70-744.106q

Number: 70-744
Passing Score: 800
Time Limit: 120 min

70-744

Website: https://vceplus.com
VCE to PDF Converter: https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus

https://vceplus.com/

Securing Windows Server 2016

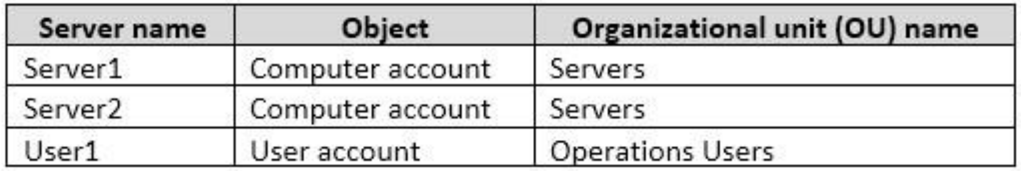
Exam A

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

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

The relevant objects in the domain are configured as shown in the following table.



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

You need to assign User1 the right to restore files and folders on Server1 and Server2.

Solution: You create a Group Policy object (GPO), link it to the Operations Users OU, and modify the Users Rights Assignment in the GPO.

https://vceplus.com/

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

VCEplus.com

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

QUESTION 2

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 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?

VCEplus.com

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/virtualization/windowscontainers/about/

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 multiple Hyper-V hosts.

VCEplus .com

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:
Explanation:

References: https://docs.microsoft.com/en-us/virtualization/windowscontainers/about/

VCEplus .com

QUESTION 4
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. 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 host all of the applications.

Does this meet the goal?

A. Yes

VCEplus.com

B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/virtualization/windowscontainers/about/

QUESTION 5
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.

VCEplus.com

What should you recommend?

A. Instruct all users to sign in to a client computer by using a Microsoft account.
B. 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.
C. Instruct all administrators to use a local Administrators account when they sign in to a client computer.
D. Move the computer accounts of the domain controllers to a new organizational unit (OU). Remove the permissions to the new OU from the Domain Admins group.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References:
https://en.wikipedia.org/wiki/Pass_the_hash#Mitigations

VCEplus.com

QUESTION 6

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

Correct Answer: BC
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:
Explanation:

References:
https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/hardware-software-requirements https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/planning-bastion-environment

QUESTION 7

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.

VCEplus.com

What should you tell User1 to do first on Server2?

A. From a command prompt, runntdsutil.exe.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://blogs.technet.microsoft.com/privatecloud/2014/05/14/just-enough-administration-step-by-step/

VCEplus.com

QUESTION 8
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 deploy a new server named FinanceServer5, and join FinanceServer5 to the domain.

You need to ensure that the passwords of the local administrators of FinanceServer5 are available to the LAPS administrators.

What should you do?

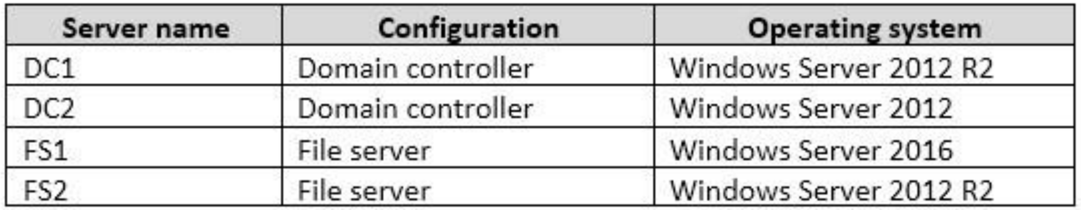
A. On FinanceServer5, register AdmPwd.dll.
B. On FinanceServer5, install the LAPS Windows PowerShell module.
C. In the domain, modify the permissions for the computer account of FinanceServer5.
D. In the domain, modify the permissions of the Domain Controllers organizational unit (OU).

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References:
https://gallery.technet.microsoft.com/Step-by-Step-Deploy-Local-7c9ef772

QUESTION 9
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.



Server name	Configuration	Operating system
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

You need to manage FS1 and FS2 by using Just Enough Administration (JEA).

What should you do before you can implement JEA?

A. Install Microsoft.NET Framework 4.6.2 on FS2.
B. Install Microsoft.NET Framework 4.6.2 on FS1.
C. Install Windows Management Framework 5.0 on FS2.
D. Upgrade DC1 to Windows Server 2016.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://blogs.technet.microsoft.com/privatecloud/2014/05/14/just-enough-administration-step-by-step/

QUESTION 10

VCEplus .com

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

Correct Answer: C
Section: (none)
Explanation

VCEplus .com

Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/hh852346(v=ws.11).aspx#BKMK_ConfigComputerGroups

QUESTION 11
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server5 that has the Windows Server Update Services server role installed.

You need to configure Windows Server Update Services (WSUS) on Server5 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: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/hh852346(v=ws.11).aspx#bkmk_3.5.ConfigSSL

QUESTION 12
Your network contains an Active Directory domain named contoso.com. The domain contains 1,000 client computers that run Windows 8.1 and 1,000 client computers that run Windows 10.

You deploy a Windows Server Update Services (WSUS) server. You create a computer group for each organizational unit (OU) that contains client computers. You configure all of the client computers to receive updates from WSUS.

You discover that all of the client computers appear in the Unassigned Computers computer group in the Update Services console.

You need to ensure that the client computers are added automatically to the computer group that corresponds to the location of the computer account in Active Directory.

Which two actions should you perform? Each correct answer presents part of the solution.

A. From Group Policy objects (GPOs), configure the Enable client-side targeting setting.
B. From the Update Services console, configure the Computers option.
C. From Active Directory Users and Computers, create a domain local distribution group for each WSUS computer group.
D. From Active Directory Users and Computers, modify the flags attribute of each OU.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References:
https://technet.microsoft.com/en-us/library/dd252762.aspx https://technet.microsoft.com/en-us/library/cc720433(v=ws.10).aspx **QUESTION 13**
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

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

Server1 has a volume named Volume1.

A central access policy named Policy1 is deployed to the domain.

You need to apply Policy1 to Volume1.

Which tool should you use?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/deploy-a-central-access-policy--demonstration-steps-#BKMK_1.4

VCEplus .com

QUESTION 14

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

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

Server1 has a shared folder named Share1.

You need to encrypt the contents to Share1.

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)

VCEplus .com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://msdn.microsoft.com/en-us/library/dd163562.aspx

QUESTION 15

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

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

Server1 has a shared folder named Share1.

VCEplus .com

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:
Explanation:

VCEplus

References: https://support.microsoft.com/en-za/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,windows-server-2008-r2,-windows-8,-and-windows-server-2012 https://blogs.technet.microsoft.com/filecab/2012/05/03/smb-3-security-enhancements-in-windows-server-2012/

QUESTION 16
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

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

VCEplus.com

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:
Explanation:

References: https://technet.microsoft.com/en-us/library/hh831434(v=ws.11).aspx

VCEplus.com

QUESTION 17
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

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

You need to create Work Folders on Server1.

Which tool should you use?

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

VCEplus .com

H. File Server Resource Manager (FSRM)

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

References:
https://blogs.technet.microsoft.com/canitpro/2015/01/19/step-by-step-creating-a-work-folders-test-lab-deployment-in-windows-server-2012-r2/
https://technet.microsoft.com/en-us/library/dn265974(v=ws.11).aspx

QUESTION 18
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

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

Server1 has a volume named Volume1.

VCEplus .com

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:
Explanation:

References:

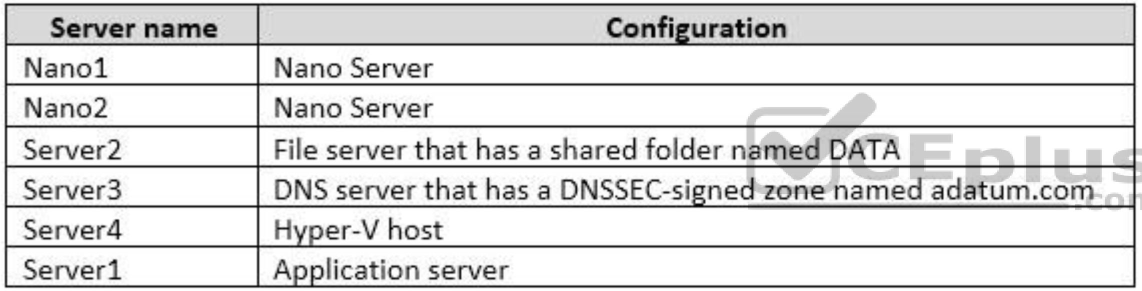
https://technet.microsoft.com/en-us/library/cc732431(v=ws.11).aspx

QUESTION 19

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.

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 execute D:\Folder1 on Nano1 from being scanned by Windows Defender.

Which cmdlet should you run?

A. Set-StorageSetting
B. Set-FsrmFileScreenException

C. Set-MpPreference
D. Set-DtcAdvancedSetting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

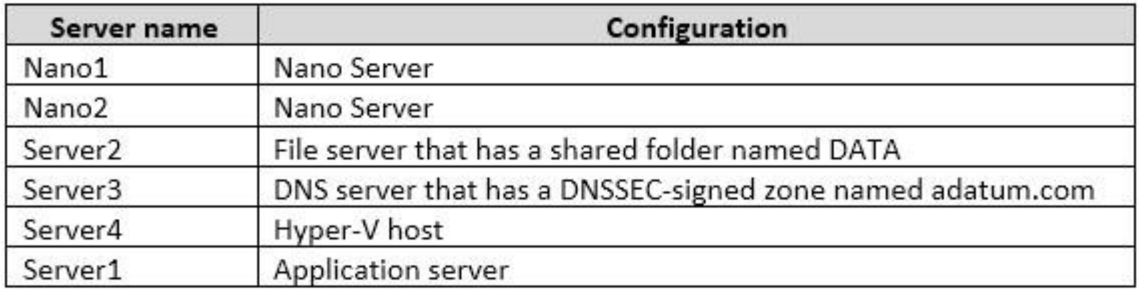
References: http://www.thomasmaurer.ch/2016/07/how-to-disable-and-configure-windows-defender-on-windows-server-2016-using-powershell/

QUESTION 20
HOTSPOT

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

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.

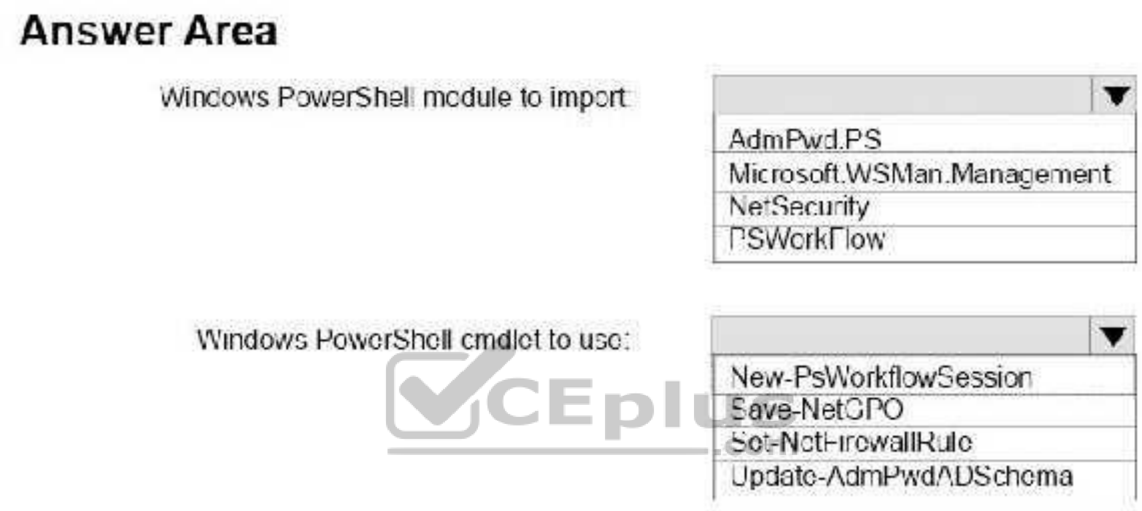
You have an organizational unit (OU) named Marketing that contains the computers in the marketing department. You have an OU named Finance that contains the computers in the finance department. You have an OU named AppServers that contains application servers. A Group Policy object (GPO) named GP1 is 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 you can implement the Local Administrator Password Solution (LAPS) for the finance department computers.

What should you do in the contoso.com forest? To answer, select the appropriate options in the answer area.

