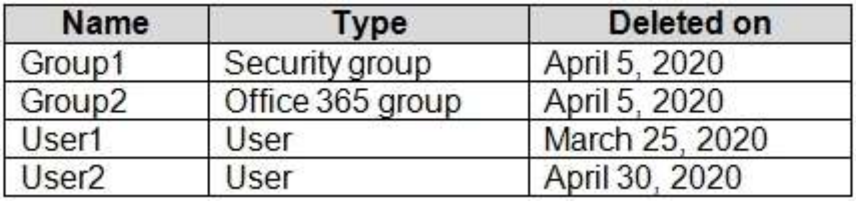
- **Vendor:** Microsoft
- **Exam Code:** AZ-500
- **Exam Name:** Microsoft Azure Security Technologies
- **New Updated Questions from Braindump2go (Updated in Dec./2020)**

QUESTION 192

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



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

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

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

Answer: BC
Explanation:
Deleted users and deleted Office 365 groups are available for restore for 30 days.
You cannot restore a deleted security group.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-restore-deleted

QUESTION 193

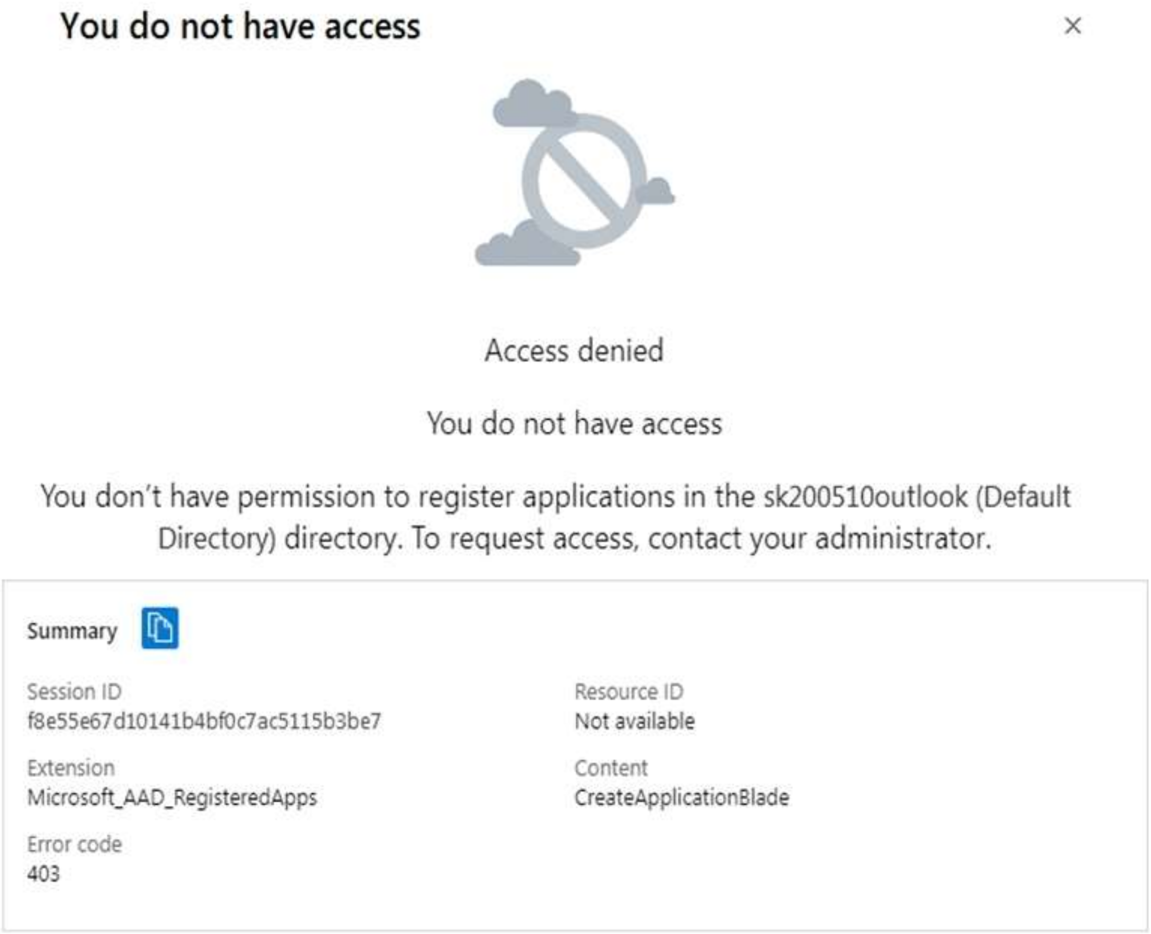
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1.
You plan to publish several apps in the tenant.
You need to ensure that User1 can grant admin consent for the published apps.
Which two possible user roles can you assign to User1 to achieve this goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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

Answer: BC
Explanation:

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

QUESTION 194
You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant.
When a developer attempts to register an app named App1 in the tenant, the developer receives the error message shown in the following exhibit.



You do not have access

×

Access denied

You do not have access

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

Summary

Session ID
f8e55e67d10141b4bf0c7ac5115b3be7

Resource ID
Not available

Extension
Microsoft_AAD_RegisteredApps

Content
CreateApplicationBlade

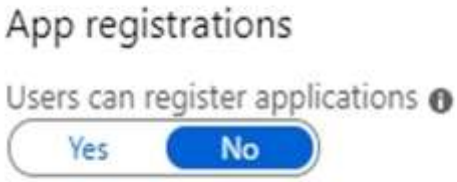
Error code
403

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

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

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

QUESTION 195
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.



