

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 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 3

- (Exam Topic 4)

You have an Azure web app named WebApp1. You upload a certificate to WebApp1.

You need to make the certificate accessible to the app code of WebApp1. What should you do?

- A. Add a user-assigned managed identity to WebApp1.
- B. Add an app setting to the WebApp1 configuration.
- C. Enable system-assigned managed identity for the WebApp1.
- D. Configure the TLS/SSL binding for WebApp1.

Answer: B

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate-in-code>

NEW QUESTION 4

- (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.	<input type="radio"/>	<input type="radio"/>
From VM1, you can upload data to the blob storage of storage1.	<input type="radio"/>	<input type="radio"/>
From VM2, you can upload data to the blob storage of storage1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1.	<input type="radio"/>	<input checked="" type="radio"/>
From VM1, you can upload data to the blob storage of storage1.	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, you can upload data to the blob storage of storage1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 5

- (Exam Topic 4)

You have an Azure subscription that contains the resources shown in the following table.

Name	Type
User1	Azure Active Directory (Azure AD) user
User2	Azure Active Directory (Azure AD) user
Group1	Azure Active Directory (Azure AD) group
Vault1	Azure key vault

User1 is a member of Group1. Group1 and User2 are assigned the Key Vault Contributor role for Vault1.

On January 1, 2019, you create a secret in Vault1. The secret is configured as shown in the exhibit. (Click the Exhibit tab.)

Create a secret

Upload options

Manual

* Name ⓘ

Password1

* Value

••••••••••

Content type (optional)

Set activation date? ⓘ

Activation Date

2019-03-01 12:00:00 AM

(UTC+02:00) -- Current Time Zone --

Set expiration Date? ⓘ

Expiration Date

2020-03-01 12:00:00 AM

(UTC+02:00) -- Current Time Zone --

Enabled?

Yes No

User2 is assigned an access policy to Vault1. The policy has the following configurations:

- > Key Management Operations: Get, List, and Restore
- > Cryptographic Operations: Decrypt and Unwrap Key
- > Secret Management Operations: Get, List, and Restore

Group1 is assigned an access to Vault1. The policy has the following configurations:

- > Key Management Operations: Get and Recover
- > Secret Management Operations: List, Backup, and Recover

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

Statements	Yes	No
On January 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input type="radio"/>
On June 1, 2019, User2 can view the value of Password1.	<input type="radio"/>	<input type="radio"/>
On June 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
On January 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input checked="" type="radio"/>
On June 1, 2019, User2 can view the value of Password1.	<input checked="" type="radio"/>	<input type="radio"/>
On June 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 6

- (Exam Topic 4)

You have an Azure subscription that contains four Azure SQL managed instances.

You need to evaluate the vulnerability of the managed instances to SQL injection attacks. What should you do first?

- A. Create an Azure Sentinel workspace.
- B. Enable Advanced Data Security.
- C. Add the SQL Health Check solution to Azure Monitor.
- D. Create an Azure Advanced Threat Protection (ATP) instance.

Answer: B

NEW QUESTION 7

- (Exam Topic 4)

You have an Azure environment.

You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001 standards. What should you use?

- A. Azure Sentinel
- B. Azure Active Directory (Azure AD) Identity Protection
- C. Azure Security Center
- D. Azure Advanced Threat Protection (ATP)

Answer: C

Explanation:

Reference:

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

NEW QUESTION 8

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1. You plan to publish several apps in the tenant.

You need to ensure that User1 can grant admin consent for the published apps.

Which two possible user roles can you assign to User1 to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Application developer
- B. Security administrator
- C. Application administrator
- D. User administrator
- E. Cloud application administrator

Answer: CE

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent>

NEW QUESTION 9

- (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

Resource Providers

- Microsoft.Compute
- Microsoft.Network
- Microsoft.Security
- Microsoft.Solutions

Answer Area

Role1:

Role2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Resource Providers

- Microsoft.Compute
- Microsoft.Network
- Microsoft.Security
- Microsoft.Solutions

Answer Area

Role1: Microsoft.Network

Role2: Microsoft.Network

NEW QUESTION 10

- (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.

SQL1 has the following settings:

- Auditing: On
- Audit log 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. Yes No

Audit events for DB2 are written to storage1 and storage2. Yes No

Storage3 can be used as an audit log destination for DB3. Yes No

- 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 15

- (Exam Topic 4)

You have an Azure Sentinel workspace that has the following data connectors:

- > Azure Active Directory Identity Protection
- > Common Event Format (CEF)
- > Azure Firewall

You need to ensure that data is being ingested from each connector.

From the Logs query window, which table should you query for each connector? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Azure Active Directory Identity Protection:

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

Azure Firewall:

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

CEF:

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application, table Description automatically generated

NEW QUESTION 19

- (Exam Topic 4)

You plan to deploy Azure container instances.

You have a containerized application that validates credit cards. The application is comprised of two containers: an application container and a validation container.

The application container is monitored by the validation container. The validation container performs security checks by making requests to the application container and waiting for responses after every transaction.

You need to ensure that the application container and the validation container are scheduled to be deployed together. The containers must communicate to each other only on ports that are not externally exposed.

What should you include in the deployment?

- A. application security groups
- B. network security groups (NSGs)
- C. management groups
- D. container groups

Answer: D

Explanation:

Azure Container Instances supports the deployment of multiple containers onto a single host using a container group. A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process.

Reference:

<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups>

NEW QUESTION 22

- (Exam Topic 4)

You have an Azure subscription.

You plan to create a custom role-based access control (RBAC) role that will provide permission to read the Azure Storage account.

Which property of the RBAC role definition should you configure?

- A. NotActions []
- B. DataActions []
- C. AssignableScopes []
- D. Actions []

Answer: D

Explanation:

To 'Read a storage account', ie. list the blobs in the storage account, you need an 'Action' permission. To read the data in a storage account, ie. open a blob,

you need a 'DataAction' permission.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions>

NEW QUESTION 26

- (Exam Topic 4)

From the Azure portal, you are configuring an Azure policy.

You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects.

Which effect requires a managed identity for the assignment?

- A. AuditIfNotExist
- B. Append
- C. DeployIfNotExist
- D. Deny

Answer: C

Explanation:

When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.

References:

<https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources>

NEW QUESTION 28

- (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 32

- (Exam Topic 4)

You have 15 Azure virtual machines in a resource group named RG1. All virtual machines run identical applications.

You need to prevent unauthorized applications and malware from running on the virtual machines. What should you do?

- A. Configure Azure Active Directory (Azure AD) Identity Protection.
- B. From Microsoft Defender for Cloud, configure adaptive application controls.
- C. Apply an Azure policy to RGI.
- D. Apply a resource lock to RGI.

Answer: B

Explanation:

Microsoft Defender for Cloud helps you prevent, detect, and respond to threats. Defender for Cloud gives you increased visibility into, and control over, the security of your Azure resources. It provides integrated security monitoring and policy management across your Azure subscriptions. It helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions.

Defender for Cloud helps you optimize and monitor the security of your virtual machines by:

- > Providing security recommendations for the virtual machines. Example recommendations include: app system updates, configure ACLs endpoints, enable antimalware, enable network security groups, and apply disk encryption.
- > Monitoring the state of your virtual machines.

<https://learn.microsoft.com/en-us/azure/security/fundamentals/virtual-machines-overview>

NEW QUESTION 35

- (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.	<input type="radio"/>	<input type="radio"/>
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	<input type="radio"/>	<input type="radio"/>
User3 can activate the Security Administrator role.	<input type="radio"/>	<input type="radio"/>

- 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>

- (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 50

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant and a root management group. You create 10 Azure subscriptions and add the subscriptions to the root management group.

You need to create an Azure Blueprints definition that will be stored in the root management group. What should you do first?

- A. Add an Azure Policy definition to the root management group.
- B. Modify the role-based access control (RBAC) role assignments for the root management group.
- C. Create a user-assigned identity.
- D. Create a service principal.

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin>

NEW QUESTION 52

- (Exam Topic 4)

Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant. You need to recommend an integration solution that meets the following requirements:

Ensures that password policies and user logon restrictions apply to user accounts that are synced to the Tenant Minimizes the number of servers required for the solution.

Which authentication method should you include in the recommendation?

- A. federated identity with Active Directory Federation Services (AD FS)
- B. password hash synchronization with seamless single sign-on (SSO)
- C. pass-through authentication with seamless single sign-on (SSO)

Answer: C

Explanation:

* 1. Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant

>> Pass-Through Authentication enforce on-premises user account states, password policies, and sign-in hours.

* 2. Minimizes the number of servers required for the solution.

>> Pass-through needs a lightweight agent to be installed one (or more) on-premises servers.

>> PW Hash also require installing Azure AD Connect on your existing DC.

NEW QUESTION 53

- (Exam Topic 4)

Your on-premises network contains the servers shown in the following table.

Name	Operating system	Description
Server1	Windows Server 2019	Hyper-V host hosting four virtual machines that run Windows Server 2022
Server2	Windows Server 2019	File server that has the Azure Arc agent installed
Server3	SUSE Linux Enterprise Server (SLES)	Database server that has the Azure Arc agent installed

You have an Azure subscription That contains multiple virtual machines that run either Windows Server 2019 Of SLES.

