70-744 Q&As

Securing Windows Server 2016

Pass Microsoft 70-744 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4lead.com/70-744.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

You have 10 Hyper-V hosts that run Windows Server 2016.

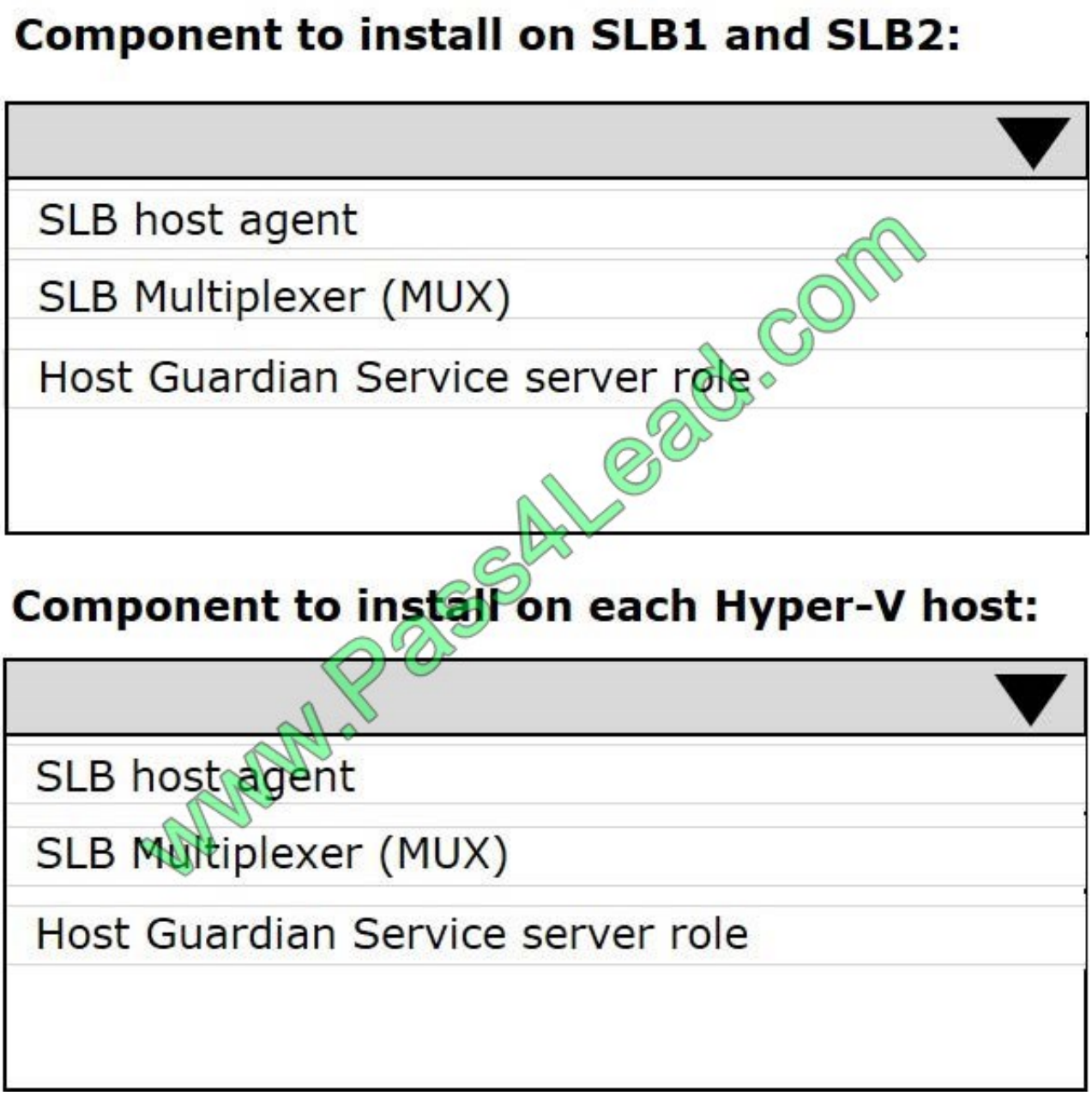
Each Hyper-V host has eight virtual machines that run a distributed web application named App1. You plan to implement a Software Load Balancing (SLB) solution for client access to App1.

