



Microsoft

Exam Questions az-500

Microsoft Azure Security Technologies

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

- (Exam Topic 4)

You plan to use Azure Log Analytics to collect logs from 200 servers that run Windows Server 2016.

You need to automate the deployment of the Microsoft Monitoring Agent to all the servers by using an Azure Resource Manager template.

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

```
{
  "type": "Microsoft.Compute/virtualMachines/extensions",
  "name": "[concat(parameter('vmname'), /OMSExtension)]",
  "apiVersion": "[variables('apiVersion')]",
  "location": "[resourceGroup().location]",
  "dependsOn": [
    "[concat('Microsoft.Compute/virtualMachines/', parameters('vmName'))]"
  ],
  "properties": {
    "publisher": "Microsoft.EnterpriseCloud.Monitoring",
    "type": "MicrosoftMonitoringAgent",
    "typeHandlerVersion": "1.0",
    "autoUpgradeMinorVersion": true,
    "settings": {
      "workspaceId": "[variable('var1')]"
    },
    "protectedSettings": {
      "workspaceKey": "[variable('var2')]"
    }
  }
}
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://blogs.technet.microsoft.com/manageabilityguys/2015/11/19/enabling-the-microsoft-monitoring-agent-in>

NEW QUESTION 2

- (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 3

- (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

* Name ⓘ

* Value

Content type (optional)

Set activation date? ⓘ

Activation Date

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

Set expiration Date? ⓘ

Expiration Date

(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 4

- (Exam Topic 4)

You have an Azure Container Registry named Registry1.

You add role assignment for Registry1 as shown in the following table.

User	Role
User1	AcrPush
User2	AcrPull
User3	AcrImageSigner
User4	Contributor

Which users can upload images to Registry1 and download images from Registry1? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Upload images: ▼

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

Download images: ▼

User2 only
User1 and User2 only
User2 ad User4 only
User1, User2, and User4
User1, User2, User3, and User4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: User1 and User4 only
 Owner, Contributor and AcrPush can push images. Box 2: User1, User2, and User4
 All, except AcrImageSigner, can download/pull images.

Role/Permission	Access Resource Manager	Create/delete registry	Push image	Pull image	Delete image data	Change policies	Sign images
Owner	X	X	X	X	X	X	
Contributor	X	X	X	X	X	X	
Reader	X			X			
AcrPush			X	X			
AcrPull				X			
AcrDelete					X		
AcrImageSigner							X

References:
<https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles>

NEW QUESTION 5

- (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 6

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

Name	Type	Resource group
RG1	Resource group	Not applicable
RG2	Resource group	Not applicable
RG3	Resource group	Not applicable
SQL1	Azure SQL Database	RG3

Transparent Data Encryption (TDE) is disabled on SQL1.
 You assign policies to the resource groups as shown in the following table.

Name	Condition	Effect if condition is false	Assignment
Policy1	TDE enabled	Deny	RG1, RG2
Policy2	TDE enabled	DeployIfNotExists	RG2, RG3
Policy3	TDE enabled	Audit	RG1

You plan to deploy Azure SQL databases by using an Azure Resource Manager (ARM) template. The databases will be configured as shown in the following table.
 NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
SQL1 will have TDE enabled automatically.	<input type="radio"/>	<input type="radio"/>
The deployment of SQL2 will fail.	<input type="radio"/>	<input type="radio"/>
SQL3 will be deployed and marked as noncompliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

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

NEW QUESTION 7

- (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 8

- (Exam Topic 4)

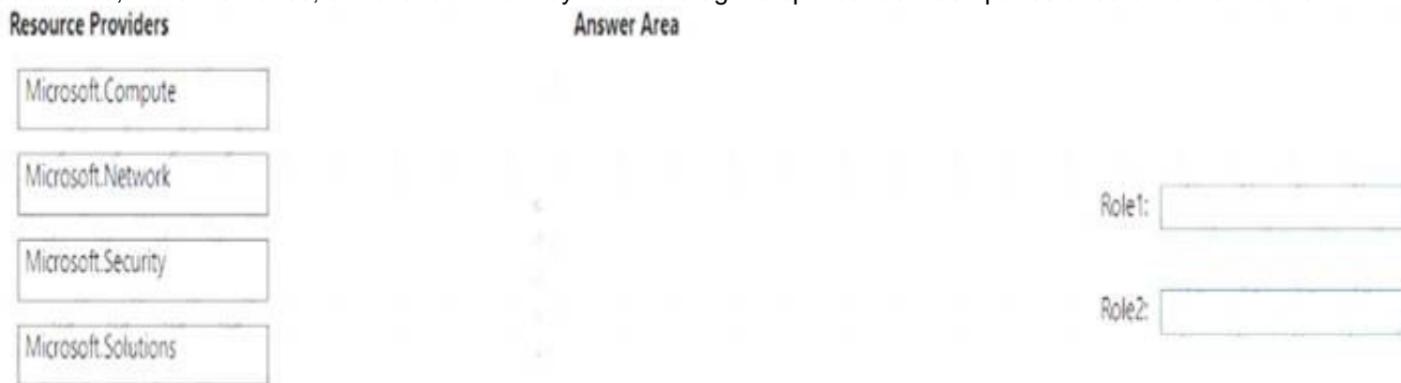
You have an Azure subscription.

You plan to create two custom roles named Role1 and Role2.

The custom roles will be used to perform the following tasks:

- Members of Role1 will manage application security groups.
- Members of Role2 will manage Azure Bastion. You need to add permissions to the custom roles.

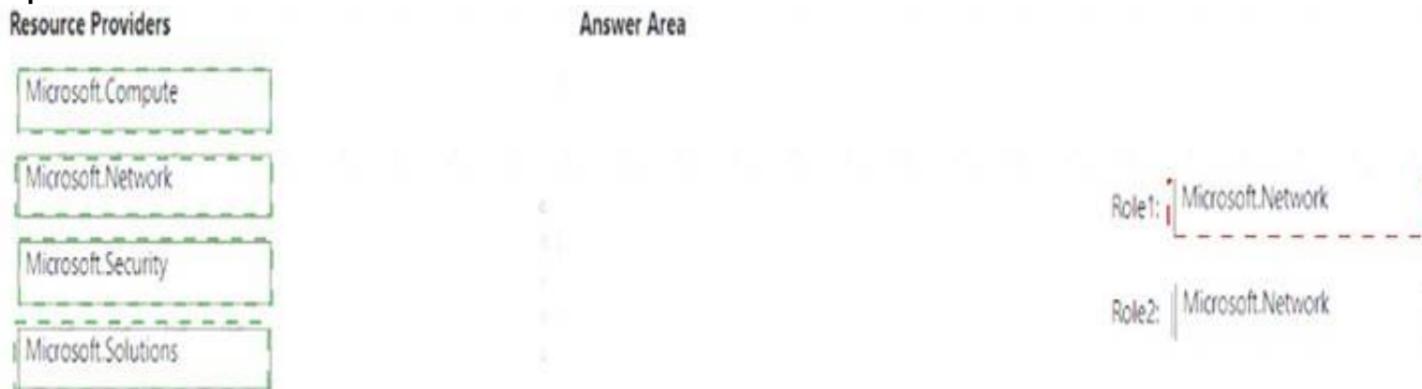
Which resource provider should you use for each role? To answer, drag the appropriate resource providers to the correct roles. Each resource provider may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 9

- (Exam Topic 4)

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

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

You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.

Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.

Solution: You recommend the use of password hash synchronization and seamless SSO. Does the solution meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 10

- (Exam Topic 4)

You have a hybrid configuration of Azure Active Directory (Azure AD).

All users have computers that run Windows 10 and are hybrid Azure AD joined.

You have an Azure SQL database that is configured to support Azure AD authentication.

Database developers must connect to the SQL database by using Microsoft SQL Server Management Studio (SSMS) and authenticate by using their on-premises Active Directory account.

You need to tell the developers which authentication method to use to connect to the SQL database from SSMS. The solution must minimize authentication prompts.

Which authentication method should you instruct the developers to use?

- A. SQL Login
- B. Active Directory – Universal with MFA support
- C. Active Directory – Integrated
- D. Active Directory – Password

Answer: C

Explanation:

Azure AD can be the initial Azure AD managed domain. Azure AD can also be an on-premises Active Directory Domain Services that is federated with the Azure AD.

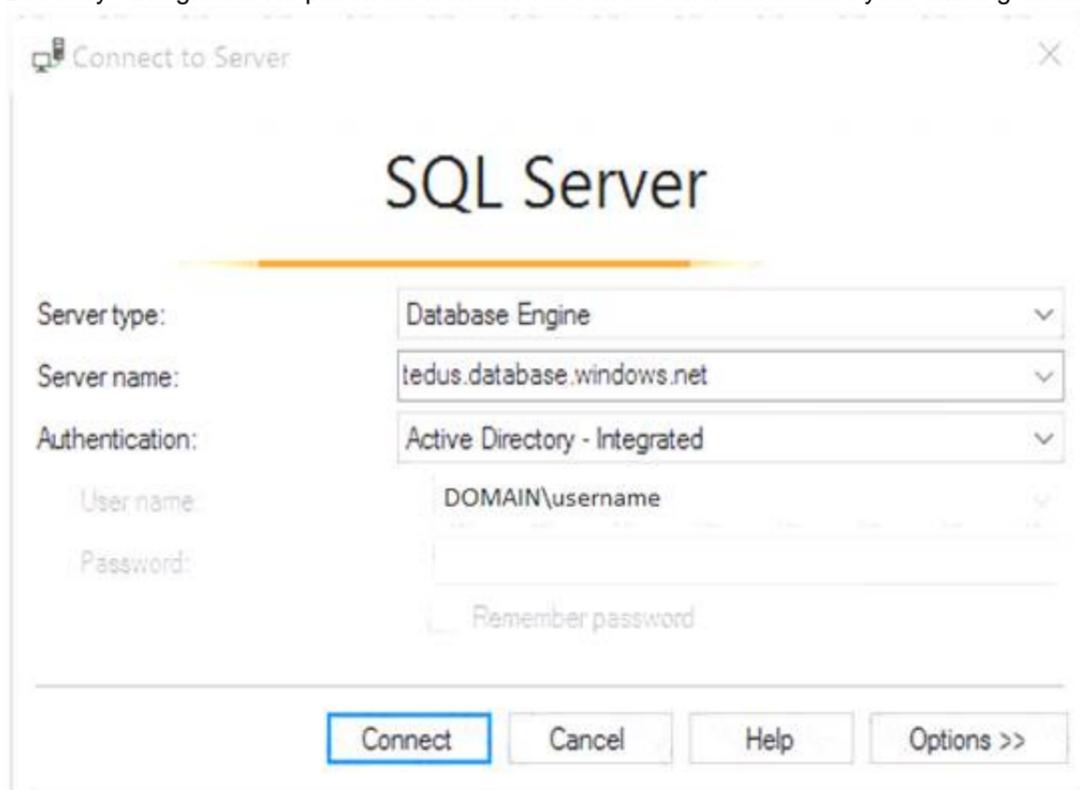
Using an Azure AD identity to connect using SSMS or SSDT

The following procedures show you how to connect to a SQL database with an Azure AD identity using SQL Server Management Studio or SQL Server Database Tools.