Operating systems:

- SLES only
- Windows Server only
- SLES and Windows Server

Platforms:

- Azure virtual machines only
- Azure virtual machines and Hyper-V virtual machines only
- Azure Arc-enabled servers and Azure virtual machines only
- Azure virtual machines, Hyper-V virtual machines, and Azure Arc-enabled servers

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Operating systems:

- SLES only
- Windows Server only
- SLES and Windows Server**

Platforms:

- Azure virtual machines only
- Azure virtual machines and Hyper-V virtual machines only
- Azure Arc-enabled servers and Azure virtual machines only**
- Azure virtual machines, Hyper-V virtual machines, and Azure Arc-enabled servers

NEW QUESTION 58

- (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 an Azure Subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.

You need to deploy Microsoft Antimalware to the virtual machines. Solution: You add an extension to each virtual machine.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

You can use Visual Studio to enable and configure the Microsoft Antimalware service. This entails selecting Microsoft Antimalware extension from the dropdown list under Installed Extensions and click Add to configure with default antimalware configuration.

References:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware>

NEW QUESTION 63

- (Exam Topic 4)

You have an Azure Storage account that contains a blob container named container1 and a client application named App1.

You need to enable App1 access to container1 by using Azure Active Directory (Azure AD) authentication. What should you do? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

From Azure AD:

- Register App1.
- Create an access package.
- Implement an application proxy.
- Modify the authentication methods.

From the storage account:

- Add a private endpoint.
- Regenerate the access key.
- Configure Access control (IAM).
- Generate a shared access signature (SAS).

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://azure.microsoft.com/en-in/blog/announcing-the-preview-of-aad-authentication-for-storage/> <https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/common/storage-auth-aad-rbac-portal>

NEW QUESTION 64

- (Exam Topic 4)

You have an Azure subscription that uses Azure Active Directory (Azure AD) Privileged Identity Management (PIM). A PIM user that is assigned the User Access Administrator role reports receiving an authorization error when performing a role assignment or viewing the list of assignments. You need to resolve the issue by ensuring that the PIM service principal has the correct permissions for the subscription. The solution must use the principle of least privilege. Which role should you assign to the PIM service principle?

- A. Contributor
- B. User Access Administrator
- C. Managed Application Operator
- D. Resource Policy Contributor

Answer: B

NEW QUESTION 69

- (Exam Topic 4)

You plan to implement an Azure function named Function1 that will create new storage accounts for containerized application instances. You need to grant Function1 the minimum required privileges to create the storage accounts. The solution must minimize administrative effort. What should you do? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Assign role to:

- A group account
- A system-assigned managed identity
- A user account
- A user-assigned managed identity

Role assignment to create:

- Built-in role assignment
- Classic administrator role assignment
- Custom role-based access control (RBAC) role assignment

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview> <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/howto-assign-access>

NEW QUESTION 74

- (Exam Topic 4)

Your company has an Active Directory forest with a single domain, named weylanindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.

After syncing all on-premises identities to Azure AD, you are informed that users with a givenName attribute starting with LAB should not be allowed to sync to Azure AD.

Which of the following actions should you take?

- A. You should make use of the Synchronization Rules Editor to create an attribute-based filtering rule.
- B. You should configure a DNAT rule on the Firewall.
- C. You should configure a network traffic filtering rule on the Firewall.
- D. You should make use of Active Directory Users and Computers to create an attribute-based filtering rule.

Answer: A

Explanation:

Use the Synchronization Rules Editor and write attribute-based filtering rule. Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration>

NEW QUESTION 76

- (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 (NSG) 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 RG1
- 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 81

- (Exam Topic 4)

You have an Azure subscription that contains the following Azure firewall:

- Name: Fw1
- Azure region: UK West
- Private IP address: 10.1.3.4
- Public IP address: 23.236.62.147

The subscription contains the virtual networks shown in the following table.

Name	Location	IP address space	Peered with
Vnet1	UK West	10.1.0.0/16	Vnet2
Vnet2	East US	10.2.0.0/16	Vnet1, Vnet3
Vnet3	West US	10.3.0.0/16	Vnet2,

The subscription contains the subnets shown in the following table.

Name	Virtual network	IP address range
Subnet1-1	Vnet1	10.1.1.0/24
Subnet1-2	Vnet1	10.1.2.0/24
AzureFirewallSubnet	Vnet1	10.1.3.0/24
Subnet2-1	Vnet2	10.2.1.0/24
Subnet3-1	Vnet3	10.3.1.0/24

The subscription contains the routes shown in the following table.

Name	Subnet	IP address prefix	Next hop type	Next hop IP address
Rt1	Subnet1-1	0.0.0.0/0	Virtual appliance	10.1.3.4
Rt2	Subnet1-2	10.1.1.0/24	Virtual appliance	10.1.3.4
Rt3	Subnet2-1	10.1.1.0/24	Virtual appliance	10.1.3.4
Rt4	Subnet3-1	10.2.1.0/24	Virtual appliance	10.1.3.4

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
Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.	<input type="radio"/>	<input type="radio"/>
Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.	<input type="radio"/>	<input type="radio"/>
Traffic from Subnet3-1 to the internet is routed through Fw1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.	<input checked="" type="radio"/>	<input type="radio"/>
Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.	<input type="radio"/>	<input checked="" type="radio"/>
Traffic from Subnet3-1 to the internet is routed through Fw1.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 82

- (Exam Topic 4)

You have an Azure subscription named Sub1 that contains the resources shown in the following table.

Name	Type	Region	Resource group
Sa1	Azure Storage account	East US	RG1
VM1	Azure virtual machine	East US	RG2
KV1	Azure key vault	East US 2	RG1
SQL1	Azure SQL database	East US 2	RG2

You need to ensure that you can provide VM1 with secure access to a database on SQL1 by using a contained database user. What should you do?

- A. Enable a managed service identity on VM1.
- B. Create a secret in KV1.
- C. Configure a service endpoint on SQL1.
- D. Create a key in KV1.

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm>

NEW QUESTION 83

- (Exam Topic 4)

You are configuring just in time (JIT) VM access to a set of Azure virtual machines.

You need to grant users PowerShell access to the virtual machine by using JIT VM access. What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Permission that must be granted to users on VM:

Read
Update
View
Write

TCP port that must be allowed:

22
25
3389
5986

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- * 1. Read permission
- * 2. 5986

<https://docs.microsoft.com/en-us/azure/security-center/just-in-time-explained#what-permissions-are-needed-to-c>

NEW QUESTION 87

- (Exam Topic 4)

You have an Azure subscription that contains an Azure key vault named ContosoKey1. You create users and assign them roles as shown in the following table.

Name	Subscription role assignment	ContosoKey1 role assignment
User1	Owner	None
User2	Security Admin	None
User3	None	User Access Administrator
User4	None	Key Vault Contributor

You need to identify which users can perform the following actions:

- > Delegate permissions for ContosoKey1.
- > Configure network access to ContosoKey1.

Which users should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Delegate permissions for ContosoKey1:

▼

- User1 only
- User1 and User2 only
- User1 and User3 only
- User1 and User4 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

Configure network access to ContosoKey1:

▼

- User1 only
- User1 and User2 only
- User1 and User3 only
- User1 and User4 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-guide>

NEW QUESTION 91

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant. The tenant contains users that are assigned Azure AD Premium Plan 2 licenses.

You have an partner company that has a domain named The fabrikam.com domain contains a user named user'. User' has an email address of user1@fabrikam.com.

You to provide User1 with to the resources in the tenant The solution must meet the following requirements: > user1 must be able to sign in by using the user1@fabrikam.com credentials

- > You must be able to grant User1 access to the resources in the tenant
- > Administrative effort must be minimized.

What should you do?

- A. Create a user account for user1.
- B. Create an invite for User1.
- C. To the tenant add fabrikamcom as a custom domain
- D. Set Enable guest self-service sign up via user flows to Yes for the tenant.

Answer: B

NEW QUESTION 95

- (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: User1 -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 7

You need to collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account. To complete this task, sign in to the Azure portal.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account, you can follow these steps:

- > In the Azure portal, search for and select the virtual machine named VM1.
- > In the left pane, select Diagnostic settings.
- > Select Add diagnostic setting.
- > In the Add diagnostic setting pane, enter the following information:
- > Name: Enter a name for the diagnostic setting.
- > Destination: Select Storage account.
- > Storage account: Select the storage account you want to use.
- > Logs: Select Windows Event Logs.
- > Categories: Select Security.
- > Event types: Select Audit Failure.
- > Select Save.

NEW QUESTION 97

- (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 resource graph and an assignment that is scoped to a management group. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/governance/management-groups/create>

NEW QUESTION 100

- (Exam Topic 4)

You onboard Azure Sentinel. You connect Azure Sentinel to Azure Security Center.

You need to automate the mitigation of incidents in Azure Sentinel. The solution must minimize administrative effort.

What should you create?

- A. an alert rule
- B. a playbook
- C. a function app
- D. a runbook

Answer: B

NEW QUESTION 103

- (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.

i The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
<input type="checkbox"/> GR Group1	Group	Default Access

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

Allow users to request access to this application? Yes No

To which group should assigned users be added?

Require approval before granting access to this application? Yes No

Who is allowed to approve access to this application?

To which role should users be assigned in this application?

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 108

- (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.	<input type="radio"/>	<input type="radio"/>
You can start VM2.	<input type="radio"/>	<input type="radio"/>
You can create a virtual machine in RG2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 113

- (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 116

- (Exam Topic 4)

You have an Azure subscription that contains the resources shown in the following table.

