

# Microsoft

## Exam Questions az-500

Microsoft Azure Security Technologies



### 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 named Subscription1 that contains the resources shown in the following table.

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

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

- > An Azure Sentinel workspace
- > An Azure Event Grid instance

You need to ingest the CEF messages from the NVAs to Azure Sentinel.

What should you configure for each subscription? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Subscription1:

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

Subscription2:

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 4**

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso1812.onmicrosoft.com that contains the users shown in the following table.

Name	Username	Type
User1	User1@contoso1812.onmicrosoft.com	Member
User2	User2@contoso1812.onmicrosoft.com	Member
User3	User3@contoso1812.onmicrosoft.com	Member
User4	User4@outlook.com	Guest

You create an Azure Information Protection label named Label1. The Protection settings for Label1 are configured as shown in the exhibit. (Click the Exhibit tab.)

**Protection**

Contoso1812 - Azure Information Protection

**Protections settings**

- Azure (cloud key)
- HYOK (AD RMS)

Select the protection action type

- Set permissions
- Set user-defined permissions (Preview)

USERS	PERMISSIONS
AuthenticatedUsers	Viewer
User1@contoso1812.onmicrosoft.com	Co-Author
User2@contoso1812.onmicrosoft.com	Reviewer

[+Add permissions](#)

Label1 is applied to a file named File1.

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

Statements	Yes	No
User1 can print File1.	<input type="radio"/>	<input type="radio"/>
User3 can read File1.	<input type="radio"/>	<input type="radio"/>
User4 can print File1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can print File1.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can read File1.	<input checked="" type="radio"/>	<input type="radio"/>
User4 can print File1.	<input type="radio"/>	<input checked="" type="radio"/>

**NEW QUESTION 5**

- (Exam Topic 4)

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

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

User1 is a member of Group1. Group1 and User2 are assigned the Key Vault Contributor role for Vault1. On January 1, 2019, you create a secret in Vault1. The secret is configured as shown in the exhibit. (Click the Exhibit tab.)

### Create a secret

Upload options

Manual

\* Name ⓘ

Password1

\* Value

••••••••••

Content type (optional)

Set activation date? ⓘ

Activation Date

2019-03-01 12:00:00 AM

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

Set expiration Date? ⓘ

Expiration Date

2020-03-01 12:00:00 AM

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

Enabled?  Yes  No

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

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

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

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

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 6**

- (Exam Topic 4)

You have an Azure 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 7**

- (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 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

**Resource Providers**

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

**Answer Area**

Role1:

Role2:

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Resource Providers**

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

**Answer Area**

Role1: Microsoft.Network

Role2: Microsoft.Network

**NEW QUESTION 9**

- (Exam Topic 4)

You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the Exhibit tab.)

**BASICS**

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

**AUTHENTICATION**

Enable RBAC No

**NETWORKING**

HTTP application routing Yes  
 Network configuration Basic

**MONITORING**

Enable container monitoring No

**TAGS**

You plan to deploy the cluster to production. You disable HTTP application routing.

You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.

What should you do?

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

**Answer: A**

**Explanation:**

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.

References:

<https://docs.microsoft.com/en-us/azure/aks/ingress-tls>

**NEW QUESTION 10**

- (Exam Topic 4)

You have an app that uses an Azure SQL database.

You need to be notified if a SQL injection attack is launched against the database. What should you do?

- A. Modify the Diagnostics settings for the database.
- B. Deploy the SQL Health Check solution in Azure Monitor.
- C. Enable Azure Defender for SQL for the database.
- D. Enable server-level auditing for the database.

**Answer: C**

**NEW QUESTION 10**

- (Exam Topic 4)

You plan to deploy Azure container instances.

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

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

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

What should you include in the deployment?

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

**Answer: D**

**Explanation:**

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

Reference:

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

**NEW QUESTION 11**

- (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)

You have an Azure subscription that uses Microsoft Defender for Cloud. The subscription contains the Azure Policy definitions shown in the following table.

Name	Type	Category
Policy1	Policy	Regulatory Compliance
Policy2	Policy	Security Center
Initiative1	Initiative	Regulatory Compliance
Initiative2	Initiative	Security Center

Which definitions can be assigned as a security policy in Defender for Cloud?

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

**Answer: D**

**NEW QUESTION 17**

- (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 connect to each virtual machine and add a Windows feature. Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

**Explanation:**

Microsoft Antimalware is deployed as an extension and not a feature. References:

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

**NEW QUESTION 21**

- (Exam Topic 4) You have an Azure SQL database. You implement Always Encrypted.

You need to ensure that application developers can retrieve and decrypt data in the database.

Which of the following pieces of information should you provide to the developers? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

**Answer: CE**

**Explanation:**

Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.

References:

<https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine>

**NEW QUESTION 23**

- (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 24**

- (Exam Topic 4)

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

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

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

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

On which virtual machines is the Log Analytics agent installed?

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

**Answer:** D

**Explanation:**

When automatic provisioning is On, Security Center provisions the Log Analytics Agent on all supported Azure VMs and any new ones that are created.

Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>

**NEW QUESTION 29**

- (Exam Topic 4)

You have five Azure subscriptions linked to a single Azure Active Directory (Azure AD) tenant. You create an Azure Policy initiative named SecurityPolicyInitiative1.

You identify which standard role assignments must be configured on all new resource groups.

You need to enforce SecurityPolicyInitiative1 and the role assignments when a new resource group is created. 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**

- Publish an Azure Blueprints version
- Assign an Azure blueprint.
- Create a policy assignment.
- Create a custom role-based access control (RBAC) role.
- Create a dedicated management subscription.
- Create an Azure Blueprints definition.
- Create an initiative assignment.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal> <https://docs.microsoft.com/en-us/azure/azure-australia/azure-policy>

**NEW QUESTION 32**

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL database named sql1. You plan to audit sql1.

You need to configure the audit log destination. The solution must meet the following requirements:

- Support querying events by using the Kusto query language.
- Minimize administrative effort. What should you configure?

- A. an event hub
- B. a storage account
- C. a Log Analytics workspace

**Answer: C**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-log-analytics-wizard>

**NEW QUESTION 35**

- (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. Apply an Azure policy to RG1.
- B. From Azure Security Center, configure adaptive application controls.
- C. Configure Azure Active Directory (Azure AD) Identity Protection.
- D. Apply a resource lock to RG1.