You deploy two new virtual machines named SLB1 and SLB2.

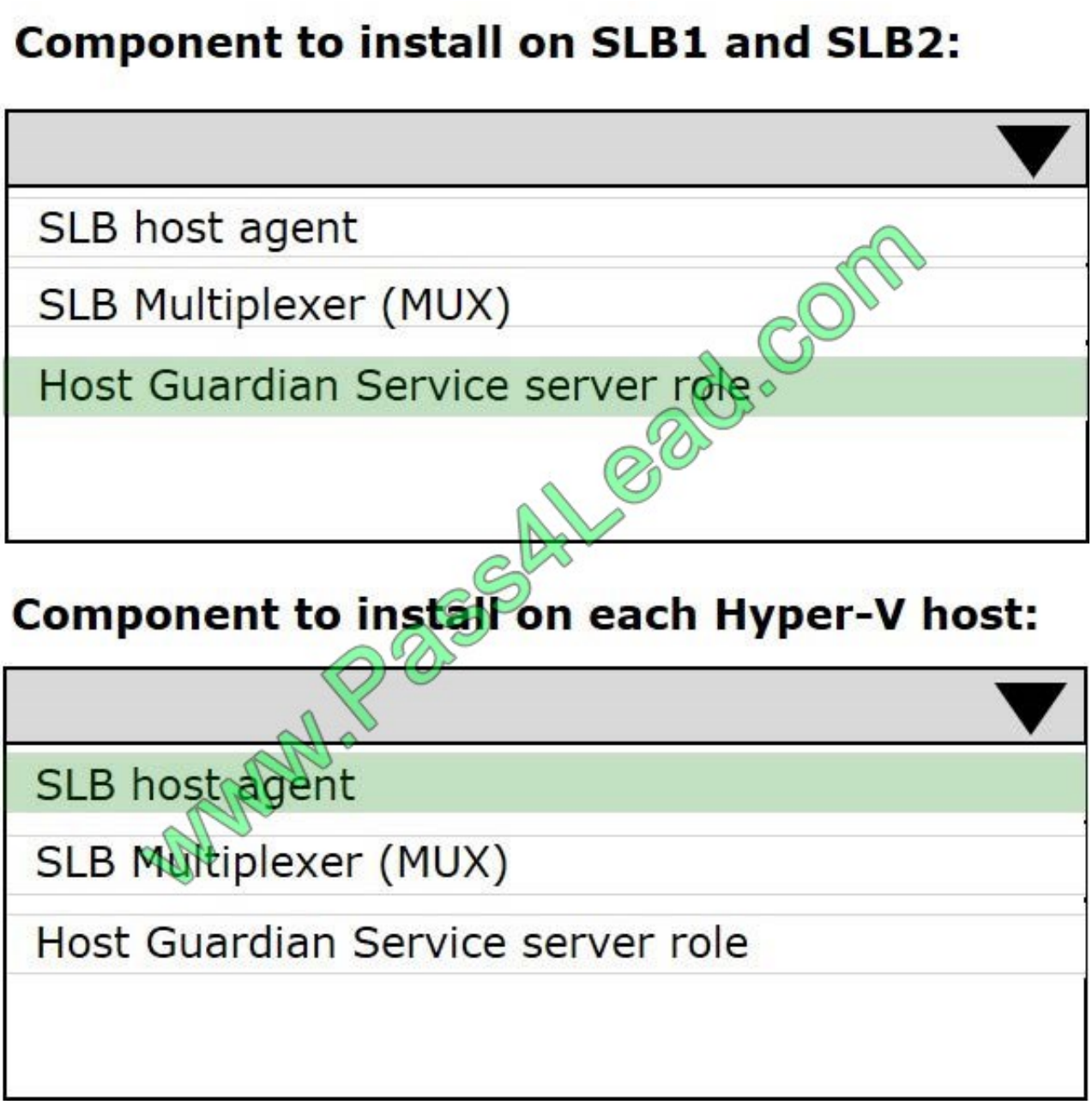
You need to install the required components on the Hyper-V hosts and the new servers for the planned implementation.