Active Directory integrated authentication

Use this method if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

* 1. Start Management Studio or Data Tools and in the Connect to Server (or Connect to Database Engine) dialog box, in the Authentication box, select Active Directory - Integrated. No password is needed or can be entered because your existing credentials will be presented for the connection.



* 2. Select the Options button, and on the Connection Properties page, in the Connect to database box, type the name of the user database you want to connect to. (The AD domain name or tenant ID" option is only supported for Universal with MFA connection options, otherwise it is greyed out.)

References:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/sql-database/sql-database-aad-authentication>

NEW QUESTION 10

- (Exam Topic 4)

Your network contains an Active Directory forest named contoso.com. You have an Azure Directory (Azure AD) tenant named contoso.com.

You plan to configure synchronization by using the Express Settings installation option in Azure AD Connect. You need to identify which roles and groups are required to perform the planned configurations. The solution must use the principle of least privilege.

Which two roles and groups should you identify? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: CE

Explanation:

References:

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

NEW QUESTION 15

- (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 20

- (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 23

- (Exam Topic 4)

You have an Azure subscription that is linked to an Azure AD tenant and 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

The subnets of the virtual networks have the service endpoints shown in the following table.

Subnet	Service endpoint
VNET1/Subnet1	Microsoft.Storage
VNET1/Subnet2	Microsoft.KeyVault
VNET2/Subnet1	Microsoft.Storage, Microsoft.KeyVault

You create the resources shown in the following table.

Name	Type
storage1	Azure Storage account
Vault1	Azure Key Vault

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
Connections from VM1 to storage1 always use IP address 10.1.1.5.	<input type="radio"/>	<input type="radio"/>
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	<input type="radio"/>	<input type="radio"/>
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Connections from VM1 to storage1 always use IP address 10.1.1.5.	<input checked="" type="radio"/>	<input type="radio"/>
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	<input type="radio"/>	<input checked="" type="radio"/>
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 28

- (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. the Security & Compliance admin center
- B. SQL query editor in Azure
- C. File Explorer in Windows
- D. AzCopy

Answer: D

Explanation:

References:

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

NEW QUESTION 32

- (Exam Topic 4)

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

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

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

- > Maximum activation duration (hours): 2
- > Send email notifying admins of activation: Disable
- > Require incident/request ticket number during activation: Disable
- > Require Azure Multi-Factor Authentication for activation: Enable
- > Require approval to activate this role: Enable
- > Selected approver: Group1

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

Name	Assignment type
User1	Active
User2	Eligible
user3	Eligible

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

Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	<input type="radio"/>	<input type="radio"/>
User2 can request to activate the Password Administrator role.	<input type="radio"/>	<input type="radio"/>
If User3 wants to activate the Password Administrator role, the user can approve their own request.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

YES (Already active)

YES (The user will be prompted for MFA regardless the MFA Status of the user) NO (Even the user is included in the group, a user can't approve itself)

<https://docs.microsoft.com/es-es/azure/active-directory/privileged-identity-management/pim-deployment-plan> (Require approval section)

NEW QUESTION 36

- (Exam Topic 4)

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

Name	Type
RG1	Resource group
VM1	Virtual machine

You perform the following tasks:

Create a managed identity named Managed1. Create a Microsoft 365 group named Group1.

You need to identify which service principals were created and which identities can be assigned the Reader role for RG1. What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Service Principles: App1 only
 Managed1 and VM1 only
 Managed1, VM1, and App1 only
 Managed1, VM1, App1, and Group1

Identities: App1 only
 Managed1 and VM1 only
 Managed1, VM1, and App1 only
 Managed1, VM1, App1, and Group1

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Service Principles: App1 only
 Managed1 and VM1 only
 Managed1, VM1, and App1 only
 Managed1, VM1, App1, and Group1

Identities: App1 only
 Managed1 and VM1 only
 Managed1, VM1, and App1 only
 Managed1, VM1, App1, and Group1

NEW QUESTION 41

- (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 43

- (Exam Topic 4)

You have an Azure subscription that contains a storage account and an Azure web app named App1. App1 connects to an Azure Cosmos DB database named Cosmos1 that uses a private endpoint named Endpoint1. Endpoint1 has the default settings.

You need to validate the name resolution to Cosmos1. Which DNS zone should you use?

- A. Endpoint1. Privatelink, blob, core, windows, net
- B. Endpoint1. Privatelink, database, azure, com
- C. Endpoint1. Privatelink, azurewebsites, net
- D. Endpoint1. Privatelink, documents, azure, com

Answer: D

NEW QUESTION 46

- (Exam Topic 4)

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

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

