Microsoft

Exam Questions SC-100

Microsoft Cybersecurity Architect

NEW QUESTION 1
- (Exam Topic 3)
You are designing a new Azure environment based on the security best practices of the Microsoft Cloud Adoption Framework for Azure. The environment will contain one subscription for shared infrastructure components and three separate subscriptions for applications.
You need to recommend a deployment solution that includes network security groups (NSGs) Azure Key Vault, and Azure Bastion. The solution must minimize deployment effort and follow security best practices of the Microsoft Cloud Adoption Framework for Azure. What should you include in the recommendation?

A. the Azure landing zone accelerator
B. the Azure Will-Architected Framework
C. Azure Security Benchmark v3
D. Azure Advisor

Answer: A

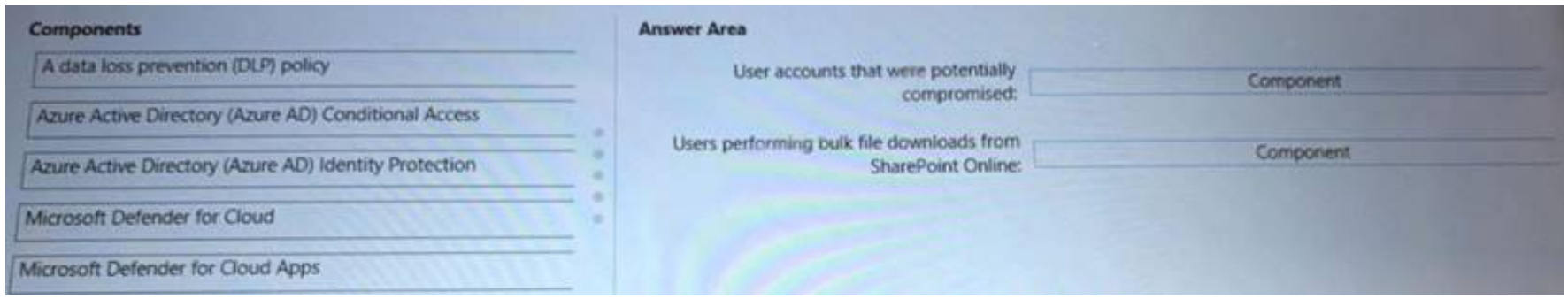
NEW QUESTION 2
- (Exam Topic 3)
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points. You need to recommend configurations to increase the score of the Secure management ports controls. Solution: You recommend enabling adaptive network hardening.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
JIT:
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-s
Adaptive Network Hardening:
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify

NEW QUESTION 3
- (Exam Topic 3)
You have a Microsoft 365 subscription
You need to recommend a security solution to monitor the following activities:
• User accounts that were potentially compromised
• Users performing bulk file downloads from Microsoft SharePoint Online
What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each Correct selection is worth one Point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks https://docs.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exf https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users

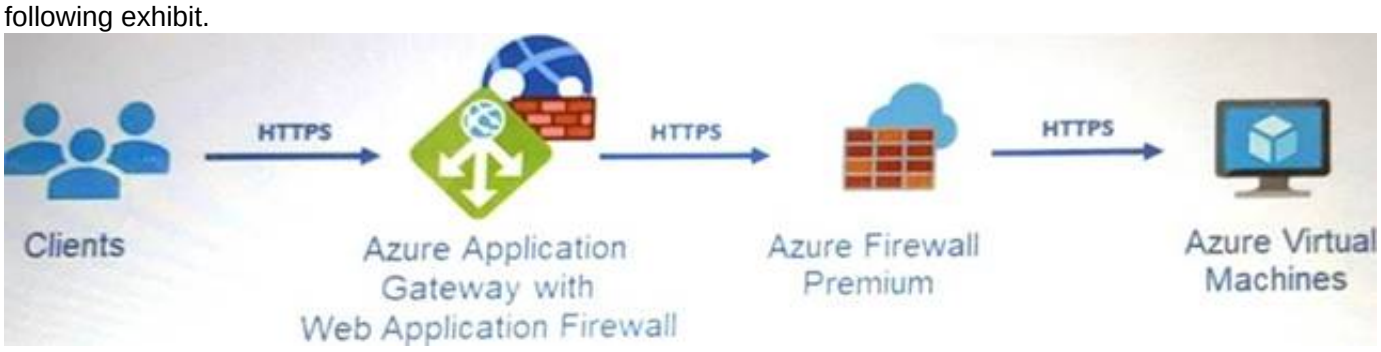
NEW QUESTION 4
- (Exam Topic 3)
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points. You need to recommend configurations to increase the score of the Secure management ports controls.
Solution: You recommend onboarding all virtual machines to Microsoft Defender for Endpoint. Does this meet the goal?

A. Yes
B. No

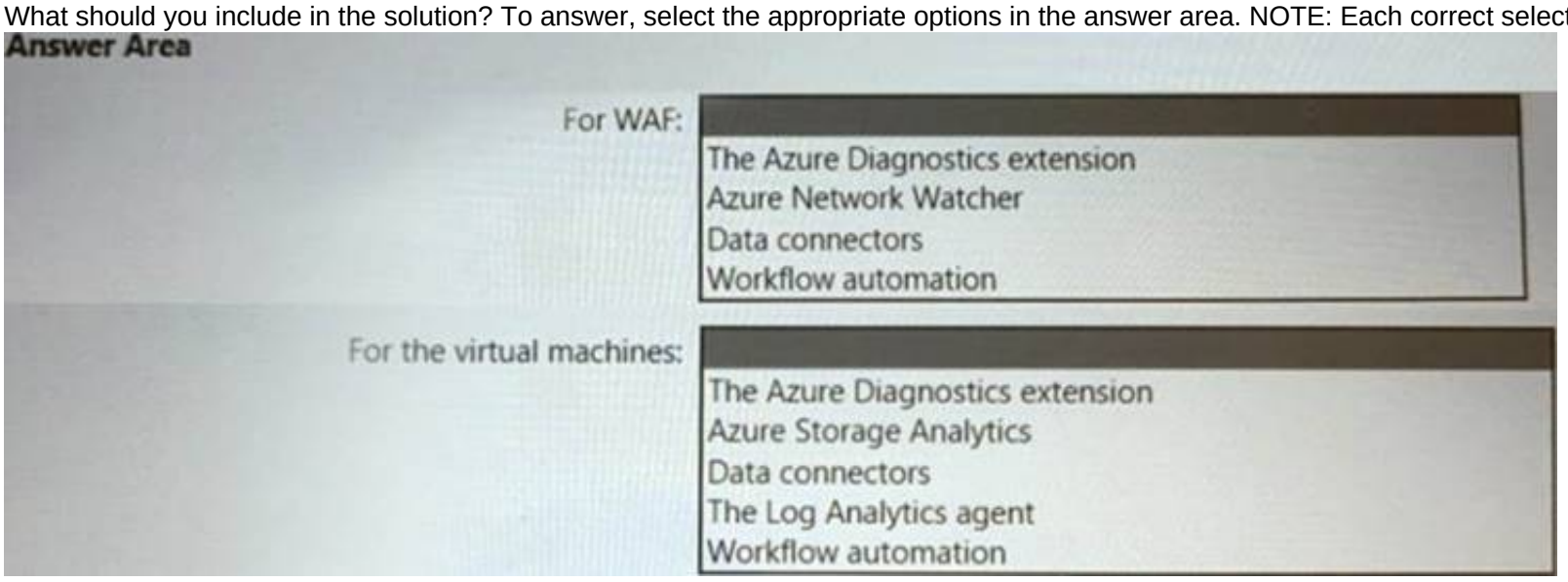
Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

NEW QUESTION 5
- (Exam Topic 3)
Your company uses Microsoft Defender for Cloud and Microsoft Sentinel. The company is designing an application that will have the architecture shown in the following exhibit.



You are designing a logging and auditing solution for the proposed architecture. The solution must meet the following requirements-.
• Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.
• Use Defender for Cloud to review alerts from the virtual machines.
What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

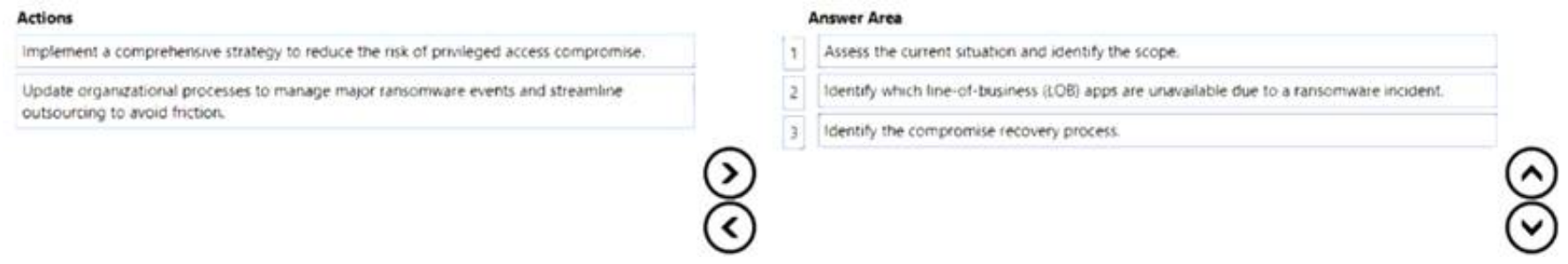
Explanation:
Graphical user interface Description automatically generated

NEW QUESTION 6
- (Exam Topic 3)
Your company wants to optimize ransomware incident investigations.
You need to recommend a plan to investigate ransomware incidents based on the Microsoft Detection and Response Team (DART) approach.
Which three actions should you recommend performing in sequence in the plan? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 7
- (Exam Topic 3)
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You have an Amazon Web Services (AWS) implementation.
You plan to extend the Azure security strategy to the AWS implementation. The solution will NOT use Azure Arc. Which three services can you use to provide security for the AWS resources? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

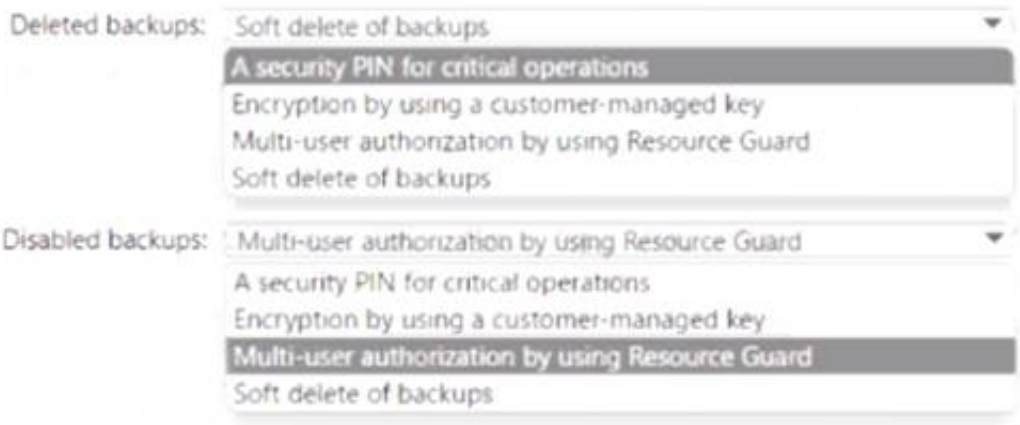
A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
B. Azure Active Directory (Azure AD) Conditional Access
C. Microsoft Defender for servers
D. Azure Policy
E. Microsoft Defender for Containers

Answer: BDE

Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/supported-machines-endpoint-solutions-clouds-conta

NEW QUESTION 8
- (Exam Topic 3)
You have an Azure subscription and an on-premises datacenter. The datacenter contains 100 servers that run Windows Server. AJI the servers are backed up to a Recovery Services vault by using Azure Backup and the Microsoft Azure Recovery Services (MARS) agent.
You need to design a recovery solution for ransomware attacks that encrypt the on-premises servers. The solution must follow Microsoft Security Best Practices and protect against the following risks:
• A compromised administrator account used to delete the backups from Azure Backup before encrypting the servers
• A compromised administrator account used to disable the backups on the MARS agent before encrypting the servers
What should you use for each risk? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