**Answer: B**

**Explanation:**

Adaptive application control is an intelligent, automated end-to-end application whitelisting solution from Azure Security Center. It helps you control which applications can run on your Azure and non-Azure VMs (Windows and Linux), which, among other benefits, helps harden your VMs against malware. Security Center uses machine learning to analyze the applications running on your VMs and helps you apply the specific whitelisting rules using this intelligence.

Reference:

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

**NEW QUESTION 37**

- (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 Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription. Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

**Explanation:**

References:

<https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-configure-using-azure-a>

**NEW QUESTION 40**

- (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 44**

- (Exam Topic 4)

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

Name	Days to retain deleted vaults	Purge protection	Permission model
KeyVault1	10	Enabled	Azure role-based access control (Azure RBAC)
KeyVault2	15	Disabled	Azure role-based access control (Azure RBAC)

The subscription contains the users shown in the following table.

Name	Role	Assigned to
Admin1	Key Vault Contributor	KeyVault1
Admin2	Key Vault Secrets Officer	KeyVault2
Admin3	Key Vault Administrator	KeyVault1

On June 1, you perform the following actions:

- Delete a key named key1 from KeyVault1.
- Delete a secret named secret 1 from KeyVault2.

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

Statements	Yes	No
Admin1 can recover key1 on June 5.	<input type="radio"/>	<input type="radio"/>
Admin2 can purge secret1 on June 12.	<input type="radio"/>	<input type="radio"/>
Admin3 can recover key1 on June 17.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Yes  
Yes No

**NEW QUESTION 46**

- (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 47**

- (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 51**

- (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 storage5 services:

Protected storage accounts:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Monitored storage5 services:

Protected storage accounts:

**NEW QUESTION 53**

- (Exam Topic 4)

Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Seattle	10.10.0.0/16	190.15.1.0/24
New York	172.16.0.0/16	194.25.2.0/24

The company has an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Multi-factor authentication (MFA) status
User1	Enabled
User2	Enforced

The MFA service settings are configured as shown in the exhibit. (Click the Exhibit tab.)

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

10.10.0.0/16  
194.25.2.0/24

verification options [learn more](#)

Methods available to users:

- Call to phone
- Text message to phone

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

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 2: No

Use of Microsoft Authenticator is not required.

Note: Microsoft Authenticator is a multifactor app for mobile devices that generates time-based codes used during the Two-Step Verification process.

Box 3: No

The New York IP address subnet is included in the "skip multi-factor authentication for request. References:

<https://www.cayosoft.com/difference-enabling-enforcing-mfa/>

**NEW QUESTION 55**

- (Exam Topic 4)

You have an Azure subscription that uses Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

A PIM user that is assigned the User Access Administrator role reports receiving an authorization error when performing a role assignment or viewing the list of assignments.

You need to resolve the issue by ensuring that the PIM service principal has the correct permissions for the subscription. The solution must use the principle of least privilege.

Which role should you assign to the PIM service principle?

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

**Answer:** B

**NEW QUESTION 58**

- (Exam Topic 4)

You plan to implement an Azure function named Function1 that will create new storage accounts for containerized application instances.

You need to grant Function1 the minimum required privileges to create the storage accounts. The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Assign role to:

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

Role assignment to create:

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Reference:

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

**NEW QUESTION 63**

- (Exam Topic 4)

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

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

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

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

The subscription contains the subnets shown in the following table.

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

The subscription contains the routes shown in the following table.

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

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

Answer Area

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

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

**NEW QUESTION 65**

- (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 69**

- (Exam Topic 4)

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

Name	Type
container1	Container
folder1	File Share
table1	Table

In storage1, you create a shared access signature (SAS) named SAS1 as shown in the following exhibit.

Allowed services ⓘ  
 Blob  File  Queue  Table

Allowed resource types ⓘ  
 Service  Container  Object

Allowed permissions ⓘ  
 Read  Write  Delete  List  Add  Create  Update  Process  Immutable storage

Allowed blob index permissions ⓘ  
 Read/Write  Filter

Start and expiry date/time ⓘ  
 Start    
 End

Allowed IP addresses ⓘ

Allowed protocols ⓘ  
 HTTPS only  HTTPS and HTTP

Preferred routing tier ⓘ  
 Basic (default)  Microsoft network routing  Internet routing  
 ⓘ Some routing options are disabled because the endpoints are not published.

Signing key ⓘ

**Generate SAS and connection string**

To which resources can User1 write on July 1, 2022 by using SAS1 and key 1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

SAS1:

Key1:

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**



**NEW QUESTION 74**

- (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**

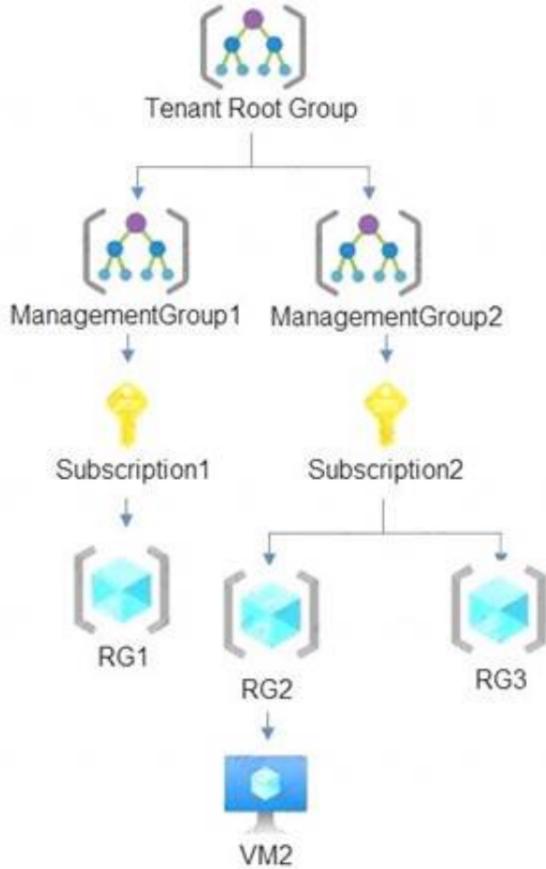
Provide access to DDoS rapid response support during active attacks: DDoS Network Protection

Protect Basic SKU public IP addresses: DDoS IP Protection

**NEW QUESTION 78**

- (Exam Topic 4)

You have the hierarchy of Azure resources shown in the following exhibit.



RG1, RG2, and RG3 are resource groups. RG2 contains a virtual machine named VM1. You assign role-based access control (RBAC) roles to the users shown in the following table.