Subnet1 and Subnet2 have a Microsoft.Storage service endpoint configured.

You have an Azure Storage account named storageacc1 that is configured as shown in the following exhibit.

Save | Discard | Refresh

Allow access from

All networks Selected networks

Configure network security for your storage accounts. [Learn more.](#)

Virtual networks

Secure your storage account with virtual networks. [+ Add existing virtual network](#)
[+ Add new virtual network](#)

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIPTION
No network selected.					

Firewall

Add IP ranges to allow access from the internet on your on-premises networks. [Learn more.](#)

Address Range

13.80.73.87

IP address or CIDR

Exceptions

Allow trusted Microsoft services to access this storage account ⓘ

Allow read access to storage logging from any network

Allow read access to storage metrics from any network

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

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>
From VM2, you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>
From VM3 , you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Yes

The public IP of VM1 is allowed through the firewall.

Box 2: No

The allowed virtual network list is empty so VM2 cannot access storageacc1 directly. The public IP address of VM2 is not in the allowed IP list so VM2 cannot access storageacc1 over the Internet.

Box 3: No

The allowed virtual network list is empty so VM3 cannot access storageacc1 directly. VM3 does not have a public IP address so it cannot access storageacc1 over the Internet.

Reference:

<https://docs.microsoft.com/en-gb/azure/storage/common/storage-network-security>

NEW QUESTION 49

- (Exam Topic 4)

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

Name	Operating system
VM1	Windows 10
VM2	Windows Server 2016
VM3	Windows Server 2019
VM4	Ubuntu Server 18.04 LTS

You create an MDM Security Baseline profile named Profile1.

You need to identify to which virtual machines Profile1 can be applied. Which virtual machines should you identify?

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

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines>

NEW QUESTION 52

- (Exam Topic 4)

You plan to deploy an app that will modify the properties of Azure Active Directory (Azure AD) users by using Microsoft Graph. You need to ensure that the app can access Azure AD. What should you configure first?

- A. a custom role-based access control (RBAC) role
- B. an external identity
- C. an Azure AD Application Proxy
- D. an app registration

Answer: D

Explanation:

Reference:

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

NEW QUESTION 53

- (Exam Topic 4)

You are collecting events from Azure virtual machines to an Azure Log Analytics workspace. You plan to create alerts based on the collected events. You need to identify which Azure services can be used to create the alerts.

Which two services should you identify? Each correct answer presents a complete solution NOTE: Each correct selection is worth one point.

- A. Azure Monitor
- B. Azure Security Center
- C. Azure Analytics Services
- D. Azure Sentinel
- E. Azure Advisor

Answer: AD

Explanation:

<https://docs.microsoft.com/en-us/azure/analysis-services/analysis-services-overview>

NEW QUESTION 58

- (Exam Topic 4)

You have an Azure subscription that contains the storage accounts shown in the following, table.

Name	Performance	Account kind	Azure Data Lake Storage Gen2
storage1	Standard	BlobStorage	Enabled
storage2	Premium	BlockBlobStorage	Disabled
storage3	Standard	Storage	Disabled
storage4	Premium	FileStorage	Disabled
storage5	Standard	StorageV2	Enabled

You enable Microsoft Defender for Storage.

Which storage services of storages are monitored by Microsoft Defender for Storage, and which storage accounts are protected by Microsoft Defender for Storage? To answer, select the appropriate options in the answer area.

Answer Area

Monitored storage services:

Protected storage accounts:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Monitored storage services:

Protected storage accounts:

NEW QUESTION 61

- (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 62

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL Database logic server named SQL1 and an Azure virtual machine named VM1. VM1 uses a private IP address only.

The Firewall and virtual networks settings for SQL1 are shown in the following exhibit.

Save Discard + Add client IP

Deny public network access Yes No

i Click here to create a new private endpoint.
[Create Private Endpoint](#)

Minimum TLS Version 1.0 1.1 1.2

Connection Policy Default Proxy Redirect

Allow Azure services and resources to access this server Yes No

Client IP address: 89.212.25.106

Rule name	Start IP	End IP

No firewall rules configured.

Virtual networks
[+ Add existing virtual network](#) [+ Create new virtual network](#)

Rule name	Virtual network	Subnet
No vnet rules for this server.		

You need to ensure that VM1 can connect to SQL1. The solution must use the principle of least privilege. What should you do?

- A. Add an existing virtual network.
- B. Set Connection Policy to Proxy.
- C. Create a new firewall rule.
- D. Set Allow Azure services and resources to access this server to Yes.

Answer: C

NEW QUESTION 66

- (Exam Topic 4)

You have an Azure subscription that contains an app named App1. App1 has the app registration shown in the following table.

API	Permission	Type	Admin consent required	Status
Microsoft.Graph	User.Read	Delegated	No	None
Microsoft.Graph	Calendars.Read	Delegated	No	None

You need to ensure that App1 can read all user calendars and create appointments. The solution must use the principle of least privilege. What should you do?

- A. Add a new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.
- B. Add a new Application API permission for Microsoft.Graph Calendars.ReadWrite.
- C. Select Grant admin consent.
- D. Add a new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.Shared.

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/graph/permissions-reference#calendars-permissions>