Hot Area:



Answer Area

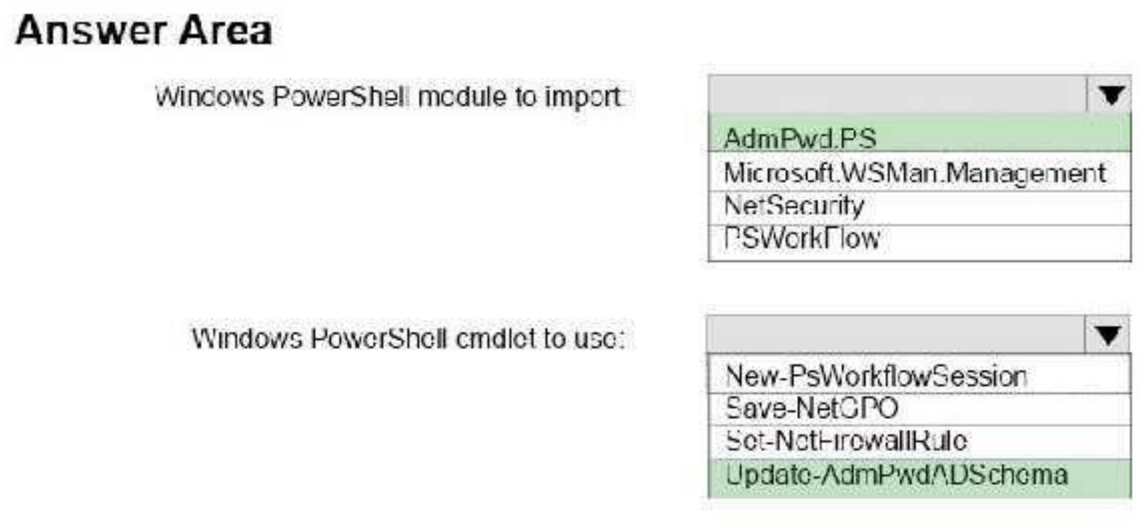
Windows PowerShell module to import

- AdmPwd.PS
- Microsoft.WSMan.Management
- NetSecurity
- PSWorkFlow

Windows PowerShell cmdlet to use:

- New-PsWorkflowSession
- Save-NetGPO
- Set-NetFirewallRule
- Update-AdmPwdADSchema

Correct Answer:



Answer Area

Windows PowerShell module to import:

- [✓ AdmPwd.PS]
- Microsoft.WSMan.Management
- NetSecurity
- PSWorkFlow

Windows PowerShell cmdlet to use:

- New-PsWorkflowSession
- Save-NetGPO
- Set-NetFirewallRule
- [✓ Update-AdmPwdADSchema]

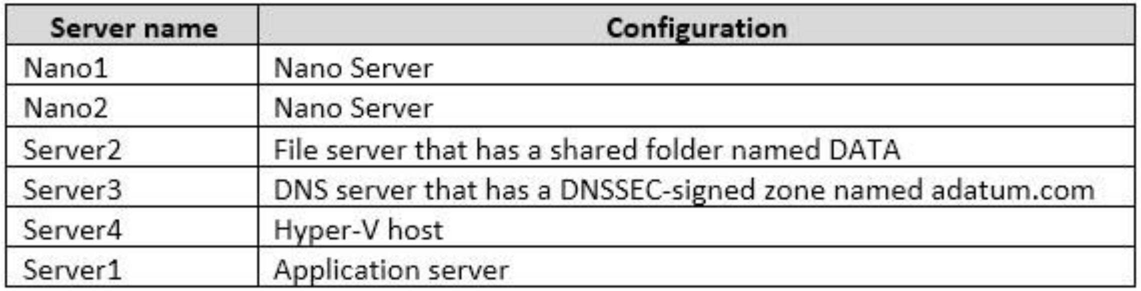
Section: (none)
Explanation

Explanation/Reference:
References: https://learn-powershell.net/2016/10/08/setting-up-local-administrator-password-solution-laps/

QUESTION 21
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.

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 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. DNS Client from Administrative Templates
D. Name Resolution Policy from Windows Settings

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/ee649182(v=ws.10).aspx

QUESTION 22

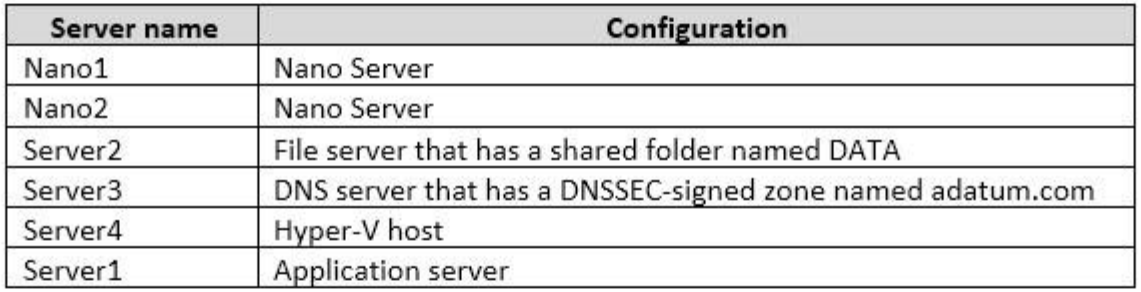
www.vceplus.com - Free Questions & Answers - Online Courses - Convert VCE to PDF - VCEplus.com

VCEplus .com

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.

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 you can deploy a shielded virtual machine to Server4.

Which server role should you deploy?

VCEplus .com

https://vceplus.com/

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

Correct Answer: D
Section: (none)
Explanation

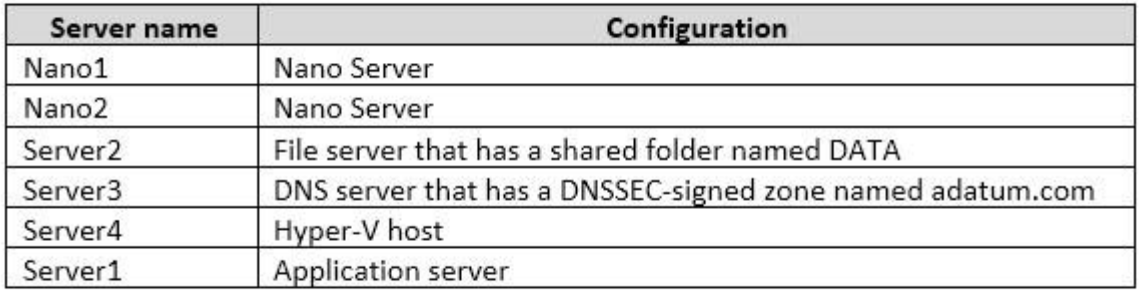
Explanation/Reference:
Explanation:

References: https://blogs.technet.microsoft.com/datacentersecurity/2016/03/16/windows-server-2016-and-host-guardian-service-for-shielded-vms/

QUESTION 23
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.

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

Correct Answer: D
Section: (none)
Explanation

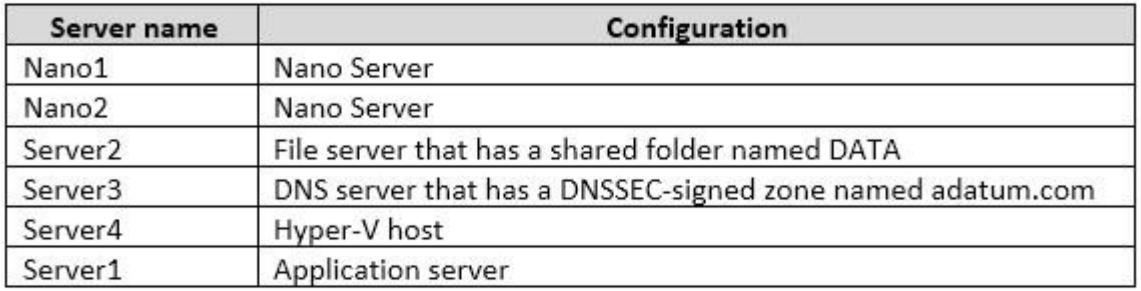
Explanation/Reference:
Explanation:

References:
https://support.microsoft.com/en-za/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,windows-server-2008-r2,-windows-8,-and-windows-server-2012

QUESTION 24
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.

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

VCEplus.com

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

Correct Answer: B
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/jj679890(v=ws.11).aspx#BKMK_rec3

QUESTION 25
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?

VCEplus.com

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
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/working-with-detection-settings

QUESTION 26
Your network contains an Active Directory domain named contoso.com.

You create a Microsoft Operations Management Suite (OMS) workspace.

VCEplus.com

You need to connect several computers directly to the workspace.

Which two pieces of information do you require? Each correct answer presents part of the solution.

A. the ID of the workspace
B. the name of the workspace
C. the URL of the workspace
D. the key of the workspace

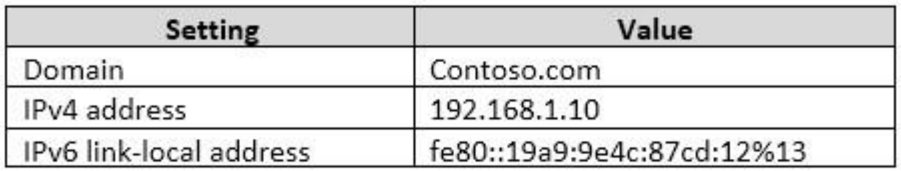
Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-windows-agents

QUESTION 27
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).

You need to install the ATA Center on Server1.

What should you do first?

A. Install Microsoft Security Compliance Manager (SCM).
B. Obtain an SSL certificate.
C. Assign an additional IPv4 address.D. Remove Server1 from the domain.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/install-ata-step1

QUESTION 28
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.

VCEplus .com

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:

QUESTION 29
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 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 enable the Containers feature, and then you install the PowerShell for Docker module. You restart the server.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 30

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 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 enable the Containers feature, and then you install the Hyper-V server role. You restart the server.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 31

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 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 enable the Containers feature, and then you restart the server.

VCEplus.com

Does this meet the goal?

A. Yes

B. No

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 32
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.

VCEplus.com

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

QUESTION 33

VCEplus .com

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

VCEplus .com

QUESTION 34
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 Windows PowerShell, you run the **New-ADAuthenticationPolicy** cmdlet.

Does this meet the goal?

A. Yes
B. No

VCEplus.com

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 35
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

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

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.

VCEplus.com

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:
References: https://4sysops.com/archives/file-server-resource-manager-fsrm-part-3-quota-management/

QUESTION 36

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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/system-center/vmm/guarded-deploy-host?toc=/windows-server/virtualization/ https://docs.microsoft.com/en-us/windows-server/get-started/deploy-nano-server

QUESTION 37

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. the Windows Biometric Framework (WBF)
C. VM Shielding Tools for Fabric Management
D. BitLocker Network Unlock

VCEplus.com

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabricguarded-host-prerequisites

QUESTION 38
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. Create an event subscription
B. Create a Data Collector-Set
C. Install Microsoft Monitoring Agent on Server1
D. Join Server1 to the domain

VCEplus.com

Correct Answer: C
Section: (none)
Explanation

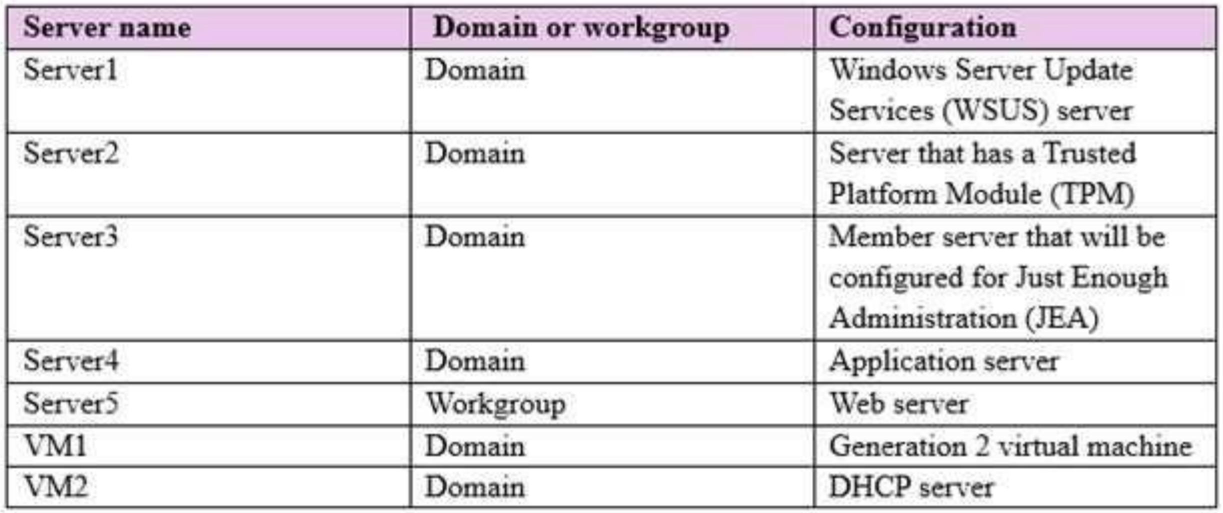
Explanation/Reference:
References: https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-windows-agents

