Level: Advanced

Microsoft Azure Exam AZ-104 Certification

← Back to the **Course**

Microsoft Entra - **Practice Mode**

Completed on Tue, 07 Oct 2025

1st	3/7	42.86%	FAIL
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	7	3	4	0	0
Total	All Domains	7	3	4	0	0

Review the Answers

Filter By

Question 1

Correct

Domain: Manage Azure identities and governance

A tenant administrator wants to ensure that guest users added to a Microsoft Entra ID tenant cannot invite additional guest users.

Proposed Solution: Restrict the "Guest inviter role" in the tenant settings under External Collaboration Settings in the Microsoft Entra admin center to disable guests' ability to invite other users.

Is this proposed solution correct? (Select Yes or No)

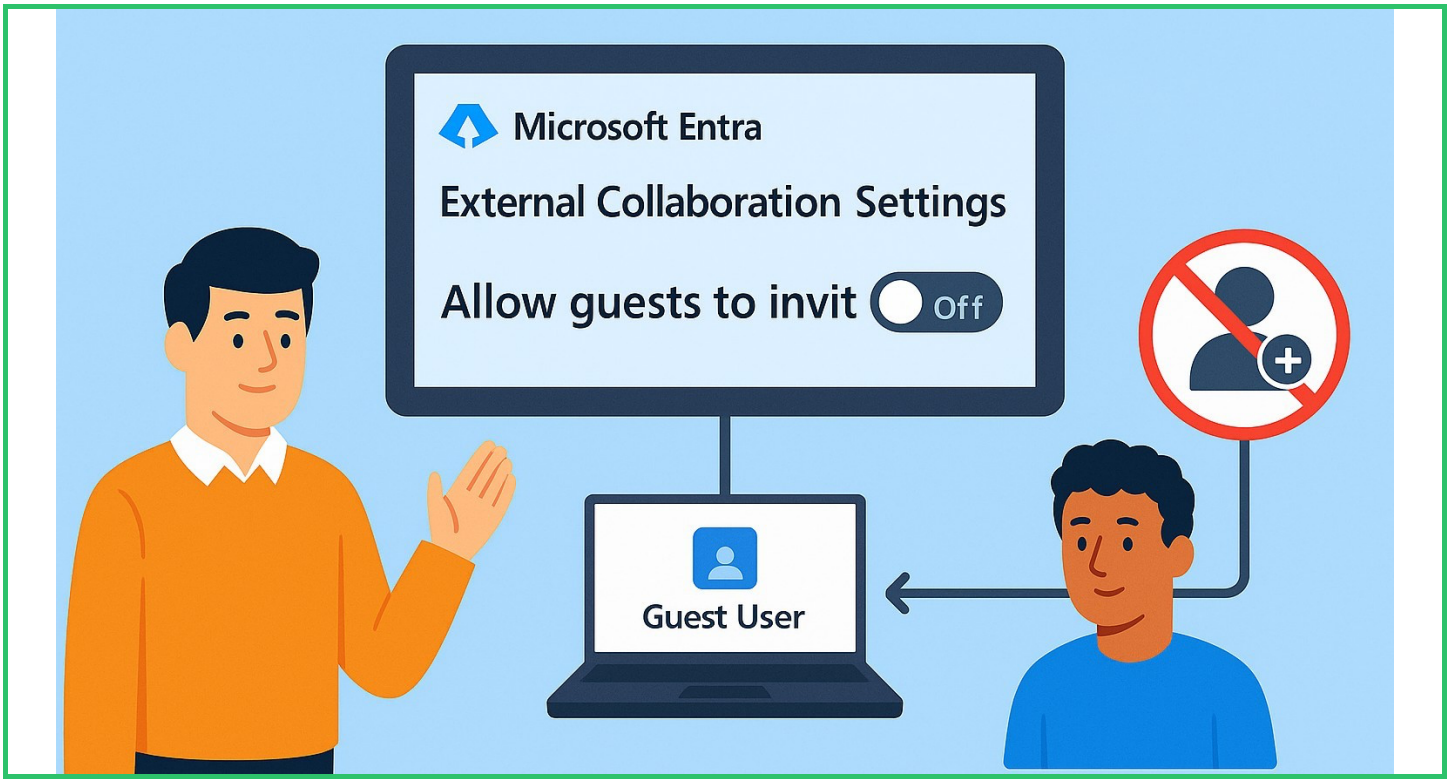
◯ A. Yes right

B. No

Explanation:

Correct Answer: A

The proposed solution is correct because restricting the "Guest inviter role" in the Microsoft Entra ID tenant settings under External Collaboration Settings is a valid and effective approach to ensure that guest users cannot invite additional users into the directory.



