Question: 291

CertyIQ

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains a user named User1.
You configure app governance integration.
User1 needs to view the App governance dashboard. The solution must use the principle of the least privilege.
Which role should you assign to User1, and which portal should User1 use to view the dashboard? To answer, selec
the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Role:

- Application Administrator
- Application Developer
- Cloud Application Administrator

Portal:

- The Microsoft 365 admin center
- The Microsoft 365 Defender portal
- The Microsoft Defender for Cloud Apps portal
- The Microsoft Purview compliance portal

LIVEWORKSHEETS

Question: 298

CertyIQ

Case Study -
Overview -
Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure AD tenant named fabrikam.com.
Existing Environment. Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.
The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales

LIVEWORKSHEETS

•All users must be synced from AD DS to the contoso.com Azure AD tenant.
•App1 must have a redirect URI pointed to https://contoso.com/auth-response.
•License allocation for new users must be assigned automatically based on the location of the user.
•Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
•Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
•The helpdesk administrators must be able to manage licenses for only the users in their respective office.
•Users must be forced to change their password if there is a probability that the users' identity was compromised.
You need to meet the planned changes and technical requirements for App1.
What should you implement?

A.a policy set in Microsoft Intune

B.Azure AD Application Proxy

C.an app configuration policy in Microsoft Intune

D.an app registration in Azure AD

LIVEWORKSHEETS

Question: 299 CertyIQ

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 Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.
You deploy an Azure subscription and enable Microsoft 365 Defender.
You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.
Solution: From the Microsoft 365 Defender portal, you add the Google Workspace app connector.
Does this meet the goal?

A.Yes

B.No

LIVEWORKSHEETS

Question: 300

CertyIQ

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 Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.
You deploy an Azure subscription and enable Microsoft 365 Defender.
You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.
Solution: From the Microsoft 365 Defender portal, you add the Microsoft Azure app connector.
Does this meet the goal?

A.Yes

B.No

LIVEWORKSHEETS

Question: 301 CertyIQ

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 Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.
You deploy an Azure subscription and enable Microsoft 365 Defender.
You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.
Solution: From the Microsoft 365 Defender portal, you add the Amazon Web Services app connector.
Does this meet the goal?

A.Yes

B.No

LIVEWORKSHEETS

Question: 304

CertyIQ

HOTSPOT

-

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

Name	Type	Location
RG1	Resource group	East US
Managed1	Managed identity	East US
Managed2	Managed identity	West US

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

LIVEWORKSHEETS

Name	Location	Identity
VM1	East US	System-assigned
VM2	West US	System-assigned
VM3	East US	Managed1
VM4	West US	*None*

Which identities can be assigned the Owner role for RG1, and to which virtual machines can you assign Managed2?
To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Identities with Owner role:

- Managed1 only
- Managed1, VM1, and VM3 only
- Managed1, Managed2, and VM1 only
- Managed1, Managed2, VM1, and VM2 only
- Managed1, Managed2, VM1, VM2, and VM3 only

Virtual machines assigned to Managed2:

- VM4 only
- VM2 and VM4 only
- VM1, VM2, and VM4 only
- VM1, VM2, VM3, and VM4

LIVEWORKSHEETS

Question: 306 CertyIQ

HOTSPOT
-
You have a Microsoft Entra tenant that contains multiple storage accounts.
You plan to deploy multiple Azure App Service apps that will require access to the storage accounts.
You need to recommend an identity solution to provide the apps with access to the storage accounts. The solution must minimize administrative effort.
Which type of identity should you recommend, and what should you recommend using to control access to the storage accounts? To answer, select the appropriate options in the answer area.

LIVEWORKSHEETS

Answer Area

Identity type:

- Microsoft Entra user
- Service principal
- System-assigned managed identity
- User-assigned managed identity

To control access, use:

- Microsoft Entra Domain Services
- Role-based access control (RBAC)
- Shared access signature (SAS) tokens
- X.509 certificates

LIVEWORKSHEETS

Question: 309

CertyIQ

HOTSPOT
-
You have an Azure subscription named Sub1 that contains a storage account named storage1.
You need to deploy two apps named App1 and App2 that will have the following configurations:
•App1 will be deployed as a registered app in Sub1.
•App1 will access storage1 by using Microsoft Entra authentication.
•App2 will access storage1 by using a single Microsoft Entra identity.
•App2 be hosted on two new virtual machines named VM1 and VM2.
The solution must minimize administrative effort.
Which type of identity will each app use to access storage1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

App1:

- User-assigned managed identity
- Microsoft Entra group account
- Microsoft Entra user account
- Service principal
- System-assigned managed identity

App2:

- User-assigned managed identity
- Microsoft Entra group account
- Microsoft Entra user account
- Service principal
- System-assigned managed identity

LIVEWORKSHEETS

Question: 310

CertyIQ

HOTSPOT

-

You have a Microsoft 365 E5 subscription.

You need to configure app consent for the subscription. The solution must meet the following requirements:

- Disable user consent to apps.
- Configure admin consent workflow for apps.

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

NOTE: Each correct selection is worth one point.

Answer Area

Disable user consent to apps:

- Microsoft 365 admin center
- Microsoft 365 Apps admin center
- Microsoft 365 Defender portal
- Microsoft Purview compliance portal

Configure admin consent workflow for apps:

- Microsoft Entra admin center
- Microsoft 365 admin center
- Microsoft 365 Defender portal
- Microsoft Purview compliance portal

LIVEWORKSHEETS

Question: 312

CertyIQ

HOTSPOT

-

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

Name	Type	Name	Type
VM1	Virtual machine	VM1	Virtual machine
App1	Azure App Service web app	App1	Azure App Service web app
Managed1	Managed identity	Managed1	Managed identity
Managed2	Managed identity	*Not applicable*	*Not applicable*

You create a Microsoft Entra user named User1.

Which identities can you add to VM1 and App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct answer is worth one point.

LIVEWORKSHEETS

Answer Area

VM1:

- User1 only
- Managed2 only
- Managed1 and Managed2 only
- Managed2 and User1 only
- Managed1, Managed2, and User1

App1:

- User1 only
- Managed2 only
- Managed2 and User1 only
- A system-assigned managed identity only
- A system-assigned managed identity and Managed2 only
- A system-assigned managed identity, Managed2, and User1

LIVEWORKSHEETS

Question: 317

CertyIQ

HOTSPOT

-

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

Name	Type
VM1	Virtual machine
App1	Azure App Service web app
Managed1	Managed identity
Managed2	Managed identity

You create a Microsoft Entra user named User1.

Which identities can you add to VM1 and App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct answer is worth one point.

Answer Area

LIVEWORKSHEETS