QUESTION 39
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 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/Windows PowerShell
B. Windows Logs/Security
C. Applications and Services Logs/Microsoft/Windows/PowerShell/Operational
D. Windows Logs/Application

Correct Answer: C

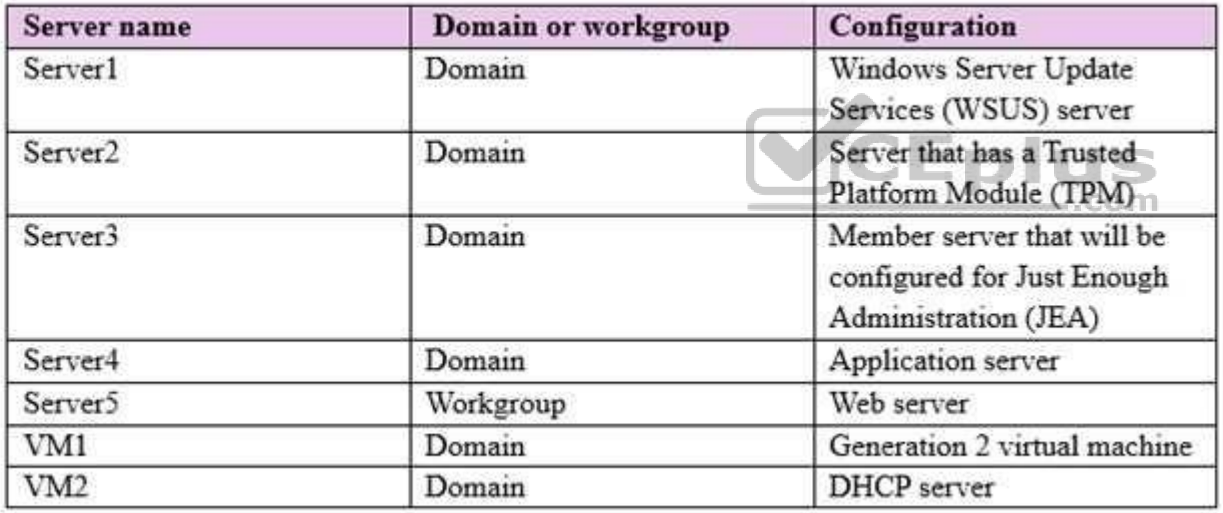
Section: (none)
Explanation
Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit_script

QUESTION 40
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.

VCEplus .com

End of repeated scenario.

You need to create a Role Capability file on Server3. Which file should you create?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/jea/role-capabilities#create-a-role-capability-file

QUESTION 41
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.

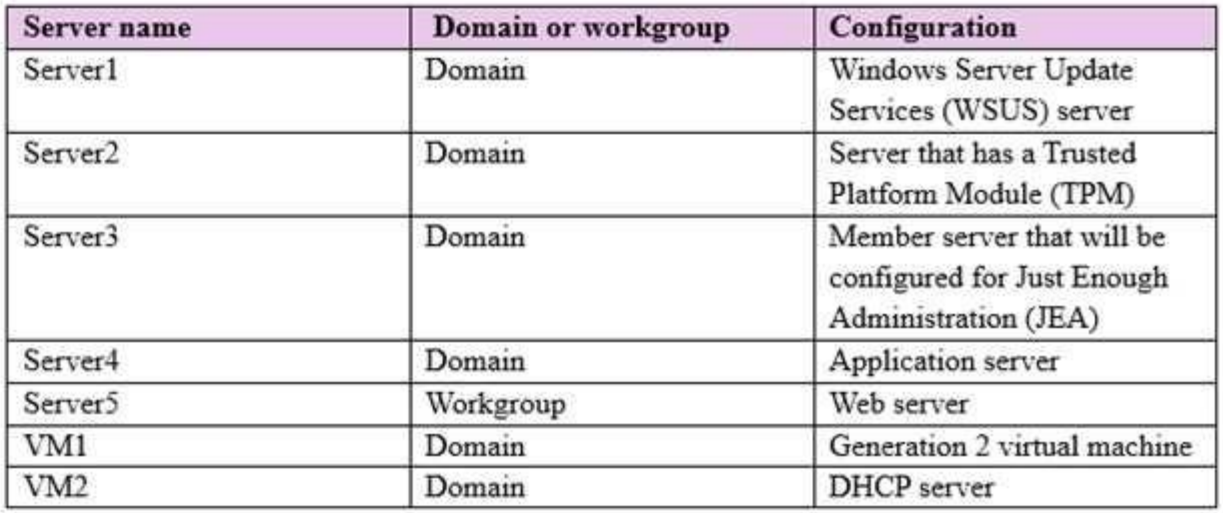
VCEplus .com

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.

VCEplus.com



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 implement BitLocker Network Unlock for all of the laptops. Which server role should you deploy to the network?

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

Correct Answer: C

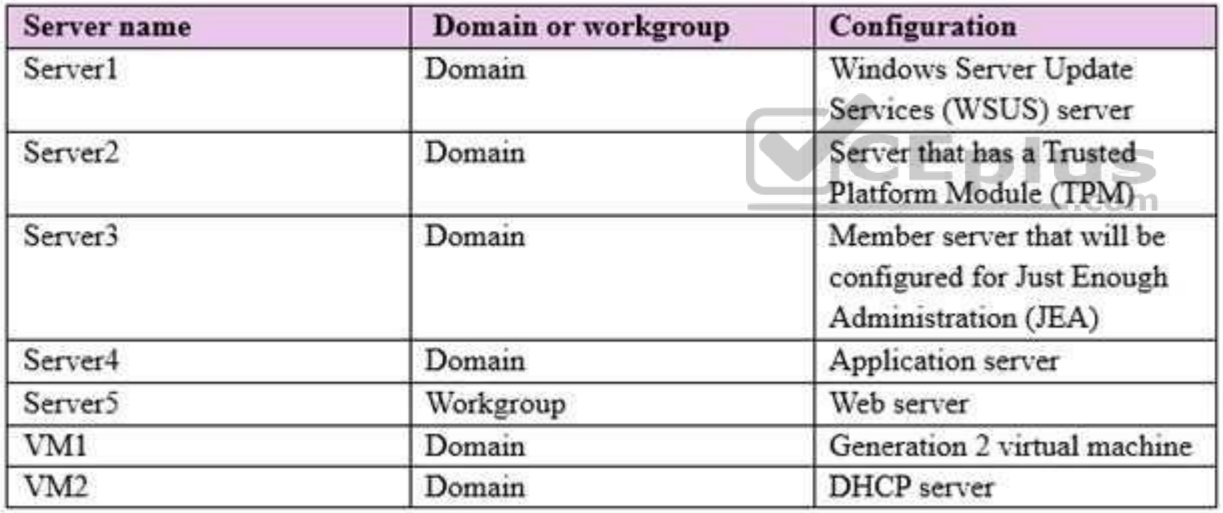
Section: (none)
Explanation
Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-how-to-enable-network-unlock

QUESTION 42
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.

VCEplus .com

End of repeated scenario.

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows/device-security/applocker/configure-the-application-identity-service

QUESTION 43
Your network contains an Active Directory domain named contoso.com. The domain contains a certification authority (CA).

VCEplus .com

You need to implement code integrity policies and sign them by using certificates issued by the CA.

You plan to use the same certificate to sign policies on multiple computers.

You duplicate the Code Signing certificate template and name the new template CodeIntegrity.

How should you configure the CodeIntegrity template?

A. Enable the Allow private key to be exported setting and modify the Key Usage extension.
B. Disable the Allow private key to be exported setting and modify the Application Policies extension.
C. Disable the Allow private key to be exported setting and disable the Basic Constraints extension.
D. Enable the Allow private key to be exported setting and enable the Basic Constraints extension

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References: https://blogs.technet.microsoft.com/ukplatforms/2017/05/04/create-code-integrity-signing-certificate/ **QUESTION 44**

VCEplus.com

DRAG DROP

Your network contains an Active Directory domain named contoso.com. The domain contains a user named User1 and a computer named Computer1. Remote Server Administration Tools (RSAT) is installed on Computer1.

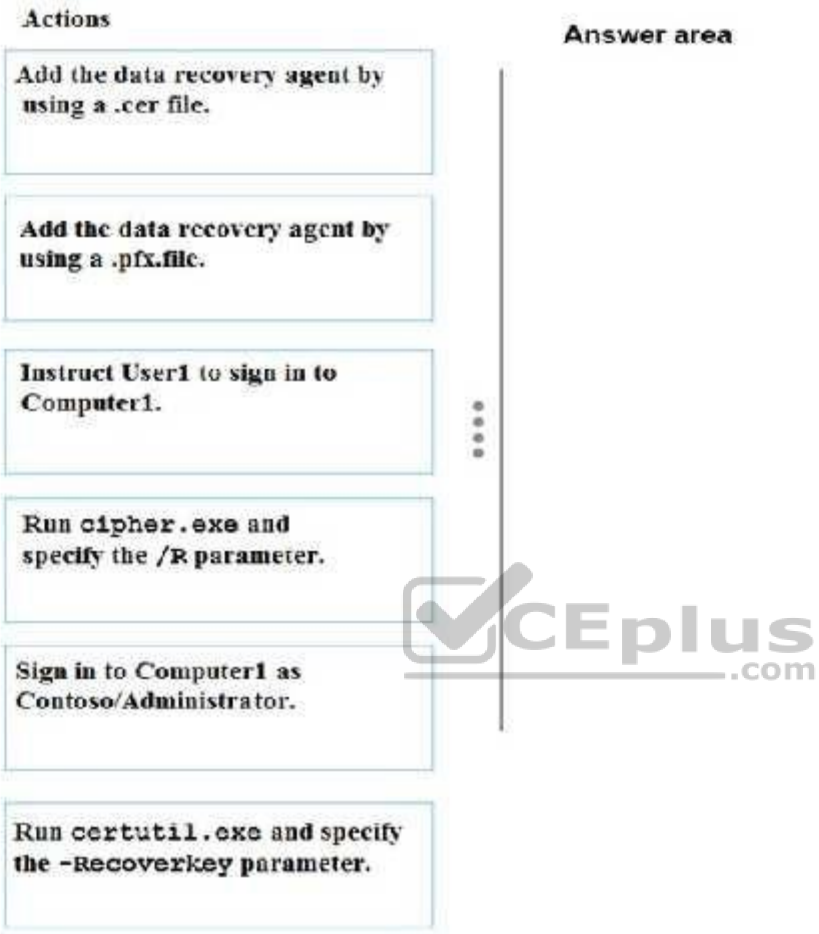
You need to add User1 as a data recovery agent in the domain.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

VCEplus.com

VCEplus.com



Actions

Add the data recovery agent by using a .cer file.

Add the data recovery agent by using a .pfx.file.

Instruct User1 to sign in to Computer1.

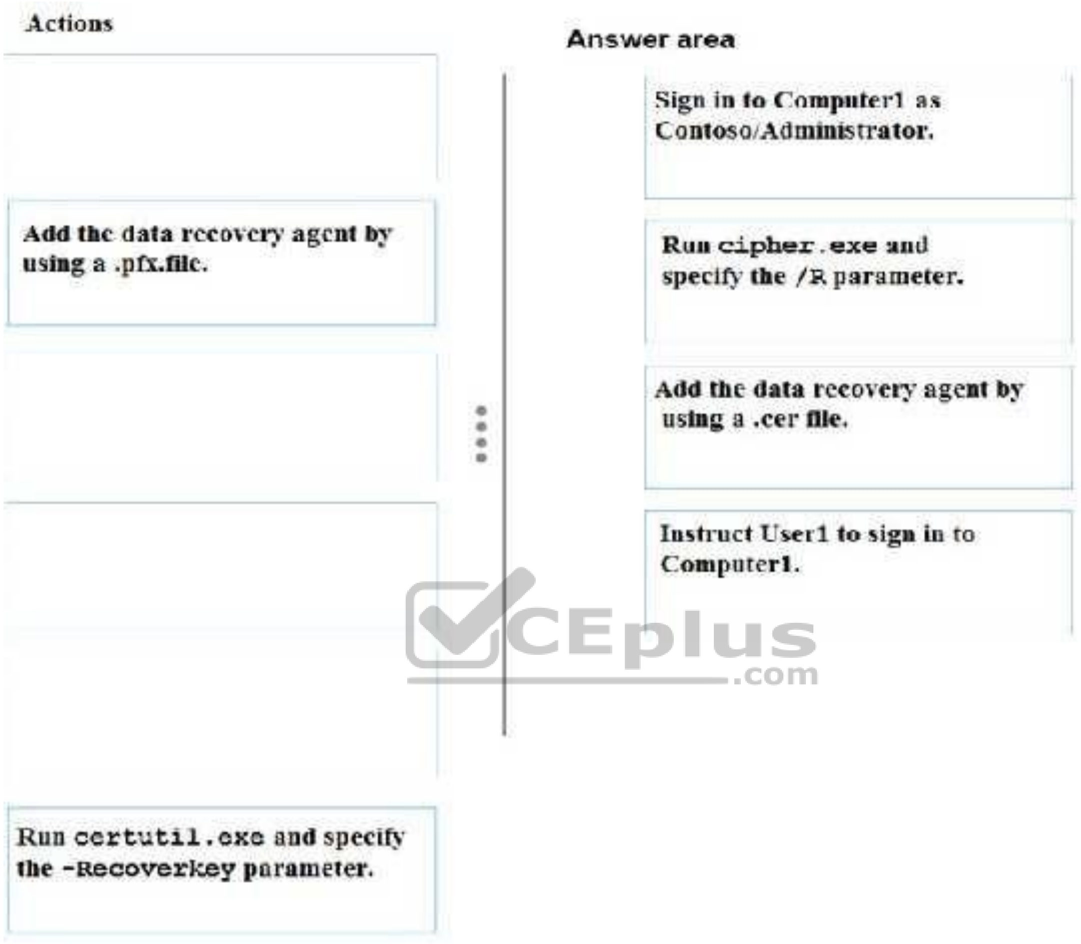
Run cipher.exe and specify the /R parameter.

Sign in to Computer1 as Contoso/Administrator.

Run certutil.exe and specify the -Recoverkey parameter.

VCEplus.com

Correct Answer:



Actions

Add the data recovery agent by using a .pfx.file.

Run certutil.exe and specify the -Recoverkey parameter.

Answer area

Sign in to Computer1 as Contoso/Administrator.

Run cipher.exe and specify the /R parameter.

Add the data recovery agent by using a .cer file.

Instruct User1 to sign in to Computer1.

Section: (none)
Explanation

Explanation/Reference:
Explanation:

References:
https://msdn.microsoft.com/library/cc875821.aspx#EJAA
https://www.serverbrain.org/managing-security-2003/using-the-cipher-command-to-add-data-recovery-agent.html **QUESTION 45**

VCEplus.com

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 FinanceAdministartors can view the password of the local Administrator accounts on the servers in an organizational unit (OU) named FinanceServers.

You need to prevent the FinanceAdministartors members from viewing the local administrators ‘passwords on the servers in FinanceServers. Which permission should you remove from FinanceAdministartors?

A. all extended rights
B. read all properties
C. read permissions
D. list contents

Correct Answer: A
Section: (none)
Explanation

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

VCEplus.com

QUESTION 46
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.

https://vceplus.com/

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

Correct Answer: AEF
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/microsoft-identity-manager/working-with-self-service-password-reset

QUESTION 47
You have a file server named FS1 that runs Windows Server 2016.

You plan to disable SMB 1.0 on the server.

You need to verify which computers access FS1 by using SMB 1.0.

What should you run first?

A. **Debug-FileShare**
B. **Set-FileShare**
C. **Set-SmbShare**

VCEplus .com

D. **Set-SmbServerConfiguration**

E. **Set-SmbClientConfiguration**

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48

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.

VCEplus .com

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
References: https://www.techrepublic.com/article/pro-tip-securing-windows-local-administrator-password-with-laps/

QUESTION 49

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-PamRole**

C. **New-ADGroup**

D. **New-PamGroup**

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/identitymanager/mimpam/vlatest/new-pamgroup

QUESTION 50
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 answer presents part of the solution.

A. From Server1, run the **New-PAMTrust** cmdlet.

B. From a domain controller in contoso.com, 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-PAMTrust** cmdlet.

E. From a domain controller in admin.contoso.com, run the **New-PAMDomainConfiguration** cmdlet.

F. From Server1, run the **New- PAMDomainConfiguration** cmdlet.

VCEplus.com

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference: References: 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-corpforests

QUESTION 51

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.

VCEplus.com

Solution: You run the **New-NetFirewallRule -DisplayName "Rule1" -Direction Inbound -LocalPort 8080 -Protocol TCP -Action Allow -Profile Domain** command.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52

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.

VCEplus .com

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 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

VCEplus .com

Explanation/Reference:
References: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd448531(v=ws.10)

QUESTION 53
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows10.

The network uses the 172.16.0.0/16 address space.

Computer1 has an application named App1.exe that is located in D:\Apps\. App1.exe is configured to accept connections on TCP port 8080.

You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.

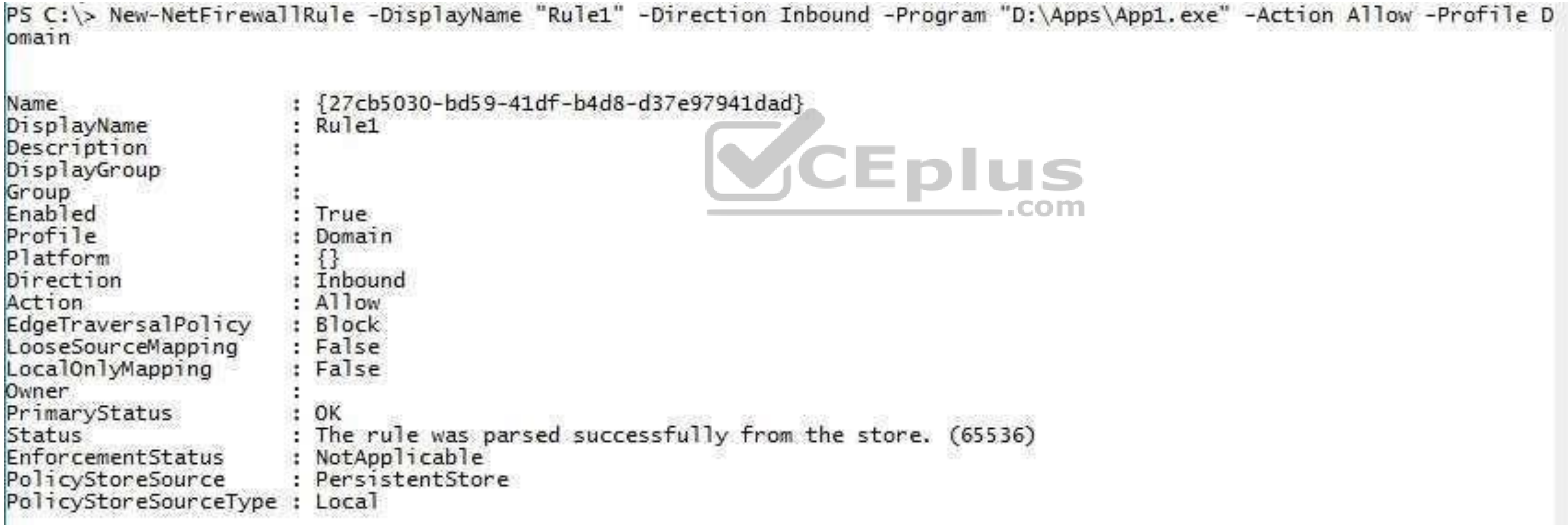
Solution: You run the **New-NetFirewallRule –DisplayName "Rule1" –Direction Inbound –Program "D:\Apps\App1.exe" –Action Allow -Profile Domain** command.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

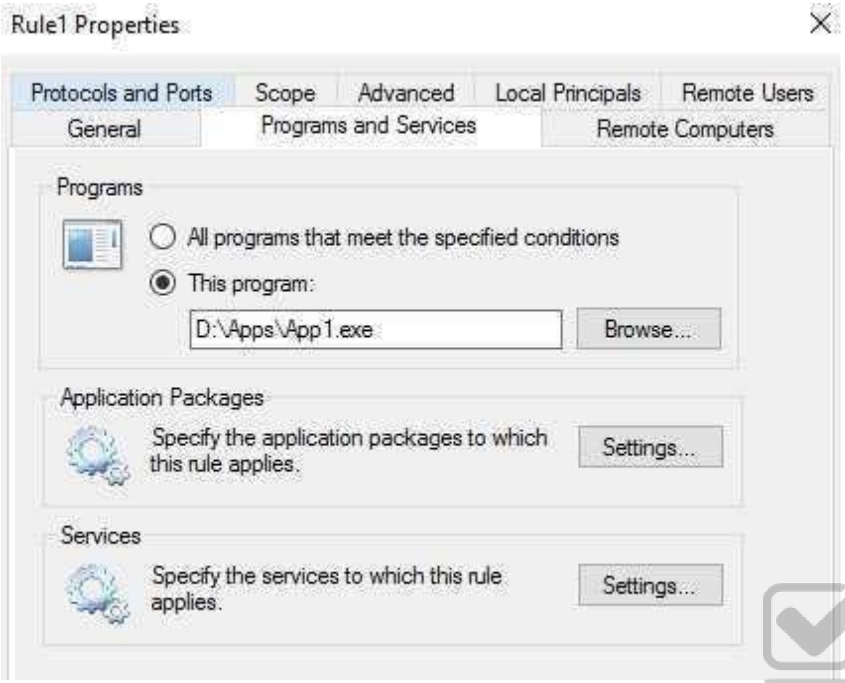
Explanation/Reference:
Explanation:



```
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
```

VCEplus.com



Rule1 Properties

Programs

○ All programs that meet the specified conditions

● This program:

D:\Apps\App1.exe

Application Packages

Specify the application packages to which this rule applies.

Services

Specify the services to which this rule applies.

VCEplus.com

QUESTION 54

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

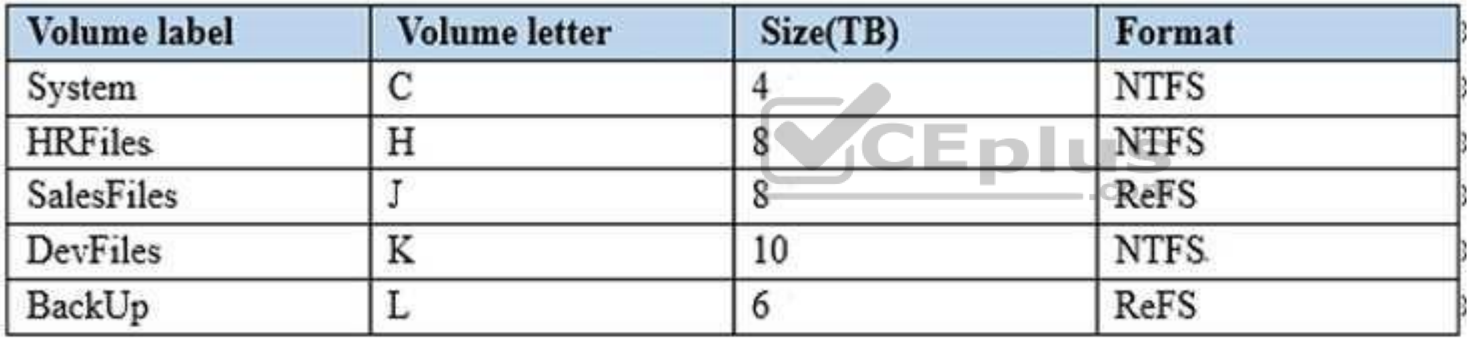
Correct Answer: B
Section: (none)
Explanation

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

QUESTION 55
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 (BitLocker).

Solution: You run the **Lock-BitLocker** cmdlet.

Does this meet the goal?

A. Yes
B. No

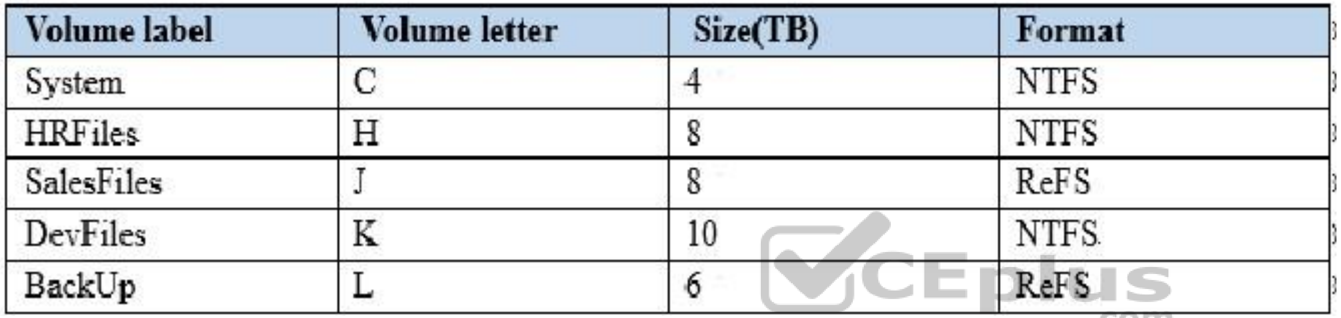
Correct Answer: B
Section: (none)
Explanation

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

QUESTION 56
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 (BitLocker).

Solution: You run the **manage-bde.exe** command and specify the *–on* parameter.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/manage-bde-on

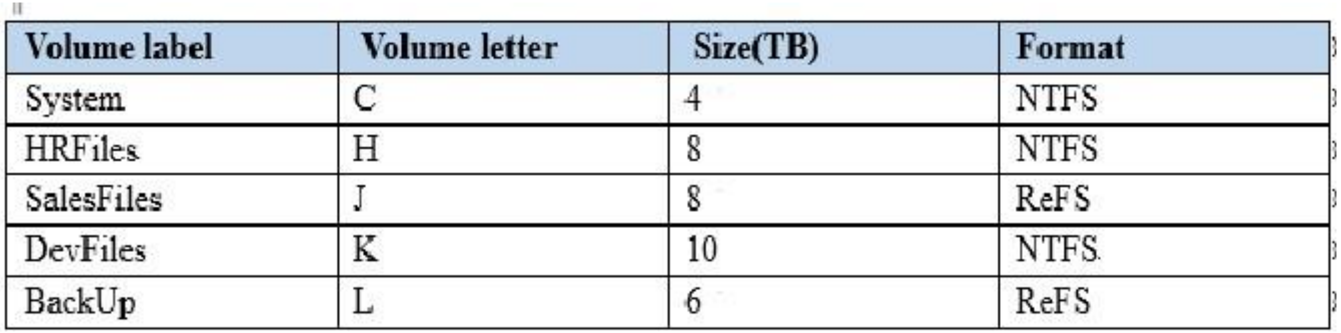
VCEplus .com

QUESTION 57

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 (BitLocker).

VCEplus .com

Solution: You run the **Enable-BitLocker** cmdlet.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 58

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.

VCEplus.com

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 HGS1, run the **Export-HgsKeyProtectionState** cmdlet, and then run the **Import-HgsGuardian** cmdlet.
B. On Hyper1, run the **Invoke-WebRequest** cmdlet, and then run the **Import-HgsGuardian** cmdlet.
C. On the virtual machine, retrieve the metadata of the guarded fabric, and then import the metadata.
D. On Hyper1, run the **Export-HgsKeyProtectionState** cmdlet, and then run the **Import-HgsGuardian** cmdlet.

Correct Answer: B
Section: (none)
Explanation

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

VCEplus.com

QUESTION 59
DRAG DROP

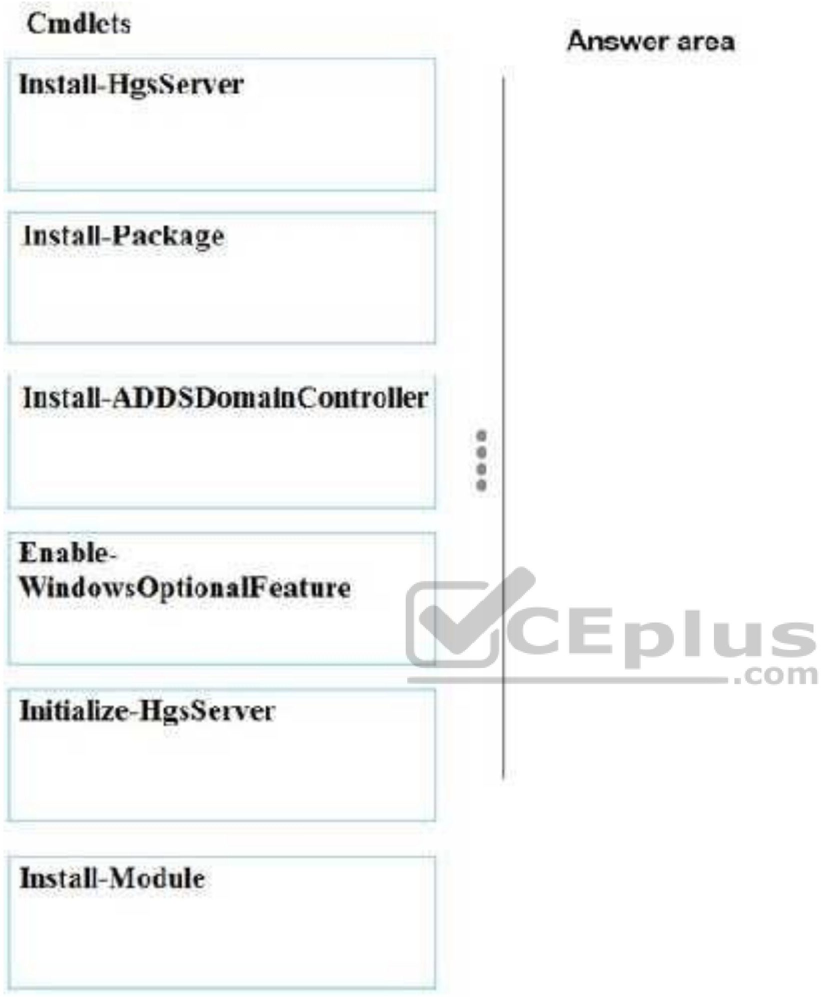
Your network contains an Active Directory domain named contoso.com. The domain contains several Hyper-V hosts.

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? To answer move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.

Select and Place:



Cmdlets

Install-HgsServer

Install-Package

Install-ADDSDomainController

Enable-WindowsOptionalFeature

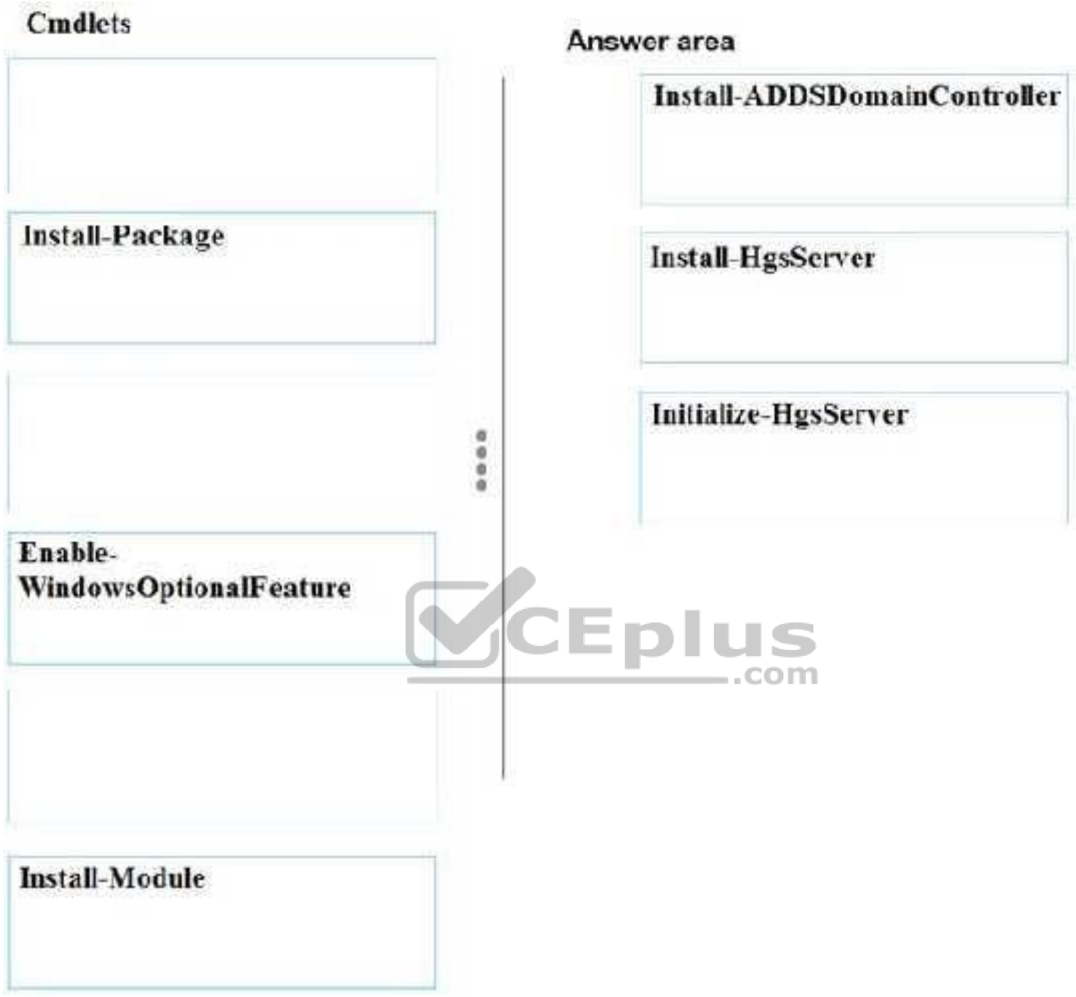
Initialize-HgsServer

Install-Module

Answer area

Correct Answer:

VCEplus .com



Cmdlets

Install-Package

Enable-WindowsOptionalFeature

Install-Module

Answer area

Install-ADDSDomainController

Install-HgsServer

Initialize-HgsServer

Section: (none)
Explanation

Explanation/Reference:

Explanation:

References: https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabric-setting-up-the-host-guardian-service-hgs

QUESTION 60

VCEplus.com

You are building a guarded fabric.

You need to configure Admin-trusted attestation.

Which cmdlet should you use?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabric-add-host-information-for-admin-trustedattestation

VCEplus.com

QUESTION 61
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

You need to allow network administrators to use Just Enough Administration (JEA) to change the TCP/IP settings on Server1. The solution must use the principle of least privilege.

How should you configure the session configuration file?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 62
Your network contains an Active Directory domain named contoso.com.

You download Microsoft Security Compliance Toolkit 1.0 and all the security baselines.

You need to deploy one of the security baselines to all the computers in an organizational unit (OU) named OU1.

What should you do?

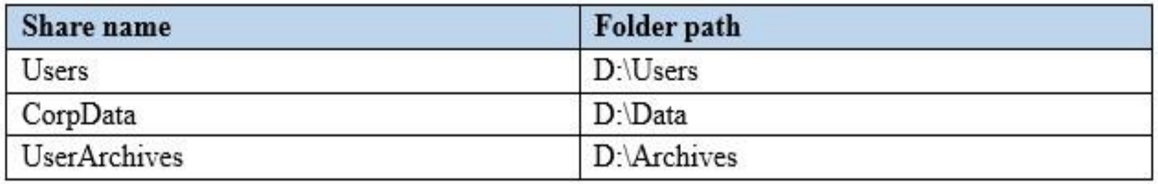
A. Run **1gpo.exe** and specify the */g* parameter. From Policy Analyzer, click **Add**.
B. From Group Policy Management, create and link a Group Policy object (GPO). Select the GPO and run the Import Settings Wizard.
C. From Group Policy Management, click **Group Policy Objects**, and then click **Manage Backups…**
D. From Group Policy Management, create and link a Group Policy object (GPO). Run **1gpo.exe** and specify the */g* parameter.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/distribute-certificates-to-client-computers-by-using-group-policy

QUESTION 63
You have a virtual machine named FS1 that runs Windows Server 2016.

FS1 has the shared folders shown in the following table.



Share name	Folder path
Users	D:\Users
CorpData	D:\Data
UserArchives	D:\Archives

You need to ensure that each user can store 10 GB of files in \\FS1\Users.

What should you do?

A. From File Explorer, open the properties of volume D, and then modify the Quota settings.
B. Install the File Server Resource Manager role service, and then create a file screen.
C. From File Explorer, open the properties of D:\Users, and then modify the Advanced sharing settings.
D. Install the File Server Resource Manager role service, and then create a quota.

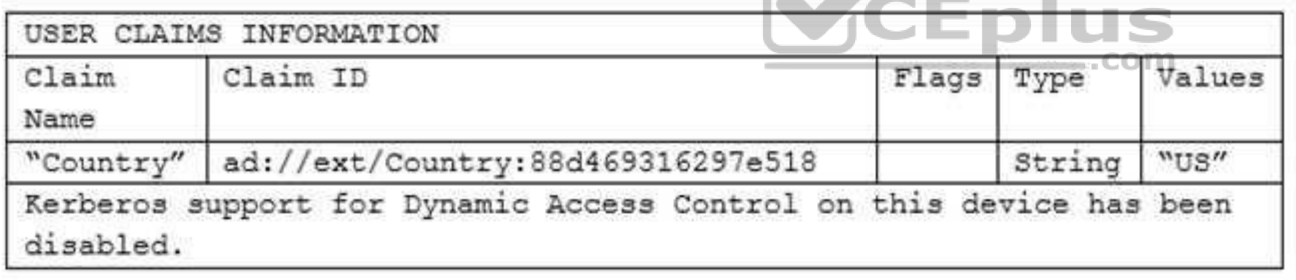
Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows-server/storage/fsrm/create-quota

QUESTION 64
Your network contains an Active Directory domain named contoso.com. The domain contains domain controllers that run Windows Server 2016.

