

## Exam Questions az-500

Microsoft Azure Security Technologies

<https://www.2passeasy.com/dumps/az-500/>



### NEW QUESTION 1

- (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 2

- (Exam Topic 4)

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

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

What should you use?

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

**Answer: B**

### NEW QUESTION 3

- (Exam Topic 4)

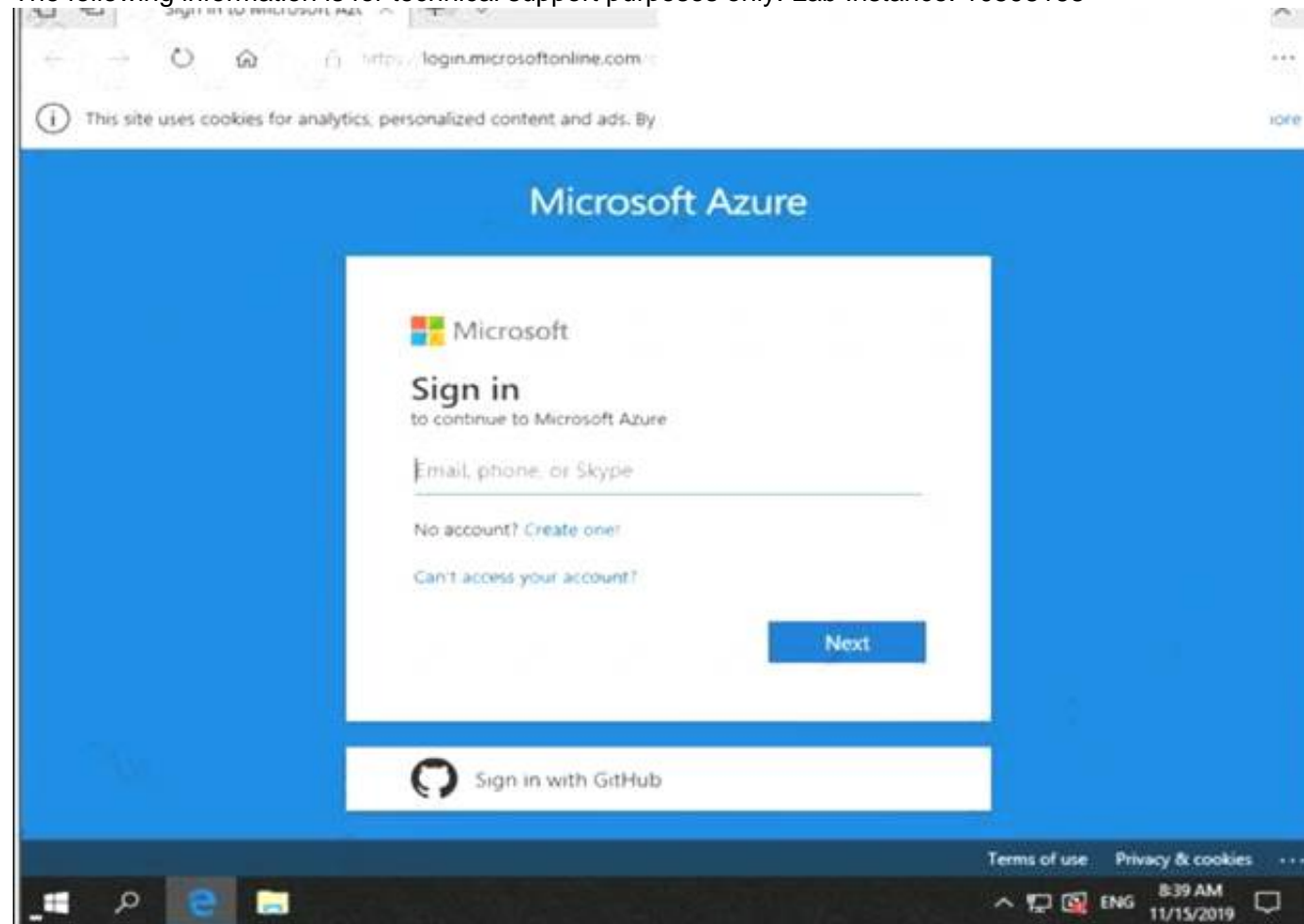
Use the following login credentials as needed:

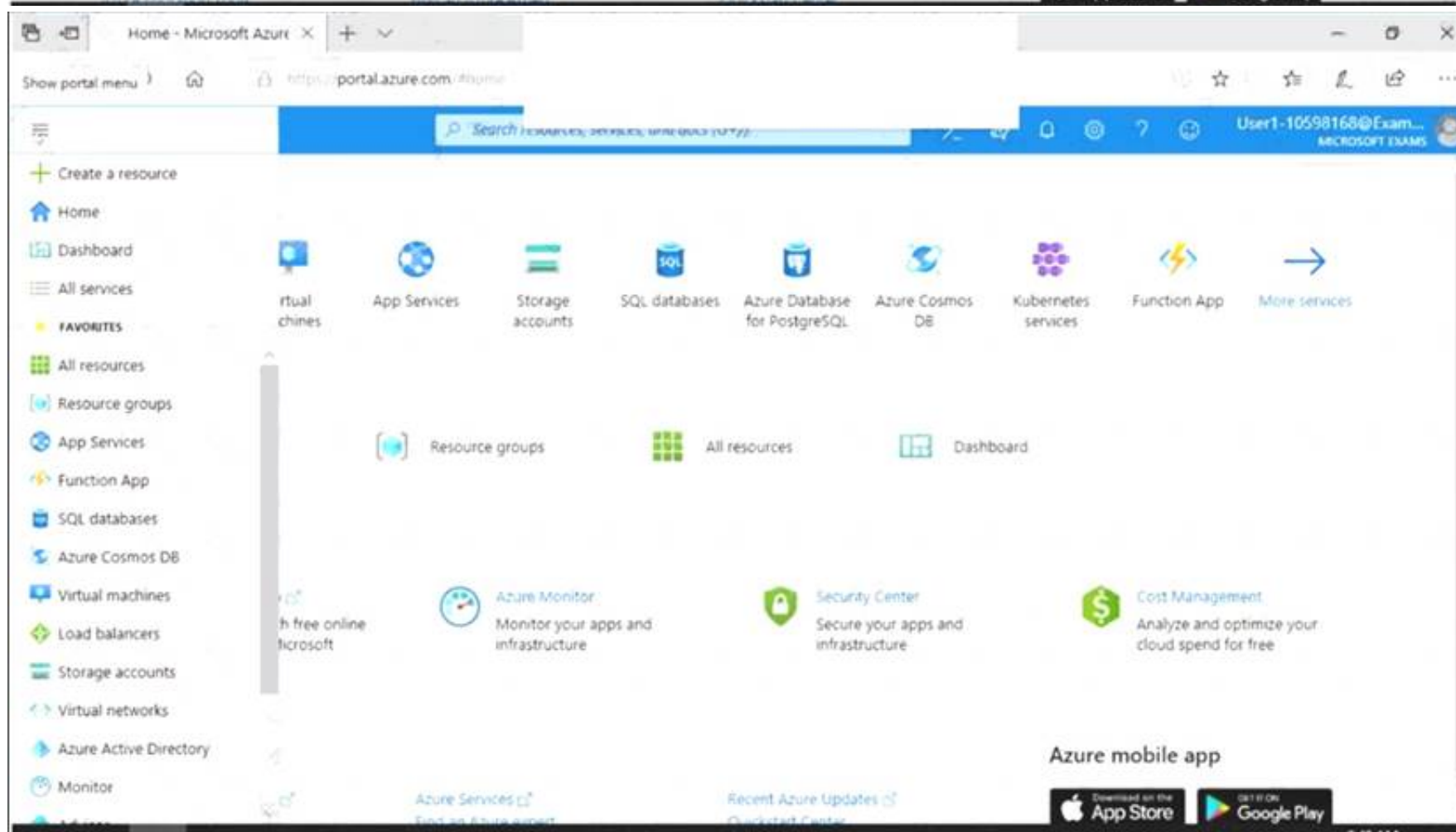
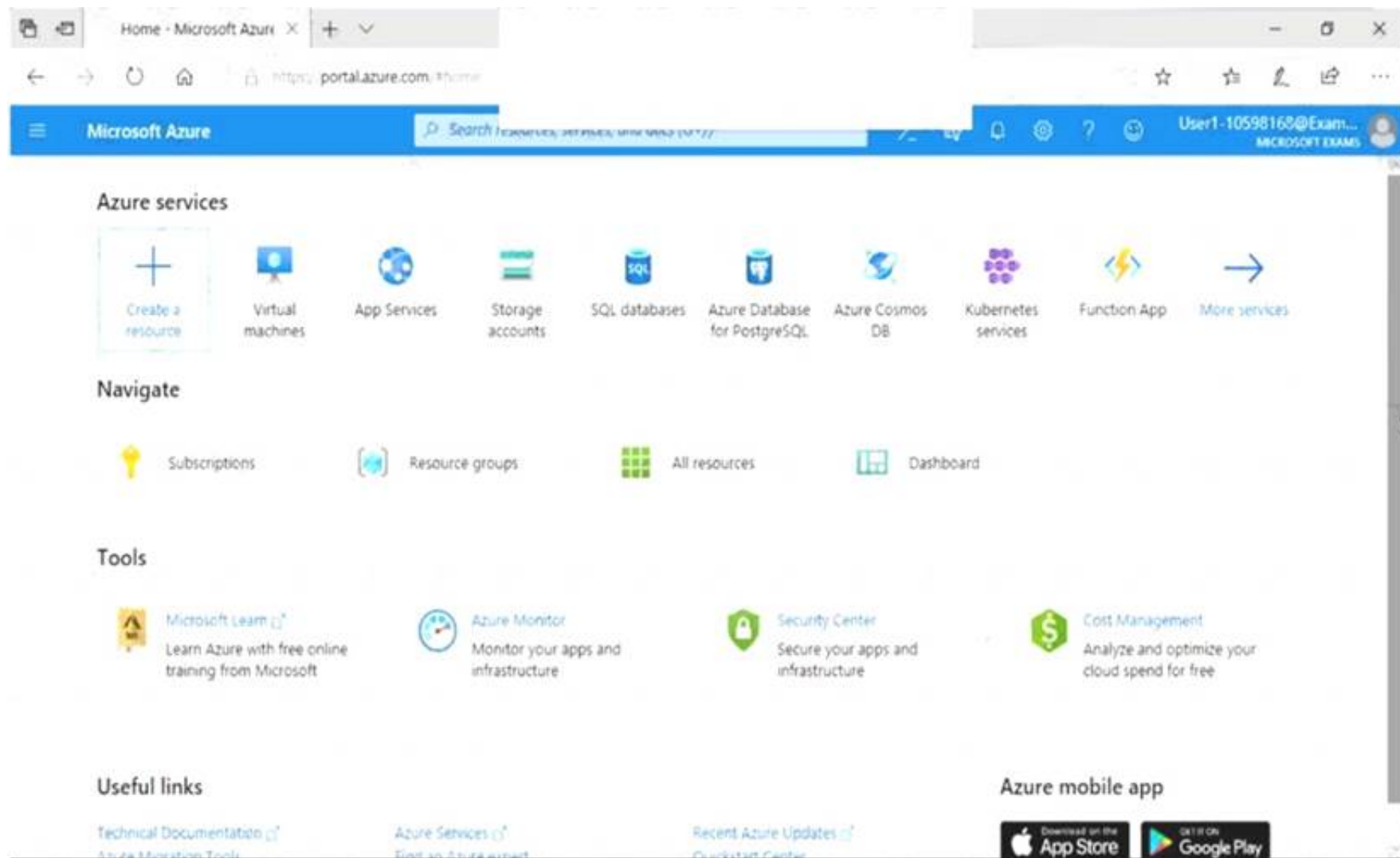
To enter your username, place your cursor in the Sign in box and click on the username below.