NEW QUESTION 68

- (Exam Topic 4)

You have an Azure subscription that contains virtual machines. You enable just in time (JIT) VM access to all the virtual machines. You need to connect to a virtual machine by using Remote Desktop. What should you do first?

- A. From Azure Directory (Azure AD) Privileged Identity Management (PIM), activate the Security administrator user role.
- B. From Azure Active Directory (Azure AD) Privileged Identity Management (PIM), activate the Owner role for the virtual machine.
- C. From the Azure portal, select the virtual machine, select Connect, and then select Request access.
- D. From the Azure portal, select the virtual machine and add the Network Watcher Agent virtual machine extension.

Answer: C

Explanation:

Reference:

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

NEW QUESTION 71

- (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 75

- (Exam Topic 4)

You have an Azure subscription that contains a

You need to grant user1 access to blob1. The solution must ensure that the access expires after six days. What should you use?

- A. a shared access policy
- B. a shared access signature (SAS)
- C. role-based access control (RBAC)
- D. a managed identity

Answer: C

Explanation:

Depending on how you want to authorize access to blob data in the Azure portal, you'll need specific permissions. In most cases, these permissions are provided via Azure role-based access control (Azure RBAC). For more information about Azure RBAC, see [What is Azure role-based access control \(Azure RBAC\)?](#).

<https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal>

NEW QUESTION 80

- (Exam Topic 4)

You have an Azure subscription.

You plan to implement Azure DDoS Protection. The solution must meet the following requirement:

* Provide access to DDoS rapid response support during active attacks.

* Protect Basic SKU public IP addresses.

You need to recommend which type of DDoS projection to use for each requirement.

What should you recommend? To answer, drag the appropriate DDoS projection types to the correct requirements. Each DDoS Projection type may be used once, or not at all. You may need to drag the split bar between panes or scroll to view connect.

NOTE: Each correct selection is worth one point.

DDoS Protection types

- DDoS infrastructure protection
- DDoS IP Protection
- DDoS Network Protection

Answer Area

Provide access to DDoS rapid response support during active attacks:

Protect Basic SKU public IP addresses:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

DDoS Protection types

- DDoS infrastructure protection
- DDoS IP Protection
- DDoS Network Protection

Answer Area

Provide access to DDoS rapid response support during active attacks:

DDoS Network Protection

Protect Basic SKU public IP addresses:

DDoS IP Protection

NEW QUESTION 81

- (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 (AzureAD). 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 create a site-to-site VPN between the virtual network and the on-premises network. Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

You can 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. References:

<https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network>

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

NEW QUESTION 82

- (Exam Topic 4)

You have an Azure Active directory tenant that syncs with an Active Directory Domain Services (AD DS) domain.

You plan to create an Azure file share that will contain folders and files.

Which identity store can you use to assign permissions to the Azure file share and folders within the share? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Azure files share:

Folders in the file share:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Azure files share:

AD DS only

Folders in the file share:

AD DS and Azure AD

NEW QUESTION 86

- (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 App1.

You need to identify the owners of Group2 and the users of App1.

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 88

- (Exam Topic 4)

You have an Azure subscription that contains an Azure Data Lake Storage Gen2 account named storage1. You deploy an Azure Synapse Analytics workspace named synapsews1 to a managed virtual network. You need to enable access from synapsews1 to storage1. What should you configure?

- A. a virtual network gateway
- B. a network security group (NSG)
- C. a private endpoint
- D. peering

Answer: C

NEW QUESTION 89

- (Exam Topic 4)

You create an alert rule that has the following settings:

- > Resource: RG1
- > Condition: All Administrative operations
- > Actions: Action groups configured for this alert rule: ActionGroup1
- > Alert rule name: Alert1

You create an action rule that has the following settings:

- > Scope: VM1
- > Filter criteria: Resource Type = "Virtual Machines"
- > Define on this scope: Suppression
- > Suppression config: From now (always)
- > Name: ActionRule1

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
If you start VM1, an alert is triggered.	<input type="radio"/>	<input type="radio"/>
If you start VM2, an alert is triggered.	<input type="radio"/>	<input type="radio"/>
If you add a tag to RG1, an alert is triggered.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1:
 The scope for the action rule is set to VM1 and is set to suppress alerts indefinitely.
 Box 2:
 The scope for the action rule is not set to VM2. Box 3:
 Adding a tag is not an administrative operation. References:
<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log>
<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-action-rules>

NEW QUESTION 92

- (Exam Topic 4)

You have the Azure resource shown in the following table.

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

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

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

Answer: D

NEW QUESTION 93

- (Exam Topic 4)

You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days. How should you complete the command? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

