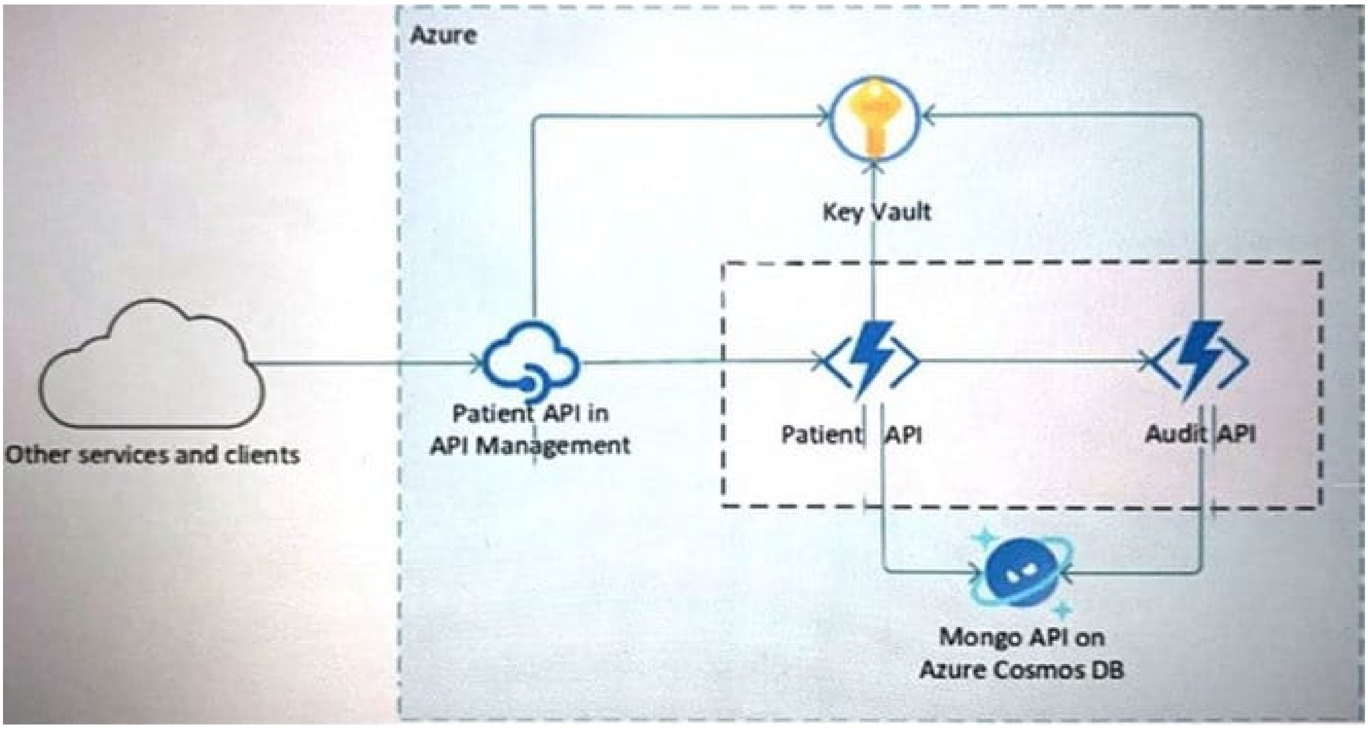
SC-100$^{Q\&As}$

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

QUESTION 1

Your company is developing a serverless application in Azure that will have the architecture shown in the following exhibit.



You need to recommend a solution to isolate the compute components on an Azure virtual network. What should you include in the recommendation?

A. Azure Active Directory (Azure AD) enterprise applications

B. an Azure App Service Environment (ASE)

C. Azure service endpoints

D. an Azure Active Directory (Azure AD) application proxy

Correct Answer: B

The Azure App Service Environment v2 is an Azure App Service feature that provides a fully isolated and dedicated environment for securely running App Service apps at high scale. This capability can host your:

1.

Windows web apps

2.

Linux web apps

3.

Docker containers

4.

Mobile apps

5.

Functions

App Service environments (ASEs) are appropriate for application workloads that require:

Very high scale.

Isolation and secure network access.

High memory utilization.

Customers can create multiple ASEs within a single Azure region or across multiple Azure regions. This flexibility makes ASEs ideal for horizontally scaling stateless application tiers in support of high requests per second (RPS) workloads.

Reference: https://docs.microsoft.com/en-us/azure/app-service/environment/intro

QUESTION 2

You have a Microsoft 365 subscription.

You are designing a user access solution that follows the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).

You need to recommend a solution that automatically restricts access to Microsoft Exchange Online, SharePoint Online, and Teams in near-real-time (NRT) in response to the following Azure AD events:

1.

A user account is disabled or deleted.

2.

The password of a user is changed or reset.

3.

All the refresh tokens for a user are revoked.

4.

Multi-factor authentication (MFA) is enabled for a user.

Which two features should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. continuous access evaluation

B. Azure AD Application Proxy

C. a sign-in risk policy

D. Azure AD Privileged Identity Management (PIM)

E. Conditional Access

Correct Answer: AE

Continuous access evaluation

Key benefits

User termination or password change/reset: User session revocation will be enforced in near real time.

Network location change: Conditional Access location policies will be enforced in near real time.

Token export to a machine outside of a trusted network can be prevented with Conditional Access location policies.

Scenarios

There are two scenarios that make up continuous access evaluation, critical event evaluation and Conditional Access policy evaluation.

*

Critical event evaluation Continuous access evaluation is implemented by enabling services, like Exchange Online, SharePoint Online, and Teams, to subscribe to critical Azure AD events. Those events can then be evaluated and enforced near real time. Critical event evaluation doesn\\'t rely on Conditional Access policies so it\\'s available in any tenant. The following events are currently evaluated:

User Account is deleted or disabled Password for a user is changed or reset Multi-factor authentication is enabled for the user Administrator explicitly revokes all refresh tokens for a user High user risk detected by Azure AD Identity Protection

*

Conditional Access policy evaluation

Exchange Online, SharePoint Online, Teams, and MS Graph can synchronize key Conditional Access policies for evaluation within the service itself.