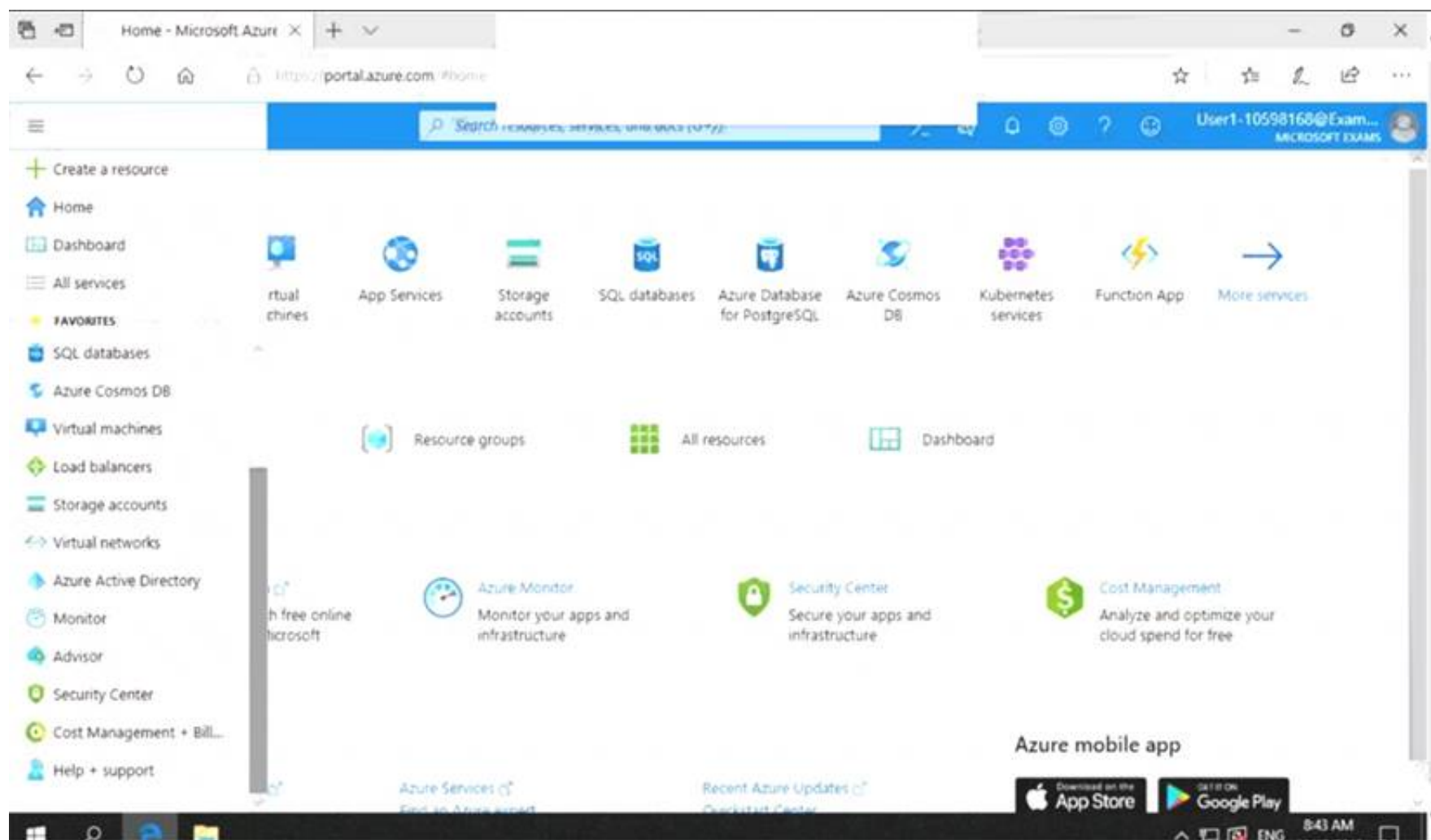
To enter your password, place your cursor in the Enter password box and click on the password below. Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only: Lab Instance: 10598168







You need to prevent HTTP connections to the rg1lod10598168n1 Azure Storage account. To complete this task, sign in to the Azure portal.

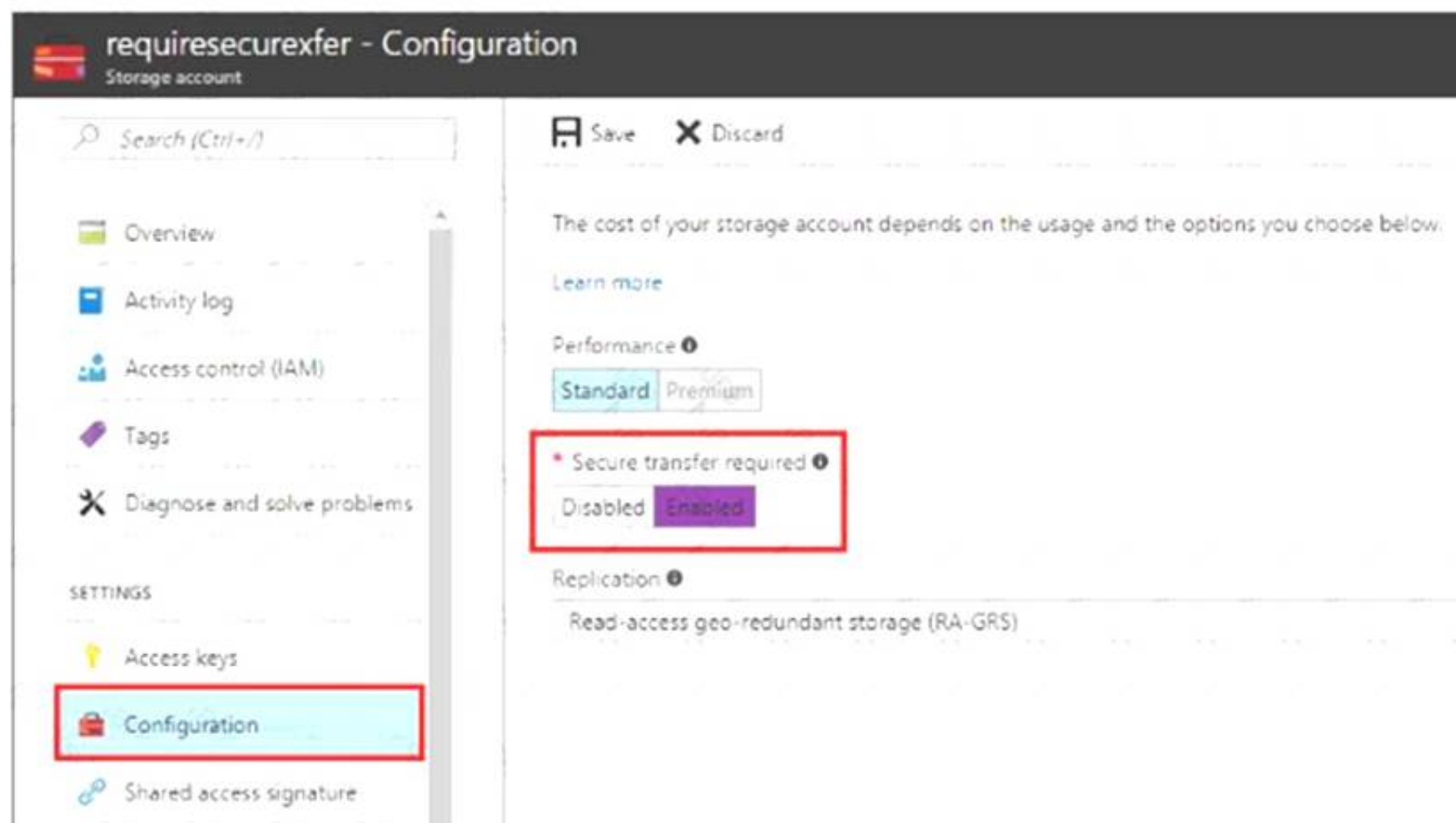
- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

The "Secure transfer required" feature is now supported in Azure Storage account. This feature enhances the security of your storage account by enforcing all requests to your account through a secure connection. This feature is disabled by default.

- \* 1. In Azure Portal select you Azure Storage account rg1lod10598168n1.
- \* 2. Select Configuration, and Secure Transfer required.