This ensures that only authorized roles, like Global Admins or User Admins, can add new guests. It helps organizations maintain stronger security by reducing the risk of unauthorized access or accidental over-permissioning. This setting supports the principle of least privilege, where users only get the permissions they truly need. Admins can configure this directly in the Microsoft Entra admin center by turning off the "Allow guests to invite" option with no custom scripts or third-party tools required.

References:

Limit who can invite guests

Configure external collaboration settings for B2B in Microsoft Entra External ID

Ask our Experts

Did you like this **Question?**

Question 2

Incorrect

Domain: Manage Azure identities and governance

A multinational corporation plans to manage license assignments in Microsoft Entra ID for its global teams. You are tasked with implementing region-specific license assignments while adhering to the following constraints:

Dynamic user management must be enabled.

Excess license usage or underutilization must be prevented.

Region-based compliance reports must be generated post-implementation.

Arrange the steps in the correct sequence to meet the above constraints.

Your Answer		Correct Answer	
1.	A. Create dynamic groups for users based on their geographical location	1.	D. Identify available license quotas for each region
2.	D. Identify available license quotas for each region	2.	A. Create dynamic groups for users based on their geographical location
3.	B. Assign licenses to region-specific dynamic groups	3.	B. Assign licenses to region-specific dynamic groups
4.	E. Adjust license assignments to avoid exceeding quotas	4.	E. Adjust license assignments to avoid exceeding quotas
5.	C. Use Microsoft Entra ID monitoring to generate compliance reports by region	5.	C. Use Microsoft Entra ID monitoring to generate compliance reports by region

Explanation:

Correct Answers : D, A, B, E and C

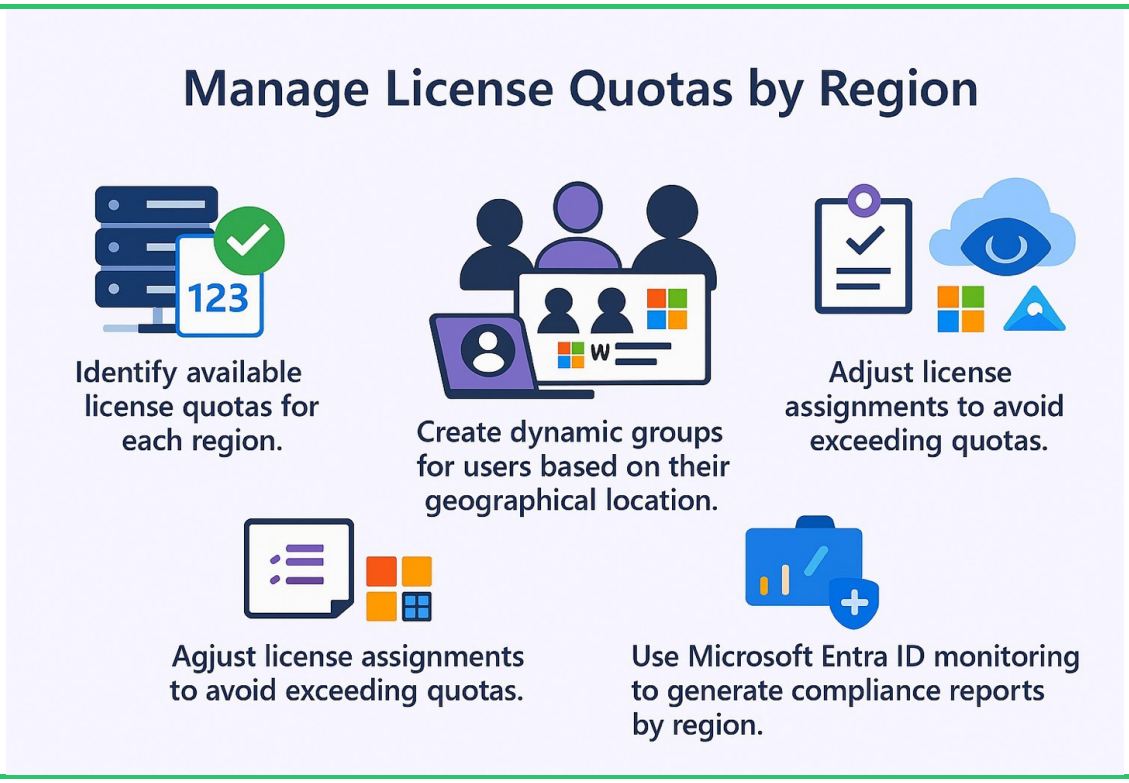
Identify available license quotas for each region.