Which components should you install? Select the Appropriate in selection area.

Hot Area:



Correct Answer:

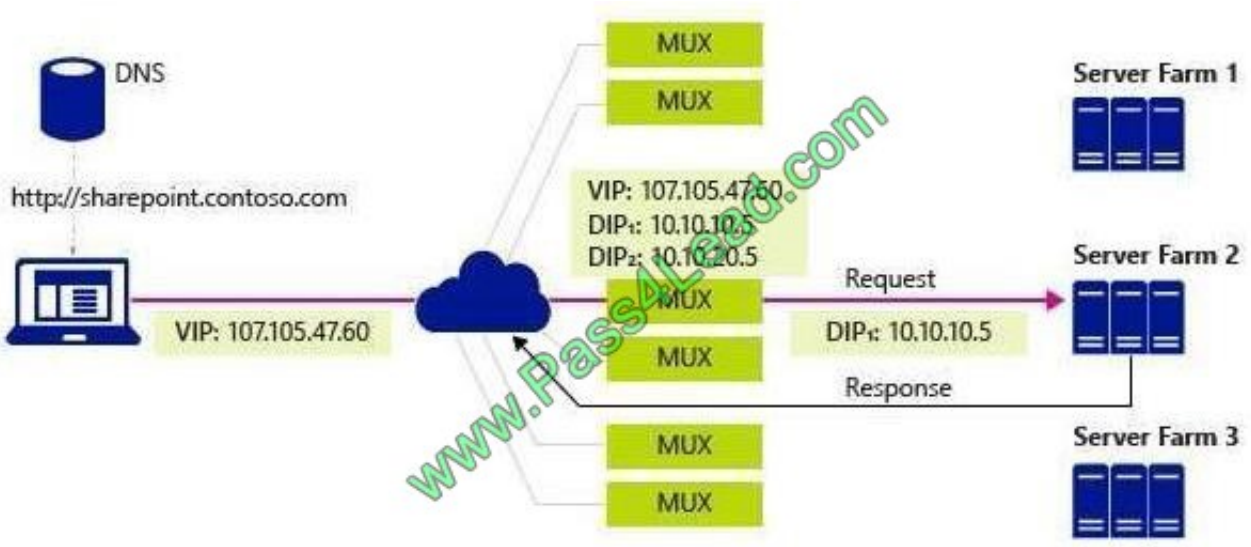


Component to install on SLB1 and SLB2: SLB Multiplexer (MUX)

Component to install on each Hyper-V host:SLB Host Agent

https://blogs.technet.microsoft.com/tip_of_the_day/2016/06/28/tip-of-the-day-demystifying-software-definednetworking-terms-the-components/ https://technet.microsoft.com/en-us/library/mt632286.aspxSLB Host Agent ?When you deploy SLB, you must use System Center, Windows PowerShell, or anothermanagement 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 processesinbound network traffic and maps VIPs (virtual IPs) toDIPs (datacenter IPs), then forwards the traffic to the correct DIP. Each MUX also uses BGP to publish VIProutes to edge routers. BGP Keep Alive notifies MUXeswhen a MUX fails, which allows active MUXes to redistribute the load in case of a MUX failure ?

essentiallyproviding load balancing for the load balancers.



QUESTION 2

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Serve1, that runs Windows Server 2016.

A technician is testing the deployment of Credential Guard on Server1.

You need to verify whether Credential Guard is enabled on Server1.

What should you do?