The Job Title attribute for a domain user named User1 has a value of Sales Manager.

User1 runs **whoami/claims** and receives the following output.



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

You need to ensure that the security token of User1 has a claim for Job Title.

What should you do?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
References: https://www.nyazit.com/how-to-configure-dynamic-access-control-in-windows-server-2012-r2-2/

QUESTION 65
Your network has an internal network and a perimeter network. Only the servers on the perimeter network can access the Internet. You create a Microsoft Operations Management Suite (OMS) instance in Microsoft Azure.

You deploy Microsoft Monitoring Agent to all the servers on both the networks.

You discover that only the servers on the perimeter network report to OMS.

You need to ensure that all the servers report to OMS.

What should you do?

A. Install a Web Application Proxy on the perimeter network and install an OMS Gateway on the internal network. Publish the OMS Gateway from the Web Application Proxy.
B. Install a Web Application Proxy and an OMS Gateway on the perimeter network. Publish the OMS Gateway from the Web Application Proxy.
C. Configure the network firewalls to allow the internal servers to access the IP addresses of the Azure OMS instance by using TCP port 443.
D. On the internal servers, run the **Add-AzureRmUsageConnect** cmdlet and specify the *–AdminUri* parameter.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-oms-gateway

QUESTION 66
Your network contains an Active Directory domain named contoso.com. The domain contains a member server named Server5 that runs Windows Server 2016.

You need to configure Server5 as a Just Enough Administrator (JEA) endpoint.

Which two actions should you perform? Each correct answer presents part of the solution.

VCEplus.com

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

Correct Answer: CE
Section: (none)
Explanation

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

QUESTION 67
You have a server named Server1 that runs Windows Server 2016.

VCEplus.com

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/powershell/module/Microsoft.PowerShell.Core/get-pssessioncapability?view=powershell-6&viewFallbackFrom=powershell-5.0.

VCEplus.com

QUESTION 68

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

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-NetFirewallSecurityFilter**
H. **Get-NetFirewallApplicationFilter**

VCEplus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/module/netsecurity/get-netfirewallprofile?view=win10-ps

QUESTION 69

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

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:
References: https://docs.microsoft.com/en-us/powershell/module/netsecurity/get-netfirewallrule?view=win10-ps

QUESTION 70
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

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

You need to identify 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:

References: https://docs.microsoft.com/en-us/powershell/module/netsecurity/get-netipsecrule?view=win10-ps

QUESTION 71

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

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:

References: https://docs.microsoft.com/en-us/powershell/module/netsecurity/get-netfirewallsetting?view=win10-ps

VCEplus.com

QUESTION 72
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 Name Resolution Policy Table (NRPT)
C. a zone transfer policy
D. a connection security rule

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://nedimmehic.org/2017/04/04/how-to-deploy-and-configure-dns-2016-part5/

VCEplus.com

QUESTION 73
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 the accounting department to connect to Server11 What

should you recommend implementing?

A. Just Enough Administration (JEA)
B. AppLocker rules

C. Privileged Access Management (PAM)
D. connection security rules

Correct Answer: D
Section: (none)
Explanation

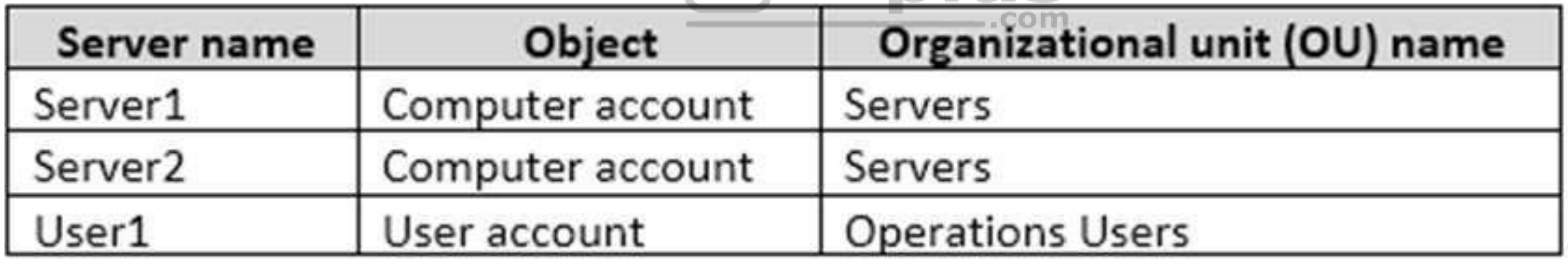
Explanation/Reference:
References: https://support.microsoft.com/en-us/help/942957/security-rules-for-windows-firewall-and-for-ipsec-based-connections-in

QUESTION 74
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

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

The relevant objects in the domain are configured as shown in the following table.



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

You need to assign User1 the right to restore files and folders on Server1 and Server2.

Solution: You add User1 to the Backup Operators group on Server1 and Server2.

Does this meet the goal?

A. Yes
B. No

VCEplus.com

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 75
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.

VCEplus.com

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
Section: (none)
Explanation

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

QUESTION 76

VCEplus.com

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. 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 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

VCEplus.com

Explanation/Reference:

QUESTION 77
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 contain 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.

VCEplus.com

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:
References: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd421709(v=ws.10)#what-is-an-inbound-rule

QUESTION 78
You work for a hosting company named Contoso, Ltd.

Contoso has multiple Hyper-V hosts that run Windows Server 2016.

You are configuring Software Defined Networking (SDN).

VCEplus.com

You need to configure Datacenter Firewall to control the traffic to virtual machines.

Which cmdlet should you use?

A. **Set-Acl**
B. **Grant-VMConnectAccess**
C. **New-NetworkControllerAccessControlList**
D. **New-NetFirewallRule**

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/windows-server/networking/sdn/manage/configure-datacenter-firewall-acls
https://docs.microsoft.com/en-us/powershell/module/networkcontroller/new-networkcontrolleraccesscontrollist?view=win10-ps

QUESTION 79

You have a Hyper-V host named Hyper1 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.

NOTE: Each correct selection is worth one point.

A. Disable all the Hyper-V integration services for FS1.
B. On Hyper1, enable BitLocker Drive Encryption (BitLocker) for the drive that contains the VHDX file for FS1.
C. Disable the virtualization extensions for FS1.
D. Enable shielding for FS1.
E. Enable BitLocker Drive Encryption (BitLocker) for all the volumes on FS1.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference: References: https://docs.microsoft.com/en-us/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vms

QUESTION 80

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 **/quarantine** switch.
B. Enable SID filtering on the trust.
C. Run **netdom.exe** and specify the **/transitive** switch.

VCEplus.com

D. Enable SID history on the trust.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
References: https://www.petri.com/windows-server-2016-set-privileged-access-management

QUESTION 81
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. Security Configuration and Analysis
B. Group Policy Management
C. System Configuration
D. Server Manager

VCEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://4sysops.com/archives/security-compliance-manager-deploy-baselines/#deploy-a-baseline-to-a-workgroup-server

QUESTION 82
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.

VCEplus.com

What should you do?

A. From the settings of VM1, configure Integration Services
B. From Server1, configure the Enforce drive encryption type on fixed data drives Group Policy setting.
C. From the settings of VM1, enable a Trusted Platform Module(TPM).
D. From the settings of VM1, enable Secure Boot.

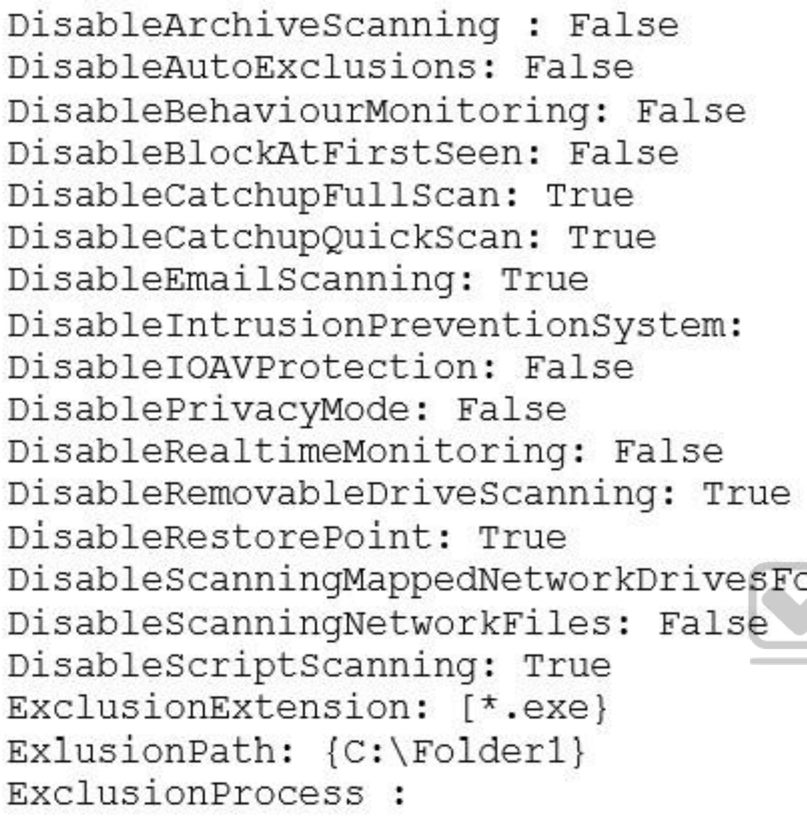
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/learn-more/generation-2-virtual-machine-security-settings-for-hyper-v

QUESTION 83
You have a server named Server1 that runs Windows Server 2016.

Windows Defender on Server1 has the following configurations.

VCEplus.com



```
DisableArchiveScanning : False
DisableAutoExclusions: False
DisableBehaviourMonitoring: False
DisableBlockAtFirstSeen: False
DisableCatchupFullScan: True
DisableCatchupQuickScan: True
DisableEmailScanning: True
DisableIntrusionPreventionSystem:
DisableIOAVProtection: False
DisablePrivacyMode: False
DisableRealtimeMonitoring: False
DisableRemovableDriveScanning: True
DisableRestorePoint: True
DisableScanningMappedNetworkDrivesForFullScan: True
DisableScanningNetworkFiles: False
DisableScriptScanning: True
ExclusionExtension: [*.exe}
ExlusionPath: {C:\Folder1}
ExclusionProcess :
```

Server1 has the following files:

- C:\Folder1\File1.exe
- C:\Folder2\File2.bat
- C:\Folder2\File3.com

Which files will be scanned for malware?

A. File1.exe and File3.com only
B. File2.bat only
C. File1.exe, File2.bat, and File3.com

VCEplus .com

D. File1.exe only
E. File2.bat and File3.com only
F. File3.com only

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/configure-extension-file-exclusions-windows-defender-antivirus

QUESTION 84
You have a Host Guardian Service (HGS) and a guarded host.

You have a VHDX file that contains an image of Windows Server 2016.

You need to provision a virtual machine by using a shielded template.