Create dynamic groups for users based on their geographical location.

Assign licenses to region-specific dynamic groups.

Adjust license assignments to avoid exceeding quotas.

Use Microsoft Entra ID monitoring to generate compliance reports by region



Step1 - Identify available license quotas for each region:

The first step is understanding the available licensing quotas per region to ensure proper allocation. This involves analyzing the total number of licenses purchased and comparing them with the active users in each geographical location. By doing so, the organization can prevent oversubscription or underutilization, a critical compliance requirement. This ensures that the foundation for assigning licenses is set accurately.

Step2 - Create dynamic groups for users based on their geographical location: Dynamic groups in Microsoft Entra ID enable automatic user assignments based on predefined rules. For this step, create groups that filter users based on attributes like country, city, or department. For example, a rule like (user.department -eq "Europe Sales") can be applied to segregate users in Europe. This automation ensures that license management is scalable and eliminates manual effort.

Step3 - Assign licenses to region-specific dynamic groups:

After creating the groups, licenses must be assigned to these dynamic groups. Group-based licensing in Microsoft Entra ID simplifies the assignment of licenses to all users within a group. By assigning licenses at the group level, the organization ensures that all group members receive appropriate access based on their region, reducing the risk of missed assignments or duplications.

Step4 - Adjust license assignments to avoid exceeding quotas:

At this stage, adjust license assignments to align with the quotas identified in Step 1. This involves reviewing dynamic group membership to ensure compliance with regional limits. If necessary, reallocate licenses to ensure that no group exceeds its allocation. Microsoft Entra provides notifications about license conflicts or insufficient quantities, allowing the administrator to resolve issues before finalizing assignments.

Step5 - Use Microsoft Entra ID monitoring to generate compliance reports by region: Finally, generate compliance and usage reports using Microsoft Entra ID insights. These reports help validate that the assigned licenses meet regional needs and comply with the organization's policies.

References:

View Microsoft 365 account license and service details with PowerShell

Manage rules for dynamic membership groups in Microsoft Entra ID

Assign or unassign licenses for users in the Microsoft 365 admin center

What is the Usage and insights report in Microsoft Entra ID?

Ask our Experts

Did you like this **Question?**

Question 3 Incorrect

Domain: Manage Azure identities and governance

Your organization requires external users to be periodically reviewed for access to shared resources. These reviews must automatically trigger access removal if reviewers do not approve them. Additionally, users must be reminded before each review cycle to take necessary action. Which three of the following services would best meet the requirements for managing these access reviews and reminders? (Select three)

Your Answer

A. Microsoft Entra ID Governance - Access reviews

B. Conditional Access authentication context

D. Guest invitation management

Correct Answer

A. Microsoft Entra ID Governance - Access reviews

E. Privileged Identity Management (PIM)

F. Microsoft Entra entitlement management

Explanation:

