Microsoft.Pre.SC-100.18q - DEMO

Number: SC-100
Passing Score: 800
Time Limit: 120 min

Exam Code: SC-100
Exam Name: Microsoft Cybersecurity Architect
Certification Provider: Microsoft
Corresponding Certification: Microsoft Certified: Cybersecurity Architect Expert
Website: https://VCEup.com/

Topic 01

QUESTION 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.

A.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
You need to recommend a solution to resolve the virtual machine issue. What should you include in the recommendation?

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5
You need to recommend a solution to secure the MedicalHistory data in the ClaimsDetail table. The solution must meet the Contoso developer requirements.
What should you include in the recommendation?

A. Transparent Data Encryption (TDE)
B. Always Encrypted
C. row-level security (RLS)
D. dynamic data masking
E. data classification

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
You need to recommend a solution to meet the security requirements for the virtual machines. What should you include in the recommendation?

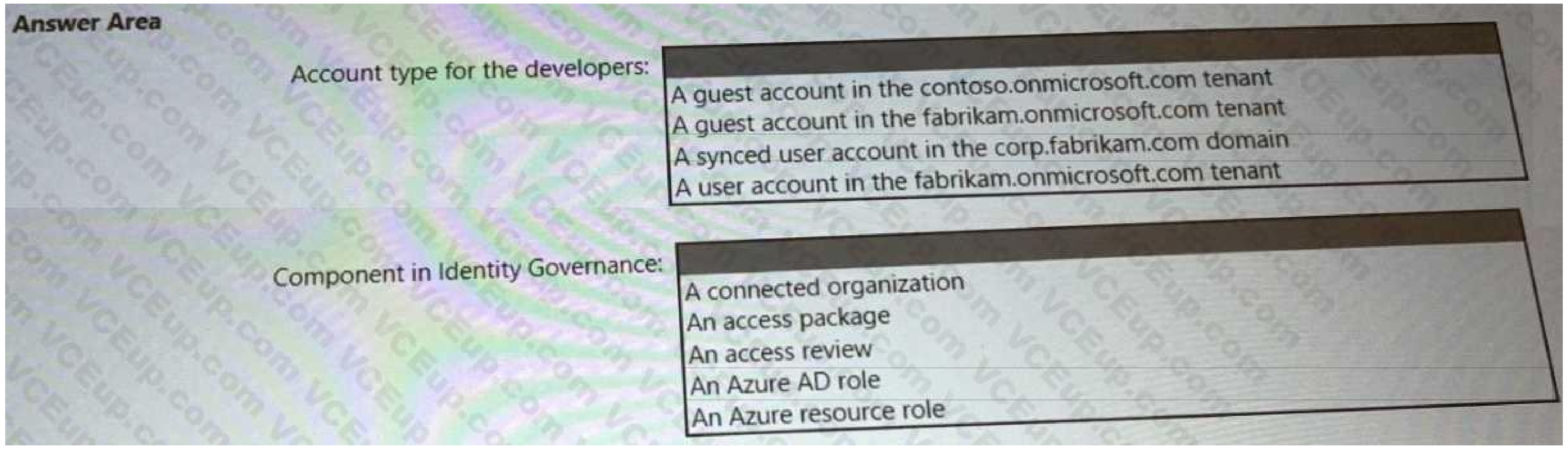
A. an Azure Bastion host
B. a network security group (NSG)
C. just-in-time (JIT) VM access
D. Azure Virtual Desktop

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
HOTSPOT
What should you create in Azure AD to meet the Contoso developer requirements?

Hot Area:

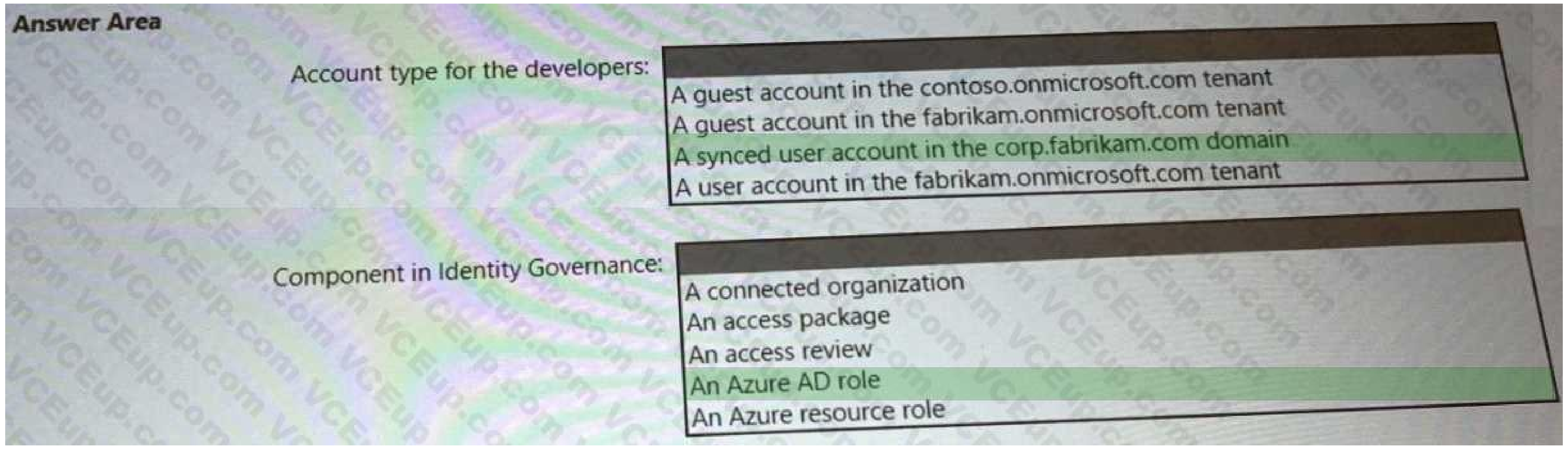


Answer Area

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:

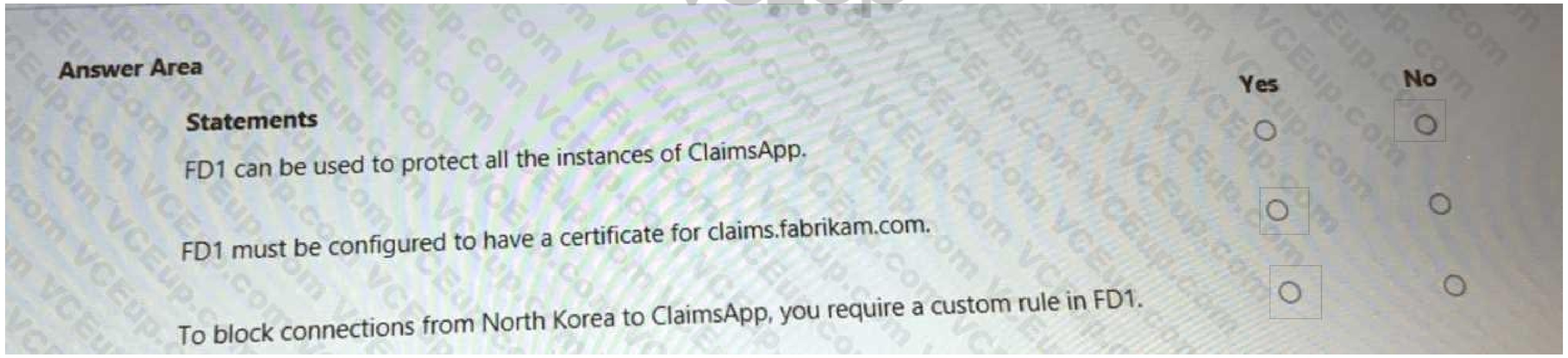
- A connected organization
- An access package
- An access review
- [✓ An Azure AD role]
- An Azure resource role

Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
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.

