Microsoft

Exam Questions az-500

Microsoft Azure Security Technologies

NEW QUESTION 1
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.
Solution: You deploy an Azure AD Application Proxy.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:

➢ Create Azure Virtual Network.

➢ Create a custom DNS server in the Azure Virtual Network.

➢ Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.

➢ Configure forwarding between the custom DNS server and your on-premises DNS server. Reference:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

NEW QUESTION 2
- (Exam Topic 4)
You have an Azure subscription.
You configure the subscription to use a different Azure Active Directory (Azure AD) tenant. What are two possible effects of the change? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Role assignments at the subscription level are lost.
B. Virtual machine managed identities are lost.
C. Virtual machine disk snapshots are lost.
D. Existing Azure resources are deleted.

Answer: AB

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associ

NEW QUESTION 3
- (Exam Topic 4)
You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Description
EventHub1	Azure Event Hubs	Not applicable
Adf1	Azure Data Factory	Not applicable
NVA1	Network virtual appliance (NVA)	The NVA sends security event messages in the Common Event Format (CEF).

You have an Azure subscription named Subscription2 that contains the following resources:

➢ An Azure Sentinel workspace

➢ An Azure Event Grid instance
You need to ingest the CEF messages from the NVAs to Azure Sentinel.
What should you configure for each subscription? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Subscription1: ⌄

An Azure Log Analytics agent on a Linux virtual machine
A Data Factory pipeline
An Event Hubs namespace
An Azure Service Bus queue

Subscription2: ⌄

A new Azure Log Analytics workspace
A new Azure Sentinel data connector
A new Azure Sentinel playbook
A new Event Grid resource provider

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated

NEW QUESTION 4
- (Exam Topic 4)
You have Azure Resource Manager templates that you use to deploy Azure virtual machines.
You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.
What should you use?

A. security policies in Azure Security Center
B. Azure Logic Apps
C. an Azure Desired State Configuration (DSC) virtual machine extension
D. Azure Advisor

Answer: C

NEW QUESTION 5
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.
Subnet1 and Subnet2 have a network security group {NSG). The NSG has an outbound rule that has the following configurations:
• Port; Any
• Source: Any
• Priority: 100
• Action: Deny
• Protocol: Any
• Destination: Storage
The subscription contains a storage account named storage1.
You create a private endpoint named Private1 that has the following settings:
• Resource type: Microsoft.Storage/storageAccounts
• Resource: storage1
• Target sub-resource: blob
• Virtual network: VNet1
• Subnet: Subnet1
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1.	○	○
From VM1, you can upload data to the blob storage of storage1.	○	○
From VM2, you can upload data to the blob storage of storage1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1.	○	○
From VM1, you can upload data to the blob storage of storage1.	○	○
From VM2, you can upload data to the blob storage of storage1.	○	○

NEW QUESTION 6
- (Exam Topic 4)
Lab Task
Task 5

A user named Debbie has the Azure app installed on her mobile device.
You need to ensure that debbie@contoso.com is alerted when a resource lock is deleted.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Create an Azure Resource Manager service principal. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify a name and a role for the service principal, such as Contributor.
Grant permission to the service principal to access the secrets in the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to assign the Key Vault Secrets User role to the service principal at the scope of the key vault or individual secrets.
Enable template deployment for the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to set the enabledForTemplateDeployment property of the key vault to true.
Reference the secrets in the template by using their resource ID. You can use the listSecrets function to get the resource ID of a secret in the key vault. You need to specify the name of the key vault and the name of the secret as parameters.
Deploy the template by using Azure PowerShell, Azure CLI, or REST API. You can use the New-AzResourceGroupDeployment cmdlet, the az deployment group create command, or the Deployments - Create Or Update REST API to do this. You need to provide the template file or URI and any required parameters. You also need to provide the credentials of the service principal.

NEW QUESTION 7
- (Exam Topic 4)
You have multiple development teams that will create apps in Azure.
You plan to create a standard development environment that will be deployed for each team.
You need to recommend a solution that will enforce resource locks across the development environments and ensure that the locks are applied in a consistent manner.
What should you include in the recommendation?

A. an Azure policy
B. an Azure Resource Manager template
C. a management group
D. an Azure blueprint

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

NEW QUESTION 8
- (Exam Topic 4)
You have an Azure subscription.
You plan to create two custom roles named Role1 and Role2.
The custom roles will be used to perform the following tasks:
• Members of Role1 will manage application security groups.
• Members of Role2 will manage Azure Bastion. You need to add permissions to the custom roles.
Which resource provider should you use for each role? To answer, drag the appropriate resource providers to the correct roles. Each resource provider 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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Resource Providers		Answer Area	
Microsoft.Compute			
Microsoft.Network		Role1:	Microsoft.Network
Microsoft.Security		Role2:	Microsoft.Network
Microsoft.Solutions			

NEW QUESTION 9
- (Exam Topic 4)
You have an Azure subscription that contains three storage accounts, an Azure SQL managed instance named SQL and three Azure SQL databases. The storage accounts are configured as shown in the following table.
SQ11 has the following settings:
• Auditing: On
• Audit tog destination: storage1
The Azure SQL databases are configured as shown in the following table.

Answer Area

Statements	Yes	No
Audit events for DB1 are written to storage1.	○	○
Audit events for DB2 are written to storage1 and storage2.	○	○
Storage3 can be used as an audit log destination for DB3.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/auditing-configure https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview

NEW QUESTION 10
- (Exam Topic 4)
You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Region	Description
HubVNet	East US	HubVNet is a virtual network connected to the on-premises network by using a site-to-site VPN that has BGP route propagation enabled. HubVNet contains a subnet named HubVNetSubnet0.
SpokeVNet	East US	SpokeVNet is a virtual network connected to HubVNet by using VNet peering. SpokeVNet contains a subnet named SpokeVNetSubnet0.

The Azure virtual machines on SpokeVNetSubnet0 can communicate with the computers on the on-premises network.
You plan to deploy an Azure firewall to HubVNet. You create the following two routing tables:

≫ RT1: Includes a user-defined route that points to the private IP address of the Azure firewall as a next hop address
≫ RT2: Disables BGP route propagation and defines the private IP address of the Azure firewall as the default gateway
You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.
To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet 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.

Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

RT1:

RT2:

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

RT1: GatewaySubnet

RT2: HubVNetSubnet0

NEW QUESTION 10
- (Exam Topic 4)
You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the Exhibit tab.)

BASICS

Subscription	Microsoft Azure Sponsorship
Resource group	AzureBackupRG_eastus2_1
Region	East US
Kubernetes cluster name	akscluster2
Kubernetes version	1.1 1.5
DNS name prefix	akscluster2
Node count	3
Node size	Standard_DS2_v2
Virtual nodes (preview)	Disabled

AUTHENTICATION

Enable RBAC	No

NETWORKING

HTTP application routing	Yes
Network configuration	Basic

MONITORING

Enable container monitoring	No

TAGS

You plan to deploy the cluster to production. You disable HTTP application routing.
You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.
What should you do?

A. Create an AKS Ingress controller.
B. Install the container network interface (CNI) plug-in.
C. Create an Azure Standard Load Balancer.
D. Create an Azure Basic Load Balancer.

