Vendor: Microsoft

Exam Code:AZ-500

Exam Name: Microsoft Azure Security Technologies

Version: Demo

QUESTION 1

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.

The company is developing an application named App1. App1 will run as a service on server that runs Windows Server 2016. App1 will authenticate to contoso.com and access Microsoft Graph to read directory data.

You need to delegate the minimum required permissions to App1.

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

Select and Place:

Actions

Grant permissions

Add a delegated permission.

Configure Azure AD Application Proxy.

Add an application permission.

Create an app registration.

Answer Area

Correct Answer:

Actions

Add a delegated permission.

Configure Azure AD Application Proxy.

Answer Area

Create an app registration.

Add an application permission.

Grant permissions

Step 1: Create an app registration

First the application must be created/registered.

Step 2: Add an application permission

Application permissions are used by apps that run without a signed-in user present.

Step 3: Grant permissions

Incorrect Answers:

Delegated permission

Delegated permissions are used by apps that have a signed-in user present.

Application Proxy:

Azure Active Directory\\'s Application Proxy provides secure remote access to on-premises web applications.

References:

https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-permissions-and-consent

---

QUESTION 2

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.

Hot Area:

Answer Area

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. |

Correct Answer:

Answer Area

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. |

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:
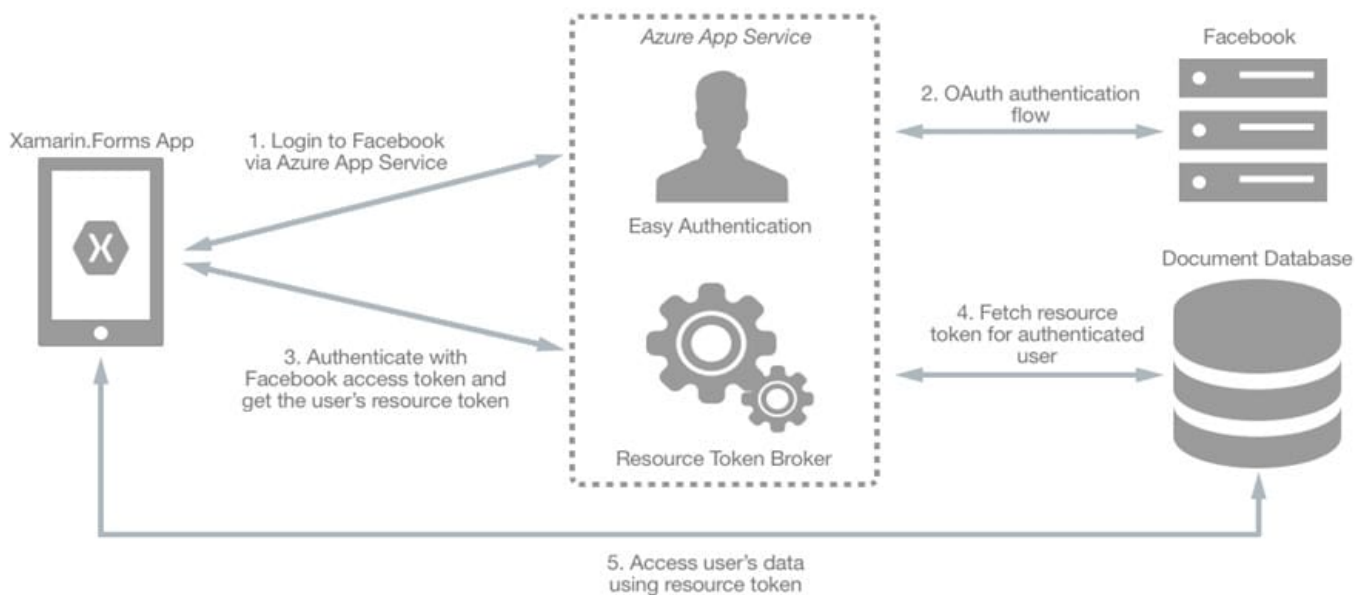
QUESTION 3

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 AD roles.

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

Select and Place:

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).	

Correct Answer:

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

QUESTION 4

SIMULATION

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. See the explanation below.

Correct Answer: A

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

1.

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.

2.

Select the server hosting the Homepage database and click on Manage backups.

3.

Click on Configure policies.

4.

Ensure that the Weekly Backups option is ticked.

5.

Configure the How long would you like weekly backups to be retained option to 8 weeks.

6.

Click Apply to save the changes.

QUESTION 5

SIMULATION

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

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

A. See the explanation below.

Correct Answer: A

To enable the RDP port in an NSG, follow these steps:

1.

Sign in to the Azure portal.

2.

In Virtual Machines, select VM1

3.

In Settings, select Networking.

4.

In Inbound port rules, check whether the port for RDP is set correctly. The following is an example of the configuration:

Priority: 300 Name: Port_3389 Port(Destination): 3389 Protocol: TCP Source: Any Destinations: Any Action: Allow

Reference: https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-nsg-problem

---

QUESTION 6

DRAG DROP

You have an Azure subscription named Sub1.

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

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

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

Select and Place:

Create a JSON file

Run the update-AzureRmManagementGroup cmdlet

Create an XML file

Run the New-AzureRmRoleDefinition cmdlet

Run the New-AzureRmRoleAssignment cmdlet

Correct Answer:

Run the update-AzureRmManagementGroup cmdlet	Create a JSON file
Create an XML file	Run the New-AzureRmRoleDefinition cmdlet
	Run the New-AzureRmRoleAssignment cmdlet

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

---

QUESTION 7

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

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

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

A. Assign User! the Authentication Policy Administrator role.

B. Enable Azure AD Password Protection.

C. Configure a multi-factor authentication (MFA) registration policy.

D. Create a new app registration.

Correct Answer: C

QUESTION 8

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 create a site-to-site VPN between the virtual network and the on-premises network.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

You can connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:

Create Azure Virtual Network.

Create a custom DNS server in the Azure Virtual Network.

Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.

Configure forwarding between the custom DNS server and your on-premises DNS server.

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

---

QUESTION 9

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

Correct Answer: A

QUESTION 10

You have an Azure virtual machine named VM1.

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

You need to resolve the issue causing the high-severity recommendation.

What should you do?

A. Add the Microsoft Antimalware extension to VM1.

B. Install Microsoft System Center Security Management Pack for Endpoint Protection on VM1.

C. Add the Network Watcher Agent for Windows extension to VM1.

D. Onboard VM1 to Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

Correct Answer: A

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

---

QUESTION 11

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

Correct Answer: D

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

---

QUESTION 12

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

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

A. Azure Security Center

B. Azure Policy

C. Azure AD Privileged Identity Management (PIM)

D. Azure Blueprints

Correct Answer: D

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

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as: Role Assignments Policy Assignments Azure Resource Manager templates Resource Groups

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