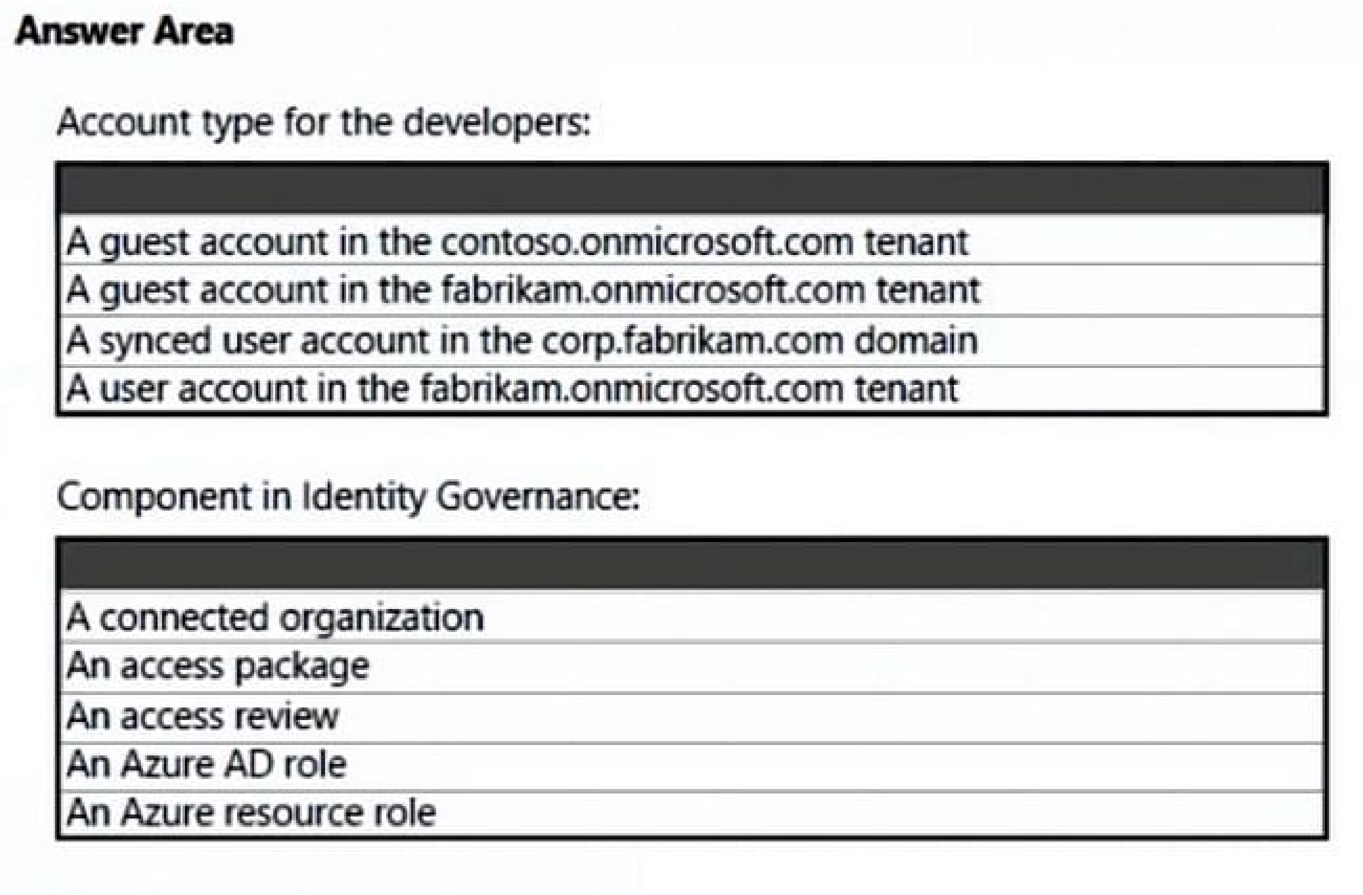
This process enables the scenario where users lose access to organizational files, email, calendar, or tasks from Microsoft 365 client apps or SharePoint Online immediately after network location changes.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation

QUESTION 3

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

Hot Area:



Answer Area

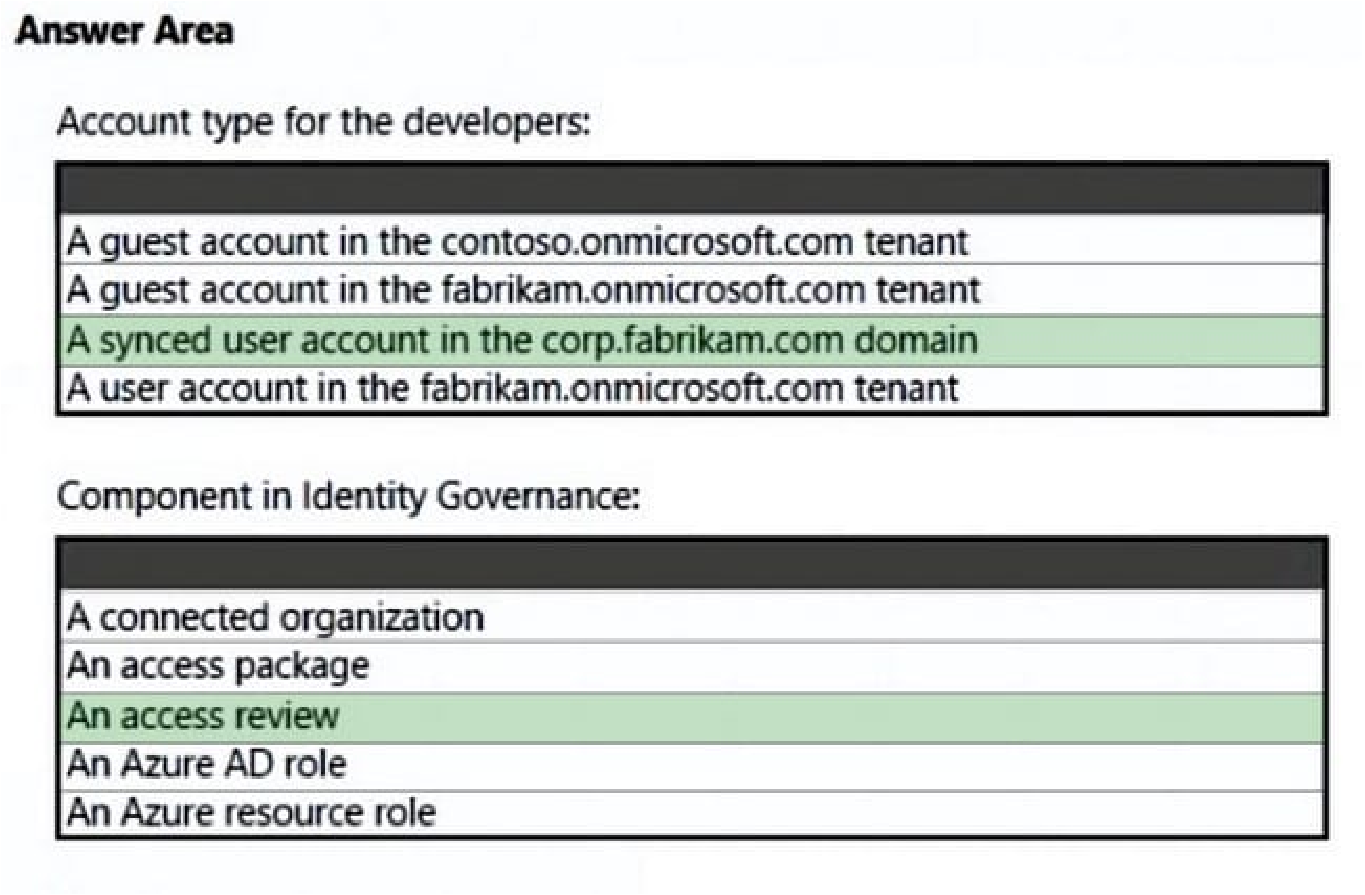
Account type for the developers:

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

Correct Answer:



Answer Area

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

Box 1: A synced user account

Need to use a synched user account.