```
New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'
```

`-Location 'East US'`

<div style="border: 1px solid black; padding: 2px;"> <div style="border-bottom: 1px solid black; padding: 2px;">-EnabledForDeployment</div> <div style="border-bottom: 1px solid black; padding: 2px;">-EnablePurgeProtection</div> <div style="padding: 2px;">-Tag</div> </div>	<div style="border: 1px solid black; padding: 2px;"> <div style="border-bottom: 1px solid black; padding: 2px;">-Confirm</div> <div style="border-bottom: 1px solid black; padding: 2px;">-DefaultProfile</div> <div style="border-bottom: 1px solid black; padding: 2px;">-EnableSoftDelete</div> <div style="padding: 2px;">-SKU</div> </div>
--	---

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: -EnablePurgeProtection

If specified, protection against immediate deletion is enabled for this vault; requires soft delete to be enabled as well.

Box 2: -EnableSoftDelete

Specifies that the soft-delete functionality is enabled for this key vault. When soft-delete is enabled, for a grace period, you can recover this key vault and its contents after it is deleted.

References:

<https://docs.microsoft.com/en-us/powershell/module/azurermskeyvault/new-azurermskeyvault>

NEW QUESTION 94

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD). The Azure AD tenant contains the users shown in the following table.

Name	Source	Password
User1	Azure AD	Adatum123
User2	Azure AD	N3w3rT0Gue33
User3	On-premises Active Directory	ComplexPassword33

You configure the Authentication methods – Password Protection settings for adatum.com as shown in the following exhibit.

Custom smart lockout

Lockout threshold ⓘ ✓

Lockout duration in seconds ⓘ ✓

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ ✓

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

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 will be prompted to change the password on the next sign-in.	<input type="radio"/>	<input type="radio"/>
User2 can change the password to @d@tum_C0mpleX123.	<input type="radio"/>	<input type="radio"/>
User3 can change the password to Adatum123!	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-de> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad>

NEW QUESTION 96

- (Exam Topic 4)

You have an Azure subscription that uses Microsoft Defender for Cloud. You have accounts for the following cloud services:

- Alibaba Cloud
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

What can you add to Defender for Cloud?

- A. AWS only
- B. Alibaba Cloud and AWS only
- C. Alibaba Good and GCP only
- D. AWS and GCP only
- E. Alibaba Cloud, AW
- F. and GCP

Answer: A

NEW QUESTION 97

- (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.

Operating systems:

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

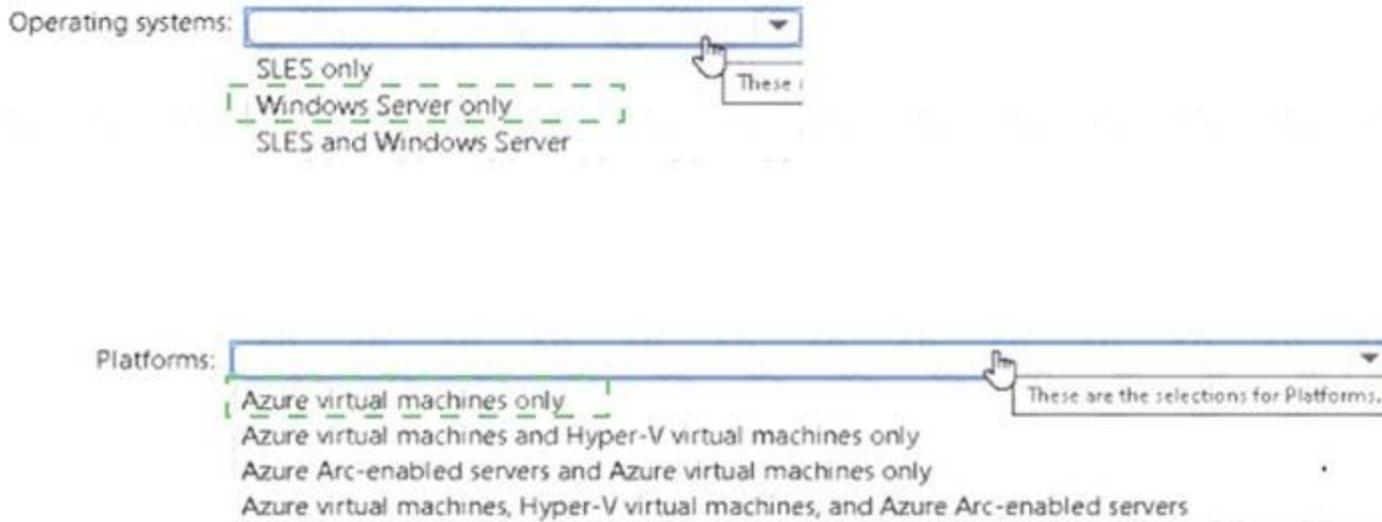
Platforms:

- 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:



NEW QUESTION 100

- (Exam Topic 4)

You have a web app named WebApp1.

You create a web application firewall (WAF) policy named WAF1. You need to protect WebApp1 by using WAF1.

What should you do first?

- A. Deploy an Azure Front Door.
- B. Add an extension to WebApp1.
- C. Deploy Azure Firewall.

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door>

NEW QUESTION 101

- (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 106

- (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 6

You need to email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes, you can follow these steps:

- In the Azure portal, search for and select the virtual machine named VM1.
- In the left pane, select Alerts.
- Select New alert rule.
- In the New alert rule pane, enter the following information:
 - Name: Enter a name for the alert rule.
 - Description: Enter a description for the alert rule.
 - Condition: Select Metric measurement.
 - Resource: Select the virtual machine named VM1.
 - Metric: Select Percentage CPU.
 - Operator: Select Greater than.
 - Threshold: Enter 70.
 - Aggregation type: Select Average.
 - Period: Select 15 minutes.
- In the Actions pane, select Add action group.
- In the Add action group pane, enter the following information:
 - Name: Enter a name for the action group.
 - Short name: Enter a short name for the action group.
 - Email recipient: Enter the email address of the user you want to receive the alert. For example, admin1@contoso.com.
 - Select OK.

NEW QUESTION 107

- (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 112

- (Exam Topic 4)

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

Name	Type
storage1	Storage account
KeyVault1	Azure key vault

You need to configure storage1 to regenerate keys automatically every 90 days. Which cmdlet should you run?

- A. set -A=StorageAccount
- B. Add-A:StorageAccountmanagementPolicyAction
- C. Set-A:StorageAccountmanagementPolicy
- D. Add-AsKeyVaultmanageStorageAccount

Answer: D

NEW QUESTION 116

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. The User administrator role is assigned to a user named Admin1. An external partner has a Microsoft account that uses the user1@outlook.com sign in. Admin1 attempts to invite the external partner to sign in to the Azure AD tenant and receives the following error message: "Unable to invite user user1@outlook.com Generic authorization exception." You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant. What should you do?

- A. From the Roles and administrators blade, assign the Security administrator role to Admin1.
- B. From the Organizational relationships blade, add an identity provider.
- C. From the Custom domain names blade, add a custom domain.
- D. From the Users blade, modify the External collaboration settings.

Answer: D

Explanation:

You need to allow guest invitations in the External collaboration settings.

NEW QUESTION 120

- (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 125

- (Exam Topic 4)

You have an Azure subscription that contains two virtual machines named VM1 and VM2 that run Windows Server 2019. You are implementing Update Management in Azure Automation. You plan to create a new update deployment named Update1. You need to ensure that Update1 meets the following requirements:

- Automatically applies updates to VM1 and VM2.
- Automatically adds any new Windows Server 2019 virtual machines to Update1. What should you include in Update1?

- A. a security group that has a Membership type of Dynamic Device
- B. a security group that has a Membership type of Assigned
- C. a Kusto query language query
- D. a dynamic group query

Answer: D

NEW QUESTION 126

- (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	<i>Not applicable</i>	<i>None</i>	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 128

- (Exam Topic 4)

You create an Azure subscription with Azure AD Premium P2.

You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure roles.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

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

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 133

- (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 134

- (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 138

- (Exam Topic 4)

You have an Azure subscription that contains a user named User1 and a storage account named storage 1. The storage1 account contains the resources shown in the following table:

Name	Type
container1	Container
folder1	File share
table1	Table

User1 is assigned the following roles for storage1:

- Storage Blob Data Reader
- Storage Table Data Contributor
- Storage File Data SMB Share Reader

Statements	Yes	No
On October 1, 2022, if User1 accesses folder1 by using SAS1, he can delete the files in folder1.	<input type="radio"/>	<input type="radio"/>
On October 1, 2022, if User1 maps folder1 as a network drive by using his Azure Active Directory (Azure AD) credentials, he can delete the files in folder1.	<input type="radio"/>	<input type="radio"/>
On October 1, 2022, User1 can delete the rows in table1 by using SAS1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
No, Yes, No

NEW QUESTION 143

- (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 147

- (Exam Topic 4)

HOTSPOT

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

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

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

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and
| Summarize failed_login_attempts=
latest_failed_login=arg_max(TimeGenerated by Account
| where failed login attempts > 5
```

Dropdown menu options: ActivityID, DataType, EventID, QuantityUnit

Dropdown menu options: Count(), Countif(), Makeset(), Split()

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
The following example identifies user accounts that failed to log in more than five times in the last day, and when they last attempted to log in.

```
let timeframe = 1d; SecurityEvent
| where TimeGenerated > ago(1d)
| where AccountType == 'User' and EventID == 4625 // 4625 - failed log in
| summarize failed_login_attempts=count(), latest_failed_login=arg_max(TimeGenerated, Account) by Account
| where failed_login_attempts > 5
| project-away Account1 References:
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples
```

NEW QUESTION 152

- (Exam Topic 4)

You have an Azure subscription named Sub1. Sub1 has an Azure Storage account named Storage1 that contains the resources shown in the following table.

Name	Type
Container1	Blob container
Share1	File share

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

Which tool can you use to access the contents in Container1 and Share1 by using the SAS? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Tools for Container1:

- Robocopy.exe
- Azure Storage Explorer
- File Explorer

Tools for Share1:

- Robocopy.exe
- Azure Storage Explorer
- File Explorer

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Tools for Container1:

- Robocopy.exe
- Azure Storage Explorer
- File Explorer

Tools for Share1:

- Robocopy.exe
- Azure Storage Explorer
- File Explorer

NEW QUESTION 157

- (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 162

- (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 166

- (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 passowrds [\(learn more\)](#)

- 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 169

- (Exam Topic 4)

You have an Azure subscription that contains an Azure key vault. The role assignments for the key vault are shown in the following exhibit.

```
[
  {
    "RoleAssignmentId": "3336fcfb-33d8-4c8a-85b6-d8edd964762b",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa",
    "DisplayName": "User1",
    "SignInName": "User1@contoso.com",
    "RoleDefinitionName": "Owner",
    ...
  },
  {
    "RoleAssignmentId": "9d080a14-246e-4500-8b8b-077bfec22f7c",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
    "DisplayName": "User2",
    "SignInName": "User2@contoso.com",
    "RoleDefinitionName": "Key Vault Crypto Officer",
    "RoleAssignmentId": "i",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
    "DisplayName": "User3",
    "SignInName": "User3@contoso.com",
    "RoleDefinitionName": "Key Vault Secrets Officer",
    ...
  },
  {
    "RoleAssignmentId": "f1e46302-c5d0-4519-9ee7-128594eea97c",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG3/providers/Microsoft.KeyVault/vaults/KeyVault1/keys/Key1",
    "DisplayName": "User4",
    "SignInName": "User4@contoso.com",
    "RoleDefinitionName": "Key Vault Administrator",
    ...
  }
]
```

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

Answer Area

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

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

NEW QUESTION 171

- (Exam Topic 4)

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

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

You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.

Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.

Solution: You recommend the use of pass-through authentication and seamless SSO with password hash synchronization.

Does the solution meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

NEW QUESTION 174

- (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 179

- (Exam Topic 4)

You have an Azure subscription that contains a user named User1 and an Azure Container Registry named ConReg1.

You enable content trust for ContReg1.

You need to ensure that User1 can create trusted images in ContReg1. The solution must use the principle of least privilege.

Which two roles should you assign to User1? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. AcrQuarantineReader
- B. Contributor
- C. AcrPush
- D. AcrImageSigner
- E. AcrQuarantineWriter

Answer: CD

Explanation:

References:

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

NEW QUESTION 182

- (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 1

You need to configure Azure to allow RDP connections from the Internet to a virtual machine named VM1. The solution must minimize the attack surface of VM1.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To configure Azure to allow RDP connections from the Internet to a virtual machine named VM1, you can follow the steps below:

- Create a new inbound security rule in the network security group (NSG) that is associated with the virtual network subnet that contains VM1. The rule should allow RDP traffic from the Internet to the virtual network subnet. You can use the Azure portal, Azure PowerShell, or Azure CLI to create the rule.
- Configure the network security group (NSG) to associate it with the virtual network subnet that contains VM1.
- Configure the virtual machine to allow RDP traffic. You can use the Azure portal, Azure PowerShell, or Azure CLI to configure the virtual machine.

To minimize the attack surface of VM1, you can use the following best practices:

- Use a strong password for the local administrator account on the virtual machine.
- Use Network Security Groups (NSGs) to restrict traffic to only the necessary ports and protocols.
- Use Azure Security Center to monitor and protect your virtual machines.

NEW QUESTION 185

- (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 189

- (Exam Topic 4)

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

Azure Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents.

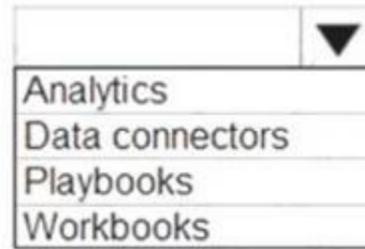
You need to identify which Azure Sentinel components to configure to meet the following requirements:

- When Azure Sentinel identifies a threat, an incident must be created.
- A ticket must be logged in the service management platform when an incident is created in Azure Sentinel.

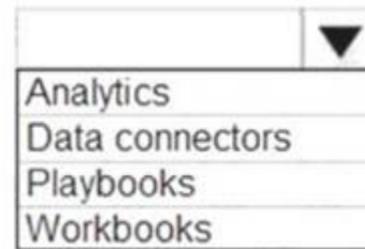
Which component should you identify for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

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



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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 191

- (Exam Topic 4)

You have two Azure subscriptions named Sub1 and Sub2. Sub1 contains a resource group named RG1 and an Azure policy named Policy1.

You need to remediate the non-compliant resources in Sub1 based on Policy1.

How should you complete the PowerShell script? To answer, drag the appropriate values to the correct targets. Each value 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.

Values

- Get-AzPolicyRemediation
- Set-AzContext
- Set-AzResourceGroup
- Start-AzPolicyComplianceScan
- Start-AzPolicyRemediation

Answer Area

```
$policyAssignmentId = "/subscriptions/f0710c27-9663-4c05-19f8-1b4be01e86a5/providers/Microsoft.Authorization/f
```

Value -Subscription "Sub1"

Value -PolicyAssignmentId \$policyAssignmentId -Name "policy1" -ResourceDiscovery

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

> For the first blank, use Set-AzContext to set the current subscription context.

> For the second blank, use Start-AzPolicyRemediation policy assignment.

to create and start a policy remediation for a

The final script should look like this:

```
$policyAssignmentId = "/subscriptions/f0710c27-9663-4c05-1978-1bdbedle86as/providers/Microsoft.
Authorization/f Value Set-AzContext
-Subscription "Sub1" ValuSetart-AzPolicyRemediation
-PolicyAssignmentId $policyAssignmentId -Name "policy1" -ResourceDiscovery
```

NEW QUESTION 196

- (Exam Topic 4)

Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.

You need to configure each subscription to have the same role assignments. What should you use?

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

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview#blueprint-definition> <https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>

NEW QUESTION 198

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group2	Disabled

The tenant contains the named locations shown in the following table.

Name	IP address range	Trusted location
Seattle	193.77.10.0/24	Yes
Boston	154.12.18.0/24	No

You create the conditional access policies for a cloud app named App1 as shown in the following table.

Name	Include	Exclude	Condition	Grant
Policy1	Group1	Group2	Locations: Boston	Block access
Policy2	Group1	None	Locations: Any location	Grant access, Require multi-factor authentication
Policy3	Group2	Group1	Locations: Boston	Block access
Policy4	User2	None	Locations: Any location	Grant access, Require multi-factor authentication

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 access App1 from an IP address of 154.12.18.10.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 193.77.10.15.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 154.12.18.34.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access App1 from an IP address of 193.77.10.15.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 154.12.18.34.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 201

- (Exam Topic 4)

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant.

When a developer attempts to register an app named App1 in the tenant, the developer receives the error message shown in the following exhibit.

You do not have access ×



Access denied

You do not have access

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

Summary 	
Session ID	Resource ID
f8e55e67d10141b4bf0c7ac5115b3be7	Not available
Extension	Content
Microsoft_AAD_RegisteredApps	CreateApplicationBlade
Error code	
403	

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

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 202

- (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:

Assignable scope:

- 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 204

- (Exam Topic 4)

You have a Azure subscription.

You enable Azure Active Directory (Azure AD) Privileged identify (PIM).

Your company's security policy for administrator accounts has the following conditions:

* The accounts must use multi-factor authentication (MFA).

* The account must use 20-character complex passwords.

* The passwords must be changed every 180 days.

* The account must be managed by using PIM.

You receive alerts about administrator who have not changed their password during the last 90 days. You need to minimize the number of generated alerts.

Which PIM alert should you modify?

- A. Roles don't require multi-factor authentication for activation.
- B. Administrator aren't using their privileged roles
- C. Roles are being assigned outside of Privileged identity Management
- D. Potential state accounts in a privileged role.

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure>

NEW QUESTION 209

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains a user named Admin1. Admin1 is assigned the Application developer role.

You purchase a cloud app named App1 and register App1 in Azure AD.

Admin1 reports that the option to enable token encryption for App1 is unavailable.

You need to ensure that Admin1 can enable token encryption for App1 in the Azure portal. What should you do?

- A. Upload a certificate for App1.
- B. Modify the API permissions of App1.
- C. Add App1 as an enterprise application.
- D. Assign Admin1 the Cloud application administrator role.

Answer: C

Explanation:

This is a tricky one because uploading a certificate is also required. However, the question states that the Token Encryption option is unavailable. This is because the app is not added as an enterprise application. When the app is added as an enterprise application, the Token Encryption option will be available. Then you can upload the certificate.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/howto-saml-token-encryption>

NEW QUESTION 213

- (Exam Topic 4)

You have an Azure subscription named Subcription1 that contains an Azure Active Directory (Azure AD) tenant named contosos.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 Subcription1

Answer: A

Explanation:

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

NEW QUESTION 215

- (Exam Topic 4)

You create resources in an Azure subscription as shown in the following table.

Name	Type	Region
RG1	Resource group	West Europe
VNET1	Azure virtual network	West Europe
Contoso1901	Azure Storage account	West Europe

VNET1 contains two subnets named Subnet1 and Subnet2. Subnet1 has a network ID of 10.0.0.0/24. Subnet2 has a network ID of 10.1.1.0/24.

Contoso1901 is configured as shown in the exhibit. (Click the Exhibit tab.)

```
PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet
ByPass          : Logging, Metrics
DefaultAction   : Deny
IpRules         : [193.77.0.0/16,...]
VirtualNetworkRules : [/subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1,...]

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.IpRules
Action IPAddressOrRange
-----
Allow  193.77.0.0/16

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRules
Action VirtualNetworkResourceId                               State
-----
Allow  /subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1 Succeeded

PS C:\> _
```

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
An Azure virtual machine on Subnet1 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>
An Azure virtual machine on Subnet2 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Yes
 Access from Subnet1 is allowed. Box 2: No
 No access from Subnet2 is allowed. Box 3: Yes
 Access from IP address 193.77.10.2 is allowed.

NEW QUESTION 218

- (Exam Topic 4)

Your company uses Azure DevOps.

You need to recommend a method to validate whether the code meets the company's quality standards and code review standards.

What should you recommend implementing in Azure DevOps?

- A. branch folders
- B. branch permissions
- C. branch policies
- D. branch locking

Answer: C

Explanation:

Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.

References:

<https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azuredevops&viewFallbackFrom=vsts>

NEW QUESTION 223

- (Exam Topic 4)

You need to recommend which virtual machines to use to host App1. The solution must meet the technical requirements for KeyVault1.

Which virtual machines should you use?

- A. VM1 only
- B. VM1 and VM2 only

- C. VM1, VM2, and VM4 only
- D. VM1, VM2, VM3, and VM4

Answer: D

NEW QUESTION 225

- (Exam Topic 4)

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

Name	Location	Virtual network name
VM1	East US	VNET1
VM2	West US	VNET2
VM3	East US	VNET1
VM4	West US	VNET3

All the virtual networks are peered. You deploy Azure Bastion to VNET2. Which virtual machines can be protected by the bastion host?

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

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/bastion/vnet-peering>

NEW QUESTION 226

- (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 227

- (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 230

- (Exam Topic 4)

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

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

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

Name	Usage location
User1	United States
User2	Germany

You create the groups shown in the following table.

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

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

Dynamic membership rules

Save Discard Got feedback?

Configure Rules Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

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

+ Add expression + Get custom extension properties

Rule syntax

Edit

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

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

Statements

Yes No

User1 is a member of Group1 and Group2.

User2 is a member of Group2 only.

Managed1 is a member of Group1 and Group2.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated

Reference:

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

NEW QUESTION 233

- (Exam Topic 4)

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

Name	Type
VM1	Virtual machine
VNET1	Virtual network
storage1	Storage account
Vault1	Key vault

You plan to enable Azure Defender for the subscription. Which resources can be protected by using Azure Defender?

- A. VM1, VNET1, storage1, and Vault1
- B. VM1, VNET1, and storage1 only
- C. VM1, storage1, and Vault1 only
- D. VM1 and VNET1 only
- E. VM1 and storage1 only

Answer: A

Explanation:

Reference:

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

NEW QUESTION 238

- (Exam Topic 4)

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

Name	Operating system	State
VM1	Windows Server 2008 R2 Service Pack 1 (SP1)	Running
VM2	Windows Server 2012 R2	Running
VM3	Windows Server 2016	Stopped
VM4	Ubuntu Server 18.04 LTS	Running

For which virtual machine can you enable Update Management?

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

Answer: C

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/automation/automation-update-management?toc=%2Fazure%2Fautomat>

NEW QUESTION 243

- (Exam Topic 4)

You have an Azure subscription that contains several Azure SQL databases and an Azure Sentinel workspace.

You need to create a saved query in the workspace to find events reported by Advanced Threat Protection for Azure SQL Database.

What should you do?

- A. From Azure CLI run the Get-AzOperationalInsightsworkspace cmdlet.
- B. From the Azure SQL Database query editor, create a Transact-SQL query.
- C. From the Azure Sentinel workspace, create a Kusto Query Language query.
- D. From Microsoft SQL Server Management Studio (SSMS), create a Transact-SQL query.

Answer: C

NEW QUESTION 245

- (Exam Topic 4)

You have an Azure subscription linked to an Azure Active Directory Premium Plan 1 tenant. You plan to implement Azure Active Directory (Azure AD) Identity Protection.

You need to ensure that you can configure a user risk policy and a sign-in risk policy. What should you do first?

- A. Purchase Azure Active Directory Premium Plan 2 licenses for all users.
- B. Register all users for Azure Multi-Factor Authentication (MFA).
- C. Enable security defaults for Azure AD.
- D. Upgrade Azure Security Center to the standard tier.

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa>

NEW QUESTION 249

- (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 are assigned to the following role definition:

```

"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 251

- (Exam Topic 4)

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

Name	Type
VM1	Virtual machine
VNET1	Virtual network
storage1	Storage account
Vault1	Key vault

You plan to enable Microsoft Defender for Cloud for the subscription. Which resources can be protected by using Microsoft Defender for Cloud?

- A. VM1, VNET1, and storage1 only
- B. VM1, storage1, and Vault1 only
- C. VM1, VNET1, storage1, and Vault1
- D. VM1 and storage1 only
- E. VM1 and VNET only

Answer: C

NEW QUESTION 253

- (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 258

- (Exam Topic 4)

You have an Azure subscription that contains the Azure Log Analytics workspaces shown in the following table.

Name	Location	Description
Workspace1	East US	Used by Azure Sentinel
Workspace2	West US	Not applicable

You create the virtual machines shown in the following table.

Name	Location	Operating system	Connected to
VM1	East US	Windows Server 2019	None
VM2	East US	Windows Server 2019	Workspace2
VM3	West US	Windows Server 2019	None
VM4	West US	Windows Server 2019	Workspace2

You plan to use Azure Sentinel to monitor Windows Defender Firewall on the virtual machines. Which virtual machines you can connect to Azure Sentinel?

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

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall>

NEW QUESTION 259

- (Exam Topic 4)

You have an Azure subscription named Sub1.

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

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

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

Answer: D

Explanation:

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

References:

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

NEW QUESTION 264

- (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 265

- (Exam Topic 4)

Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.

You need to configure each subscription to have the same role assignments. What should you use?

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

Answer: D

Explanation:

Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- > Role Assignments
- > Policy Assignments
- > Azure Resource Manager templates
- > Resource Groups

Reference:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>

NEW QUESTION 268

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL database named SQL1 and an Azure key vault named KeyVault1. KeyVault1 stores the keys shown in the following table.

Name	Type	RSA key size	Elliptic curve name
Key1	RSA	2048	Not applicable
Key2	RSA	3072	Not applicable
Key3	RSA	4096	Not applicable
Key4	EC	Not applicable	P-512

You need to configure Transparent Data Encryption (TDE). TDE will use a customer-managed key for SQL1?

- A. Key1, Key2, Key3, and Key4
- B. Key1 only
- C. Key2 only
- D. Key1 and key2 only
- E. Key2 and Key3 only

Answer: E

NEW QUESTION 269

- (Exam Topic 4)

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

Name	Type
DB1	Azure Cosmos DB account
VM1	Virtual machine
VM2	Virtual machine
VNET1	Virtual network
NSG1	Network security group (NSG)

Both VM1 and VM2 connect to VNET1 and are configured to use NSG1. You need to ensure that only VM1 and VM2 can access DB1. What should you do?

- A. Add the IP address range of VNET1 to the Firewall setting of DB1.
- B. For NSG1, configure a rule that has a service tag.
- C. Create an application security group.
- D. Configure DB1 to allow access from only VNET1.

Answer: B

NEW QUESTION 270

- (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 272

- (Exam Topic 4)

You have an Azure subscription that uses Microsoft Sentinel.

You need to create a Microsoft Sentinel notebook that will use the Guided Investigation - Anomaly Lookup template.

What should you create first?

- A. an analytics rule
- B. a Log Analytics workspace
- C. an Azure Machine Learning workspace
- D. a hunting query

Answer: A

NEW QUESTION 277

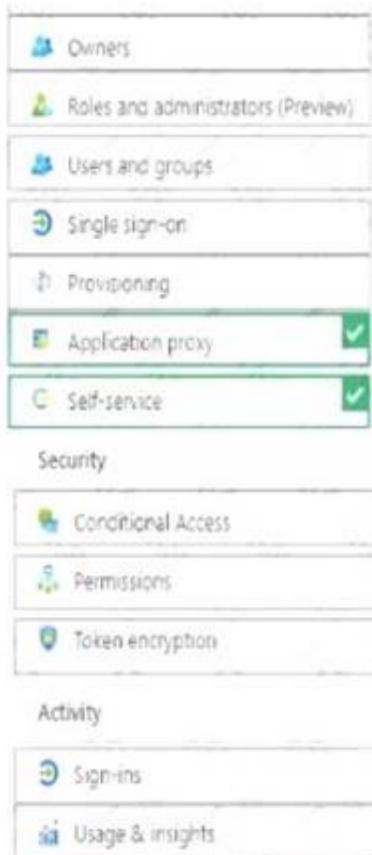
- (Exam Topic 4)

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 279

- (Exam Topic 4)

You are evaluating the security of 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.

5 / 5

Answer Area

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	<input type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the private IP address of VM3.	<input type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the private IP address of VM5.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Q1: No { and it should not be allowed as only TCP 80 is allowed from the "Internet" service tag

Q2: Yes {as it should be for VMs in the same local subnet pinging each other on private IP and no NSG configured}

Q3: Yes {VM5 is in subnet where 1st rule of NSG allows any traffic from any source to the destination}

NEW QUESTION 282

- (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: ▼

0
1
2
3

Workspaces: ▼

0
1
2
3

- 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 285

- (Exam Topic 2)

You need to meet the technical requirements for VNetwork1. What should you do first?

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

Answer: A

Explanation:

From scenario: Deploy Azure Firewall to VNetwork1 in Sub2.

Azure firewall needs a dedicated subnet named AzureFirewallSubnet. References:

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

NEW QUESTION 288

- (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 292

- (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 294

- (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 Assign
- 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-portal>

NEW QUESTION 299

.....

Relate Links

100% Pass Your az-500 Exam with ExamBible Prep Materials

<https://www.exambible.com/az-500-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>