App registrations

Users can register applications

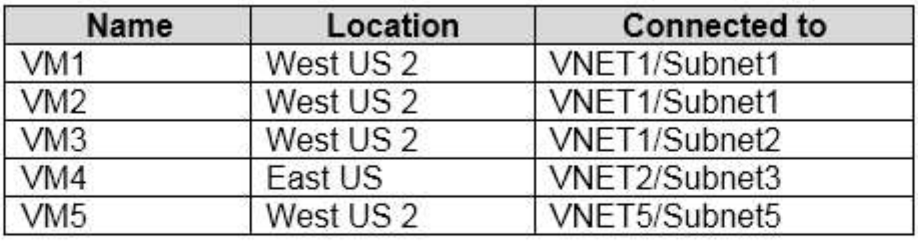
Yes [✓ No]

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

QUESTION 196
You have the Azure virtual machines shown in the following table.



Name	Location	Connected to
VM1	West US 2	VNET1/Subnet1
VM2	West US 2	VNET1/Subnet1
VM3	West US 2	VNET1/Subnet2
VM4	East US	VNET2/Subnet3
VM5	West US 2	VNET5/Subnet5

Each virtual machine has a single network interface.
You add the network interface of VM1 to an application security group named ASG1.
You need to identify the network interfaces of which virtual machines you can add to ASG1.
What should you identify?

A. VM2 only
B. VM2 and VM3 only
C. VM2, VM3, VM4, and VM5
D. VM2, VM3, and VM5 only

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups

QUESTION 197
You have an Azure subscription named Subcription1 that contains an Azure Active Directory (Azure AD) tenant named contoso.com and a resource group named RG1.
You create a custom role named Role1 for contoso.com.
You need to identify where you can use Role1 for permission delegation.
What should you identify?

A. contoso.com only
B. contoso.com and RG1 only
C. contoso.com and Subscription1 only
D. contoso.com, RG1, and Subcription1

Answer: D

QUESTION 198

You have an Azure subscription.
You enable Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
Your company's security policy for administrator accounts has the following conditions:

```
- The accounts must use multi-factor authentication (MFA).
- The accounts must use 20-character complex passwords.
- The passwords must be changed every 180 days.
- The accounts must be managed by using PIM.
```

You receive multiple alerts about administrators who have not changed their password during the last 90 days.
You need to minimize the number of generated alerts.
Which PIM alert should you modify?

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

Answer: D
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new

QUESTION 199

You have an Azure Active Directory (Azure AD) tenant named Contoso.com and an Azure Kubernetes 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.
D. From Azure AD, configure the User settings.

Answer: A
Explanation:
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli

QUESTION 200

You have an Azure subscription that contains an Azure Container Registry named Registry1. The subscription uses the Standard use tier of Azure Security Center.
You upload several container images to Register1.
You discover that vulnerability security scans were not performed.
You need to ensure that the images are scanned for vulnerabilities when they are uploaded to Registry1.
What should you do?

A. From the Azure portal modify the Pricing tier settings.
B. From Azure CLI, lock the container images.
C. Upload the container images by using AzCopy.
D. Push the container images to Registry1 by using Docker

Answer: A
Explanation:
https://charbelnemnom.com/scan-container-images-in-azure-container-registry-with-azure-security-center/

QUESTION 201

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 event hub

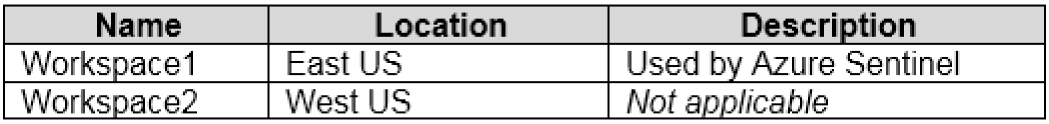
B. an Azure Log Analytics workspace

C. an Azure Storage account

Answer: B

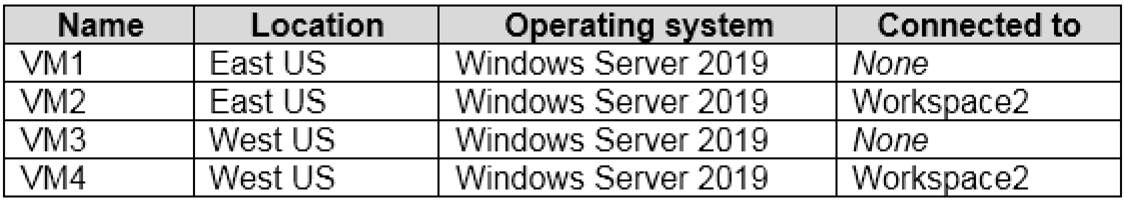
QUESTION 202

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



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

You create the virtual machines shown in the following table.



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

You plan to use Azure Sentinel to monitor Windows Defender Firewall on the virtual machines.

Which virtual machines you can connect to Azure Sentinel?

A. VM1 only

B. VM1 and VM3 only

C. VM1, VM2, VM3, and VM4

D. VM1 and VM2 only

Answer: C

Explanation:

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