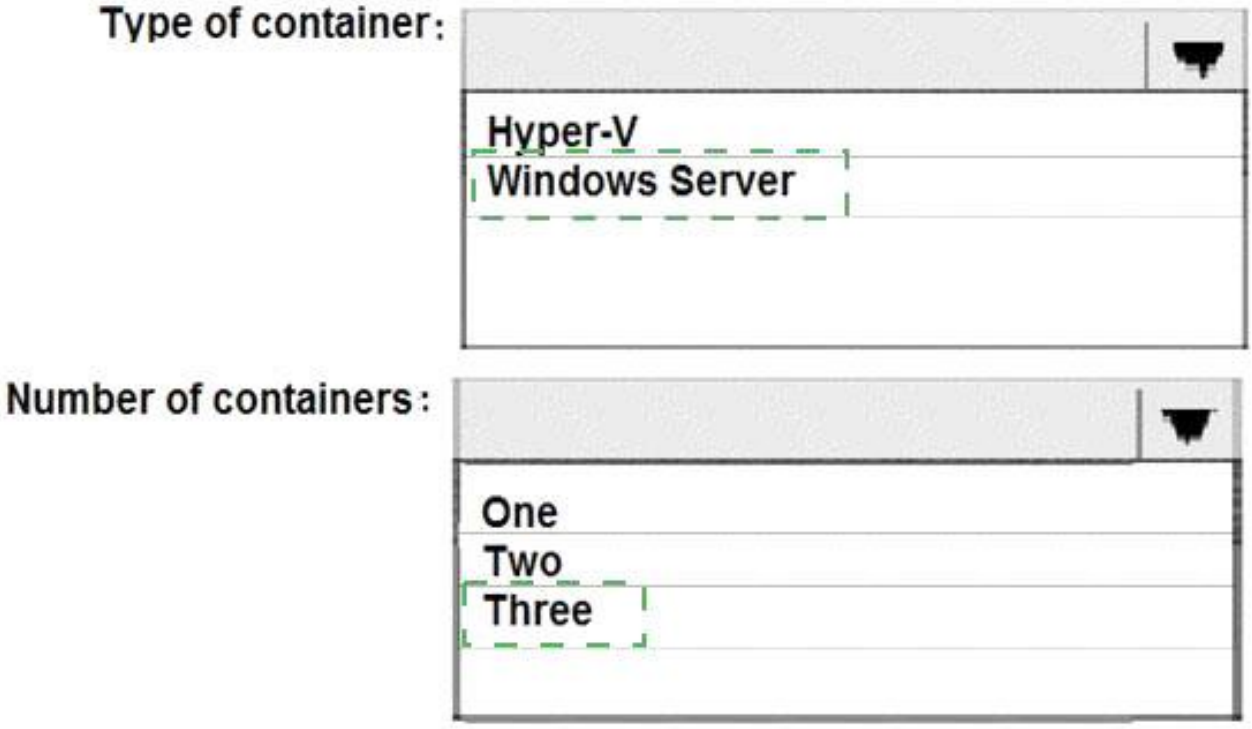
To create the EFS data recovery certificate:

