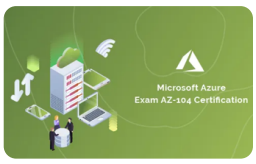


Level: Advanced

Microsoft Azure Exam AZ-104 Certification

Back to the **Course**

Manage Azure identities and governance - **Practice Mode**

Completed on Tue, 30 Sep 2025

Attempt | Marks Obtained | Your Score | Result

Share this Report in Social Media Share

Download Report

Domain wise Quiz Performance Report

No.	Domain	Total Question	Correct	Incorrect	Unattempted	Marked for Review
1	Manage Azure identities and governance	15	8	7	0	0
Total	All Domains	15	8	7	0	0

Review the Answers

Filter By

Question 1

Incorrect

Domain: Manage Azure identities and governance

Contoso Inc. is migrating its user management system to Microsoft Entra. The IT administrator is tasked with adding and updating employee profile information in the Microsoft Entra admin center. The IT administrator needs to ensure that each user's profile reflects accurate details. What category should the IT administrator navigate to in the Microsoft Entra admin center to update an employee's profile with the new job title and department?

- A. Identity wrong
- B. Job Information right

C. Contact Info

D. Parental Controls

E. Settings

Explanation:

Correct Answer: B

Option B is CORRECT because in the Microsoft Entra admin center, the "Job Information" category serves as a dedicated section for administrators to manage and update user profiles with job-related details, including job titles and departments. This category is crucial in ensuring that user profiles accurately reflect each user's role within the organization. By navigating to the "Job Information" section, IT administrators can efficiently update employees' profiles with the new job title and department, thereby maintaining the integrity and accuracy of user profiles across the organization's Microsoft Entra environment.

To update the employee's job title or department the IT administrator needs to perform the following steps -

Sign in to the Microsoft Entra admin center

Browse to Identity → Users → All users

Select the employee

Select Edit properties

Navigate to the Job Information section to update the employee's job title or department

Option A is INCORRECT because this category typically deals with user-specific information such as username, display name, and user principal name. It is primarily focused on managing identity-related data for users in the Microsoft Entra environment.

Option C is INCORRECT because this category is dedicated to managing contact information for users, including phone numbers, email addresses, and mailing addresses. It does not encompass job-related details such as job title and department.

Option D is INCORRECT because this category in the Microsoft Entra admin center focuses on settings related to managing access and permissions for minors. It is unrelated to updating user profiles with job-specific information.

Option E is INCORRECT because while the "Settings" category may offer various options for configuring the Microsoft Entra environment, it does not specifically address updating user profiles with job-related information like job title and department.

Reference:

https://learn.microsoft.com/en-us/entra/fundamentals/how-to-manage-user-profile-info?WT.mc_id=AZ-MVP-5004069#add-or-change-profile-information

Ask our Experts

Did you like this **Question?**

Question 2 Incorrect

Domain: Manage Azure identities and governance

Contoso Inc. is implementing Microsoft Entra for managing group properties and group membership. The IT administrator needs to create a new group and add members using the Microsoft Entra admin center. Based on the scenario, which statements are correct regarding creating a group and adding members in Microsoft Entra? (Select 3 options)

Your Answer

- The IT administrator must have the Groups Administrator or User Administrator role to create a basic group and add members simultaneously.
- The IT administrator needs a P1 or P2 license and the Privileged Role Administrator role to enable the option for assigning Microsoft Entra roles to the group.
- The IT administrator can add Owners or Members to the group during the group creation process

Correct Answer

- The IT administrator must have the Groups Administrator or User Administrator role to create a basic group and add members simultaneously.
- The IT administrator can add Owners or Members to the group during the group creation process
- The IT administrator can edit a group's name, description, or membership type at any time without role restrictions

Explanation:

Correct Answers: A, C, and E

Option A is CORRECT because in the Microsoft Entra admin center, creating a basic group and adding members simultaneously is a privileged action that requires specific administrative roles. The Groups Administrator or User Administrator roles are essential for this task. These roles empower the IT administrator with the necessary permissions to manage groups and their membership efficiently. Without these roles, the IT administrator won't have the authority to perform such actions, ensuring proper access control and security within the organization's Microsoft Entra environment.

Option C is CORRECT because during the group creation process, the IT administrator can assign ownership and membership roles to users right from the outset. This flexibility streamlines the group management process, allowing the IT administrator to establish the group's structure and permissions effectively. By adding Owners or Members during the creation phase, the IT administrator ensures that the group is properly configured and ready for use as soon as it is created.

Option E is CORRECT because the IT administrator can modify various aspects of a group, including its name, description, or membership type, at any time. This flexibility enables him to adapt the group settings to meet changing organizational needs efficiently. The IT administrator can make these changes without being restricted by specific roles in the Microsoft Entra admin center. This ensures that the group remains dynamic and aligned with the organization's objectives over time.

Option B is INCORRECT because the availability of the Group email address option depends on the group type selected during the group creation process in the Microsoft Entra admin center, and not on the IT administrator's action. This option is not available for all group types. This option is only available for Microsoft 365 group types.

Option D is INCORRECT because while the IT administrator may need a P1 or P2 license and the Privileged Role Administrator role to assign Microsoft Entra roles to a group, these requirements do not apply to enable the option for assigning roles. The IT administrator can create a group without these requirements but won't be able to assign roles without meeting them.

Reference:

https://learn.microsoft.com/en-us/entra/fundamentals/how-to-manage-groups?WT.mc_id=AZ-MVP-5004069#create-a-basic-group-and-add-members

Ask our Experts

Did you like this **Question?**

Question 3 Correct

Domain: Manage Azure identities and governance

Contoso Inc. is implementing Microsoft Entra Privileged Identity Management (PIM) to enhance security measures. However, they are uncertain about the licensing requirements for PIM usage.

Proposed Solution:

Contoso Inc. must ensure they possess either Microsoft Entra ID Governance licenses or Microsoft Entra ID P2 licenses for PIM usage. These licenses cover various user categories, including role assignments, group memberships, approval privileges, and access review duties. Is this proposed solution correct? (Select True or False)

A. True right

B. False

Explanation:

Correct Answer: A

Option A is CORRECT because it addresses the licensing requirements for Microsoft Entra Privileged Identity Management (PIM) implementation, which was the problem posed in the question. It emphasizes the critical need for either Microsoft Entra ID Governance licenses or Microsoft Entra ID P2 licenses to facilitate various aspects of PIM usage, including role assignments, group memberships, approval privileges, and access review duties. By acquiring the appropriate licenses, Contoso Inc. can ensure compliance with licensing regulations and effectively integrate PIM into its security framework to manage privileged identities securely and efficiently.

Option B is INCORRECT because the above-proposed solution is True.

Reference:

https://learn.microsoft.com/en-us/entra/fundamentals/licensing#microsoft-entra-privileged-identity-management

Ask our Experts

Did you like this **Question?**

Question 4 Correct

Domain: Manage Azure identities and governance

Contosos Ltd. is transitioning its license management to group-based licensing in Microsoft Entra ID for improved efficiency. The IT lead is assigning licenses to departmental groups. The lead needs to ensure that licenses are automatically managed when users join or leave the Finance Department's security group. Which aspect of group-based licensing facilitates this automatic management?

A. Group-based licensing disables unnecessary service plans automatically

B. Group-based licensing supports synchronization with on-premises Microsoft Entra ID group

C. Group-based licensing automatically adjusts license assignments based on group membership changes right

D. Group-based licensing requires manual intervention for license adjustments

E. Group-based licensing is limited to Microsoft 365 products only

---

Explanation:

Correct Answer: C

Option C is CORRECT because it is one of the key features of group-based licensing in Microsoft Entra ID. With group-based licensing, licenses are assigned based on the membership of specific groups. When users join or leave these groups, the license assignments are automatically adjusted accordingly. This automation ensures that users have the appropriate licenses assigned to them as their roles within the organization change, without the need for manual intervention. In the scenario provided, the IT lead is assigning licenses to departmental groups. By utilizing group-based licensing, it can be ensured that licenses for the Finance Department are automatically managed when users join or leave the Finance Department's security group.

Option A is INCORRECT because it suggests that group-based licensing automatically disables unnecessary service plans, which is not accurate. It primarily focuses on managing license assignments based on group membership changes, rather than service plan management.

Option B is INCORRECT because it correctly states that group-based licensing supports synchronization with on-premises Microsoft Entra ID groups. However, synchronization alone doesn't directly address the requirement of automatically managing licenses based on group membership changes.

Option D is INCORRECT because group-based licensing is designed to automate the process of license adjustments based on group membership changes, eliminating the need for manual intervention.

Option E is INCORRECT because group-based licensing can be used for various Microsoft products and services, not limited to Microsoft 365 products.

Reference:

https://learn.microsoft.com/en-us/entra/fundamentals/concept-group-based-licensing#features

Ask our Experts

Did you like this **Question?**

Question 5 Correct

Domain: Manage Azure identities and governance

Contoso Ltd. is planning to enforce conditional access policies to control access to their Microsoft Entra tenant based on specific conditions. Which license is required to implement risk-based conditional access?

A. Microsoft Entra ID Free - Security defaults

B. Microsoft Entra ID P2 right

C. Microsoft Entra ID P1

D. Office 365

E. Microsoft Entra ID Free - Global Administrators only

Explanation:

Correct Answer: B

Option B is CORRECT because Microsoft Entra ID P2 includes all features of P1 and adds additional advanced security capabilities, including risk-based conditional access policies. This feature allows organizations to dynamically adjust access controls based on the risk level associated with a user's sign-in attempt, device location, or other contextual factors. Microsoft Entra ID P2 enables administrators to define specific conditions under which access is granted or denied, helping organizations enforce security policies more effectively. This granular control enhances security posture by allowing organizations to respond dynamically to emerging threats or suspicious activities. It offers a holistic security solution that helps organizations protect their digital assets and mitigate cybersecurity risks effectively.

Option A is INCORRECT because the free version of Microsoft Entra only includes basic security features like protecting Microsoft Entra tenant admin accounts with MFA, the Mobile app as a second factor, and Self-service password reset (SSPR). It does not support advanced conditional access policies like risk-based conditional access.

Option C is INCORRECT because Microsoft Entra ID P1 offers some advanced security features, but it does not include risk-based conditional access policies, which are available in the P2 version. Some of the features of Microsoft Entra ID P1 are Fraud alerts, MFA Reports, Custom greetings for phone calls, Conditional Access, etc.

Option D is INCORRECT because the Office 365 license provides access to features like Remember MFA for trusted devices, Self-service password reset (SSPR), Admin control over verification methods, etc. They do not include the security features necessary for implementing risk-based conditional access policies.

Option E is INCORRECT because even though it's a free version, it only allows access for global administrators and does not include the necessary features for implementing risk-based conditional access policies. It includes some features like Admin control over verification methods, Remember MFA for trusted devices, Self-service password reset (SSPR), etc.

Reference:

https://learn.microsoft.com/en-us/entra/fundamentals/licensing#authentication

Ask our Experts

Did you like this **Question?**

Question 6 Correct

Domain: Manage Azure identities and governance

You want to invite an external guest user to your Microsoft Entra ID tenant.

You enable the send invite message checkbox while sending the email invitation.

Which of the following are mandatory field(s) that are required to be validated and send the invitation request? (Select Two)

- [x] A. Email right
- [ ] B. Display Name
- [ ] C. CC recipient
- [x] D. Invite redirect URL right

Explanation:

Correct Answer: A and D

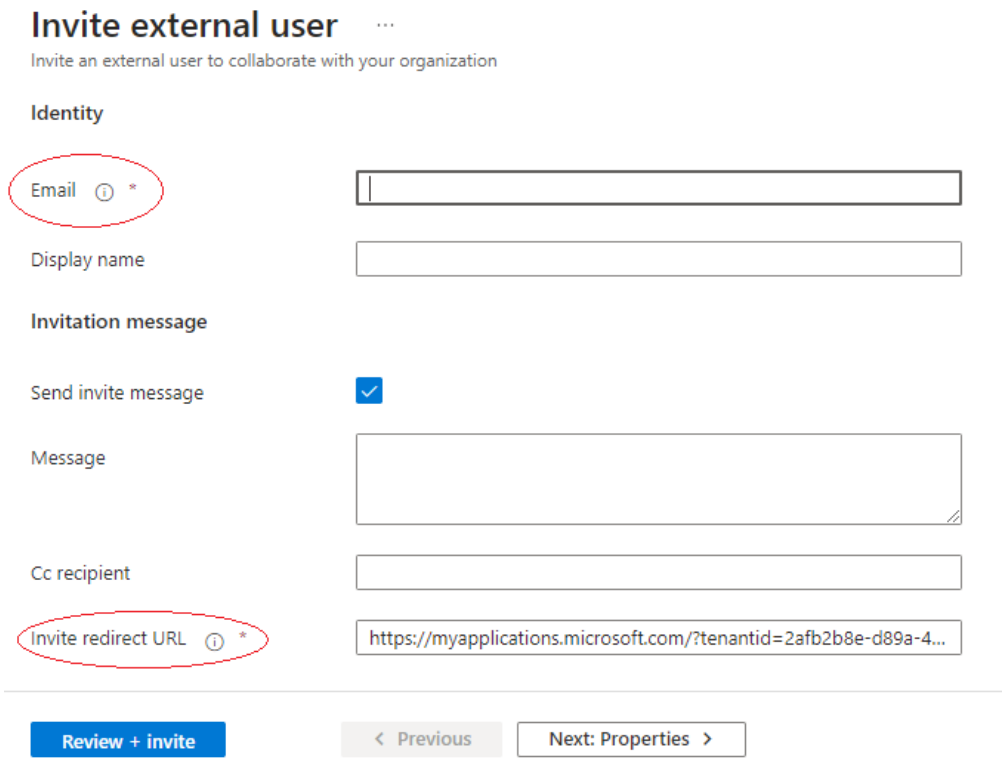
Option A is CORRECT because to invite an external guest user to your Microsoft Entra ID tenant, you need to specify the email address of the external guest user to whom the invitation will be sent. Without the email address, the system would not know where to send the invitation. Thus, Email is a mandatory field that needs to be updated to validate the invitation request.

Option D is CORRECT because the invite redirect URL is the URL to which the user is redirected once the invitation is redeemed. After the external guest user accepts the invitation, they need to be redirected somewhere, such as a sign-up page or a landing page with more information. Providing the redirect URL is necessary for the invitation process to proceed smoothly. By default, if no changes are made in the invite redirect URL field, the user will be redirected to the MyApplications page. Thus, the invite redirect URL is a mandatory field that needs to be included to validate the invitation request.

Option B is INCORRECT because while displaying the name of the guest user may be desirable for personalization purposes, it's not mandatory for sending the invitation. If the Display Name field is left blank while sending the request, the system allocates the username part of the email address as the default Display Name for that specific guest user.

Option C is INCORRECT because the CC recipient field is required to include additional recipients who will receive a copy of the email invitation alongside the guest user. However, it's not mandatory to send the invitation to the external guest user.

Architectural Diagram/Snapshots:



Reference:

How to create or delete users in Microsoft Entra ID

Ask our Experts

Did you like this **Question?**

Question 7

Incorrect

Domain: Manage Azure identities and governance

You have an external user named "External User" in your Microsoft Entra ID tenant.

You want to convert the user into an Internal user. Which specific tile option do you select in the My Feed section of the overview blade to convert an external user to an internal user?

- A. B2B Invitation wrong
- B. Account Status
- C. Edit properties
- D. B2B collaboration right

Explanation:

Correct Answer: D

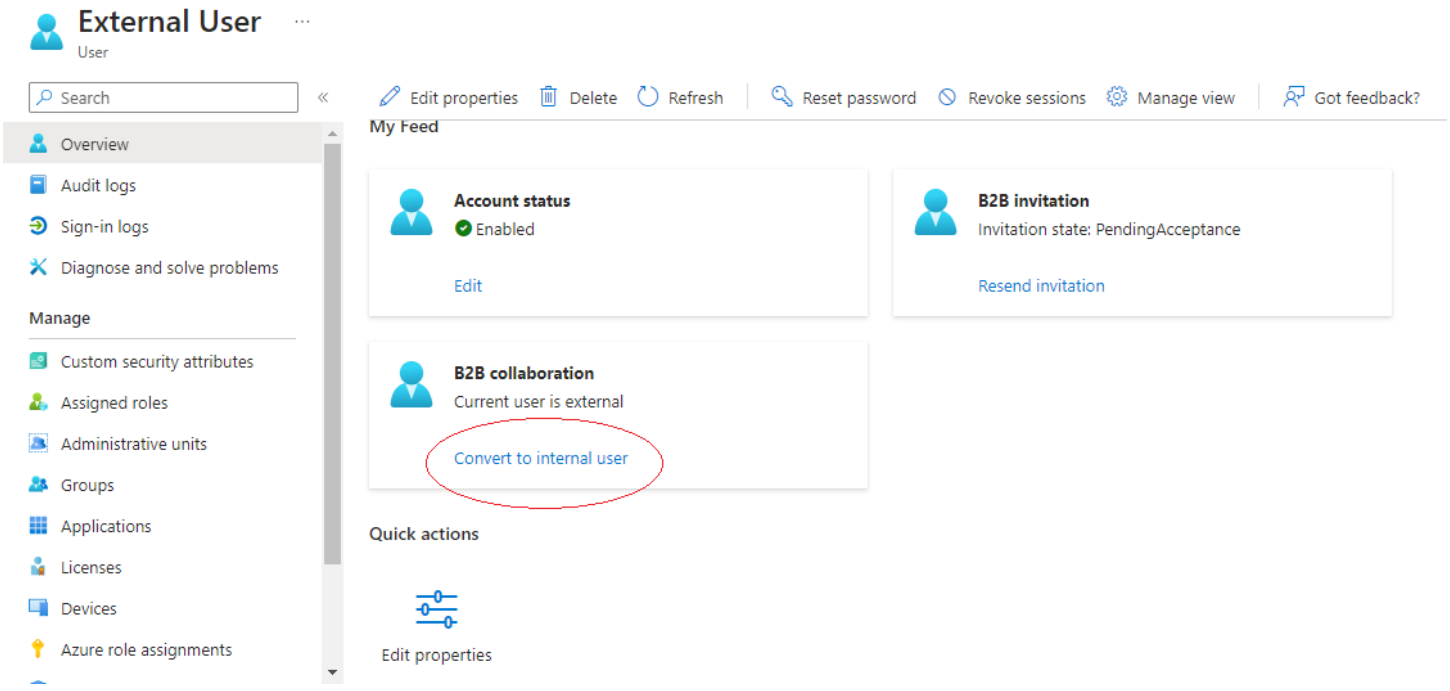
Option D is CORRECT because it pertains to B2B collaboration, which encompasses facilitating collaboration between external users and those within your organization's environment. This typically involves functionalities geared towards regulating access rights and securely sharing resources with external partners. The process of transitioning an external user to an internal user involves changing their status from an external collaborator to an internal member within your organization's ecosystem. This capability to convert an external user into an internal one is accessible through the B2B collaboration tile located within the My Feed section of the overview blade.

Option A is INCORRECT because the B2B invitation typically involves inviting external users to collaborate with your organization. It's used for inviting external users to access resources within your organization's environment. However, converting an external user to an internal user is a different process and does not directly involve inviting them via B2B invitation. One can check the status of the Invitation state (Accepted or Pending), and resend the invitation using the B2B invitation tile.

Option B is INCORRECT because the Account Status option is used to display information about the status of user accounts within your organization's tenant. It indicates whether a user account is enabled or disabled. However, it doesn't inherently provide functionality for converting an external user to an internal user.

Option C is INCORRECT because the Edit Properties option would typically allow administrators to modify various properties or attributes associated with a user account. This could include details such as display name, contact information, and more. While this option might allow administrators to make changes to a user's profile, it doesn't specifically offer functionality for converting an external user to an internal user.

Architectural Diagram/Snapshots:



Reference:

https://learn.microsoft.com/en-us/entra/identity/users/convert-external-users-internal#converting-an-external-user

Ask our Experts

Did you like this **Question?**

Question 8 Incorrect

Domain: Manage Azure identities and governance

You own a Microsoft Entra ID tenant named "test.onmicrosoft.com".

The tenant contains two users, named, User1 and User2. User1 and User2 are members of Group1 and Group2 respectively having no roles assigned to them.

You enable the self-service password reset feature for Group1 only.

Under the authentication methods, you select two methods to reset the password, 1) mobile phone and 2) security questions. Under security questions, you select the number of security questions required to reset as 3. Refer to the below exhibit for details:

Name	Member of	Role Assigned	Number of Methods required to reset	Authentication Methods	Number of Questions Required to reset
User 1	Group 1	None	2	Mobile Phone, Secret Questions	3
User 2	Group 2	None	None	None	None

Proposed Solution: User1 can immediately reset password by answering three security questions correctly. Is this proposed solution correct? (Select True or False)

A. True wrong

B. False right

Explanation:

Correct Answer: B

Option B is CORRECT because while User1 is a member of Group1 for which the self-service password reset feature is enabled, the

selected authentication methods for password reset are mobile phone and security questions. The scenario mentions that two authentication methods are selected for password reset: mobile phone and security questions. This means that when User1 attempts to reset their password, they would need to authenticate using both of these methods. The proposed solution suggests that User1 can immediately reset its password by answering three security questions correctly. However, it overlooks the requirement for User1 to authenticate using both selected methods: mobile phone and security questions. Since the proposed solution only mentions answering security questions, it does not address the need for User1 to authenticate using the mobile phone method. Therefore, it's not a correct solution and the statement is false.

Option A is INCORRECT because the above-proposed solution is False.

Reference:

https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr#enable-self-service-password-reset

Ask our Experts

Did you like this **Question?**

Question 9

Correct

Domain: Manage Azure identities and governance

You own a Microsoft Entra ID tenant named “test.onmicrosoft.com”.

The tenant contains two users, named, User1 and User2. User1 and User2 are members of Group1 and Group2 respectively and no roles are assigned to them.

You enable the self-service password reset feature for Group1 only. Under the authentication methods, you select two methods to reset the password, 1) mobile phone and 2) security questions. Under security questions, you select the number of security questions required to reset as 3. Refer to the below exhibit for details:

Name	Member of	Role Assigned	Number of Methods required to reset	Authentication Methods	Number of Questions Required to reset
User 1	Group 1	None	2	Mobile Phone, Secret Questions	3
User 2	Group 2	None	None	None	None

Proposed Solution: User2 can reset password using the text code received on mobile phone. Is this proposed solution correct? (Select True or False)

A. True

B. False right

Explanation:

Correct Answer: B

Option B is correct answer : Although User2 is a member of Group2 and the self-service password reset feature is enabled only for Group1, User2 cannot reset their password using a text code received on their mobile phone. The self-service password reset feature is only enabled for Group1, not Group2. Therefore, User2 does not have access to the self-service password reset functionality. Therefore, the proposed solution is incorrect and the statement is false.

Reference:

Enable Microsoft Entra self-service password reset - Microsoft Entra ID

Ask our Experts

Did you like this **Question?**

Question 10

Incorrect

Domain: Manage Azure identities and governance

You have an Azure subscription named testSubscription1.

In testSubscription1, you create an alert rule named testAlert1 of alert type Anomaly. Now you want to edit the alert rule you created previously.

Which information can you change for the alert rule from the Edit alert rule panel?

A. Alert start date right

B. Alert end date right

C. Alert type

D. Alert name wrong

E. Alert view right

Explanation:

Correct Answer: A, B and E

Option A is correct, you can change the alert start date from the Edit alert rule panel. This allows you to specify when the alert

should begin monitoring.

Option B is correct, you can also change the alert end date. This lets you define when the alert should stop monitoring.

Option C is incorrect, Once an alert rule is created, the alert type (e.g., Anomaly, Metric, Log) cannot be changed. If you need a different alert type, you must create a new alert rule.

Option D is incorrect, The alert name is set when you create the alert rule and cannot be changed later. If you need a different name, you would have to create a new alert rule with the desired name.

Option E is Correct, you can change the alert view, which determines how the alert data is displayed and managed.

Reference:

https://learn.microsoft.com/en-us/azure/cost-management-billing/understand/analyze-unexpected-charges#create-an-anomaly-alert

Manage your alert rules - Azure Monitor | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 11

Incorrect

Domain: Manage Azure identities and governance

You are creating a budget using the Azure Resource Manager Template (ARM) without filters. You enter the following values for the given fields as mentioned below -

Subscription: Contoso Inc R&D Subscription

Region: East US

Budget Name: New_Budget

Amount: 1000

Time Grain: Monthly

Start Date: YYYY-MM-DD

End Date: YYYY-MM-DD

First Threshold: 90

Contact Emails: user1@contoso.com

You receive a validation error when the budget is generated. What is the cause of the error?

- A. You are not allowed to use underscore in the Budget Name field wrong
- B. You have not provided any value for the Second Threshold field
- C. The First Threshold value should be less than 90
- D. You should provide a minimum of two email addresses
- E. Email addresses should be provided as an array of strings right

---

Explanation:

Correct Answer: E

Option E is CORRECT because in ARM templates when specifying contact emails, they should be provided as an array of strings. In the case of the scenario provided, you should enter the email address as ["user1@contoso.com"] for the Contact Emails field. Each email address should be enclosed in double quotes and separated by commas within square brackets to form an array. Failure to format the email addresses correctly would lead to a validation error. To enter multiple email addresses in the Contact Emails field, you should enter the value as ["user1@contoso.com", "user2@contoso.com"].

Option A is INCORRECT because there are no restrictions on using underscores in the Budget Name field in Azure Resource Manager Template (ARM). The error message likely stems from a different issue. For the Budget Name field only alphanumeric, underscore, and hyphen characters are allowed.

Option B is INCORRECT because while thresholds are a part of the budget configuration in Azure, the absence of a second threshold does not necessarily cause a validation error. It might be optional depending on the specific requirements.

Option C is INCORRECT because the threshold value can be greater than or equal to 90. The threshold value is always in percent and can be between 0.01 and 1000. When the cost exceeds the threshold value a notification is sent to the contact emails. The error message would not relate to this specific condition.

Option D is INCORRECT because there is no specific minimum requirement for the number of contact emails in ARM templates for budget creation. While it's generally a good practice to have multiple contacts for redundancy and notification purposes, it's not a validation requirement. Therefore, the absence of a second email address wouldn't directly cause a validation error.

Reference:

https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/quick-create-budget-template?tabs=no-filter%2Cportal#deploy-the-template

Ask our Experts

Did you like this **Question?**

Question 12 Correct

Domain: Manage Azure identities and governance

Your company uses Microsoft Entra ID to manage access to Azure resources. A project team needs temporary access to a sensitive resource group for a 2-week sprint. The access should be granted only after manager approval and must automatically expire after the sprint ends.

Which feature should you use to meet this requirement?

A. Assign a permanent role using Microsoft Entra ID

B. Create a Conditional Access policy

C. Use Microsoft Entra ID Privileged Identity Management with an access review right

D. Enable Multi-Factor Authentication (MFA) for the resource group

---

Explanation:

Correct Answer: C

Option C is CORRECT because Microsoft Entra ID Privileged Identity Management (PIM) allows just-in-time access to privileged roles, includes approval workflows, and supports time-bound access. Access reviews can be used to ensure that permissions are still needed and can automatically revoke access when no longer required. This solution aligns perfectly with the requirement for temporary, approved access.

Option A is INCORRECT because this option would give users continuous access to the resource group, which contradicts the requirement for temporary access. Permanent role assignments are suitable for users who need ongoing access, but in this case, the access should be time-bound and approved, making this option unsuitable.

Option B is INCORRECT because Conditional Access policies are used to enforce access controls based on conditions like user location, device compliance, or risk level. While powerful for securing access, they do not provide mechanisms for temporary access or approval workflows. Therefore, this option does not meet the scenario's needs.

Option D is INCORRECT because While enabling MFA enhances security by requiring additional verification during sign-in, it does not control the duration or approval of access. MFA is a good practice for protecting resources, but it does not fulfill the scenario's need for temporary, manager-approved access with automatic expiration.

Reference:

https://learn.microsoft.com/en-us/azure/advisor/advisor-cost-recommendations#optimize-virtual-machine-vm-or-virtual-machine-scale-set-vmss-spend-by-resizing-or-shutting-down-underutilized-instances

Ask our Experts

Did you like this **Question?**

Question 13 Correct

Domain: Manage Azure identities and governance

You have an Azure subscription. You want to implement role-based access control (RBAC) to assign users with particular permissions depending on their job responsibilities.

Which built-in role should you assign to a user to grant them full access to manage resources within the subscription, except for access to user and group management in Microsoft Entra ID?

A. Owner

B. Reader

C. Contributor right

D. User Access Administrator

Explanation:

Correct Answer: C

Option C is CORRECT because the Contributor role grants full access to manage all resources within an Azure subscription, which aligns with the requirement. However, it explicitly does not allow assigning roles in Azure RBAC. This role also doesn't provide access to user and group management in Microsoft Entra ID, meeting the specified requirement.

Option A is INCORRECT because the Owner role grants full access to manage all resources within an Azure subscription, including the ability to assign roles in Azure RBAC. However, it doesn't specifically restrict access to user and group management in Microsoft Entra ID. Therefore, while this role grants the necessary permissions for managing resources, it doesn't meet the requirement of excluding access to user and group management.

Option B is INCORRECT because the Reader role allows viewing all resources within an Azure subscription but doesn't permit making any changes. Since the requirement is to grant full access to manage resources, the Reader role is not suitable as it doesn't provide the necessary permissions for managing resources.

Option D is INCORRECT because the User Access Administrator role specifically focuses on managing user access to Azure resources. While it allows managing access to resources, it doesn't grant full access to manage all resources within an Azure subscription, which is required in our scenario. Additionally, it doesn't restrict access to user and group management in Microsoft Entra ID.

Reference:

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#general

Ask our Experts

Did you like this **Question?**

Question 14 Correct

Domain: Manage Azure identities and governance

A multinational company utilizes Azure for its cloud infrastructure. The IT department needs to efficiently assign roles at different scopes within Azure while ensuring proper access management and compliance.

They want to grant a contractor access to deploy resources within a specific resource group named "project-rg1" without granting access to other resources.

Which Azure scope and role assignment should be implemented for this scenario?

- A. Resource Group; Contributor role right
- B. Subscription; Contributor role
- C. Resource Group; Reader role
- D. Management Group; Contributor role
- E. Subscription; Owner role

Explanation:

Correct Answer: A

Option A is CORRECT because assigning the Contributor role at the Resource Group scope grants the contractor the necessary permissions to deploy, manage, and delete Azure resources within the specific resource group named "project-rg1." However, it does not provide access to resources outside of this resource group, aligning with the organization's requirement to restrict access to only the designated resources. The Contributor role allows the contractor to perform actions such as creating and managing resources like virtual machines, databases, or web apps, while still maintaining limitations within the defined scope. This approach enhances security by adhering to the principle of least privilege, ensuring that the contractor can fulfill their responsibilities effectively while minimizing the risk of unauthorized access to sensitive resources outside of their designated scope.

Option B is INCORRECT because assigning the Contributor role at the Subscription scope would grant the contractor permission to manage resources across the entire subscription, including resources outside the "project-rg1" resource group. This violates the organization's requirement to limit access to a specific resource group.

Option C is INCORRECT because assigning the Reader role at the Resource Group scope would only provide the contractor with read-only access to resources within the "project-rg1" resource group. It would not allow them to deploy or modify resources, which is necessary for their role.

Option D is INCORRECT because Management Groups are used to manage access, policies, and compliance across multiple subscriptions. Assigning the Contributor role to the Management Group scope would grant permissions across all subscriptions and resource groups under that management group, which exceeds the scope needed for the contractor's task within the "project-rg1" resource group.

Option E is INCORRECT because assigning the Owner role at the Subscription scope would grant the contractor full control over all resources within the subscription, which goes beyond the requirement of restricting access to the "project-rg1" resource group. The Owner role includes permissions to manage access control, billing, and all Azure resources, posing a security risk and violating the principle of least privilege.

Reference:

https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-steps

Ask our Experts

Did you like this **Question?**

Question 15 Incorrect

Domain: Manage Azure identities and governance

A multinational corporation with various departments and teams spread across different regions has migrated its infrastructure to Microsoft Azure. The corporation's finance department requires read-only access to all Azure resources for monitoring purposes. At which scope should the IT administrator assign the Reader role to the finance department to meet this requirement?

A. Management group right

B. Subscription

C. Resource group wrong

D. Resource

Explanation:

Correct Answer: A

Option A is CORRECT. If the finance department needs read-only access to all Azure resources across multiple subscriptions, assigning the Reader role at the management group level is appropriate. This provides comprehensive monitoring capabilities across the entire management group

Option B is INCORRECT. If the finance department only needs read-only access to resources within a specific subscription, assigning the Reader role at the subscription level is sufficient. This ensures they can monitor all resources within that particular subscription.

Option C is INCORRECT because assigning the Reader role at the resource group scope would only provide read-only access to resources within that specific resource group. Since the scenario states that the finance department requires access to all Azure resources, assigning the role to the subscription scope would be more suitable.

Option D is INCORRECT because assigning the Reader role at the resource scope would only provide read-only access to a specific Azure resource. The scenario requires access to all Azure resources, so assigning the role to the subscription scope would be more appropriate.

Reference:

https://learn.microsoft.com/en-us/Azure/role-based-access-control/role-assignments

Azure built-in roles - Azure RBAC | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Finish Review