A. From a command prompt fun the credwiz.exe command.

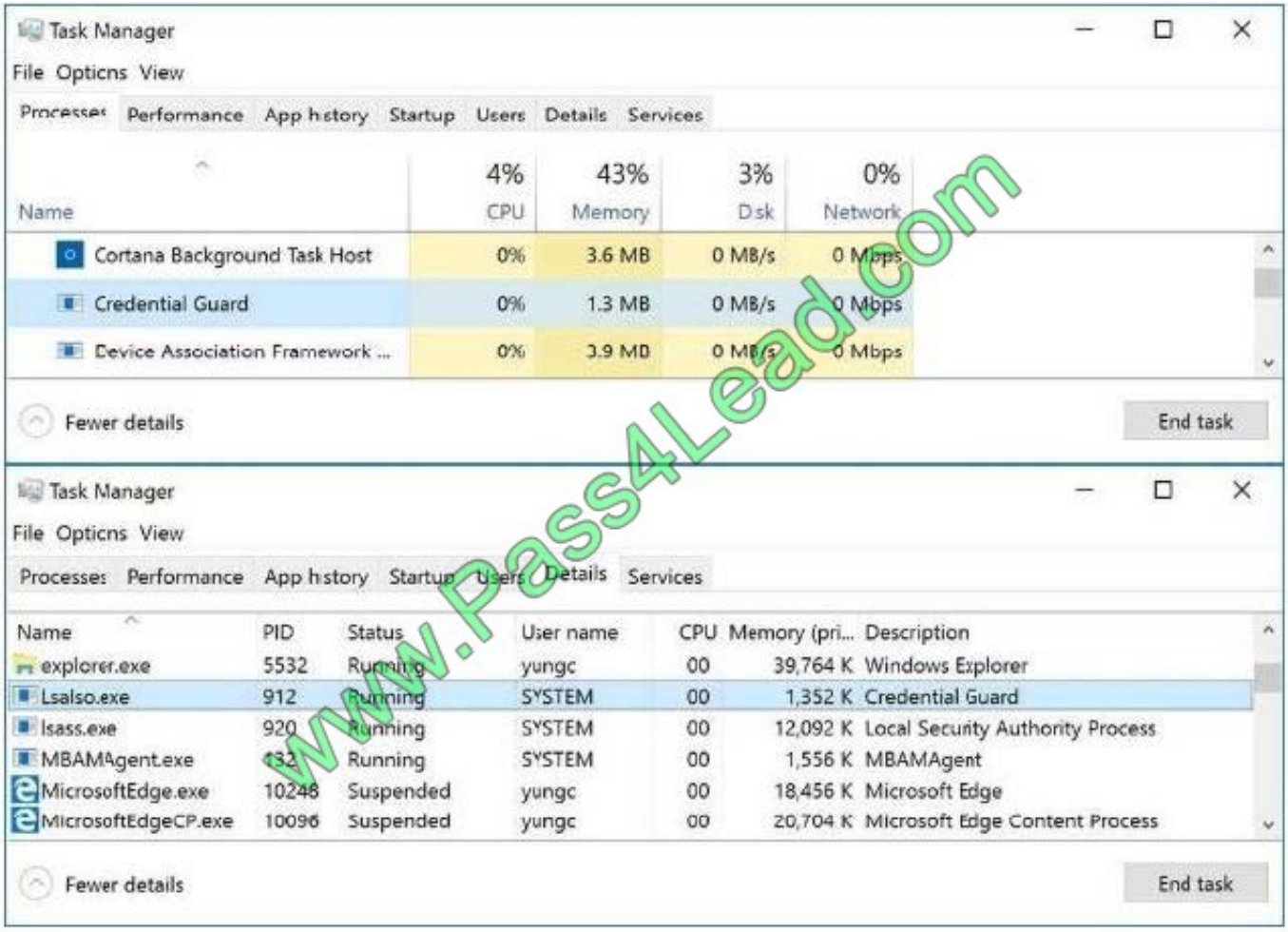
B. From Task Manager, review the processes listed on the Details tab.

C. From Server Manager, click Local Server, and review the properties of Server!

D. From Windows PowerShell, run the Get-WsManCredSSP cmdlet.

Correct Answer: B

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 Detailspage as below.



QUESTION 3

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

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

You need to prevent NTLM authentication on Server1.

Solution: From a Group Policy, you configure the Kerberos Policy. Does this meet the goal?