- Certreq
- Certutil
- Cipher
- Efsui

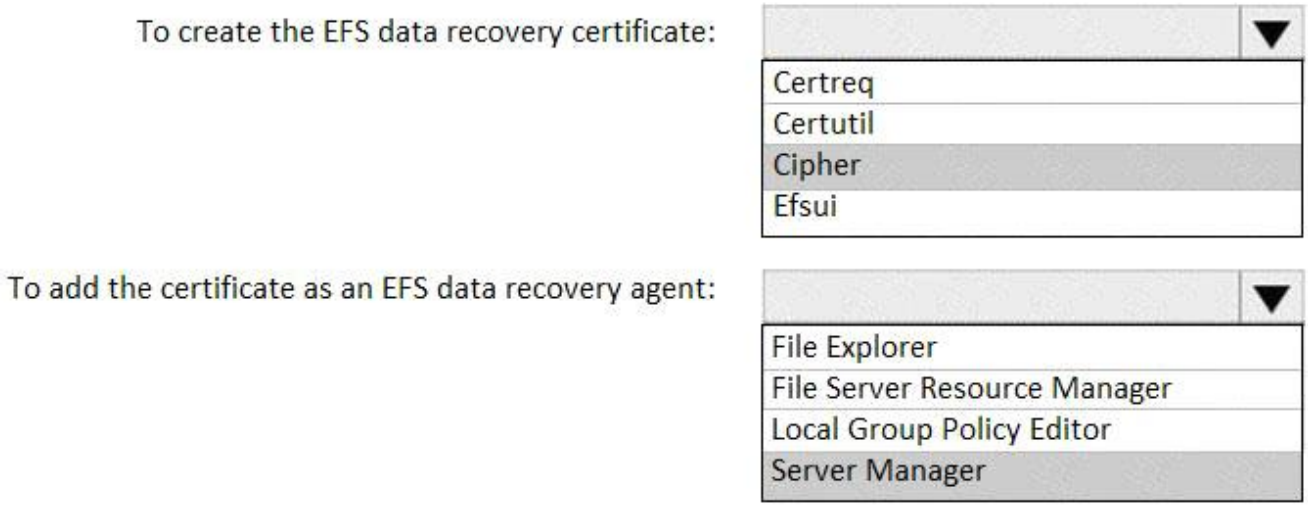
To add the certificate as an EFS data recovery agent:

- File Explorer
- File Server Resource Manager
- Local Group Policy Editor
- Server Manager

Answer:



Explanation



References:
https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/crea
https://www.rootusers.com/configure-efs-recovery-agent/

NO.9 Your network contains two Active Directory forests named contoso.com and adatum.com. Contoso.com contains a Hyper-V host named Server1. Server1 is a member of a group named HyperHosts. Adatum.com contains a server named Server2. Server1 and Server2 run Windows Server 2016.
Contoso.com trusts adatum.com.
You plan to deploy shielded virtual machines to Server1.
Which component should you install and which cmdlet should you run on Server1? To answer, select the appropriate options in the answer area.

Component to install on Server1:

The Active Directory Domain Services server role
The Host Guardian Hyper-V Support feature
The Host Guardian Service server role

Cmdlet to run on Server1:

Set-HgsClientConfiguration
Get-HgsAttestationBaselinePolicy
Export-HgsGuardian
Import-HgsGuardian

Answer:

Explanation

Component to install on Server1:

The Active Directory Domain Services server role
The Host Guardian Hyper-V Support feature
The Host Guardian Service server role

Cmdlet to run on Server1:

Set-HgsClientConfiguration
Get-HgsAttestationBaselinePolicy
Export-HgsGuardian
Import-HgsGuardian

Key for this question is Admin-trusted attestation or (AD mode) for guarded fabric "Server1.contoso.com", whileServer2.adatum.com is running the Host Guardian Service.

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

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

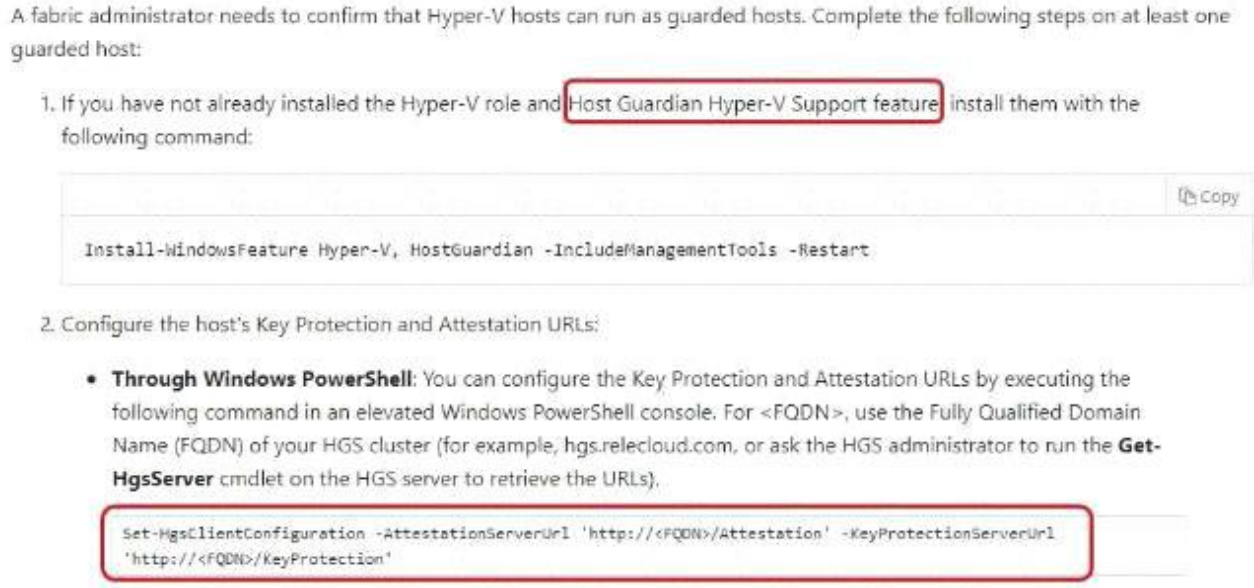
- **Operating system**: Windows Server 2016 Datacenter edition

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

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

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

https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabricconfi st-successfully


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

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

Copy

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

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

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

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

NO.10 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

Answer: B

Explanation
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 sessionconfiguration.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 groupmembership.The Get-PSSessionCapability cmdlet reduces complexity when auditing these endpoints by letting youdetermine 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

NO.11 Windows Firewall rules can be configured using PowerShell.
The "Set-NetFirewallProfile" cmdlet configures settings that apply to the per-profile configurations of the Windows Firewall with Advanced Security.
What is the default setting for the AllowInboundRules parameter when managing a GPO?

A. FALSE

B. NotConfigured

Answer: B

Explanation

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

NO.12 You have server named Server1.

You need to configured PowerShell logging to capture dynamic code generation. the solution must minimize the number of events that are logged.

What should you configured?

A. Script block logging

B. Module logging

C. System-wide transcription

D. Protected event logging

Answer: B

Explanation

References:

https://www.rootusers.com/enable-and-configure-module-script-block-and-transcription-logging-in-windows-po

NO.13 HOTSPOT

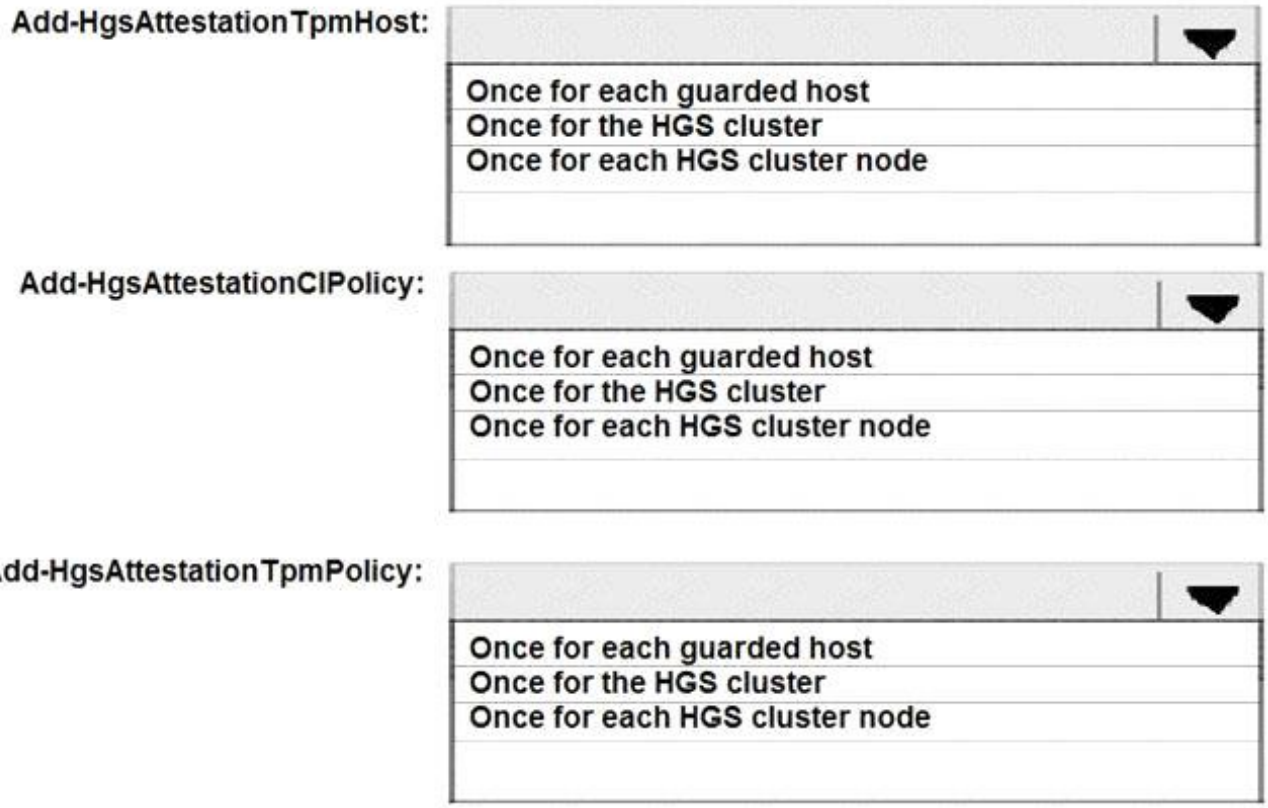
You plan to implement a guarded fabric in TPM-trusted attestation mode. The fabric will contain a three-node Host Guardian Service (HGS) cluster and four guarded hosts.