Reference:

<https://techcommunity.microsoft.com/t5/Azure/quot-Secure-transfer-required-quot-is-available-in-Azure-Storag>

**NEW QUESTION 4**

- (Exam Topic 4)

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



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

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

#### Custom smart lockout

Lockout threshold ⓘ

Lockout duration in seconds ⓘ

#### Custom banned passwords

Enforce custom list ⓘ 

Yes

No

Custom banned password list ⓘ 

Adatum

#### Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ 

Yes

No

Mode ⓘ 

Enforced

Audit

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 will be prompted to change the password on the next sign-in.	<input type="radio"/>	<input type="radio"/>
User2 can change the password to @d@tum_C0mpleX123.	<input type="radio"/>	<input type="radio"/>
User3 can change the password to Adatum123!.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

Text Description automatically generated

Reference:

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

#### NEW QUESTION 5

- (Exam Topic 4)

You have an Azure subscription that contains 100 virtual machines and has Azure Security Cent,-. 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 Key Vault managed storage account Key
- C. the Azure Active Directory (Azure AD) ID
- D. the system-assigned managed identity
- E. the primary shared key
- F. the workspace ID

Answer: AC

#### Explanation:

https://docs.microsoft.com/en-us/azure/azure-arc/servers/onboard-service-principal

### NEW QUESTION 6

- (Exam Topic 4)

You need to configure a weekly backup of an Azure SQL database named Homepage. The backup must be retained for eight weeks. To complete this task, sign in to the Azure portal.

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

You need to configure the backup policy for the Azure SQL database.

- In the Azure portal, type Azure SQL Database in the search box, select Azure SQL Database from the search results then select Homepage. Alternatively, browse to Azure SQL Database in the left navigation pane.
- Select the server hosting the Homepage database and click on Manage backups.
- Click on Configure policies.
- Ensure that the Weekly Backups option is ticked.
- Configure the How long would you like weekly backups to be retained option to 8 weeks.
- Click Apply to save the changes.

### NEW QUESTION 7

- (Exam Topic 4)

Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The company develops an application named App1. App1 is registered in Azure AD. You need to ensure that App1 can access secrets in Azure Key Vault on behalf of the application users. What should you configure?

- A. an application permission without admin consent
- B. a delegated permission without admin consent
- C. a delegated permission that requires admin consent
- D. an application permission that requires admin consent

**Answer:** B

#### Explanation:

Delegated permissions - Your client application needs to access the web API as the signed-in user, but with access limited by the selected permission. This type of permission can be granted by a user unless the permission requires administrator consent.

### NEW QUESTION 8

- (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 9

- (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 10

- (Exam Topic 4)

You need to configure network connectivity between a virtual network named VNET1 and a virtual network named VNET2. The solution must ensure that virtual machines connected to VNET1 can communicate with virtual machines connected to VNET2.

To complete this task, sign in to the Azure portal and modify the Azure resources.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

You need to configure VNet Peering between the two networks. The questions states, “The solution must ensure that virtual machines connected to VNET1 can communicate with virtual machines connected to VNET2”. It doesn’t say the VMs on VNET2 should be able to communicate with VMs on VNET1. Therefore, we need to configure the peering to allow just the one-way communication.

\* 1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET1. Alternatively, browse to Virtual Networks in the left navigation pane.

\* 2. In the properties of VNET1, click on Peerings.

\* 3. In the Peerings blade, click Add to add a new peering.

\* 4. In the Name of the peering from VNET1 to remote virtual network box, enter a name such as VNET1-VNET2 (this is the name that the peering will be displayed as in VNET1)

\* 5. In the Virtual Network box, select VNET2.

\* 6. In the Name of the peering from remote virtual network to VNET1 box, enter a name such as VNET2-VNET1 (this is the name that the peering will be displayed as in VNET2).

There is an option Allow virtual network access from VNET to remote virtual network. This should be left as Enabled.

\* 7. For the option Allow virtual network access from remote network to VNET1, click the slider button to Disabled.

\* 8. Click the OK button to save the changes. Reference:

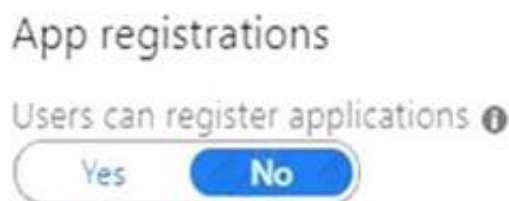
<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering>

#### NEW QUESTION 10

- (Exam Topic 4)

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant and a user named User1.

The App registrations settings for the tenant are configured as shown in the following exhibit.



You plan to deploy an app named App1.

You need to ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. App Configuration Data Owner for the subscription
- B. Managed Application Contributor for the subscription
- C. Cloud application administrator in Azure AD
- D. Application developer in Azure AD.

**Answer:** D

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task>

#### NEW QUESTION 11

- (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 14

- (Exam Topic 4)

You are troubleshooting a security issue for an Azure Storage account.

You enable the diagnostic logs for the storage account. What should you use to retrieve the diagnostics logs?

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

**Answer:** D

**Explanation:**

References:

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

#### NEW QUESTION 17

- (Exam Topic 4)

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

What should you use to retrieve the diagnostics logs?

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

**Answer:** A

**Explanation:**

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

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

References:

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

#### NEW QUESTION 18

- (Exam Topic 4)

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



Name	Resource group
VM1	RG1
VM2	RG2
VM3	RG1
VM4	RG2

You need to ensure that the virtual machines in RG1 have the Remote Desktop port closed until an authorized user requests access. What should you configure?

- A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- B. an application security group
- C. Azure Active Directory (Azure AD) conditional access
- D. just in time (JIT) VM access

**Answer:** D

**Explanation:**

Just-in-time (JIT) virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

Note: When just-in-time is enabled, Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the just-in-time solution.

When a user requests access to a VM, Security Center checks that the user has Role-Based Access Control (RBAC) permissions that permit them to successfully request access to a VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the amount of time that was specified. After the time has expired, Security Center restores the NSGs to their previous states. Those connections that are already established are not being interrupted, however.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time>

**NEW QUESTION 20**

- (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 Azure storage account access keys. Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**Explanation:**

Generating new storage account keys will invalidate all SAS's that were based on the previous keys.

**NEW QUESTION 21**

- (Exam Topic 4)

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

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

Each user is assigned an Azure AD Premium P2 license.

You plan to onboard and configure Azure AD identity Protection.

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

NOTE: Each correct selection is worth one point

Answer Area

Users who can onboard Azure AD Identity Protection:

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

Users who can remediate users and configure policies:

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

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

Answer Area

Users who can onboard Azure AD Identity Protection:

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

Users who can remediate users and configure policies:

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

NEW QUESTION 26

- (Exam Topic 4)

You have an Azure subscription that uses Microsoft Sentinel.

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

What should you create first?

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

Answer: A

NEW QUESTION 29

- (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 34

- (Exam Topic 4)

You have an Azure subscription named Sub1.

In Azure Security Center, you have a workflow automation named WF1. WF1 is configured to send an email message to a user named User1. You need to modify WF1 to send email messages to a distribution group named Alerts. What should you use to modify WF1?

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

**Answer: C**

**Explanation:**

Reference:

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

<https://docs.microsoft.com/en-us/learn/modules/resolve-threats-with-azure-security-center/6-exerciseconfigure-p>

**NEW QUESTION 35**

- (Exam Topic 4)

You are configuring network connectivity for two Azure virtual networks named VNET1 and VNET2. You need to implement VPN gateways for the virtual networks to meet the following requirements:

- \* VNET1 must have six site-to-site connections that use BGP.
- \* VNET2 must have 12 site-to-site connections that use BGP.
- \* Costs must be minimized.

Which VPN gateway SKI) should you use for each virtual network? To answer, drag the appropriate SKUs to the correct networks. Each SKU may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

References:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku>

**NEW QUESTION 40**

- (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 42

- (Exam Topic 4)

You need to ensure that when administrators deploy resources by using an Azure Resource Manager template, the deployment can access secrets in an Azure key vault named KV11597200.

To complete this task, sign in to the Azure portal.

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

You need to configure an option in the Advanced Access Policy of the key vault.

- In the Azure portal, type Azure Key Vault in the search box, select Azure Key Vault from the search results then select the key vault named KV11597200. Alternatively, browse to Azure Key Vault in the left navigation pane.
- In the properties of the key vault, click on Advanced Access Policies.
- Tick the checkbox labelled Enable access to Azure Resource Manager for template deployment.
- Click Save to save the changes.

#### NEW QUESTION 44

- (Exam Topic 4)

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

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 48

- (Exam Topic 4)

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

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

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

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

You need to configure auditing for SQL1.

Which storage accounts and Log Analytics workspaces can you use as the audit log destination? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Storage accounts that can be used as the audit log destination:

Storage1 only  
Storage2 only  
Storage1 and Storage2 only  
Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

Analytics1 only  
Analytics1 and Analytics2 only  
Analytics1 and Analytics3 only  
Analytics1, Analytics2, and Analytics3

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:



Answer Area

Storage accounts that can be used as the audit log destination:

Storage1 only

Storage2 only

Storage1 and Storage2 only

Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

Analytics1 only

Analytics1 and Analytics2 only

Analytics1 and Analytics3 only

Analytics1, Analytics2, and Analytics3

NEW QUESTION 52

- (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 57

- (Exam Topic 4)

You have an Azure subscription mat contains a resource group named RG1. RG1 contains a storage account named storage1.

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

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

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

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

Answer Area

Statements	Yes	No
User1 can read data in storage1.	<input type="radio"/>	<input type="radio"/>
User2 can read data in storage1.	<input type="radio"/>	<input type="radio"/>
User3 can restore storage1 from a backup in Azure Backup.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area	Statements	Yes	No
	User1 can read data in storage1.	<input checked="" type="radio"/>	<input type="radio"/>
	User2 can read data in storage1.	<input checked="" type="radio"/>	<input type="radio"/>
	User3 can restore storage1 from a backup in Azure Backup.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 61

- (Exam Topic 4)

You plan to create an Azure Kubernetes Service (AKS) cluster in an Azure subscription. The manifest of the registered server application is shown in the following exhibit.

Save Discard Upload Download

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

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 63

- (Exam Topic 4)

You have an Azure subscription named Subscription1 that contains a resource group named RG1 and the users shown in the following table.

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

You perform the following tasks:

- Assign User1 the Network Contributor role for Subscription1.
- Assign User2 the Contributor role for RG1.

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

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

**Answer:** A

#### NEW QUESTION 67

- (Exam Topic 4)

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

Name	Source
User1	Azure AD
User2	Azure AD
User3	On-premises Active Directory

The tenant contains the groups shown in the following table.

Name	Members
Group1	User1, User2, User3
Group2	User2

You configure a multi-factor authentication (MFA) registration policy that and the following settings:

- Assignments:
- Include: Group1
- Exclude Group2

Controls: Require Azure MFA registration Enforce Policy: On

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

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input checked="" type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user's next Azure AD authentication.	<input type="radio"/>	<input checked="" type="radio"/>
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input checked="" type="radio"/>	<input type="radio"/>

#### NEW QUESTION 72

- (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 76

- (Exam Topic 4)

You have an Azure subscription that contains a resource group named RG1 and a security group serverless RG1 contains 10 virtual machine, a virtual network VNET1, and a network security group (NSG) named NSG1. ServerAdmins can access the virtual machines by using RDP.

You need to ensure that NSG1 only RDP connections to the virtual for a maximum of 60 minutes when a member of ServerAdmins requests access. What should you configure?

- A. an Azure Active Directory (Azure AD) Privileged identity Management (PIM) role assignment.
- B. a just in time (JIT) VM access policy in Azure Security Center
- C. an azure policy assigned to RG1.
- D. an Azure Bastion host on VNET1.

**Answer:** B

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/just-in-time-explained>

#### NEW QUESTION 77

- (Exam Topic 4)

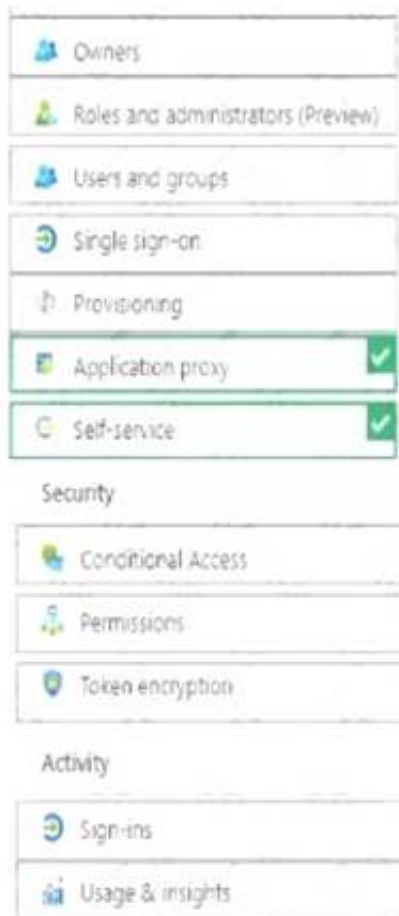
You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2 and a registered app named App1.

You create an app-specific role named Role1.

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

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





- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

NEW QUESTION 82

- (Exam Topic 4)

You have an Azure Sentinel deployment.

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 87

- (Exam Topic 3)

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

Which tools should you use? To answer, drag the appropriate tools to the correct resources. Each tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Tools

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

Answer Area

OU2:

Tool

User1:

Tool

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Table Description automatically generated

NEW QUESTION 92

- (Exam Topic 3)  
You need to encrypt storage1 to meet the technical requirements. Which key vaults can you use?

- A. KeyVault1 only
- B. KeyVault2 and KeyVault3 only
- C. KeyVault1 and KeyVault3 only
- D. KeyVault1 KeyVault2 and KeyVault3

Answer: B

Explanation:  
The storage account and the key vault must be in the same region and in the same Azure Active Directory (Azure AD) tenant, but they can be in different subscriptions.  
Storage1 is in the West US region. KeyVault1 is the only key vault in the same region. Reference:  
https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview

NEW QUESTION 95

- (Exam Topic 3)  
You need to delegate the creation of RG2 and the management of permissions for RG1. Which users can perform each task? To answer select the appropriate options in the answer area. NOTE: Each correct selection is worth one point

Create RG2:

Admin3 only

Admin2 and Admin3 only

Admin3 and Admin4 only

Admin2, Admin3, and Admin4 only

Admin1, Admin2, Admin3, and Admin4

Manage RG1 permissions:

Admin4 only

Admin1 and Admin4 only

Admin3 and Admin4 only

Admin1 Admin2, and Admin4 only

Admin1, Admin2, Admin3, and Admin4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Graphical user interface, text, application, chat or text message Description automatically generated  
Box 1: Admin3 only  
The Contributor role has the necessary write permissions to create the resource group. Box 2: Admin4 only  
You need Owner level access to be able to manage permissions. The Contributor role can do most things but cannot modify permissions on existing objects.

NEW QUESTION 100

- (Exam Topic 2)  
You are evaluating the security of VM1, VM2, and VM3 in Sub2.  
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 105

- (Exam Topic 2)

HOTSPOT

You assign User8 the Owner role for RG4, RG5, and RG6.

In which resource groups can User8 create virtual networks and NSGs? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User8 can create virtual networks in:

▼

RG4 only

RG6 only

RG4 and RG6 only

RG4, RG5, and RG6

User8 can create NSGs in:

▼

RG4 only

RG4 and RG5 only

RG4 and RG6 only

RG4, RG5, and RG6

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box1: RG6 only as there is not option for RG5 & RG6 which it should be. Box2: RG4 & RG6

NEW QUESTION 106

- (Exam Topic 1)

You need to configure SQLDB1 to meet the data and application requirements.

Which three actions should you recommend be performed 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
From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.	
In SQLDB1, create contained database users.	
Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS).	<div> <div>⬅</div> <div>➡</div> </div> <div> <div>⬆</div> <div>⬇</div> </div>
In Azure AD, create a system-assigned managed identity.	
In Azure AD, create a user-assigned managed identity.	

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

From the Azure portal, create an Azure AD administrator for LitwareSQLServer1 Connect to SQLDB1 by using SSMS  
 In SQLDB1, create contained database users <https://www.youtube.com/watch?v=pEPyPsGEevw>

**NEW QUESTION 109**

- (Exam Topic 1)

You need to create Role1 to meet the platform protection requirements.

How should you complete the role definition of Role1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```

{
  "Name": "Role1",
  "Id": "11111111-1111-1111-1111-111111111111",
  "IsCustom" : true,
  "Description": "VM storage operator"
  "Actions" : [
    {
      "Microsoft.Compute/":
      {
        disks/**,
        storageAccounts/**,
        virtualMachines/disks/**,
      },
    },
    "NotActions": [
      ],
    "AssignableScopes" : [
      {
        "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1"
        "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4"
      }
    ]
  }
}
  
```

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**



1) Microsoft.Compute/  
 2) disks  
 3) /subscription/{subscriptionId}/resourceGroups/{Resource Group Id}  
 A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

#### NEW QUESTION 114

- (Exam Topic 1)

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

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

To configure the registration settings:

▼

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

To configure the consent settings:

▼

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Reference:

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

#### NEW QUESTION 115

- (Exam Topic 4)

You need to configure a Microsoft SQL server named Web11597200 only to accept connections from the Subnet0 subnet on the VNET01 virtual network. To complete this task, sign in to the Azure portal.

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

You need to allow access to Azure services and configure a virtual network rule for the SQL Server.

- In the Azure portal, type SQL Server in the search box, select SQL Server from the search results then select the server named web11597200. Alternatively, browse to SQL Server in the left navigation pane.
- In the properties of the SQL Server, click Firewalls and virtual networks.
- In the Virtual networks section, click on Add existing. This will open the Create/Update virtual network rule window.
- Give the rule a name such as Allow\_VNET01-Subnet0 (it doesn't matter what name you enter for the exam).
- In the Virtual network box, select VNET01.
- In the Subnet name box, select Subnet0.
- Click the OK button to save the rule.
- Back in the Firewall / Virtual Networks window, set the Allow access to Azure services option to On.

#### NEW QUESTION 118

- (Exam Topic 4)

On Monday, you configure an email notification in Azure Security Center to notify user user1@contoso.com. On Tuesday, Security Center generates the security alerts shown in the following table.

Time	Description	Severity
01:00	Failed RDP brute force attack	Medium
01:01	Successful RDP brute force attack	High
06:10	Suspicious process executed	High
09:00	Malicious SQL activity	High
11:15	Network communication with a malicious machine detected	Low
13:30	Suspicious process executed	High
14:00	Failed RDP brute force attack	Medium
16:01	Successful RDP brute force attack	High
23:20	Possible outgoing spam activity detected	Low
23:25	Modified system binary discovered in dump file	High
23:30	Malicious SQL activity	High

How many email notifications will user1@contoso.com receive on Tuesday? To answer, select the appropriate options in the answer area.  
 NOTE: Each correct selection is worth one point.

Total number of Security Center email notifications about an RDP

brute force attack on Tuesday:

	▼
1	
2	
3	
4	

Total number of Security Center email notifications on Tuesday:

	▼
3	
4	
6	
9	
11	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

#### NEW QUESTION 119

- (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 124

- (Exam Topic 4)

You have an Azure subscription that contains an Azure key vault named Vault1. On January 1, 2019, Vault1 stores the following secrets.

```

Enabled      : False
Expires      :
NotBefore    : 5/1/19 12:00:00 AM
Created      : 12/20/18 2:55:00 PM
Updated      : 12/20/18 2:55:00 PM
ContentType  :
Tags         :
TagTable     :
VaultName    : vault1
Name         : Password1
Version      :
Id           : https://vault1.vault.azure.net:443/secrets/Password1

Enabled      : True
Expires      : 5/1/19 12:00:00 AM
NotBefore    : 3/1/19 12:00:00 AM
Created      : 12/20/18 3:00:00 PM
Updated      : 12/20/18 3:00:00 PM
ContentType  :
Tags         :
TagsTable    :
VaultName    : vault1
Name         : Password2
Version      :
Id           : https://vault1.vault.azure.net:443/secrets/Password2

```

Which can each secret be used by an application? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Password1:

	▼
Never	
Always	
Only after May 1, 2019	

Password2:

	▼
Never	
Always	
Only between March 1, 2019 and May 1. 2019	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Never Password1 is disabled.

Box 2: Only between March 1, 2019 and May 1, Password2:

```

Expires      : 5/1/19 12:00:00 AM
NotBefore    : 3/1/19 12:00:00 AM

```

Reference:

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

**NEW QUESTION 128**

- (Exam Topic 4)

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

Name	Type	In resource group
cont1	Container instance	RG1
VNET1	Virtual network	RG1
App1	App Service app	RG1
VM1	Virtual machine	RG1
User1	User	<b>Not applicable</b>

You create a custom RBAC role in Subscription1 by using the following JSON file.

```
{
  "Name": "Role1",
  "IsCustom": true,
  "Description": "Role1 description",
  "Actions": [
    "*/Read",
    "Microsoft.Compute/*"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/subscriptions/923a419a-4358-40fb-b4a9-b8af43dd0c92/resourceGroups/RG1"
  ]
}
```

You assign Role1 to User1 on 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 add VM1 to VNET1.	<input type="radio"/>	<input type="radio"/>
User1 can start and stop App1.	<input type="radio"/>	<input type="radio"/>
User1 can start and stop cont1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Text Description automatically generated  
Reference:  
<https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompu>

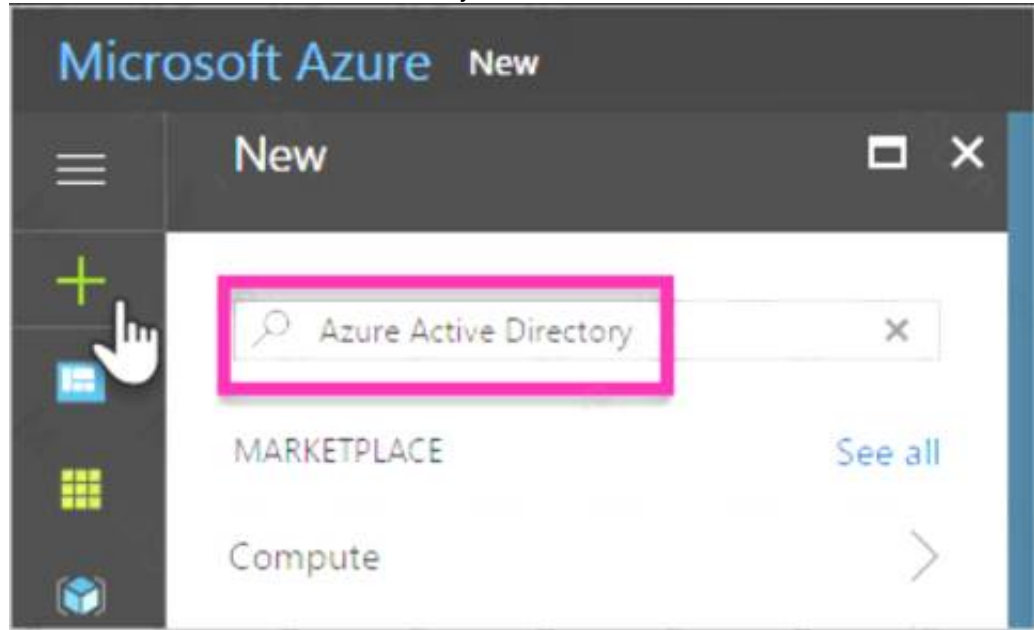
NEW QUESTION 129

- (Exam Topic 4)  
You need to create a new Azure Active Directory (Azure AD) directory named 10317806.onmicrosoft.com. The new directory must contain a user named user10317806 who is configured to sign in by using Azure Multi-Factor Authentication (MFA).

- A. Mastered
- B. Not Mastered

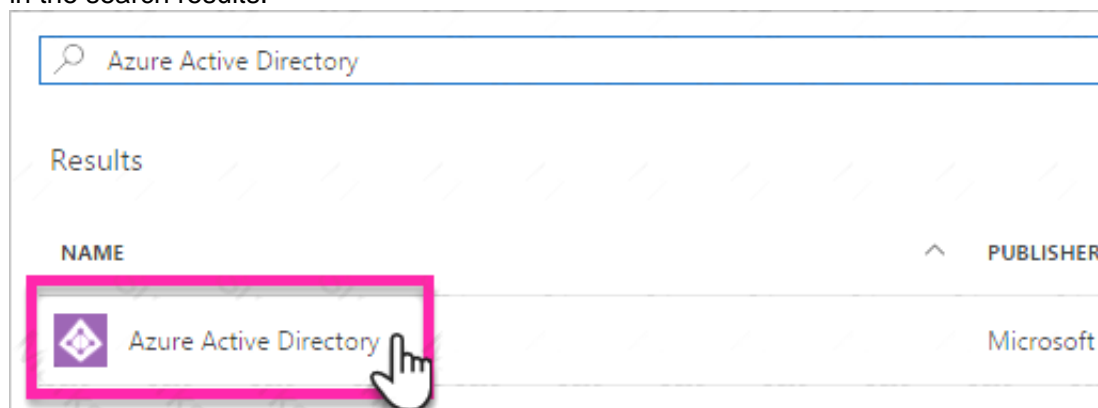
Answer: A

Explanation:  
To create a new Azure AD tenant:  
\* 1. Browse to the Azure portal and sign in with an account that has an Azure subscription.  
\* 2. Select the plus icon (+)  
and search for Azure Active Directory.





\* 3. Select Azure Active Directory in the search results.

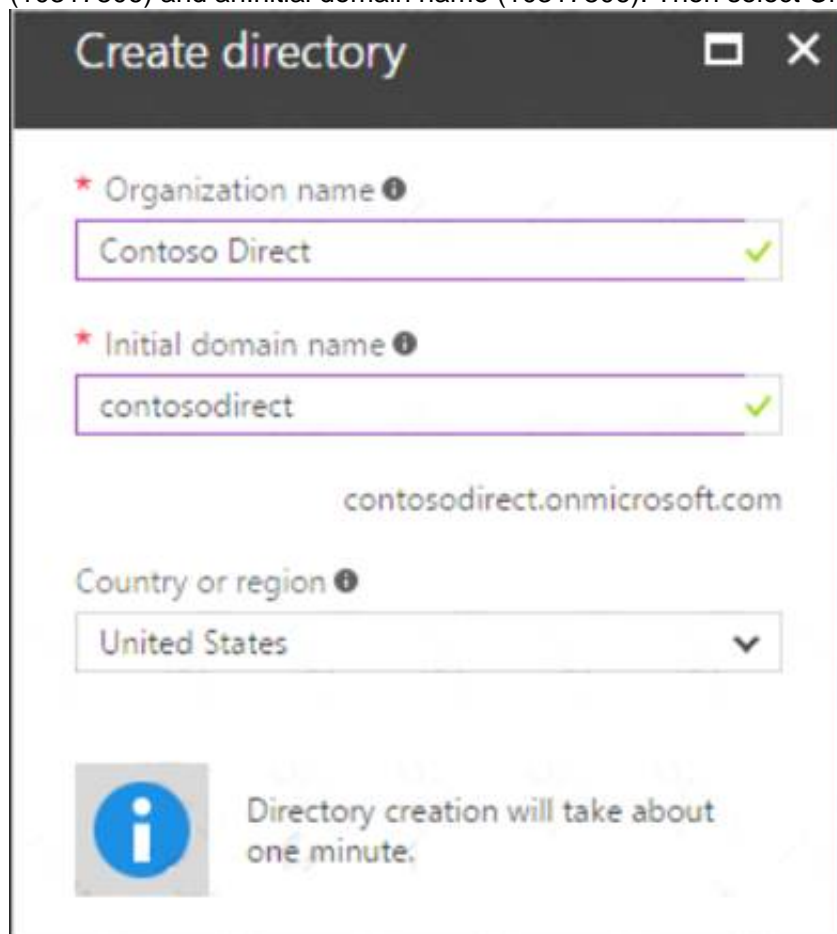


\* 4. Select Create.

\* 5. Provide an Organization name

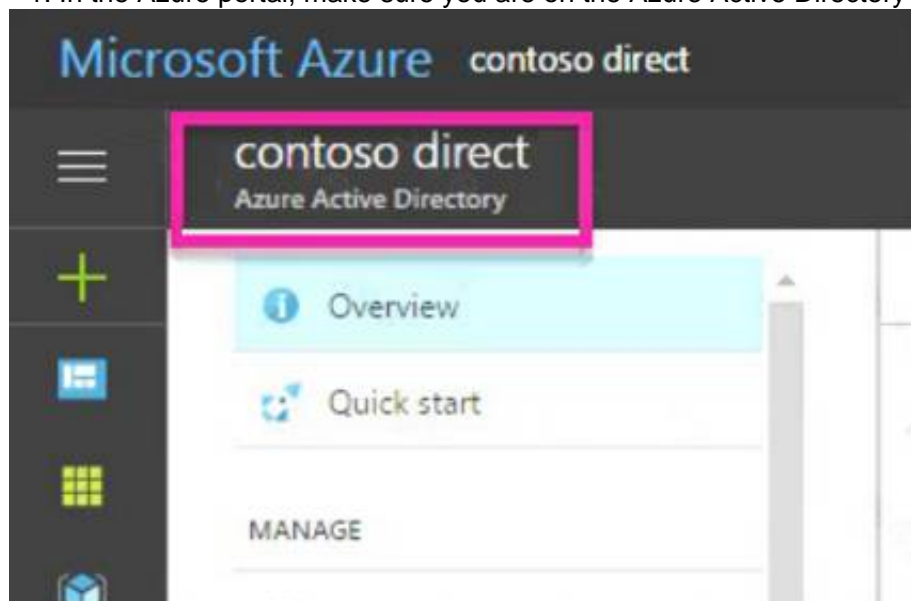
This will create the directory named 10317806.onmicrosoft.com.

(10317806) and an initial domain name (10317806). Then select Create.

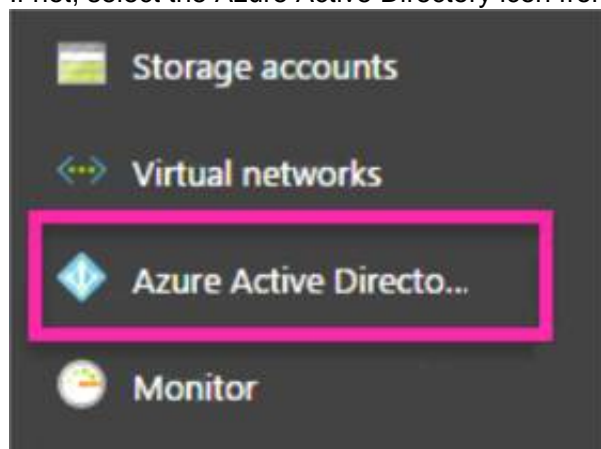


\* 6. After directory creation is complete, select the information box to manage your new directory. To create the user:

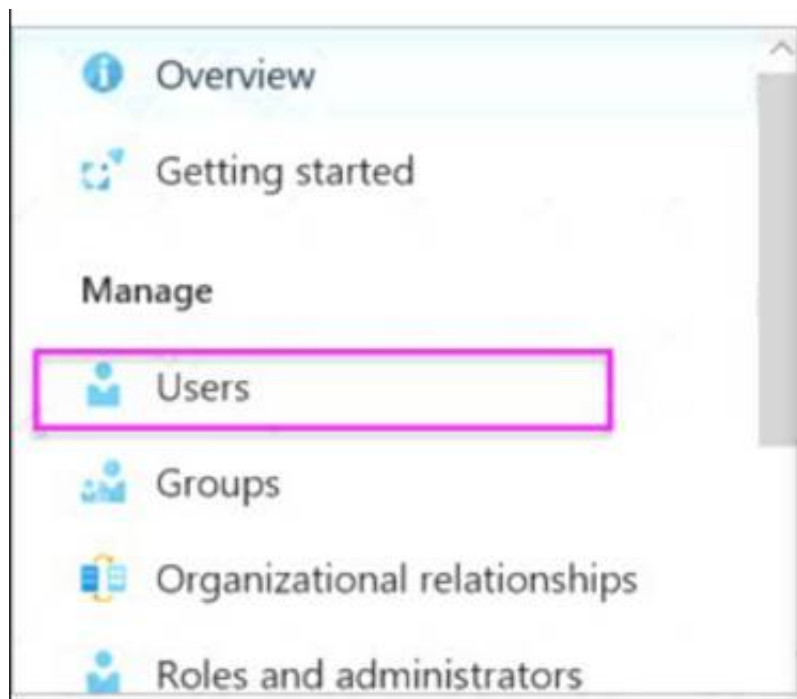
\* 1. In the Azure portal, make sure you are on the Azure Active Directory fly out.



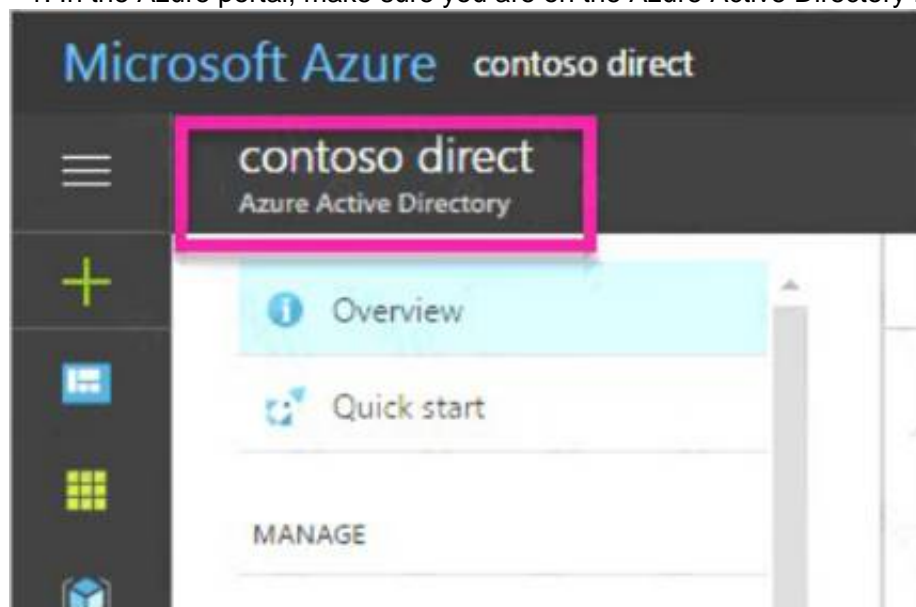
If not, select the Azure Active Directory icon from the left services navigation.



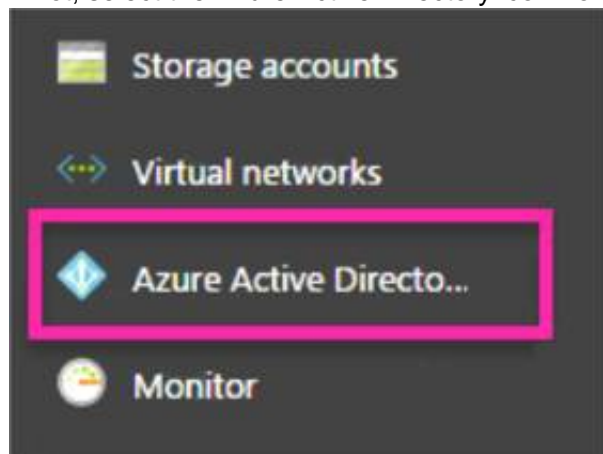
\* 2. Under Manage, select Users.



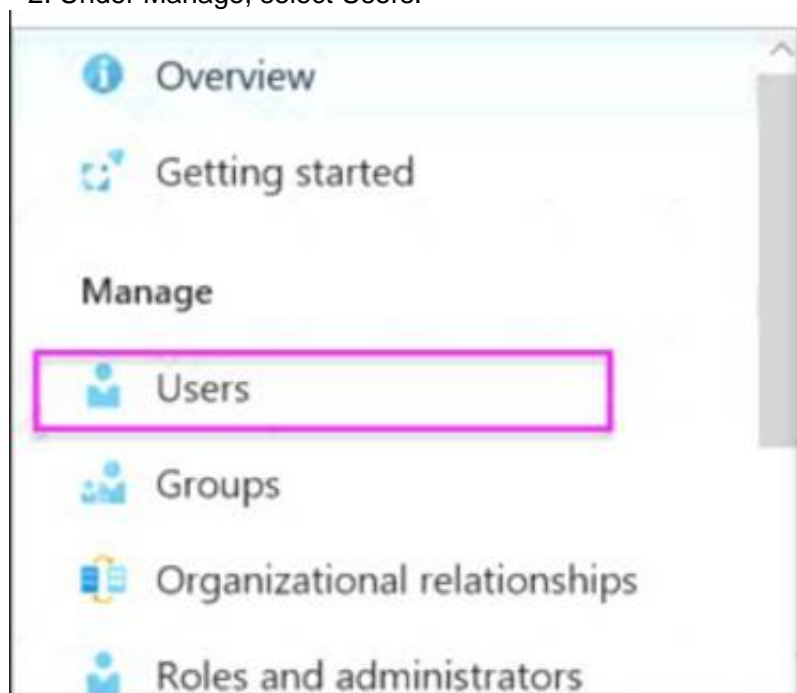
- \* 3. Select All users and then select New user.
- \* 4. Provide a Name and User name (user10317806) for the user. When you're done, select Create.
- To enable MFA:
- \* 1. In the Azure portal, make sure you are on the Azure Active Directory fly out.



If not, select the Azure Active Directory icon from the left services navigation.



- \* 2. Under Manage, select Users.



- \* 3. Click on the Multi-Factor Authentication link.
  - \* 4. Tick the checkbox next to the user's name and click the Enable link.
- Reference:

<https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant>

### NEW QUESTION 130

- (Exam Topic 4)

You need to ensure that a user named user2-12345678 can manage the properties of the virtual machines in the RG1lod12345678 resource group. The solution must use the principle of least privilege.

To complete this task, sign in to the Azure portal.

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

- > Sign in to the Azure portal.
- > Browse to Resource Groups.
- > Select the RG1lod12345678 resource group.
- > Select Access control (IAM).
- > Select Add > role assignment.
- > Select Virtual Machine Contributor (you can filter the list of available roles by typing 'virtual' in the search box) then click Next.
- > Select the +Select members option and select user2-12345678 then click the Select button.
- > Click the Review + assign button twice.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal?tabs=current>

### NEW QUESTION 131

- (Exam Topic 4)

You need to ensure that the AzureBackupReport log for the Vault1 Recovery Services vault is stored in the WS11641655 Azure Log Analytics workspace.

To complete this task, sign in to the Azure portal and modify the Azure resources.

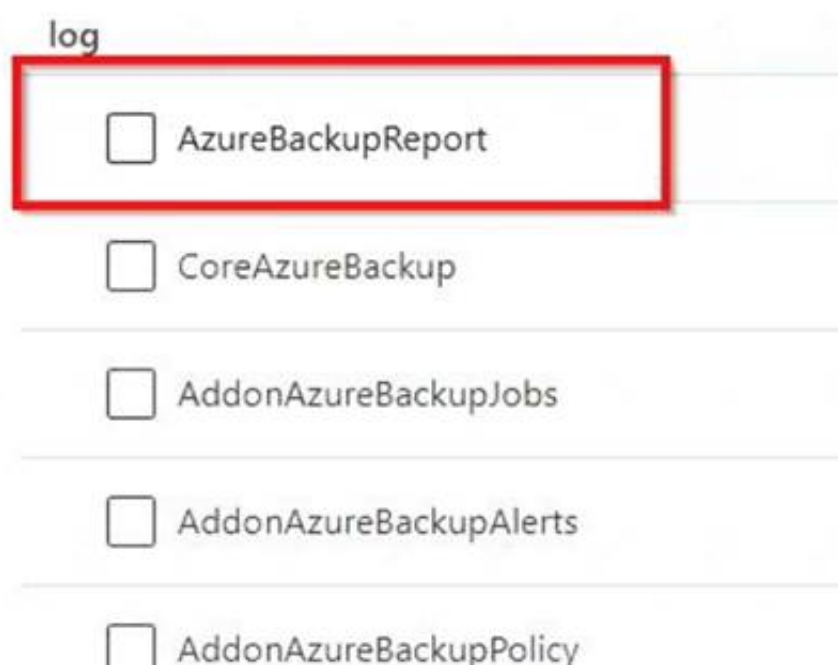
- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

- \* 1. In the Azure portal, type Recovery Services Vaults in the search box, select Recovery Services Vaults from the search results then select Vault1. Alternatively, browse to Recovery Services Vaults in the left navigation pane.
- \* 2. In the properties of Vault1, scroll down to the Monitoring section and select Diagnostic Settings.
- \* 3. Click the Add a diagnostic setting link.
- \* 4. Enter a name in the Diagnostic settings name box.
- \* 5. In the Log section, select AzureBackupReport.

#### Category details



log

☒ AzureBackupReport

☐ CoreAzureBackup

☐ AddonAzureBackupJobs

☐ AddonAzureBackupAlerts

☐ AddonAzureBackupPolicy

- \* 6. In the Destination details section, select Send to log analytics

## Destination details

☐ Send to Log Analytics

☐ Archive to a storage account

☐ Stream to an event hub

\* 7. Select the WS11641655 Azure Log Analytics workspace.

\* 8. Click the Save button to save the changes. Reference:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-diagnostic-events>

### NEW QUESTION 132

- (Exam Topic 4)

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

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

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

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

Solution: You create an initiative and an assignment that is scoped to the Tenant Root Group management group.

Does this meet the goal?

A. Yes

B. No

**Answer: A**

#### Explanation:

Reference:

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

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

### NEW QUESTION 137

- (Exam Topic 4)

You have an Azure subscription.

You need to create and deploy an Azure policy that meets the following requirements:

➤ When a new virtual machine is deployed, automatically install a custom security extension.

➤ Trigger an autogenerated remediation task for non-compliant virtual machines to install the extension. What should you include in the policy? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Definition effect:

Append  