A. Yes

B. No

Correct Answer: B

References: https://www.rootusers.com/implement-ntlm-blocking-in-windows-server-2016/

QUESTION 4

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

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-guardRemote Credential Guard requirementsTo use Windows Defender Remote Credential Guard, the Remote Desktop client and remote host must meetthe 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-incredentials. This requires the user\\'s account be able tosign in to both the client device and the remote host.Must be running the Remote Desktop Classic Windows application. The Remote Desktop Universal WindowsPlatform application doesn\\'t support WindowsDefender Remote Credential Guard.Must use Kerberos authentication to connect to the remote host. If the client cannot connect to a domaincontroller, then RDP attempts to fall back to NTLM.Windows Defender Remote Credential Guard does not allow NTLM fallback because this would exposecredentials 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 5

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

https://technet.microsoft.com/en-us/library/cc720466%28v=ws.10%29.aspx?f=255and MSPPError=-2147217396 WSUSutil.exe is a tool that you can use to manage your WSUS server from the command line. WSUSutil.exeis located in the % drive%\\Program Files\\UpdateServices\\Tools folder on your WSUS server.You can run specific commands with WSUSutil.exe to perform specific functions, as summarized in thefollowing 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.
moveconten t	Changes the file system location where the WSUS server stores update files, and optionally copies any update files from the old location to the new location	• Hard drive is full • Disk fails
reset	Checks that every update metadata row in the database has corresponding update files stored in the file system. If update files are missing or have been corrupted, WSUS downloads the update files again.	• After restoring the WSUS database. • When troubleshooting

QUESTION 6

Encryption-supported VMs are intended for use where the fabric administrators are fully trusted.

For example, an enterprise might deploy a guarded fabric in order to ensure VM disks are encrypted at-rest for compliance purposes.

Shielded VMs are intended for use in fabrics where the data and state of the VM must be protected from both fabric administrators and untrusted software that might be running on the Hyper-V hosts.

Is the Virtual Machine Connection (Console), HID devices (e.g. keyboard, mouse) ON or OFF for Encryption Supported VM\\'s?

A. Off

B. On

Correct Answer: B

QUESTION 7

Your network contains an Active Directory domain named contoso.com. The domain contains a DNS server named Server1 that runs Windows Server 2016.

A domain-based Group Policy object (GPO) is used to configure the security policy of Server1.

You plan to use Security Compliance Manager (SCM) 4.0 to compare the security policy of Server1 to the WS2012 DNS Server Security 1.0 baseline.

You need to import the security policy into SCM. What should you do first?

A. From Security Configuration and Analysis, use the Export Template option.

B. Run the Copy-GPO cmdlet and specify the -TargetName parameter.

C. Run the Backup-GPO cmdlet and specify the -Path parameter.

D. Run the secedit.exe command and specify the/export parameter.

Correct Answer: C

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 issuitable to import to SCM 4.0

QUESTION 8

Name	Configuration
Server1	Host Guardian Service (HGS)
Server2	Host Guardian Service (HGS)
Server3	Host Guardian Service (HGS)
Server4	Hyper-V host
Server5	Hyper-V host

You have a guarded fabric that consists of the servers shown in the following table.

You need to ensure that you can start the shielded virtual machines on the Hyper-V hosts if the Hyper-V hosts cannot connect to the HGS. What should you do?

A. On Server1, run Set-HgsKeyProtectionConfiguration.

B. On Server1, Server2, and Server3, configure admin-trusted attestation.

C. On Server1, run Set-HgsKeyProtectionAttestationSignerCertificatePolicy.

D. On Server4, and Server5, disable the heartbeat integration service on the shielded virtual machines.

Correct Answer: B

https://docs.microsoft.com/en-us/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-admin-trusted-attestation-creating-a-security-group

QUESTION 9

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

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 aUser.