All the hosts will have matching hardware and will run the same workload.

You need to add the hosts to the HGS cluster.

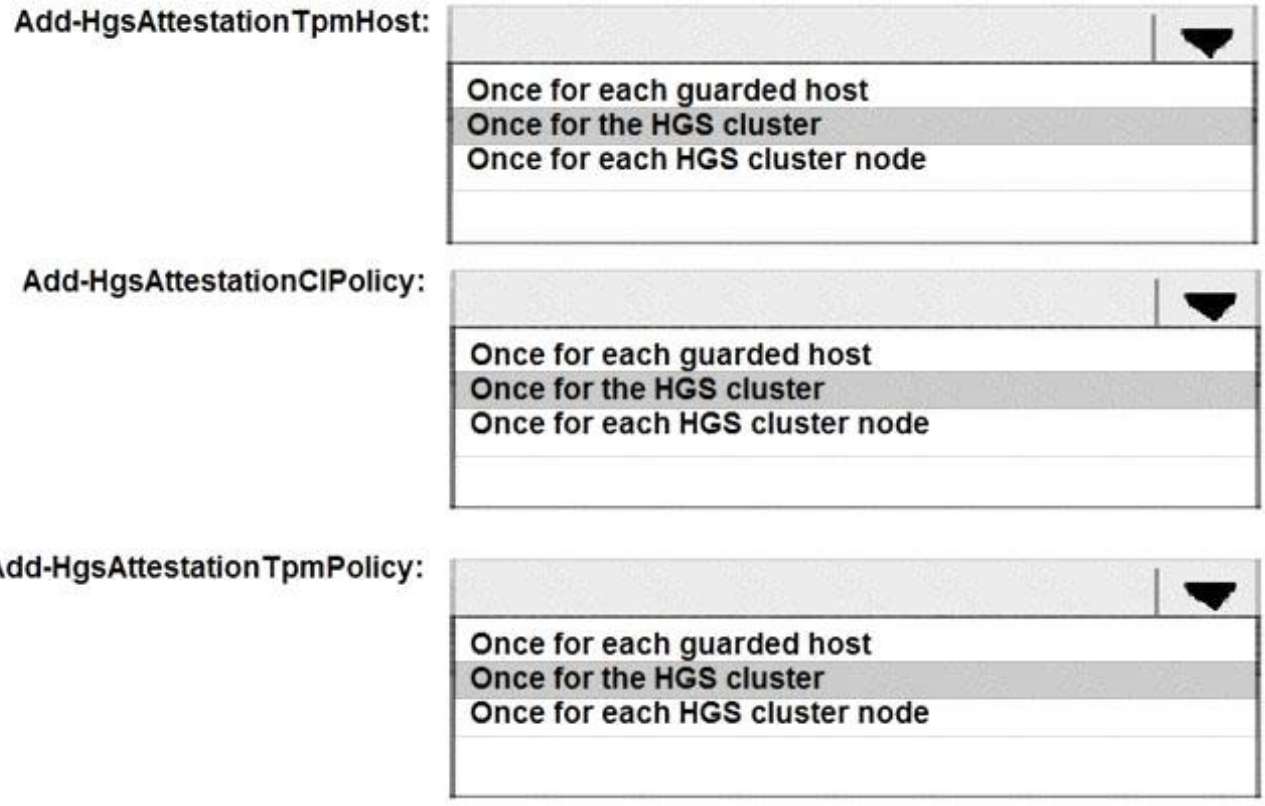
What is the minimum number of times you must run each cmdlet to implement the HGS cluster? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation



References:

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

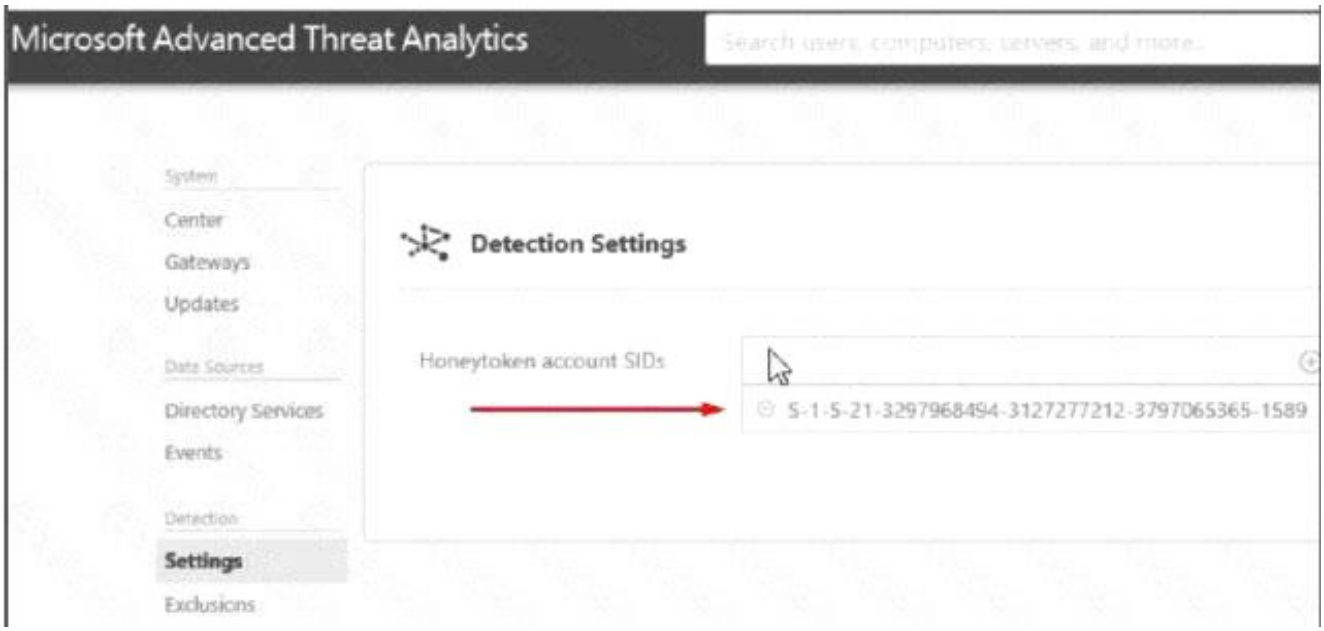
vm/guarded-fabric-tpm-

NO.14 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. Server4
B. Server3
C. Server2
D. Server1
Answer: A
Explanation
https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard-requirements Hardware and software requirementsTo provide basic protections against OS level attempts to read Credential Manager domain credentials, NTLMand Kerberos derived credentials, WindowsDefender 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)

NO.15 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 UPN of User1
B. the Globally Unique Identifier (GUID) of User1
C. the SID of User1
D. the SAM account name of User1
Answer: C
Explanation
https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-prerequisites
A user account of a user who has no network activities.This account is configured as the ATA Honeytoken user.To configure the Honeytoken user you need the SID of the user accoun



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 - anyauthentication associated with this (normally dormant)account will trigger an alert.

NO.16 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? To answer, select the appropriate options in the answer area.

Computers on which to review the event logs:	only client computers only domain controllers only member servers
Event logs to review:	Applications and Services Logs\Microsoft\Windows\Diagnostics-Networking\Operational Applications and Services Logs\Microsoft\Windows\NTLM\Operational Applications and Services Logs\Microsoft\Windows\SMCClient\Security Windows Logs\Security Windows Logs\System

Answer:

Answer Area

If Priv.User1 requests the Group1 PAM role at 07:00, **[answer choice].**

the request will be denied
Priv.User1 will be added to Group1 immediately
Priv.User1 will be added to Group1 as soon as the request is approved
Priv.User1 will be added to Group1 at 8:00

If Priv.User2 requests the Group1 PAM role at 09:00, **[answer choice].**

the request will be denied
Priv.User2 will be added to Group1 immediately
Priv.User2 will be added to Group1 as soon as the request is approved

Explanation

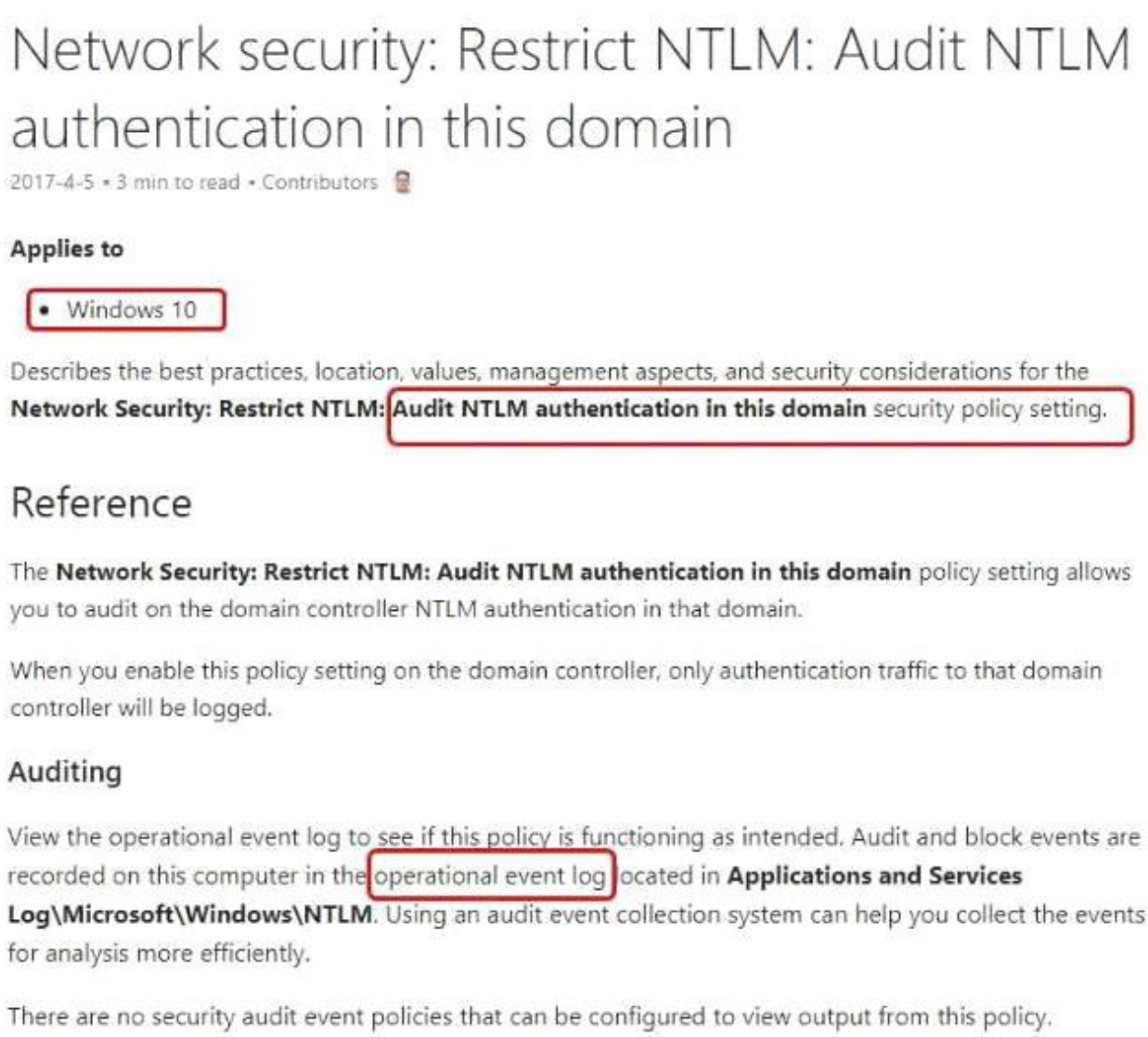
Computers on which to review the event logs:

only client computers
only domain controllers
only member servers

Event logs to review:

Applications and Services Logs\Microsoft\Windows\Diagnostics-Networking\Operational
Applications and Services Logs\Microsoft\Windows\NTLM\Operational
Applications and Services Logs\Microsoft\Windows\SMBClient\Security
Windows Logs\Security
Windows Logs\System

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 memberservers! See below for further information.
https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/network-security-restrict-ntlm this-domainVia lab testing, most of the NTLM audit logs are created on Windows 10 clients, except that you use WindowsServer 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.

NO.17 Read the following statement carefully and answer YES or NO.
You create a rule "Allow Everyone to run Windows except Registry Editor" that allows everyone in the organization to run Windows but does not allow anyone to run Registry Editor.
The effect of this rule would prevent users such as help desk personnel from running a program that is necessary for their support tasks.
To resolve this problem, you create a second rule that applies to the Helpdesk user group: "Allow Helpdesk to run Registry Editor." However, if you created a deny rule that did not allow any users to run Registry Editor, would the deny rule override the second rule that allows the Helpdesk user group to run Registry Editor?
A. NO
B. YES
Answer: B

NO.18 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows10.
The network uses the 172.16.0.0/16 address space.
Computer1 has an application named App1.exe that is located in D:\Apps\. App1.exe is configured to accept connections on TCP port 8080.
You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.
Solution: You run the New-NetFirewallRule -DisplayName "Rule1" -Direction Inbound -Program "D:\Apps\App1.exe" -Action Allow -Profile Domain command.
Does this meet the goal?

A. No

B. Yes

Answer: B

NO.19 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. Storage Explorer

B. Server Manager

C. Shared Folders

D. Disk Management

E. File Explorer

F. File Server Resource Manager (FSRM)

G. System Configuration

H. Computer Management

Answer: F

NO.20 Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1.
You implement the Host Guardian Service (HGS) configured for admin-trusted attestation.
You install the Hyper-V server role on Server1.
You need to add Server1 to the guarded hosts.
What should you do?

A. Install the Host Guardian Hyper-V Support feature on Server1 and add Server1 to a domain security group.

B. Install the Device Health Attestation server role on Server1 and add Server1 to a domain security group.

C. On Server1, install the Device Health Attestation server role and a computer certificate from a trusted certification authority (CA).

D. On Server1, install the Host Guardian Hyper-V Support feature and a computer certificate from a trusted certification authority (CA).

Answer: A

Explanation

References:

https://docs.microsoft.com/en-us/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-guarded-h

https://docs.microsoft.com/en-us/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-admin-tru