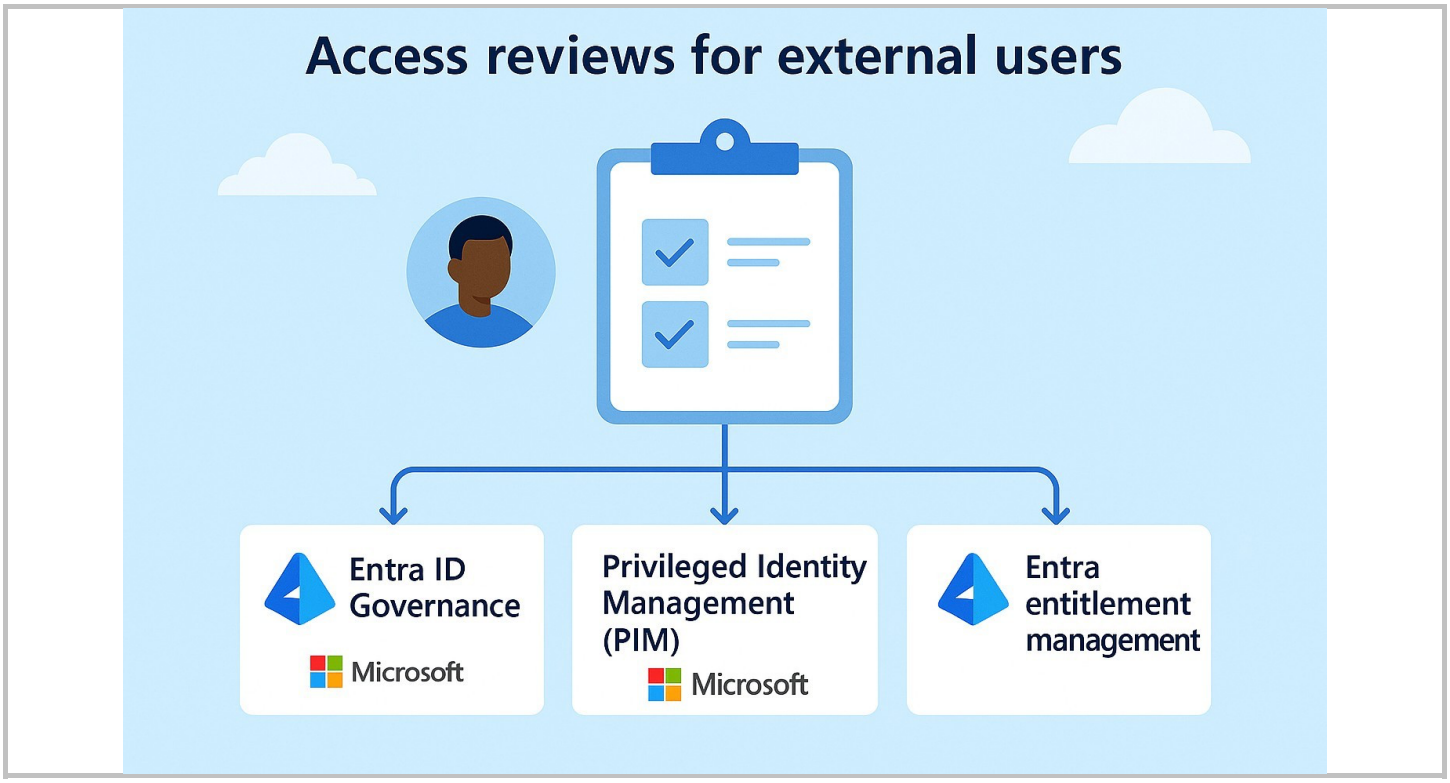
Correct Answers: A, E and F

review and validate access for internal and external users. This service allows organizations to automate the review process, ensuring that access is retained only for users whose access is approved by designated reviewers. If access is not approved, it can automatically trigger removal, satisfying the requirement to enforce compliance. This functionality is critical for managing external users, as it prevents unnecessary or overprivileged access to sensitive resources. The ability to integrate these reviews with other governance workflows, such as entitlement management, makes this feature indispensable for the given scenario. Access reviews help maintain security and operational efficiency by automating an otherwise manual and error-prone process.

Option E: Privileged Identity Management (PIM) is because it is essential for controlling access to privileged roles, including those assigned to external users. While primarily focused on privileged accounts, PIM supports the review of role assignments and implements just-in-time (JIT) access for critical resources. This aligns with the scenario's need for periodic access reviews, ensuring external users are granted temporary access that expires if not renewed or reapproved. PIM's integration with notification and expiration workflows further enhances governance, making it possible to enforce stricter access policies while maintaining

compliance. Though not limited to external users, PIM adds an extra layer of security and governance, making it relevant in the context of periodic reviews for sensitive roles.

Option F: Microsoft Entra entitlement management is correct because it is an effective tool for automating the management of external user access throughout its lifecycle. It facilitates workflows for access requests, approvals, and notifications, and it integrates seamlessly with access review processes. This includes automated reminders that notify external users before a review cycle begins, prompting them to take the necessary steps to maintain their access. Entitlement management plays a crucial role in supporting collaboration with external users while ensuring control and compliance. By aligning with access reviews, it enables a more comprehensive approach to access governance, making it an essential component in managing external user access. Its ability to automate and simplify complex governance workflows is key to effective external user management.



Option B: Conditional Access authentication context is incorrect because it focuses on securing access to resources through policies that enforce conditions such as multi-factor authentication (MFA) or device compliance. While it is valuable for ensuring secure access in real time, it does not support periodic reviews or the automation of access removal. Conditional Access is geared toward managing and enforcing access policies dynamically based on user context, but it does not address the governance aspects of reviewing or notifying external users about access. Thus, it does not meet the requirements of this scenario.

Option C: Microsoft Entra ID Protection is incorrect because it is designed to identify and mitigate identity-related risks, such as detecting compromised accounts or suspicious login behavior. It leverages risk-based policies to enforce conditional access controls, ensuring that only legitimate users can access resources. However, it does not include functionality for periodic access reviews, automated notifications, or access removal workflows. While crucial for securing identities, it is not relevant to governance tasks like reviewing and managing external user access as described in the scenario.

Option D: Guest invitation management is incorrect because it is primarily used to invite, approve, and monitor external users' initial access to organizational resources. While it ensures that external users are onboarded securely, it does not provide functionality for periodic access reviews or automated removal of access if not approved. Its role ends after the external user is granted access, and it does not handle ongoing governance tasks like reviews or notifications. As a result, this feature does not address the requirements of this scenario.

References:

https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview

https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-overview

Ask our Experts

Did you like this **Question?**

Question 4 Correct

Domain: Manage Azure identities and governance

You are managing a Microsoft Entra ID tenant for a global organization with several subsidiaries. As part of the shift to a remote-first workforce, you've already enabled Self-Service Password Reset (SSPR) across the tenant.

However, specific departments have unique compliance requirements:

The Marketing team only needs one authentication method to reset their passwords.

The Legal and Finance teams handle sensitive data and must use two authentication methods for additional security.

What should you configure to meet these department-specific requirements while ensuring the overall SSPR configuration remains secure and efficient? (Select three)

A. Configure SSPR for the entire organization with phone and email as authentication methods, but allow the Legal and Finance departments to add security questions for further verification

- [x] B. Create group-based SSPR policies to apply different authentication methods based on group membership right
- [x] C. Configure SSPR to require only one authentication method for the Marketing department and two methods for Legal and Finance right
- [x] D. Configure MFA as a global requirement for all users, with exceptions only for the Marketing department using a conditional access policy right

E. Implement a rule for SSPR that blocks access to password reset for users from high-risk geographical locations unless they perform MFA

Explanation:

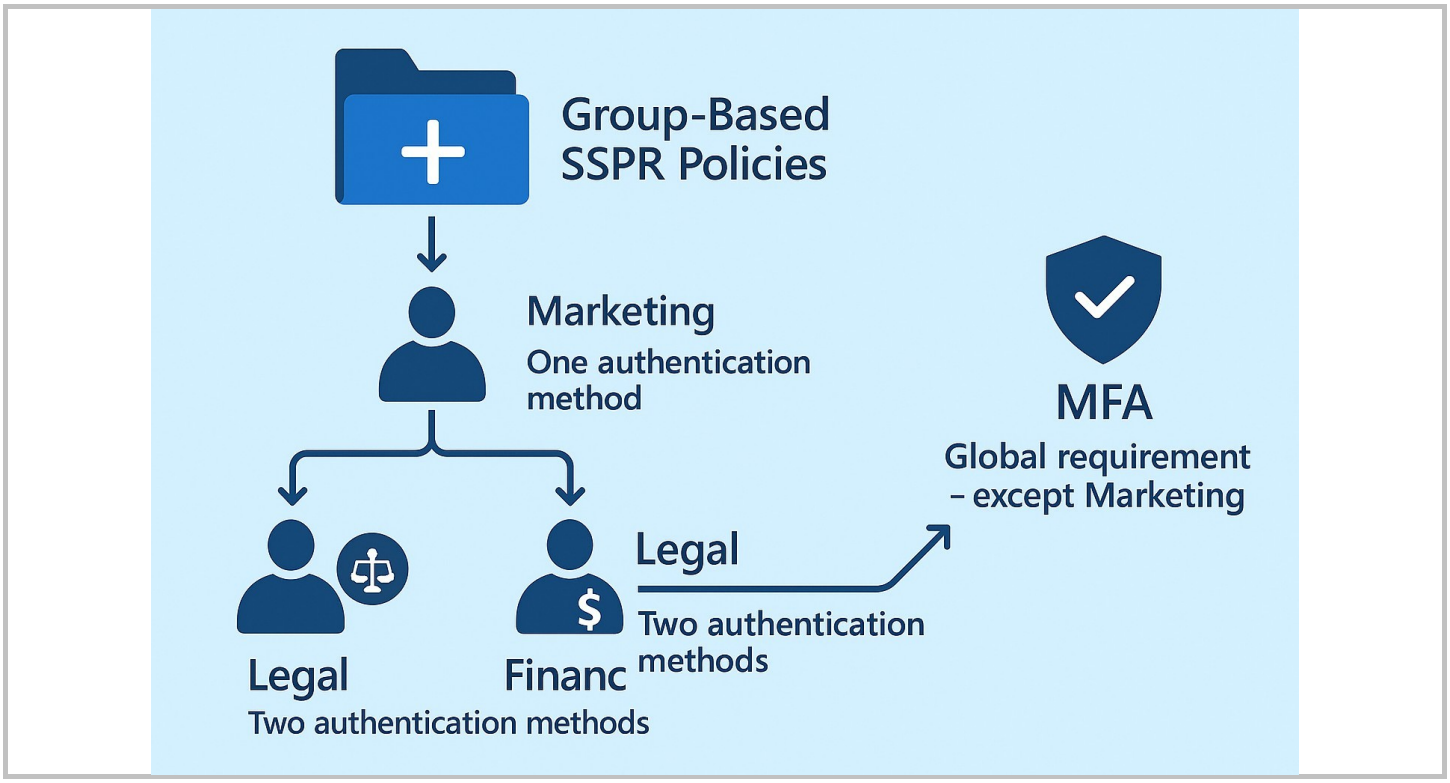
Correct Answers: B, C and D

Option B is correct because by creating group-based policies, you can tailor the authentication requirements for specific groups within the organization. For example, the Marketing department can be assigned to a group that allows them to use only one

authentication method, while the Legal and Finance departments can be assigned to a separate group that requires two-factor authentication (such as phone and email, or email and security questions). Group-based policies allow for granular control over the security settings for different groups of users, ensuring that you can balance convenience and security. Using Microsoft Entra ID groups to manage these policies is a scalable solution, especially in large organizations with diverse compliance needs. This method ensures that you meet specific compliance and security standards for each department without unnecessarily complicating the SSPR setup for the entire organization.

Option C is correct because configuring SSPR policies to enforce one authentication method for the Marketing department (e.g., email verification) and two authentication methods for the Legal and Finance departments (e.g., phone verification and email verification) addresses both the security and convenience needs of each department. This configuration ensures that the Marketing department, which does not have strict security requirements, can reset their passwords efficiently with fewer steps, minimizing friction. On the other hand, the Legal and Finance departments, which manage sensitive information, can be required to use more secure methods like multi-factor authentication (MFA). This strategy is flexible and aligns with Microsoft's security guidelines, ensuring that each department's security needs are met without compromising the user experience for those in less sensitive roles.

Option D is correct because MFA as a global requirement for all users ensures a higher level of security, especially in a remote-first organization where users may be accessing the environment from different locations and devices. By applying a global MFA policy and making exceptions for the Marketing department using a conditional access policy, you can ensure that more sensitive departments like Legal and Finance are always required to use MFA, while Marketing users can be exempted from this requirement. Conditional access policies can be fine-tuned to apply or exempt MFA requirements based on user roles, locations, or device compliance. This makes MFA a strong, organization-wide security policy while allowing flexibility for less critical departments. Applying this strategy at the global level strengthens overall security, reduces the attack surface, and ensures compliance with organizational security standards for all users except those in the Marketing department.



Option A is incorrect because security questions are not considered a secure authentication method, particularly for departments like Legal and Finance that handle sensitive information. Security questions can be susceptible to social engineering attacks or easily guessed answers. Additionally, SSPR configurations should prioritize stronger methods, such as phone and email verification, which

are commonly used in multi-factor authentication (MFA) scenarios. According to Microsoft's best practices, relying on security questions as the primary supplementary method for sensitive departments fails to meet modern security standards. As a result, this approach does not align with the security requirements for the Legal and Finance departments.

Option E is correct because it focuses on blocking access to SSPR for users based on their geographical location, which could be problematic in a remote-first workforce. Many employees will be working from various locations worldwide, and restricting SSPR based on geographic location could create unnecessary friction. Additionally, MFA would already be enforced through other configurations such as conditional access policies, so it may be redundant to introduce geographic restrictions specifically for SSPR access. The need for geographic restrictions should be evaluated carefully, as remote work may involve users from a wide range of locations, and enforcing such restrictions could potentially create more complexity than necessary.

References:

https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks

https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-mfa-strength#create-a-conditional-access-policy

Ask our Experts

Did you like this **Question?**

Question 5

Correct

Domain: Manage Azure identities and governance

Your organization has implemented a compliance-driven access policy requiring precise role assignments to Azure resources. You are tasked with analyzing operational scenarios and assigning the appropriate Azure built-in roles to meet specific, nuanced requirements. Failure to assign the correct roles could compromise system integrity or operational efficiency. Match the following Azure built-in roles to their corresponding description.

Note: To match roles with the correct scenario, you need to drag and drop the appropriate role into the corresponding answer area. Carefully consider the constraints and permissions described.

Your Answers

A. Virtual Machine Contributor

Role responsible for enabling application lifecycle tasks such as scaling compute resources, performing system diagnostics, and applying security updates for deployed services, excluding administrative controls over data access policies

B. Network Contributor

Role is essential for configuring and managing subnet architectures, enforcing network security through rules, and overseeing communication flows within Azure infrastructure, but it cannot influence cross-resource dependencies

C. Storage Blob Data Contributor

Role granting permissions to facilitate granular object-level operations within storage accounts, allowing restricted management of blob containers and SAS tokens, yet prohibiting changes to encryption or replication configurations

D. User Access Administrator

Role mandated to oversee delegation of resource-level permissions for teams, allowing boundary-specific access controls while restricting the ability to make any direct resource alterations

Correct Answers

A. Virtual Machine Contributor

Role responsible for enabling application lifecycle tasks such as scaling compute resources, performing system diagnostics, and applying security updates for deployed services, excluding administrative controls over data access policies

B. Network Contributor

Role is essential for configuring and managing subnet architectures, enforcing network security through rules, and overseeing communication flows within Azure infrastructure, but it cannot influence cross-resource dependencies

C. Storage Blob Data Contributor

Role granting permissions to facilitate granular object-level operations within storage accounts, allowing restricted management of blob containers and SAS tokens, yet prohibiting changes to encryption or replication configurations

D. User Access Administrator

Role mandated to oversee delegation of resource-level permissions for teams, allowing boundary-specific access controls while restricting the ability to make any direct resource alterations

Explanation:

Correct Answers: 1-C, 2-A, 3-B and 4-D

Virtual Machine Contributor

Role responsible for enabling application lifecycle tasks such as scaling compute resources, performing system diagnostics, and applying security updates for deployed services, excluding administrative controls over data access policies

Network Contributor

Role is essential for configuring and managing subnet architectures, enforcing network security through rules, and overseeing communication flows within Azure infrastructure, but it cannot influence cross-resource dependencies