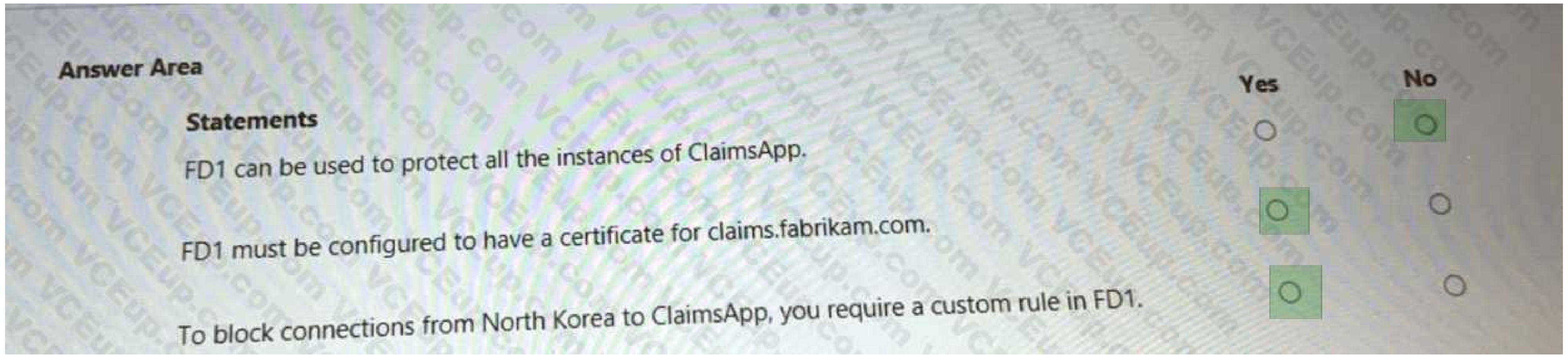
Hot Area:



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.	○	○

Correct Answer:



Answer Area

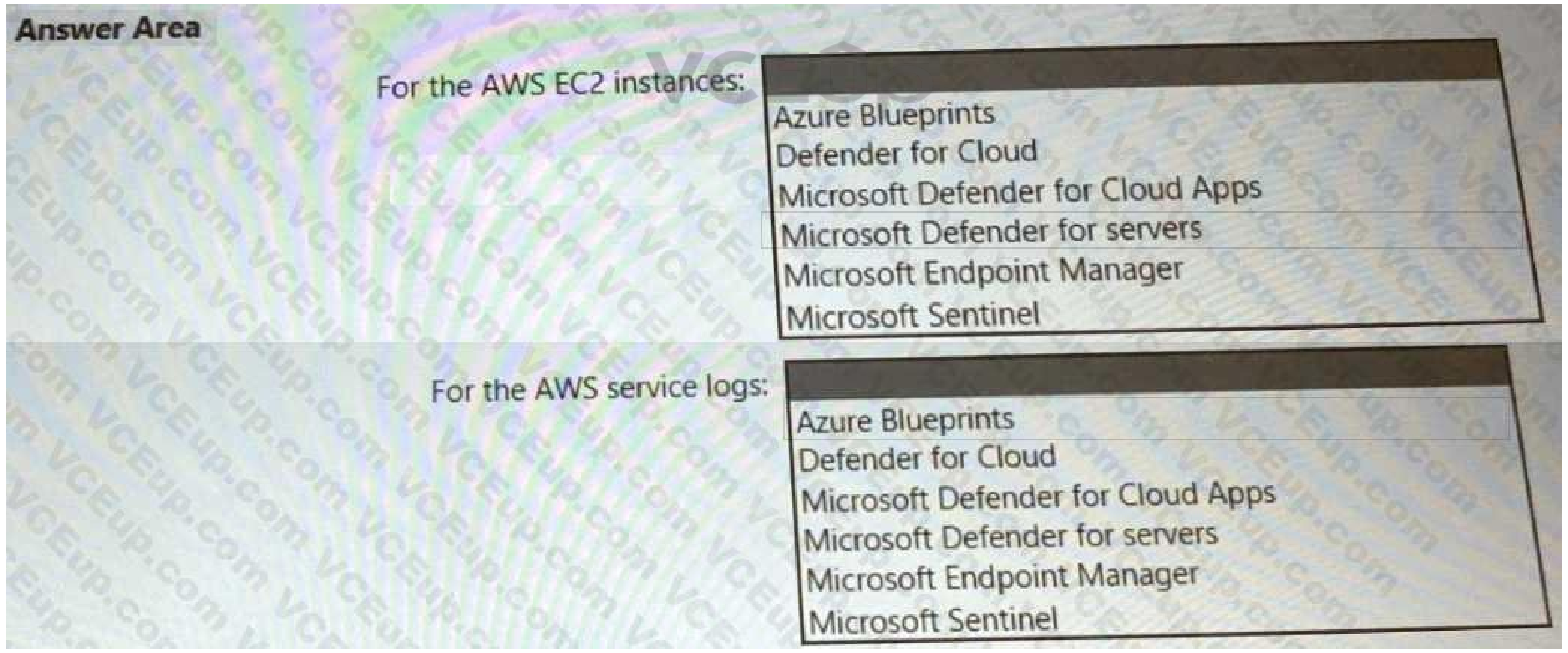
Statements	Yes	No
FD1 can be used to protect all the instances of ClaimsApp.	○	[✓ ○]
FD1 must be configured to have a certificate for claims.fabrikam.com.	[✓ ○]	○
To block connections from North Korea to ClaimsApp, you require a custom rule in FD1.	[✓ ○]	○

Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
HOTSPOT
You need to recommend a solution to meet the AWS requirements.
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

