

Question: 158**HOTSPOT**

-

You have an Azure subscription that contains the following virtual machine:

- Name: V1
- Azure region: East US
- System-assigned managed identity: Disabled

You create the managed identities shown in the following table.

Name	Location
Managed1	East US
Managed2	East US
Managed3	West US

You perform the following actions:

- Assign Managed1 to V1.
- Create a resource group named RG1 in the West US region.

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
You can assign Managed2 to V1.	☐	☐
You can assign Managed3 to V1.	☐	☐
You can assign VM1 the Owner role for RG1.	☐	☐

HOTSPOT

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

Name	In resource group	Number of days to retain deleted key vaults	Purge protection
KeyVault1	RG1	15	Enabled
KeyVault2	RG1	10	Disabled

The subscription contains the users shown in the following table.

Name	Role
Admin1	Key Vault Administrator
Admin2	Key Vault Contributor
Admin3	Key Vault Certificates Officer
Admin4	Owner

On June 1, Admin4 performs the following actions:

- Deletes a certificate named Certificate1 from KeyVault1
- Deletes a secret named Secret1 from KeyVault2

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
Admin1 can recover Secret1 on June 7.	☐	☐
Admin2 can purge Certificate1 on June 12.	☐	☐
Admin3 can purge Certificate1 on June 14.	☐	☐

Question: 163

CertyIQ

HOTSPOT

-

You have a Microsoft 365 tenant.

You configure a conditional access policy as shown in the Conditional Access policy exhibit. (Click the Conditional Access policy tab.)

Home > ContosoAzureAD > Security > Conditional Access

Policy1 ...

Conditional access policy

 Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Policy1

Assignments

Users and groups ⓘ

[All users](#)

Cloud apps or actions ⓘ

[All cloud apps](#)

Conditions ⓘ

[0 conditions selected](#)

Access controls

Grant ⓘ

[1 control selected](#)

Session ⓘ

[0 controls selected](#)

Grant



Control user access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☒ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ
[See list of approved client apps](#)

☐ Require app protection policy ⓘ
[See list of policy protected client apps](#)

☐ Require password change ⓘ

For multiple controls

☐ Require all the selected controls

☒ Require one of the selected controls

Enable policy

Report-only

On

Off

Save

Select

You view the User administrator role settings as shown in the Role setting details exhibit. (Click the Role setting details tab.)

... > Privileged Identity Management > ContosoAzureAD > User Administrator >

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

 Edit

Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes

 LIVEWORKSHEETS

Allow permanent eligible assignment	No
Expire eligible assignments after	15 day(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	No

You view the User administrator role assignments as shown in the Role assignments exhibit. (Click the Role assignments tab.)

... > ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD >



User Administrator | Assignments

Privileged Identity Management | Azure AD roles

»

[+ Add assignments](#) [Settings](#) [Refresh](#) [Export](#) | [Got feedback?](#)

Eligible assignments Active assignments Expired assignments



User Administrator | Assignments

Privileged Identity Management | Azure AD roles

>>

[+ Add assignments](#) [Settings](#) [Refresh](#) [Export](#) | [Got feedback?](#)

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

Name	Principal name	Type	Scope	Membership
User Administrator				
Admin1	Admin1@m365x629615.onmicrosoft.com	User	Directory	Direct
Admin2	Admin2@m365x629615.onmicrosoft.com	User	Directory	Direct
Admin3	Admin3@m365x629615.onmicrosoft.com	User	Directory	Direct

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

Statements	Yes	No
Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.	☐	☐
Admin2 can request activation of the User administrator role for a period of two hours.	☐	☐
If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice.	☐	☐

Question: 164**HOTSPOT**

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

Name	User risk level
User1	Low
User2	Medium
User3	High

You have the Azure AD Identity Protection policies shown in the following table.

Type	Users	User risk	Sign-in risk	Controls
User risk policy	All users	Low and above	Unconfigured	Block access
Sign-in risk policy	All users	Unconfigured	High	Block access

You review the Risky users report and the Risky sign-ins report and perform actions for each user as shown in the following table.

User	Action
User1	Confirm user compromised
User2	Confirm sign-in safe
User3	Dismiss user risk
User2	Confirm user compromised

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

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

Statements	Yes	No
User1 can sign in by using multi-factor authentication (MFA).	☐	☐
User2 can sign in by using multi-factor authentication (MFA).	☐	☐
User3 can sign in from an anonymous IP address.	☐	☐

Question: 166

CertyIQ

DRAG DROP

You have a Microsoft 365 E5 subscription and an Azure subscription.

You need to meet the following requirements:

- Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials.
- Delegate the ability to create new virtual machines.

What should you use for each requirement? To answer, drag the appropriate features to the correct requirements. Each feature 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.

Features

Azure AD built-in roles

Azure AD managed identities

Azure role-based access control (Azure RBAC)

Answer Area

Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials:

Delegate the ability to create new virtual machines:

Question: 168

CertyIQ

HOTSPOT

-

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant. The AD DS domain contains the organizational units (OUs) shown in the following table.

Name	Description
OU1	Syncs with Azure AD
OU2	Does NOT sync with Azure AD

You need to create a break-glass account named BreakGlass.

Where should you create BreakGlass, and which role should you assign to BreakGlass? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Location:

▼

Azure AD
OU1
OU2

Role:

▼

Billing Administrator
Global Administrator
Owner
Privileged Role Administrator

Question: 170

CertyIQ

HOTSPOT

-

You have an Azure subscription.

You need to create two custom roles named Role1 and Role2. The solution must meet the following requirements:

- Users that are assigned Role1 can manage application security groups.
- Users that are assigned Role2 can manage Azure Firewall.

Which resource provider permissions are required for each role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.