VCEplus .com

Which three files should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a TPM baseline policy file
B. a TPM identifier file
C. a shielding data .pdk file
D. a signature for the .vhdx file
E. an unattended.xml file

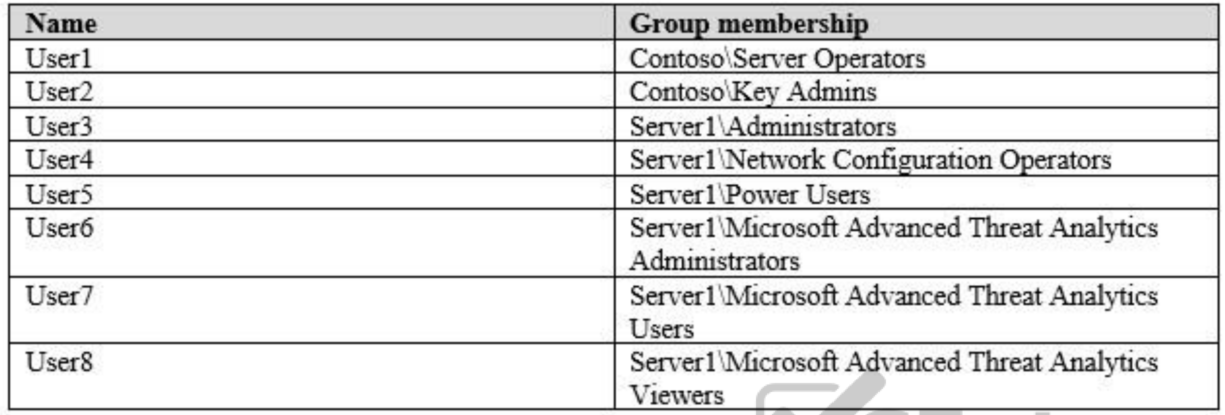
Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-create-a-shielded-vm-template https://docs.microsoft.com/en-us/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-tenant-creates-shielding-data
QUESTION 85

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. User7
B. User8
C. User1
D. User6

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References:

www.vceplus.com - Free Questions & Answers - Online Courses - Convert VCE to PDF - VCEplus.com

https://docs.microsoft.com/en-us/advanced-threat-analytics/install-ata-step1

QUESTION 86

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
Section: (none)
Explanation

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

QUESTION 87

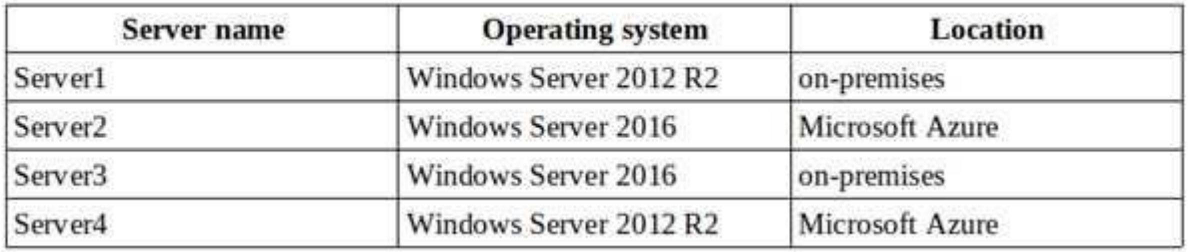
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 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:
References: https://docs.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard

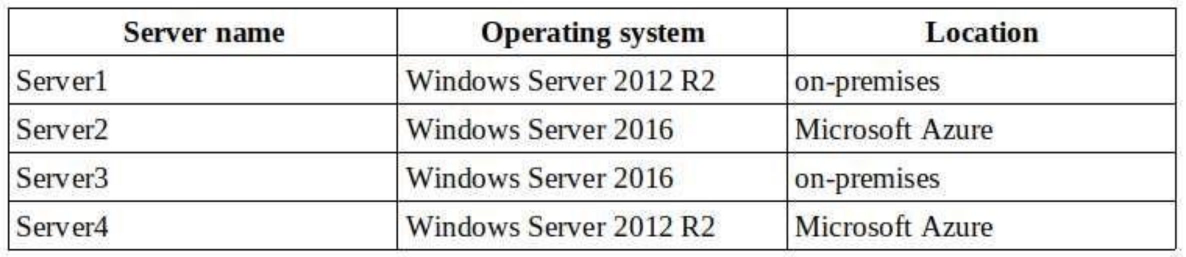
QUESTION 88
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Your network contains an Active Directory domain named contoso.com. All 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 Server1.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 89
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. On Server1, install the Host Guardian Hyper-V Support feature and a computer certificate from a trusted certification authority (CA).

VCEplus .com

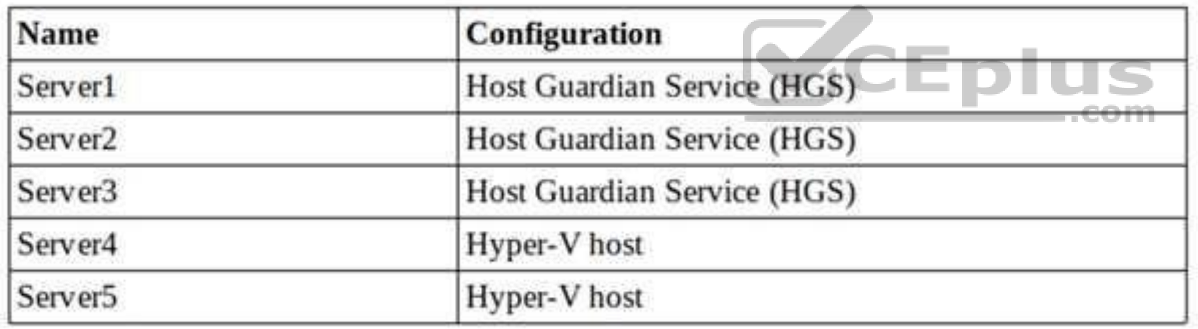
B. On Server1, install the Device Health Attestation server role and a computer certificate from a trusted certification authority (CA).

C. Install the Host Guardian Hyper-V Support feature on Server1 and add Server1 to a domain security group.
D. Install the Device Health Attestation server role on Server1 and add Server1 to a domain security group.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 90
You have a guarded fabric that consists of the servers shown in the following table.



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 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.

VCEplus.com

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 91
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 Windows10. Computer 1 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?

VCEplus.com

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard#reqs

QUESTION 92
HOTSPOT

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

You have a backup of a Group Policy object (GPO) named GPO1 that has the following settings:

VCEplus.com

- Change the system time: User1
- Minimum password length: 12 characters
- Password must meet complexity requirements: Disabled

You have a backup of a GPO named GPO2 that has the following settings:

- Change the system time: User2
- Minimum password length: 7 characters
- Password must meet complexity requirements: Not Defined

You create a GPO named GP03 that has the following settings:

- Change the system time: User3
- Minimum password length: 9 characters
- Password must meet complexity requirements: Enabled

You import the GPO1 settings into GP03, and then you import the GPO2 settings into GPO3. You need to identify the GPO3 settings after the imports.

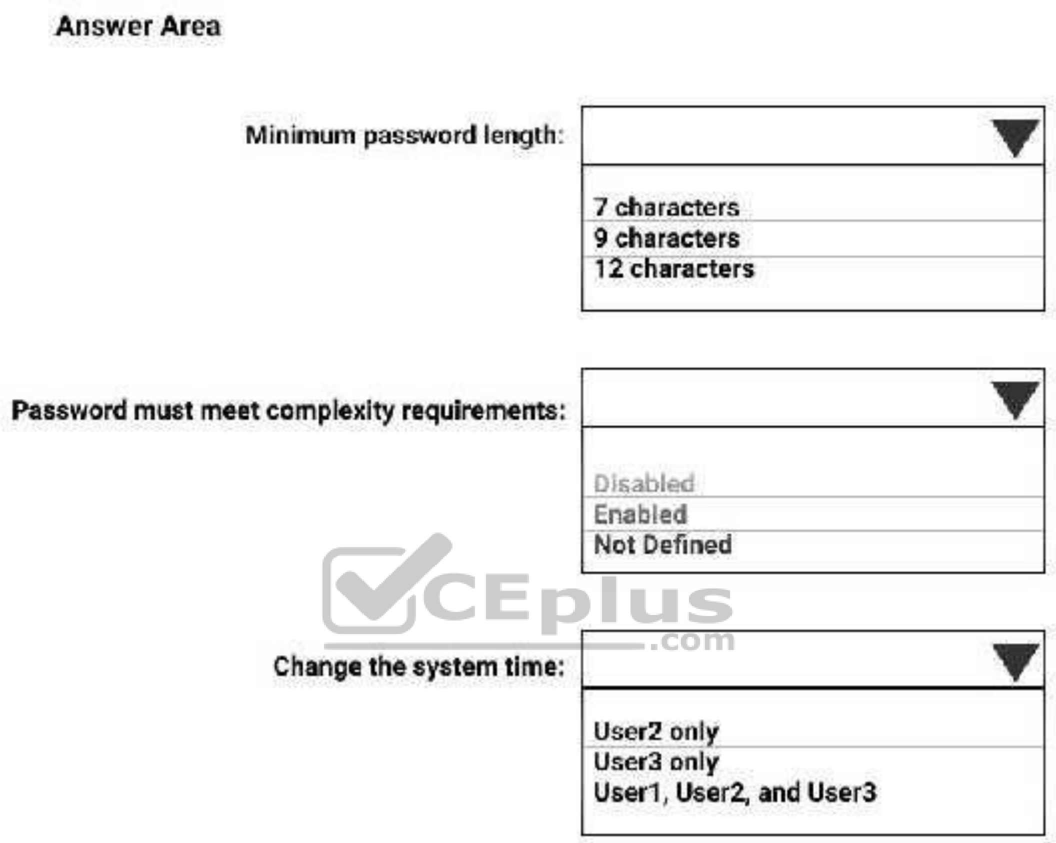
What should you identity? To answer. select the appropriate options of the answer area.

VCEplus.com

NOTE: Each correct selection is worth one point.

Hot Area:

VCEplus.com



Answer Area

Minimum password length:

- 7 characters
- 9 characters
- 12 characters

Password must meet complexity requirements:

- Disabled
- Enabled
- Not Defined

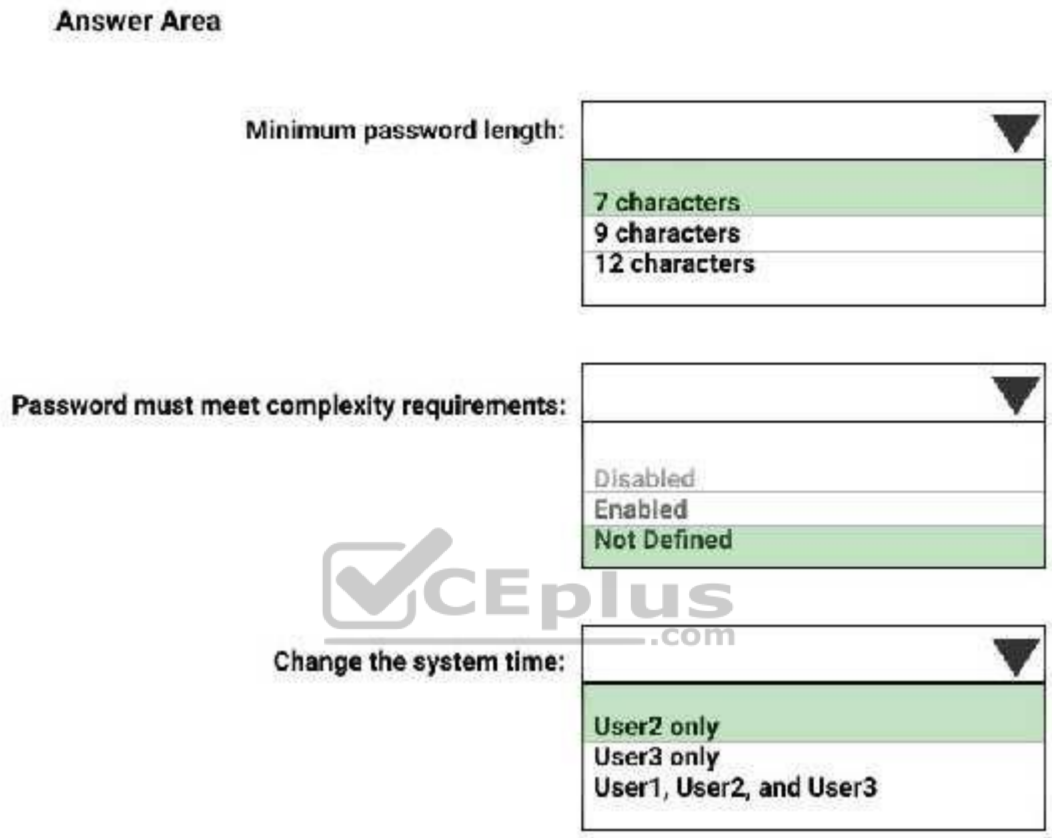
Change the system time:

- User2 only
- User3 only
- User1, User2, and User3

VCEplus.com

Correct Answer:

VCEplus .com



Answer Area

Minimum password length:

- 7 characters
- 9 characters
- 12 characters

Password must meet complexity requirements:

- Disabled
- Enabled
- Not Defined

Change the system time:

- User2 only
- User3 only
- User1, User2, and User3

VCEplus .com

Section: (none)
Explanation

Explanation/Reference:
References: https://searchwindowsserver.techtarget.com/feature/Group-Policy-Management-Console

QUESTION 93
Your network contains an Active Directory forest named contoso.com. The functional level of the forest and the domain is Windows Server 2012 R2.

VCEplus .com

You plan to use Local Administrator Password Solution (LAPS) for all member servers.

You need to prepare the forest for LAPS.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Run the **Set-AdmPwdComputerSelfPermission** cmdlet.
B. Install the LAPS client-side extension on all domain controllers.
C. Run the **Update-AdmPwdADSchema** cmdlet.
D. Run the **Set-AdmPwdAuditing** cmdlet.
E. Deploy an enterprise certification authority (CA).

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
References: https://blog.thesysadmins.co.uk/deploying-microsoft-laps-part-1.html

VCEplus .com

QUESTION 94
Your network contains an Active Directory domain named contoso.com. 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 6AC1786C-016F-11D2945F-00C04fB984F9.

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\{6AC1786C-016F-11D2-945F-00CO4fB984F9} folder to Server1.
B. From Windows PowerShell, run the **Backup-GPO** cmdlet.
C. Modify the permissions of the \\contoso.com\sysvol\contoso.com\Policies\6AC1786-016F-11D2-945F-00C04fB984F9) folder.
D. From Windows PowerShell, run the **Copy-GPO** cmdlet.

Correct Answer: B

VCEplus .com

Section: (none)
Explanation
Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/module/grouppolicy/backup-gpo?view=win10-ps

QUESTION 95
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 System Information, review System Summary.
C. From a command prompt, run the tsecimp.exe command.
D. From Server Manager, click Local Server, and review the properties of Server1.

VCEplus .com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage

QUESTION 96
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 VM1, configure the require additional authentication at startup Group Policy setting.
B. From the settings of VM1, enable Secure Boot.
C. From Server1, install the BitLocker feature.

VCEplus.com

D. From VM1, configure the Enforce drive encryption type on fixed data drives Group Policy setting.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.dell.com/support/article/za/en/zadhs1/sln171842/using-the-group-policy-editor-to-enable-bitlocker-authentication-in-the-pre-bootenvironment-for-windows-7-8-8-1-10?lang=en

QUESTION 97
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. System Configuration
B. Microsoft Security Compliance manager (SCM) 4.0
C. Security Templates
D. Local Computer Policy

VCEplus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
You have a server named Server1.

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

What should you configure?

A. protected event logging

B. script block logging
C. module logging
D. system-wide transcription

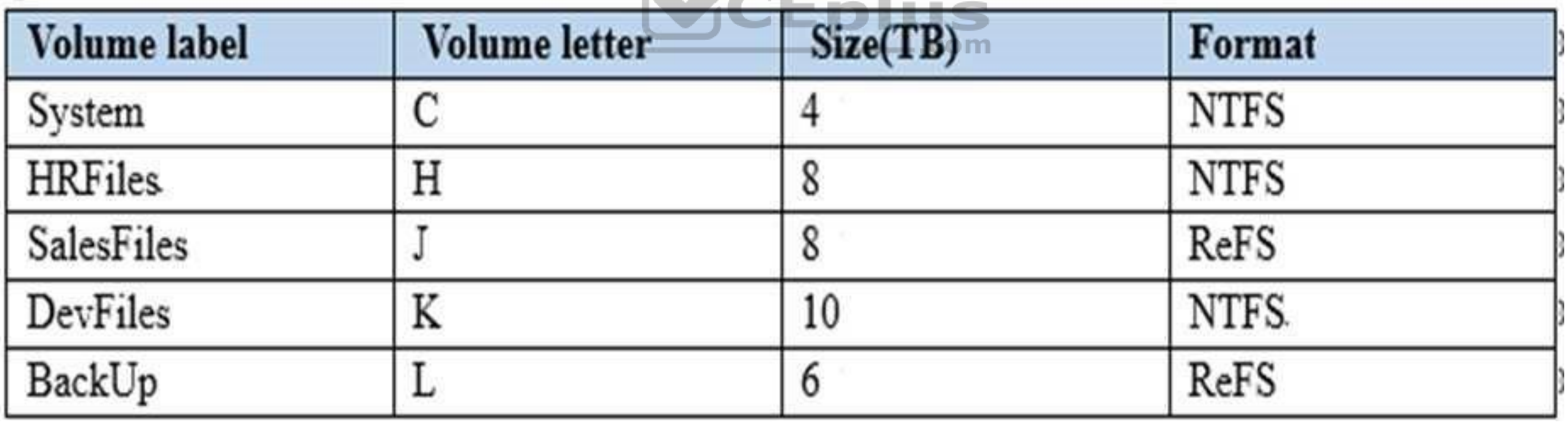
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
References: https://www.rootusers.com/enable-and-configure-module-script-block-and-transcription-logging-in-windows-powershell/

QUESTION 99
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 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 (BitLocker).

Solution: You run the **manage-bde.exe** command and specify the **–lock** parameter.

Does this meet the goal?

A. Yes

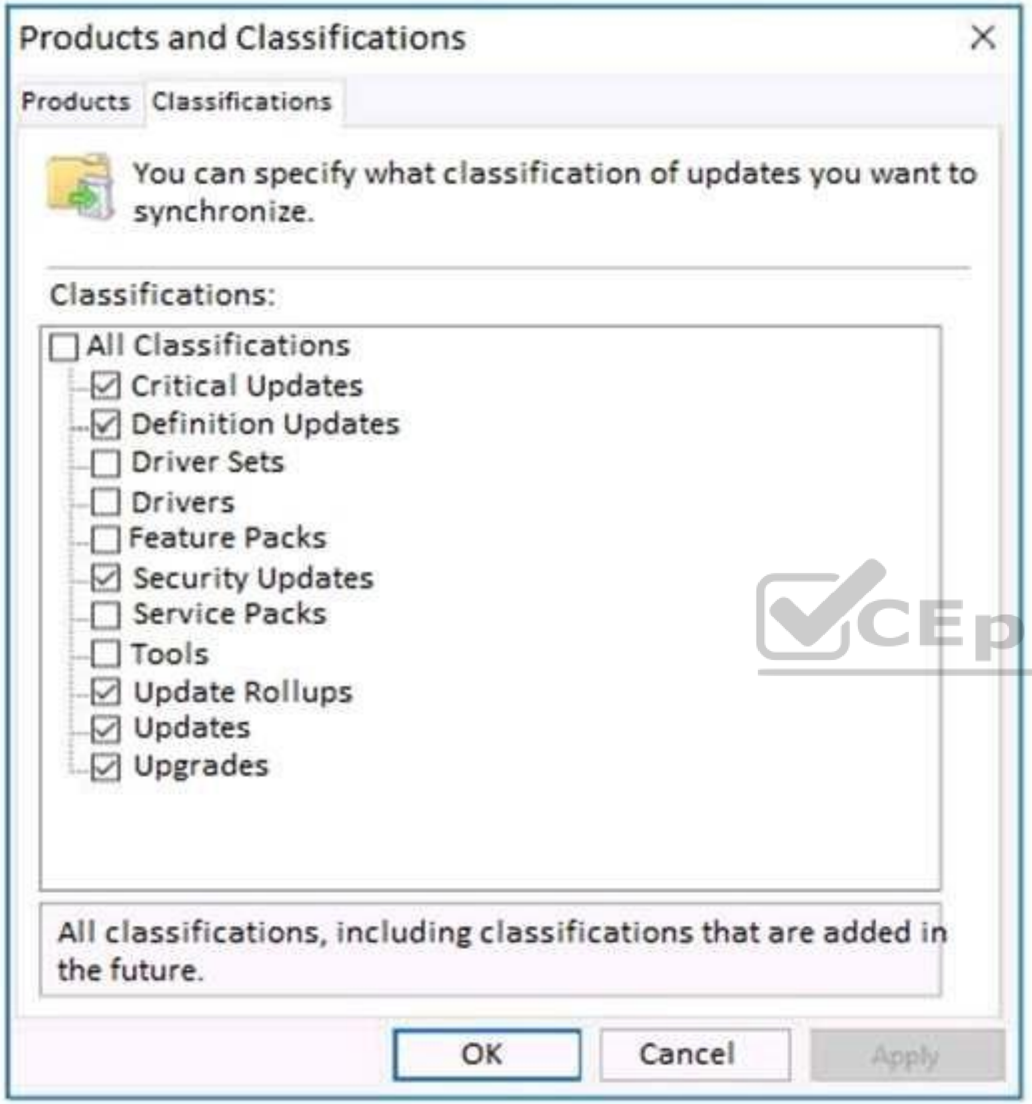
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/manage-bde-lock

QUESTION 100
You have several servers that run Windows Server 2016. All the servers were recently configured to use a new Windows Server Update Services (WSUS) server named WSUS1. WSUS1 is configured to download updates as shown in the exhibit. (Click the **Exhibit** tab.)

VCEplus.com



Products and Classifications

You can specify what classification of updates you want to synchronize.

Classifications:

- □ All Classifications
  - ☑ Critical Updates
  - ☑ Definition Updates
  - □ Driver Sets
  - □ Drivers
  - □ Feature Packs
  - ☑ Security Updates
  - □ Service Packs
  - □ Tools
  - ☑ Update Rollups
  - ☑ Updates
  - ☑ Upgrades

All classifications, including classifications that are added in the future.

You discover that the servers have out-of-date Windows Defender definitions. The servers receive security updates from WSUS1.

You need to ensure that the servers receive the latest Windows Defender definitions.

VCEplus.com

What should you do?

A. Create a new computer group in WSUS
B. Create an auto-approval rule in WSUS
C. Modify the products and classifications in WSUS
D. Create a new Group Policy object (GPO) that contains the Automatic Updates settings

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/manage-protection-update-schedule-windows-defender-antivirus

QUESTION 101
You have a server named Server1.

You need to configure Windows Defender to perform a full scan every day at 21:00.

VCEplus.com

What should you do?

A. From Control Panel, configure the Security and Maintenance settings
B. Run the **Set-ScheduledJob** cmdlet
C. From the Setting app, modify the Windows Defender settings
D. Run the **Set-MpPreference** cmdlet

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/powershell/module/defender/set-mppreference?view=win10-ps

QUESTION 102
You have a server named Server1 that runs Windows Server 2016. Server1 contains a folder named Folder1. Folder1 is shared as Share1.

You need to enable SMB encryption for Share1.

What should you do?

A. From Shared Folders, modify the Security settings of Share1
B. From File and Storage Services in Server Manager, modify the properties of Share1
C. From File Explorer, modify the Advanced Sharing settings of Share1
D. From File Explorer, modify the Security settings of Folder1

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/windows-server/storage/file-server/smb-security

QUESTION 103
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 the domain controllers to a new organizational unit (OU). Remove the permissions to the new OU from the Domain Admins group.
B. Configure the Domain Admins groups as a restricted group.
C. Remove all the members from the Domain Admins group, and then remove the Domain Admins group from all other groups.
D. Instruct all administrators to use a restricted Remote Desktop connection when they sign in to a client computer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References:

https://download.microsoft.com/download/7/7/a/77abc5bd-8320-41af-863c-6ecfb10cb4b9/mitigating%20pass-the-hash%20(pth)%20attacks%20and%20other%20credential%20theft%20techniques_english.pdf

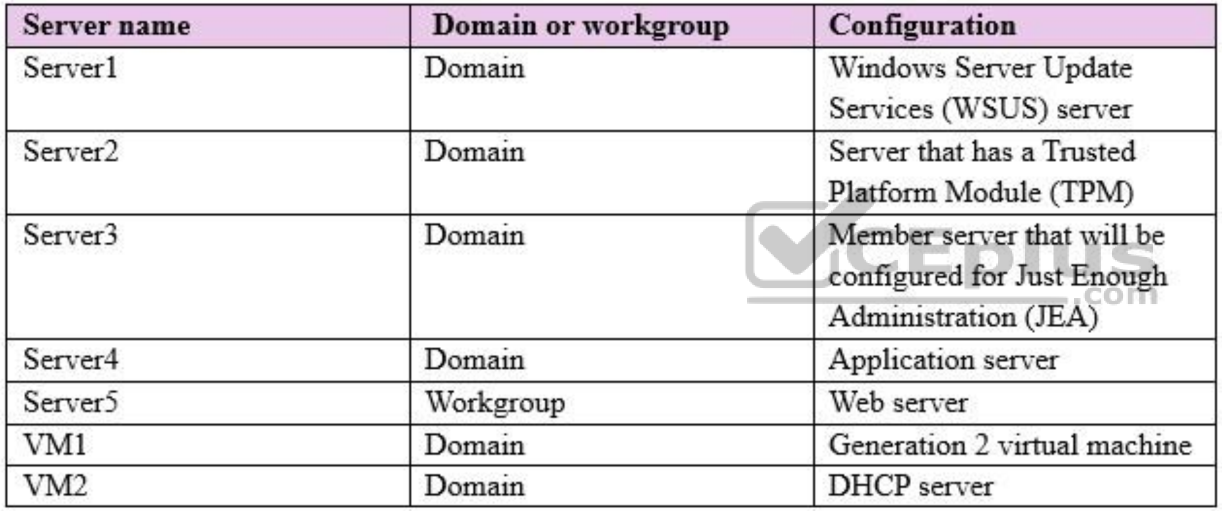
QUESTION 104

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 ensure that you can view Windows PowerShell code that was generated dynamically and executed on the computers in OU1.

What should 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 policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/powershell/wmf/whats-new/script-logging

QUESTION 105
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. Audit Process Creation and Audit Process Termination
B. Turn on PowerShell Transcription
C. Enable Protected Event Logging
D. Turn on PowerShell Script Block Logging

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/powershell/wmf/whats-new/script-logging

VCEplus.com

QUESTION 106

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: http://woshub.com/manage-local-administrator-passwords-with-laps/

VCEplus.com

https://vceplus.com/