DeployIfNotExists  
EnforceOPAConstraint  
EnforceRegoPolicy  
Modify

Assignment remediation task:

A managed identity that has the Contributor role  
A managed identity that has the User Access Administrator role  
A service principal that has the Contributor role  
A service principal that has the User Access Administrator role

A. Mastered

B. Not Mastered

**Answer: A**

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources>



### NEW QUESTION 138

- (Exam Topic 4)

You need to prevent administrators from performing accidental changes to the Homepage app service plan. To complete this task, sign in to the Azure portal.

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

You need to configure a 'lock' for the app service plan. A read-only lock ensures that no one can make changes to the app service plan without first deleting the lock.

- In the Azure portal, type App Service Plans in the search box, select App Service Plans from the search results then select Homepage. Alternatively, browse to App Service Plans in the left navigation pane.
- In the properties of the app service plan, click on Locks.
- Click the Add button to add a new lock.
- Enter a name in the Lock name field. It doesn't matter what name you provide for the exam.
- For the Lock type, select Read-only.
- Click OK to save the changes.

### NEW QUESTION 142

- (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 145

- (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 150

- (Exam Topic 4)

You have an Azure subscription that contains a web app named App1 and an Azure key vault named Vault1. You need to configure App1 to store and access the secrets in Vault1.

How should you configure App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Configure App1 to authenticate by using a:

Key
Certificate
Passphrase
User-assigned managed identity
System-assigned managed identity

Configure a Key Vault reference for App1 from the:

Extensions blade
General settings tab
TLS/SSL settings blade
Application settings tab

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Reference:

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

#### NEW QUESTION 154

- (Exam Topic 4)

You have a Microsoft Sentinel deployment.

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

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

**Answer Area**

Deploy:

Forward events to Microsoft Sentinel by using:

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

**Answer Area**

Deploy:

Forward events to Microsoft Sentinel by using:

#### NEW QUESTION 158

- (Exam Topic 4)

You have Azure Resource Manager templates that you use to deploy Azure virtual machines.

You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.

What should you use?

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

**Answer:** C

#### NEW QUESTION 161

- (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 166

- (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 170

- (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 171**

- (Exam Topic 4)

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

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

**Actions**

**Answer Area**

Create an access review program.

Set Reviewers to Selected users.

Create an access review audit.

Create an access review control.

Set Reviewers to Group owners.

Set Reviewers to Members.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Step 1: Create an access review program Step 2: Create an access review control Step 3: Set Reviewers to Group owners

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

**Reviewers**

Reviewers

Programs

Link to program

Group owners

Group owners

Selected users

Members (self)

References:

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

**NEW QUESTION 175**

- (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 NVET1, 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 176**

- (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 179**

- (Exam Topic 4)

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

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

All the virtual networks are peered. You deploy Azure Bastion to VNET2.

Which virtual machines can be protected by the bastion host?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 183**

- (Exam Topic 4)

You need to ensure that User2-11641655 has all the key permissions for KeyVault11641655. To complete this task, sign in to the Azure portal and modify the Azure resources.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

You need to assign the user the Key Vault Secrets Officer role.

- In the Azure portal, type Key Vaults in the search box, select Key Vaults from the search results then select KeyVault11641655. Alternatively, browse to Key Vaults in the left navigation pane.
- In the key vault properties, select Access control (IAM).
- In the Add a role assignment section, click the Add button.
- In the Role box, select the Key Vault Secrets Officer role from the drop-down list.
- In the Select box, start typing User2-11641655 and select User2-11641655 from the search results.
- Click the Save button to save the changes.

**NEW QUESTION 188**

- (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 191**

- (Exam Topic 4)

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

You plan to implement an application that will consist of the resources shown in the following table.

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

Users will authenticate by using their Azure AD user account and access the Cosmos DB account by using resource tokens.

You need to identify which tasks will be implemented in CosmosDB1 and WebApp1.

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

NOTE: Each correct selection is worth one point.

CosmosDB1:

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

WebApp1:

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

- A. Mastered
- B. Not Mastered

**Answer: A**

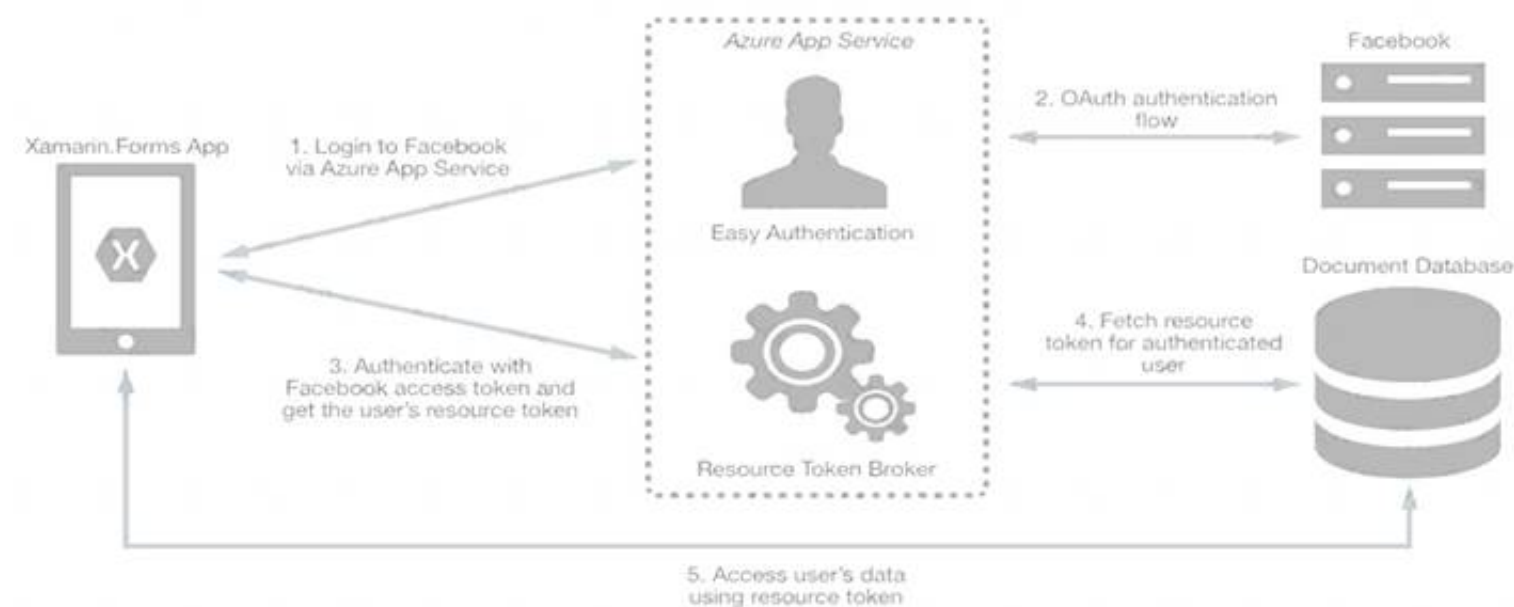
**Explanation:**

CosmosDB1: Create database users and generate resource tokens.