Incorrect:

*

Not A user account in the fabrikam.onmicrosoft.com tenant

The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.

*

Guest accounts would not meet the requirements.

Note: 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 ContosoDevelopers 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.

Contoso Developers 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 Contoso developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Box 2: An access review

Scenario: Every month, the membership of the ContosoDevelopers group must be verified.

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User\\'s access can be reviewed on a regular basis to make sure only

the right people have continued access.

Access review is part of Azure AD Identity governance.

Reference:

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

QUESTION 4

You have a Microsoft 365 tenant.

Your company uses a third-party software as a service (SaaS) app named App1 that is integrated with an Azure AD tenant.

You need to design a security strategy to meet the following requirements:

- Users must be able to request access to App1 by using a self-service request.
- When users request access to App1, they must be prompted to provide additional information about their request.
- Every three months, managers must verify that the users still require access to App1. What should you include in the design?

A.

Microsoft Entra Identity Governance

B.

connected apps in Microsoft Defender for Cloud Apps

C.

access policies in Microsoft Defender for Cloud Apps

D.

Azure AD Application Proxy

Correct Answer: A

QUESTION 5

Your company is developing an invoicing application that will use Azure Active Directory (Azure AD) B2C. The application will be deployed as an App Service web app.

You need to recommend a solution to the application development team to secure the application from identity-related attacks.

Which two configurations should you recommend? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Azure AD workbooks to monitor risk detections

B. Azure AD Conditional Access integration with user flows and custom policies

C. smart account lockout in Azure AD B2C

D. access packages in Identity Governance

E. custom resource owner password credentials (ROPC) flows in Azure AD B2C

Correct Answer: BC

B. Azure AD Conditional Access integration with user flows and custom policies

C. Smart account lockout in Azure AD B2C.

Conditional Access in Azure Active Directory (Azure AD) is a feature that enables you to enforce security policies and control access to applications based on specific conditions

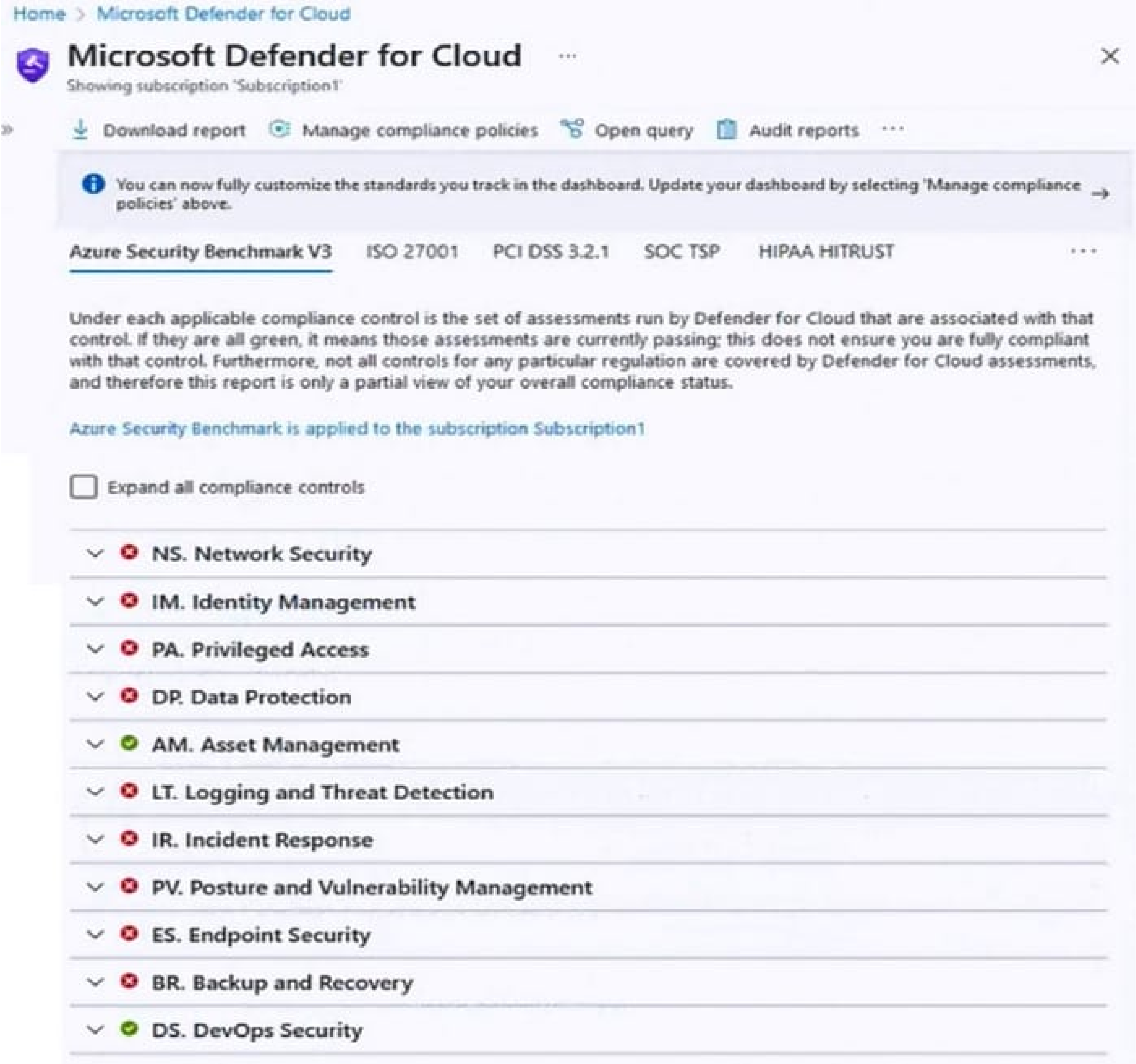
https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management

https://docs.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user-flow?pivots=b2c-user-flow

QUESTION 6

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You are evaluating the Azure Security Benchmark V3 report as shown in the following exhibit.


Home > Microsoft Defender for Cloud
Microsoft Defender for Cloud
Download report
Manage compliance policies
Open query
Audit reports
Azure Security Benchmark V3
ISO 27001
PCI DSS 3.2.1
SOC TSP
HIPAA HITRUST

Showing subscription 'Subscription1'

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above.

Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

Azure Security Benchmark is applied to the subscription Subscription1

□ Expand all compliance controls

- ✗ NS. Network Security
- ✗ IM. Identity Management
- ✗ PA. Privileged Access
- ✗ DP. Data Protection
- ✓ AM. Asset Management
- ✗ LT. Logging and Threat Detection
- ✗ IR. Incident Response
- ✗ PV. Posture and Vulnerability Management
- ✗ ES. Endpoint Security
- ✗ BR. Backup and Recovery
- ✓ DS. DevOps Security

You need to verify whether Microsoft Defender for servers is installed on all the virtual machines that run Windows. Which compliance control should you evaluate?

A. Asset Management

B. Posture and Vulnerability Management

C. Data Protection

D. Endpoint Security

E. Incident Response

Correct Answer: D

Microsoft Defender for servers compliance control installed on Windows

Defender for clout "Endpoint Security" azure security benchmark v3

Endpoint Security covers controls in endpoint detection and response, including use of endpoint detection and response (EDR) and anti-malware service for endpoints in Azure environments.

Security Principle: Enable Endpoint Detection and Response (EDR) capabilities for VMs and integrate with SIEM and security operations processes.

Azure Guidance: Azure Defender for servers (with Microsoft Defender for Endpoint integrated) provides EDR capability to prevent, detect, investigate, and respond to advanced threats.

Use Microsoft Defender for Cloud to deploy Azure Defender for servers for your endpoint and integrate the alerts to your SIEM solution such as Azure Sentinel.

Incorrect:

Not A: Asset Management covers controls to ensure security visibility and governance over Azure resources, including recommendations on permissions for security personnel, security access to asset inventory, and managing approvals for

services and resources (inventory, track, and correct).

Not B: Posture and Vulnerability Management focuses on controls for assessing and improving Azure security posture, including vulnerability scanning, penetration testing and remediation, as well as security configuration tracking, reporting,

and correction in Azure resources.

Not C: Data Protection covers control of data protection at rest, in transit, and via authorized access mechanisms, including discover, classify, protect, and monitor sensitive data assets using access control, encryption, key and certificate

management in Azure.

Not E: Incident Response covers controls in incident response life cycle - preparation, detection and analysis, containment, and post-incident activities, including using Azure services such as Microsoft Defender for Cloud and Sentinel to

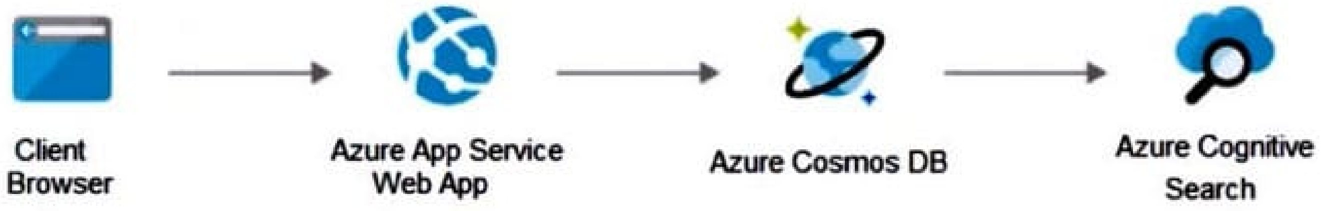
automate the incident response process.

Reference: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security

QUESTION 7

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 on-premises network contains an e-commerce web app that was developed in Angular and Node,js. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.

Solution: You recommend implementing Azure Front Door with Azure Web Application Firewall (WAF).

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead use solution: You recommend creating private endpoints for the web app and the database layer.

Note:

How to Use Azure Private Endpoints to Restrict Public Access to WebApps.

As an Azure administrator or architect, you are sometimes asked the question: “How can we safely deploy internal business applications to Azure App Services?”

These applications characteristically are:

Not accessible from the public internet.

Accessible from within the on-premises corporate network

Accessible via an authorized VPN client from outside the corporate network.

For such scenarios, we can use Azure Private Links, which enables private and secure access to Azure PaaS services over Azure Private Endpoints, along with the Site-to-Site VPN, Point-to-Site VPN, or the Express Route. Azure Private

Endpoint is a read-only network interface service associated with the Azure PAAS Services. It allows you to bring deployed sites into your virtual network, limiting access to them at the network level.

It uses one of the private IP addresses from your Azure VNet and associates it with the Azure App Services. These services are called Private Link resources. They can be Azure Storage, Azure Cosmos DB, SQL, App Services Web App,

your own / partner owned services, Azure Backups, Event Grids, Azure Service Bus, or Azure Automations.

Reference: https://www.varonis.com/blog/securing-access-azure-webapps

QUESTION 8

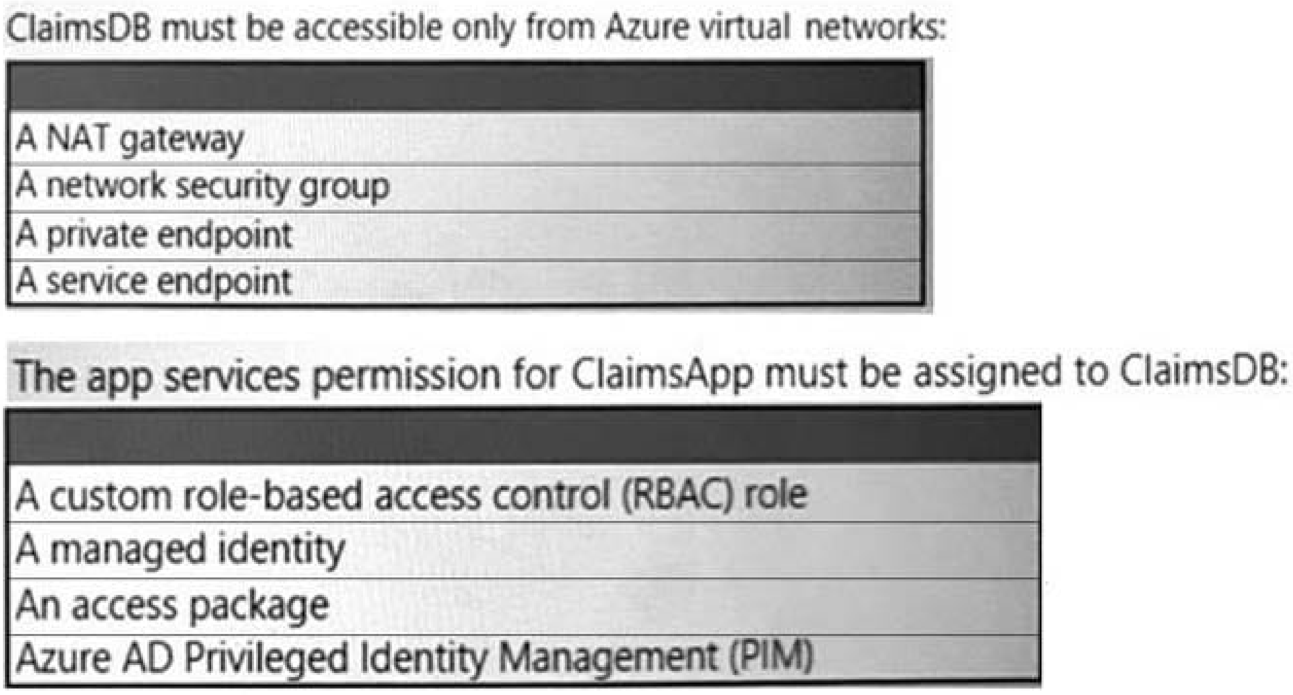
HOTSPOT

You need to recommend a solution to meet the requirements for connections to ClaimsDB.

What should you recommend using for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



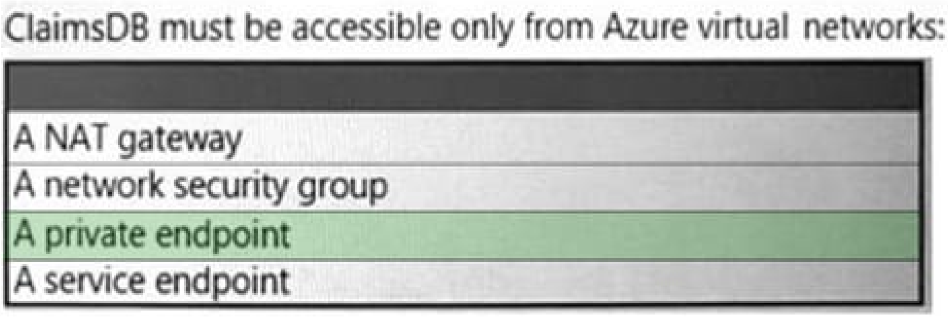
ClaimsDB must be accessible only from Azure virtual networks:

- A NAT gateway
- A network security group
- A private endpoint
- A service endpoint

The app services permission for ClaimsApp must be assigned to ClaimsDB:

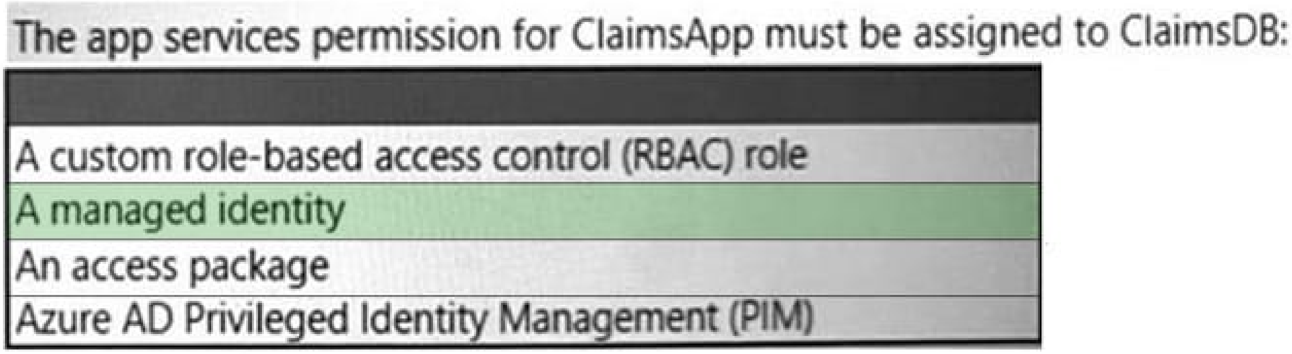
- A custom role-based access control (RBAC) role
- A managed identity
- An access package
- Azure AD Privileged Identity Management (PIM)

Correct Answer:



ClaimsDB must be accessible only from Azure virtual networks:

A NAT gateway
A network security group
[✓ A private endpoint]
A service endpoint



The app services permission for ClaimsApp must be assigned to ClaimsDB:

A custom role-based access control (RBAC) role
[✓ A managed identity]
An access package
Azure AD Privileged Identity Management (PIM)

Box 1: A private endpoint Scenario: An Azure SQL database named ClaimsDB that contains a table named ClaimDetails

Requirements. ClaimsApp Deployment.

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specifications:

1.

ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.

2.

Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.

3.

ClaimsApp will access data in ClaimsDB.

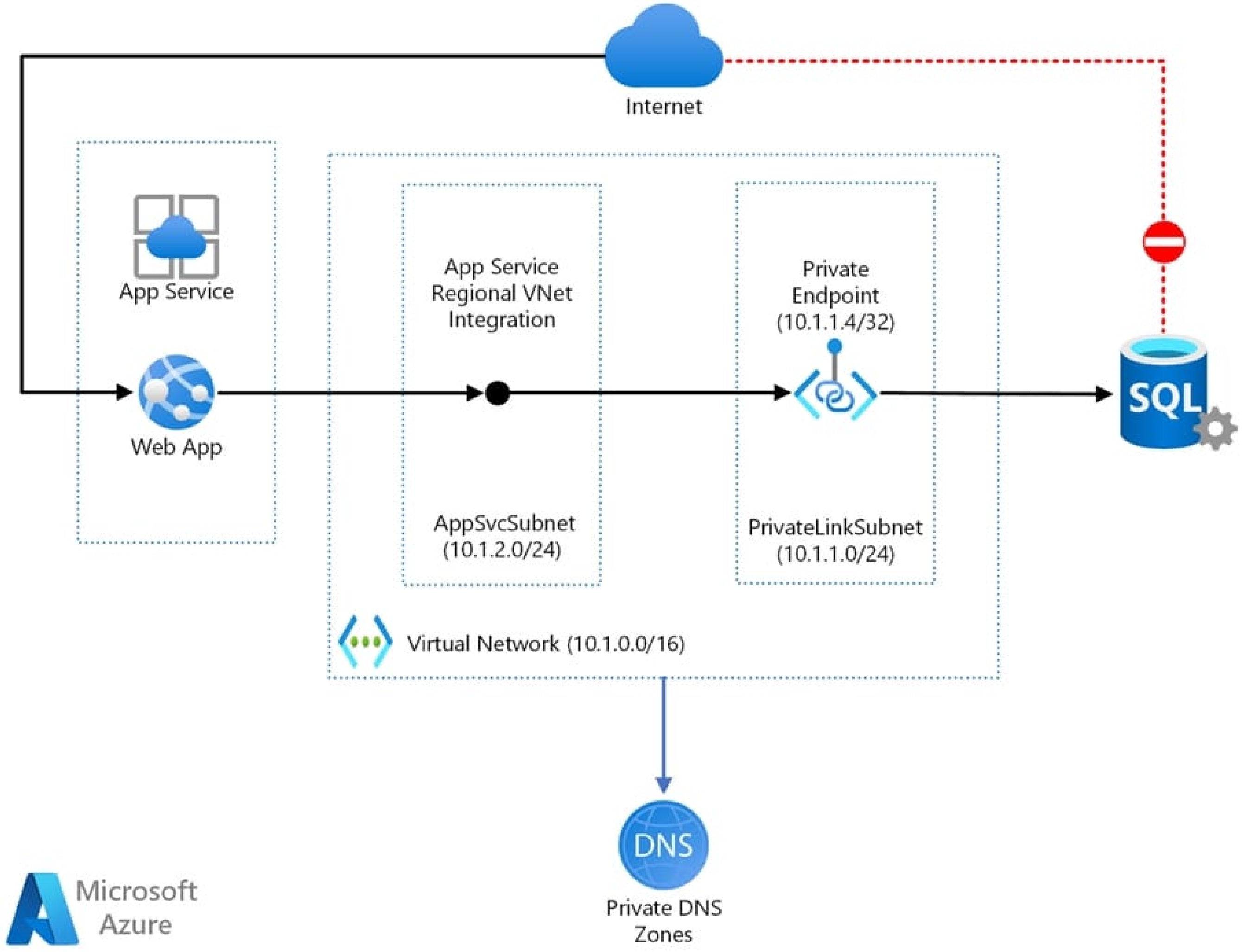
4.

ClaimsDB must be accessible only from Azure virtual networks.

5.

The app services permission for ClaimsApp must be assigned to ClaimsDB.

Web app private connectivity to Azure SQL Database. Architecture: Workflow



1.

Using Azure App Service regional VNet Integration, the web app connects to Azure through an AppSvcSubnet delegated subnet in an Azure Virtual Network.

2.

In this example, the Virtual Network only routes traffic and is otherwise empty, but other subnets and workloads could also run in the Virtual Network.

3.

The App Service and Private Link subnets could be in separate peered Virtual Networks, for example as part of a hub-and-spoke network configuration.

4.

Azure Private Link sets up a private endpoint for the Azure SQL Database in the PrivateLinkSubnet of the Virtual Network.

5.

The web app connects to the SQL Database private endpoint through the PrivateLinkSubnet of the Virtual Network.

The database firewall allows only traffic coming from the PrivateLinkSubnet to connect, making the database inaccessible from the public internet.

Box 2: A managed identity Managed identities for Azure resources provide Azure services with an automatically managed identity in Azure Active Directory. Using a managed identity, you can authenticate to any service that supports Azure AD authentication without managing credentials.

Reference: https://docs.microsoft.com/en-us/azure/architecture/example-scenario/private-web-app/private-web-app
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identities-status

QUESTION 9

Your company is developing a new Azure App Service web app.

You are providing design assistance to verify the security of the web app.

You need to recommend a solution to test the web app for vulnerabilities such as insecure server configurations, cross-site scripting (XSS), and SQL injection.

What should you include in the recommendation?

A. dynamic application security testing (DAST)

B. static application security testing (SAST)

C. interactive application security testing (IAST)

D. runtime application self-protection (RASP)

Correct Answer: A

Dynamic application security testing (DAST) is a process of testing an application in an operating state to find security vulnerabilities. DAST tools analyze programs while they are executing to find security vulnerabilities such as memory

corruption, insecure server configuration, cross-site scripting, user privilege issues, SQL injection, and other critical security concerns.

Incorrect:

Not B: SAST tools analyze source code or compiled versions of code when the code is not executing in order to find security flaws.

Not C: IAST (interactive application security testing) analyzes code for security vulnerabilities while the app is run by an automated test, human tester, or any activity “interacting” with the application functionality.

IAST works inside the application, which makes it different from both static analysis (SAST) and dynamic analysis (DAST). This type of testing also doesn\\'t test the entire application or codebase, but only whatever is exercised by the

functional test.

Not D: Runtime Application Self Protection (RASP) is a security solution designed to provide personalized protection to applications. It takes advantage of insight into an application\\'s internal data and state to enable it to identify threats at

runtime that may have otherwise been overlooked by other security solutions.

RASP\\'s focused monitoring makes it capable of detecting a wide range of threats, including zero-day attacks. Since RASP has insight into the internals of an application, it can detect behavioral changes that may have been caused by a novel

attack. This enables it to respond to even zero-day attacks based upon how they affect the target application.

Reference: https://docs.microsoft.com/en-us/azure/security/develop/secure-develop

QUESTION 10

You design cloud-based software as a service (SaaS) solutions.

You need to recommend a recovery solution for ransomware attacks. The solution must follow Microsoft Security Best Practices.

What should you recommend doing first?

A. Develop a privileged identity strategy.

B. Implement data protection.

C. Develop a privileged access strategy.

D. Prepare a recovery plan.

Correct Answer: D

Recommend a ransomware strategy by using Microsoft Security Best Practices The three important phases of ransomware protection are:

*

create a recovery plan

*

limit the scope of damage

*

harden key infrastructure elements

Plan for ransomware protection and extortion-based attacks Phase 1 of ransomware protection is to develop a recovery plan. The first thing you should do for these attacks is prepare your organization so that it has a viable alternative to paying the ransom. While attackers in control of your organization have a variety of ways to pressure you into paying, the demands

primarily focus on two categories:

Pay to regain access

Pay to avoid disclosure

Reference:

https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/

https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/2-plan-for-ransomware-protection-extortion-based-attacks

QUESTION 11

HOTSPOT

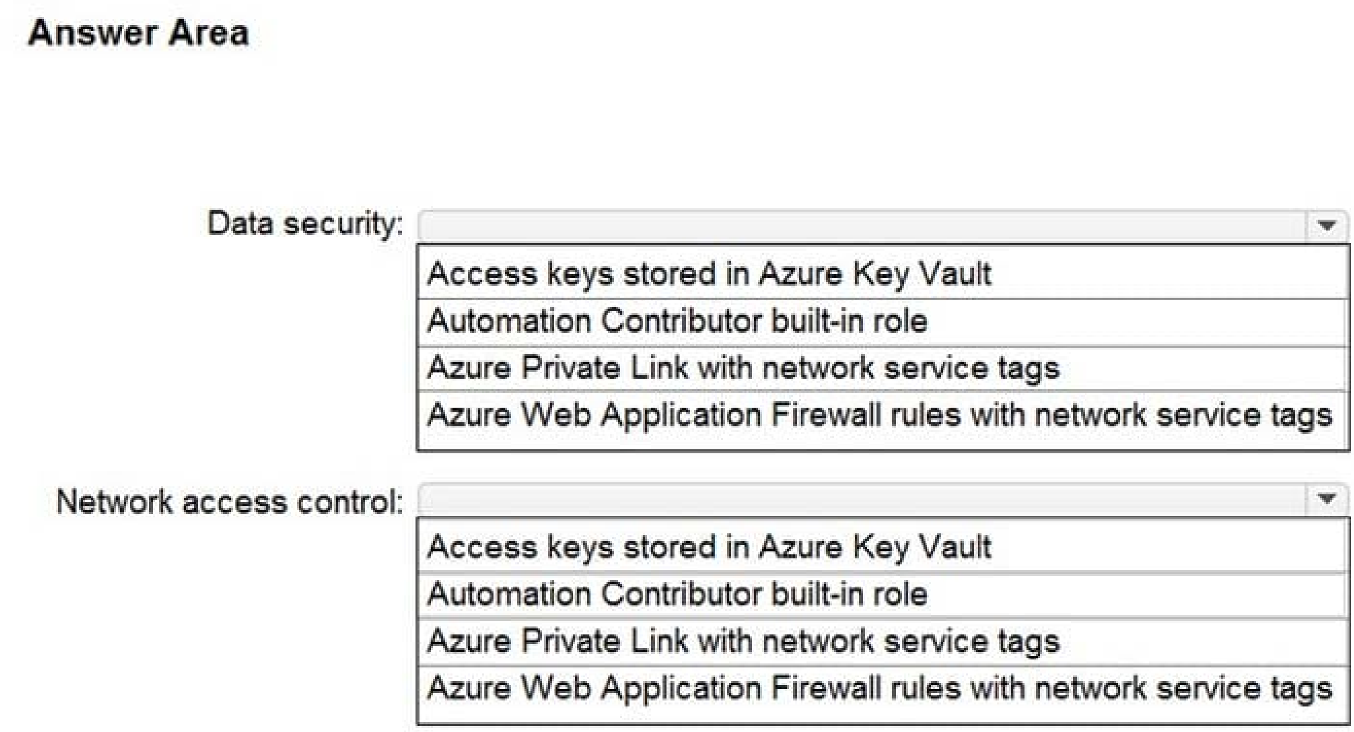
You are designing security for a runbook in an Azure Automation account. The runbook will copy data to Azure Data Lake Storage Gen2.

You need to recommend a solution to secure the components of the copy process.

What should you include in the recommendation for each component? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

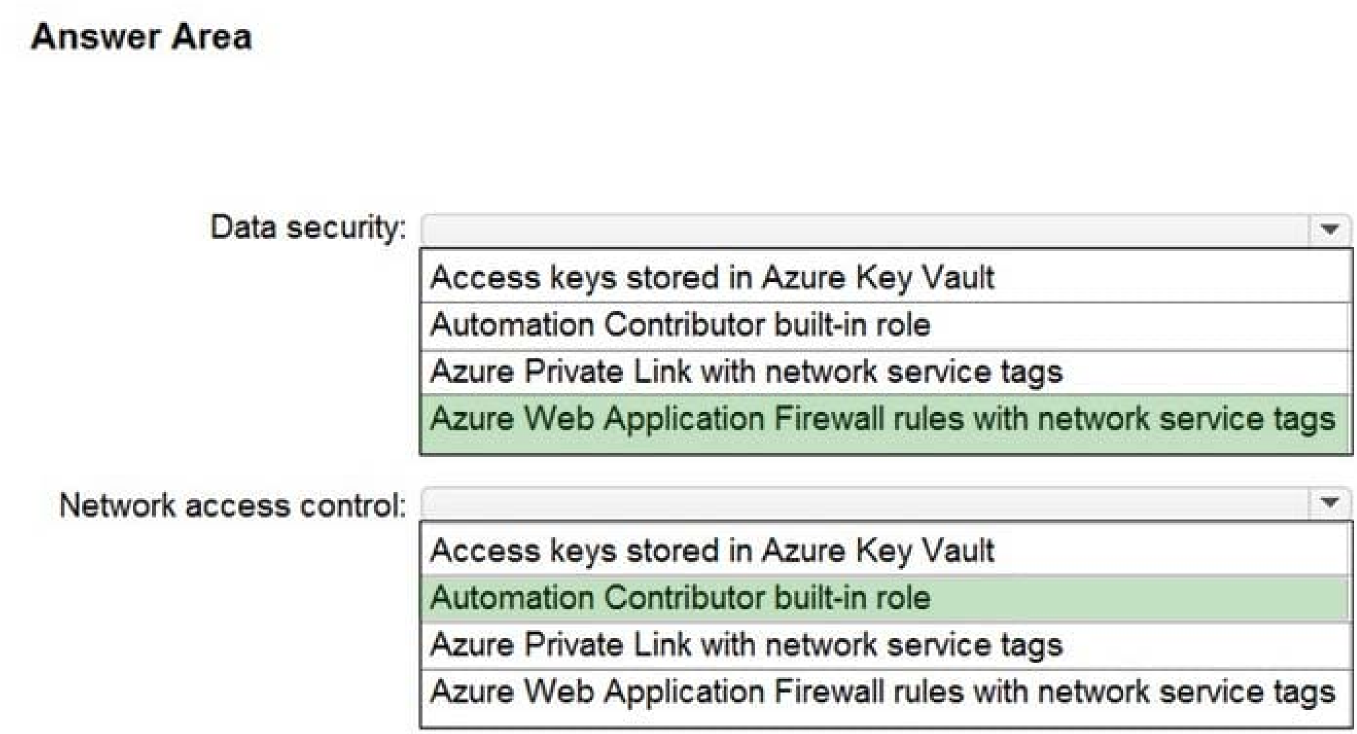


Answer Area

Data security: ▼
- Access keys stored in Azure Key Vault
- Automation Contributor built-in role
- Azure Private Link with network service tags
- Azure Web Application Firewall rules with network service tags

Network access control: ▼
- Access keys stored in Azure Key Vault
- Automation Contributor built-in role
- Azure Private Link with network service tags
- Azure Web Application Firewall rules with network service tags

Correct Answer:



Answer Area

Data security:

- Access keys stored in Azure Key Vault
- Automation Contributor built-in role
- Azure Private Link with network service tags
- [✓ Azure Web Application Firewall rules with network service tags]

Network access control:

- Access keys stored in Azure Key Vault
- [✓ Automation Contributor built-in role]
- Azure Private Link with network service tags
- Azure Web Application Firewall rules with network service tags

Box 1: Azure Web Application Firewall with network service tags A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change, minimizing the complexity of frequent updates to network security rules.

You can use service tags to define network access controls on network security groups, Azure Firewall, and user-defined routes.

Incorrect:

* Not Azure private link with network service tags Network service tags are not used with Private links.

Box 2: Automation Contributor built-in role

The Automation Contributor role allows you to manage all resources in the Automation account, except modifying other user\\'s access permissions to an Automation account.

Reference: https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview

https://docs.microsoft.com/en-us/azure/automation/automation-role-based-access-control

QUESTION 12

You have an Azure subscription that contains virtual machines.

Port 3389 and port 22 are disabled for outside access.

You need to design a solution to provide administrators with secure remote access to the virtual machines. The solution must meet the following requirements:

1.

Prevent the need to enable ports 3389 and 22 from the internet.

2.

Only provide permission to connect the virtual machines when required.

3.

Ensure that administrators use the Azure portal to connect to the virtual machines.

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

NOTE: Each correct selection is worth one point.

A. Configure Azure VPN Gateway.

B. Enable Just Enough Administration (JEA).

C. Configure Azure Bastion.

D. Enable just-in-time (JIT) VM access.

E. Enable Azure AD Privileged Identity Management (PIM) roles as virtual machine contributors.

Correct Answer: CD

C: Bastion provides secure remote access.

It uses RDP/SSH session is over TLS on port 443.

Note: Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network.

It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines don\\'t need a public IP address, agent, or special client

software.

D: Lock down inbound traffic to your Azure Virtual Machines with Microsoft Defender for Cloud\\'s just-in-time (JIT) virtual machine (VM) access feature. This reduces exposure to attacks while providing easy access when you need to connect

to a VM.

Meets the requirement: Only provide permission to connect the virtual machines when required

Incorrect:

Not B: Does not address: Only provide permission to connect the virtual machines when required

Just Enough Administration (JEA) is a security technology that enables delegated administration for anything managed by PowerShell. With JEA, you can:

Reduce the number of administrators on your machines using virtual accounts or group-managed service accounts to perform privileged actions on behalf of regular users.

Limit what users can do by specifying which cmdlets, functions, and external commands they can run.

Better understand what your users are doing with transcripts and logs that show you exactly which commands a user executed during their session.

Not E: Does not help with the remote access.

Note: Classic Virtual Machine Contributor: Lets you manage classic virtual machines, but not access to them, and not the virtual network or storage account they\\'re connected to.

