Question: 378 CertyIQ

Case Study -
Overview -
ADatum Corporation is a consulting company in Montreal.
ADatum recently acquired a Vancouver-based company named Litware, Inc.
Existing Environment. ADatum Environment
The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.
ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.
ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.
The tenant contains the users shown in the following table.

Name	Role
User1	None
User2	None
User3	User administrator
User4	Privileged role administrator
User5	Identity Governance Administrator

The tenant contains the groups shown in the following table.

LIVEWORKSHEETS

•Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
- Email
- Phone
- Security questions
- The Microsoft Authenticator app
•Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
•The principle of least privilege must be used.
You need to modify the settings of the User administrator role to meet the technical requirements.
Which two actions should you perform for the role? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A.Select Require justification on activation.

B.Select Require ticket information on activation.

C.Modify the Expire eligible assignments after setting.

D.Set all assignments to Eligible.

E.Set all assignments to Active.

LIVEWORKSHEETS

Question: 380

CertyIQ

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3.
You have two Azure AD roles that have the Activation settings shown in the following table.

Name	Required justification on activation	Require approval to activate	Approvers
Role1	No	Yes	User1
Role2	Yes	No	None

The Azure AD roles have the Assignment settings shown in the following table.

Role	Allow permanent eligible assignment	Allow Permanent activate assignment	Require justification on active assignment
Role1	Yes	Yes	Yes
Role2	No	Yes	Yes

The Azure AD roles have the eligible users shown in the following table.

Role	Eligible assignment
Role1	User1, User2
Role2	User3

LIVEWORKSHEETS

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
If User1 requests Role1, the request will be approved automatically.	○	○
User1 can approve the request of User3 for Role2.	○	○
User1 must provide justification to approve the request of User2 for Role1.	○	○

LIVEWORKSHEETS

Question: 381

CertyIQ

HOTSPOT

-

You have a hybrid Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Application Administrator
Admin3	Cloud Application Administrator
Admin4	Application Developer
User1	None

You plan to deploy an on-premises app named App1. App1 will be registered in Azure AD and will use Azure AD Application Proxy.

You need to delegate the installation of the Application Proxy connector and ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.

Which user should perform the installation, and which role should you assign to User1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

LIVEWORKSHEETS

User that should perform the installation:

- Admin1
- Admin2
- Admin3
- Admin4

Assign User1 the role of:

- Application Administrator
- Application Developer
- Cloud Application Administrator
- Global Administrator

LIVEWORKSHEETS

Question: 382 CertyIQ

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of administrative unit
User1	AU1
User2	AU1
User3	AU1
User4	AU2
User5	Not a member of an administrative unit

The users are assigned the roles shown in the following table.

User	Role	Role scope
User1	Password Administrator	Organization
User2	Global Reader	Organization
User3	*None*	*Not applicable*
User4	Password Administrator	AU1
User5	*None*	*Not applicable*

For which users can User1 and User4 reset passwords? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

LIVEWORKSHEETS

Answer Area

User 1:

- User3 only
- User2 and User5 only
- User3 and User5 only
- User2, User3, and User5 only
- User3, User4 and User5 only
- User2, User3, User4, and User5

User 4:

- User3 only
- User2 and User3 only
- User3 and User5 only
- User1, User2, and User3 only

LIVEWORKSHEETS

Question: 387 CertyIQ

HOTSPOT
-
You have an Azure subscription.
Azure AD logs are sent to a Log Analytics workspace.
You need to query the logs and graphically display the number of sign-ins per user.

LIVEWORKSHEETS

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

Answer Area

```
SigninLogs
| where ResultType == 0
| [ ▼ ]  login_count = count() by Identity
| [ ▼ ]  columnchart
```

- extend
- print
- project
- render
- summarize

- extend
- print
- project
- render
- summarize

LIVEWORKSHEETS

Question: 390 CertyIQ

HOTSPOT
-
You have a Microsoft 365 E5 subscription.
You need to create a dynamic user group that will include all the users that do NOT have a department defined in their user profile.
How should you complete the membership rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

(user.department [▼] [▼])

-eq	""
-match	null
-ne	$null
-notIn	"null"

LIVEWORKSHEETS

Question: 395

CertyIQ

HOTSPOT
-
You have an Azure AD tenant.
You perform the tasks shown in the following table.

Date	Task
March 1	Register four enterprise applications named App1, App2, App3, and App4.
March 15	From the tenant, update the following settings for App1: App roles, Users and groups, Client secret, and Self-service.
March 20	From the tenant, update the following settings for App2: App roles, Users and groups, Client secret, and Self-service.
March 25	From the tenant, update the following settings for App3: App roles, Users and groups, Client secret, and Self-service.
March 30	From the tenant, update the following settings for App4: App roles, Users and groups, Client secret, and Self-service.

On April 5, an administrator deletes App1, App2, App3, and App4.
You need to restore the apps and the settings.

LIVEWORKSHEETS

NOTE: Each correct selection is worth one point.

Answer Area

Apps:

- No apps
- App4 only
- App3 and App4 only
- App2, App3, and App4 only
- App1, App2, App3, and App4

App4 settings:

- No settings
- Self-service only
- App roles and Client secret only
- Users and groups and Self-service only
- App roles, Users and groups, Client secret, and Self-service

LIVEWORKSHEETS

Question: 396 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 GitHub app connector.
Does this meet the goal?

A.Yes

B.No

LIVEWORKSHEETS

Question: 405

CertyIQ

DRAG DROP

-

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

Name	Type	Description
User1	User	*Not applicable*
User2	User	*Not applicable*
Vault1	Azure Key Vault	Contains a secret named Secret1
Vault2	Azure Key Vault	Contains a secret named Secret2
Secret1	Secret	Stored in Vault1
Secret2	Secret	Stored in Vault2

The subscription uses Privileged Identity Management (PIM).
You need to configure the following access controls by using PIM:
•Ensure that User1 can read and update Secret1.
•Ensure that User2 can read the contents of the secrets stored in Vault2.
The solution must follow the principle of least privilege.
Which authorization method should you use for each user? To answer, drag the appropriate authorization methods to the correct users. Each authorization method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Authorization methods

- The GET Secret Permissions Access Policy permission
- The Key Vault Secrets Officer RBAC role
- The Key Vault Reader RBAC role
- The Key Vault Secrets User RBAC role
- The LIST Secret Permissions Access Policy permission
- The SET Secret Permissions Access Policy permission

Answer Area

User1:

User2:

LIVEWORKSHEETS