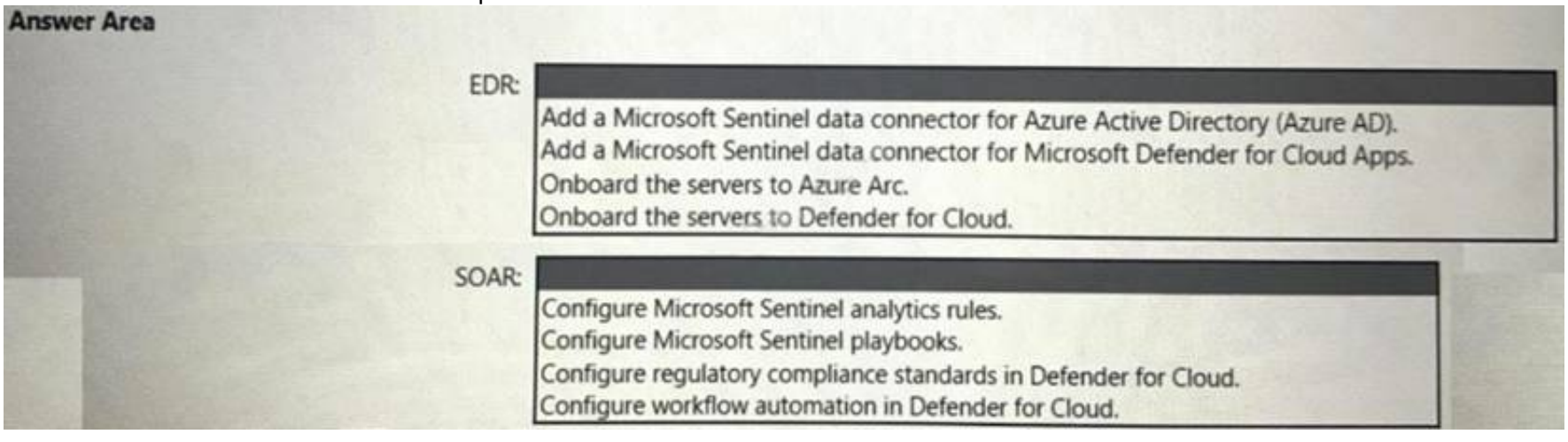
NEW QUESTION 9
- (Exam Topic 3)
A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription.
All the on-premises servers in the perimeter network are prevented from connecting directly to the internet. The customer recently recovered from a ransomware attack.
The customer plans to deploy Microsoft Sentinel.
You need to recommend configurations to meet the following requirements:
• Ensure that the security operations team can access the security logs and the operation logs.
• Ensure that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network.
Which two configurations can you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Azure Active Directory (Azure AD) Conditional Access policies
B. a custom collector that uses the Log Analytics agent
C. resource-based role-based access control (RBAC)
D. the Azure Monitor agent

Answer: CD

Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent

NEW QUESTION 10
- (Exam Topic 3)
You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.
The Azure subscription contains a Microsoft Sentinel workspace. Microsoft Sentinel data connectors are
configured for Microsoft 365, Microsoft 365 Defender, Defender for Cloud, and Azure. You plan to deploy Azure virtual machines that will run Windows Server.
You need to enable extended detection and response (EDR) and security orchestration, automation, and response (SOAR) capabilities for Microsoft Sentinel.
How should you recommend enabling each capability? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
For SOAR read this https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks Endpoint detection and response (EDR) and eXtended detection and response (XDR) are both part of
Microsoft Defender.
https://docs.microsoft.com/en-us/microsoft-365/security/defender/eval-overview?view=o365-worldwide

NEW QUESTION 10
- (Exam Topic 3)
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.

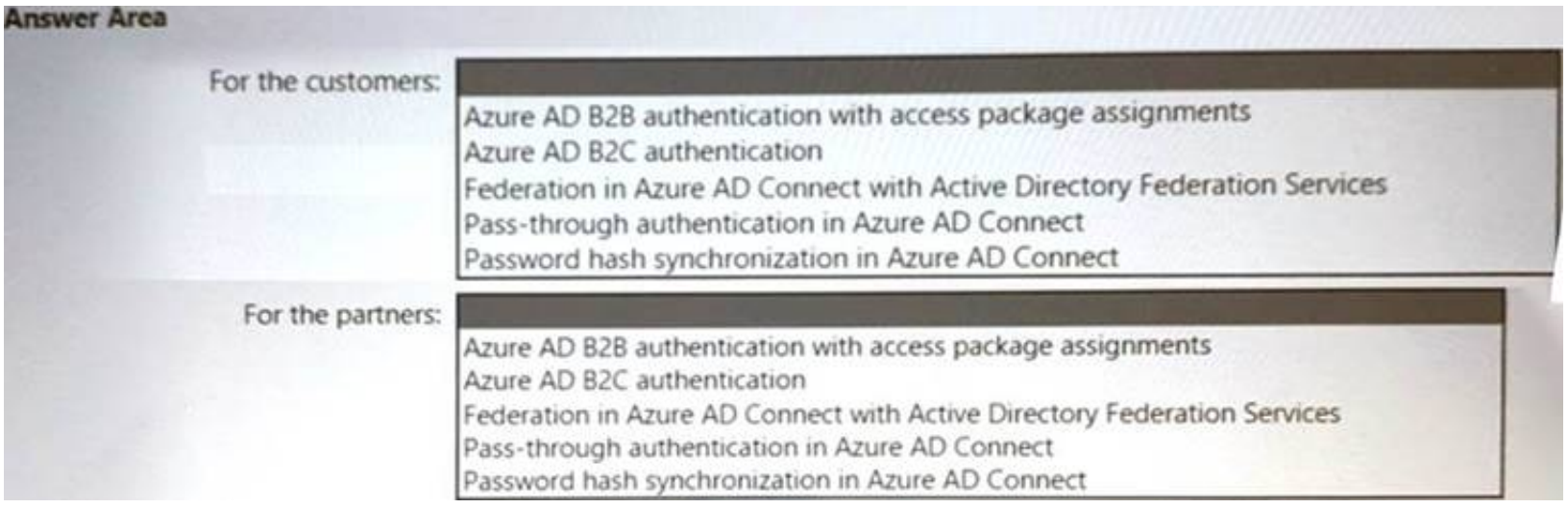
You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.
Solution: You recommend implementing Azure Front Door with Azure Web Application Firewall (WAF). Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 15
- (Exam Topic 3)
Your company has a Microsoft 365 E5 subscription, an Azure subscription, on-premises applications, and Active Directory Domain Services (AD DSV You need to recommend an identity security strategy that meets the following requirements:
• Ensures that customers can use their Facebook credentials to authenticate to an Azure App Service website
• 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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated
Box 1 --> https://docs.microsoft.com/en-us/azure/active-directory-b2c/overview
Box 2 -- > https://docs.microsoft.com/en-us/azure/active-directory/external-identities/identity-providers

NEW QUESTION 17
- (Exam Topic 3)
You have a customer that has a Microsoft 365 subscription and an Azure subscription.
The customer has devices that run either Windows, iOS, Android, or macOS. The Windows devices are deployed on-premises and in Azure.
You need to design a security solution to assess whether all the devices meet the customer's compliance rules. What should you include in the solution?

A. Microsoft Information Protection
B. Microsoft Defender for Endpoint
C. Microsoft Sentinel
D. Microsoft Endpoint Manager

Answer: D

Explanation:
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#open-the-compliance-dashboa

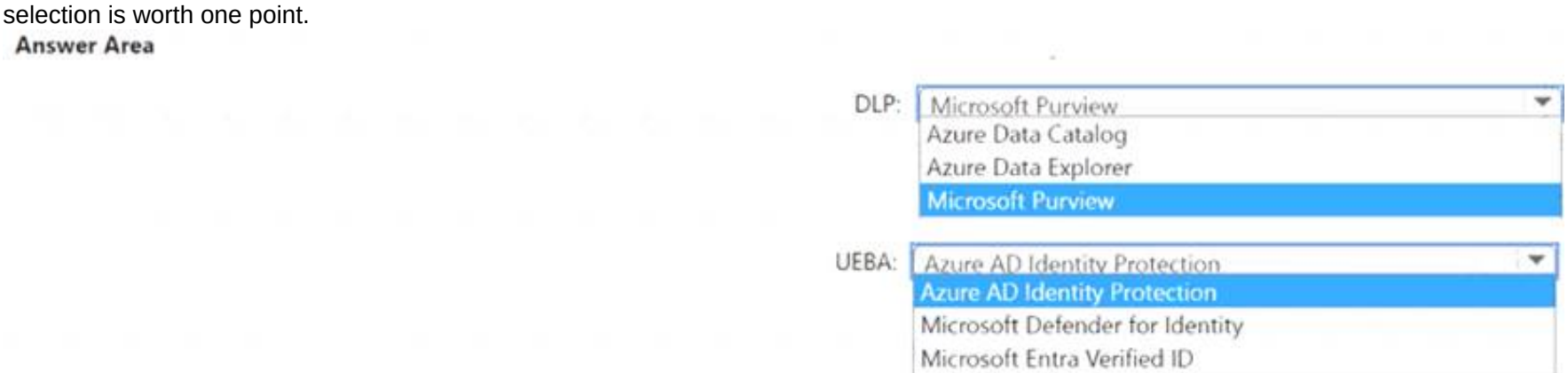
NEW QUESTION 19
- (Exam Topic 3)
Your company has a third-party security information and event management (SIEM) solution that uses Splunk and Microsoft Sentinel. You plan to integrate Microsoft Sentinel with Splunk.
You need to recommend a solution to send security events from Microsoft Sentinel to Splunk. What should you include in the recommendation?

A. Azure Event Hubs
B. Azure Data Factor
C. a Microsoft Sentinel workbook
D. a Microsoft Sentinel data connector

Answer: D

Explanation:
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-side-by-side-with-splunk-via-ev

NEW QUESTION 20
- (Exam Topic 3)
You are designing the security architecture for a cloud-only environment.
You are reviewing the integration point between Microsoft 365 Defender and other Microsoft cloud services based on Microsoft Cybersecurity Reference Architectures (MCRA).
You need to recommend which Microsoft cloud services integrate directly with Microsoft 365 Defender and meet the following requirements:
• Enforce data loss prevention (DLP) policies that can be managed directly from the Microsoft 365 Defender portal.
• Detect and respond to security threats based on User and Entity Behavior Analytics (UEBA) with unified alerting.
What should you include in the recommendation for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

NEW QUESTION 22
- (Exam Topic 3)
Your company has an on-premises network and an Azure subscription.
The company does NOT have a Site-to-Site VPN or an ExpressRoute connection to Azure.
You are designing the security standards for Azure App Service web apps. The web apps will access Microsoft SQL Server databases on the network.
You need to recommend security standards that will allow the web apps to access the databases. The solution must minimize the number of open internet-accessible endpoints to the on-premises network.
What should you include in the recommendation?

A. a private endpoint
B. hybrid connections
C. virtual network NAT gateway integration
D. virtual network integration

Answer: B

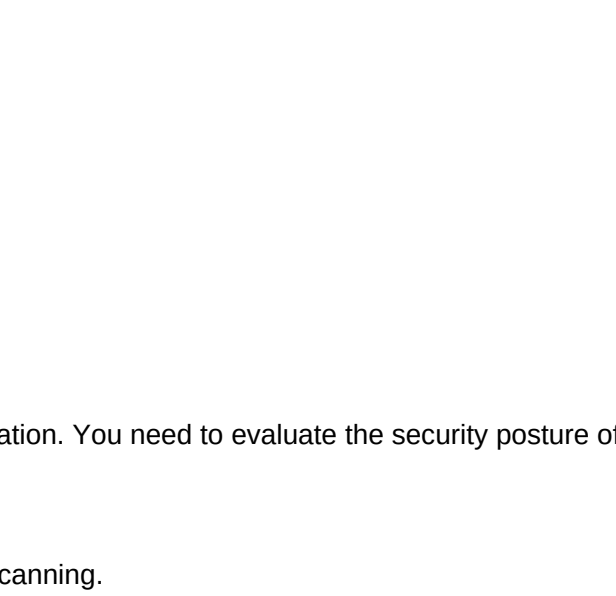
Explanation:
https://docs.microsoft.com/en-us/azure/app-service/app-service-hybrid-connections

NEW QUESTION 23
- (Exam Topic 3)
You have an Azure subscription that is used as an Azure landing zone for an application. You need to evaluate the security posture of all the workloads in the landing zone. What should you do first?

A. Add Microsoft Sentinel data connectors.
B. Configure Continuous Integration/Continuous Deployment (CI/CD) vulnerability scanning.
C. Enable the Defender plan for all resource types in Microsoft Defender for Cloud.
D. Obtain Azure Active Directory Premium Plan 2 licenses.

Answer: A

NEW QUESTION 27
- (Exam Topic 3)
You are planning the security levels for a security access strategy.
You need to identify which job roles to configure at which security levels. The solution must meet security best practices of the Microsoft Cybersecurity Reference Architectures (MCRA).
Which security level should you configure for each job role? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 31
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription and an Azure subscription. You are designing a Microsoft Sentinel deployment.
You need to recommend a solution for the security operations team. The solution must include custom views and a dashboard for analyzing security events. What should you recommend using in Microsoft Sentinel?

A. playbooks
B. workbooks
C. notebooks
D. threat intelligence

Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview

NEW QUESTION 33
- (Exam Topic 3)
A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription.
All the on-premises servers in the perimeter network are prevented from connecting directly to the internet. The customer recently recovered from a ransomware attack.
The customer plans to deploy Microsoft Sentinel.
You need to recommend configurations to meet the following requirements:
• Ensure that the security operations team can access the security logs and the operation logs.
• Ensure that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network.
Which two configurations can you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Configure Azure Active Directory (Azure AD) Conditional Access policies.
B. Use the Azure Monitor agent with the multi-homing configuration.
C. Implement resource-based role-based access control (RBAC) in Microsoft Sentinel.
D. Create a custom collector that uses the Log Analytics agent.

Answer: BC

NEW QUESTION 38
- (Exam Topic 3)
You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.
The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.
You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.
Which security control should you recommend?

A. Azure Active Directory (Azure AD) Conditional Access App Control policies
B. OAuth app policies in Microsoft Defender for Cloud Apps
C. app protection policies in Microsoft Endpoint Manager
D. application control policies in Microsoft Defender for Endpoint

Answer: D

Explanation:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/sele

NEW QUESTION 40
- (Exam Topic 3)
Your company plans to evaluate the security of its Azure environment based on the principles of the Microsoft Cloud Adoption Framework for Azure.

You need to recommend a cloud-based service to evaluate whether the Azure resources comply with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).
What should you recommend?

A. Compliance Manager in Microsoft Purview
B. Microsoft Defender for Cloud
C. Microsoft Sentinel
D. Microsoft Defender for Cloud Apps

Answer: D

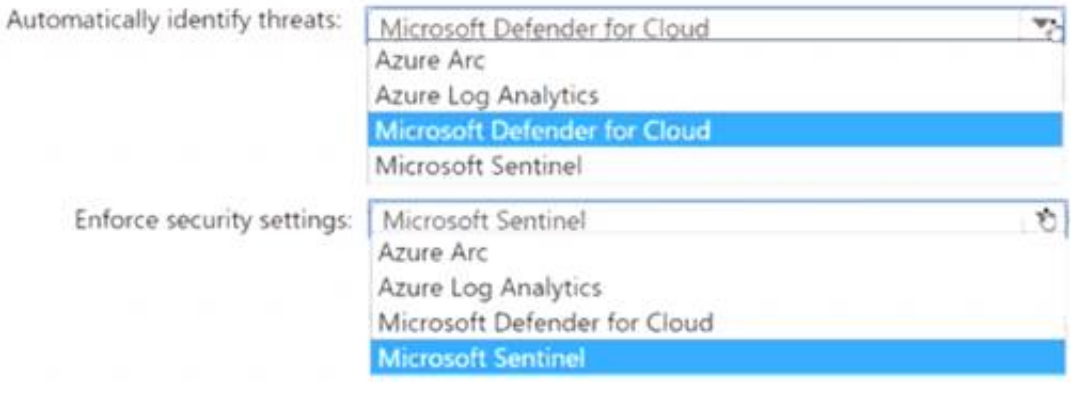
NEW QUESTION 45
- (Exam Topic 3)
You have an on-premises network that has several legacy applications. The applications perform LDAP queries against an existing directory service. You are migrating the on-premises infrastructure to a cloud-only infrastructure.
You need to recommend an identity solution for the infrastructure that supports the legacy applications. The solution must minimize the administrative effort to maintain the infrastructure.
Which identity service should you include in the recommendation?

A. Azure Active Directory Domain Services (Azure AD DS)
B. Azure Active Directory (Azure AD) B2C
C. Azure Active Directory (Azure AD)
D. Active Directory Domain Services (AD DS)

Answer: A

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory-domain-services/overview

NEW QUESTION 46
- (Exam Topic 3)
You have a multi-cloud environment that contains an Azure subscription and an Amazon Web Services (AWS) account.
You need to implement security services in Azure to manage the resources in both subscriptions. The solution must meet the following requirements:
• Automatically identify threats found in AWS CloudTrail events.
• Enforce security settings on AWS virtual machines by using Azure policies.
What should you include in the solution for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

NEW QUESTION 47
- (Exam Topic 3)
You have Windows 11 devices and Microsoft 365 E5 licenses.
You need to recommend a solution to prevent users from accessing websites that contain adult content such as gambling sites. What should you include in the recommendation?

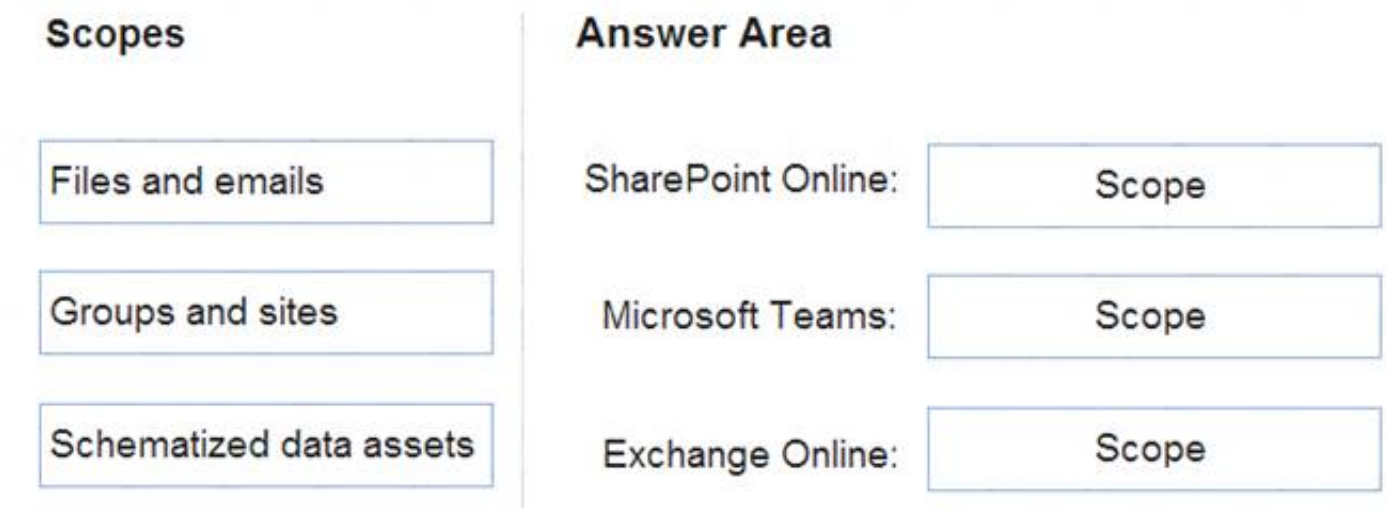
A. Microsoft Endpoint Manager

B. Compliance Manager
C. Microsoft Defender for Cloud Apps
D. Microsoft Defender for Endpoint

Answer: D

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-w

NEW QUESTION 48
- (Exam Topic 3)
Your company has Microsoft 365 E5 licenses and Azure subscriptions.
The company plans to automatically label sensitive data stored in the following locations:
• Microsoft SharePoint Online
• Microsoft Exchange Online
• Microsoft Teams
You need to recommend a strategy to identify and protect sensitive data.
Which scope should you recommend for the sensitivity label policies? To answer, drag the appropriate scopes to the correct locations. Each scope may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Groups and sites Box 2: Groups and sites Box 3: Files and emails –
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide Go to label scopes

NEW QUESTION 53
- (Exam Topic 3)
Your company has a Microsoft 365 E5 subscription.
Users use Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive for sharing and collaborating. The company identifies protected health information (PHI) within stored documents and communications. What should you recommend using to prevent the PHI from being shared outside the company?

A. insider risk management policies
B. data loss prevention (DLP) policies
C. sensitivity label policies
D. retention policies

Answer: C

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide

NEW QUESTION 54
- (Exam Topic 3)
Your company has a Microsoft 365 E5 subscription.
The company plans to deploy 45 mobile self-service kiosks that will run Windows 10. You need to provide recommendations to secure the kiosks. The solution must meet the following requirements:
• Ensure that only authorized applications can run on the kiosks.
• Regularly harden the kiosks against new threats.
Which two actions should you include in the recommendations? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Onboard the kiosks to Azure Monitor.
B. Implement Privileged Access Workstation (PAW) for the kiosks.
C. Implement Automated Investigation and Remediation (AIR) in Microsoft Defender for Endpoint.
D. Implement threat and vulnerability management in Microsoft Defender for Endpoint.
E. Onboard the kiosks to Microsoft Intune and Microsoft Defender for Endpoint.

Answer: DE

Explanation:
(https://docs.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerab

NEW QUESTION 57
- (Exam Topic 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

Answer: AD

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-o https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-w https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-custom-domain

NEW QUESTION 58
- (Exam Topic 2)
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

Answer: D

Explanation:
One of the stipulations is to meet the business requirements of minimizing costs. ExpressRoute is expensive. Given the landing zone requirements of
1) "Use a DNS namespace of litware.com"
2) "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"

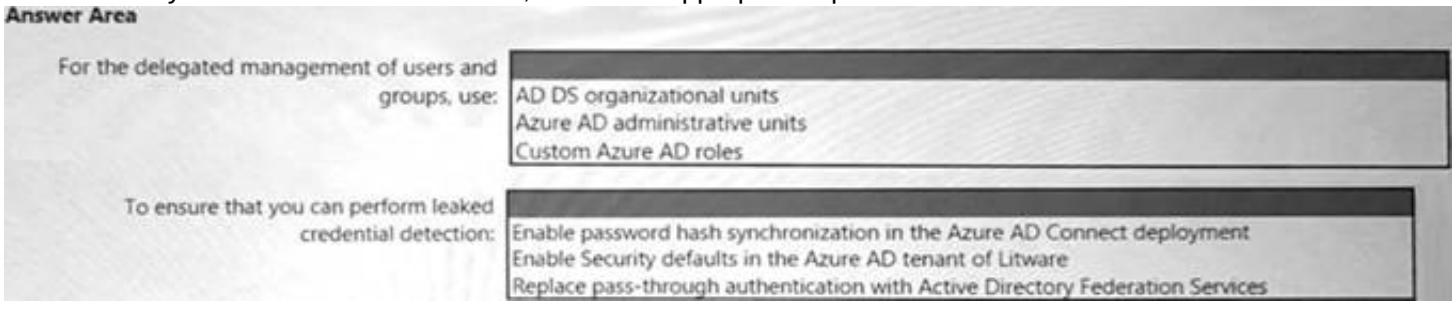
NEW QUESTION 62
- (Exam Topic 2)
You need to design a strategy for securing the SharePoint Online and Exchange Online data. The solution must meet the application security requirements.
Which two services should you leverage in the strategy? Each correct answer presents part of the solution. NOTE; Each correct selection is worth one point.

A. Azure AD Conditional Access
B. Microsoft Defender for Cloud Apps
C. Microsoft Defender for Cloud
D. Microsoft Defender for Endpoint
E. access reviews in Azure AD

Answer: AB

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session#c https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-integrate-with-microsoft-cl

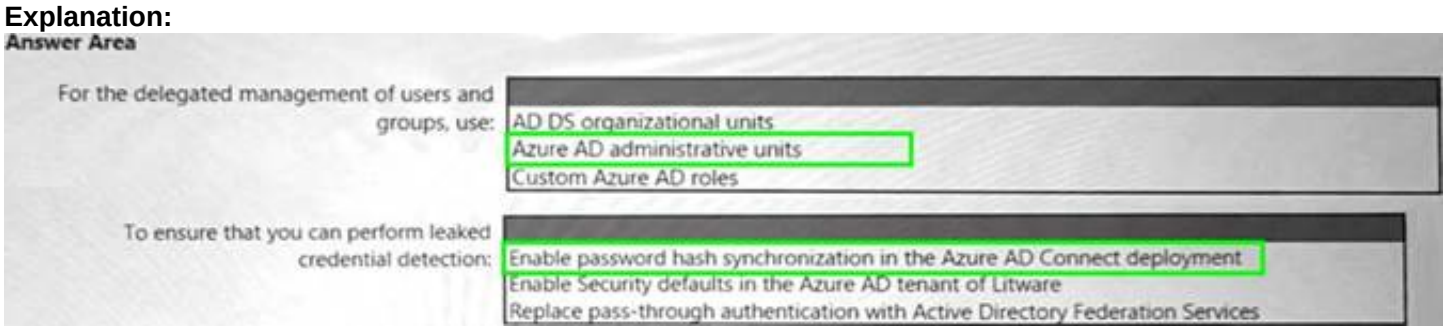
NEW QUESTION 66
- (Exam Topic 2)
You need to recommend an identity security solution for the Azure AD tenant of Litware. The solution must meet the identity requirements and the regulatory compliance requirements.
What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



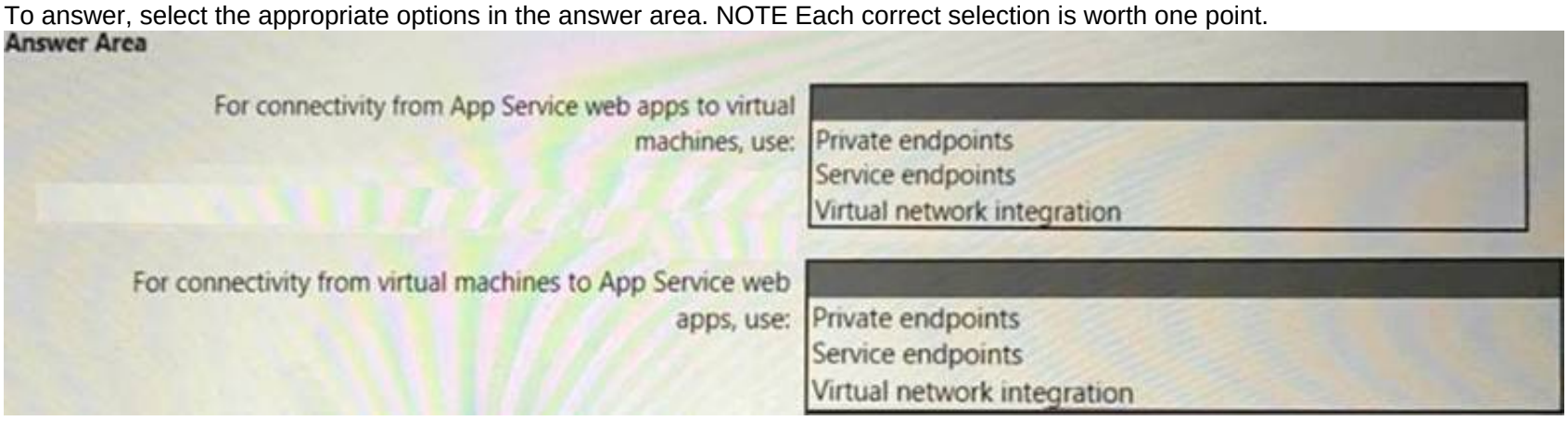
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 69
- (Exam Topic 2)
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Virtual Network Integration - correct
Virtual network integration gives your app access to resources in your virtual network, but it doesn't grant inbound private access to your app from the virtual network.
Box 2: Private Endpoints. - correct
You can use Private Endpoint for your Azure Web App to allow clients located in your private network to securely access the app over Private Link.

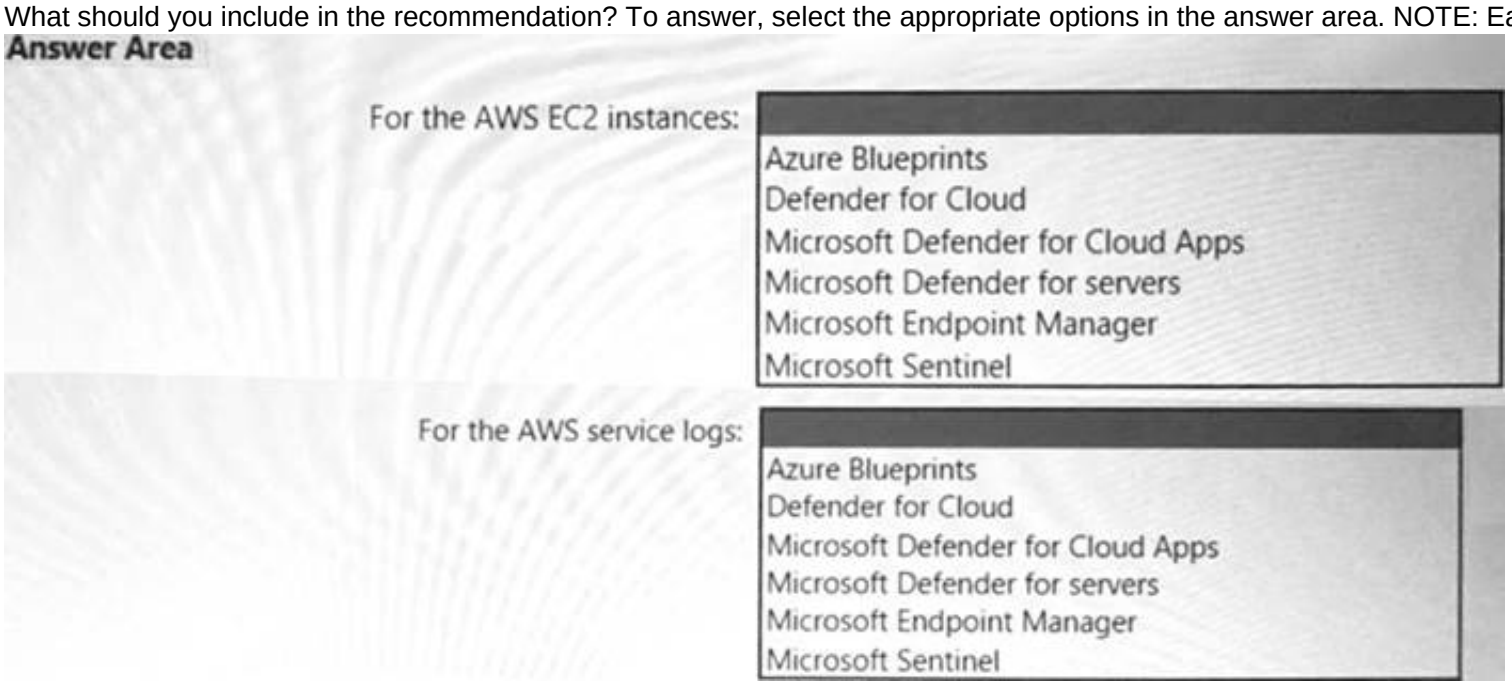
NEW QUESTION 74
- (Exam Topic 1)
You need to recommend a solution to scan the application code. The solution must meet the application development requirements. What should you include in the recommendation?

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-advanc

NEW QUESTION 79
- (Exam Topic 1)
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.

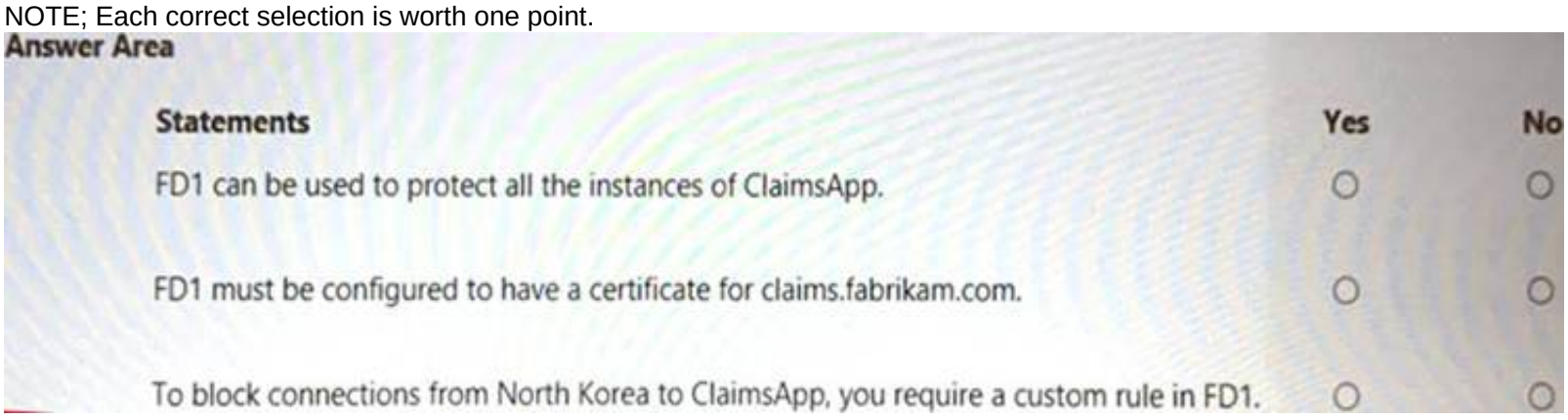


A. Mastered
B. Not Mastered

Answer: A

Explanation:

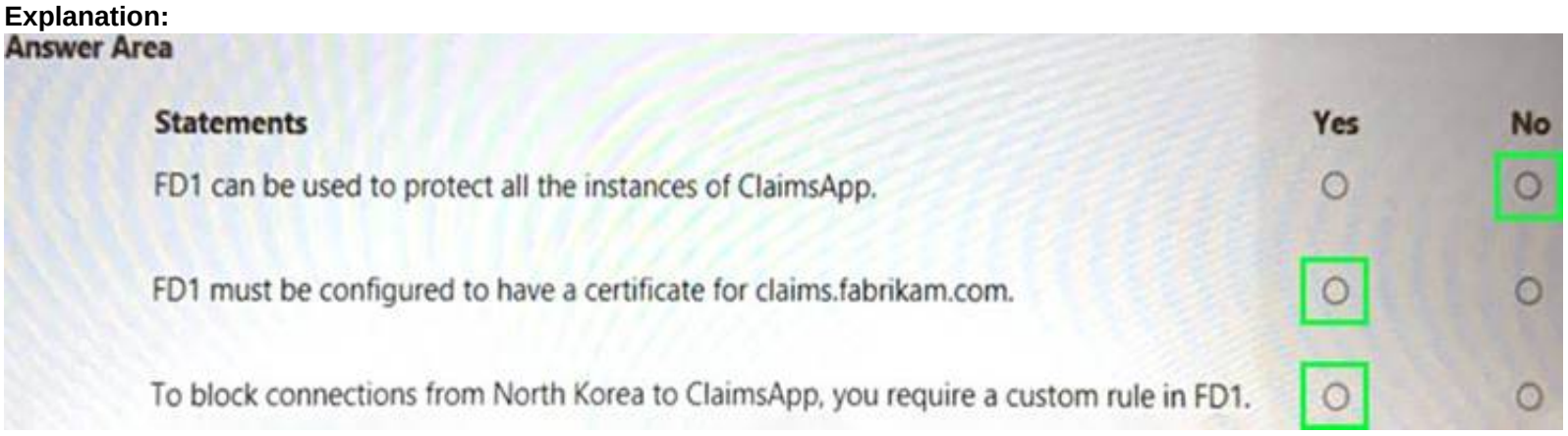
NEW QUESTION 84
- (Exam Topic 1)
You are evaluating the security of ClaimsApp.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE; Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 87
- (Exam Topic 1)
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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 88
- (Exam Topic 1)
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

Answer: A

Explanation:
The security requirement this question wants us to meet is "The secure host must be provisioned from a custom operating system image."
https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-golden-image

NEW QUESTION 90
- (Exam Topic 1)
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.

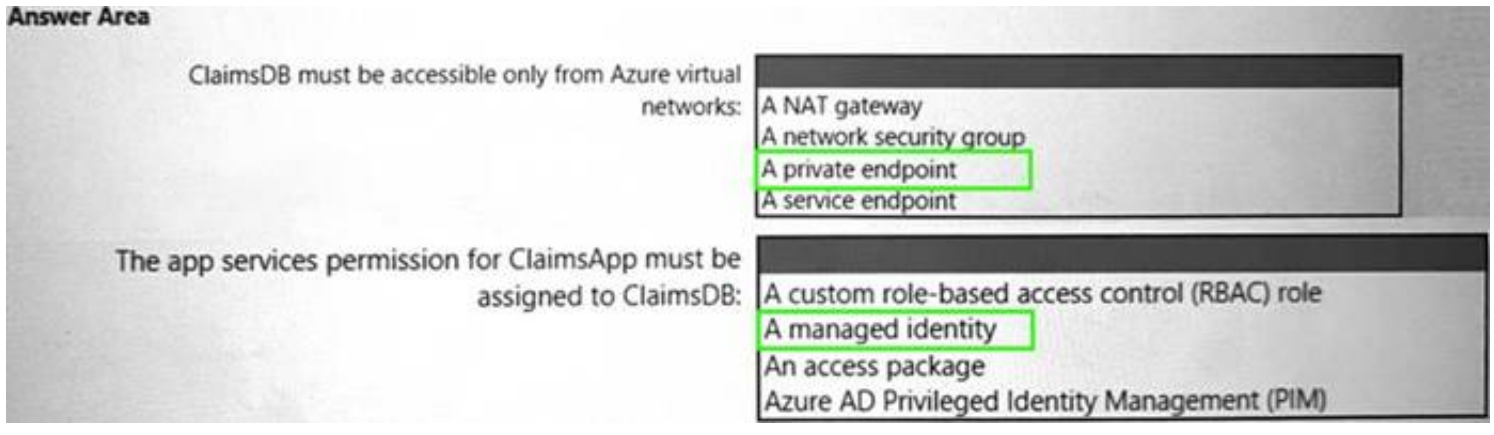
Answer Area

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)

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 95
- (Exam Topic 1)
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

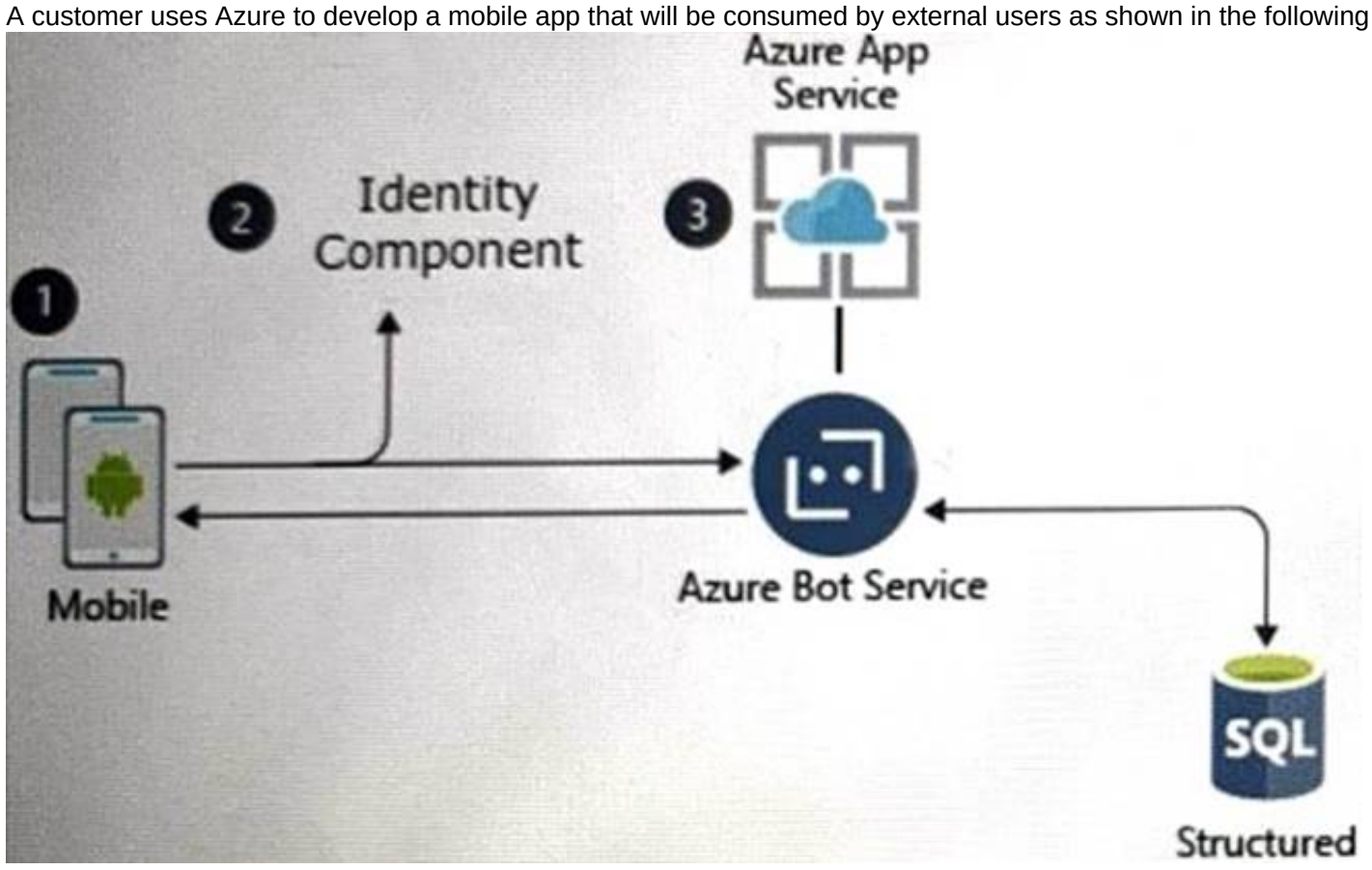
NEW QUESTION 96
- (Exam Topic 3)
Your company has an on-premises network, an Azure subscription, and a Microsoft 365 E5 subscription. The company uses the following devices:
• Computers that run either Windows 10 or Windows 11
• Tablets and phones that run either Android or iOS
You need to recommend a solution to classify and encrypt sensitive Microsoft Office 365 data regardless of where the data is stored. What should you include in the recommendation?

A. eDiscovery
B. retention policies
C. Compliance Manager
D. Microsoft Information Protection

Answer: D

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide

NEW QUESTION 97
- (Exam Topic 3)
A customer uses Azure to develop a mobile app that will be consumed by external users as shown in the following exhibit.



You need to design an identity strategy for the app. The solution must meet the following requirements:
• Enable the usage of external IDs such as Google, Facebook, and Microsoft accounts.
• Be managed separately from the identity store of the customer.
• Support fully customizable branding for each app.
Which service should you recommend to complete the design?

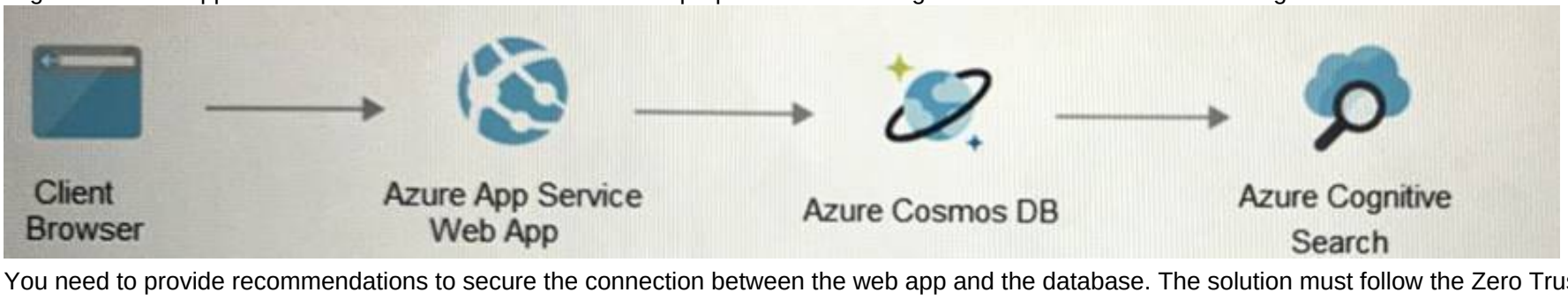
A. Azure Active Directory (Azure AD) B2C
B. Azure Active Directory (Azure AD) B2B

C. Azure AD Connect
D. Azure Active Directory Domain Services (Azure AD DS)

Answer: A

Explanation:
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-b2c/customize-ui-with-html?pivots=b2c-user-flow

NEW QUESTION 99
- (Exam Topic 3)
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 Application Gateway with Azure Web Application Firewall (WAF).
Does this meet the goal?

A. Yes
B. No

Answer: B

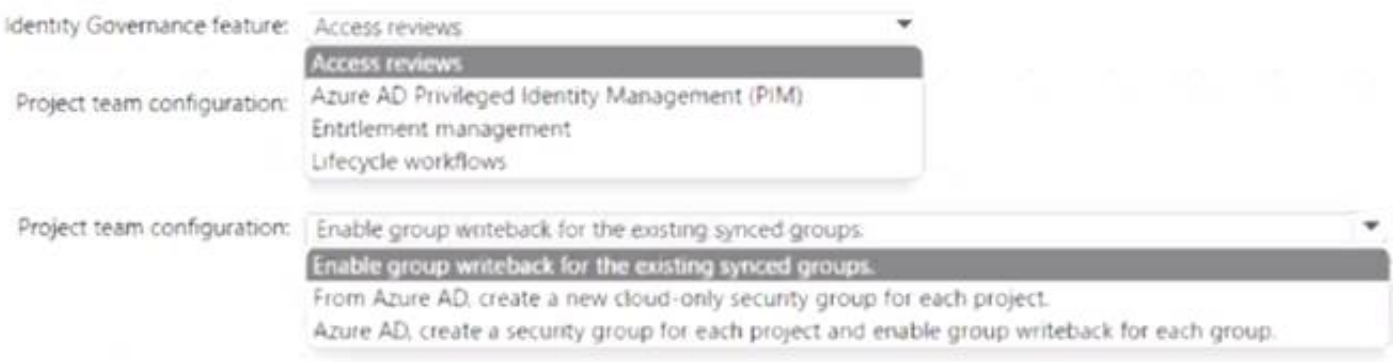
Explanation:
When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.

NEW QUESTION 102
- (Exam Topic 3)
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 Appl. What should you include in the design?

A. Azure AD Application Proxy
B. connected apps in Microsoft Defender for Cloud Apps
C. Microsoft Entra Identity Governance
D. access policies in Microsoft Defender for Cloud Apps

Answer: C

NEW QUESTION 105
- (Exam Topic 3)
Your network contains an on-premises Active Directory Domain Services (AO DS) domain. The domain contains a server that runs Windows Server and hosts shared folders The domain syncs with Azure AD by using Azure AD Connect Azure AD Connect has group writeback enabled.
You have a Microsoft 365 subscription that uses Microsoft SharePoint Online.
You have multiple project teams. Each team has an AD DS group that syncs with Azure AD Each group has permissions to a unique SharePoint Online site and a Windows Server shared folder for its project. Users routinely move between project teams.
You need to recommend an Azure AD identity Governance solution that meets the following requirements:
• Project managers must verify that their project group contains only the current members of their project team
• The members of each project team must only have access to the resources of the project to which they are assigned
• Users must be removed from a project group automatically if the project manager has MOT verified the group s membership for 30 days.
• Administrative effort must be minimized.
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.
Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 108
- (Exam Topic 3)
A customer follows the Zero Trust model and explicitly verifies each attempt to access its corporate applications.
The customer discovers that several endpoints are infected with malware. The customer suspends access attempts from the infected endpoints.
The malware is removed from the end point.
Which two conditions must be met before endpoint users can access the corporate applications again? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Microsoft Defender for Endpoint reports the endpoints as compliant.
B. Microsoft Intune reports the endpoints as compliant.
C. A new Azure Active Directory (Azure AD) Conditional Access policy is enforced.
D. The client access tokens are refreshed.

Answer: CD

Explanation:
https://www.microsoft.com/security/blog/2022/02/17/4-best-practices-to-implement-a-comprehensive-zero-trust https://docs.microsoft.com/en-us/azure/active-directory/develop/refresh-tokens

NEW QUESTION 109
- (Exam Topic 3)
You are designing the encryption standards for data at rest for an Azure resource
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For blob containers in Azure Storage, you recommend encryption that uses Microsoft-managed keys within an encryption scope.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

NEW QUESTION 113
- (Exam Topic 3)
Your company wants to optimize using Microsoft Defender for Endpoint to protect its resources against ransomware based on Microsoft Security Best Practices.
You need to prepare a post-breach response plan for compromised computers based on the Microsoft Detection and Response Team (DART) approach in Microsoft Security Best Practices.
What should you include in the response plan?

A. controlled folder access
B. application isolation
C. memory scanning
D. machine isolation
E. user isolation

Answer: D

NEW QUESTION 117
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online.
You need to recommend a solution to prevent malicious actors from impersonating the email addresses of internal senders.
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.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 118
- (Exam Topic 3)
You need to design a solution to provide administrators with secure remote access to the virtual machines. The solution must meet the following requirements:
• Prevent the need to enable ports 3389 and 22 from the internet.
• Only provide permission to connect the virtual machines when required.
• 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. Enable Azure Active Directory (Azure AD) Privileged Identity Management (PIM) roles as virtual machine contributors.
B. Configure Azure VPN Gateway.
C. Enable Just Enough Administration (JEA).
D. Enable just-in-time (JIT) VM access.
E. Configure Azure Bastion.

Answer: DE

Explanation:
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

NEW QUESTION 123
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription.
You need to recommend a solution to add a watermark to email attachments that contain sensitive data. What should you include in the recommendation?

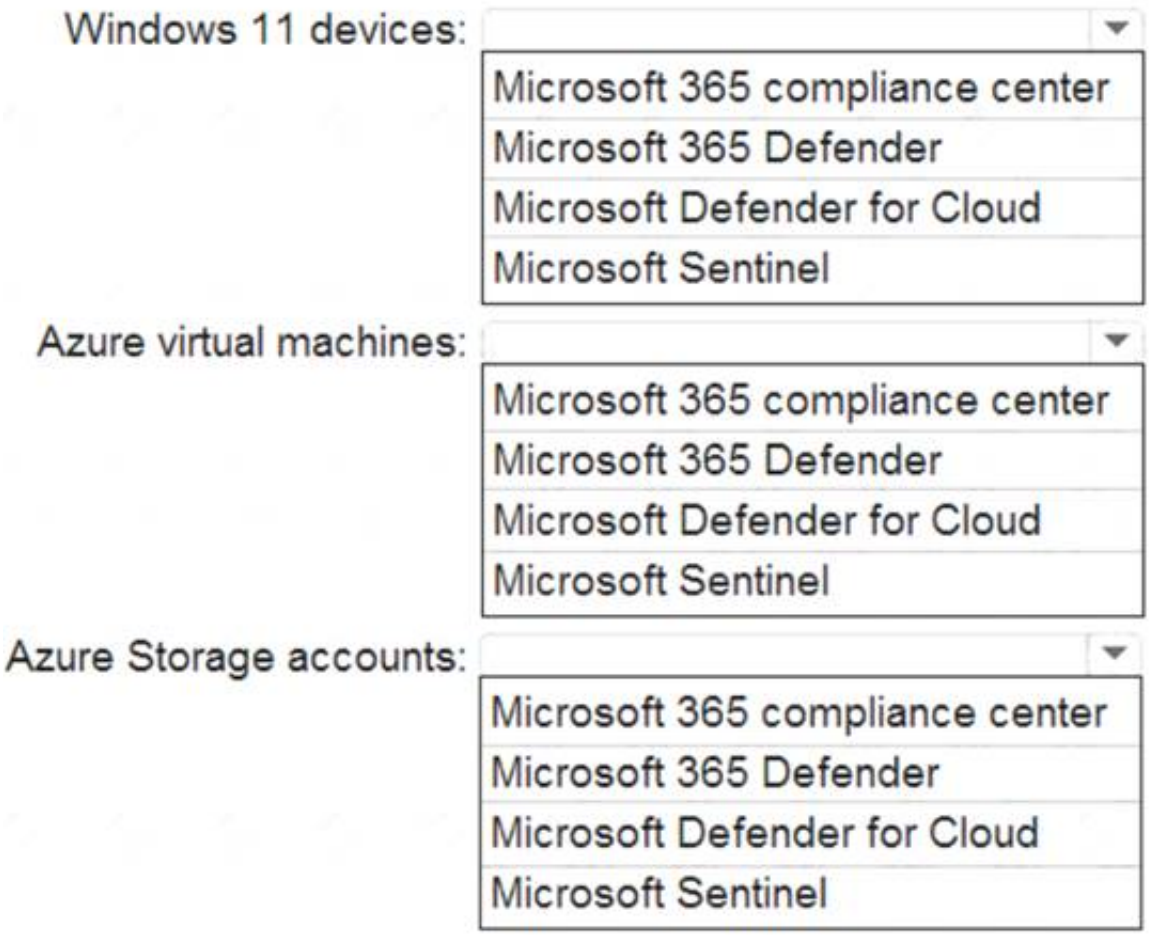
A. Microsoft Defender for Cloud Apps
B. insider risk management
C. Microsoft Information Protection
D. Azure Purview

Answer: C

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide
You can use sensitivity labels to: Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, and encryption can also restrict what actions authorized people can take on the content. Protect content in Office apps across different platforms and devices. Supported by Word, Excel, PowerPoint, and Outlook on the Office desktop apps and Office on the web. Supported on Windows, macOS, iOS, and Android.

Protect content in third-party apps and services by using Microsoft Defender for Cloud Apps. With Defender for Cloud Apps, you can detect, classify, label, and protect content in third-party apps and services, such as SalesForce, Box, or DropBox, even if the third-party app or service does not read or support sensitivity labels.

NEW QUESTION 126
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription and an Azure subscripts You need to evaluate the existing environment to increase the overall security posture for the following components:
• Windows 11 devices managed by Microsoft Intune
• Azure Storage accounts
• Azure virtual machines
What should you use to evaluate the components? To answer, select the appropriate options in the answer area.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Selection 1: Microsoft 365 Defender (Microsoft Defender for Endpoint is part of it). Selection 2: Microsoft Defender for Cloud.
Selection 3: Microsoft Defender for Cloud.
https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/8-specify-sec

NEW QUESTION 131
- (Exam Topic 3)
Your company uses Azure Pipelines and Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows for the deployment of applications to Azure.
You are updating the deployment process to align with DevSecOps controls guidance in the Microsoft Cloud Adoption Framework for Azure.
You need to recommend a solution to ensure that all code changes are submitted by using pull requests before being deployed by the CI/CD workflow.
What should you include in the recommendation?

A. custom roles in Azure Pipelines
B. branch policies in Azure Repos
C. Azure policies
D. custom Azure roles

Answer: B

NEW QUESTION 133
- (Exam Topic 3)
Your company has a hybrid cloud infrastructure that contains an on-premises Active Directory Domain Services (AD DS) forest, a Microsoft B65 subscription, and an Azure subscription.
The company's on-premises network contains internal web apps that use Kerberos authentication. Currently, the web apps are accessible only from the network.
You have remote users who have personal devices that run Windows 11.
You need to recommend a solution to provide the remote users with the ability to access the web apps. The solution must meet the following requirements:
• Prevent the remote users from accessing any other resources on the network.
• Support Azure Active Directory (Azure AD) Conditional Access.
• Simplify the end-user experience.
What should you include in the recommendation?

A. Azure AD Application Proxy

B. Azure Virtual WAN
C. Microsoft Tunnel
D. web content filtering in Microsoft Defender for Endpoint

Answer: A

Explanation:
https://docs.microsoft.com/en-us/learn/modules/configure-azure-ad-application-proxy/2-explore

NEW QUESTION 138
- (Exam Topic 3)
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend access restrictions to allow traffic from the backend IP address of the Front Door instance.
Does this meet the goal?

A. Yes
B. No

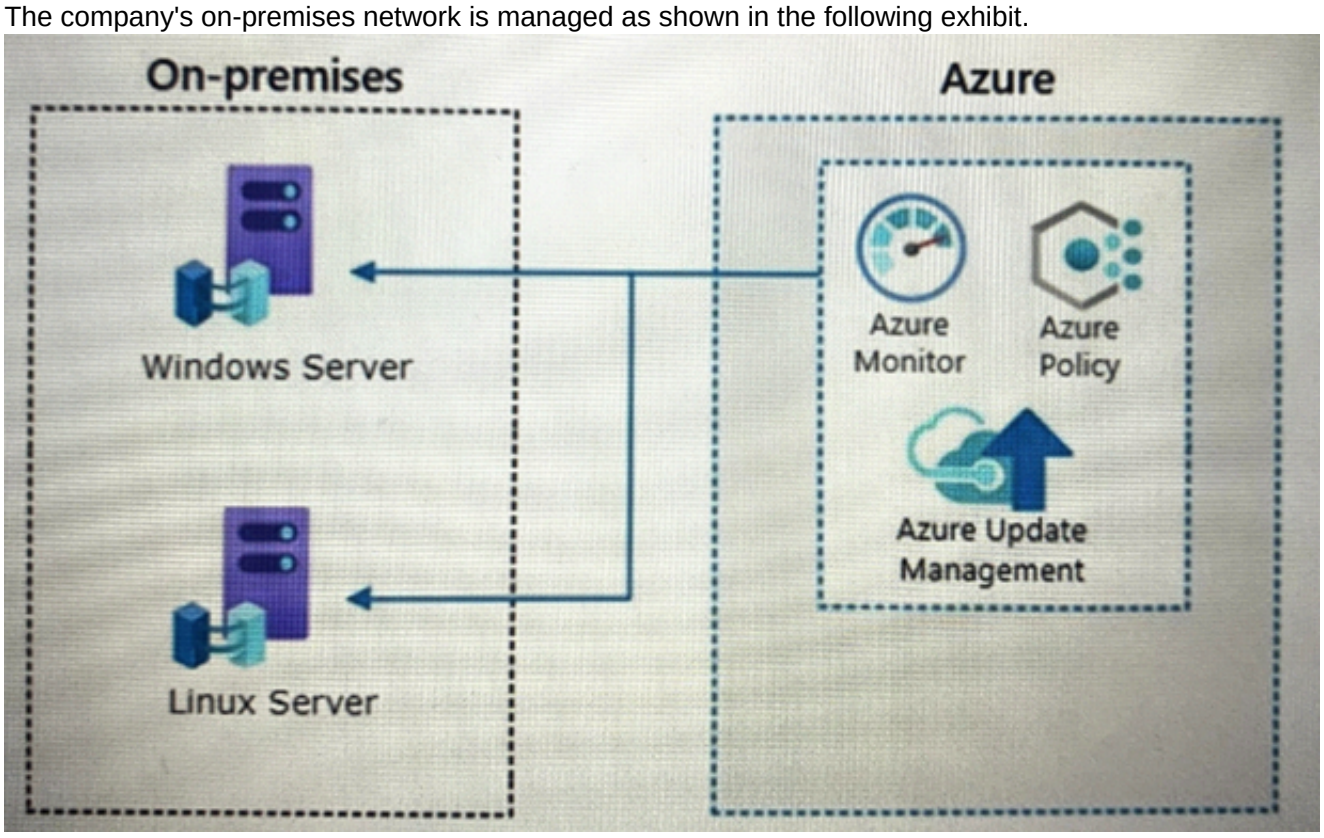
Answer: B

NEW QUESTION 139
- (Exam Topic 3)
You have an Azure subscription.
Your company has a governance requirement that resources must be created in the West Europe or North Europe Azure regions.
What should you recommend using to enforce the governance requirement?

A. regulatory compliance standards in Microsoft Defender for Cloud
B. custom Azure roles
C. Azure Policy assignments
D. Azure management groups

Answer: C

NEW QUESTION 142
- (Exam Topic 3)
Your company has a hybrid cloud infrastructure.
Data and applications are moved regularly between cloud environments.
The company's on-premises network is managed as shown in the following exhibit.



You are designing security operations to support the hybrid cloud infrastructure. The solution must meet the following requirements:
- Govern virtual machines and servers across multiple environments.
- Enforce standards for all the resources across all the environment across the Azure policy.

Which two components should you recommend for the on-premises network? Each correct answer presents part of the solution.
NOTE Each correct selection is worth one point.

A. Azure VPN Gateway
B. guest configuration in Azure Policy
C. on-premises data gateway
D. Azure Bastion
E. Azure Arc

Answer: BE

Explanation:
https://docs.microsoft.com/en-us/azure/governance/machine-configuration/overview

NEW QUESTION 145
- (Exam Topic 3)
Your company has a Microsoft 365 E5 subscription.
The Chief Compliance Officer plans to enhance privacy management in the working environment. You need to recommend a solution to enhance the privacy management. The solution must meet the following requirements:
• Identify unused personal data and empower users to make smart data handling decisions.
• Provide users with notifications and guidance when a user sends personal data in Microsoft Teams.
• Provide users with recommendations to mitigate privacy risks. What should you include in the recommendation?

A. Microsoft Viva Insights
B. Advanced eDiscovery
C. Privacy Risk Management in Microsoft Priva
D. communication compliance in insider risk management

Answer: C

Explanation:
Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you:Detect overexposed personal data so that users can secure it.Spot and limit transfers of personal data across departments or regional borders.Help users identify and reduce the amount of unused personal data that you store.
https://www.microsoft.com/en-us/security/business/privacy/microsoft-priva-risk-management

NEW QUESTION 150
- (Exam Topic 3)
Your company has a hybrid cloud infrastructure.
The company plans to hire several temporary employees within a brief period. The temporary employees will need to access applications and data on the company' premises network.
The company's security policy prevents the use of personal devices for accessing company data and applications.
You need to recommend a solution to provide the temporary employee with access to company resources. The solution must be able to scale on demand.
What should you include in the recommendation?

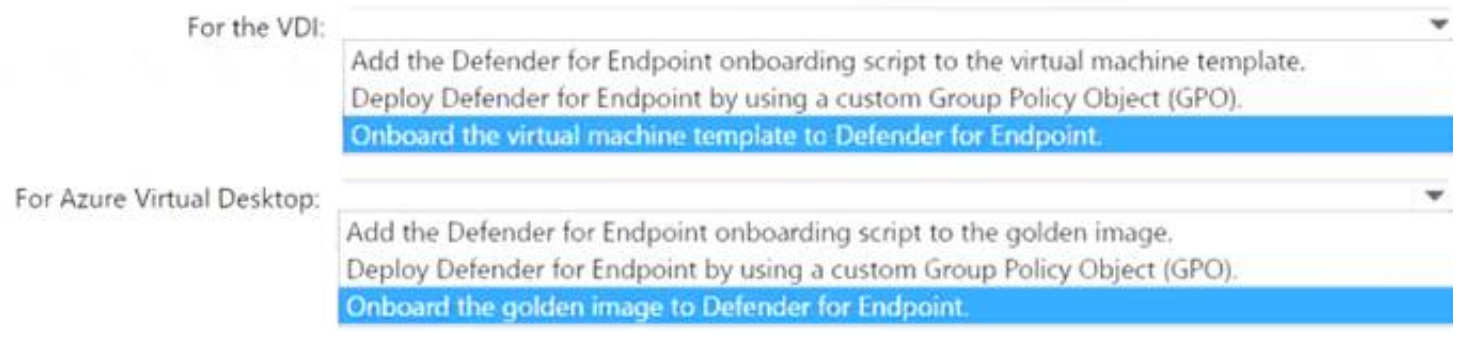
A. Migrate the on-premises applications to cloud-based applications.
B. Redesign the VPN infrastructure by adopting a split tunnel configuration.
C. Deploy Microsoft Endpoint Manager and Azure Active Directory (Azure AD) Conditional Access.
D. Deploy Azure Virtual Desktop, Azure Active Directory (Azure AD) Conditional Access, and Microsoft Defender for Cloud Apps.

Answer: D

Explanation:
https://docs.microsoft.com/en-us/azure/architecture/example-scenario/wvd/windows-virtual-desktop https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-microsoft-defender-for-c

NEW QUESTION 153
- (Exam Topic 3)
You have an Active Directory Domain Services (AD DS) domain that contains a virtual desktop infrastructure (VDI). The VDI uses non-persistent images and cloned virtual machine templates. VDI devices are members of the domain.
You have an Azure subscription that contains an Azure Virtual Desktop environment. The environment contains host pools that use a custom golden image. All the Azure Virtual Desktop deployments are members of a single Azure Active Directory Domain Services (Azure AD DS) domain.
You need to recommend a solution to deploy Microsoft Defender for Endpoint to the hosts. The solution must meet the following requirements:
• Ensure that the hosts are onboarded to Defender for Endpoint during the first startup sequence.
• Ensure that the Microsoft Defender 365 portal contains a single entry for each deployed VDI host.
• Minimize administrative effort.
What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

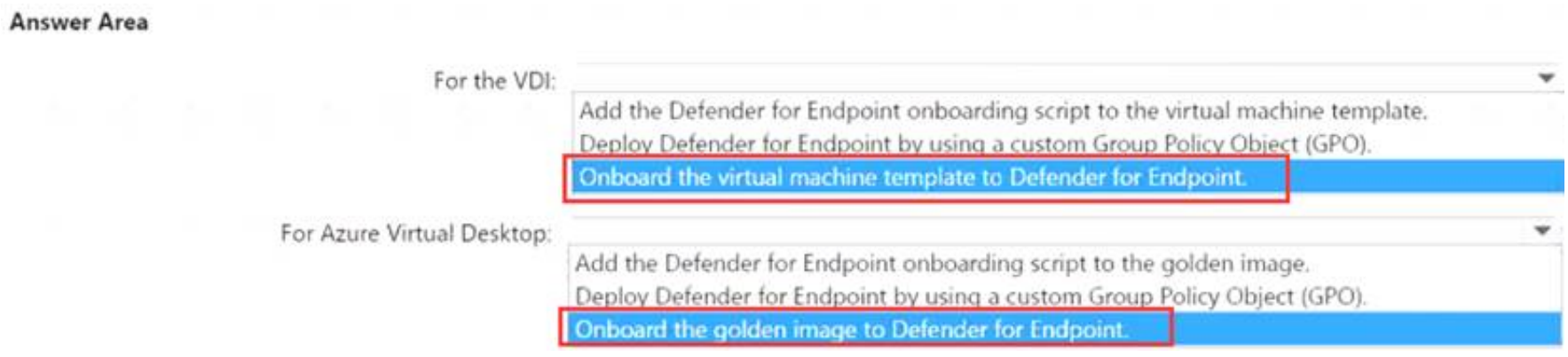
Answer Area



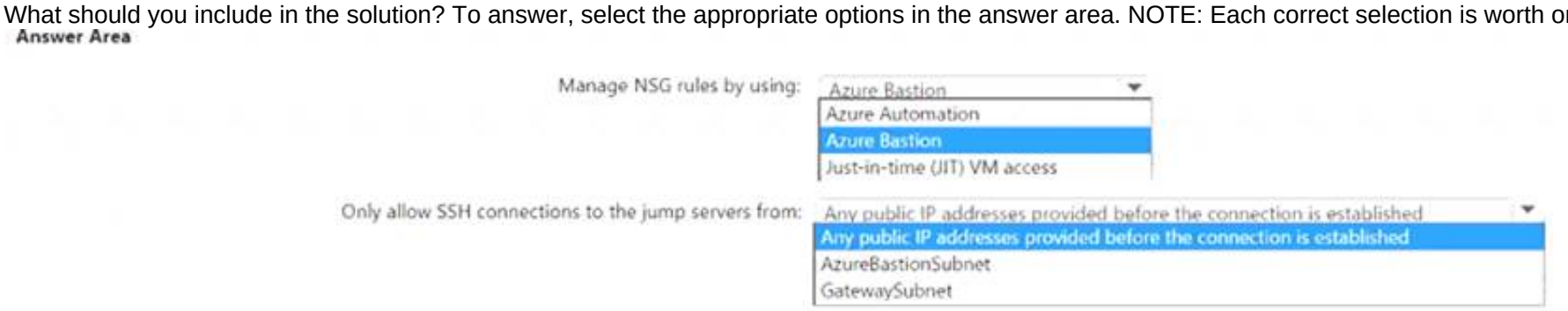
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 156
- (Exam Topic 3)
You plan to deploy a dynamically scaling, Linux-based Azure Virtual Machine Scale Set that will host jump servers. The jump servers will be used by support staff who connect from personal and kiosk devices via the internet. The subnet of the jump servers will be associated to a network security group (NSG).
You need to design an access solution for the Azure Virtual Machine Scale Set. The solution must meet the following requirements:
• Ensure that each time the support staff connects to a jump server; they must request access to the server.
• Ensure that only authorized support staff can initiate SSH connections to the jump servers.
• Maximize protection against brute-force attacks from internal networks and the internet.
• Ensure that users can only connect to the jump servers from the internet.
• Minimize administrative effort.
What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

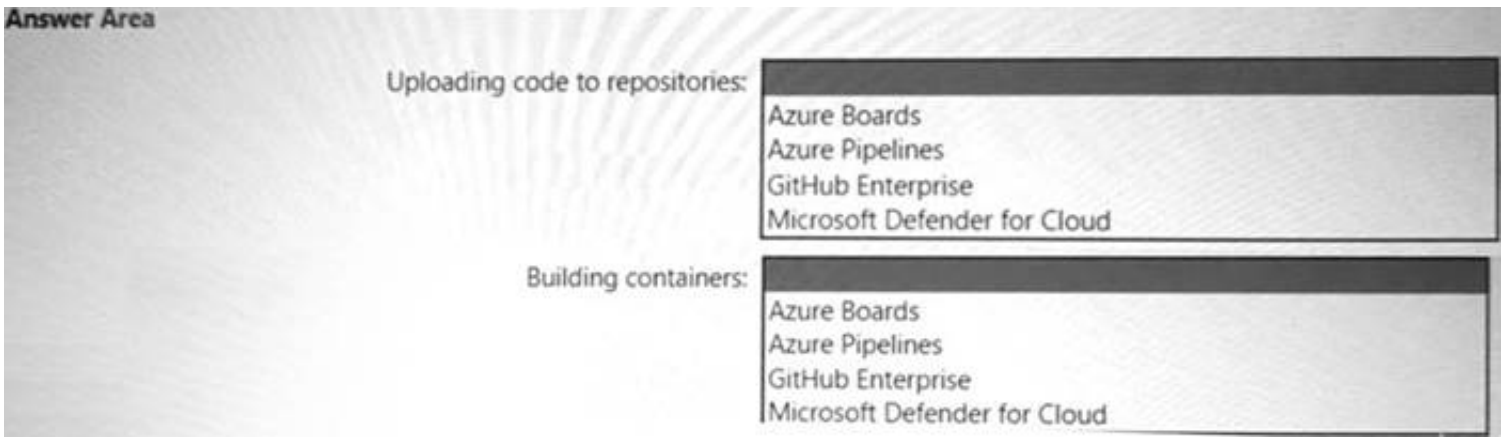
Explanation:

NEW QUESTION 159
- (Exam Topic 3)
You have an Azure AD tenant that syncs with an Active Directory Domain Services {AD DS) domain. Client computers run Windows and are hybrid-joined to Azure AD.
You are designing a strategy to protect endpoints against ransomware. The strategy follows Microsoft Security Best Practices.
You plan to remove all the domain accounts from the Administrators group on the Windows computers. You need to recommend a solution that will provide users with administrative access to the Windows
computers only when access is required. The solution must minimize the lateral movement of ransomware
attacks if an administrator account on a computer is compromised.
What should you include in the recommendation?

A. Local Administrator Password Solution (LAPS)
B. Privileged Access Workstations (PAWs)
C. Azure AD Privileged Identity Management (PIM)
D. Azure AD identity Protection

Answer: A

NEW QUESTION 162
- (Exam Topic 3)
Your company has an Azure App Service plan that is used to deploy containerized web apps. You are designing a secure DevOps strategy for deploying the web apps to the App Service plan. You need to recommend a strategy to integrate code scanning tools into a secure software development lifecycle. The code must be scanned during the following two phases:
Uploading the code to repositories Building containers
Where should you integrate code scanning for each phase? To answer, select the appropriate options in the answer area.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://docs.github.com/en/enterprise-cloud@latest/get-started/learning-about-github/about-github-advanced-sec https://microsoft.github.io/code-with-engineering-playbook/automated-testing/tech-specific-samples/azdo-conta

NEW QUESTION 166
- (Exam Topic 3)
Your company has an on-premise network in Seattle and an Azure subscription. The on-premises network contains a Remote Desktop server.
The company contracts a third-party development firm from France to develop and deploy resources to the virtual machines hosted in the Azure subscription.
Currently, the firm establishes an RDP connection to the Remote Desktop server. From the Remote Desktop connection, the firm can access the virtual machines hosted in Azure by using custom administrative tools installed on the Remote Desktop server. All the traffic to the Remote Desktop server is captured by a firewall, and the firewall only allows specific connections from France to the server.
You need to recommend a modern security solution based on the Zero Trust model. The solution must minimize latency tor developers.
Which three actions should you recommend? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Configure network security groups (NSGs) to allow access from only specific logical groupings of IP address ranges.
B. Implement Azure Firewall to restrict host pool outbound access.
C. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations.
D. Migrate from the Remote Desktop server to Azure Virtual Desktop.
E. Deploy a Remote Desktop server to an Azure region located in France.

Answer: BCD

Explanation:
https://docs.microsoft.com/en-us/azure/firewall/protect-azure-virtual-desktop

NEW QUESTION 170
- (Exam Topic 3)
Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government.
You need to review the current subscription for NIST 800-53 compliance. What should you do first?

A. From Defender for Cloud, review the secure score recommendations.
B. From Microsoft Sentinel, configure the Microsoft Defender for Cloud data connector.
C. From Defender for Cloud, review the Azure security baseline for audit report.
D. From Defender for Cloud, add a regulatory compliance standard.

Answer: D

Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regula

NEW QUESTION 172
- (Exam Topic 3)
You have an Azure subscription. The subscription contains 50 virtual machines that run Windows Server and 50 virtual machines that run Linux. You need to perform vulnerability assessments on the virtual machines. The solution must meet the following requirements:
• Identify missing updates and insecure configurations.
• Use the Qualys engine. What should you use?

A. Microsoft Defender for Servers
B. Microsoft Defender Threat Intelligence (Defender TI)
C. Microsoft Defender for Endpoint
D. Microsoft Defender External Attack Surface Management (Defender EASM)

Answer: A

NEW QUESTION 177
- (Exam Topic 3)
Your company has a Microsoft 365 E5 subscription. The company wants to identify and classify data in Microsoft Teams, SharePoint Online, and Exchange Online. You need to recommend a solution to identify documents that contain sensitive information. What should you include in the recommendation?

A. data classification content explorer
B. data loss prevention (DLP)
C. eDiscovery
D. Information Governance

Answer: B

NEW QUESTION 179
- (Exam Topic 3)
You have a hybrid cloud infrastructure.
You plan to deploy the Azure applications shown in the following table.

Name	Type	Requirement
App1	An Azure App Service web app accessed from Windows 11 devices on the on-premises network	Protect against attacks that use cross-site scripting (XSS).
App2	An Azure App Service web app accessed from mobile devices	Allow users to authenticate to App2 by using their LinkedIn account.

What should you use to meet the requirement of each app? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

App1:
App2:

Azure AD B2B authentication with Conditional Access
Azure AD B2C custom policies with Conditional Access
Azure Application Gateway Web Application Firewall policies
Azure Firewall
Azure VPN Gateway with network security group rules
Azure VPN Point-to-Site connections

App2:

Azure AD B2B authentication with Conditional Access
Azure AD B2C custom policies with Conditional Access
Azure Application Gateway Web Application Firewall policies
Azure Firewall
Azure VPN Gateway with network security group rules
Azure VPN Point-to-Site connections

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text Description automatically generated with medium confidence

NEW QUESTION 183
- (Exam Topic 3)
Your company plans to move all on-premises virtual machines to Azure. A network engineer proposes the Azure virtual network design shown in the following table.

Virtual network name	Description	Peering connection
Hub VNet	Linux and Windows virtual machines	VNet1, VNet2
VNet1	Windows virtual machines	Hub VNet
VNet2	Linux virtual machines	Hub VNet
VNet3	Windows virtual machine scale sets	VNet4
VNet4	Linux virtual machine scale sets	VNet3

You need to recommend an Azure Bastion deployment to provide secure remote access to all the virtual machines. Based on the virtual network design, how many Azure Bastion subnets are required?

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: C

Explanation:
https://docs.microsoft.com/en-us/azure/bastion/vnet-peering
https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure-bastion

NEW QUESTION 186
- (Exam Topic 3)
You have an Azure subscription that contains a Microsoft Sentinel workspace.

Your on-premises network contains firewalls that support forwarding event logs m the Common Event Format (CEF). There is no built-in Microsoft Sentinel connector for the firewalls
You need to recommend a solution to ingest events from the firewalls into Microsoft Sentinel. What should you include m the recommendation?

A. an Azure logic app
B. an on-premises Syslog server
C. an on-premises data gateway
D. Azure Data Factory

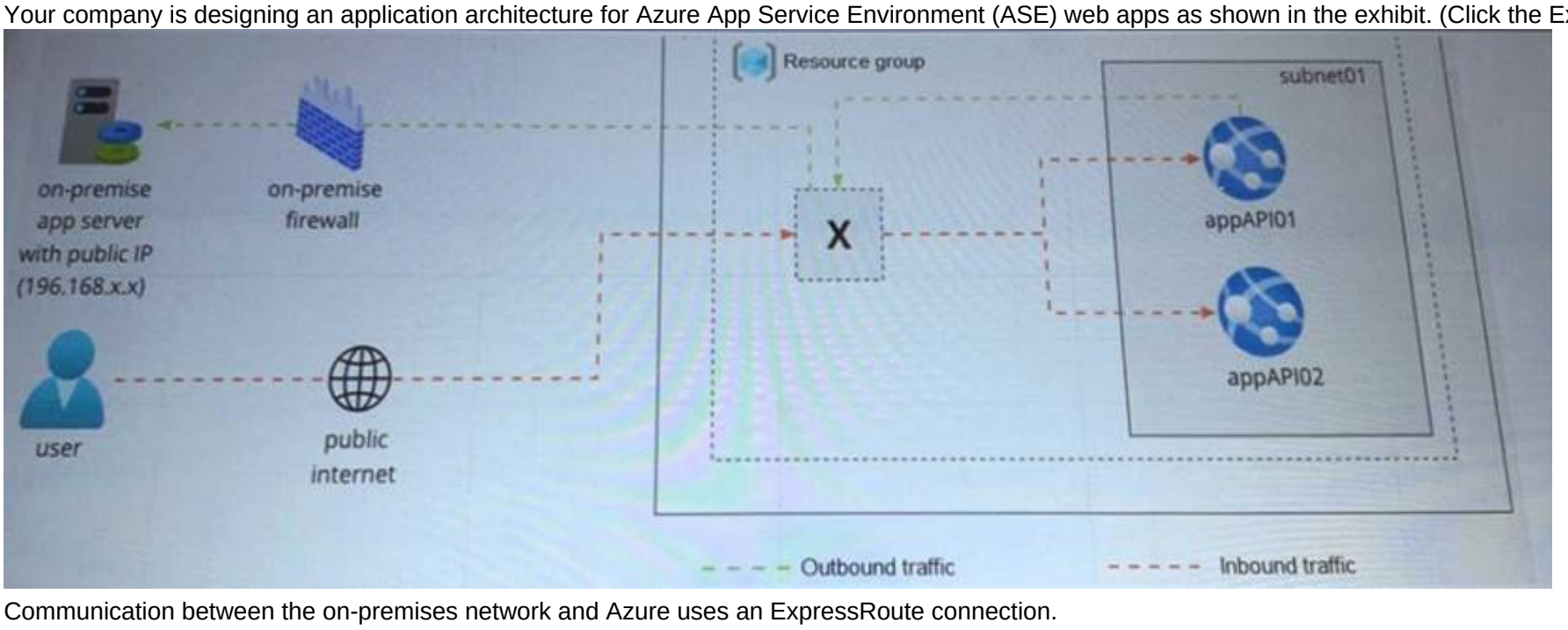
Answer: B

NEW QUESTION 190
- (Exam Topic 3)
You have an Azure subscription. The subscription contains 100 virtual machines that run Windows Server. The virtual machines are managed by using Azure Policy and Microsoft Defender for Servers.
You need to enhance security on the virtual machines. The solution must meet the following requirements:
• Ensure that only apps on an allowlist can be run.
• Require administrators to confirm each app added to the allowlist.
• Automatically add unauthorized apps to a blocklist when an attempt is made to launch the app.
• Require administrators to approve an app before the app can be moved from the blocklist to the allowlist. What should you include in the solution?

A. a compute policy in Azure Policy
B. admin consent settings for enterprise applications in Azure AD
C. adaptive application controls in Defender for Servers
D. app governance in Microsoft Defender for Cloud Apps

Answer: C

NEW QUESTION 194
- (Exam Topic 3)
Your company is designing an application architecture for Azure App Service Environment (ASE) web apps as shown in the exhibit. (Click the Exhibit tab.)



Communication between the on-premises network and Azure uses an ExpressRoute connection.
You need to recommend a solution to ensure that the web apps can communicate with the on-premises application server. The solution must minimize the number of public IP addresses that are allowed to access the on-premises network.
What should you include in the recommendation?

A. Azure Traffic Manager with priority traffic-routing methods
B. Azure Application Gateway v2 with user-defined routes (UDRs).
C. Azure Front Door with Azure Web Application Firewall (WAF)
D. Azure Firewall with policy rule sets

Answer: C

Explanation:
https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview

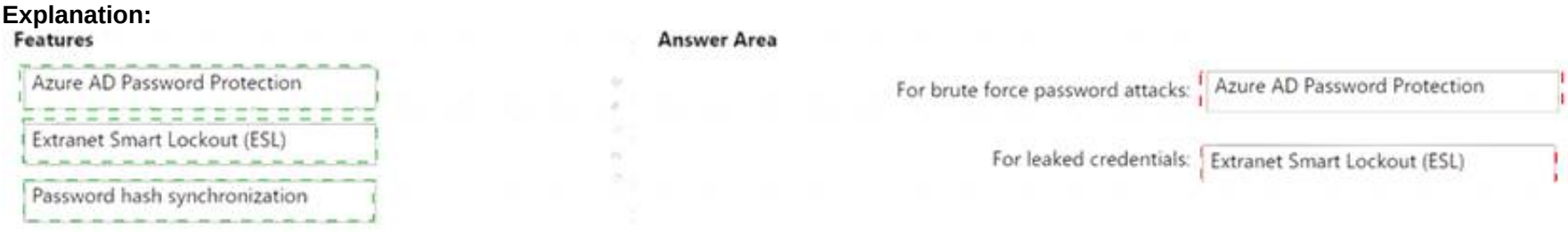
NEW QUESTION 197
- (Exam Topic 3)
You have a hybrid Azure AD tenant that has pass-through authentication enabled. You are designing an identity security strategy.
You need to minimize the impact of brute force password attacks and leaked credentials of hybrid identities.
What should you include in the design? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Features	Answer Area	
Azure AD Password Protection	For brute force password attacks:	
Extranet Smart Lockout (ESL)	For leaked credentials:	
Password hash synchronization		

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 198
- (Exam Topic 3)
You have a Microsoft 365 subscription that syncs with Active Directory Domain Services (AD DS).
You need to define the recovery steps for a ransomware attack that encrypted data in the subscription The solution must follow Microsoft Security Best Practices.
What is the first step in the recovery plan?

A. Disable Microsoft OneDnve sync and Exchange ActiveSync.
B. Recover files to a cleaned computer or device.
C. Contact law enforcement.
D. From Microsoft Defender for Endpoint perform a security scan.

Answer: A

NEW QUESTION 203
- (Exam Topic 3)
You have 50 Azure subscriptions.
You need to monitor resource in the subscriptions for compliance with the ISO 27001:2013 standards. The solution must minimize the effort required to modify the list of monitored policy definitions for the subscriptions.
NOTE: Each correct selection is worth one point.

A. Assign an initiative to a management group.
B. Assign a policy to each subscription.
C. Assign a policy to a management group.
D. Assign an initiative to each subscription.
E. Assign a blueprint to each subscription.
F. Assign a blueprint to a management group.

Answer: AF

Explanation:
https://docs.microsoft.com/en-us/azure/governance/management-groups/overview https://docs.microsoft.com/en-us/azure/governance/blueprints/overview https://docs.microsoft.com/en-us/azure/governance/policy/samples/iso-27001 https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

NEW QUESTION 205
- (Exam Topic 3)
You have the following on-premises servers that run Windows Server:
• Two domain controllers in an Active Directory Domain Services (AD DS) domain
• Two application servers named Server1 and Server2 that run ASP.NET web apps
• A VPN server named Server3 that authenticates by using RADIUS and AD DS End users use a VPN to access the web apps over the internet.
You need to redesign a user access solution to increase the security of the connections to the web apps. The solution must minimize the attack surface and follow the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).
What should you include in the recommendation?

A. Configure connectors and rules in Microsoft Defender for Cloud Apps.
B. Configure web protection in Microsoft Defender for Endpoint.
C. Publish the web apps by using Azure AD Application Proxy.
D. Configure the VPN to use Azure AD authentication.

Answer: C

NEW QUESTION 207
- (Exam Topic 3)
You are designing the encryption standards for data at rest for an Azure resource
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For Azure SQL databases, you recommend Transparent Data Encryption (TDE) that uses customer-managed keys (CMKs).
Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 209
- (Exam Topic 3)
You have an Azure subscription that contains virtual machines, storage accounts, and Azure SQL databases.
All resources are backed up multiple times a day by using Azure Backup. You are developing a strategy to protect against ransomware attacks.
You need to recommend which controls must be enabled to ensure that Azure Backup can be used to restore the resources in the event of a successful ransomware attack.
Which two controls should you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Use Azure Monitor notifications when backup configurations change.
B. Require PINs for critical operations.
C. Perform offline backups to Azure Data Box.
D. Encrypt backups by using customer-managed keys (CMKs).
E. Enable soft delete for backups.

Answer: AB

Explanation:
https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware 'You need to recommend which CONTROLS must be enabled to ENSURE that Azure Backup can be used to RESTORE the resources in the event of a successful ransomware attack.' Whilst helpful for auditing purposes and detection of a malicious attack, monitoring configuration changes and alerting after a change is made does not represent a CONTROL which ENSURES Azure Backup can be used to RESTORE the resources.

NEW QUESTION 213
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SC-100 Practice Exam Features:

* SC-100 Questions and Answers Updated Frequently

* SC-100 Practice Questions Verified by Expert Senior Certified Staff

* SC-100 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SC-100 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year