Name	Type
SQL1	Azure SQL Database server
DB1	Azure SQL database on SQL1
DB2	Azure SQL database on SQL1
storage1	Storage account
storage2	Storage account
Workspace1	Log Analytics workspace

SQL1 has the following configurations:

- Auditing: Enabled
- Audit log destination: storage1, Workspace1
- DB1 has the following configurations:
 - Auditing: Enabled
 - Audit log destination: storage2
- DB2 has auditing disabled.

Where are the audit logs for DB1 and DB2 stored? To answer, select the appropriate options in the answer area

NOTE: Each correct selection is worth one point.

Answer Area

DB1: storage1, storage2, and Workspace1
 storage2 only

DB2: storage1 and Workspace1 only
 storage2 and Workspace1 only
storage1, storage2, and Workspace1

DB2: Workspace1 only
 No audit logs created
 storage1 only
Workspace1 only
 storage1 and Workspace1

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area

DB1: storage1, storage2, and Workspace1
 storage2 only

DB2: storage1 and Workspace1 only
 storage2 and Workspace1 only
storage1, storage2, and Workspace1

DB2: Workspace1 only
 No audit logs created
 storage1 only
Workspace1 only
 storage1 and Workspace1

NEW QUESTION 121

- (Exam Topic 4)

You have Azure virtual machines that have Update Management enabled. The virtual machines are configured as shown in the following table.

Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West US	RG1
VM3	Windows Server 2016	West US	RG2
VM4	Ubuntu Server 18.04 LTS	West US	RG2
VM5	Red Hat Enterprise Linux 7.4	East US	RG1
VM6	CentOS 7.5	East US	RG1

You schedule two update deployments named Update1 and Update2. Update1 updates VM3. Update2 updates VM6. Which additional virtual machines can be updated by using Update1 and Update2? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Update1:
 VM2 only
 VM4 only
 VM1 and VM2 only
VM1, VM2, VM4, VM5, and VM6

Update2:
 VM5 only
 VM1 and VM5 only
 VM4 and VM5 only
 VM1, VM2, and VM5 only
VM1, VM2, VM3, VM4, and VM5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Update1: VM1 and VM2 only
 VM3: Windows Server 2016 West US RG2 Update2: VM4 and VM5 only
 VM6: CentOS 7.5 East US RG1
 For Linux, the machine must have access to an update repository. The update repository can be private or public.
 References:
<https://docs.microsoft.com/en-us/azure/automation/automation-update-management>

NEW QUESTION 124

- (Exam Topic 4)
 You have an Azure Active Directory (Azure AD) tenant that contains two administrative units named AU1 and AU2. Users are assigned to the administrative units as shown in the following table.

User name	Member of
Admin1	AU1
Admin2	AU1
Admin3	AU2
Admin4	AU2
User1	AU1

Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>
Admin2 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>
Admin3 can reset the password of Admin4.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

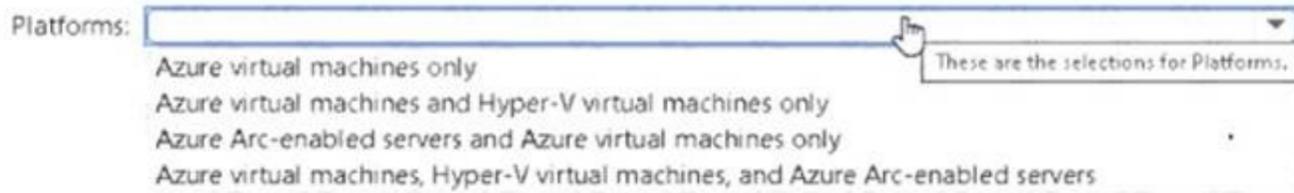
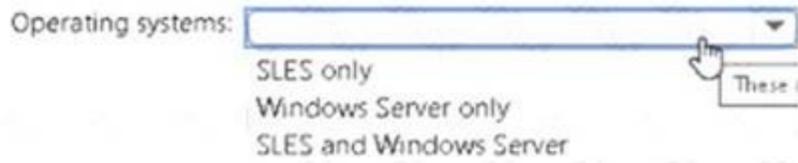
Statements	Yes	No
Admin1 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can reset the password of User3.	<input checked="" type="radio"/>	<input type="radio"/>
Admin3 can reset the password of Admin4.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 129

- (Exam Topic 4)
 Your on-premises network contains the servers shown in the following table.

Name	Operating system	Description
Server1	Windows Server 2019	Hyper-V host hosting four virtual machines that run Windows Server 2022
Server2	Windows Server 2019	File server that has the Azure Arc agent installed
Server3	SUSE Linux Enterprise Server (SLES)	Database server that has the Azure Arc agent installed

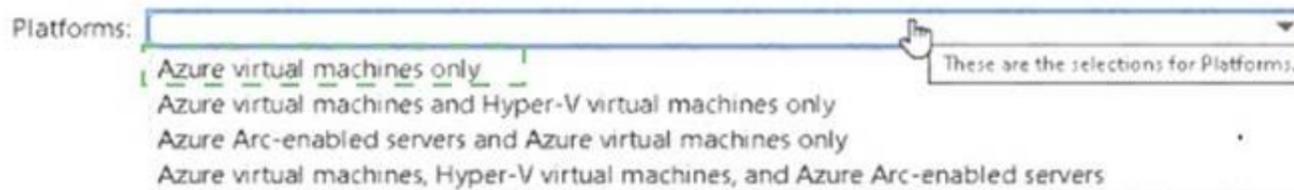
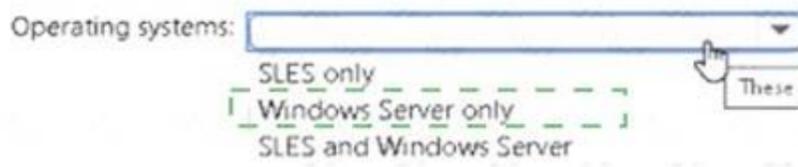
You have an Azure subscription that contains multiple virtual machines that run either Windows Server 2019 or SLES. You plan to implement adaptive application controls in Microsoft Defender for Cloud. Which operating systems and platforms can you monitor? To answer, select the appropriate options in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 132

- (Exam Topic 4)

Your on-premises network contains a Hyper-V virtual machine named VM1. You need to use Azure Arc to onboard VM1 to Microsoft Defender for Cloud. What should you install first?

- A. the Azure Monitor agent
- B. the Azure Connected Machine agent
- C. the Log Analytics agent
- D. the guest configuration agent

Answer: B

NEW QUESTION 135

- (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 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 Sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service. You need to revoke all access to Sa1.

Solution: You generate new SASs. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead you should create a new stored access policy.

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 affects 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 140

- (Exam Topic 4)

You have an Azure subscription named Sub1.

You have an Azure Active Directory (Azure AD) group named Group1 that contains all the members of your IT team.

You need to ensure that the members of Group1 can stop, start, and restart the Azure virtual machines in Sub1. The solution must use the principle of least privilege.

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
Create a JSON file.	<input type="text"/>
Run the Update-AzureRmManagementGroup cmdlet.	<input type="text"/>
Create an XML file.	<input type="text"/>
Run the New-AzureRmRoleDefinition cmdlet.	
Run the New-AzureRmRoleAssignment cmdlet.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure>

NEW QUESTION 144

- (Exam Topic 4)

You have an Azure Container Registry named ContReg1 that contains a container image named image1. You enable content trust for ContReg1.

After content trust is enabled, you push two images to ContReg1 as shown in the following table.

Name	Details
image2	Image was pushed with client content trust enabled.
image3	Image was pushed with client content trust disabled.

Which images are trusted images?

- A. image1 and image2 only
- B. image2 only
- C. image1, image2, and image3

Answer: B

Explanation:

Azure Container Registry implements Docker's content trust model, enabling pushing and pulling of signed images.

To push a trusted image tag to your container registry, enable content trust and push the image with docker push.

To work with trusted images, both image publishers and consumers need to enable content trust for their Docker clients. As a publisher, you can sign the images you push to a content trust-enabled registry.

Reference:

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust>

NEW QUESTION 147

- (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.

Actions

Answer Area

- Create a private link to storage1.
- Enable Active Directory Domain Services (AD DS) authentication on storage1.
- Implement Azure AD Connect.
- Create a service endpoint to storage1.
- Assign share-level permissions for share1.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 150

- (Exam Topic 4)

You have an Azure Sentinel deployment.

You need to create a scheduled query rule named Rule1. What should you use to define the query rule logic for Rule1?

- A. a Transact-SQL statement
- B. a JSON definition
- C. GraphQL
- D. a Kusto query

Answer: D

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

NEW QUESTION 153

- (Exam Topic 4)

You have an Azure subscription and the computers shown in the following table.

Name	Operating system	Description
VM1	Windows Server 2012 R2	Azure virtual machine
VM2	Red Hat Enterprise Linux (RHEL) 8.2	Azure virtual machine
Server1	Windows Server 2019	On-premises physical computer connected to Microsoft Defender for Cloud
VMSS1_0	Windows Server 2022	Azure virtual machine in a virtual machine scale set

You need to perform a vulnerability scan of the computers by using Microsoft Defender for Cloud. Which computers can you scan?

- A. VM1 only
- B. VM1 and VM2 only
- C. Server1 and VMSS1.0 only
- D. VM1, VM2, and Server1 only
- E. VM1, VM2, Server1, and VMSS1.0

Answer: A

NEW QUESTION 154

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant. You have the deleted objects shown in the following table.

Name	Type	Deleted on
Group1	Security group	April 5, 2020
Group2	Office 365 group	April 5, 2020
User1	User	March 25, 2020
User2	User	April 30, 2020

On May 4, 2020, you attempt to restore the deleted objects by using the Azure Active Directory admin center. Which two objects can you restore? Each correct answer presents a complete solution.
 NOTE: Each correct selection is worth one point.

- A. Group1
- B. Group2
- C. User2
- D. User1

Answer: BC

Explanation:

Deleted users and deleted Office 365 groups are available for restore for 30 days. You cannot restore a deleted security group.
 Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-restore-deleted>

NEW QUESTION 159

- (Exam Topic 4)

You have the Azure Information Protection conditions shown in the following table.

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

You have the Azure Information Protection labels shown in the following table.

Name	Applies to	Use label	Set the default label
Global	Not applicable	None	None
Policy1	User1	Label1	None
Policy2	User1	Label2	None

You need to identify how Azure Information Protection will label files.

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

If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

▼

No label

Label1 only

Label2 only

Label1 and Label2

If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:

▼

No label

Label1 only

Label2 only

Label1 and Label2

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Label 2 only

How multiple conditions are evaluated when they apply to more than one label

> The labels are ordered for evaluation, according to their position that you specify in the policy: The label positioned first has the lowest position (least sensitive) and the label positioned last has the highest position (most sensitive).

> The most sensitive label is applied.

> The last sublabel is applied.

Box 2: No Label

Automatic classification applies to Word, Excel, and PowerPoint when documents are saved, and apply to Outlook when emails are sent. Automatic classification does not apply to Microsoft Notepad.

References:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

NEW QUESTION 163

- (Exam Topic 4)

You have 20 Azure subscriptions and a security group named Group1. The subscriptions are children of the root management group. Each subscription contains a resource group named RG1.

You need to ensure that for each subscription RG1 meets the following requirements:

- > The members of Group1 are assigned the Owner role.
- > The modification of permissions to RG1 is prevented.

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

NOTE: Each correct selection is worth one point.

Configure role-based access control (RBAC) role assignments by using:

▼
Azure Blueprints
Azure Policy
Azure Security Center

Prevent the modification of permissions to RG1 by using:

▼
A resource lock
A role-based access control (RBAC) role assignment at the resource group level
Azure Blueprint assignments in locking mode

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Configure role-based access control (RBAC) role assignments by using:

▼
Azure Blueprints
Azure Policy
Azure Security Center

Prevent the modification of permissions to RG1 by using:

▼
A resource lock
A role-based access control (RBAC) role assignment at the resource group level
Azure Blueprint assignments in locking mode

NEW QUESTION 164

- (Exam Topic 4)

You have an Azure subscription that contains a user named User1. You need to ensure that User1 can perform the following tasks:

- Create groups.
- Create access reviews for role-assignable groups.
- Assign Azure AD roles to groups.

The solution must use the principle of least privilege. Which role should you assign to User1?

- A. Groups administrator
- B. Authentication administrator
- C. Identity Governance Administrator
- D. Privileged role administrator

Answer: C

NEW QUESTION 165

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL server named SQL1. SQL1 contains. You need to use Microsoft Defender for Cloud to complete a vulnerability assessment for DB1. What should you do first?

- A. From Advanced Threat Protection types, select SQL injection vulnerability.
- B. Configure the Send scan report to setting.
- C. Set Periodic recurring scans to ON.
- D. Enable the Microsoft Defender for SQL plan.

Answer: A

NEW QUESTION 170

- (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 174

- (Exam Topic 4)

You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role
User1	Global administrator
User2	Security administrator
User3	Security reader
User4	License administrator

Each user is assigned an Azure AD Premium P2 license.

You plan to onboard and configure Azure AD Identity Protection.

Which users can onboard Azure AD Identity Protection, remediate users, and configure policies? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Answer Area

Users who can onboard Azure AD Identity Protection:

User1 only
 User1 and User2 only
 User1, User 2, and User3 only
 User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

User1 and User2 only
 User1 and User3 only
 User1, User 2, and User3 only
 User1, User 2, User3, and User 4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Users who can onboard Azure AD Identity Protection:

User1 only
 User1 and User2 only
 User1, User 2, and User3 only
 User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

User1 and User2 only
 User1 and User3 only
 User1, User 2, and User3 only
 User1, User 2, User3, and User 4

NEW QUESTION 179

- (Exam Topic 4)

You have an Azure subscription.

You need to deploy an Azure virtual WAN to meet the following requirements:

- Create three secured virtual hubs located in the East US, West US, and North Europe Azure regions.
- Ensure that security rules sync between the regions. What should you use?

- A. Azure Firewall Manager
- B. Azure Virtual Network Manager
- C. Azure Network Function Manager
- D. Azure Front Door

Answer: A

NEW QUESTION 180

- (Exam Topic 4)

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Region	Subnet
VNET1	West US	Subnet11 and Subnet12
VNET2	West US 2	Subnet21
VNET3	East US	Subnet31

The subscription contains the virtual machines shown in the following table.

Name	Network interface	Connected to
VM1	NIC1	Subnet11
VM2	NIC2	Subnet11
VM3	NIC3	Subnet12
VM4	NIC4	Subnet21
VM5	NIC5	Subnet31

On NIC1, you configure an application security group named ASG1. On which other network interfaces can you configure ASG1?

- A. NIC2 only
- B. NIC2, NIC3, NIC4, and NIC5
- C. NIC2 and NIC3 only
- D. NIC2, NIC3, and NIC4 only

Answer: C

Explanation:

Only network interfaces in VNET1, which consists of Subnet11 and Subnet12, can be configured in ASG1, as all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.

Reference:

<https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/>

NEW QUESTION 181

- (Exam Topic 4)

You have an Azure subscription that contains the resources shown in the following table.

Name	Type
LB1	Azure Standard Load Balancer
VM1	Virtual machine
SQL1	Azure SQL Database
VMSS1	Virtual machine scale set

You plan to deploy an Azure Private Link service named APL1. Which resource must you reference during the creation of APL1?

- A. VMSS1
- B. VM1
- C. SQL
- D. LB1

Answer: D

NEW QUESTION 186

- (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	10.1.1.5	20.224.219.170
VM2	VNET1/Subnet2	10.1.2.5	20.224.219.230
VM3	VNET2/Subnet1	10.11.1.5	40.122.155.212

You have an Azure Cosmos DB account named cosmos1 configured as shown in the following exhibit.

Allow access from

All networks Selected networks

Configure network security for your Azure Cosmos DB account. Learn more

Statements	Yes	No
VM1 can access cosmos1 over the internet.	<input type="radio"/>	<input type="radio"/>
VM2 can access cosmos1 over the internet.	<input type="radio"/>	<input type="radio"/>
VM3 can access cosmos1 over the internet.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
 Yes, Yes, No

NEW QUESTION 188

- (Exam Topic 4)

You work at a company named Contoso, Ltd. that has the offices shown in the following table.

Name	IP address space
Boston	180.15.10.0/24
Seattle	132.32.15.0/24

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com. All contoso.com users have Azure Multi-Factor Authentication (MFA) enabled. The tenant contains the users shown in the following table.

Name	User device	Last sign-in	During last sign-in, user selected Don't ask again for 14 days
User1	Device1	June 1	Yes
User2	Device2	June 3	No

The multi-factor settings for contoso.com are configured as shown in the following exhibit.

multi-factor authentication

users service settings

app passwords [\(learn more\)](#)

- Allow users to create app passwords to sign in to non-browser apps
- Do not allow users to create app passwords to sign in to non-browser apps

trusted ips [\(learn more\)](#)

- Skip multi-factor authentication for requests from federated users on my intranet
- Skip multi-factor authentication for requests from following range of IP address subnets

180.15.10.0/24

verification options [\(learn more\)](#)

Methods available to users:

- call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app or hardware token

remember multi-factor authentication [\(learn more\)](#)

- Allow users to remember multi-factor authentication on devices they trust
 Days before a device must re-authenticate (1-60):

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 to Device1 from the Seattle office on June 10, the user will be prompted for MFA.	<input type="radio"/>	<input type="radio"/>
When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.	<input type="radio"/>	<input type="radio"/>
When User1 signs in to to a new device from the Seattle office on June 7, the user will be prompted for MFA.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA.	<input type="radio"/>	<input checked="" type="radio"/>
When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.	<input checked="" type="radio"/>	<input type="radio"/>
When User1 signs in to to a new device from the Seattle office on June 7, the user will be prompted for MFA.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 191

- (Exam Topic 4)

Lab Task

Task 7

You need to ensure that connections through an Azure Application Gateway named Homepage-AGW are inspected for malicious requests.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Enable Web Application Firewall (WAF) for the application gateway. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select a WAF policy and a WAF mode for the application gateway. You can choose a predefined policy or create a custom policy with your own rules and exclusions.

Configure WAF policy settings. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select the managed rulesets and rule groups that you want to enable or disable for the WAF policy. You can also configure custom rules to match specific patterns or conditions and take actions such as blocking or logging requests.

Monitor WAF logs. You can use different types of logs in Azure to manage and troubleshoot the application gateway and the WAF policy. You can access some of these logs through the portal, such as metrics and health probes. You can also export the logs to Azure Storage, Event Hubs, or Log Analytics and view them in different tools, such as Azure Monitor, Excel, or Power BI.

NEW QUESTION 195

- (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 196

- (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: User1-28681041@ExamUsers.com

Azure Password: GpO Ae4@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 9

You need to ensure that the rg1lod28681041n1 Azure Storage account is encrypted by using a key stored in the KeyVault28681041 Azure key vault.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To ensure that the rg1lod28681041n1 Azure Storage account is encrypted by using a key stored in the KeyVault28681041 Azure key vault, you can follow these steps:

- In the Azure portal, search for and select the storage account named rg1lod28681041n1.
- In the left pane, select Encryption.
- In the Encryption pane, select Customer-managed key.
- In the Customer-managed key pane, select Select from Key Vault.

- > In the Select from Key Vault pane, enter the following information:
- > Key vault: Select the KeyVault28681041 Azure key vault.
- > Key: Select the key you want to use.
- > Select Save.

NEW QUESTION 197

- (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 199

- (Exam Topic 4)

You have two Azure virtual machines in the East US2 region as shown in the following table.

Name	Operating system	Type	Tier
VM1	Windows Server 2008 R2	A3	Basic
VM2	Ubuntu 16.04-DAILY-LTS	L4s	Standard

You deploy and configure an Azure Key vault. You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2. What should you modify on each virtual machine? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

VM1: ▼

The operating system version

The tier

The type

VM2: ▼

The operating system version

The tier

The type

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

VM1: The Tier

The Tier needs to be upgraded to standard.

Disk Encryption for Windows and Linux IaaS VMs is in General Availability in all Azure public regions and Azure Government regions for Standard VMs and VMs with Azure Premium Storage.

VM2: the operating system

References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/generation-2#generation-1-vs-generation-2-ca>

NEW QUESTION 201

- (Exam Topic 4)

You have an Azure resource group that contains 100 virtual machines. You have an initiative named Initiative1 that contains multiple policy definitions. Initiative1 is assigned to the resource group. You need to identify which resources do NOT match the policy definitions. What should you do?

- A. From Azure Security Center, view the Regulatory compliance assessment.
- B. From the Policy blade of the Azure Active Directory admin center, select Compliance.
- C. From Azure Security Center, view the Secure Score.
- D. From the Policy blade of the Azure Active Directory admin center, select Assignments.

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/how-to/get-compliance-data#portal>

NEW QUESTION 202

- (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 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 Sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service. You need to revoke all access to Sa1.

Solution: You create a new stored access policy. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Shared access signatures provides access to a particular resource such as blob. Stored access policies are a group of Shared Access Signatures (SAS). In order to revoke access to a SAS you can either:

* 1. Rotate the Key1 or Key 2, that is the access keys used to sign the SAS. Rotating the access keys used to sign the SAS, invalidates any previously signed SAS hence revoking the SAS issued before

* 2. Remove the stored access policy which an SAS is linked to. If a Stored Access Policy is removed, it also invalidates the SASs linked to the Stored Access Policy.

NEW QUESTION 206

- (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

NEW QUESTION 211

- (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 logs 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 215

- (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 216

- (Exam Topic 4)

You are securing access to the resources in an Azure subscription.

A new company policy states that all the Azure virtual machines in the subscription must use managed disks. You need to prevent users from creating virtual machines that use unmanaged disks.

What should you use?

- A. Azure Monitor
- B. Azure Policy
- C. Azure Security Center
- D. Azure Service Health

Answer: B

NEW QUESTION 221

- (Exam Topic 4) You have an Azure subscription. You plan to create a storage account.

You need to use customer-managed keys to encrypt the tables in the storage account.

From Azure Cloud Shell, which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.

Cmdlets

Answer Area

New-AzStorageAccountKey		
New-AzStorageTable	➤	⬆
Register-AzProviderFeature	⬅	⬇
New-AzStorageAccount		
Register-AzResourceProvider		

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text, table Description automatically generated with medium confidence

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-key-vault?tabs=pow>

NEW QUESTION 223

- (Exam Topic 4)

You have an Azure subscription that contains an Azure Files share named share1 and a user named User1. Identity-based authentication is configured for share1. User1 attempts to access share1 from a Windows 10 device by using SMB. Which type of token will Azure Files use to authorize the request?

- A. OAuth 20
- B. JSON Web Token (JWT)
- C. Kerberos
- D. SAML

Answer: C

Explanation:

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service>

NEW QUESTION 228

- (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 232

- (Exam Topic 4)

You have an Azure subscription that contains an Azure web app named App1.

You plan to configure a Conditional Access policy for App1. The solution must meet the following requirements:

- Only allow access to App1 from Windows devices.
- Only allow devices that are marked as compliant to access App1.

Which Conditional Access policy settings should you configure? To answer, drag the appropriate settings to the correct requirements. Each setting 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.

Policy settings	Answer Area
Cloud apps or actions	Only allow access to App1 from Windows devices: <input type="text"/>
Conditions	Only allow devices that are marked as compliant to access App1: <input type="text"/>
Grant	
Session	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Policy settings	Answer Area
Cloud apps or actions	Only allow access to App1 from Windows devices: <input type="text" value="Conditions"/>
Conditions	Only allow devices that are marked as compliant to access App1: <input type="text" value="Conditions"/>
Grant	
Session	

NEW QUESTION 233

- (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 an Azure Subscription named Sub1. Sub1 contains an Azure virtual machine named VM1 that runs Windows Server 2016.

You need to encrypt VM1 disks by using Azure Disk Encryption.

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
Configure secrets for the Azure key vault.	
Create an Azure key vault.	
Run Set-AzureRmStorageAccount.	
Configure access policies for the Azure key vault.	
Run Set-AzureRmVmDiskEncryptionExtension.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/encrypt-disks>

NEW QUESTION 237

- (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: User1-28681041@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 10

You need to create a new Azure AD directory named 28681041.onmicrosoft.com. The new directory must contain a new user named user1@28681041.onmicrosoft.com.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To create a new Azure AD directory named 28681041.onmicrosoft.com that contains a new user named user1@28681041.onmicrosoft.com, you can follow these steps:

- In the Azure portal, search for and select Azure Active Directory.
- In the left pane, select Domains.
- Select Add domain.
- In the Add a custom domain pane, enter the following information:
- Domain name: Enter the domain name you want to use. For example, 28681041.onmicrosoft.com.
- Add domain: Select Add domain.
- In the left pane, select Users.
- Select New user.
- In the New user pane, enter the following information:
- User name: Enter the user name you want to use. For example, user1@28681041.onmicrosoft.com.
- Name: Enter the name of the user.
- Password: Enter a password for the user.
- Groups: Select the groups you want the user to be a member of.
- Select Create.

You can find more information on these topics in the following Microsoft documentation:

- Add a custom domain name to Azure Active Directory
- Create a new user in your organization - Azure Active Directory

NEW QUESTION 241

- (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	<i>Not applicable</i>
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.	<input type="radio"/>	<input type="radio"/>
You can create obj1.	<input type="radio"/>	<input type="radio"/>
You can create OBJ3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
You can create IPobject1.	<input type="radio"/>	<input checked="" type="radio"/>
You can create obj1.	<input type="radio"/>	<input checked="" type="radio"/>
You can create OBJ3.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 246

- (Exam Topic 4)

You have an Azure subscription named Subscription1 that contains an Azure Active Directory (Azure AD) tenant named contoso.com and a resource group named RG1.

You create a custom role named Role1 for contoso.com.

You need to identify where you can use Role1 for permission delegation. What should you identify?

- A. contoso.com only
- B. contoso.com and RGT only
- C. contoso.com and Subscription1 only
- D. contoso.com, RG1, and Subscription1

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles>

NEW QUESTION 247

- (Exam Topic 4)

You have an Azure subscription that contains a user named User1. User1 is assigned the Reader role for the subscription.

You plan to create a custom role named Role1 and assign Role1 to User1.

You need to ensure that User1 can create and manage application security groups by using the Azure portal. Which two permissions should you add to Role1? To answer, select the appropriate permission in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Add permissions

Microsoft Monitoring Insights Microsoft.SecurityGraph	Microsoft Monitoring Insights Enable your workforce to be productive on all their devices, while keeping your organization's information protected.	Microsoft Monitoring Insights Microsoft.DynamicsTelemetry	Microsoft Network Connect cloud and on-premises infrastructure and services to provide your customers and users the best.
Microsoft Operations Management A simplified management solution for any enterprise	Microsoft Policy Insights Summarize policy states for the subscription level policy definition.	Microsoft Portal Build, manage, and monitor all Azure products in a single, unified console.	Microsoft Power BI Dedicated Manage Power BI Premium dedicated capacities for exclusive use by an organization.
Microsoft Power Platform Microsoft.PowerPlatform	Microsoft Project Babylon Microsoft.ProjectBabylon	Microsoft Purview Microsoft.Purview	Microsoft Resource Graph Powerful tool to query, explore, and analyze your cloud resources at scale.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

* 1. Microsoft Portal 2. Microsoft Network

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/azure-services-resource-providers>

NEW QUESTION 249

- (Exam Topic 4)

You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.

You create a service endpoint for Subnet1.

Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.

You need to deploy Docker containers to VM1. The containers must be able to access Azure Storage resources and Azure SQL databases by using the service endpoint.

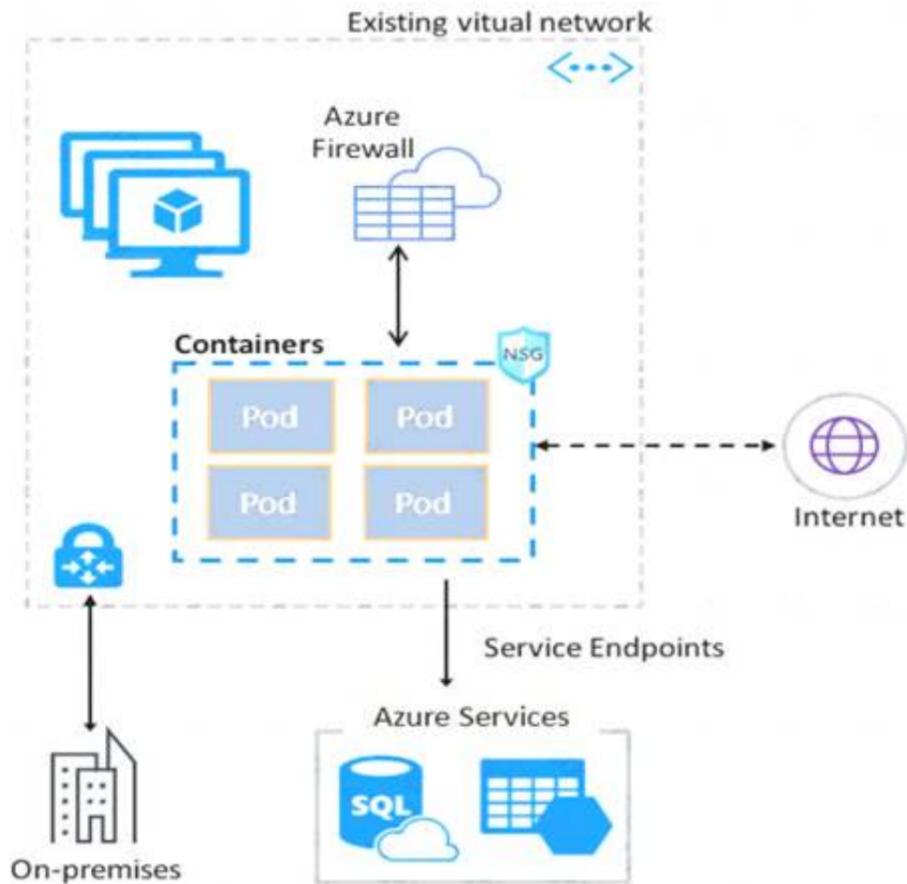
- A. Create an application security group and a network security group (NSG).
- B. Edit the docker-compose.yml file.
- C. Install the container network interface (CNI) plug-in.

Answer: C

Explanation:

The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual Machine. The plug-in supports both Linux and Windows platform. The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers and virtual network resources. The plug-in doesn't rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines.

The following picture shows how the plug-in provides Azure Virtual Network capabilities to Pods:



References:
<https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview>

NEW QUESTION 251

- (Exam Topic 4)

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Subscription role	Azure AD user role
User1	Owner	None
User2	Contributor	None
User3	Security Admin	None
User4	None	Service administrator

You create a resource group named RG1.

Which users can modify the permissions for RG1 and which users can create virtual networks in RG1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Users who can modify the permissions for RG1:

▼

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Users who can create virtual networks in RG1:

▼

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Only an owner can change permissions on resources.

Box 2: A Contributor can create/modify/delete anything in the subscription but cannot change permissions.

NEW QUESTION 254

- (Exam Topic 4)

You have an Azure Sentinel workspace that contains an Azure Active Directory (Azure AD) connector, an Azure Log Analytics query named Query1 and a playbook named Playbook1.
 Query1 returns a subset of security events generated by Azure AD.
 You plan to create an Azure Sentinel analytic rule based on Query1 that will trigger Playbook1. You need to ensure that you can add Playbook1 to the new rule.
 What should you do? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Create the rule and set the type to:

- Fusion
- Microsoft Security incident creation
- Scheduled

Configure the playbook to include:

- A managed connector
- A system-assigned managed identity
- A trigger
- Diagnostic settings

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom> <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

NEW QUESTION 255

- (Exam Topic 4)

You have an Azure subscription named Subcription1 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 Subcription2 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. NOTE: Each correct selection is worth one point.

Answer Area

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:

Answer Area

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

NEW QUESTION 256

- (Exam Topic 4)

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have an Amazon Web Service (AWS) account named AWS1 that is connected to defender for Cloud.

You need to ensure that AWS foundational Security Best Practices. The solution must minimize administrative effort. What should you do in Defender for Cloud?

- A. Create a new customer assessment.
- B. Assign a built-in assessment.
- C. Assign a built-in compliance standard.
- D. Create a new custom standard.

Answer: C

NEW QUESTION 258

- (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 259

- (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.	<input type="radio"/>	<input type="radio"/>
You can add a new key named Item1.	<input type="radio"/>	<input type="radio"/>
You can add a new secret named Item2.	<input type="radio"/>	<input type="radio"/>

- 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 Soft-deleted status <https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview>

NEW QUESTION 262

- (Exam Topic 4)

You have an Azure subscription that contains the following resources:

- > A virtual network named VNET1 that contains two subnets named Subnet1 and Subnet2.
- > A virtual machine named VM1 that has only a private IP address and connects to Subnet1.

You need to ensure that Remote Desktop connections can be established to VM1 from the internet.

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

Configure a network security group (NSG).

Create a network rule collection.

Create a NAT rule collection.

Create a new subnet.

Deploy Azure Application Gateway.

Deploy Azure Firewall.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Configure a network security group (NSG).

Create a network rule collection.

Create a NAT rule collection.

Create a new subnet.

Deploy Azure Application Gateway.

Deploy Azure Firewall.

Answer Area

Create a new subnet.

Deploy Azure Firewall.

Create a NAT rule collection.

NEW QUESTION 264

- (Exam Topic 4)

You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.

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

- Create an access review program.
- Set Reviewers to Selected users.
- Create an access review audit.
- Create an access review control.
- Set Reviewers to Group owners.
- Set Reviewers to Members.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: Create an access review program Step 2: Create an access review control Step 3: Set Reviewers to Group owners
 In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.



References:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review> <https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls>

NEW QUESTION 265

- (Exam Topic 4)

You have an Azure subscription that contains the alerts shown in the following exhibit.

All Alerts

+ New alert rule | Edit columns | Manage alert rules | View classic alerts | Refresh | Change state

Don't see a subscription? Open Directory + Subscription settings

Subscription: Azure Pass - Sponsorship | Resource group: Type to start filtering... | Resource type: 0 selected | Resource: Type to start filtering... | Time range: Past hour

Monitor service: 15 selected | Monitor condition: 2 selected | Severity: Sev 4 | Alert state: 3 selected | Smart group id: Smart group id

All Alerts | Alerts By Smart Group (Preview)

Search by name (case-insensitive)

NAME	SEVERITY	MONITOR C...	ALERT STATE	AFFECT...	MONITOR SERV...	SIGNAL TYPE	FIRE TIME	SU...
Alert1	Sev4	Fired	New		ActivityLog Ad...	Log	6/6/2019, 11:23:53 ...	Azure ...
Alert1	Sev4	Fired	Acknowledged		ActivityLog Ad...	Log	6/6/2019, 11:23:52 ...	Azure ...
Alert2	Sev4	Fired	Acknowledged		ActivityLog Ad...	Log	6/6/2019, 11:23:25 ...	Azure ...
Alert2	Sev4	Fired	Closed		ActivityLog Ad...	Log	6/6/2019, 11:23:24 ...	Azure ...

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.

The state of Alert1 that was fired at 11:23:52

▼
cannot be changed
can be changed to Closed only
can be changed to New only
can be changed to New or Closed

The state of Alert2 that was fired at 11:23:24

▼
cannot be changed
can be changed to Acknowledged only
can be changed to New only
can be changed to New or Acknowledged

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-overview>

NEW QUESTION 266

- (Exam Topic 4)

You have an Azure subscription that contains the custom roles shown in the following table.

Name	Type
Role1	Azure Active Directory (Azure AD)
Role2	Azure subscription

In the Azure portal, you plan to create new custom roles by cloning existing roles. The new roles will be configured as shown in the following table.

Name	Type
Role3	Azure AD
Role4	Azure subscription

Which roles can you clone to create each new role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Role3:

▼
Role1 only
Built-in Azure AD roles only
Role1 and built-in Azure AD roles only
Role1, built-in Azure AD roles, and built-in Azure subscription roles

Role4:

▼
Role2 only
Built-in Azure AD roles only
Role2 and built-in Azure subscription roles only
Role2, built-in Azure subscription roles, and built-in Azure AD roles

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-create> <https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal>

NEW QUESTION 268

- (Exam Topic 4)

You have an Azure subscription that contains a Microsoft Sentinel workspace.

Microsoft 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 Microsoft Sentinel components to configure to meet the following requirements:

- When Microsoft 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 Microsoft 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:

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	

NEW QUESTION 272

- (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 VNet 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 274

- (Exam Topic 4)

You have an Azure AD tenant that contains the users shown in the following table.

Name	Description
User1	Uses app password authentication for the Mail and Calendar app in Windows 10
User2	Uses Outlook on the web

You need to ensure that the users cannot create app passwords. The solution must ensure that User1 can continue to use the Mail and Calendar app. What should you do?

- A. Assign User1 the Authentication Policy Administrator role.
- B. Enable Azure AD Password Protection.
- C. Configure a multi-factor authentication (MFA) registration policy.
- D. Create a new app registration.

Answer: C

NEW QUESTION 277

- (Exam Topic 4)

You have a management group named MG1 that contains an Azure subscription and a resource group named RG1. RG1 contains a virtual machine named VM1. You have the custom Azure roles shown in the following table.

Name	Scoped to
Role1	MG1
Role2	RG1

The permissions for Role1 are shown in the following role definition file.

```

"permissions": [
  {
    "actions": [
      "Microsoft.Compute/virtualMachines/*"
    ],
    "notActions": [
      "Microsoft.Compute/virtualMachines/delete"
    ],
    "dataActions": [],
  }
]
  
```

The permissions for Role2 are shown in the following role definition file.

```

"permissions": [
  {
    "actions": [
      "Microsoft.Compute/virtualMachines/*"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]
  
```

You assign the roles to the users shown in the following table.

Name	Role
User1	Role1
User2	Role1, Role2
User3	Role2

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
User1 can delete VM1.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM1.	<input type="radio"/>	<input type="radio"/>
User3 can delete VM1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can delete VM1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can delete VM1.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can delete VM1.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 278

- (Exam Topic 4)

You have an Azure subscription named Sub1 that contains the Azure key vaults shown in the following table:

Name	Region	Resource group
Vault1	West Europe	RG1
Vault2	East US	RG1
Vault3	West Europe	RG2
Vault4	East US	RG2

In Sub1, you create a virtual machine that has the following configurations:

- > Name: VM1
- > Size: DS2v2
- > Resource group: RG1
- > Region: West Europe
- > Operating system: Windows Server 2016

You plan to enable Azure Disk Encryption on VM1.

In which key vaults can you store the encryption key for VM1?

- A. Vault1 or Vault3 only
- B. Vault1, Vault2, Vault3, or Vault4
- C. Vault1 only
- D. Vault1 or Vault2 only

Answer: A

Explanation:

In order to make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the Key Vault and the VMs to be co-located in the same region. Create and use a Key Vault that is in the same region as the VM to be encrypted.

Reference:

<https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites>

NEW QUESTION 283

- (Exam Topic 4)

You have an Azure subscription that contains an Azure key vault named Vault1. In Vault1, you create a secret named Secret1.

An application developer registers an application in Azure Active Directory (Azure AD). You need to ensure that the application can use Secret1.

What should you do?

- A. In Azure AD, create a role.
- B. In Azure Key Vault, create a key.
- C. In Azure Key Vault, create an access policy.
- D. In Azure AD, enable Azure AD Application Proxy.

Answer: C

Explanation:

"You may need to configure the target resource to allow access from your application. For example, if you request a token to Key Vault, you need to make sure you have added an access policy that includes your application's identity. Otherwise, your calls to Key Vault will be rejected, even if they include the token"

<https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet>

NEW QUESTION 285

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL database named DB1 in the East US Azure region. You create the storage accounts shown in the following table.

Name	Location	Performance	Premium account type
storage1	East US	Standard	Not applicable
storage2	East US	Premium	Block blobs
storage3	East US	Premium	File shares
storage4	East US 2	Standard	Not applicable

You plan to enable auditing for DB1.

Which storage accounts can you use as the auditing destination for DB1?

- A. storage1 only
- B. storage1 and storage4 only
- C. Storage2 and storage3 only
- D. storage1, storage2 and storage3 only

Answer: C

NEW QUESTION 286

- (Exam Topic 4)

You have an Azure subscription that contains a web app named Appl. App1 provides users with product images and videos. Users access App1 by using a URL of [HTTPS://appl.contoso.com](https://appl.contoso.com). You deploy two server pools named Pool1 and Pool2. Pool1 hosts product images. Pool2 hosts product videos. You need to optimize

The performance of Appl. The solution must meet the following requirements:

- Minimize the performance impact of TLS connections on Pool1 and Pool2.
- Route user requests to the server pools based on the requested URL path. What should you include in the solution?

- A. Azure Traffic Manager
- B. Azure Bastion
- C. Azure Application Gateway
- D. Azure Front Door

Answer: C

NEW QUESTION 288

- (Exam Topic 4)

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Category
Initiative1	Initiative definition	Security Center
Initiative2	Initiative definition	My Custom Category
Policy1	Policy definition	Security Center
Policy2	Policy definition	My Custom Category

You need to identify which initiatives and policies you can add to Subscription1 by using Azure Security Center. What should you identify?

- A. Policy1 and Policy2 only
- B. Initiative1 only
- C. Initiative1 and Initiative2 only
- D. Initiative1, Initiative2, Policy1, and Policy2

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/custom-security-policies>

NEW QUESTION 290

- (Exam Topic 4)

You are troubleshooting a security issue for an Azure Storage account. You enable the diagnostic logs for the storage account.

What should you use to retrieve the diagnostics logs?

- A. Azure Storage Explorer
- B. SQL query editor in Azure
- C. File Explorer in Windows
- D. Azure Security Center

Answer: A

Explanation:

If you want to download the metrics for long-term storage or to analyze them locally, you must use a tool or write some code to read the tables. You must download the minute metrics for analysis. The tables do not appear if you list all the tables in your storage account, but you can access them directly by name. Many storage-browsing tools are aware of these tables and enable you to view them directly (see Azure Storage Client Tools for a list of available tools). Microsoft provides several graphical user interface (GUI) tools for working with the data in your Azure Storage account. All of the tools outlined in the following table are free.

Azure Storage client tool	Supported platforms	Block Blob	Page Blob	Append Blob	Tables	Queues	Files
Azure portal	Web	Yes	Yes	Yes	Yes	Yes	Yes
Azure Storage Explorer	Windows, OSX	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Visual Studio Cloud Explorer	Windows	Yes	Yes	Yes	Yes	Yes	No

References:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-metrics?toc=%2fazure%2fstorage%2f> <https://docs.microsoft.com/en-us/azure/storage/common/storage-explorers>

NEW QUESTION 292

- (Exam Topic 4)

Your company recently created an Azure subscription.

You have been tasked with making sure that a specified user is able to implement Azure AD Privileged Identity Management (PIM).

Which of the following is the role you should assign to the user?

- A. The Global administrator role.
- B. The Security administrator role.
- C. The Password administrator role.
- D. The Compliance administrator role.

Answer: A

Explanation:

To start using PIM in your directory, you must first enable PIM.

* 1. Sign in to the Azure portal as a Global Administrator of your directory.

You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.

Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started>

NEW QUESTION 294

- (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 295

- (Exam Topic 4)

You have the Azure virtual networks shown in the following table.

Name	Location	Subnet	Peered network
VNET1	East US	Subnet1	VNET2
VNET2	West US	Subnet2, Subnet3	VNET1
VNET4	East US	Subnet4	None

You have the Azure virtual machines shown in the following table.

Name	Application security group	Network security group (NSG)	Connected to	Public IP address
VM1	ASG1	NSG1	Subnet1	No
VM2	ASG2	NSG1	Subnet2	No
VM3	ASG2	NSG1	Subnet3	Yes
VM4	ASG4	NSG1	Subnet4	Yes

The firewalls on all the virtual machines allow ping traffic. NSG1 is configured as shown in the following exhibit. Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
110	Allow_RDP	3389	Any	Any	Any	Allow
130	Rule1	Any	Any	ASG1	Any	Allow
140	Rule2	Any	Any	ASG2	Any	Allow
150	Rule3	Any	Any	ASG4	Any	Allow
160	Rule4	Any	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBou...	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

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
VM1 can ping VM3 successfully.	<input type="radio"/>	<input type="radio"/>
VM2 can ping VM4 successfully.	<input type="radio"/>	<input type="radio"/>
VM3 can be accessed by using Remote Desktop from the internet.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Yes

VM1 and VM3 are on peered VNets. The firewall rules with a source of ASG1 and ASG2 allow 'any' traffic on 'any' protocol so pings are allowed between VM1 and VM3.

Box 2: No

VM2 and VM4 are on separate VNets and the VNets are not peered. Therefore, the pings would have to go over the Internet. VM4 does have a public IP and the firewall allows pings. However, for VM2 to be able to ping VM4, VM2 would also need a public IP address. In Azure, pings don't go out through the default gateway as they would in a physical network. For an Azure VM to ping external IPs, the VM must have a public IP address assigned to it.

Box 3: Yes

VM3 has a public IP address and the firewall allows traffic on port 3389.

NEW QUESTION 298

- (Exam Topic 4)

You have an Azure subscription that contains a blob container named cont1. Cont1 has the access policies shown in the following exhibit.

Save

Stored access policies

Identifier	Start time	Expiry time	Permissions
Policy1			r ...

Add policy

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

The maximum number of additional stored access policies that you can add to cont1 is [answer choice].

The maximum number of additional immutable blob storage policies that you can add to cont1 is [answer choice].

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The maximum number of additional stored access policies that you can add to cont1 is [answer choice].

The maximum number of additional immutable blob storage policies that you can add to cont1 is [answer choice].

NEW QUESTION 301

- (Exam Topic 4)

You have an Azure subscription that uses Microsoft Defender for Cloud.

You need to use Defender for Cloud to review regulatory compliance with the Azure CIS 1.4,0 standard. The solution must minimize administrative effort.

What should you do first?

- A. Assign an Azure policy.
- B. Manually add the Azure CIS 1.4.0 standard.
- C. Disable one of the Out of the box standards.
- D. Add a custom initiative.

Answer: A

NEW QUESTION 305

- (Exam Topic 4)

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Azure region	Connected to	Associated network security group (NSG)
VM1	West US	VNET1/Subnet1	None
VM2	West US	VNET1/Subnet2	NSG2
VM3	Central US	VNET2/Subnet1	NSG3
VM4	West US	VNET3/Subnet1	NSG4

VNET1, VNET2, and VNET3 are peered with each other. You perform the following actions:

- * Create two application security groups named ASG1 and ASG2 in the West US region.
- * Add the network interface of VM1 to ASG1.

Answer Area

ASG1:

ASG2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

ASG1:

ASG2:

NEW QUESTION 308

- (Exam Topic 4)

You have an on-premises network and an Azure subscription.

You have the Microsoft SQL Server instances shown in the following table.

Name	Type
sql1	Azure SQL managed instance
sql2	SQL Server 2019 on an Azure virtual machine that runs Windows Server 2019
sql3	SQL Server 2019 on an Azure virtual machine that runs Red Hat Enterprise Linux (RHEL) 8.3
sql4	On-premises physical server that runs Windows Server 2016 and has SQL Server 2016 installed

You plan to implement Microsoft Defender for SQL.

Which SQL Server instances will be protected by Microsoft Defender for SQL?

- A. sql1 and sql2 only
- B. sql1, sql2, and sql3 only
- C. sql1, sql2, and sql4 only
- D. sql1, sql2, sql3, and sql4

Answer: D

NEW QUESTION 313

- (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.	<input type="radio"/>	<input type="radio"/>
User2 can configure firewalls and virtual networks for Vault1.	<input type="radio"/>	<input type="radio"/>
User3 can add access policies to Vault1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can configure firewalls and virtual networks for Vault1.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can add access policies to Vault1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 316

- (Exam Topic 4)

Lab Task

Task 2

You need to ensure that the events in the NetworkSecurityGroupRuleCounter log of the VNET01-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 318

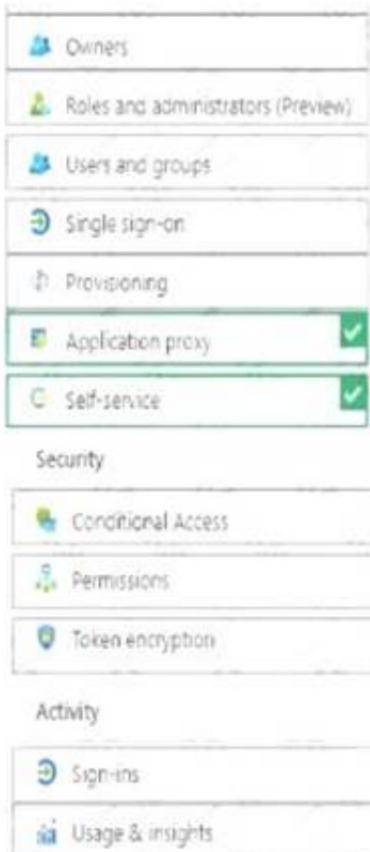
- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2 and a registered app named App1.

You create an app-specific role named Role1.

You need to assign Role1 to User1 and enable User2 to request access to App1.

Which two settings should you modify? To answer select the appropriate settings in the answer area NOTE: Each correct selection is worth one part.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

NEW QUESTION 321

- (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

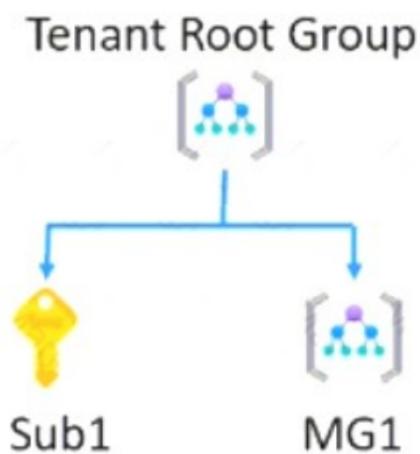
Explanation:

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 322

- (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 326

- (Exam Topic 3)

You need to perform the planned changes for OU2 and User1.

Which tools should you use? To answer, drag the appropriate tools to the correct resources. Each tool 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.

Tools

- The Azure portal
- Azure AD Connect
- The Active Directory admin center
- Active Directory Sites and Services
- Active Directory Users and Computers

Answer Area

OU2:	Tool
User1:	Tool

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
 Table Description automatically generated

NEW QUESTION 328

- (Exam Topic 3)

You need to configure support for Azure Sentinel notebooks to meet the technical requirements. What is the minimum number of Azure container registries and Azure Machine Learning workspaces required?

Container registries:

Workspaces:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
 Table Description automatically generated with medium confidence
 Reference:
<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

NEW QUESTION 332

- (Exam Topic 2)

You are evaluating the security of VM1, VM2, and VM3 in Sub2. 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 the Internet, you can connect to the web server on VM1 by using HTTP.	<input type="radio"/>	<input type="radio"/>
From the Internet, you can connect to the web server on VM2 by using HTTP.	<input type="radio"/>	<input type="radio"/>
From the Internet, you can connect to the web server on VM3 by using HTTP.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	<input checked="" type="radio"/>	<input type="radio"/>
From the Internet, you can connect to the web server on VM2 by using HTTP.	<input type="radio"/>	<input checked="" type="radio"/>
From the Internet, you can connect to the web server on VM3 by using HTTP.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 337

- (Exam Topic 2)

You are evaluating the effect of the application security groups on the network communication between the virtual machines in Sub2. 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, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input type="radio"/>
From VM2, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input type="radio"/>
From VM1, you can connect to the web server on VM4.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No. VM4 is in Subnet13 which has NSG3 attached to it. VM1 is in ASG1. NSG3 would only allow ICMP pings from ASG2 but not ASG1. Only TCP traffic is allowed from ASG1. NSG3 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

Box 2: Yes.

VM2 is in ASG2. Any protocol is allowed from ASG2 so ICMP ping would be allowed.

Box3. VM1 is in ASG1. TCP traffic is allowed from ASG1 so VM1 could connect to the web server as connections to the web server would be on ports TCP 80 or TCP 443.

NEW QUESTION 341

- (Exam Topic 1)

You need to ensure that you can meet the security operations requirements. What should you do first?

- A. Turn on Auto Provisioning in Security Center.
- B. Integrate Security Center and Microsoft Cloud App Security.
- C. Upgrade the pricing tier of Security Center to Standard.
- D. Modify the Security Center workspace configuration.

Answer: C

Explanation:

The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier also adds advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware, and more.

Scenario: Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center. References:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing>

NEW QUESTION 344

- (Exam Topic 1)

You need to ensure that the Azure AD application registration and consent configurations meet the identity and access requirements.

What should you use in the Azure portal? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

To configure the registration settings:

▼

- Azure AD – User settings
- Azure AD – App registrations settings
- Enterprise Applications – User settings

To configure the consent settings:

▼

- Azure AD – User settings
- Azure AD – App registrations settings
- Enterprise Applications – User settings

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent>

NEW QUESTION 346

- (Exam Topic 1)

You need to deploy AKS1 to meet the platform protection requirements.

Which four 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.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions	Answer Area
Deploy an AKS cluster.	
Create a client application.	
Create a server application.	
Create an RBAC binding.	
Create a custom RBAC role.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Scenario: Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials. Litewire plans to deploy AKS1, which is a managed AKS (Azure Kubernetes Services) cluster. Step 1: Create a server application

To provide Azure AD authentication for an AKS cluster, two Azure AD applications are created. The first application is a server component that provides user authentication.

Step 2: Create a client application

The second application is a client component that's used when you're prompted by the CLI for authentication. This client application uses the server application for the actual authentication of the credentials provided by the client.

Step 3: Deploy an AKS cluster.

Use the az group create command to create a resource group for the AKS cluster. Use the az aks create command to deploy the AKS cluster.

Step 4: Create an RBAC binding.

Before you use an Azure Active Directory account with an AKS cluster, you must create role-binding or cluster role-binding. Roles define the permissions to grant, and bindings apply them to desired users. These assignments can be applied to a given namespace, or across the entire cluster.

Reference:

<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration>

NEW QUESTION 348

- (Exam Topic 1)

You need to meet the identity and access requirements for Group1. What should you do?

- A. Add a membership rule to Group1.
- B. Delete Group1. Create a new group named Group1 that has a membership type of Office 365. Add users and devices to the group.
- C. Modify the membership rule of Group1.
- D. Change the membership type of Group1 to Assigne
- E. Create two groups that have dynamic membership
- F. Add the new groups to Group1.

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership> Scenario:

Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1.

The tenant currently contain this group:

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership> <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-porta>

NEW QUESTION 353

- (Exam Topic 1)

You need to ensure that users can access VM0. The solution must meet the platform protection requirements. What should you do?

- A. Move VM0 to Subnet1.
- B. On Firewall, configure a network traffic filtering rule.
- C. Assign RT1 to AzureFirewallSubnet.
- D. On Firewall, configure a DNAT rule.

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat>

NEW QUESTION 358

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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](#)