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.geekcert.com/70-744.html

100% Passing Guarantee
100% Money Back Assurance

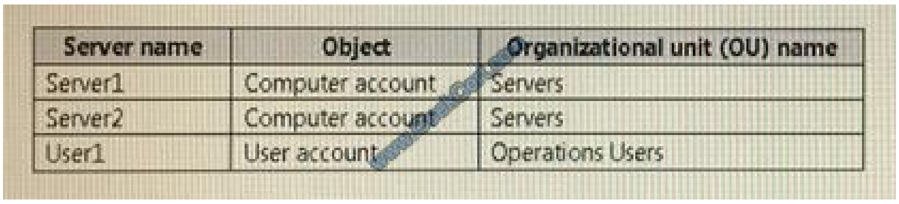
Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

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

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

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2016. All client computers run Windows 10. The relevant objects in the domain are configured as shown in the following table.



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

You need to assign User1 the right to restore files and folders on Server1 and Server2. Solution: You create a Group Policy object (GPO), you link the GPO to the Servers OU, and then you modify the Users Rights Assignment in the GPO. Does this meet the goat?

A. Yes

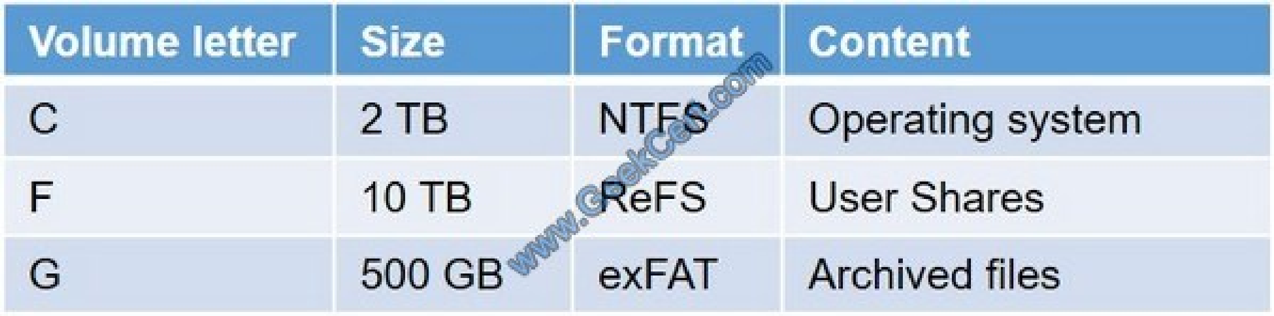
B. No

Correct Answer: B

References: https://technet.microsoft.com/en-us/library/cc771990(v=ws.11).aspx

QUESTION 2

Your network contains an Active Directory domain named contoso.com. You plan to implement encryption on a file server named Server1. Server1 has TPM 2.0 and uses Secure Boot Server1 has the volumes configured as shown in the



Volume letter	Size	Format	Content
C	2 TB	NTFS	Operating system
F	10 TB	ReFS	User Shares
G	500 GB	exFAT	Archived files

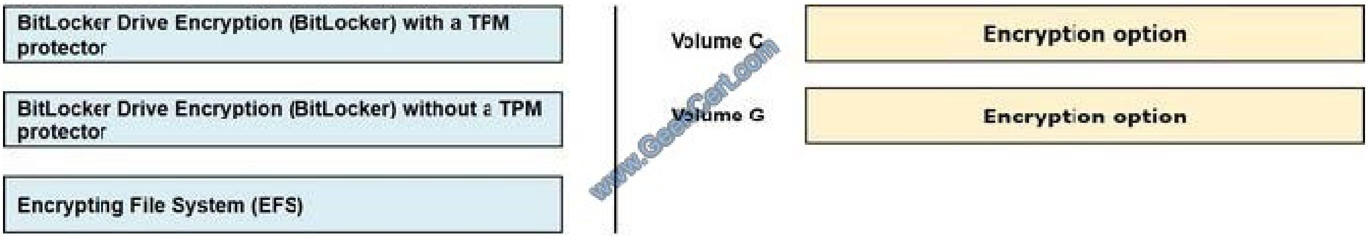
following table.

You need to encrypt the contents of volumes C and G. The solution must use the highest level of security possible.

What should you use to encrypt the contents of each volume? To answer, drag the appropriate encryption options to the correct volumes. Each encryption option may be used once, more than once, or not at all. You may need to drag the split

bar between panes or scroll to view content.