Name	Role	Added to resource
User1	Contributor	Tenant Root Group
User2	Virtual Machine Contributor	Subscription2
User3	Virtual Machine Administrator Login	RG2

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

Statements	Yes	No
User1 can deploy virtual machines to RG1.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM2.	<input type="radio"/>	<input type="radio"/>
User3 can reset the password of the built-in Administrator account of VM2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Statements	Yes	No
User1 can deploy virtual machines to RG1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can delete VM2.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can reset the password of the built-in Administrator account of VM2.	<input type="radio"/>	<input checked="" type="radio"/>

**NEW QUESTION 79**

- (Exam Topic 4)

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

Name	Multi-factor authentication (MFA) status
User1	Disabled
User2	Disabled
User3	Enforced

In Azure AD Privileged Identity Management (PIM), the Role settings for the Contributor role are configured as shown in the exhibit. (Click the Exhibit tab.)

**Role settings** □ ×

**Assignment**

Allow permanent eligible assignment

Expire eligible assignments after

Allow permanent active assignment

Expire active assignments after

Require Multi-Factor Authentication on active assignment

Require justification on active assignment

**Activation**

Activation maximum duration (hours)

Require Multi-Factor Authentication on activation

Require justification on activation

Require ticket information on activation

Require approval to activate

*Select approvers*  
 No member or group selected

You assign users the Contributor role on May 1, 2019 as shown in the following table.

Name	Assignment type
User1	Eligible
User2	Active
User3	Active

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**

On May 15, 2019, User1 can activate the Contributor role.  Yes  No

On May 15, 2019, User2 can use the Contributor role.  Yes  No

On June 15, 2019, User3 can activate the Contributor role.  Yes  No

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

References:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assi>

**NEW QUESTION 81**

- (Exam Topic 4)

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

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

**Answer Area**

Permission that must be granted to users on VM:

Read
Update
View
Write

TCP port that must be allowed:

22
25
3389
5986

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

\* 1. Read permission

\* 2. 5986

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

**NEW QUESTION 83**

- (Exam Topic 4)

You have an Azure AD turned that contains a user named User1. You purchase an App named App1.

User1 needs to publish App1 by using Azure AD Application Proxy. Which role should you assign to User1?

- A. Hybrid identity Administrator
- B. Cloud App Security Administrator
- C. Application Administrator
- D. Cloud Application Administrate

**Answer:** C

**NEW QUESTION 87**

- (Exam Topic 4)

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

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

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

- > Delegate permissions for ContsosKey1.
- > Configure network access to ContosoKey1.

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

NOTE: Each correct selection is worth one point.

Delegate permissions for ContosoKey1:

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

Configure network access to ContosoKey1:

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 92**

- (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 96**

- (Exam Topic 4)

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

Name	Type	In resource group
8372f433-2dcd-4361-b5ef-5b188fed87d0	Subscription ID	Not applicable
RG1	Resource group	Not applicable
VM1	Virtual machine	RG1
VNET1	Virtual network	RG1
storage	Storage account	RG1
User1	User account	Not applicable

