IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **SC-100**

Title : Microsoft Cybersecurity Architect

Version : DEMO

1. Topic 1, Fabrikam, Inc Case Study 1

OverView
Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.

On-premises Environment
The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.

Azure Environment
Fabrikam has the following Azure resources:
• An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabnkam.com
• A single Azure subscription named Sub1
• A virtual network named Vnetl in the East US Azure region
• A virtual network named Vnet2 in the West Europe Azure region
• An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAR enabled
• A Microsoft Sentinel workspace
• An Azure SQL database named ClaimsDB that contains a table named ClaimDetails
• 20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud
• A resource group named TestRG that is used for testing purposes only
• An Azure Virtual Desktop host pool that contains personal assigned session hosts
All the resources in Sub1 are in either the East US or the West Europe region.

Partners
Fabrikam has contracted a company named Contoso, Ltd. to develop applications.
Contoso has the following infrastructure-.
• An Azure AD tenant named contoso.onmicrosoft.com
• An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of Fabrikam Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security Group named Contoso Developers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.
The ContosoDevelopers group is assigned the db.owner role for the ClaimsDB database.

Compliance Event
Fabrikam deploys the following compliance environment:
• Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.
• Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.
• Qualys is used as the standard vulnerability assessment tool for servers.

Problem Statements
The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation-. Machines should have a vulnerability assessment solution. All the virtual machines must be compliant in Defender for Cloud.

ClaimApp Deployment
Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specification
• ClaimsApp will be deployed to Azure App Service instances that connect to Vnetl and Vnet2.
• Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.
• ClaimsApp will access data in ClaimsDB.
• ClaimsDB must be accessible only from Azure virtual networks.
• The app services permission for ClaimsApp must be assigned to ClaimsDB.

Application Development Requirements
Fabrikam identifies the following requirements for application development:
• Azure DevTest labs will be used by developers for testing.
• All the application code must be stored in GitHub Enterprise.
• Azure Pipelines will be used to manage application deployments.
• All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text. Scanning must be done at the time the code is pushed to a repository.

Security Requirement
Fabrikam identifies the following security requirements:
• Internet-accessible applications must prevent connections that originate in North Korea.
• Only members of a group named InfraSec must be allowed to configure network security groups (NSGs} and instances of Azure Firewall, VJM. And Front Door in Sub1.
• Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

AWS Requirements
Fabrikam identifies the following security requirements for the data hosted in ContosoAWSV.
• Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.
• Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Contoso Developer Requirements
Fabrikam identifies the following requirements for the Contoso developers;
• Every month, the membership of the ContosoDevelopers group must be verified.
• The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.
• The Comoro developers must be prevented from viewing the data in a column named MedicalHistory in

the ClaimDetails table.

Compliance Requirement
Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPPA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

You need to recommend a solution to meet the security requirements for the InfraSec group.
What should you use to delegate the access?
A. a subscription
B. a custom role-based access control (RBAC) role
C. a resource group
D. a management group
Answer: B

2.You need to recommend a solution to scan the application code. The solution must meet the application development requirements.
What should you include in the recommendation?
A. Azure Key Vault
B. GitHub Advanced Security
C. Application Insights in Azure Monitor
D. Azure DevTest Labs
Answer: B
Explanation:
https://docs.microsoft.com/en-us/learn/modules/introduction-github-advanced-security/2-what-is-github-advanced-security

3.You need to recommend a solution to resolve the virtual machine issue.
What should you include in the recommendation? (Choose Two)
A. Onboard the virtual machines to Microsoft Defender for Endpoint.
B. Onboard the virtual machines to Azure Arc.
C. Create a device compliance policy in Microsoft Endpoint Manager.
D. Enable the Qualys scanner in Defender for Cloud.
Answer: A, D
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/switch-to-mde-phase-3?view=o365-worldwide

4.HOTSPOT
What should you create in Azure AD to meet the Contoso developer requirements?

Account type for the developers:	
	A guest account in the contoso.onmicrosoft.com tenant
	A guest account in the fabrikam.onmicrosoft.com tenant
	A synced user account in the corp.fabrikam.com domain
	A user account in the fabrikam.onmicrosoft.com tenant

Component in Identity Governance:	
	A connected organization
	An access package
	An access review
	An Azure AD role
	An Azure resource role

Answer:

Account type for the developers:	
	A guest account in the contoso.onmicrosoft.com tenant
	A guest account in the fabrikam.onmicrosoft.com tenant
	A synced user account in the corp.fabrikam.com domain
	A user account in the fabrikam.onmicrosoft.com tenant

Component in Identity Governance:	
	A connected organization
	An access package
	An access review
	An Azure AD role
	An Azure resource role

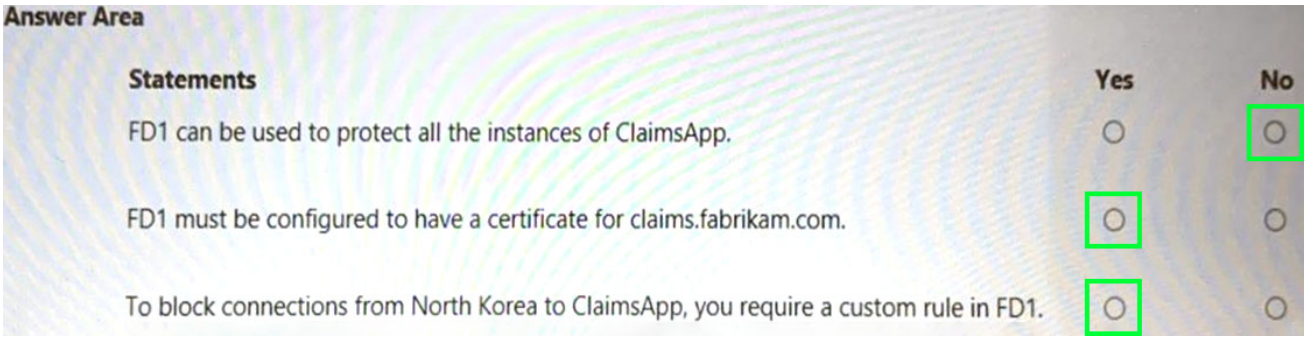
Explanation:
Box 1: A synced user account -
Need to use a synched user account.
Box 2: An access review
https://docs.microsoft.com/en-us/azure/active-directory-domain-services/synchronization
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

5.HOTSPOT
You are evaluating the security of ClaimsApp.
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
FD1 can be used to protect all the instances of ClaimsApp.	○	○
FD1 must be configured to have a certificate for claims.fabrikam.com.	○	○
To block connections from North Korea to ClaimsApp, you require a custom rule in FD1.	○	○

Answer:



Explanation:

No

Yes

Yes