Select and Place:



BitLocker Drive Encryption (BitLocker) with a TPM protector

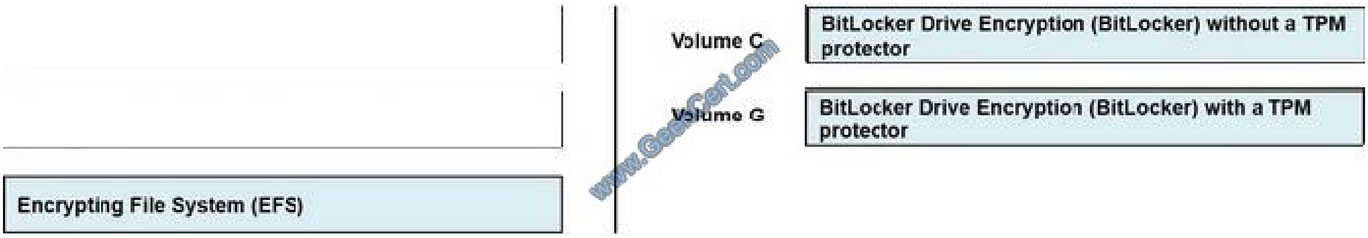
BitLocker Drive Encryption (BitLocker) without a TPM protector

Encrypting File System (EFS)

Volume C: Encryption option

Volume G: Encryption option

Correct Answer:



Encrypting File System (EFS)

Volume C: BitLocker Drive Encryption (BitLocker) without a TPM protector

Volume G: BitLocker Drive Encryption (BitLocker) with a TPM protector

QUESTION 3

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

You implement Local Administrator Password Solution (LAPS) on a member sever named Server1.

You need to retrieve the password of the local Administrator of Server1.

What should you do?

A. From Active Directory Administrative Center, view the content of the Password Settings Container.

B. Run the Get-ADComputerServiceAccount cmdlet

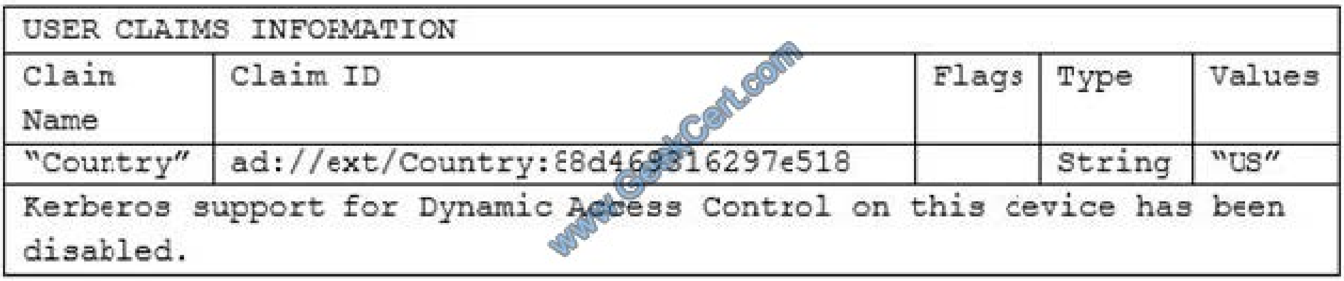
C. Run the Get-ADComputer cmdlet.

D. From Active Directory Administrative Center, view the attributes of the computer object of Server1.

Correct Answer: A

QUESTION 4

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				
Clain Name	Claim ID	Flags	Type	Values
"Courtry"	ad://ext/Country:£8d469816297e518		String	"US"
Kerberos support for Dynamic Access Control on this cevice has been disabled.				

Kerberos support for Dynamic Access Control on this device has been disabled.

You need to ensure that the security token of User1 has a claim for Job Title. What should you do?

A. From Windows PowerShell, run the New-ADClaimTransformPolicy cmdlet and specify the -Name parameter

B. From Active Directory Users and Computers, modify the properties of the User1 account.

C. From Active Directory Administrative Center, add a claim type.

D. From a Group Policy object (GPO), configure KDC support for claims, compound authentication, and Kerberos armoring.

Correct Answer: C

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 5

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one

correct solution, while others might not have a correct solution.

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

You deploy Windows Server 2016 to a server named Server1.

You need to ensure that you can run Windows Containers on Server1.

Solution: On server1, you install the DockerMsftProvider PowerShell and the Docker package. You restart the server.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

https://docs.microsoft.com/en-us/virtualization/windowscontainers/deploy-containers/deploy-containers-on-server

QUESTION 6

Your network contains an Active Directory domain named contoio.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 Served1.

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 is executed successfully from Server1.

What should you do?

A. From Advanced Audit Policy in GPO1 configure auditing for directory service changes.

B. Run the (Get-Module ActiveDirectory).LogPipelineExecutionDetails - $false command.

C. Run the (Get-Module ArtiveDirectory).LogPipelineExecutionDetails = $true command.

D. From Advanced Audit Policy in GPO1 configure auditing for other privilege use events.

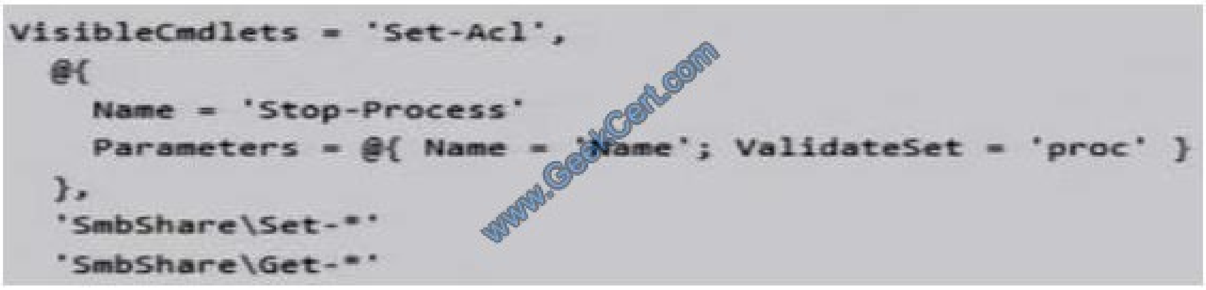
E. From Administrative Templates in GPO1, configure an Event Logging policy.

F. From Administrative Templates in GPO1, configure a Windows PowerShell policy.

Correct Answer: C

QUESTION 7

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.

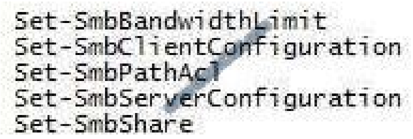
B. Modify the properties of any share.

C. Stop any process.

D. View the NTFS permissions of any folder.

Correct Answer: B

https://docs.microsoft.com/en-us/powershell/jea/role-capabilitiesFocus on the 3rd Visible Cmdlets in this question `SmbShare\\Set-*\\'The PowerShell "SmbShare" module has the following "Set-*" cmdlets, as reported by "Get-Command -ModuleSmbShare" 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 8

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:

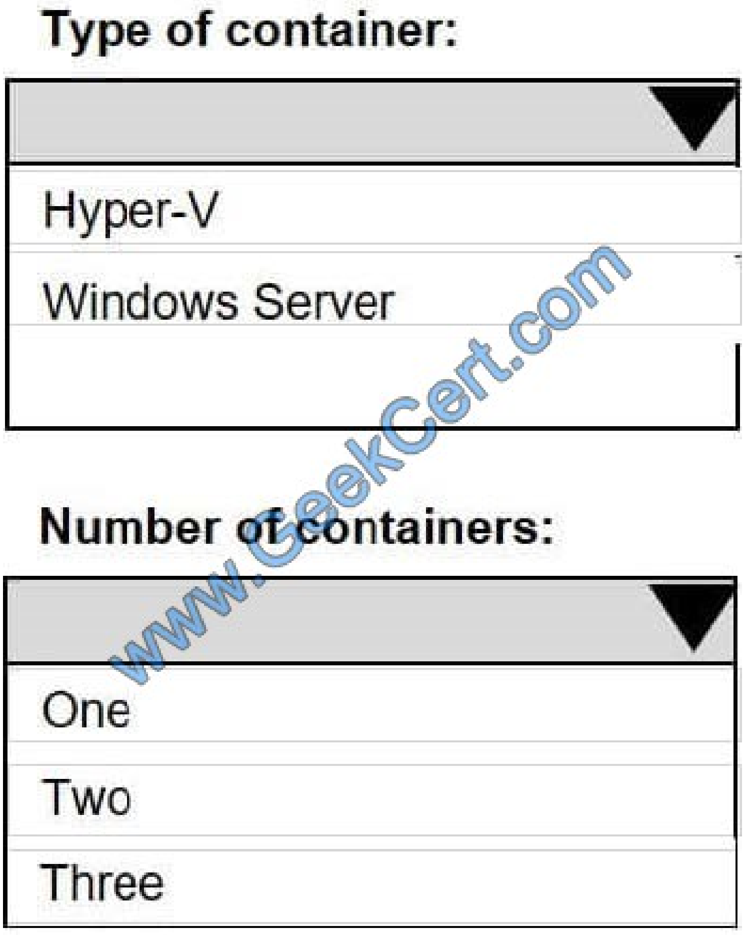
-be accessible by using a different IP address.

-have access to a unique file system.

-start as quickly as possible.

What should you recommend? To answer, select the appropriate options in the answer area.

Hot Area:



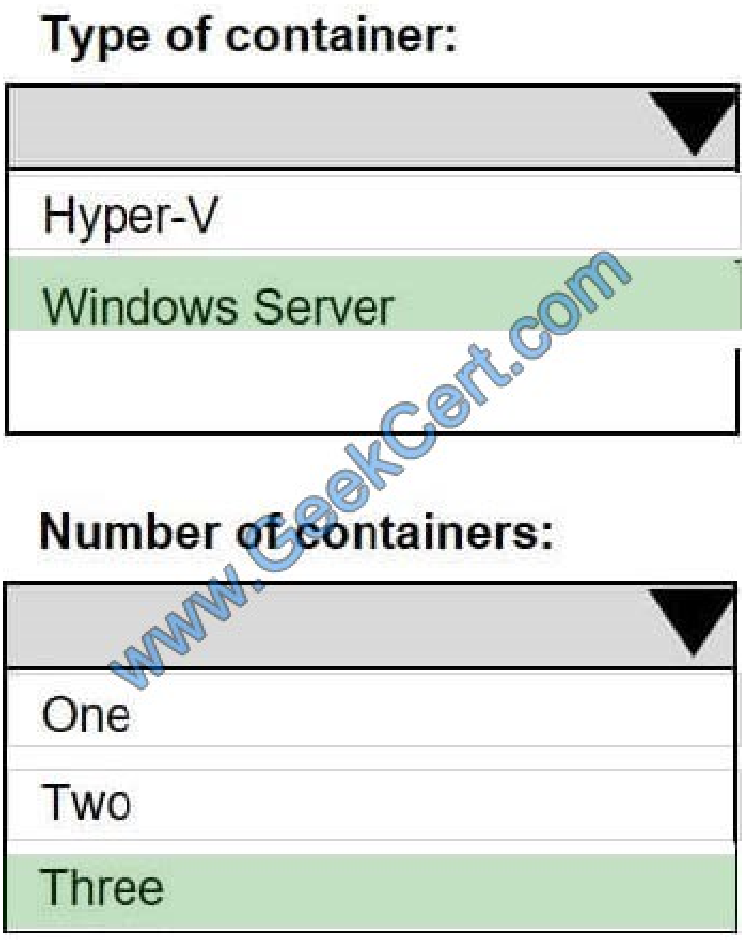
Type of container:

- Hyper-V
- Windows Server

Number of containers:

- One
- Two
- Three

Correct Answer:



Type of container:

Hyper-V

[✓ Windows Server]

Number of containers:

One

Two

[✓ Three]

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 samecomputer.

References:

https://docs.microsoft.com/en-us/dotnet/standard/modernize-with-azure-and-containers/modernize-existing-apps-to-cloud-optimized/deploy-existing-net-apps-as-windows-containers

https://blogs.msdn.microsoft.com/msgulfcommunity/2015/06/20/what-is-windows-server-containers-and-hyper-v-containers/

QUESTION 9

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

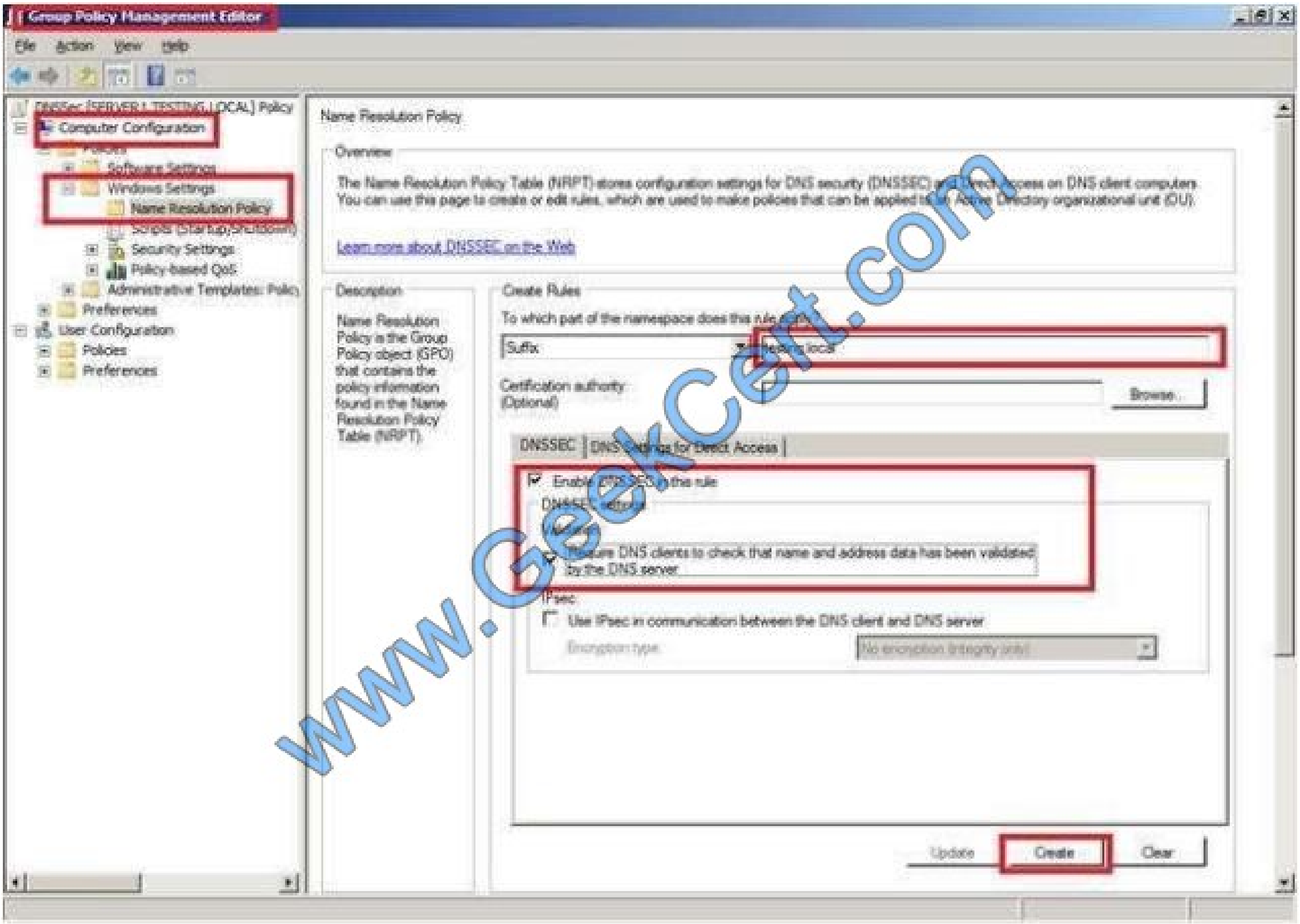
B. a zone transfer policy

C. a Name Resolution Policy Table (NRPT)

D. a connection security rule

Correct Answer: C

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



The Name Resolution Policy Table (NRPT) stores configuration settings for DNS security (DNSSEC) and DirectAccess on DNS client computers. You can use this page to create or edit rules, which are used to make policies that can be applied to an Active Directory organizational unit (OU).

Name Resolution Policy is the Group Policy object (GPO) that contains the policy information found in the Name Resolution Policy Table (NRPT).

To which part of the namespace does this rule apply? Suffix testing.local

Certification authority (Optional)

☑ Enable DNSSEC in this rule

DNSSEC settings

Validation

☑ Require DNS clients to check that name and address data has been validated by the DNS server

IPsec

☐ Use IPsec in communication between the DNS client and DNS server

Encryption type: No encryption (integrity only)

QUESTION 10

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

You are deploying Microsoft Advanced Threat Analytics (ATA).

You create a user named User1.

You need to configure the user account of User1 as a Honeytoken account.

Which information must you use to configure the Honeytoken account?

A. the SAM account name of User1

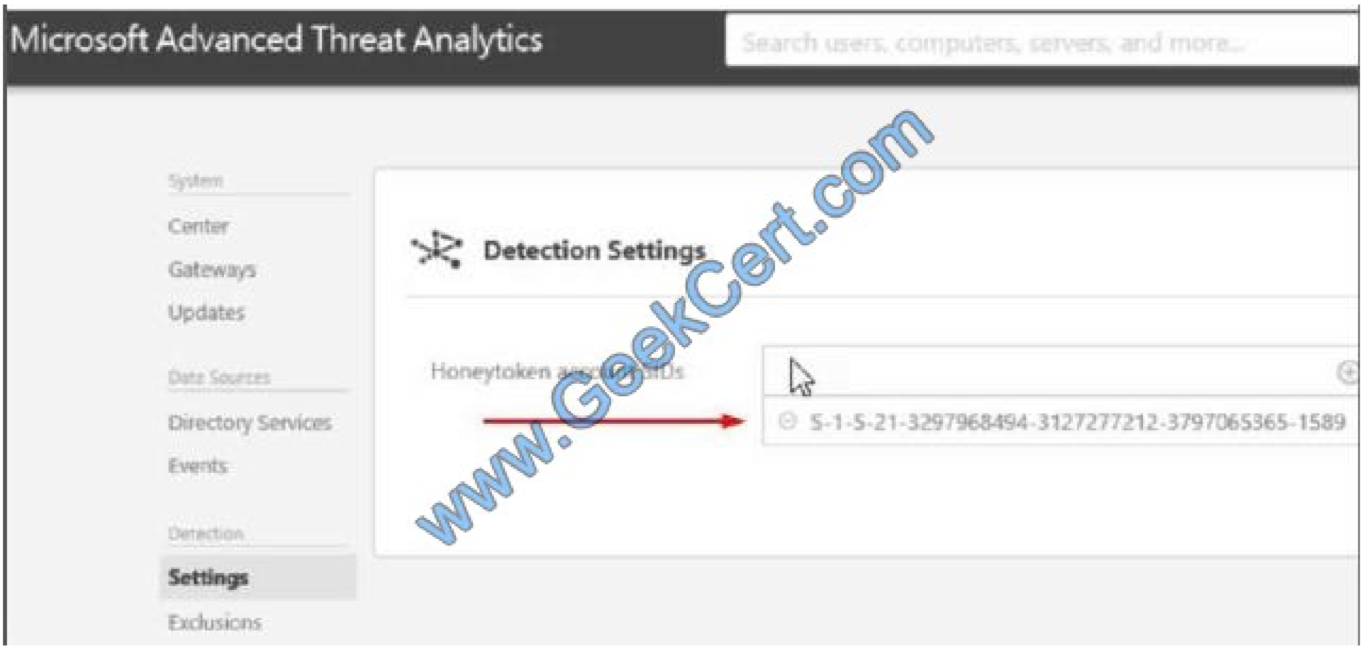
B. the Globally Unique Identifier (GUID) of User1

C. the SID of User1

D. the UPN of User1

Correct Answer: C

https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-prerequisitesA 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.



