Exam : **AZ-801**

Title : Configuring Windows Server Hybrid Advanced Services

Version : DEMO

1. Topic 1, Fabrikam inc

Case study
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview
Fabrikam, Inc. is a manufacturing company that has a main office in Chicago and a branch office in Paris.

Existing Environment
Identity Infrastructure
Fabrikam has an Active Directory Domain Services (AD DS) forest that syncs with an Azure Active Directory (Azure AD) tenant. The AD DS forest contains two domains named corp.fabrikam.com and europe.fabrikam.com.

Chicago Office On-Premises Servers
The office in Chicago contains on-premises servers that run Windows Server 2016 as shown in the following table.

Name	Type	Configuration
HV1	Physical	Hyper-V host
HV2	Physical	Hyper-V host
APP1	Virtual machine	Application server
APP2	Virtual machine	Application server
APP3	Virtual machine	Application server
APP4	Virtual machine	Application server
DC1	Virtual machine	Domain controller
Archive1	Physical	File server
DHCP1	Virtual machine	DHCP server
Fileserver1	Virtual machine	File server
WEB1	Virtual machine	Web server
WEB2	Virtual machine	Web server
AADC1	Virtual machine	Azure AD Connect

All the servers in the Chicago office are in the corp.fabrikam.com domain.
All the virtual machines in the Chicago office are hosted on HV1 and HV2. HV1 and HV2 are nodes in a failover cluster named Cluster1.
WEB1 and WEB2 run an Internet Information Services (IIS) website. Internet users connect to the website by using a URL of https://www.fabrikam.com.
All the users in the Chicago office run an application that connects to a UNC path of \\Fileserver1\Data.
Paris On-Premises Servers
The office in Paris contains a physical server named dc2.europe.fabrikam.com that runs Windows Server 2016 and is a domain controller for the europe.fabrikam.com domain. Network Infrastructure
The networks in both the Chicago and Paris offices have local internet connections. The Chicago and Paris offices are connected by using VPN connections.
The client computers in the Chicago office get IP addresses from DHCP1.

Security Risks
Fabrikam identifies the following security risks:
Some accounts connect to AD DS resources by using insecure protocols such as NTLMv1, SMB1, and unsigned LDAP.
Servers have Windows Defender Firewall enabled. Server administrators sometimes modify firewall rules and allow risky connections.

Requirements
Security Requirements
Fabrikam identifies the following security requirements:

Prevent server administrators from configuring Windows Defender Firewalls rules.
Encrypt all the data disks on the servers by using BitLocker Drive Encryption (BitLocker).
Ensure that only authorized applications can be installed or run on the servers in the forest.
Implement Microsoft Sentinel as a reporting solution to identify all connections to the domain controllers that use insecure protocols.

On-Premises Migration Plan
Fabrikam plans to migrate all the existing servers and identifies the following migration requirements:
Move the APP1 and APP2 virtual machines in the Chicago office to a new Hyper-V failover cluster named Cluster2 that will run Windows Server 2022.
- Cluster2 will contain two new nodes named HV3 and HV4.
- All virtual machine files will be stored on a Cluster Shared Volume (CSV).
Migrate Archive1 to a new failover cluster named Cluster3 that will run Windows Server 2022.
- Cluster3 will contain two physical nodes named Node1 and Node2.
- The file shares on Cluster3 will be a failover cluster role in active-passive mode.
Migrate all users, groups, and client computers from europe.fabrikam.com to corp.fabrikam.com.
- The migration will be performed by using the Active Directory Migration Tool (ADMT).
- A computer named ADMT computer will be deployed to the corp.fabrikam.com domain to run ADMT migration procedures.
- User accounts will retain their existing password.

Migrate the data share from Fileserver1 to a new server named Fileserver2 that will run Windows Server 2022. After the migration, the data share must be accessible by using the existing UNC path.

Azure Migration Plan
Fabrikam plans to migrate some resources to Azure and identifies the following migration requirements:
Create an Azure subscription named Sub1.
Create an Azure virtual network named Vnet1.
Use ExpressRoute to connect the Paris and Chicago offices to Vnet1.
License all servers for Microsoft Defender for servers.
Migrate APP3 and APP4 to Azure.
Migrate the www.fabrikam.com website to an Azure App Service web app named WebApp1.
Decommission WEB1 and WEB2.

DHCP Migration Plan
Fabrikam plans to replace DHCP1 with a new server named DHCP2 and identifies the following migration requirements:
Ensure that DHCP2 provides the same IP addresses that are currently available from DHCP1.
Prevent DHCP1 from servicing clients once services are enabled on DHCP2.
Ensure that the existing leases and reservations are migrated.

DRAG DROP
You are planning the implementation of Cluster2 to support the on-premises migration plan.
You need to ensure that the disks on Cluster2 meet the security requirements.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Add a disk resource to the cluster.	
Enable BitLocker on the volume.	
Update the BitLockerProtectorInfo property of the volume.	
Create a Cluster Shared Volume (CSV).	
Put the disk in maintenance mode.	

Answer:

Actions	Answer Area
Add a disk resource to the cluster.	Add a disk resource to the cluster.
Enable BitLocker on the volume.	Create a Cluster Shared Volume (CSV).
Update the BitLockerProtectorInfo property of the volume.	Put the disk in maintenance mode.
Create a Cluster Shared Volume (CSV).	Enable BitLocker on the volume.
Put the disk in maintenance mode.	Update the BitLockerProtectorInfo property of the volume.

Explanation:

Reference: https://docs.microsoft.com/en-us/windows-server/failover-clustering/bitlocker-on-csv-in-ws-2022

2.HOTSPOT

You need to implement a security policy solution to authorize the applications. The solution must meet the security requirements.

Which service should you use to enforce the security policy, and what should you use to manage the policy settings? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Enforce the security policy:
- Microsoft Defender Application Control
- Microsoft Defender Application Guard
- Microsoft Defender Credential Guard
- Microsoft Defender for Endpoint

Manage the policy settings:
- Configuration profiles in Microsoft Intune
- Compliance policies in Microsoft Intune
- Group Policy Objects (GPOs)

Answer:

Answer Area

Explanation:
Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/wdac-and-applocker-overview

3.You are remediating the firewall security risks to meet the security requirements.
What should you configure to reduce the risks?
A. a Group Policy Object (GPO)
B. adaptive network hardening in Microsoft Defender for Cloud
C. a network security group (NSG) in Sub1
D. an Azure Firewall policy
Answer: A
Explanation:
Firewall rules configured in a Group Policy Object cannot be modified by local server administrators.
Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/create-an-inbound-port-rule

4.You are planning the deployment of Microsoft Sentinel.
Which type of Microsoft Sentinel data connector should you use to meet the security requirements?
A. Threat Intelligence - TAXII
B. Azure Active Directory
C. Microsoft Defender for Cloud
D. Microsoft Defender for Identity
Answer: D
Explanation:
Reference: https://docs.microsoft.com/en-us/defender-for-identity/cas-isp-legacy-protocols

5.You are planning the migration of Archive1 to support the on-premises migration plan.
What is the minimum number of IP addresses required for the node and cluster roles on Cluster3?
A. 2
B. 3

C. 4
D. 5
Answer: B
Explanation:
One IP for each of the two nodes in the cluster and one IP for the cluster virtual IP (VIP).