QUESTION 10

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

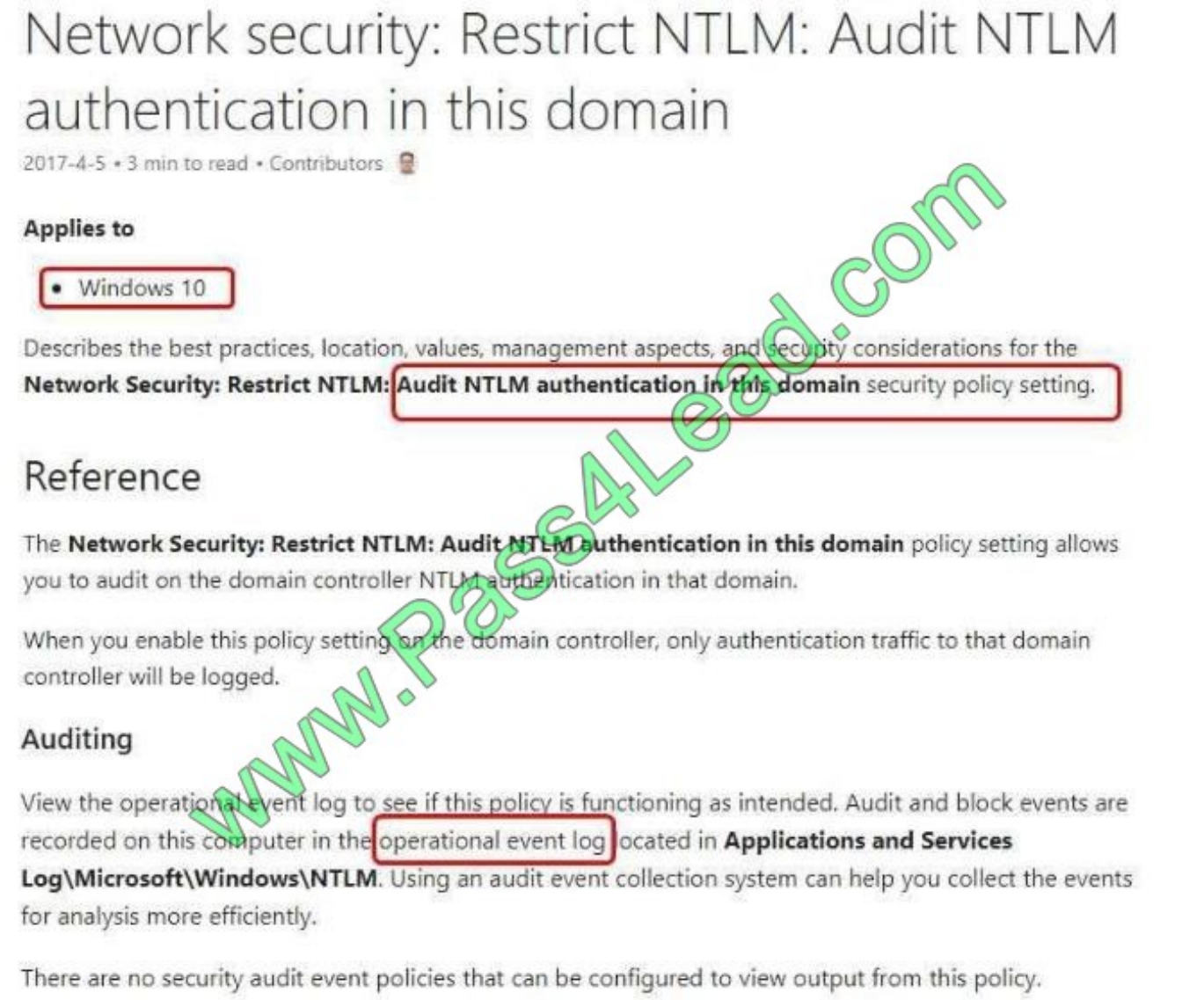
F. Event logs to review: Applications and Services Logs\\Microsoft\\Windows\\SMBClient\\Security

G. Event logs to review: Windows Logs\\Security

H. Event logs to review: Windows Logs\\System

Correct Answer: AE

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-ntlmaudit-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 11

Note: This question b part of a series of questions that use the same or simitar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains an Active Directory domain named contoso.com The domain contains a server named Server1 that runs Windows Server 2016.

Server1 has a shared folder named Share1.

You need to ensure that all access to Share1 uses SMB Encryption.

Which tool should you use?

A. File Explorer

B. Shared Folders

C. Server Manager

D. Disk Management

E. Storage Explorer

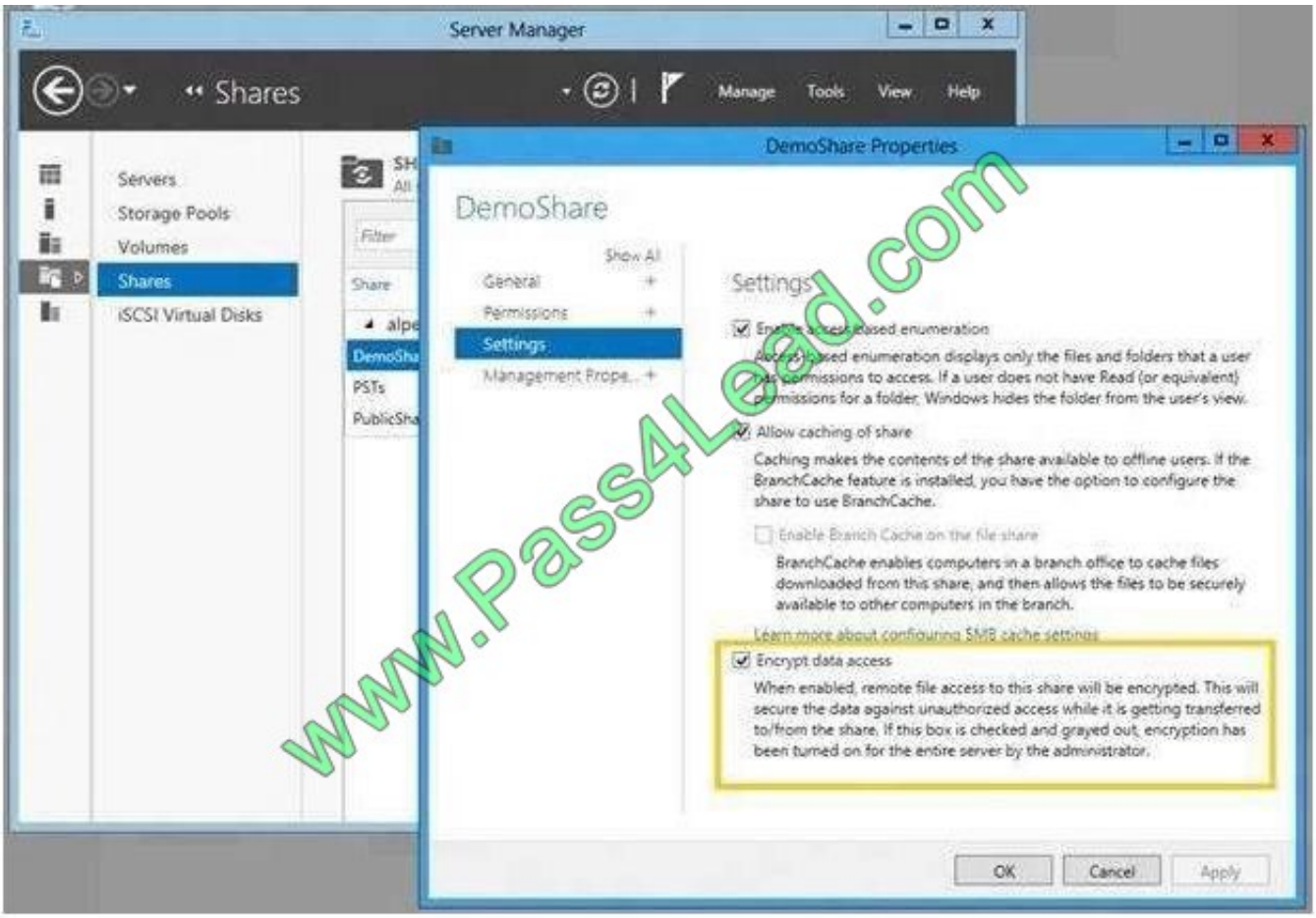
F. Computer Management

G. System Configuration

H. File Server Resource Manager (FSRM)>

Correct Answer: C

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



QUESTION 12

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

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.

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.pass4lead.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: