

Question: 355**HOTSPOT -**

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com. The company has a business partner named Fabrikam, Inc.

Fabrikam uses Azure AD and has two verified domain names of fabrikam.com and litwareinc.com. Both domain names are used for Fabrikam email addresses.

You plan to create an access package named package1 that will be accessible only to the users at Fabrikam.

You create a connected organization for Fabrikam.

You need to ensure that the package1 will be accessible only to users who have fabrikam.com email addresses.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To allow access for users who have fabrikam.com email addresses, configure:

☐	An access package assignment in Identity Governance
☐	An access package policy in Identity Governance
☐	A conditional access policy in Azure AD
☐	The External collaboration settings in Azure AD

To block access for users who have litwareinc.com email addresses, configure:

☐	An access package assignment in Identity Governance
☐	An access package policy in Identity Governance
☐	A conditional access policy in Azure AD
☐	The External collaboration settings in Azure AD

Question: 358**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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.

You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure AD, you modify the Diagnostics settings.
Does this meet the goal?

- A. Yes
- B. No

Question: 359**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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.

You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure Monitor, you create a data collection rule.

Does this meet the goal?

A. Yes

B. No

Question: 361

CertyIQ

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant contains the users shown in the following table.

Name	Role
User1	None
User2	Privileged authentication administrator
User3	Global administrator

In Azure AD Privileged Identity Management (PIM), you configure the Global administrator role as shown in the following exhibit.

 Edit

Setting	State
Activation maximum duration (hours)	1 hour(s)
vRequire justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	No
Approvers	None

Assignment

Setting	State
Allow permanent eligible assignment	Yes
Expire eligible assignments after	-
Allow permanent active assignment	Yes
Expire active assignments after	-

User1 is eligible for the Global administrator role.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Statements	Yes	No
User1 requires Azure Multi-Factor Authentication (MFA) to activate the Global administrator role.	☐	☐
User2 must approve all activation requests for the Global administrator role.	☐	☐
User2 and User3 can edit the Global administrator role assignment.	☐	☐

Question: 363**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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.

You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure Monitor, you modify the action group.

Does this meet the goal?

A. Yes

B. No

Question: 364**HOTSPOT -**

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant.

The tenant contains the groups shown in the following table.

Name	Source	Member of
Group1	Cloud	Group3
Group2	Active Directory domain	None
Group3	Cloud	None

The tenant contains the users shown in the following table.

Name	Directory-synced	Member of
User1	No	Group1
User2	No	Group2
User3	Yes	Group3

You create an access review as shown in the following table.

Setting	Value
Review type	Teams + Groups
Review scope	All users
Group	Group2, Group3

Review type	Teams + Groups
Review scope	All users
Group	Group2, Group3
Reviewers	Users review own access
If reviewers don't respond	Remove access

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 will be removed automatically from Group 1 if the user does not respond to the review request.	☐	☐
User 2 will be removed automatically from Group 3 if the user does not respond to the review request.	☐	☐
User 3 will be removed automatically from Group 2 if the user does not respond to the review	☐	☐

HOTSPOT -

You have an Azure Active Directory (Azure AD) ten-ant: that contains the groups shown in the following table.

Name	Owner	Number of internal users	Number of guest users
Group1	User1	500	25
Group2	User2	295	100

You create an access review for Group1 as shown in the following table.

Setting	Value
Review type	Teams + Groups
Review scope	All users
Reviewers	Users review own access

You create an access review for Group2 as shown in the following table.

Setting	Value
Review type	Teams + Groups
Review scope	Guest users only
Reviewers	Group owner

What is the minimum number of Azure Active Directory Premium P2 licenses required for each group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Group1: ▼

1
500
525

Group2: ▼

1
100
295
395

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a group named All Company and has the following Identity Governance settings:

- ⇒ Block external users from signing in to this directory: Yes
- ⇒ Remove external user: Yes
- ⇒ Number of days before removing external user from this directory: 30

On March 11, 2022, you create an access package named Package1 that has the following settings:

⇒ Resource roles

1. Name: All Company
2. Type: Group and Team
3. Role: Member

⇒ Lifecycle

1. Access package assignment expire: On date
2. Assignment expiration date: April 1, 2022

On March 1, 2022, you assign Package1 to the guest users shown in the following table.

Name	Email address
Guest1	guest1@outlook.com
Guest2	guest2@outlook.com

On March 2, 2022, you assign the Reports reader role to Guest1.

On April 1, 2022, you invite a guest user named Guest3 to contoso.com.

On April 4, 2022, you add Guest3 to the All Company group.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Statements

Yes

No

On May 5, 2022, the Guest1 account is in contoso.com.

☐
☐

On May 5, 2022, the Guest2 account is in contoso.com.

☐
☐

On May 5, 2022, the Guest3 account is in contoso.com.

☐
☐

Question: 370

CertyIQ

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains three users named User1, User2, and User3. You create a group named Group1. You add User2 and User3 to Group1. You configure a role in Azure AD Privileged Identity Management (PIM) as shown in the Application Administrator exhibit. (Click the Application Administrator tab.)

Role setting details - Application Administrator

Privileged Identity Management | Azure AD roles

 Edit

Activation

Setting	State
Activation maximum duration (hours)	5 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	Yes
Approvers	0 Member(s), 1 Group(s)

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)

Require Azure Multi-Factor Authentication on acti...	No
Require justification on active assignment	Yes

Group1 is configured as the approver for the Application administrator role.
You configure User2 to be eligible for the Application administrator role.
For User1 you add an assignment to the Application administrator role as shown in the Assignment exhibit. (Click the Assignment tab.)