Reference: https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.2 https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

QUESTION 13

HOTSPOT

Your company has a Microsoft 365 E5 subscription, an Azure subscription, on-premises applications, and Active Directory Domain Services (AD DS).

You need to recommend an identity security strategy that meets the following requirements:

1.

Ensures that customers can use their Facebook credentials to authenticate to an Azure App Service website

2.

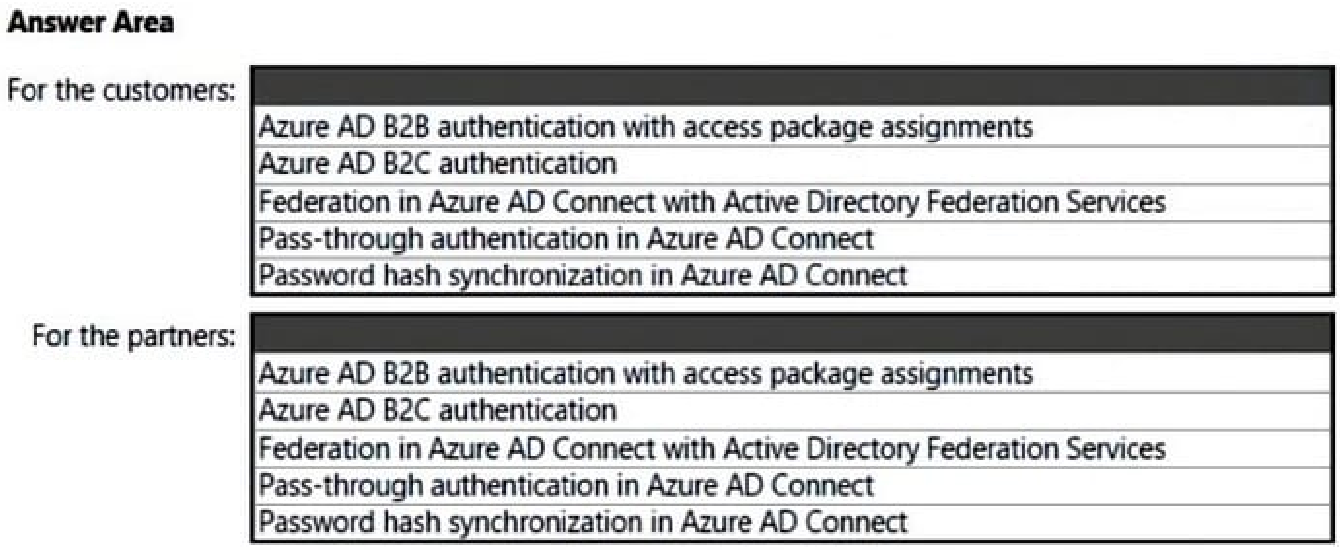
Ensures that partner companies can access Microsoft SharePoint Online sites for the project to which they are assigned

The solution must minimize the need to deploy additional infrastructure components.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

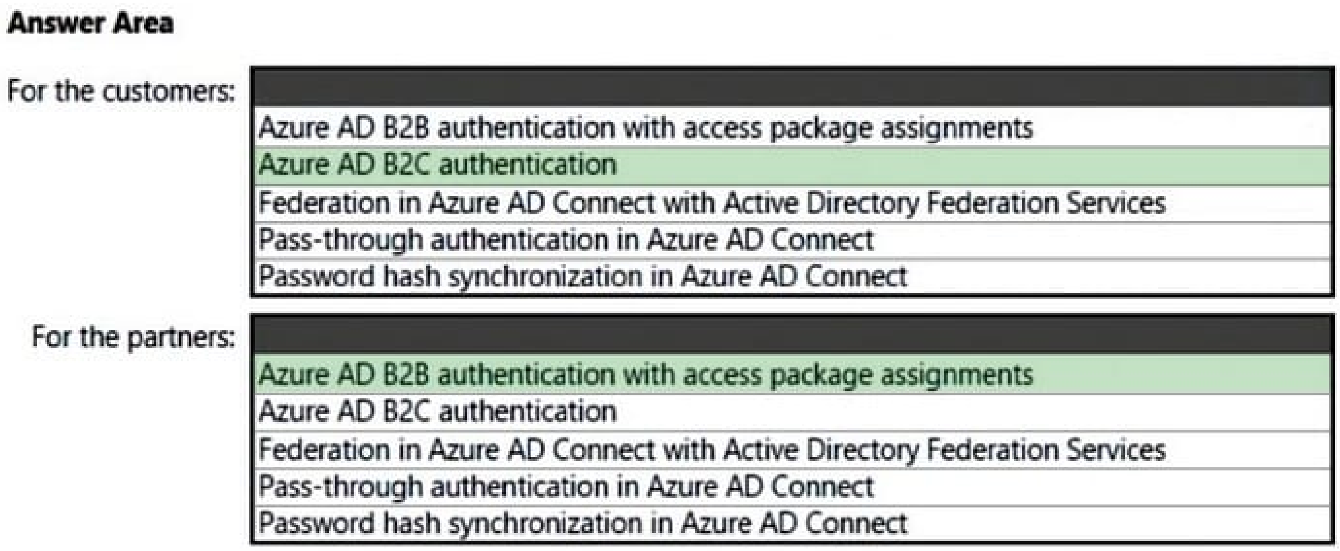
For the customers:

- Azure AD B2B authentication with access package assignments
- Azure AD B2C authentication
- Federation in Azure AD Connect with Active Directory Federation Services
- Pass-through authentication in Azure AD Connect
- Password hash synchronization in Azure AD Connect

For the partners:

- Azure AD B2B authentication with access package assignments
- Azure AD B2C authentication
- Federation in Azure AD Connect with Active Directory Federation Services
- Pass-through authentication in Azure AD Connect
- Password hash synchronization in Azure AD Connect

Correct Answer:



Answer Area

For the customers:

- Azure AD B2B authentication with access package assignments
- [✓ Azure AD B2C authentication]
- Federation in Azure AD Connect with Active Directory Federation Services
- Pass-through authentication in Azure AD Connect
- Password hash synchronization in Azure AD Connect

For the partners:

- [✓ Azure AD B2B authentication with access package assignments]
- Azure AD B2C authentication
- Federation in Azure AD Connect with Active Directory Federation Services
- Pass-through authentication in Azure AD Connect
- Password hash synchronization in Azure AD Connect

Box 1: Azure AD B2C authentication

Ensures that customers can use their Facebook credentials to authenticate to an Azure App Service website.

You can set up sign-up and sign-in with a Facebook account using Azure Active Directory B2C.

Box 2: Azure AD B2B authentication with access package assignments

Govern access for external users in Azure AD entitlement management

Azure AD entitlement management uses Azure AD business-to-business (B2B) to share access so you can collaborate with people outside your organization. With Azure AD B2B, external users authenticate to their home directory, but have a

representation in your directory. The representation in your directory enables the user to be assigned access to your resources.

Incorrect:

Not: Password hash synchronization in Azure AD connect

The partners are not integrated with AD DS.

Reference: https://docs.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-facebook?pivots=b2c-user-flow

https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users

https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-integration