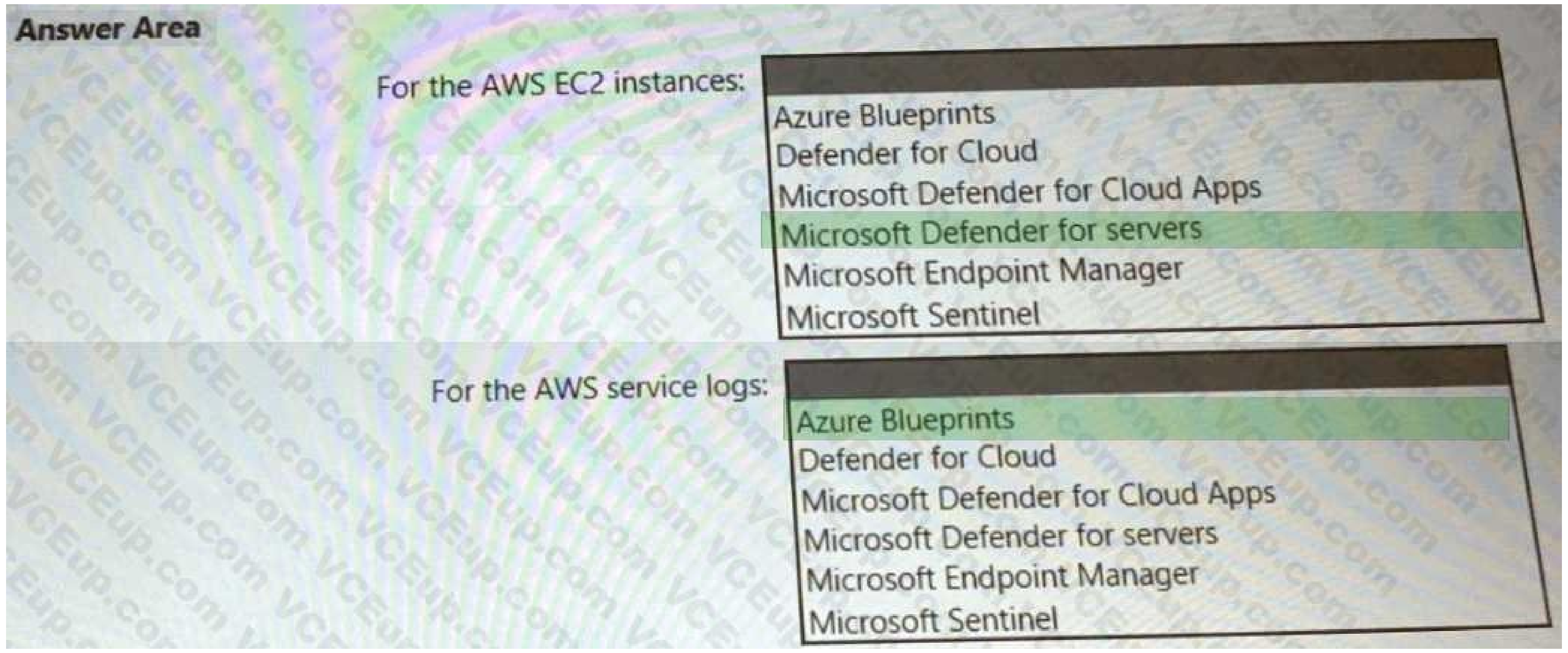
For the AWS EC2 instances:

- Azure Blueprints
- Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for servers
- Microsoft Endpoint Manager
- Microsoft Sentinel

For the AWS service logs:

- Azure Blueprints
- Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for servers
- Microsoft Endpoint Manager
- Microsoft Sentinel

Correct Answer:



Answer Area

For the AWS EC2 instances:

- Azure Blueprints
- Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for servers
- Microsoft Endpoint Manager
- Microsoft Sentinel

For the AWS service logs:

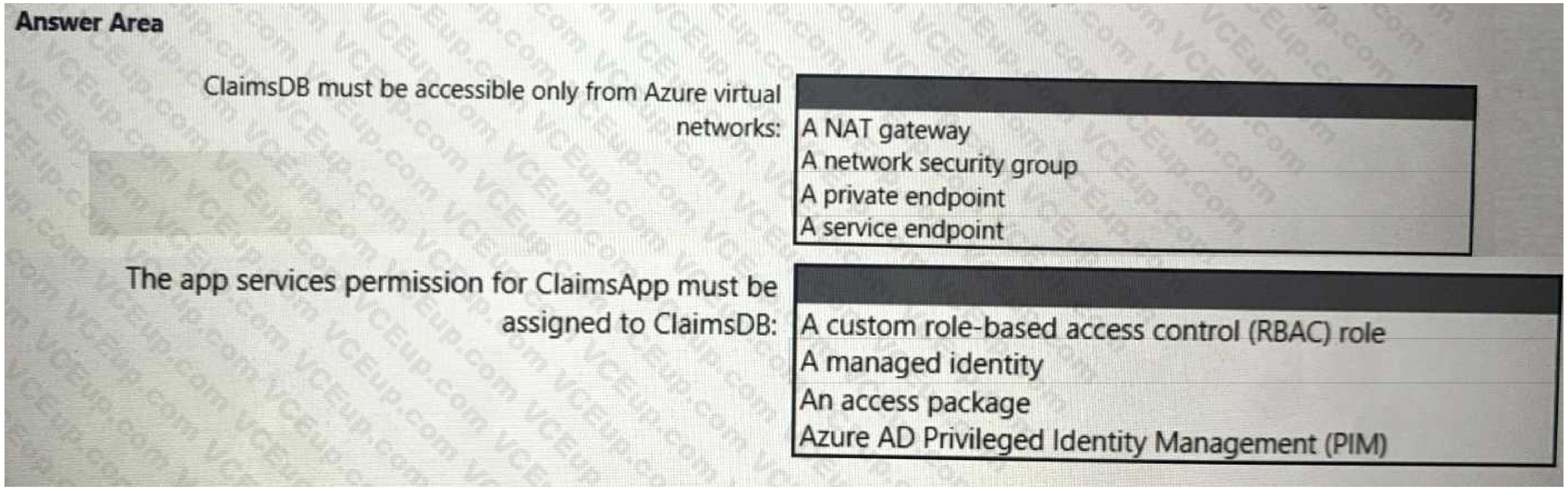
- Azure Blueprints
- Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for servers
- Microsoft Endpoint Manager
- Microsoft Sentinel

Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
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:



Answer Area

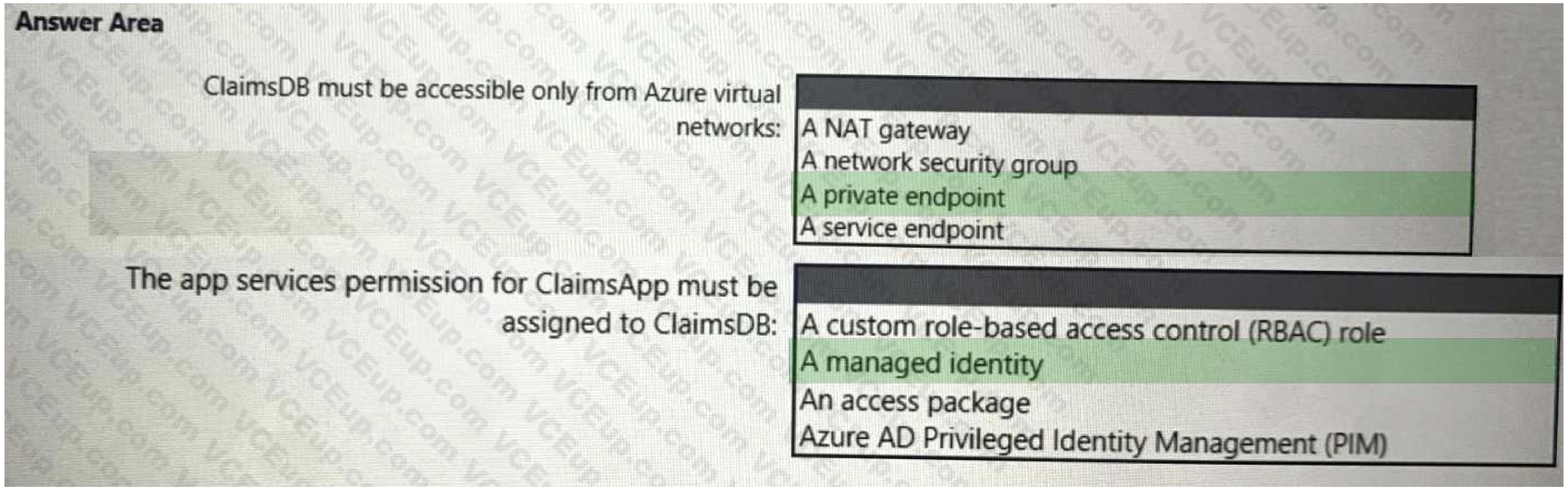
ClaimsDB must be accessible only from Azure virtual networks:

- 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:



Answer 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:

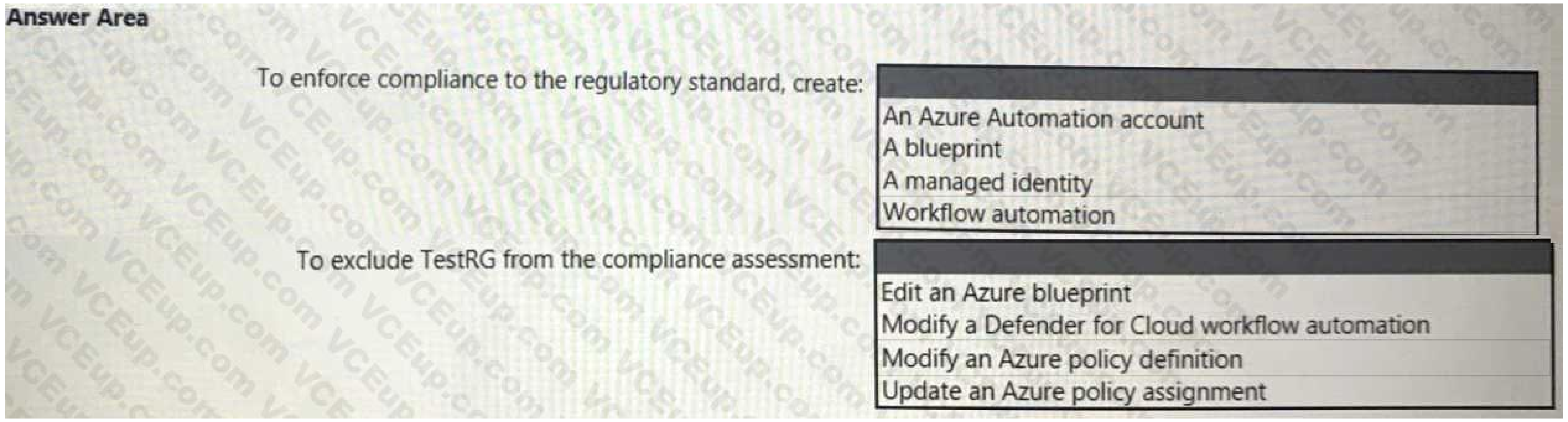
- A custom role-based access control (RBAC) role
- [✓ A managed identity]
- An access package
- Azure AD Privileged Identity Management (PIM)

Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
HOTSPOT
You need to recommend a solution to meet the compliance requirements.
What should you recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

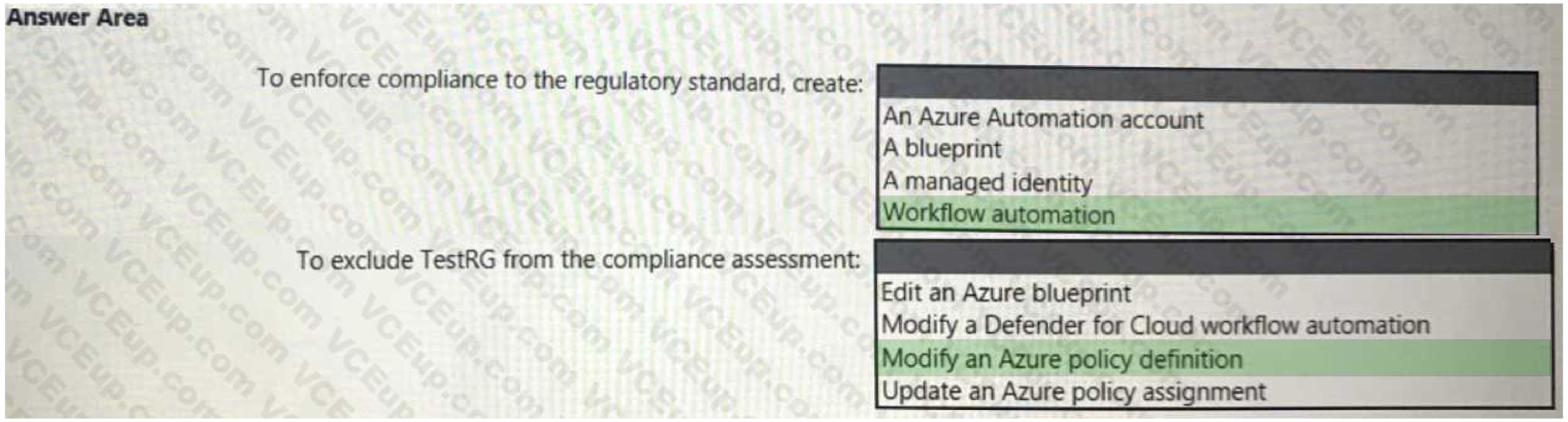
To enforce compliance to the regulatory standard, create:

- An Azure Automation account
- A blueprint
- A managed identity
- Workflow automation

To exclude TestRG from the compliance assessment:

- Edit an Azure blueprint
- Modify a Defender for Cloud workflow automation
- Modify an Azure policy definition
- Update an Azure policy assignment

Correct Answer:



Answer Area

To enforce compliance to the regulatory standard, create:

- An Azure Automation account
- A blueprint
- A managed identity
- [✓ Workflow automation]

To exclude TestRG from the compliance assessment:

- Edit an Azure blueprint
- Modify a Defender for Cloud workflow automation
- [✓ Modify an Azure policy definition]
- Update an Azure policy assignment

Section: (none)
Explanation

Explanation/Reference:

Topic 02

QUESTION 1

Overview

Litware, inc. is a financial services company that has main offices in New York and San Francisco. litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.

Litware has grown significantly during the last two years due to mergers and acquisitions. The acquisitions include several companies based in France.

Existing Environment

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD D%) forest named Utvvare.com and is linked to 20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.

The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Planned Changes

Litware plans to implement the following changes:

- Create a management group hierarchy for each Azure AD tenant.
- Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.
- Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Business Requirements

Litware identifies the following business requirements:

- Minimize any additional on-premises infrastructure.
- Minimize the operational costs associated with administrative overhead.

Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

- Enable the management of on-premises resources from Azure, including the following:
- Use Azure Policy for enforcement and compliance evaluation.
- Provide change tracking and asset inventory.
- Implement patch management.
- Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAK) capabilities of Microsoft Sentinel. The company wants to centralize Security Operations Center (SOQ by using Microsoft Sentinel.

Identity Requirements

Litware identifies the following identity requirements:

- Detect brute force attacks that directly target AD DS user accounts.
- Implement leaked credential detection in the Azure AD tenant of Litware.
- Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.
- Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for.
- The management of group properties, membership, and licensing « The management of user properties, passwords, and licensing
- The delegation of user management based on business units.

Regulatory Compliance Requirements

Litware identifies the following regulatory compliance requirements:

- insure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.
- Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.
- Use the principle of least privilege.

Azure Landing Zone Requirements

Litware identifies the following landing zone requirements:

- Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.
- Provide a secure score scoped to the landing zone.
- Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
- Minimize the possibility of data exfiltration.
- Maximize network bandwidth.

The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:

- Be created in a dedicated subscription.
- Use a DNS namespace of litware.com.

Application Security Requirements

Litware identifies the following application security requirements:

- Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.
- Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

A.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
To meet the application security requirements, which two authentication methods must the applications support? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Security Assertion Markup Language (SAML)
B. NTLMv2
C. certificate-based authentication
D. Kerberos

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
You need to recommend a solution for securing the landing zones. The solution must meet the landing zone requirements and the business requirements.
What should you configure for each landing zone?

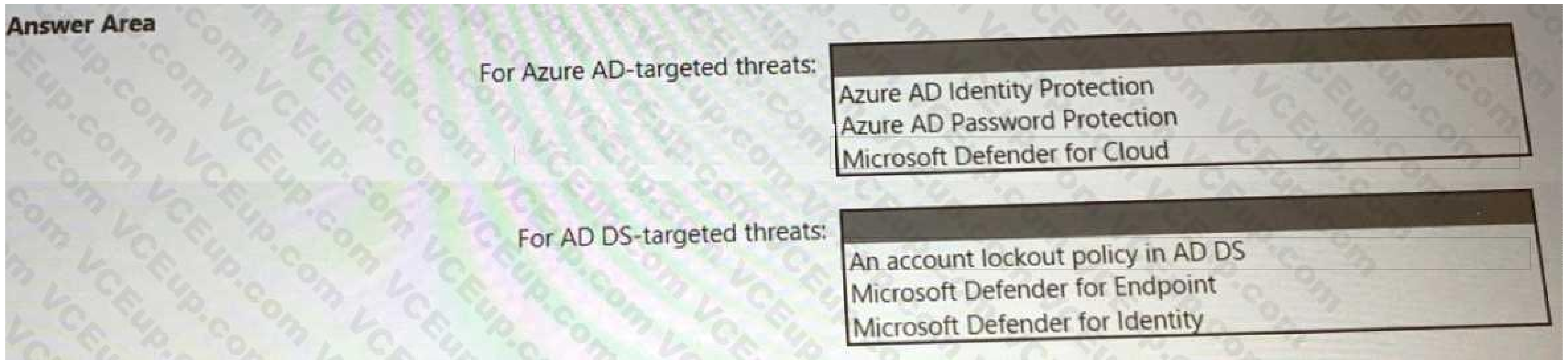
A. Azure DDoS Protection Standard
B. an Azure Private DNS zone
C. Microsoft Defender for Cloud
D. an ExpressRoute gateway

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
HOTSPOT
You need to recommend a strategy for securing the litware.com forest. The solution must meet the identity requirements. What should you include in the recommendation? To answer, select the appropriate options in the answer are a.
NOTE; Each correct selection is worth one point.

Hot Area:

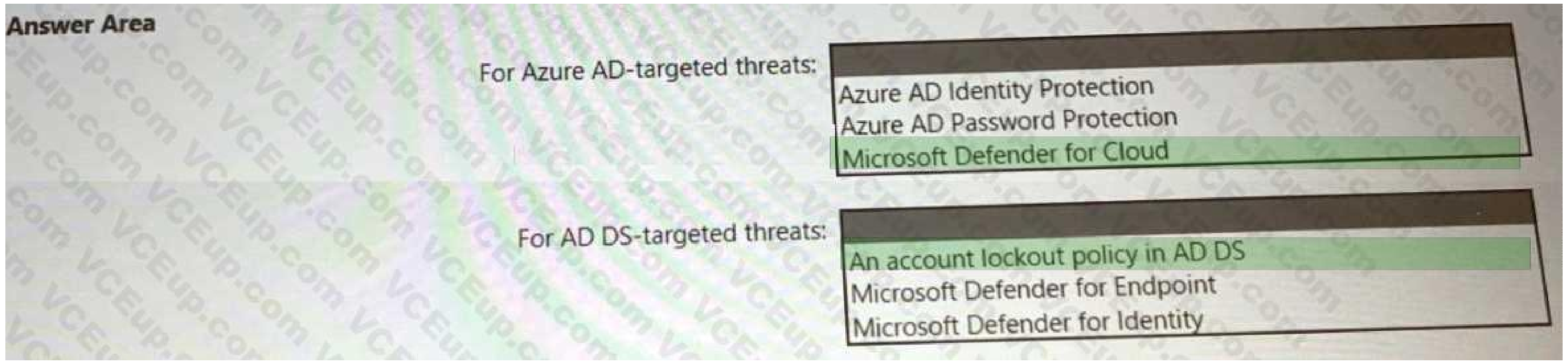


Answer Area

For Azure AD-targeted threats:
- Azure AD Identity Protection
- Azure AD Password Protection
- Microsoft Defender for Cloud

For AD DS-targeted threats:
- An account lockout policy in AD DS
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity

Correct Answer:



Answer Area

For Azure AD-targeted threats:
- Azure AD Identity Protection
- Azure AD Password Protection
- [✓ Microsoft Defender for Cloud]

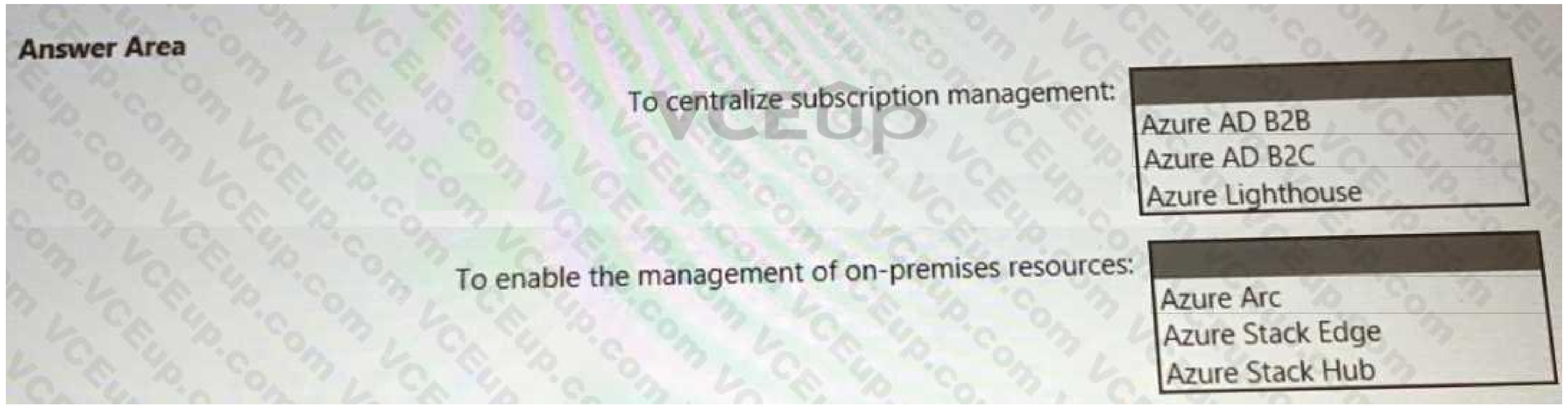
For AD DS-targeted threats:
- [✓ An account lockout policy in AD DS]
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity

Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
HOTSPOT
You need to recommend a multi-tenant and hybrid security solution that meets to the business requirements and the hybrid requirements. What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

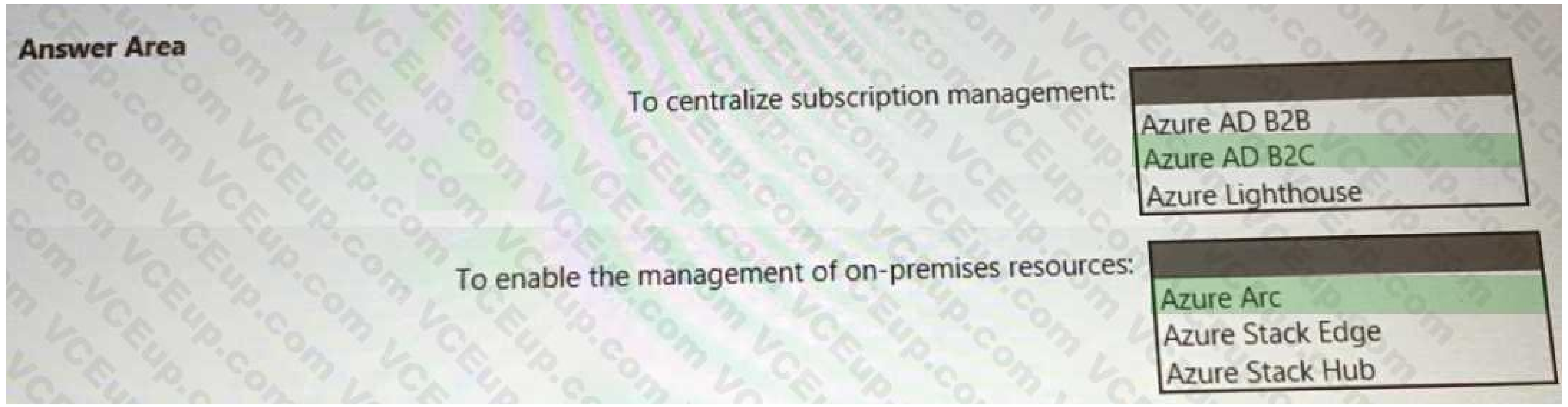


Answer Area

To centralize subscription management:
- Azure AD B2B
- Azure AD B2C
- Azure Lighthouse

To enable the management of on-premises resources:
- Azure Arc
- Azure Stack Edge
- Azure Stack Hub

Correct Answer:



Answer Area

To centralize subscription management:
- Azure AD B2B
- [✓ Azure AD B2C]
- Azure Lighthouse

To enable the management of on-premises resources:
- [✓ Azure Arc]
- Azure Stack Edge
- Azure Stack Hub

Section: (none)
Explanation

Explanation/Reference:

QUESTION 6

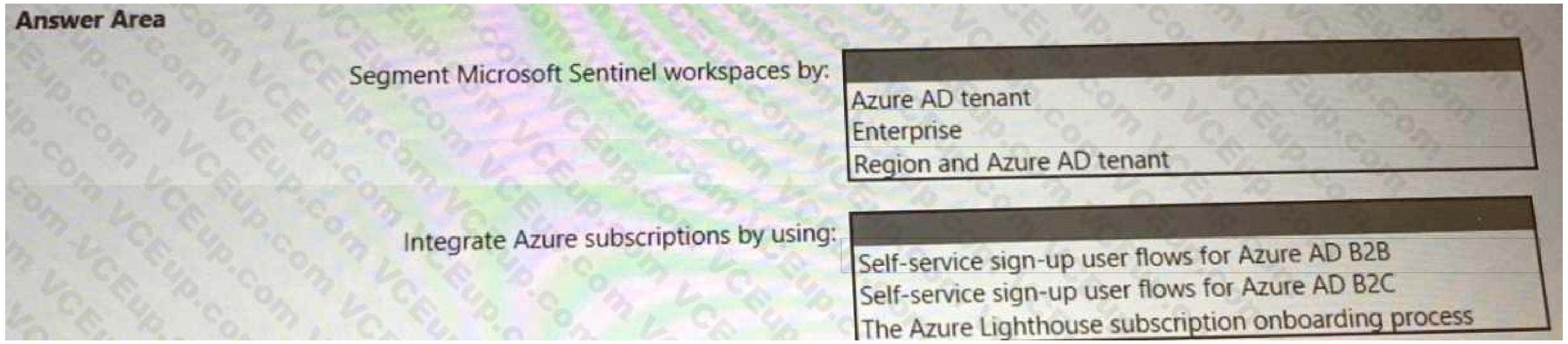
HOTSPOT

You need to recommend a SIEM and SOAR strategy that meets the hybrid requirements, the Microsoft Sentinel requirements, and the regulatory compliance requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:

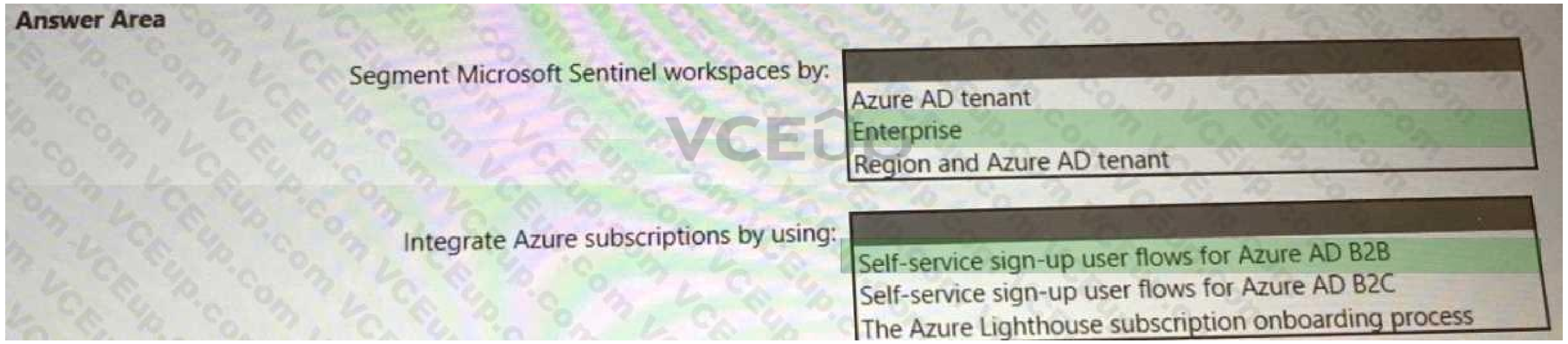


Answer Area

Segment Microsoft Sentinel workspaces by:
- Azure AD tenant
- Enterprise
- Region and Azure AD tenant

Integrate Azure subscriptions by using:
- Self-service sign-up user flows for Azure AD B2B
- Self-service sign-up user flows for Azure AD B2C
- The Azure Lighthouse subscription onboarding process

Correct Answer:



Answer Area

Segment Microsoft Sentinel workspaces by:
- Azure AD tenant
- [✓ Enterprise]
- Region and Azure AD tenant

Integrate Azure subscriptions by using:
- [✓ Self-service sign-up user flows for Azure AD B2B]
- Self-service sign-up user flows for Azure AD B2C
- The Azure Lighthouse subscription onboarding process

Section: (none)
Explanation

Explanation/Reference:

QUESTION 7

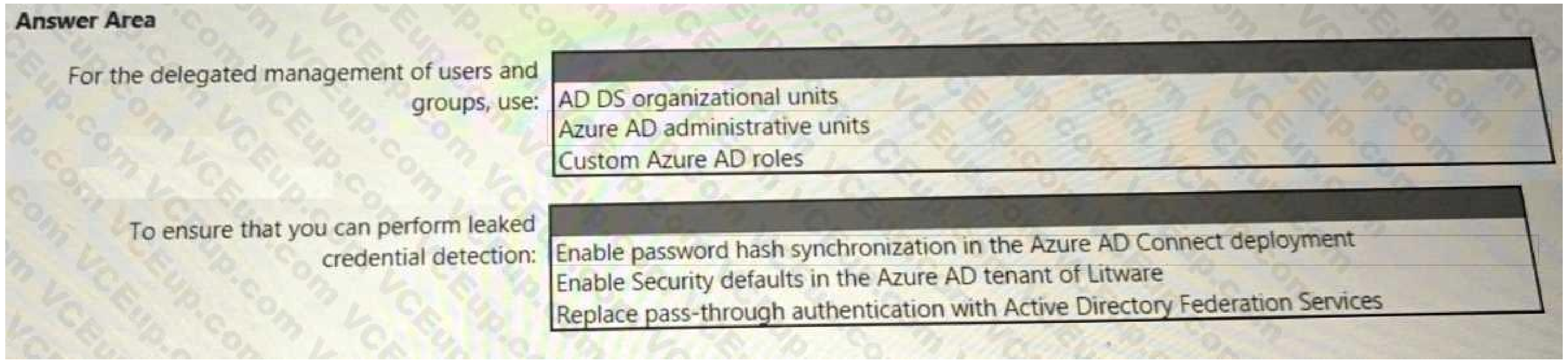
HOTSPOT

You need to recommend an identity security solution for the Azure AD tenant of Litware. The solution must meet the identity requirements and the regulatory compliance requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

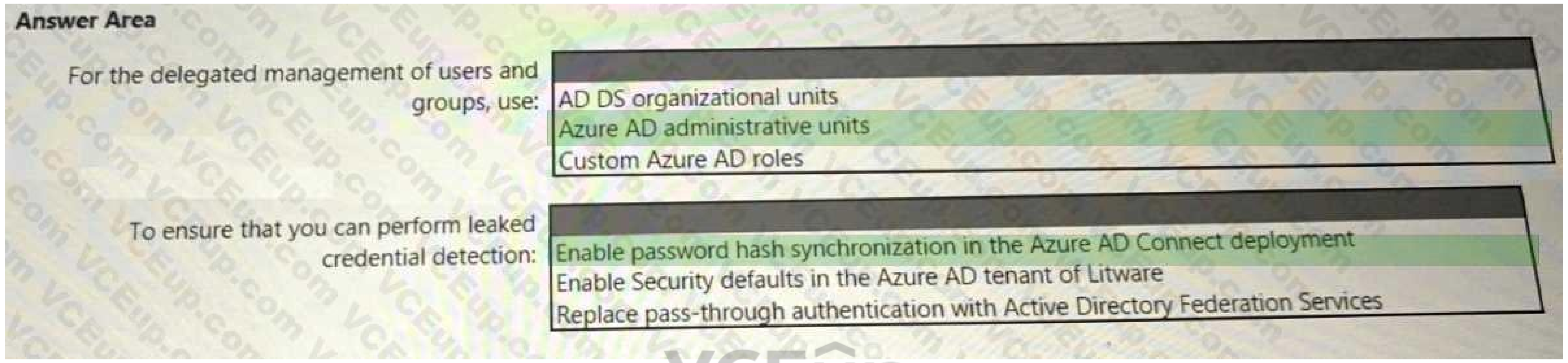
For the delegated management of users and groups, use:

- AD DS organizational units
- Azure AD administrative units
- Custom Azure AD roles

To ensure that you can perform leaked credential detection:

- Enable password hash synchronization in the Azure AD Connect deployment
- Enable Security defaults in the Azure AD tenant of Litware
- Replace pass-through authentication with Active Directory Federation Services

Correct Answer:



Answer Area

For the delegated management of users and groups, use:

- AD DS organizational units
- [✓ Azure AD administrative units]
- Custom Azure AD roles

To ensure that you can perform leaked credential detection:

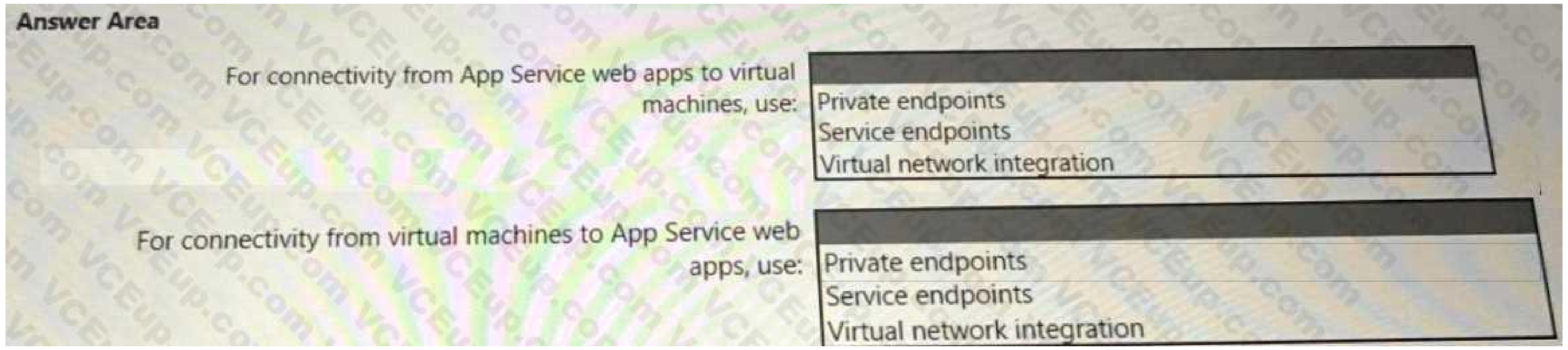
- [✓ Enable password hash synchronization in the Azure AD Connect deployment]
- Enable Security defaults in the Azure AD tenant of Litware
- Replace pass-through authentication with Active Directory Federation Services

Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
HOTSPOT
You need to recommend a strategy for App Service web app connectivity. The solution must meet the landing zone requirements. What should you recommend? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.

Hot Area:



Answer Area

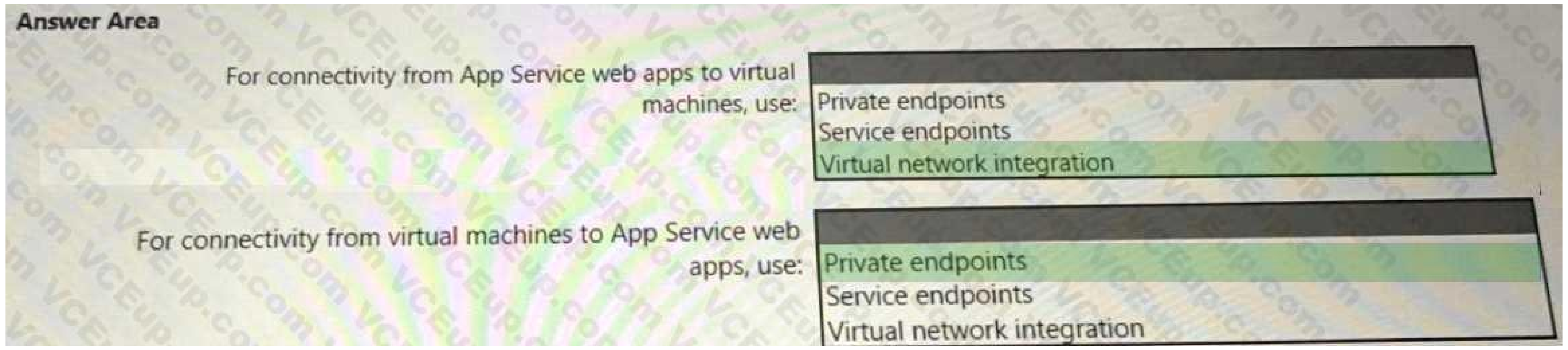
For connectivity from App Service web apps to virtual machines, use:

- Private endpoints
- Service endpoints
- Virtual network integration

For connectivity from virtual machines to App Service web apps, use:

- Private endpoints
- Service endpoints
- Virtual network integration

Correct Answer:



Answer Area

For connectivity from App Service web apps to virtual machines, use:

- Private endpoints
- Service endpoints
- Virtual network integration

For connectivity from virtual machines to App Service web apps, use:

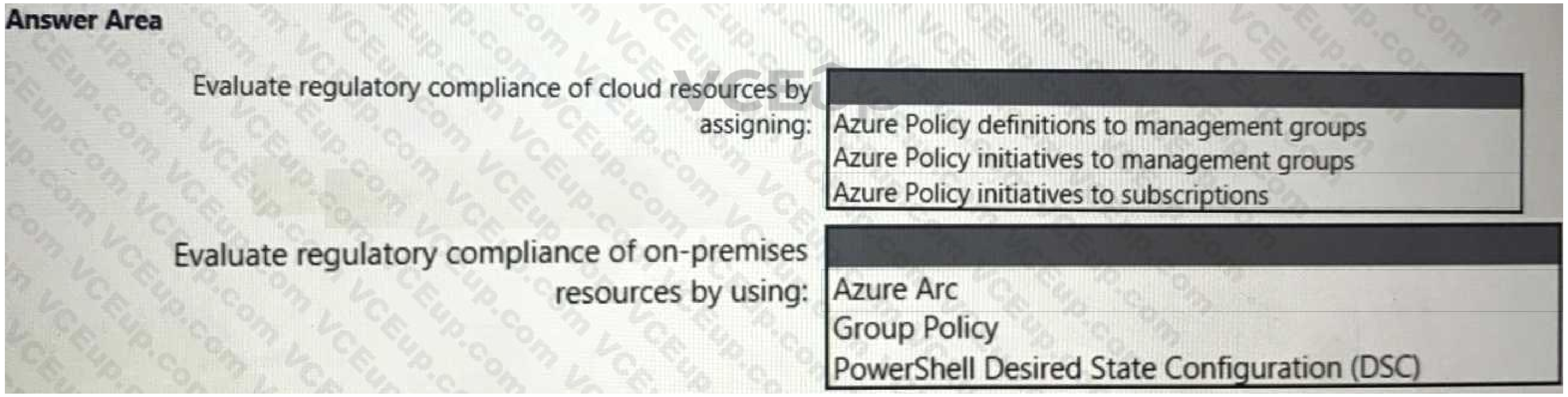
- Private endpoints
- Service endpoints
- Virtual network integration

Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
HOTSPOT
You need to recommend a solution to evaluate regulatory compliance across the entire managed environment. The solution must meet the regulatory compliance requirements and the business requirements.
What should you recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

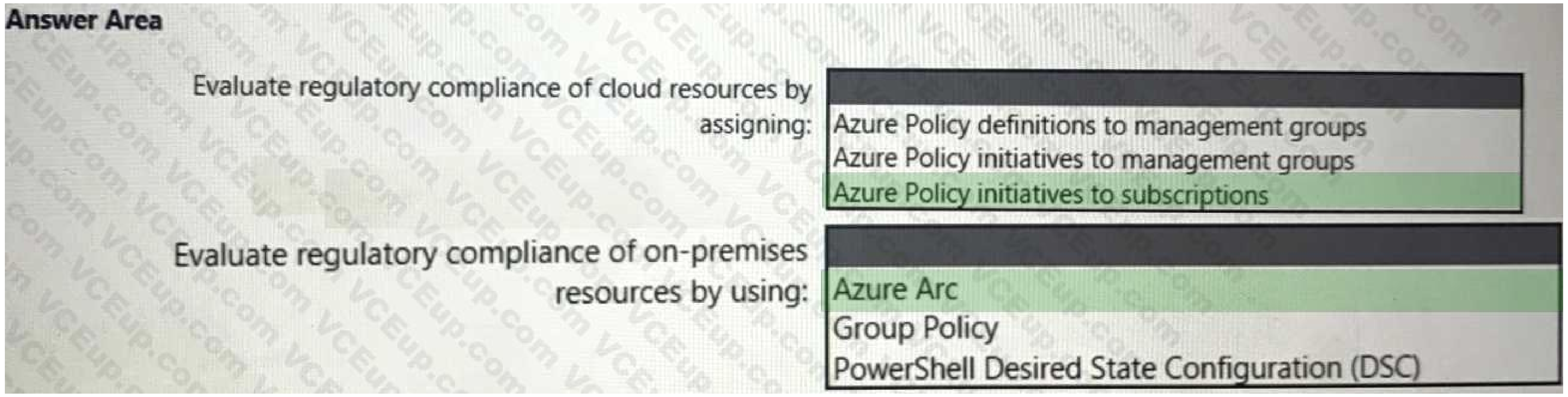
Evaluate regulatory compliance of cloud resources by assigning:

- Azure Policy definitions to management groups
- Azure Policy initiatives to management groups
- Azure Policy initiatives to subscriptions

Evaluate regulatory compliance of on-premises resources by using:

- Azure Arc
- Group Policy
- PowerShell Desired State Configuration (DSC)

Correct Answer:



Answer Area

Evaluate regulatory compliance of cloud resources by assigning:

- Azure Policy definitions to management groups
- Azure Policy initiatives to management groups
- [✓ Azure Policy initiatives to subscriptions]

Evaluate regulatory compliance of on-premises resources by using:

- [✓ Azure Arc]
- Group Policy
- PowerShell Desired State Configuration (DSC)

Section: (none)
Explanation

Explanation/Reference: