Microsoft CERTIFIED Solutions Expert Cloud Platform and Infrastructure

(70-744) Securing Windows Server 2016

QUESTION 1
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 volume named Volume1.
Dynamic Access Control is configured. A resource property named Property1 was created in the domain.
You need to ensure that Property1 is set to a value of Big for all of the files in Volume1 that are larger than 10 MB.
Which tool should you use?

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

Answer: H
Explanation:
In FSRM, "Large Files" creates a list of files conforming to a specified file spec that are a specified size or larger.

QUESTION 2
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 (rom a customized Windows image.
You need to deploy 10 Privileged Access Workstations (PAWs).
The solution must ensure that administrators can access several client applications used by all users.
Solution: You deploy 10 physical computers and configure each wie as a virtualization host.
You deploy the operating system on each host by using the customized Windows image.
On each host you create a guest virtual machine and configure the virtual machine as a PAW.
Does this meet the goal?
A. Yes
B. No

Answer: B

QUESTION 3

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 admm.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.

Answer: B, C

QUESTION 4

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 of 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)

Answer: H

QUESTION 5

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 FS2 to Windows Server 2016.

Answer: C

Explanation:

JEA is incorporated into Windows Server 2016 and Windows 10, and is also incorporated into Windows Management Framework 5.0, which you can download and install on computers running Windows Server 2012 R2.

QUESTION 6

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

You are deploying Microsoft Advanced Threat Analytics (ATA).

You create a user named User1.

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

Which information must you use to configure the Honeytoken account?

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

Answer: C

Explanation:

To configure a Honeytoken user you will need the SID of the user account, not the user name.

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

QUESTION 7

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

Start of repeated scenario

Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.

The domain contains the servers configured as shown m the following table.

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

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

You have an organizational unit (OU) named Marketing that contains the computers in the marketing department.

You have an OU named Finance that contains the computers in the finance department.

You have an OU named AppServers that contains application servers.

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

A GPO named GP2 is linked to the AppServers OU.

You install Windows Defender on Nano1.

End of repeated scenario

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

A. From 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.

Answer: D

Explanation:

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

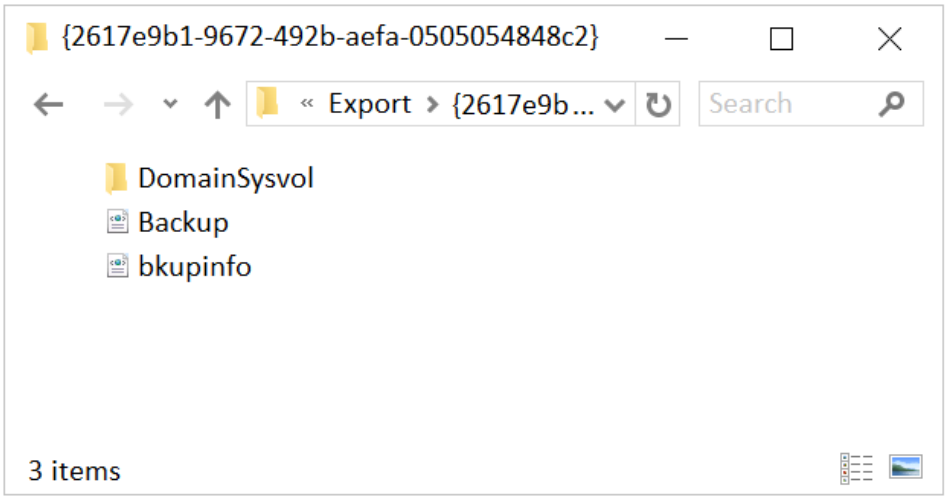
QUESTION 8

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

All domain controllers run Windows Server 2016.

The domain contains a server named Server1 that has Microsoft Security Compliance Manager (SCM) 4.0 installed.

You export the baseline shown in the following exhibit.



You have a server named Server2 that is a member of a workgroup.

You copy the (2617e9b1-9672-492b-aefa-0505054848c2) folder to Server2.

You need to deploy the baseline settings to Server2.

What should you do?

A. Download, install, and then fun the Lgpo.exe command.
B. From Group Policy Management import a Group Policy object (GPO).
C. From Windows PowerShell, run the Restore-GPO cmdlet.
D. From Windows PowerShell, run the Import-GPO cmdlet.
E. From a command prompt run the secedit.exe command and specify the /import parameter.

Answer: A

Explanation:

Server2 is a non-domain joined computer using the GPO pack feature.

Source: https://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx

LGPO.exe replaces the no-longer-maintained Local GPO tool that shipped with the Security Compliance Manager (SCM).

https://biogs.technet.microsoft.com/secgui de/2016/01/21/lgpo-exe-local-group-policy-object-utility-v1-0/

QUESTION 9

Hotspot Question

You plan to deploy three encrypted virtual machines that use Secure Boot. The virtual machines will be configured as shown in the following table.

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

How should you protect each virtual machine? To answer, select the appropriate options in the answer area.

Answer Area

VM1: [▼]
- An encryption-support virtual machine
- A shielded virtual machine

VM2: [▼]
- An encryption-support virtual machine
- A shielded virtual machine

VM3: [▼]
- An encryption-support virtual machine
- A shielded virtual machine

Answer:

Answer Area

VM1: [▼]
- An encryption-support virtual machine
- A shielded virtual machine

VM2: [▼]
- An encryption-support virtual machine
- A shielded virtual machine

VM3: [▼]
- An encryption-support virtual machine
- A shielded virtual machine

QUESTION 10

Hotspot Question

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

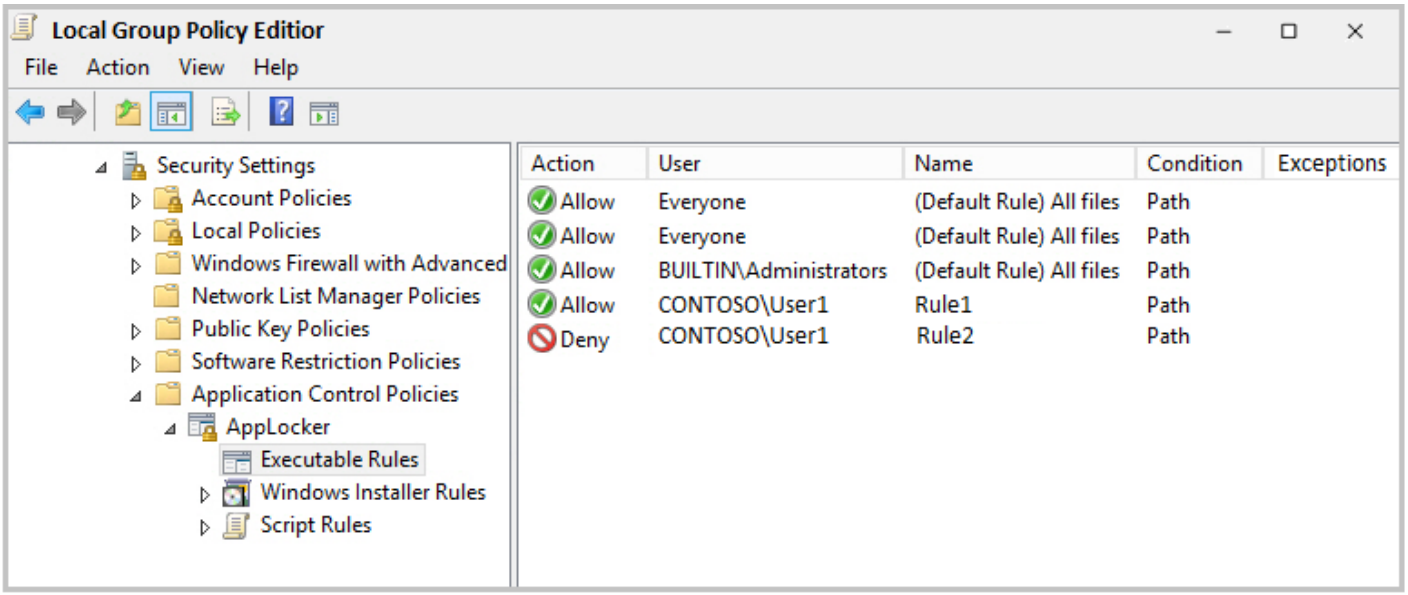
The domain contains a server named Server1 that runs Windows Server 2016.

The services on Server1 are shown in the following output.

```
PS C:\> get -service *ap*

Status     Name               DisplayName
--------   --------           -----------------
Running    AppHostSvc         Application Host Helper Service
Stopeed    AppIDSvc           Application Identity
Running    AppInfo            Application Information
Running    AppMgmt            Application Management
Running    AppReadiness       App Readiness
```

Server1 has the AppLocker rules configured as shown in the exhibit (Click the Exhibit button.)



Rule1 and Rule2 are configured a$ shown in the following table.

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

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

Answer Area

Statements	Yes	No
On Server1, User1 can run D:\Folder2\App1.exe	○	○
On Server1, User1 can run D:\Folder1\Program1.exe	○	○
If Program1.exe is copied from D:\Folder1 to D:\Folder2, User1 can run Program1.exe on Server1.	○	○

Answer:

Answer Area

Statements	Yes	No
On Server1, User1 can run D:\Folder2\App1.exe	●	○
On Server1, User1 can run D:\Folder1\Program1.exe	●	○
If Program1.exe is copied from D:\Folder1 to D:\Folder2, User1 can run Program1.exe on Server1.	○	●