You create an Azure role by using the following JSON file.

```
{
  "properties":{
    "roleName": "Role1",
    "description": "",
    "assignableScopes": [
      "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0",
      "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG1"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Compute/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

You assign Role1 to User1 for RG1.  
 For each of the following statements, select Yes if the statement is true. Otherwise, select No.  
 NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can create a new virtual machine in RG1.	<input type="radio"/>	<input type="radio"/>
User can modify the properties of storage1.	<input type="radio"/>	<input type="radio"/>
User1 can attach the network interface of VM1 to VNET1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

NO NO NO

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#compute>

**NEW QUESTION 98**

- (Exam Topic 4)

You have an Azure subscription that contains the following resources:

- > A network virtual appliance (NVA) that runs non-Microsoft firewall software and routes all outbound traffic from the virtual machines to the internet
- > An Azure function that contains a script to manage the firewall rules of the NVA
- > Azure Security Center standard tier enabled for all virtual machines
- > An Azure Sentinel workspace
- > 30 virtual machines

You need to ensure that when a high-priority alert is generated in Security Center for a virtual machine, an incident is created in Azure Sentinel and then a script is initiated to configure a firewall rule for the NVA.

How should you configure Azure Sentinel to meet the requirements? To answer, drag the appropriate components to the correct requirements. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Components	Answer Area
A data connector for Security Center	Enable alert notifications from Security Center: <input type="text" value="Component"/>
A data connector for the firewall software	Create an incident: <input type="text" value="Component"/>
A playbook	Initiate a script to configure the firewall rule: <input type="text" value="Component"/>
A rule	
A Security Events connector	
A workbook	

- 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/connect-azure-security-center>

**NEW QUESTION 99**

- (Exam Topic 4)

Lab Task

use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password. place your cursor in the Enter password box and click on the password below. Azure Username: User1 -28681041@ExamUsers.com

Azure Password: GpOAe4@IDg

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only: Lab Instance: 28681041

Task 7

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 101**

- (Exam Topic 4)

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

Users must be able to select between a Google identity or a Microsoft identity when authenticating to App1. You need to add Google as an identity provider in Azure AD.

Which two pieces of information should you configure? Each correct answer presents part of the solution. Each correct selection is worth one point

- A. a tenant name
- B. a tenant ID
- C. the endpoint URL Of an application
- D. a client ID
- E. a client secret

**Answer:** DE

**Explanation:**

<https://learn.microsoft.com/en-us/azure/app-service/configure-authentication-provider-google>

**NEW QUESTION 103**

- (Exam Topic 4)

You have been tasked with configuring an access review, which you plan to assigned to a new collection of reviews. You also have to make sure that the reviews can be reviewed by resource owners.

You start by creating an access review program and an access review control. You now need to configure the Reviewers.

Which of the following should you set Reviewers to?

- A. Selected users.
- B. Members (Self).
- C. Group Owners.
- D. Anyone.

**Answer: C**

**Explanation:**

In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.

Graphical user interface, application Description automatically generated with medium confidence



Reference:

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

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

**NEW QUESTION 107**

- (Exam Topic 4)

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

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

You create the Azure policies shown in the following table.

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

You create the resource locks shown in the following table.

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

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

Statements	Yes	No
You can start VM1.	<input type="radio"/>	<input type="radio"/>
You can start VM2.	<input type="radio"/>	<input type="radio"/>
You can create a virtual machine in RG2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

NO NO NO

- 1) cannot perform write operation because following scope(s) are locked: 'subscriptions/xxxx/resourceGroups/xxx' Please remove the lock and try again.
- 2) When creating a VM in a resource group with a Read Only lock an error is shown: "The selected resource group is read only"
- 3) Because of the read only lock virtual machines cannot be started nor stopped when the lock is added after the machine started. (not part of this use case, but still good to know.

The article referenced in the answer states different because that is scoped to blueprints.

In the Lock Resources pages is states the following regarding starting VMs:

"A ReadOnly lock on a resource group that contains a virtual machine prevents all users from starting or restarting the virtual machine. These operations require a POST request."

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources>

#### NEW QUESTION 110

- (Exam Topic 4)

You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. You review the Attack Surface Summary dashboard. You need to identify the following insights:

- Deprecated technologies that are no longer supported
- Infrastructure that will soon expire

Which section of the dashboard should you review?

- A. Securing the Cloud
- B. Sensitive Services
- C. attack surface composition
- D. Attack Surface Priorities

**Answer: C**

#### NEW QUESTION 115

- (Exam Topic 4)

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com. You plan to create several security alerts by using Azure Monitor. You need to prepare the Azure subscription for the alerts. What should you create first?

- A. An Azure Storage account
- B. an Azure Log Analytics workspace
- C. an Azure event hub
- D. an Azure Automation account

**Answer: B**

#### Explanation:

<https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-create-workspace>

#### NEW QUESTION 120

- (Exam Topic 4)

You are troubleshooting a security issue for an Azure Storage account. You enable Azure Storage Analytics logs and archive them to a storage account. What should you use to retrieve the diagnostics logs?

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

**Answer: A**

#### NEW QUESTION 121

- (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 124

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a policy definition and assignments that are scoped to resource groups. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

References:

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

**NEW QUESTION 126**

- (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 131**

- (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 132**

- (Exam Topic 4)

DRAG DROP

You create an Azure subscription.

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

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

**Actions**

**Answer Area**

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

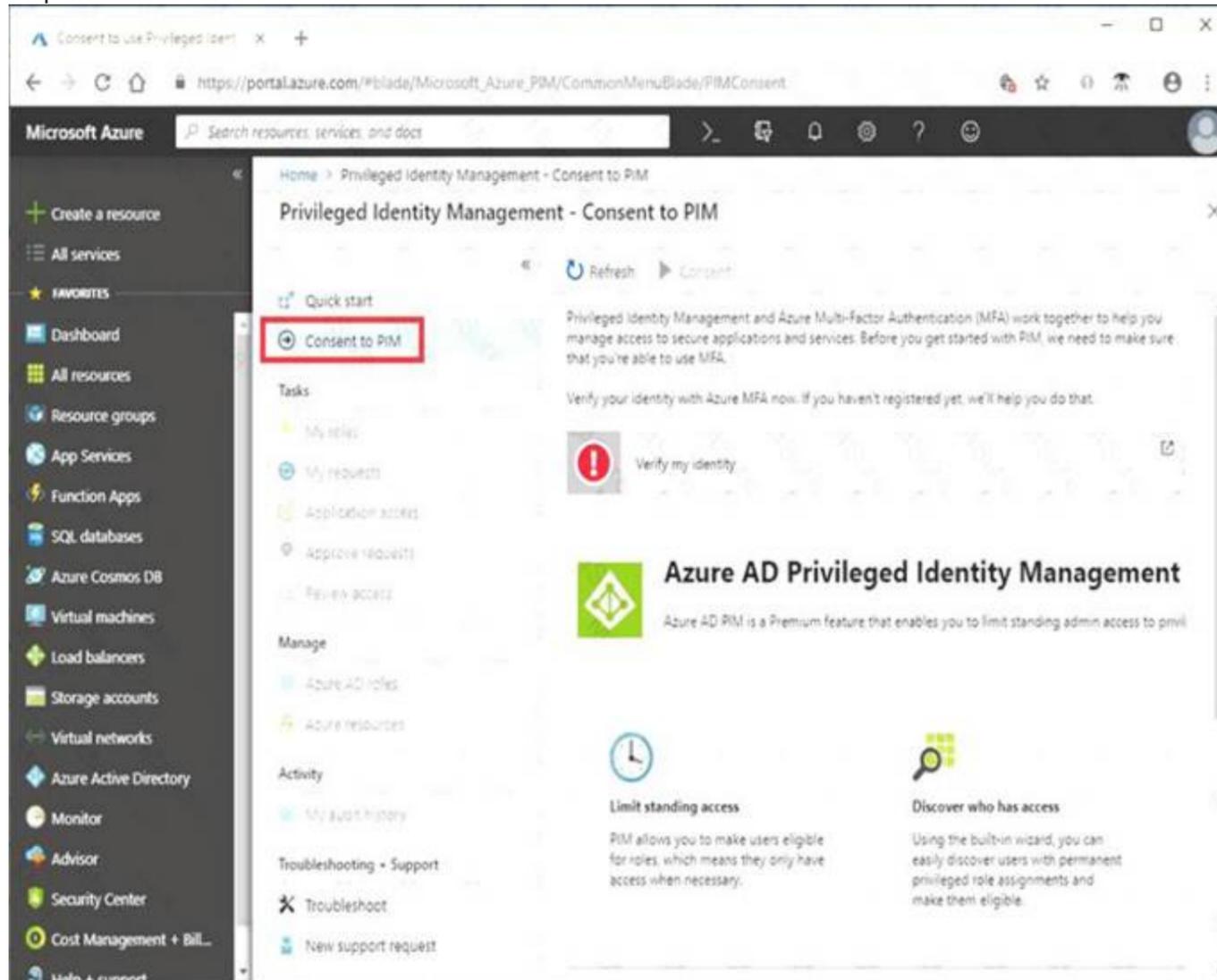


- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Step 1: Consent to PIM



Step: 2 Verify your identity by using multi-factor authentication (MFA)

Click Verify my identity to verify your identity with Azure MFA. You'll be asked to pick an account. Step 3: Sign up PIM for Azure AD roles

Once you have enabled PIM for your directory, you'll need to sign up PIM to manage Azure AD roles. References:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started>

**NEW QUESTION 134**

- (Exam Topic 4)

You have an Azure subscription named Sub1 that contains an Azure Storage account named Contosostorage1 and an Azure key vault named Contosokeyvault1.

You plan to create an Azure Automation runbook that will rotate the keys of Contosostorage1 and store them in Contosokeyvault1.

You need to implement prerequisites to ensure that you can implement the runbook.

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
Run Set-AzureRmKeyVaultAccessPolicy	
Create an Azure Automation account.	
Import PowerShell modules to the Azure Automation account.	
Create a user-assigned managed identity.	
Create a connection resource in the Azure Automation account.	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Step 1: Create an Azure Automation account

Runbooks live within the Azure Automation account and can execute PowerShell scripts. Step 2: Import PowerShell modules to the Azure Automation account Under 'Assets' from the Azure Automation account Resources section select 'to add in Modules to the runbook. To execute key vault cmdlets in the runbook, we need to add AzureRM.profile and AzureRM.key vault.

Step 3: Create a connection resource in the Azure Automation account

You can use the sample code below, taken from the AzureAutomationTutorialScript example runbook, to authenticate using the Run As account to manage Resource Manager resources with your runbooks. The AzureRunAsConnection is a connection asset automatically created when we created 'run as accounts' above. This can be found under Assets -> Connections. After the authentication code, run the same code above to get all the keys from the vault.