Azure Cosmos DB resource tokens provide a safe mechanism for allowing clients to read, write, and delete specific resources in an Azure Cosmos DB account according to the granted permissions.

WebApp1: Authenticate Azure AD users and relay resource tokens

A typical approach to requesting, generating, and delivering resource tokens to a mobile application is to use a resource token broker. The following diagram shows a high-level overview of how the sample application uses a resource token broker to manage access to the document database data:



**References:**

<https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication>

**NEW QUESTION 192**

- (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 193**

- (Exam Topic 4)

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

Name	Type
storage1	Azure Blob storage
storage2	Azure Files SMB
storage3	Azure Table storage

You need to configure authorization access.

Which authorization types can you use for each storage account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



storage1: ▼

Shared Key only
Shared access signature (SAS) only
Azure Active Directory (Azure AD) only
Shared Key and shared access signature (SAS) only
Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

storage2: ▼

Shared Key only
Shared access signature (SAS) only
Shared Key and shared access signature (SAS)

storage3: ▼

Shared Key only
Shared access signature (SAS) only
Azure Active Directory (Azure AD) only
Shared Key and shared access signature (SAS) only
Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

- 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/storage/common/authorize-data-access>

**NEW QUESTION 198**

- (Exam Topic 4)

You have multiple development teams that will create apps in Azure.

You plan to create a standard development environment that will be deployed for each team.

You need to recommend a solution that will enforce resource locks across the development environments and ensure that the locks are applied in a consistent manner.

What should you include in the recommendation?

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

**Answer:** D

**Explanation:**

Reference:

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

**NEW QUESTION 203**

- (Exam Topic 4)

You have an Azure subscription named Sub1.

You create a virtual network that contains one subnet. On the subnet, you provision the virtual machines shown in the following table.

Name	Network interface	Application security group assignment	IP address
VM1	NIC1	AppGroup12	10.0.0.10
VM2	NIC2	AppGroup12	10.0.0.11
VM3	NIC3	AppGroup3	10.0.0.100
VM4	NIC4	AppGroup4	10.0.0.200

Currently, you have not provisioned any network security groups (NSGs). You need to implement network security to meet the following requirements:

- Allow traffic to VM4 from VM3 only.
- Allow traffic from the Internet to VM1 and VM2 only.
- Minimize the number of NSGs and network security rules.

How many NSGs and network security rules should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



NSGs:

▼

1

2

3

4

Network security rules:

▼

1

2

3

4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NSGs: 1

Network security rules: 3

Not 2: You cannot specify multiple service tags or application groups) in a security rule. References:

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

NEW QUESTION 207

- (Exam Topic 4)

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

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

Currently, the domain and the tenant are not integrated.

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

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

Actions

Create a private link to storage1.

Enable Active Directory Domain Services (AD DS) authentication on storage1.

Implement Azure AD Connect.

Create a service endpoint to storage1.

Assign share-level permissions for share1.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 208

- (Exam Topic 4)

The developers at your company plan to publish an app named App11641655 to Azure.

You need to ensure that the app is registered to Azure Active Directory (Azure AD). The registration must use the sign-on URLs of <https://app.contoso.com>.

To complete this task, sign in to the Azure portal and modify the Azure resources.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Step 1: Register the Application

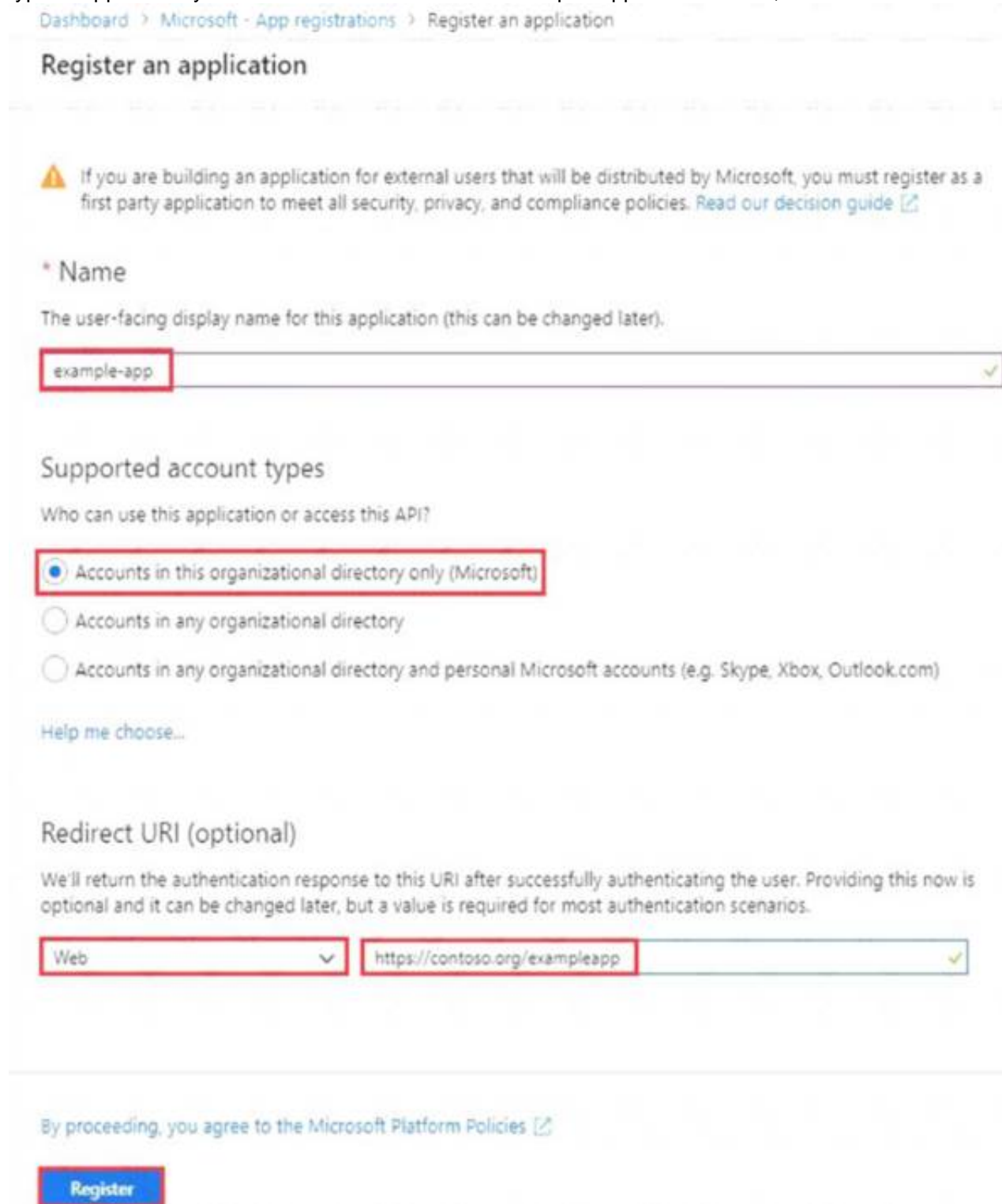
\* 1. Sign in to your Azure Account through the Azure portal.

\* 2. Select Azure Active Directory.

\* 3. Select App registrations.


\* 4. Select New registration.

\* 5. Name the application App11641655. Select a supported account type, which determines who can use the application. Under Redirect URI, select Web for the type of application you want to create. Enter the URI: <https://app.contoso.com> , where the access token is sent to.



Dashboard > Microsoft - App registrations > Register an application

## Register an application

 If you are building an application for external users that will be distributed by Microsoft, you must register as a first party application to meet all security, privacy, and compliance policies. [Read our decision guide](#)

**\* Name**

The user-facing display name for this application (this can be changed later).

example-app

**Supported account types**

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Microsoft)

☐ Accounts in any organizational directory

☐ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[Help me choose...](#)

**Redirect URI (optional)**

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

[By proceeding, you agree to the Microsoft Platform Policies](#)

**Register**

\* 6. Click Register

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

**NEW QUESTION 212**

- (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 216**

- (Exam Topic 4)

You create an Azure subscription with Azure AD Premium P2.

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

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

correct order.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 218

- (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 219

- (Exam Topic 4)  
You have the Azure key vaults shown in the following table.

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

KV1 stores a secret named Secret1 and a key for a managed storage account named Key1. You back up Secret1 and Key1.  
To which key vaults can you restore each backup? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

You can restore the Secret1 backup to:

▼

KV1 only

KV1 and KV2 only

KV1, KV2 and KV3 only

KV1, KV2 and KV4 only

KV1, KV2, KV3, KV4, and KV5

You can restore the Key1 backup to:

▼

KV1 only

KV1 and KV2 only

KV1, KV2 and KV3 only

KV1, KV2 and KV4 only

KV1, KV2, KV3, KV4, and KV5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 224

- (Exam Topic 4)

From Azure Security, you create a custom alert rule.  
You need to configure which users will receive an email message when the alert is triggered. What should you do?

- A. From Azure Monitor, create an action group.
- B. From Security Center, modify the Security policy settings of the Azure subscription.
- C. From Azure Active Directory (Azure AD). modify the members of the Security Reader role group.
- D. From Security Center, modify the alert rule.

Answer: A

Explanation:

References:  
<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups>

NEW QUESTION 227

- (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 231

- (Exam Topic 4)

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

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

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

- RT1: Includes a user-defined route that points to the private IP address of the Azure firewall as a next hop address
- RT2: Disables BGP route propagation and defines the private IP address of the Azure firewall as the default gateway

You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.

To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

RT1:

RT2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

RT1: 

GatewaySubnet

RT2: 

HubVNetSubnet0

NEW QUESTION 234

- (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 235

- (Exam Topic 4)

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

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

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

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

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

## multi-factor authentication

users service settings

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

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

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

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

180.15.10.0/24

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

Methods available to users:

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

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

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



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

#### NEW QUESTION 238

- (Exam Topic 4)

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

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

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

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

You plan to enable Azure Disk Encryption on VM1.

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

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

**Answer:** A

#### Explanation:

"Your key vault and VMs must be in the same subscription. Also, to ensure that encryption secrets don't cross regional boundaries, Azure Disk Encryption requires the Key Vault and the VMs to be co-located in the same region." <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault>

#### NEW QUESTION 241

- (Exam Topic 4)

You need to ensure that a user named Danny11597200 can sign in to any SQL database on a Microsoft SQL server named web11597200 by using SQL Server Management Studio (SSMS) and Azure Active Directory (Azure AD) credentials.

To complete this task, sign in to the Azure portal.

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

You need to provision an Azure AD Admin for the SQL Server.

- > In the Azure portal, type SQL Server in the search box, select SQL Server from the search results then select the server named web11597200. Alternatively, browse to SQL Server in the left navigation pane.
- > In the SQL Server properties page, click on Active Directory Admin.
- > Click the Set Admin button.
- > In the Add Admin window, search for and select Danny11597200.
- > Click the Select button to add Danny11597200.
- > Click the Save button to save the changes. Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?tabs=azure-powershell>

#### NEW QUESTION 244

- (Exam Topic 4)

You have a management group named Group1 that contains an Azure subscription named sub1. Sub1 has a subscription ID of 11111111-1234-1234-1234-111111111111.

You need to create a custom Azure role-based access control (RBAC) role that will delegate permissions to manage the tags on all the objects in Group1.

What should you include in the role definition of Role1? To answer, select the appropriate options in the answer area.



NOTE: Each correct selection is worth one point.

Resource provider:

Microsoft.Authorization
Microsoft.Resources
Microsoft.Support

Assignable scope:

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Text, application Description automatically generated

Note: Assigning a custom RBAC role as the Management Group level is currently in preview only. So, for now the answer to the assignable scope is the subscription level.

Reference:

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

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

**NEW QUESTION 248**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual az-500 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the az-500 Product From:

<https://www.2passeasy.com/dumps/az-500/>

## Money Back Guarantee

### **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