Answer: A

Explanation:
An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.
References:
https://docs.microsoft.com/en-us/azure/aks/ingress-tls

NEW QUESTION 12
- (Exam Topic 4)
Your network contains an Active Directory forest named contoso.com. You have an Azure Directory (Azure AD) tenant named contoso.com.
You plan to configure synchronization by using the Express Settings installation option in Azure AD Connect. You need to identify which roles and groups are required to perform the planned configurations. The solution
must use the principle of least privilege.
Which two roles and groups should you identify? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. the Domain Admins group in Active Directory
B. the Security administrator role in Azure AD
C. the Global administrator role in Azure AD
D. the User administrator role in Azure AD
E. the Enterprise Admins group in Active Directory

Answer: CE

Explanation:
 References:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

NEW QUESTION 13
- (Exam Topic 4)
Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory Azure (Azure AD) tenant named contoso.com.
The company develops a mobile application named App1. App1 uses the OAuth 2 implicit grant type to acquire Azure AD access tokens.
You need to register App1 in Azure AD.
What information should you obtain from the developer to register the application?

A. a redirect URI
B. a reply URL
C. a key
D. an application ID

Answer: A

Explanation:
For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token
responses. References:
https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code

NEW QUESTION 15
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

From Azure AD Privileged Identity Management (PIM), you configure the settings for the Security Administrator role as shown in the following exhibit.

Settings ☐ ✕

Assignment

☑ Allow permanent eligible assignment

Expire eligible assignments after

3 Months ▼

☑ Allow permanent active assignment

Expire active assignments after

1 Month ▼

☐ Require Azure Multi-Factor Authentication on active assignment

☑ Require justification on active assignment

Activation

Activation maximum duration (hours)

━━━━○▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬   5

☐ Require Azure Multi-Factor Authentication on activation

☐ Require justification on activation

☐ Require ticket information on activation

☐ Require approval to activate

* ▣ Select approvers
No member or group selected   >

From PIM, you assign the Security Administrator role to the following groups:

≫ Group1: Active assignment type, permanently assigned

≫ Group2: Eligible assignment type, permanently eligible

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	○	○
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	○	○
User3 can activate the Security Administrator role.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
Eligible Type: A role assignment that requires a user to perform one or more actions to use the role. If a user has been made eligible for a role, that means they can activate the role when they need to perform privileged tasks. There's no difference in the access given to someone with a permanent versus an eligible role assignment. The only difference is that some people don't need that access all the time.
You can choose from two assignment duration options for each assignment type (eligible and active) when you configure settings for a role. These options become the default maximum duration when a user is assigned to the role in Privileged Identity Management.
Use the Activation maximum duration slider to set the maximum time, in hours, that a role stays active before it expires. This value can be from one to 24 hours.
Box 2: Yes
Active Type: A role assignment that doesn't require a user to perform any action to use the role. Users assigned as active have the privileges assigned to the role
Box 3: Yes
User3 is member of Group2. Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource-roles

NEW QUESTION 17
- (Exam Topic 4) You have an Azure SQL database. You implement Always Encrypted.
You need to ensure that application developers can retrieve and decrypt data in the database.
Nantes's of information should you provide to the developers? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a stored access policy
B. a shared access signature (SAS)
C. the column encryption key
D. user credentials
E. the column master key

Answer: CE

Explanation:
Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.
References:
https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine

NEW QUESTION 20
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	None	Disabled
User2	Group1	Disabled
user3	Group1	Enforced

Azure AD Privileged Identity Management (PIM) is enabled for the tenant. In PIM, the Password Administrator role has the following settings:

≫ Maximum activation duration (hours): 2

≫ Send email notifying admins of activation: Disable

≫ Require incident/request ticket number during activation: Disable

≫ Require Azure Multi-Factor Authentication for activation: Enable

≫ Require approval to activate this role: Enable

≫ Selected approver: Group1

You assign users the Password Administrator role as shown in the following table.

Name	Assignment type
User1	Active
User2	Eligible
user3	Eligible

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	○	○
User2 can request to activate the Password Administrator role.	○	○
If User3 wants to activate the Password Administrator role, the user can approve their own request.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
YES (Already active)
YES (The user will be prompted for MFA regardless the MFA Status of the user) NO (Even the user is included in the group, a user can't approve itself)
https://docs.microsoft.com/es-es/azure/active-directory/privileged-identity-management/pim-deployment-plan (Require approval section)

NEW QUESTION 25
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Operating system
VM1	Windows Server 2016
VM2	Ubuntu Server 18.04 LTS

From Azure Security Center, you turn on Auto Provisioning. You deploy the virtual machines shown in the following table.

Name	Operating system
VM3	Windows Server 2016
VM4	Ubuntu Server 18.04 LTS

On which virtual machines is the Log Analytics agent installed?

A. VM3 only
B. VM1 and VM3 only
C. VM3 and VM4 only
D. VM1, VM2, VM3, and VM4

Answer: D

Explanation:
When automatic provisioning is On, Security Center provisions the Log Analytics Agent on all supported Azure VMs and any new ones that are created.
Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

NEW QUESTION 29
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault.
You need to configure maximum number of days for Which new keys are valid. The solution must minimize administrative effort.
What should you use?

A. Key Vault properties
B. Azure Policy
C. Azure Purview
D. Azure Blueprints

Answer: B

NEW QUESTION 33
- (Exam Topic 4)
You have three on-premises servers named Server1, Server2, and Server3 that run Windows Server1 and Server2 and located on the Internal network. Server3 is located on the premises network. All servers have access to Azure.
From Azure Sentinel, you install a Windows firewall data connector.
You need to collect Microsoft Defender Firewall data from the servers for Azure Sentinel. What should you do?

A. Create an event subscription from Server1, Server2 and Server3
B. Install the On-premises data gateway on each server.
C. Install the Microsoft Agent on each server.
D. Install the Microsoft Agent on Server1 and Server2 install the on-premises data gateway on Server3.

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall

NEW QUESTION 34
- (Exam Topic 4)
You have an Azure subscription that contains an instance of Azure Firewall Standard named AzFWL You need to identify whether you can use the following features with AzFW1:
• TLS inspection
• Threat intelligence
• The network intrusion detection and prevention systems (IDPS) What can you use?

A. TLS inspection only
B. threat intelligence only
C. TLS inspection and the IDPS only
D. threat intelligence and the IDPS only
E. TLS inspection, threat intelligence, and the IDPS

Answer: E

NEW QUESTION 36
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.4	13.80.73.87
VM2	VNET2/Subnet2	10.2.1.4	213.199.133.190
VM3	VNET2/Subnet2	10.2.1.5	None

Subnet1 and Subnet2 have a Microsoft.Storage service endpoint configured.
You have an Azure Storage account named storageacc1 that is configured as shown in the following exhibit.

🖫 Save ✕ Discard ↻ Refresh

Allow access from
○ All networks ⊙ Selected networks

Configure network security for your storage accounts. Learn more.

Virtual networks
Secure your storage account with virtual networks.   + Add existing virtual network
+ Add new virtual network

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIBTION

No network selected.

Firewall
Add IP ranges to allow access from the internet on your on-premises networks. Learn more.

Address Range

13.80.73.87   🗑

IP address or CIDR

Exceptions
☑ Allow trusted Microsoft services to access this storage account ⓘ
☐ Allow read access to storage logging from any network
☐ Allow read access to storage metrics from any network

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	○	○
From VM2, you can upload a blob to storageacc1.	○	○
From VM3 , you can upload a blob to storageacc1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
The public IP of VM1 is allowed through the firewall.
Box 2: No
The allowed virtual network list is empty so VM2 cannot access storageacc1 directly. The public IP address of VM2 is not in the allowed IP list so VM2 cannot access storageacc1 over the Internet.
Box 3: No
The allowed virtual network list is empty so VM3 cannot access storageacc1 directly. VM3 does not have a public IP address so it cannot access storageacc1 over the Internet.
Reference:
https://docs.microsoft.com/en-gb/azure/storage/common/storage-network-security

NEW QUESTION 37
- (Exam Topic 4)
You have an Azure subscription that contains a resource group named RG1 and a security group named ServerAdmins. RG1 contains 10 virtual machines, a virtual network named VNET1, and a network security group JNSG) named NSG1. ServerAdmins can access the virtual machines by using RDP.
You need to ensure that NSG1 only allows RDP connections to the virtual machines for a maximum of 60 minutes when a member of ServerAdmins requests access.
What should you configure?

A. an Azure policy assigned to RGI

B. a just in time (JIT) VM access policy in Microsoft Defender for Cloud
C. an Azure AD Privileged Identity Management (PiM) role assignment
D. an Azure Bastion host on VNET1

Answer: B

NEW QUESTION 38
- (Exam Topic 4)
You have a network security group (NSG) bound to an Azure subnet.
You run Get-AzureRmNetworkSecurityRuleConfig and receive the output shown in the following exhibit.

```
Name                                  :  DenyStorageAccess
Description                           :
Protocol                              :  *
SourcePortRange                       :  {*}
DestinationPortRange                  :  {*}
SourceAddressPrefix                   :  {*}
DestinationAddressPrefix              :  {Storage}
SourceApplicationSecurityGroups       :  []
DestinationApplicationSecurityGroups  :  []
Access                                :  Deny
Priority                              :  105
Direction                             :  Outbound

Name                                  :  StorageEA2Allow
ProvisionIngState                     :  Succeeded
Description                           :
Protocol                              :  *
SourcePortRange                       :  {*}
DestinationPortRange                  :  {443}
SourceAddressPrefix                   :  {*}
DestinationAddressPrefix              :  {Storage/EastUS2}
SourceApplicationSecurityGroups       :  []
DestinationApplicationSecurityGroups  :  []
Access                                :  Allow
Priority                              :  104
Direction                             :  Outbound

Name                                  :  Contoso_FTP
Description                           :
Protocol                              :  TCP
SourcePortRange                       :  {*}
DestinationPortRange                  :  {21}
SourceAddressPrefix                   :  {1.2.3.4/32}
DestinationAddressPrefix              :  {10.0.0.5/32}
SourceApplicationSecurityGroups       :  []
DestinationApplicationSecurityGroups  :  []
Access                                :  Allow
Priority                              :  504
Direction                             :  Inbound
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

Traffic destined for an Azure Storage account is [answer choice].

- able to connect to East US
- able to connect to East US 2
- able to connect to West Europe
- prevented from connecting to all regions

FTP connections from 1.2.3.4 to 10.0.0.10/32 are [answer choice].

- allowed
- dropped
- forwarded

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: able to connect to East US 2
The StorageEA2Allow has DestinationAddressPrefix {Storage/EastUS2} Box 2: dropped
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group

NEW QUESTION 40

- (Exam Topic 4)
You have an Azure subscription.
You plan to create a workflow automation in Azure Security Center that will automatically remediate a security vulnerability.
What should you create first?

A. a managed identity
B. an automation account
C. an Azure function app
D. an alert rule
E. an Azure logic app

Answer: E

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

NEW QUESTION 45
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains the resources shown in the following table.

Name	Type
User1	User
User2	User
User3	User
Group1	Security group
Group2	Security group
App1	Enterprise application

User2 is the owner of Group2.
The user and group settings for App1 are configured as shown in the following exhibit.

You enable self-service application access for App1 as shown in the following exhibit.

User3 is configured to approve access to Appl.
You need to identify the owners of Group2 and the users of Appl.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Group2 owners:

| User2 only |
| User3 only |
| User1 and User2 only |
| User2 and User3 only |
| User1, User2, and User3 |

App1 users:

| Group1 members only |
| Group2 members only |
| Group1 and Group2 members only |
| Group1 and Group2 members and User1 only |
| Group1 and Group2 members, User1, and User3 only |

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access

NEW QUESTION 47
- (Exam Topic 4)
You are troubleshooting a security issue for an Azure Storage account You enable Azure Storage Analytics logs and archive It to a storage account. What should you use to retrieve the diagnostics logs?

A. Azure Storage Explorer
B. SQL query editor in Azure
C. Azure Monitor
D. Azure Cosmos DB explorer

Answer: A

NEW QUESTION 50
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Resource group	Status
VM1	RG1	Stopped (Deallocated)
VM2	RG2	Stopped (Deallocated)

You create the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Not allowed resource types	virtualMachines	RG1
Allowed resource types	virtualMachines	RG2

You create the resource locks shown in the following table.

Name	Type	Created on
Lock1	Read-only	VM1
Lock2	Read-only	RG2

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can start VM1.	○	○
You can start VM2.	○	○
You can create a virtual machine in RG2.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

NEW QUESTION 51
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a policy definition and assignments that are scoped to resource groups. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
 References:
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-group

NEW QUESTION 54
- (Exam Topic 4)
You have the Azure resource shown in the following table.

Name	Type	Parent
Management1	Management group	Tenant Root Group
Subscription1	Subscription	Management1
RG1	Resource group	Subscription1
RG2	Resource group	Subscription1
VM1	Virtual machine	RG1
VM2	Virtual machine	RG2

You need to meet the following requirements:
* Internet-facing virtual machines must be protected by using network security groups (NSGs).
* All the virtual machines must have disk encryption enabled.
What is the minimum number of security that you should create in Azure Security Center?

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

Answer: D

NEW QUESTION 56
- (Exam Topic 4)
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to implement an application that will consist of the resources shown in the following table.

Name	Type	Description
CosmosDBAccount1	Azure Cosmos DB account	A Cosmos DB account containing a database Named CosmosDB1 that serves as a back-end tier of the application
WebApp1	Azure web app	A web app configured to serve as the middle tier of the application

Users will authenticate by using their Azure AD user account and access the Cosmos DB account by using resource tokens.
You need to identify which tasks will be implemented in CosmosDB1 and WebApp1.
Which task should you identify for each resource? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

CosmosDB1:
Authenticate Azure AD users and generate resource tokens.
Authenticate Azure AD users and relay resource tokens.
Create database users and generate resource tokens.

WebApp1:
Authenticate Azure AD users and generate resource tokens.
Authenticate Azure AD users and relay resource tokens.
Create database users and generate resource tokens.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
CosmosDB1: Create database users and generate resource tokens.
Azure Cosmos DB resource tokens provide a safe mechanism for allowing clients to read, write, and delete specific resources in an Azure Cosmos DB account according to the granted permissions.
WebApp1: Authenticate Azure AD users and relay resource tokens
A typical approach to requesting, generating, and delivering resource tokens to a mobile application is to use a resource token broker. The following diagram shows a high-level overview of how the sample application uses a resource token broker to manage access to the document database data:

References:
https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication
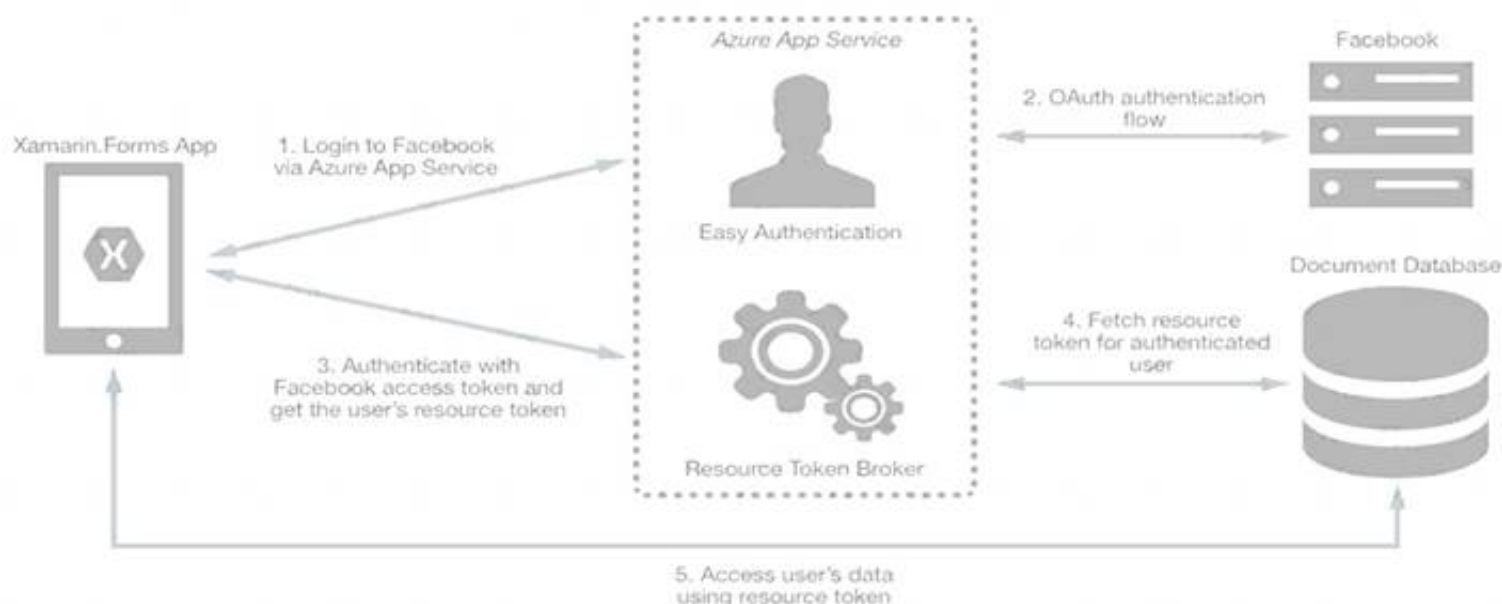
NEW QUESTION 59
- (Exam Topic 4)
You have an Azure subscription named Sub1 that contains the storage accounts shown in the following table

Name	Resource group
storage1	RG1
storage2	RG1
storage3	RG2

The storage3 storage account is encrypted by using customer-managed keys.
YOU need to enable Microsoft Defender for storage to meet the following requirements.
* The storage1 and storage2 account must be include in the defender for storage requirement.
* The storage3 account must be exclude from the Defender for Storage protections.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and them in the correct order.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 62

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains a user named User1.

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains an Azure Storage account named storage1. Storage1 contains an Azure file share named share1.

Currently, the domain and the tenant are not integrated.

You need to ensure that User1 can access share1 by using his domain credentials.

Which three actions should you perform in sequence? 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:

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard

NEW QUESTION 66

- (Exam Topic 4)

You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure SQL Database instance that is configured to support Azure AD authentication.

Database developers must connect to the database instance and authenticate by using their on-premises Active Directory account.

You need to ensure that developers can connect to the instance by using Microsoft SQL Server Management Studio. The solution must minimize authentication prompts.

Which authentication method should you recommend?

A. Active Directory - Password
B. Active Directory - Universal with MFA support
C. SQL Server Authentication
D. Active Directory - Integrated

Answer: D

Explanation:
 References:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

NEW QUESTION 69
- (Exam Topic 4)
You create an Azure subscription with Azure AD Premium P2.
You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure roles.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Discover privileged roles.	
Sign up PIM for Azure AD roles.	
Consent to PIM.	
Discover resources.	
Verify your identity by using multi-factor authentication (MFA).	

A. Mastered
B. Not Mastered

Answer: A

Explanation:
* 1. Verify your identity with MFA
* 2. Consent to PIM
* 3. Sign up PIM for AAD Roles

NEW QUESTION 74
- (Exam Topic 4)
You have an Azure subscription that contains the subnets shown in the following table.

Name	Virtual network	Location
Subnet11	VNet1	West US
Subnet12	VNet1	West US
Subnet21	VNet2	West US

The subscription contains Azure web app named WebApp1 that has the following configurations.
* Region West Us
* Virtual network VNet1
* VNet integration on: Enabled
* Outbound subnet: Subnet11
* Windows plan (West US): ASP1
You plan to deploy an Azure web app named WebApp2 that will have the following settings:
* Region: West US
* VNet integration on-Enabled
* Windows plan (West UAS): WebApp2?
To which subnets can you integrate WebApp2?

A. Subnet11 only
B. Subnet2 only
C. Subnet11 or subnet12 only
D. Subnet2 or Subnet21 only
E. Subnet11, subnet2, or Subnet21

Answer: C

NEW QUESTION 75
- (Exam Topic 4)
HOTSPOT

You suspect that users are attempting to sign in to resources to which they have no access.

You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.

How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AcccountType == 'User' and [▼] ==4625
        ActivityID
        DataType
        EventID
        QuantityUnit

| Summarie failed_login_attempts= [▼]
        Count(),
        Countif(),
        Makeset(),
        Split(),

        latest_failed_login=arg_max(TimeGenerated by Account
| where failed login attempts > 5
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The following example identifies user accounts that failed to log in more than five times in the last day, and when they last attempted to log in.
let timeframe = 1d; SecurityEvent
| where TimeGenerated > ago(1d)
| where AccountType == 'User' and EventID == 4625 // 4625 - failed log in
| summarize failed_login_attempts=count(), latest_failed_login=arg_max(TimeGenerated, Account) by Account
| where failed_login_attempts > 5
| project-away Account1 References:
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples

NEW QUESTION 76
- (Exam Topic 4)
You have an Azure subscription named Sub1. Sub1 has an Azure Storage account named Storage1 that contains the resources shown in the following table.

Name	Type
Container1	Blob container
Share1	File share

You generate a shared access signature (SAS) to connect to the blob service and the file service.

Which tool can you use to access the contents in Container1 and Share! by using the SAS? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Tools for Container1:
```
Robocopy.exe
Azure Storage Explorer
File Explorer
```

Tools for Share1:
```
Robocopy.exe
Azure Storage Explorer
File Explorer
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Tools for Container1: | Robocopy.exe |
Azure Storage Explorer |
File Explorer |

Tools for Share1: | Robocopy.exe |
Azure Storage Explorer |
File Explorer |

NEW QUESTION 81
- (Exam Topic 4)
You have a web app hosted on an on-premises server that is accessed by using a URL of https://www.contoso.com. You plan to migrate the web app to Azure. You will continue to use https://www.contoso.com. You need to enable HTTPS for the Azure web app. What should you do first?

A. Export the public key from the on-premises server and save the key as a P7b file.
B. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using TripleDES.
C. Export the public key from the on-premises server and save the key as a CER file.
D. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using AES256.

Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate#private-certificate-requirements

NEW QUESTION 85
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault. The role assignments for the key vault are shown in the following exhibit.

```
[
    {
        "RoleAssignmentId": "3336fcbf-33d8-4c8a-85b6-d8edd964762b",
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa",
        "DisplayName": "User1",
        "SignInName": "User1@contoso.com",
        "RoleDefinitionName": "Owner",
        ...
    },
    {
        "RoleAssignmentId": "9d080a14-246e-4580-8b8b-077bfec22f7c",
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
        "DisplayName": "User2",
        "SignInName": "User2@contoso.com",
        "RoleDefinitionName": "Key Vault Crypto Officer",
        "RoleAssignmentId": "(
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
        "DisplayName": "User3",
        "SignInName": "User3@contoso.com",
        "RoleDefinitionName": "Key Vault Secrets Officer",
        ...
    },
    {
        "RoleAssignmentId": "f1e46302-c5d0-4519-9ee7-128594eea97c",
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG3/providers/Microsoft.KeyVault/vaults/KeyVault1/keys/Key1",
        "DisplayName": "User4",
        "SignInName": "User4@contoso.com",
        "RoleDefinitionName": "Key Vault Administrator",
        ...
    }
]
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Answer Area

[Answer choice] can create keys in the key vault. [▼]

[Answer choice] can create secrets in the key vault. [▼]

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

[Answer choice] can create keys in the key vault.   Only User1 and User4   ▼

[Answer choice] can create secrets in the key vault.   Only User1 and User3   ▼

NEW QUESTION 87
- (Exam Topic 4)
You plan to use Azure Resource Manager templates to perform multiple deployments of identically configured Azure virtual machines. The password for the administrator account of each deployment is stored as a secret in different Azure key vaults.
You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment. The name of the key vault and the name of the secret will be provided as inline parameters.
What should you use to construct the resource ID?

A. a key vault access policy
B. a linked template
C. a parameters file
D. an automation account

Answer: C

Explanation:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli#r

NEW QUESTION 91
- (Exam Topic 4)
You have an Azure subscription that contains a storage account named storage1 and a virtual machine named VM1.
VM1 is connected to a virtual network named VNet1 that contains one subnet and uses Azure DNS.
You need to ensure that VM1 connects to storage1 by using a private IP address. The solution must minimize administrative effort.
What should you do?

A. For storage1, disable public network access.
B. Create an Azure Private DNS zone.
C. On VNet1. create a new subnet.
D. For storage1, create a new private endpoint.

Answer: D

NEW QUESTION 95
- (Exam Topic 4)
You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant. From the Azure portal, you register an enterprise application.
Which additional resource will be created in Azure AD?

A. a service principal
B. an X.509 certificate
C. a managed identity
D. a user account

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

NEW QUESTION 98
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com
You need to configure diagnostic settings for contoso.com. The solution must meet the following requirements:
• Retain loqs for two years.
• Query logs by using the Kusto query language
• Minimize administrative effort. Where should you store the logs?

A. an Azure Log Analytics workspace
B. an Azure event hub
C. an Azure Storage account

Answer: A

Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-queries

NEW QUESTION 101
- (Exam Topic 4)
You have an Azure subscription that contains an Azure Sentinel workspace.
Azure Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents.
You need to identify which Azure Sentinel components to configure to meet the following requirements:

≫ When Azure Sentinel identifies a threat, an incident must be created.

≫ A ticket must be logged in the service management platform when an incident is created in Azure Sentinel.

Which component should you identify for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

When Azure Sentinel identifies a threat, an incident must be created:	▼
	Analytics
	Data connectors
	Playbooks
	Workbooks

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:	▼
	Analytics
	Data connectors
	Playbooks
	Workbooks

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

NEW QUESTION 103
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create an initiative and an assignment that is scoped to the Tenant Root Group management group.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/overview
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-group

NEW QUESTION 108
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.
You need to ensure that User1 can create and manage administrative units. The solution must use the principle of least privilege.
Which role should you assign to User1?

A. Privileged role administrator
B. Helpdesk administrator
C. Global administrator
D. Security administrator

Answer: A

NEW QUESTION 109
- (Exam Topic 4)
You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant.
When a developer attempts to register an app named App1 in the tenant, the developer receives the error message shown in the following exhibit.

You do not have access

Access denied

You do not have access

You don't have permission to register applications in the sk200510outlook (Default Directory) directory. To request access, contact your administrator.

Summary

Session ID
f8e55e67d10141b4bf0c7ac5115b3be7

Resource ID
Not available

Extension
Microsoft_AAD_RegisteredApps

Content
CreateApplicationBlade

Error code
403

You need to ensure that the developer can register App1 in the tenant. What should you do for the tenant?

A. Modify the User settings
B. Set Enable Security default to Yes.
C. Modify the Directory properties.
D. Configure the Consent and permissions settings for enterprise applications.

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

NEW QUESTION 113
- (Exam Topic 4)
You have a management group named Group1 that contains an Azure subscription named sub1. Sub1 has a subscription ID of 11111111-1234-1234-1234-1111111111.
You need to create a custom Azure role-based access control (RBAC) role that will delegate permissions to manage the tags on all the objects in Group1.
What should you include in the role definition of Role1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Resource provider:

Microsoft.Authorization
Microsoft.Resources
Microsoft.Support

Assignable scope:

/
/Group1
/subscriptions/11111111-1234-1234-1234-1111111111

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text, application Description automatically generated
Note: Assigning a custom RBAC role as the Management Group level is currently in preview only. So, for now the answer to the assignable scope is the subscription level.
Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#step-5-assignable-scopes

NEW QUESTION 114
- (Exam Topic 4)
Lab Task
use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password. place your cursor in the Enter password box and click on the password below. Azure Username: Userl -28681041@ExamUsers.com
Azure Password: GpOAe4@IDg
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only: Lab Instance: 28681041
Task 3
The developers at your company plan to create a web app named App28681041 and to publish the app to https://www.contoso.com. You need to perform the following tasks:
• Ensure that App28681041 is registered to Azure AD.
• Generate a password for App28681041.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To register App28681041 to Azure AD and generate a password for it, you can follow these steps:
- In the Azure portal, search for and select Azure Active Directory.
- In the left pane, select App registrations.
- Select New registration.
- In the Register an application pane, enter the following information:
- Name: App28681041
- Supported account types: Select the appropriate account types for your scenario.
- Redirect URI: Leave this field blank.
- Select Register.
- In the App registrations pane, select the newly created App28681041 application.
- In the left pane, select Certificates & secrets.
- Select New client secret.
- In the Add a client secret pane, enter the following information:
- Description: Enter a description for the client secret.
- Expires: Select an appropriate expiration date for the client secret.
- Select Add.
- In the Certificates & secrets pane, copy the value of the newly created client secret.
You can find more information on this topic in the following Microsoft documentation: Quickstart: Register an application with the Microsoft identity platform.

NEW QUESTION 119
- (Exam Topic 4)
You have an Azure subscription named Sub1 that contains the resource groups shown in the following table.

Name	Location
RG1	West US
RG2	East US

You create the Azure Policy definition shown in the following exhibit.

```
{
  "mode": "All",
  "policyRule": {
    "if": {
      "anyOf": [
        {
          "field": "location",
          "notEquals": "[resourceGroup().location]"
        },
        {
          "field": "name",
          "notContains": "obj"
        }
      ]
    },
    "then": {
      "effect": "deny"
    }
  },
  "parameters": {}
}
```

You assign the policy to Sub1.
You plan to create the resources shown in the following table.

Name	Type	Location	Resource group
IPobject1	Public IP address	East US	RG2
obj1	Resource group	West US	Not applicable
OBJ3	Virtual network	West US	RG1

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can create IPobject1.	○	○
You can create obj1.	○	○
You can create OBJ3.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
You can create IPobject1.	○	○
You can create obj1.	○	○
You can create OBJ3.	○	○

NEW QUESTION 121
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault and an Azure Storage account. The key vault contains customer-managed keys. The storage account is configured to use the customer-managed keys stored In the key vault.
You plan to store data in Azure by using the following services:
* Azure Files
* Azure Blob storage
* Azure Log Analytics
* Azure Table storage
* Azure Queue storage
Which two services data encryption by using the keys stored in the key vault? Each correct answer present a complete solution.
NOTE: Each correct selection is worth one point.

A. Queue storage
B. Table storage
C. Azure Files
D. Blob storage

Answer: AC

Explanation:
https://docs.microsoft.com/en-us/azure/storage/common/account-encryption-key-create?tabs=portal

NEW QUESTION 125
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a policy initiative and assignments that are scoped to resource groups. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead use a management group.
Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously.
Reference:
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-managementgroups

NEW QUESTION 127
- (Exam Topic 4)
You have an Azure subscription that contains a virtual machine named VM1. You create an Azure key vault that has the following configurations:

> Name: Vault5

> Region: West US

> Resource group: RG1

You need to use Vault5 to enable Azure Disk Encryption on VM1. The solution must support backing up VM1 by using Azure Backup.
Which key vault settings should you configure?

A. Access policies
B. Secrets
C. Keys
D. Locks

Answer: A

Explanation:
 References:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

NEW QUESTION 128
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to rt As a result, these questions will not appear in the review screen.
You have an Azure subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sal by using several shared access signatures {SASs) and stored access policies.
You discover that unauthorized users accessed both the rile service and the blob service. You need to revoke all access to Sa1.
Solution: You regenerate the access keys. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately effects all of the shared access signatures associated with it.
References:
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

NEW QUESTION 132
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
RG1	Resource group	Used to store virtual machines
RG2	Resource group	Used to store virtual networks
ServerAdmins	Security group	Used to manage virtual machines

You need to ensure that ServerAdmins can perform the following tasks: Create virtual machine to the existing virtual network in RG2 only.
The solution must use the principle of least privilege.
Which two role-based access control (RBAC) roles should you assign to ServerAdmins? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. the Contributor role for the subscription
B. the Network Contributor role for RG2
C. A custom RBAC role for the subscription
D. a custom RBAC role for RG2
E. the Network Contributor role for RG1.
F. the Virtual Machine Contributor role for RG1.

Answer: DF

NEW QUESTION 135
- (Exam Topic 4)
You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1. You have 100 on-premises servers that run Windows Server 2012 R2 and Windows Server 2016. The servers
connect to LAW1. LAW1 is configured to collect security-related performance counters from the connected servers.
You need to configure alerts based on the data collected by LAW1. The solution must meet the following requirements:

> Alert rules must support dimensions.

> The time it takes to generate an alert must be minimized.

> resolved.

Which signal type should you use when you create the alert rules?

A. Log
B. Log (Saved Query)
C. Metric
D. Activity Log

Answer: C

Explanation:
Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold. Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics.
Note: Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric

NEW QUESTION 138
- (Exam Topic 4)
You are implementing conditional access policies.
You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.
You need to identify the risk level of the following risk events:

> Users with leaked credentials

> Impossible travel to atypical locations

> Sign ins from IP addresses with suspicious activity

Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level 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.

Levels	Answer Area
High	Impossible travel to atypical locations: [ ]
Low	Users with leaked credentials: [ ]
Medium	Sign ins from IP addresses with suspicious activity: [ ]

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Medium High Medium Refer
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events#sign-ins-from-ip

NEW QUESTION 142
- (Exam Topic 4)
You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry. You need to use automatically generated service principal for the AKS cluster to authenticate to the Azure
Container Registry.
What should you create?

A. a secret in Azure Key Vault
B. a role assignment
C. an Azure Active Directory (Azure AD) user
D. an Azure Active Directory (Azure AD) group

Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal

NEW QUESTION 144
- (Exam Topic 4)
You have an Azure subscription mat contains a resource group named RG1. RG1 contains a storage account named storage1.

You have two custom Azure rotes named Role1 and Role2 that are scoped to RG1. The permissions for Role1 are shown in the following JSON code.

```
"permissions": [
        {
            "actions": [
                "Microsoft.Storage/storageAccounts/listKevs/action".

            ],
            "notActions": [],
            "dataActions": [],
            "notDataActions": []
        }
    ]
```

The permissions for Role2 are shown in the following JSON code.

```
"permissions": [
        {
            "actions": [
                "Microsoft.Storage/storageAccounts/listKeys/action",
              "Microsoft.Storage/storageAccounts/ListAccountSas/action",
                "Microsoft.Storage/storageAccounts/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
    }
```

Answer Area

Statements	Yes	No
User1 can read data in storage1.	○	○
User2 can read data in storage1.	○	○
User3 can restore storage1 from a backup in Azure Backup.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can read data in storage1.	⌐○¬	○
User2 can read data in storage1.	⌐○¬	○
User3 can restore storage1 from a backup in Azure Backup.	○	⌐○¬

NEW QUESTION 149
- (Exam Topic 4)
You plan to create an Azure Kubernetes Service (AKS) cluster in an Azure subscription. The manifest of the registered server application is shown in the following exhibit.

Save Discard Upload Download

The editor below allows you to update this application by directly modifying its JSON representation. For more details, see: Understanding the Azure Active Directory application manifest.

```
1  {
2      "id": "d6b00db3-7ef4-4f3c-b1e7-8346f0a59546",
3      "acceptMappedClaims": null,
4      "accessTokenAcceptedVersion": null,
5      "addIns": [],
6      "allowPublicClient": null,
7      "appId": "88137405-6a75-4c20-903a-f7b18ff7d496",
8      "appRoles": [],
9      "oauth2AllowUrlPathMatching": false,
10     "createdDateTime": "2019-07-15T21:09:20Z",
11     "groupMembershipClaims": null,
12     "identifierUris": [],
13     "informationalUrls": {
14         "termsOfService": null,
15         "support": null,
16         "privacy": null,
17         "marketing": null
18     },
19     "keyCredentials": [],
20     "knownClientApplications": [],
21     "logoUrl": null,
22     "logoutUrl": null,
23     "name": "AKSAzureADServer",
24     "oauth2AllowIdTokenImplicitFlow": false,
25     "oauth2AllowImplicitFlow": false,
26     "oauth2Permissions": [],
27     "oauth2RequirePostResponse": false,
28     "optionalClaims": null,
29     "orgRestrictions": [],
30     "parentalControlSettings": {
```

You need to ensure that the AKS cluster and Azure Active Directory (Azure AD) are integrated. Which property should you modify in the manifest?

A. accessTokenAcceptedVersion
B. keyCredentials
C. groupMembershipClaims
D. acceptMappedClaims

Answer: C

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli https://www.codeproject.com/Articles/3211864/Operation-and-Maintenance-of-AKS-Applications

NEW QUESTION 153
- (Exam Topic 4)
You have 10 virtual machines on a single subnet that has a single network security group (NSG). You need to log the network traffic to an Azure Storage account. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Install the Network Performance Monitor solution.
B. Enable Azure Network Watcher.
C. Enable diagnostic logging for the NSG.
D. Enable NSG flow logs.
E. Create an Azure Log Analytics workspace.

Answer: D

Explanation:
A network security group (NSG) enables you to filter inbound traffic to, and outbound traffic from, a virtual machine (VM). You can log network traffic that flows through an NSG with Network Watcher's NSG flow log capability. Steps include:
≫ Create a VM with a network security group
≫ Enable Network Watcher and register the Microsoft.Insights provider
≫ Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability
≫ Download logged data
≫ View logged data Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal

NEW QUESTION 154
- (Exam Topic 4)

You have an Azure key vault named KeyVault1 that contains the items shown in the following table.

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In KeyVault, the following events occur in sequence:

➤ Item1 is deleted

➤ Administrator enables soft delete

➤ Item2 and Policy1 are deleted.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
You can recover Policy1.	○	○
You can add a new key named Item1.	○	○
You can add a new secret named Item2.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
NO. Policies cannot be recovered YES, Item1 is permanently deleted
NO, You cannot use the same name cause Item2 is in Seoft-deleted status https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview

NEW QUESTION 156
- (Exam Topic 4)
You have an Azure AD tenant that contains the users shown in the following table.

Name	User device
User1	Android mobile device with facial recognition
User2	Windows device with Windows Hello for Business-compatible hardware

You enable passwordless authentication for the tenant.

Which authentication method can each user use for passwordless authentication? To answer, drag the appropriate authentication methods to the correct users. Each authentication method 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.

Authentication methods

- FIDO2 security key only
- Microsoft Authenticator app only
- Windows Hello for Business only
- Microsoft Authenticator app and Windows Hello for Business only
- Windows Hello for Business and FIDO2 security key only
- Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key

Answer Area

User1: [Authentication method]

User2: [Authentication method]

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Authentication methods		Answer Area

Authentication methods

FIDO2 security key only
Microsoft Authenticator app only
Windows Hello for Business only
Microsoft Authenticator app and Windows Hello for Business only
Windows Hello for Business and FIDO2 security key only
Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key

Answer Area

User1: Microsoft Authenticator app only

User2: Windows Hello for Business only

NEW QUESTION 160
- (Exam Topic 4)
You have an Azure subscription named Subscription1 that contains a resource group named RG1 and the users shown in the following table.

Name	User principal name (UPN)	Type
User1	User1@outlook.com	Guest
User2	User2@outlook.com	Guest

You perform the following tasks:

➤ Assign User1 the Network Contributor role for Subscription1.

➤ Assign User2 the Contributor role for RG1.

To Subscription1 and RG1, you assign the following policy definition: External accounts with write permissions should be removed from your subscription.
What is the Compliance State of the policy assignments?

A. The Compliance State of both policy assignments is Non-compliant.
B. The Compliance State of the policy assignment to Subscription1 is Compliant, and the Compliance State of the policy assignment to RG1 is Non-compliant.
C. The Compliance State of the policy assignment to Subscription1 is Non-compliant, and the Compliance State of the policy assignment to RG1 is Compliant.
D. The Compliance State of both policy assignments is Compliant.

Answer: A

NEW QUESTION 164
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Resource group	Location
RG1	Resource group	Not applicable	West US
Managed1	Managed identity	RG1	West US

The subscription is linked to an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Usage location
User1	United States
User2	Germany

You create the groups shown in the following table.

Name	Type	Membership type
Group1	Security	Dynamic User
Group2	Microsoft 365	Dynamic User

The membership rules for Group1 and Group2 are configured as shown in the following exhibit.

Dynamic membership rules ··· ✕

💾 Save   ✕ Discard   ♡ Got feedback?

Configure Rules   Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. ⓘ Learn more

And/Or	Property	Operator	Value	🗑
	accountEnabled	Equals	true	
Or ⌄	usageLocation ⌄	Equals ⌄	US ⌄	🗑

╋ Add expression ╋ Get custom extension properties ⓘ

Rule syntax   ✎ Edit

(user.accountEnabled -eq true) or (user.usageLocation - eq "US")

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 is a member of Group1 and Group2.	○	○
User2 is a member of Group2 only.	○	○
Managed1 is a member of Group1 and Group2.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership

NEW QUESTION 165
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Region	Resource group
SQL1	Azure SQL database	East US	RG1
Analytics1	Azure Log Analytics workspace	East US	RG1
Analytics2	Azure Log Analytics workspace	East US	RG2
Analytics3	Azure Log Analytics workspace	West Europe	RG1

You create the Azure Storage accounts shown in the following table.

Name	Region	Resource group	Storage account type	Access tier (default)
Storage1	East US	RG1	Blob	Cool
Storage2	East US	RG2	General purpose V1	Not applicable
Storage3	West Europe	RG1	General purpose V2	Hot

You need to configure auditing for SQL1.
Which storage accounts and Log Analytics workspaces can you use as the audit log destination? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Storage accounts that can be used as the audit log destination:	Storage1 only
	Storage2 only
	Storage1 and Storage2 only
	Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:	Analytics1 only
	Analytics1 and Analytics2 only
	Analytics1 and Analytics3 only
	Analytics1, Analytics2, and Analytics3

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Storage accounts that can be used as the audit log destination:	Storage1 only
	Storage2 only
	Storage1 and Storage2 only
	Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:	Analytics1 only
	Analytics1 and Analytics2 only
	Analytics1 and Analytics3 only
	Analytics1, Analytics2, and Analytics3

NEW QUESTION 169
- (Exam Topic 4)
You have an Azure subscription that contains an Azure web app named 1 and a virtual machine named VM1. VM1 runs Microsoft SQL Server and is connected to a virtual network named VNet1. App1, VM1, and Vent are in the US Central Azure region.
You need to ensure that App1 can connect to VM1. The solution must minimize costs.

A. NAT gateway integration
B. Azure Front Door
C. regional virtual network integration
D. gateway-required virtual network integration
E. Azure Application Gateway integration

Answer: C

NEW QUESTION 171
- (Exam Topic 4)
You have an Azure subscription that contains the users shown in the following table.

Name	Subscription role	Azure Active Directory (Azure AD) user role	Multi-factor authentication (MFA) status
User1	Owner	Authentication administrator	Enabled
User2	None	Global administrator	Enforced
User3	None	Global administrator	Disabled

Which users can enable Azure AD Privileged Identity Management (PIM)?

A. User2 and User3 only
B. User1 and User2 only
C. User2 only
D. User1 only

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

NEW QUESTION 173
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault named KeyVault1 and the virtual machines shown in the following table.

Name	Private IP address	Public IP address	Connected to
VM1	10.7.0.4	51.144.245.152	VNET1/Default
VM2	10.8.0.4	104.45.9.227	VNET2/Default

You set the Key Vault access policy to Enable access to Azure Disk Encryption for volume encryption. KeyVault1 is configured as shown in the following exhibit.

Save   **Discard**

Allow access from: All networks   ● Selected networks

ⓘ Configure network access control for your key vault. Learn More

Virtual networks: ⓘ   + Add existing virtual networks   + Add new virtual network

VIRTUAL NETWORK	SUBNET	RESOURCE GROUP	SUBSCRIPTION
VNET1	default	RG1	...

Firewall: ⓘ

IPv4 ADDRESS OR CIDR

IPv4 address or CIDR   ...

Exception:

Allow trusted Microsoft services to bypass   ● Yes   ◯ No
this firewall? ⓘ

ⓘ This setting is related to firewall only. In order to access this key vault, the trusted
service must also be given explicit permissions in the Access policies section.

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
From VM1, users can manage the keys and secrets stored in KeyVault1.	◯	◯
From VM2, users can manage the keys and secrets stored in KeyVault1.	◯	◯
VM2 can use KeyVault for Azure Disk Encryption	◯	◯

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
From VM1, users can manage the keys and secrets stored in KeyVault1.	[◯]	◯
From VM2, users can manage the keys and secrets stored in KeyVault1.	[◯]	◯
VM2 can use KeyVault for Azure Disk Encryption	[◯]	◯

NEW QUESTION 178

- (Exam Topic 4)

You have a Microsoft Sentinel deployment.

You need to connect a third-party security solution to the deployment. The third-party solution will send Common Event Format (CER-formatted messages.

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.

Answer Area

Deploy:	▼
Forward events to Microsoft Sentinel by using:	▼

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Deploy:	A Windows server and a Windows Event Forwarding subscription ▼
Forward events to Microsoft Sentinel by using:	An Azure Log Analytics agent ▼

NEW QUESTION 183
- (Exam Topic 4)

You have an Azure subscription named Sub1.

In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.

You need to modify Play1 to send email messages to a distribution group named Alerts. What should you use to modify Play1?

A. Azure DevOps
B. Azure Application Insights
C. Azure Monitor
D. Azure Logic Apps Designer

Answer: D

Explanation:

You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.

References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks

NEW QUESTION 185
- (Exam Topic 4)

You have the Azure key vaults shown in the following table.

Name	Location	Azure subscription name
KV1	West US	Subscription1
KV2	West US	Subscription1
KV3	East US	Subscription1
KV4	West US	Subscription2
KV5	East US	Subscription2

KV1 stores a secret named Secret1 and a key for a managed storage account named Key1. You back up Secret1 and Key1.

To which key vaults can you restore each backup? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

You can restore the Secret1 backup to:	▼
	KV1 only
	KV1 and KV2 only
	KV1, KV2 and KV3 only
	KV1, KV2 and KV4 only
	KV1, KV2, KV3, KV4, and KV5

You can restore the Key1 backup to:	▼
	KV1 only
	KV1 and KV2 only
	KV1, KV2 and KV3 only
	KV1, KV2 and KV4 only
	KV1, KV2, KV3, KV4, and KV5

A. Mastered

B. Not Mastered

Answer: A

Explanation:
The backups can only be restored to key vaults in the same subscription and same geography. You can restore to a different region in the same geography.
https://docs.microsoft.com/en-us/azure/key-vault/general/backup?tabs=azure-cli

NEW QUESTION 190
- (Exam Topic 4)
Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.
You need to configure each subscription to have the same role assignments. What should you use?

A. Azure Security Center
B. Azure Policy
C. Azure AD Privileged Identity Management (PIM)
D. Azure Blueprints

Answer: D

Explanation:
Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of
Azure resources that implements and adheres to an organization's standards, patterns, and requirements.
Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:
➢ Role Assignments
➢ Policy Assignments
➢ Azure Resource Manager templates
➢ Resource Groups
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

NEW QUESTION 195
- (Exam Topic 4)
You have an Azure Subscription that is linked to an Azure Active Directory (Azure AD). The tenant contains the users shown in the following table.

Name	Role	Member of
User1	Security administrator	Group1
User2	Network Contributor	Group2
User3	Key Vault Contributor	Group1, Group2

You have an Azure key vault named Vault1 that has Purge protection set to Disabled. Vault1 contains the access policies shown in the following table.

Name	Key permission	Secret permission	Certificate permission
Group1	Purge	Purge	Purge
Group2	Select all	Select all	Select all

You create role assignments for Vault1 as shown in the following table.

Name	Role
User1	None
User2	Key Vault Reader
User3	User Access Administrator

For each of the following statements, Yes if the statement is true, Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	○	○
User2 can configure firewalls and virtual networks for Vault1.	○	○
User3 can add access policies to Vault1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	☑	○
User2 can configure firewalls and virtual networks for Vault1.	○	☑
User3 can add access policies to Vault1.	○	☑

NEW QUESTION 197
- (Exam Topic 4)
Lab Task
Task 2
You need to ensure that the events in the NetworkSecurityGroupRuleCounter log of the
VNETOI-Subnet0-NSG network security group (NSG) are stored in the logs31330471 Azure Storage account for 30 days.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Enable diagnostic resource logging for the NSG. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select the Rule counter category under Logs and choose
the logs31330471 storage account as the destination.
Configure the retention policy for the storage account to keep the logs for 30 days. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this.
You need to specify the days parameter as 30 for the Set-AzStorageServiceProperty cmdlet or the az storage logging update command.
View and analyze the logs in the storage account. You can use any tool that can read JSON files, such as Azure Storage Explorer or Visual Studio Code. You can also export the logs to any visualization tool, SIEM solution, or IDS of your choice

NEW QUESTION 199
- (Exam Topic 4)
You have an Azure subscription that contains an Azure SQL database named SQL1. You plan to deploy a web app named App1.
You need to provide App1 with read and write access to SQL1. The solution must meet the following requirements:

⟩ Provide App1 with access to SQL1 without storing a password.

⟩ Use the principle of least privilege.

⟩ Minimize administrative effort.

Which type of account should App1 use to access SQL1, and which database roles should you assign to App1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Account type:
| Azure Active Directory User |
| Managed identity |
| Service Principal |

Roles:
| db_datawriter only |
| db_datareader and db_datawriter |
| db owner only |

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/app-service/tutorial-connect-msi-sql-database?tabs=windowsclient%2Cd

NEW QUESTION 203
- (Exam Topic 4)
You create a new Azure subscription.
You need to ensure that you can create custom alert rules in Azure Security Center. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Onboard Azure Active Directory (Azure AD) Identity Protection.
B. Create an Azure Storage account.
C. Implement Azure Advisor recommendations.
D. Create an Azure Log Analytics workspace.
E. Upgrade the pricing tier of Security Center to Standard.

Answer: DE

Explanation:
D: You need write permission in the workspace that you select to store your custom alert. References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-custom-alert

NEW QUESTION 204
- (Exam Topic 4)
You have an Azure subscription named Sub1 that uses Microsoft Defender for Cloud. You have the management group hierarchy shown in the following exhibit.
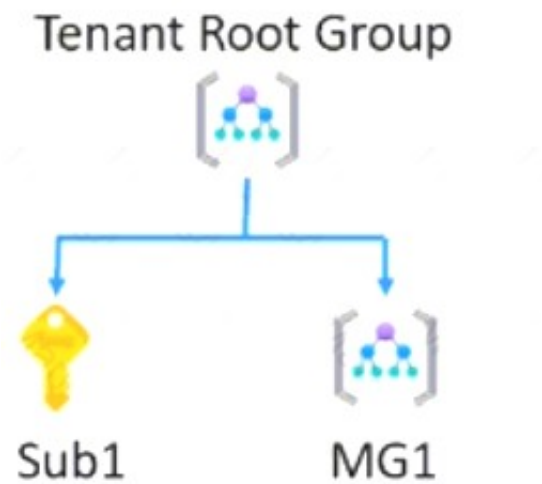
You create the definitions shown in the following table.

Name	Location	Type
Policy1	Sub1	Policy
Initiative1	Tenant Root Group	Initiative
Initiative2	Sub1	Initiative
Initiative3	MG1	Initiative

You need to use Defender for Cloud to add a security policy. Which definitions can you use as a security policy?

A. Policy1 only
B. Policy1 and Initiative1 only
C. Initiative1 and Initiative2 only
D. Initiative1, Initiative2, and Initiatives only
E. Policy1, Initiative1, Initiative2, and Initiative3

Answer: B

NEW QUESTION 209
- (Exam Topic 3)
From Azure Security Center, you need to deploy SecPol1. What should you do first?

A. Enable Azure Defender.
B. Create an Azure Management group.
C. Create an initiative.
D. Configure continuous export.

Answer: C

Explanation:
Reference:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/security-center/custom-security-policies.md https://zimmergren.net/create-custom-security-center-recommendation-with-azure-policy/

NEW QUESTION 212
- (Exam Topic 2)
You need to meet the technical requirements for VNetwork1. What should you do first?

A. Create a new subnet on VNetwork1.
B. Remove the NSGs from Subnet11 and Subnet13.
C. Associate an NSG to Subnet12.
D. Configure DDoS protection for VNetwork1.

Answer: A

Explanation:
From scenario: Deploy Azure Firewall to VNetwork1 in Sub2.
Azure firewall needs a dedicated subnet named AzureFirewallSubnet. References:

https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal

NEW QUESTION 217

......

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

az-500 Practice Exam Features:

* az-500 Questions and Answers Updated Frequently

* az-500 Practice Questions Verified by Expert Senior Certified Staff

* az-500 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* az-500 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The az-500 Practice Test Here