```
$connectionName = "AzureRunAsConnection" try
{
# Get the connection "AzureRunAsConnection "
$servicePrincipalConnection=Get-AutomationConnection -Name $connectionName "Logging in to Azure..."
Add-AzureRmAccount `
-ServicePrincipal `
-TenantId $servicePrincipalConnection.TenantId `
-ApplicationId $servicePrincipalConnection.ApplicationId `
-CertificateThumbprint $servicePrincipalConnection.CertificateThumbprint
}
```

References:

<https://www.rahulpnath.com/blog/accessing-azure-key-vault-from-azure-runbook/>

**NEW QUESTION 138**

- (Exam Topic 4)

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

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

You schedule two update deployments named Update1 and Update2. Update1 updates VM3. Update2 updates VM6.

Which additional virtual machines can be updated by using Update1 and Update2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Update1:

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

Update2:

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Update1: VM1 and VM2 only

VM3: Windows Server 2016 West US RG2 Update2: VM4 and VM5 only

VM6: CentOS 7.5 East US RG1

For Linux, the machine must have access to an update repository. The update repository can be private or public.

References:

<https://docs.microsoft.com/en-us/azure/automation/automation-update-management>

**NEW QUESTION 139**

- (Exam Topic 4)

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

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

**Answer Area**

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

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

**NEW QUESTION 142**

- (Exam Topic 4)

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

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

**Answer: B**

**NEW QUESTION 144**

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain named corp.contoso.com.

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You sync all on-premises identities to Azure AD.

You need to prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD. The solution must minimize administrative effort. What should you use?

- A. Synchronization Rules Editor
- B. Web Service Configuration Tool
- C. the Azure AD Connect wizard
- D. Active Directory Users and Computers

**Answer: A**

**Explanation:**

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

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

**NEW QUESTION 145**

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Subscription named Sub1.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.

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

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

- A. Yes
- B. No

**Answer: B**

**Explanation:**

Instead you should create a new stored access policy.

To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.

References:

<https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy>

**NEW QUESTION 150**

- (Exam Topic 4)

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

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

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

Which images are trusted images?

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

**Answer: B**

**Explanation:**

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

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

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

Reference:

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

### NEW QUESTION 155

- (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 160

- (Exam Topic 4)

You have an Azure subscription that contains 100 virtual machines and has Azure Security Center Standard tier enabled.

You plan to perform a vulnerability scan of each virtual machine.

You need to deploy the vulnerability scanner extension to the virtual machines by using an Azure Resource Manager template.

Which two values should you specify in the code to automate the deployment of the extension to the virtual machines? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. the user-assigned managed identity
- B. the workspace ID
- C. the Azure Active Directory (Azure AD) ID
- D. the Key Vault managed storage account key
- E. the system-assigned managed identity
- F. the primary shared key

**Answer:** AC

### NEW QUESTION 161

- (Exam Topic 4)

You have an Azure environment.

You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001:2013 standards.

What should you use?

- A. Azure Active Directory (Azure AD) Identity Protection
- B. Microsoft Defender for Cloud
- C. Microsoft Defender for Identity
- D. Microsoft Sentinel

**Answer:** B

### NEW QUESTION 166

- (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 171**

- (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 175**

- (Exam Topic 4)

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

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

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

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

On which virtual machines is the Microsoft Monitoring agent installed?

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

**Answer:** D

**Explanation:**

When automatic provisioning is enabled, Security Center provisions the Microsoft Monitoring Agent on all supported Azure VMs and any new ones that are created.

Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803.

References:

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

**NEW QUESTION 178**

- (Exam Topic 4)

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

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

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

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

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

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

**Answer:** C

**Explanation:**

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

Reference:

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

**NEW QUESTION 181**

- (Exam Topic 4)

You plan to use Azure Resource Manager templates to perform multiple deployments of identically configured Azure virtual machines. The password for the administrator account of each deployment is stored as a secret in different Azure key vaults.

You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment.

The name of the key vault and the name of the secret will be provided as inline parameters.

What should you use to construct the resource ID?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 182**

- (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 186**

- (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 189**

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result these questions will not appear in the review screen.

You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a policy initiative and assignments that are scoped to resource groups. Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

**NEW QUESTION 190**

- (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.

Name	Resource group	TDE
SQL2	RG2	Disabled
SQL3	RG1	Disabled

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**

SQL1 will have TDE enabled automatically.

The deployment of SQL2 will fail.

SQL3 will be deployed and marked as noncompliant.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

<https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects>

**NEW QUESTION 193**

- (Exam Topic 4)

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

Name	Type
storage1	Storage account
Vault1	Azure Key vault
Vault2	Azure Key vault

You plan to deploy the virtual machines shown in the following table.

Name	Role
VM1	<ul style="list-style-type: none"> <li>Storage Blob Data Reader for storage1</li> <li>Key Vault Reader for Vault1</li> </ul>
VM2	<ul style="list-style-type: none"> <li>Storage Blob Data Reader for storage1</li> <li>Key Vault Reader for Vault1</li> </ul>
VM3	<ul style="list-style-type: none"> <li>Storage Blob Data Reader for storage1</li> <li>Key Vault Reader for Vault1</li> <li>Key Vault Reader for Vault2</li> </ul>
VM4	<ul style="list-style-type: none"> <li>Storage Blob Data Reader for storage1</li> <li>Key Vault Reader for Vault1</li> <li>Key Vault Reader for Vault2</li> </ul>

You need to assign managed identities to the virtual machines. The solution must meet the following requirements:

- > Assign each virtual machine the required roles.
- > Use the principle of least privilege.

What is the minimum number of managed identities required?

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

**Answer: B**

**Explanation:**

We have two different sets of required permissions. VM1 and VM2 have the same permission requirements. VM3 and VM4 have the same permission requirements.

A user-assigned managed identity can be assigned to one or many resources. By using user-assigned managed identities, we can create just two managed identities: one with the permission requirements for VM1 and VM2 and the other with the permission requirements for VM3 and VM4.

Reference:

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

**NEW QUESTION 194**

- (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 197**

- (Exam Topic 4)

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

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

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

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

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

NOTE: Each correct selection is worth one point.

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

▼

Analytics
Data connectors
Playbooks
Workbooks

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

▼

Analytics
Data connectors
Playbooks
Workbooks

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 201**

- (Exam Topic 4)

Your company has an Azure subscription named Subscription1. Subscription1 is associated with the Azure Active Directory tenant that includes the users shown in the following table.

Name	Role
User1	Global administrator
User2	Billing administrator
User3	Owner
User4	Account Admin

The company is sold to a new owner.

The company needs to transfer ownership of Subscription1.

Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User:  ▼

User1
User2
User3
User4

Tool:  ▼

Azure Account Center
Azure Cloud Shell
Azure PowerShell
Azure Security Center

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Table Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer>

**NEW QUESTION 205**

- (Exam Topic 4)

From Azure Security Center, you enable Azure Container Registry vulnerability scanning of the images in Registry1.

You perform the following actions:

- > Push a Windows image named Image1 to Registry1.
- > Push a Linux image named Image2 to Registry1.
- > Push a Windows image named Image3 to Registry1.
- > Modify Image1 and push the new image as Image4 to Registry1.
- > Modify Image2 and push the new image as Image5 to Registry1.

Which two images will be scanned for vulnerabilities? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Image4
- B. Image2
- C. Image1
- D. Image3
- E. Image5

**Answer:** BC

**NEW QUESTION 208**

- (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 212**

- (Exam Topic 4)

You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) data connector. You are threat hunting suspicious traffic from a specific IP address.

You need to annotate an intermediate event stored in the workspace and be able to reference the IP address when navigating through the investigation graph.

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**

- Add the query to Favorites.
- From the Azure Sentinel workspace, run an Azure Log Analytics query.
- In a Jupyter notebook, create a reference to the IP address.
- Add a bookmark and assign a tag.
- Add a bookmark and map an entity.
- From Azure Monitor, run an Azure Log Analytics query.
- Select a query result.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:  
<https://docs.microsoft.com/en-us/azure/sentinel/bookmarks>

**NEW QUESTION 215**

- (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 220**

- (Exam Topic 4)

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

- A. OAuth 2.0
- B. JSON Web Token (JWT)
- C. Kerberos
- D. SAML

**Answer:** C

**Explanation:**

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

**NEW QUESTION 225**

- (Exam Topic 4)

Lab Task

use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below. Azure Username: User1-28681041@ExamUsers.com

Azure Password: GpOAe4@IDg

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only: Lab Instance: 28681041

Task 10

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

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

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

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

**NEW QUESTION 226**

- (Exam Topic 4)

You have an Azure subscription that contains a storage account named storage1 and several virtual machines. The storage account and virtual machines are in the same Azure region. The network configurations of the virtual machines are shown in the following table.

Name	Public IP address	Connected to
VM1	52.232.128.194	VNET1/Subnet1
VM2	52.233.129.82	VNET2/Subnet2
VM3	52.233.130.11	VNET3/Subnet3

The virtual network subnets have service endpoints defined as shown in the following table.

Name	Service endpoint
VNET1/Subnet1	Microsoft.Storage
VNET2/Subnet2	None
VNET3/Subnet3	Microsoft.KeyVault

You configure the following Firewall and virtual networks settings for storage1:

- > Allow access from: Selected networks
- > Virtual networks: VNET3\Subnet3
- > Firewall – Address range: 52.233.129.0/24

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
VM1 can connect to storage1.	<input type="radio"/>	<input type="radio"/>
VM2 can connect to storage1.	<input type="radio"/>	<input type="radio"/>
VM3 can connect to storage1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Box 1: No

VNet1 has a service endpoint configure for Azure Storage. However, the Azure storage does not allow access from VNet1 or the public IP address of VM1.

Box 2: Yes

VNet2 does not have a service endpoint configured. However, the Azure storage allows access from the public IP address of VM2.

Box 3: No

Azure storage allows access from VNet3. However, VNet3 does not have a service endpoint for Azure storage. The Azure storage also does not allow access from the public IP of VM3.

**NEW QUESTION 231**

- (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 232**

- (Exam Topic 4)

You have an Azure subscription that contains a virtual machine named VM1. You create an Azure key vault that has the following configurations:

- > Name: Vault5
- > Region: West US
- > Resource group: RG1

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 235**

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named Contoso.com and an Azure Service (AKS) cluster AKS1.

You discover that AKS1 cannot be accessed by using accounts from Contoso.com

You need to ensure AKS1 can be accessed by using accounts from Contoso.com The solution must minimize administrative effort.

What should you do first?

- A. From Azure recreate AKS1,
- B. From AKS1, upgrade the version of Kubernetes.
- C. From Azure AD, implement Azure AD Premium P2.
- D. From Azure AD, configure the User settings

**Answer:** A

**Explanation:**

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

**NEW QUESTION 237**

- (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 240**

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription named Sub1.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.

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

Solution: You regenerate the access keys. Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

**Explanation:**

To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately effects all of the shared access signatures associated with it.

References:

<https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy>

**NEW QUESTION 245**

- (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 8

You need to prevent HTTP connections to the rg1lod28681041n1 Azure Storage account.

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

To prevent HTTP connections to the rg1lod28681041n1 Azure Storage account, you can follow these steps: ➤ In the Azure portal, search for and select the storage account named rg1lod28681041n1.

- In the left pane, select Firewalls and virtual networks.
- In the Firewalls and virtual networks pane, select Selected networks.
- In the Selected networks pane, select Add existing virtual network.
- In the Add existing virtual network pane, select the virtual network that does not allow HTTP connections.
- Select Add.

**NEW QUESTION 248**

- (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 249**

- (Exam Topic 4)

You plan to deploy a custom policy initiative for Microsoft Defender for Cloud. You need to identify all the resource groups that have a Delete lock.

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

Answer Area

```
...  
  "policyRule": {  
    "if": {  
      "field": "type",  
      "equals": "Microsoft.Resources/subscriptions",  
    },  
    "then": {  
      "effect": "auditIfNotExists",  
      "details": {  
        "type": "Microsoft.Authorization/locks",  
        "existenceCondition": {  
          "field": "Microsoft.Authorization/locks/level",  
          "equals": "CanNotDelete"  
        }  
      }  
    }  
  }  
}
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Answer Area

```
...  
  "policyRule": {  
    "if": {  
      "field": "type",  
      "equals": "Microsoft.Resources/subscriptions",  
    },  
    "then": {  
      "effect": "auditIfNotExists",  
      "details": {  
        "type": "Microsoft.Authorization/locks",  
        "existenceCondition": {  
          "field": "Microsoft.Authorization/locks/level",  
          "equals": "CanNotDelete"  
        }  
      }  
    }  
  }  
}
```

NEW QUESTION 252

- (Exam Topic 4)

You have an Azure subscription named Subscription1 that contains a resource group named RG1 and a user named User1. User1 is assigned the Owner role for RG1.

You create an Azure Blueprints definition named Blueprint1 that includes a resource group named RG2 as shown in the following exhibit.

### Edit blueprint



NAME	ARTIFACT TYPE	PARAMETERS
Subscription		
+ Add artifact..		
RG2	Resource group	2 out of 2 parameters populated
User1 (User1@sk200628outlook.onmicrosoft.com) : Tag Contributor	Role assignment	1 out of 1 parameters populated
+ Add artifact..		

You assign Blueprint1 to Subscription1 by using the following settings: > Lock assignment: Read Only

> Managed Identity: System assigned

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

A locking mode of Read Only will be assigned to RG1.

Yes  No

User1 can add tags to RG2.

Yes  No

You can remove User1 from the Tag Contributor role for RG2.

Yes  No

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

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

**NEW QUESTION 255**

- (Exam Topic 4)

You have an Azure Storage account named storage1 and an Azure virtual machine named VM1. VM1 has a premium SSD managed disk.

You need to enable Azure Disk Encryption for VM1.

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**

- Run the Set-AzVMDiskEncryptionExtension cmdlet.
- Set the Key Vault access policy to **Enable access to Azure Virtual Machines for deployment.**
- Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption.**
- Generate a key vault certificate.
- Create an Azure key vault.
- Configure storage1 to use a customer-managed key.

**Answer Area**

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault>

**NEW QUESTION 260**

- (Exam Topic 4)

You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. EASM1 has discovery enabled and contains several inventory assets.

You need to identify which inventory assets are vulnerable to the most critical web app security risks. Which Defender EASM dashboard should you use?

- A. Attack Surface Summary
- B. GDPRCompliance
- C. Security Posture
- D. OWASPTopIO

**Answer:** D

**NEW QUESTION 262**

- (Exam Topic 4)

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

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

You create a resource group named RG1.

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

NOTE: Each correct selection is worth one point.

Users who can modify the permissions for RG1:

▼

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

Users who can create virtual networks in RG1:

▼

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 263**

- (Exam Topic 4)

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1. You have 100 on-premises servers that run Windows Server 2012 R2 and Windows Server 2016. The servers connect to LAW1. LAW1 is configured to collect security-related performance counters from the connected servers.

You need to configure alerts based on the data collected by LAW1. The solution must meet the following requirements:

- > Alert rules must support dimensions.
- > The time it takes to generate an alert must be minimized.

> resolved.

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

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

**Answer: C**

**Explanation:**

Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold. Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics.

Note: Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.

References:

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

**NEW QUESTION 267**

- (Exam Topic 4)

You have an Azure virtual machine named VM1.

From Azure Security Center, you get the following high-severity recommendation: "Install endpoint protection solutions on virtual machine".

You need to resolve the issue causing the high-severity recommendation. What should you do?

- A. Add the Microsoft Antimalware extension to VM1.
- B. Install Microsoft System Center Security Management Pack for Endpoint Protection on VM1.
- C. Add the Network Watcher Agent for Windows extension to VM1.
- D. Onboard VM1 to Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

**Answer: A**

**Explanation:**

Reference:

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

**NEW QUESTION 272**

- (Exam Topic 4)

You have an Azure Sentinel workspace that contains an Azure Active Directory (Azure AD) connector, an Azure Log Analytics query named Query1 and a playbook named Playbook1.

Query1 returns a subset of security events generated by Azure AD.

You plan to create an Azure Sentinel analytic rule based on Query1 that will trigger Playbook1. You need to ensure that you can add Playbook1 to the new rule.

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

NOTE: Each correct selection is worth one point.

Create the rule and set the type to:

Fusion

Microsoft Security incident creation

Scheduled

Configure the playbook to include:

A managed connector

A system-assigned managed identity

A trigger

Diagnostic settings

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Reference:

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

**NEW QUESTION 277**

- (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	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

Contoso.com contains a group naming policy. The policy has a custom blocked word list rule that includes the word Contoso.

Which users can create a group named Contoso Sales in contoso.com? To answer, select the appropriate options in the answer area.  
 NOTE: Each correct selection is worth one point.

Users who can create a security group named Contoso Sales:

Admin1 only
Admin1 and Admin2 only
Admin1 and Admin3 only
Admin1, Admin2, and Admin3

Users who can create an Office 365 group named Contoso Sales:

Admin1 only
Admin1 and Admin2 only
Admin1 and Admin3 only
Admin1, Admin2, and Admin3

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy>

**NEW QUESTION 278**

- (Exam Topic 4)

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

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

You enable passwordless authentication for the tenant.

Which authentication method can each user use for passwordless authentication? To answer, drag the appropriate authentication methods to the correct users. Each authentication method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

**Authentication methods**

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

**Answer Area**

User1:	Authentication method
User2:	Authentication method

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Authentication methods**

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

**Answer Area**

User1: Microsoft Authenticator app only

User2: Windows Hello for Business only

**NEW QUESTION 279**

- (Exam Topic 4)

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

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

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

Name	Type
Role3	Azure AD
Role4	Azure subscription

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

NOTE: Each correct selection is worth one point.

Role3:

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

Role4:

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

Reference:

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

**NEW QUESTION 280**

- (Exam Topic 4)

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

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

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

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

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

NOTE: Each correct selection is worth one point.

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

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

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

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

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

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

**NEW QUESTION 285**

- (Exam Topic 4)

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

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

**Answer:** C

**NEW QUESTION 290**

- (Exam Topic 4)

You have been tasked with applying conditional access policies for your company's current Azure Active Directory (Azure AD). The process involves assessing the risk events and risk levels.

Which of the following is the risk level that should be configured for users that have leaked credentials?

- A. None
- B. Low
- C. Medium
- D. High

**Answer:** D

**Explanation:**

These six types of events are categorized in to 3 levels of risks – High, Medium & Low:  
 Table Description automatically generated

Sign-in Activity	Risk Level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

Reference:

<http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/>

**NEW QUESTION 291**

- (Exam Topic 4)

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

Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West Europe	RG1
VM3	Windows Server 2016	West Europe	RG2
VM4	Red Hat Enterprise Linux 7.4	East US	RG2

You create an Azure Log Analytics workspace named Analytics1 in RG1 in the East US region. Which virtual machines can be enrolled in Analytics1?

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

**Answer: C**

**Explanation:**

Note: Create a workspace

- > In the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics.
- > Click Create, and then select choices for the following items:

Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace. OMS workspaces are now referred to as Log Analytics workspaces. Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate. For Resource Group, select an existing resource group that contains one or more Azure virtual machines. Select the Location your VMs are deployed to. For additional information, see which regions Log Analytics is available in.

**NEW QUESTION 295**

- (Exam Topic 4)

You have a Microsoft 365 tenant that uses an Azure Active Directory (Azure AD) tenant. The Azure AD tenant syncs to an on-premises Active Directory domain by using an instance of Azure AD Connect.

You create a new Azure subscription.

You discover that the synced on-premises user accounts cannot be assigned roles in the new subscription. You need to ensure that you can assign Azure and Microsoft 365 roles to the synced Azure AD user accounts. What should you do first?

- A. Change the Azure AD tenant used by the new subscription.
- B. Configure the Azure AD tenant used by the new subscription to use pass-through authentication.
- C. Configure the Azure AD tenant used by the new subscription to use federated authentication.
- D. Configure a second instance of Azure AD Connect.

**Answer: A**

**NEW QUESTION 297**

- (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 2012R2	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 302**

- (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 federation with Active Directory Federation Services (AD FS). Does the solution meet the goal?

- A. Yes
- B. No

**Answer: B**

**Explanation:**

A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>

**NEW QUESTION 307**

- (Exam Topic 4)

You have an Azure web app named webapp1.

You need to configure continuous deployment for webapp1 by using an Azure Repo.

What should you create first?

- A. an Azure Application Insights service
- B. an Azure DevOps organization
- C. an Azure Storage account
- D. an Azure DevTest Labs lab

**Answer: B**

**NEW QUESTION 310**

- (Exam Topic 4)

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

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

You plan to enable auditing for DB1.

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

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

**Answer: C**

**NEW QUESTION 313**

- (Exam Topic 4)

You have an Azure subscription that contains 100 virtual machines. Azure Diagnostics is enabled on all the virtual machines.

You are planning the monitoring of Azure services in the subscription. You need to retrieve the following details:

- > Identify the user who deleted a virtual machine three weeks ago.
- > Query the security events of a virtual machine that runs Windows Server 2016.

What should you use in Azure Monitor? To answer, drag the appropriate configuration settings to the correct details. Each configuration setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Settings	Answer Area
Activity log	
Logs	Identify the user who deleted a virtual machine three weeks ago: <input type="text"/>
Metrics	Query the security events of a virtual machine that runs Windows Server 2016: <input type="text"/>
Service Health	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box1: Activity log

Azure activity logs provide insight into the operations that were performed on resources in your subscription. Activity logs were previously known as “audit logs” or “operational logs,” because they report control-plane events for your subscriptions.

Activity logs help you determine the “what, who, and when” for write operations (that is, PUT, POST, or DELETE).

Box 2: Logs

Log Integration collects Azure diagnostics from your Windows virtual machines, Azure activity logs, Azure Security Center alerts, and Azure resource provider logs. This integration provides a unified dashboard for all your assets, whether they're on-premises or in the cloud, so that you can aggregate, correlate, analyze, and alert for security events.

References:

<https://docs.microsoft.com/en-us/azure/security/azure-log-audit>

**NEW QUESTION 317**

- (Exam Topic 4)

Your company recently created an Azure subscription.

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

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

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

**Answer:** A

**Explanation:**

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

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

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

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

Reference:

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

**NEW QUESTION 319**

- (Exam Topic 4)

You have an Azure subscription.

You create a new virtual network named VNet1.

You plan to deploy an Azure web app named App1 that will use VNet1 and will be reachable by using private IP addresses. The solution must support inbound and outbound network traffic.

What should you do?

- A. Create an Azure App Service Hybrid Connection.
- B. Configure regional virtual network integration.
- C. Create an App Service Environment
- D. Create an Azure application gateway.

**Answer:** D

**NEW QUESTION 322**

- (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 324**

- (Exam Topic 4)

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

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

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

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

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

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

Outbound security rules

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

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
VM1 can ping VM3 successfully.	<input type="radio"/>	<input type="radio"/>
VM2 can ping VM4 successfully.	<input type="radio"/>	<input type="radio"/>
VM3 can be accessed by using Remote Desktop from the internet.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Yes

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

Box 2: No

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

Box 3: Yes

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

**NEW QUESTION 328**

- (Exam Topic 4)

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

 Save

---

Stored access policies

Identifier	Start time	Expiry time	Permissions
Policy1			r ***

 Add policy

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

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

▼

1

2

4

7

15

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

▼

1

2

4

7

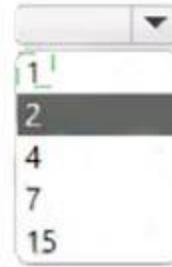
15

- A. Mastered
- B. Not Mastered

**Answer:** A

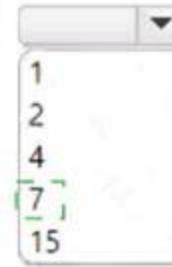
**Explanation:**

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



A dropdown menu with a downward arrow at the top. The options are 1, 2, 4, 7, and 15. The option '2' is highlighted with a dark background.

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



A dropdown menu with a downward arrow at the top. The options are 1, 2, 4, 7, and 15. The option '7' is highlighted with a dark background.

**NEW QUESTION 331**

- (Exam Topic 4)

You have an Azure subscription that contains an Azure Blob storage account blob1. You need to configure attribute-based access control (ABAC) for blob1. Which attributes can you use in access conditions?

- A. blob index tags only
- B. blob index tags and container names only
- C. file extensions and container names only
- D. blob index tags, file extensions, and container names

**Answer:** A

**NEW QUESTION 333**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

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

2nd - Questions and Answers in PDF Format

### **az-500 Practice Exam Features:**

- \* az-500 Questions and Answers Updated Frequently
- \* az-500 Practice Questions Verified by Expert Senior Certified Staff
- \* az-500 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* az-500 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The az-500 Practice Test Here](#)**