Question: 217

CertyIQ

HOTSPOT

-

You have an Azure subscription named Sub1.

You plan to use Microsoft Entra Permissions Management to manage Sub1.

You need to ensure that Permissions Management can perform the following tasks:

- Identify unused permissions assigned to applications and managed identities.
- Provide users with recommendations about which permissions to remove.
- Remove unused permissions.

The solution must follow the principle of least privilege.

Which role should you assign to the service principal of Permissions Management, and what should you use to provide recommendations and remove unused permissions? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

LIVEWORKSHEETS

Role:

- Access Review Operator Service Role
- Owner
- Reader
- User Access Administrator

Use:

- A custom report
- A role template
- An audit query
- An Autopilot rule

LIVEWORKSHEETS

HOTSPOT

-

You have an Azure subscription named Sub1 that contains a resource group named RG1. RG1 contains two Azure key vaults named KV1 and KV2 that use Azure role-based access control (Azure RBAC).

The subscription contains the users shown in the following table.

Name	Role	Scope
User1	Key Vault Administrator	Sub1
User2	Key Vault Reade	RG1
User3	Key Vault Secrets User	KV1

KV1 contains a secret named Secret1. KV2 contains a secret named Secret2.

Which users can read the values of each secret? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

LIVEWORKSHEETS

Answer Area

Secret1:

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

Secret2:

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

LIVEWORKSHEETS

Question: 241 CertyIQ

HOTSPOT

-

You have a Microsoft 365 E5 subscription that has a Conditional Access policy named Policy1.

You need to perform the following actions:

•Create a Conditional Access App Control custom policy named Custom1.

•Configure Policy1 to use Custom1.

What should you use to create Custom1, and in which settings of Policy1 should you enable Conditional Access App Control? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

LIVEWORKSHEETS

Use:

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

Settings:

- Session
- Client apps under Conditions
- Filter for devices under Condit
- Grant
- Target resources

LIVEWORKSHEETS

Question: 243 CertyIQ

HOTSPOT

-

You have a Microsoft 365 subscription that contains three users named User1, User2, and User3 and an enterprise app named App1. The subscription contains the devices shown in the following table.

Name	Compliance state
Device1	Compliant
Device2	Compliant
Device3	Compliant

The subscription contains the groups shown in the following table.

Name	Members
Group1	User1, User3
Group2	User2, User3
Group3	User1

You create two Conditional Access policies that have the following settings:

•Name: Policy1
•Users:
oInclude: Group1
oExclude: Group3
•Target resources:
oInclude: All resources
•Access controls: Block access
•Name: Policy2
•Users:
oInclude: Group2
•Target resources:
oInclude: App1
•Access controls:
oGrant access: Require device to be marked as compliant.

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

LIVEWORKSHEETS

Answer Area

Statements	Yes	No
User1 can sign in to App1 from Device1.	○	○
User2 can sign in to App1 from Device2.	○	○
User3 can sign in to App1 from Device3.	○	○

LIVEWORKSHEETS