Honeytoken account SIDs

S-1-5-21-3297968494-3127277212-3797065365-1589

https://docs.microsoft.com/en-us/advanced-threat-analytics/install-ata-step7ATA 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.

QUESTION 11

Your network contains two Active Directory forests named contoso.com and adatum.com.

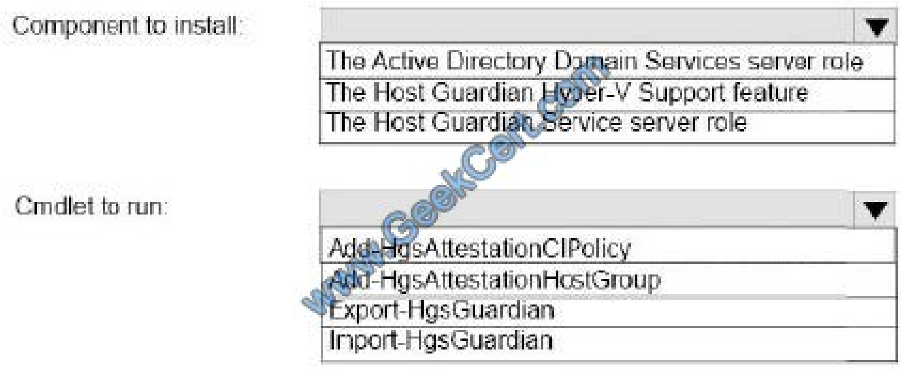
Contoso.com contains a Hyper-V host named Server1. Server1 is a member of a group named HyperHosts. Adatum.com contains a server named Server2. Server1 and Server2 run Windows Server 2016.

Contoso.com trusts adatum.com.

You plan to deploy shielded virtual machines to Server1 and to configure Admin-trusted attestation on Server2.

Which component should you install and which cmdlet should you run on Server2? To answer, select the appropriate options in the answer area.

Hot Area:



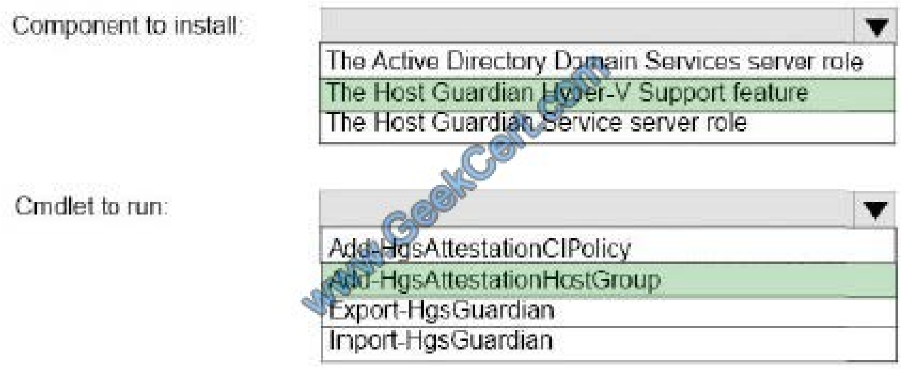
Component to install:

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

Cmdlet to run:

- Add-HgsAttestationCIPolicy
- Add-HgsAttestationHostGroup
- Export-HgsGuardian
- Inport-HgsGuardian

Correct Answer:



Component to install:

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

Cmdlet to run:

- Add-HgsAttestationCIPolicy
- Add-HgsAttestationHostGroup
- Export-HgsGuardian
- Inport-HgsGuardian

https://blogs.technet.microsoft.com/datacentersecurity/2016/03/16/windows-server-2016-and-host-guardian-service-for-shielded-vms/ https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabric-admin-trusted-attestation-creating-a-security-group

QUESTION 12

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

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

Your network contains an Active Directory forest named contoso.com. All servers run Windows Server 2016. The forest contains 2,000 client computers that run Windows 10. All client computers are deployed from a customized Windows

image.

You need to deploy 10 Privileged Access Workstations (PAWs). The solution must ensure that administrators can access several client applications used by all users.

Solution: You deploy 10 physical computers and configure them as virtualization hosts. You configure the operating system on each host as a PAW. You create a guest virtual machine by using the customized Windows image.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

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

QUESTION 13

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 a command prompt, run 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 Server1.

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

E. From a command prompt, run the tsecimp.exe command.

F. From Control Panel, open Credential Manager, and review the list of Windows Credentials.

Correct Answer: B

https://yungchou.wordpress.com/2016/10/10/credential-guard-made-easy-in-windows-10-version-1607/

QUESTION 14

You configure a server named Server1 to report to a Microsoft Azure Log Analytics workspace named Workspace1.

Several events are added to the System log on Server1.

You run queries in Workspace1, and no events are returned from Server1.

You confirm that Server1 reports to Workspace1.

You need to ensure that events from Server1 are sent to Workspace1.

What should you do?

A. From Azure Monitor, add a management solution.

B. On Server1, configure an event subscription.

C. In Workspace1, configure the Advanced settings.

D. On Server1, configure the Microsoft Monitoring Agent settings.

Correct Answer: D

QUESTION 15

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

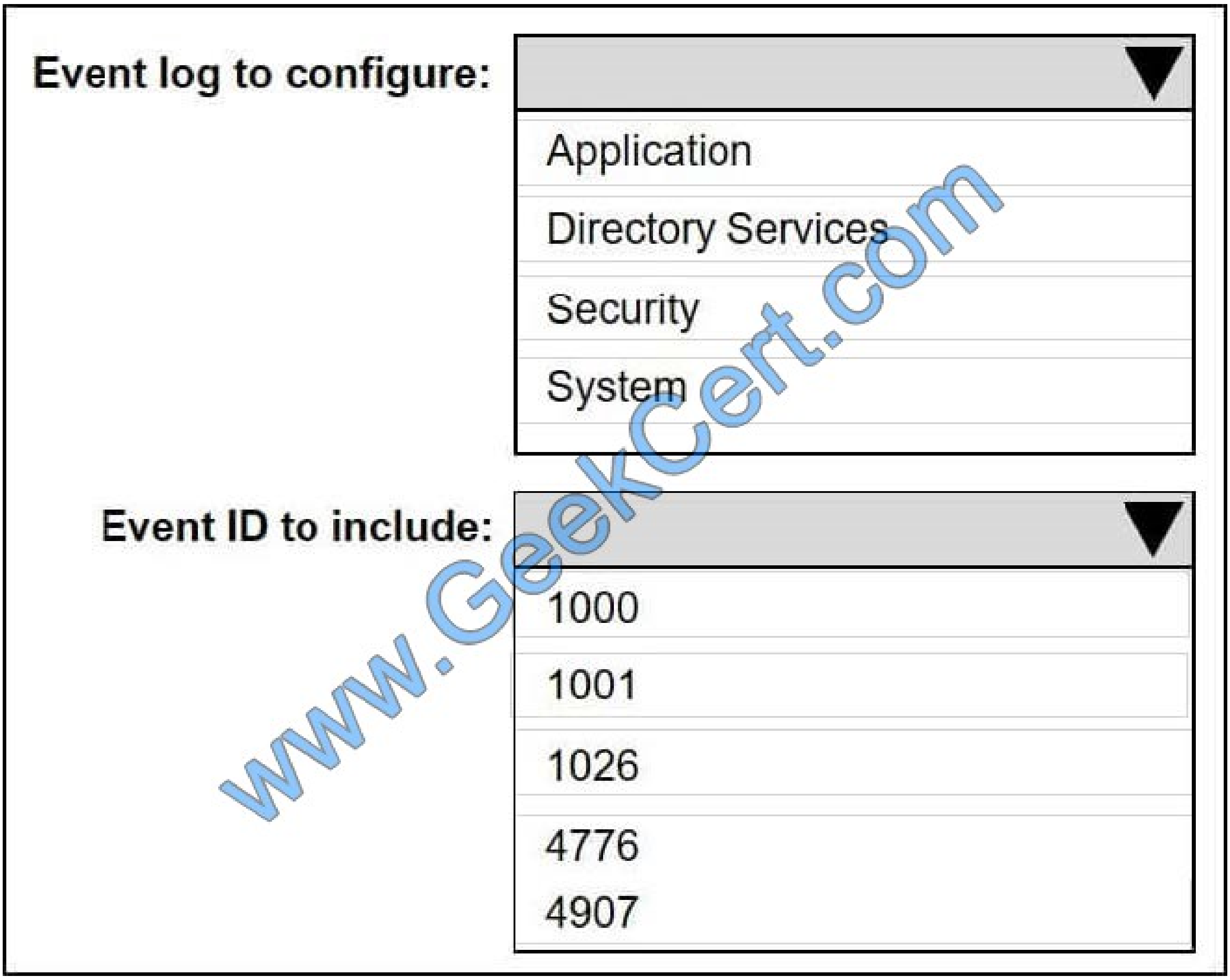
You are deploying Microsoft Advanced Threat Analytics (ATA) to the domain. You install the ATA Gateway on a server named Server1.

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? To answer, select the appropriate options in the answer are.

Hot Area:



Event log to configure: ▼

Application

Directory Services

Security

System

Event ID to include: ▼

1000

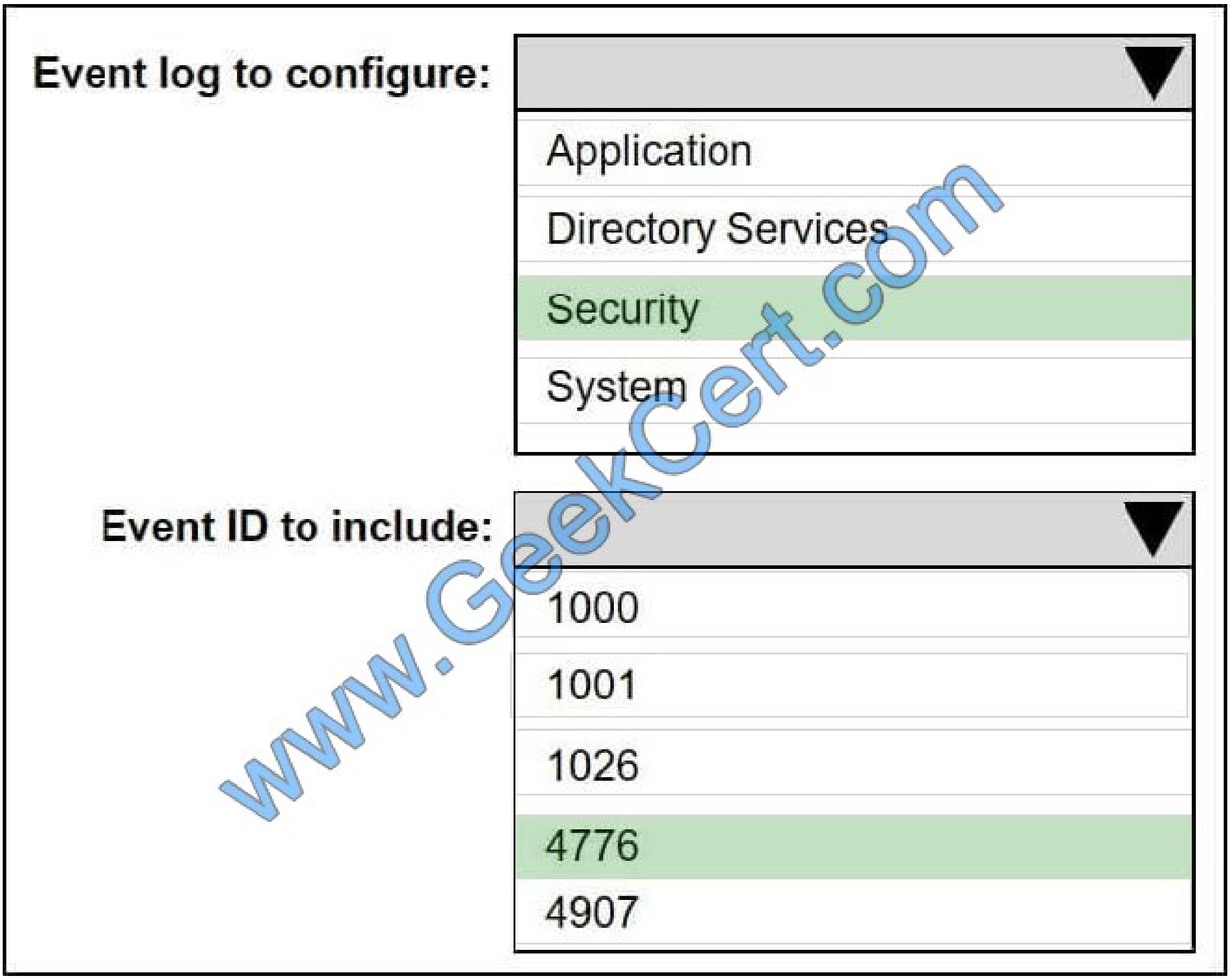
1001

1026

4776

4907

Correct Answer:



Event log to configure:

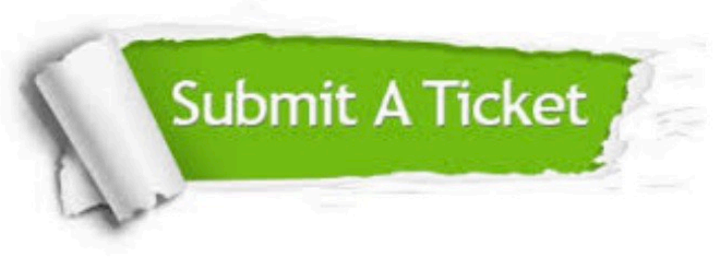
- Application
- Directory Services
- [✓ Security]
- System

Event ID to include:

- 1000
- 1001
- 1026
- [✓ 4776]
- 4907

https://docs.microsoft.com/en-us/advanced-threat-analytics/configure-event-collectionTo 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 LightweightGateway is not deployed,it can be forwarded to the ATA Gateway in one of two ways, by configuring the ATA Gateway to listen for SIEMevents or by configuring Windows Event Forwarding.

Event ID: 4776 NTLM authentication is being used against domain controllerEvent ID: 4732 A User is Added to Security-Enabled DOMAIN LOCAL Group,Event ID: 4733 A User is removed from Security-Enabled DOMAIN LOCAL GroupEvent ID: 4728 A User is Added or Removed from Security-Enabled Global Group Event ID: 4729 A User is Removed from Security-Enabled GLOBAL GroupEvent ID: 4756 A User is Added or Removed From Security-Enabled Universal GroupEvent ID: 4757 A User is Removed From Security-Enabled Universal Group


Submit A Ticket

100%