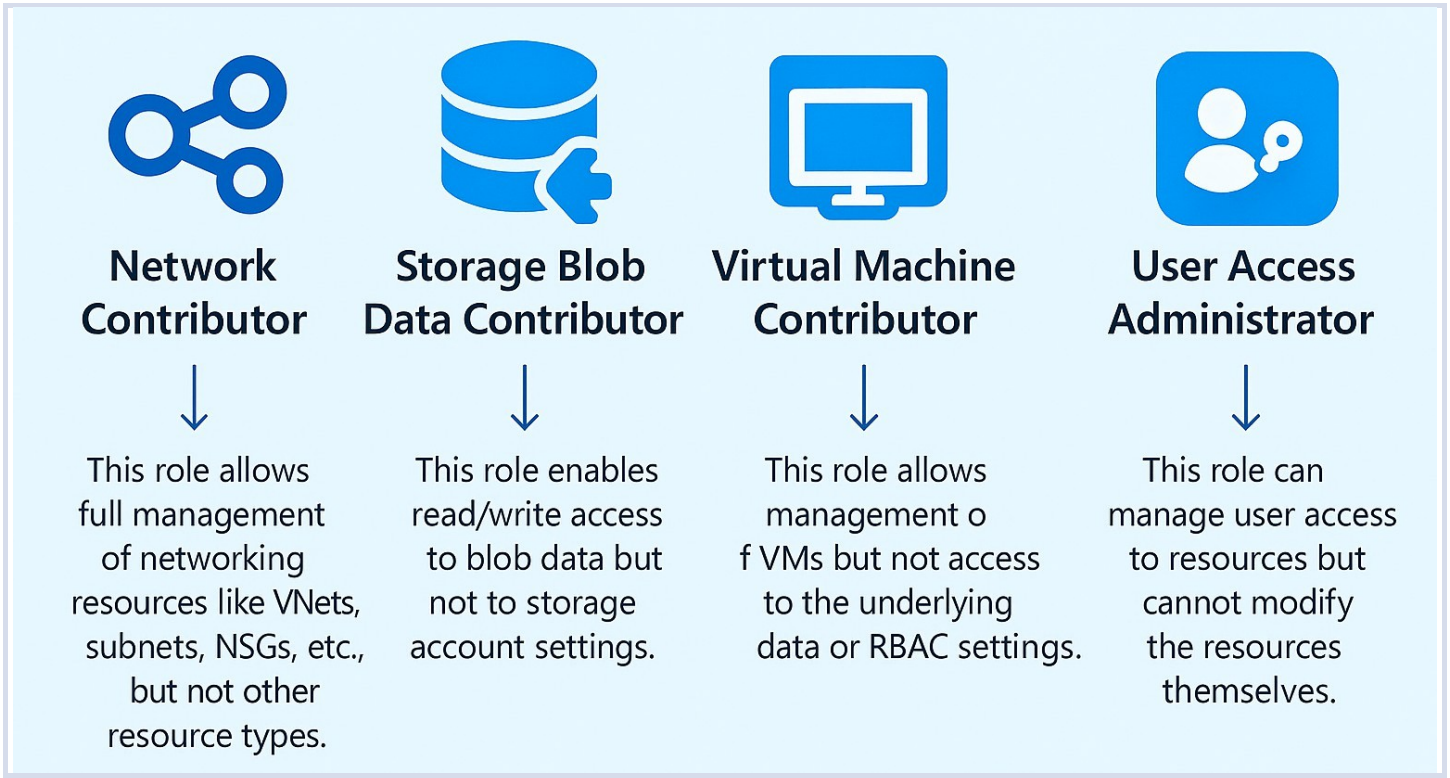
Storage Blob Data Contributor

Role granting permissions to facilitate granular object-level operations within storage accounts, allowing restricted management of blob containers and SAS tokens, yet prohibiting changes to encryption or replication configurations

User Access Administrator

Role mandated to oversee delegation of resource-level permissions for teams, allowing boundary-specific access controls while restricting the ability to make any direct resource alterations

Description	Correct Role	Explanation
A. Configuring and managing subnet architectures, enforcing network security through rules, and overseeing communication flows within Azure infrastructure, but cannot influence cross-resource dependencies.	**Network Contributor**	This role allows full management of networking resources like VNets, subnets, NSGs, etc., but not other resource types.
B. Granular object-level operations within storage accounts, allowing restricted management of blob containers and SAS tokens, yet prohibiting changes to encryption or replication configurations.	**Storage Blob Data Contributor**	This role enables read/write access to blob data but not to storage account settings.
C. Enabling application lifecycle tasks such as scaling compute resources, performing system diagnostics, and applying security updates for deployed services, excluding administrative controls over data access policies.	**Virtual Machine Contributor**	This role allows management of VMs but not access to the underlying data or RBAC settings.
D. Overseeing delegation of resource-level permissions for teams, allowing boundary-specific access controls while restricting the ability to make any direct resource alterations.	**User Access Administrator**	This role can manage user access to resources but cannot modify the resources themselves.



The Virtual Machine Contributor role is designed to grant users permissions to manage virtual machines (VMs) without providing administrative access to the underlying resource group or subscription. This includes starting, stopping, resizing, and updating virtual machines, as well as attaching or detaching disks. However, this role does not allow users to modify RBAC settings or manage other Azure resources associated with the VM, such as networks or storage accounts. This role is ideal for application teams who need to manage compute resources within predefined boundaries, ensuring operational flexibility without compromising security.

The Network Contributor role is specifically designed to enable users to manage all networking-related resources within an Azure subscription. This includes creating, modifying, and deleting virtual networks, subnets, network security groups, and configuring routing rules. However, it does not grant permission to modify or access non-network resources such as virtual machines or storage accounts. This separation ensures that network administrators can work within their domain without impacting other operational components. This role is critical for managing communication flows and ensuring secure connectivity between Azure resources while adhering to the principle of least privilege.

The Storage Blob Data Contributor role provides granular permissions to manage Azure Storage blob containers and objects. Users assigned this role can create, delete, and update blob containers, upload files, and manage access policies through SAS tokens. However, this role does not extend to broader storage account management tasks, such as configuring encryption, firewalls, or access keys. This role is ideal for scenarios where users require fine-grained access to object storage without administrative control over the underlying storage account, ensuring operational security and compliance.

The User Access Administrator role is designed to manage access to Azure resources by assigning or removing role-based access control (RBAC) permissions, without allowing modifications or management of the resources themselves. This ensures a separation between managing access and handling resources, which is crucial for maintaining organizational policies and compliance. The role is particularly beneficial in situations where teams need to delegate access rights across a large scale, ensuring that resource management responsibilities are kept distinct from access control functions. This approach helps mitigate risks associated with unauthorized changes to resources.

Reference:

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

Ask our Experts

Did you like this **Question?**

Question 6 Incorrect

Domain: Manage Azure identities and governance

You are setting up access control in a large enterprise environment. A user, "UserX", needs to manage only the storage accounts in the "MarketingRG" resource group but should not have permissions on other types of resources such as virtual machines or databases in the same group. Additionally, "UserX" should have read-only access to all resources in the "HRRG" resource group. What is the most appropriate way to assign roles for UserX to meet these requirements?

A. Assign Storage Account Contributor role at the "MarketingRG" level and Reader role at the "HRRG" level right

B. Assign a Contributor role at the "MarketingRG" level and a Reader role at the "HRRG" level

C. Assign the Owner role at the "MarketingRG" level and a Reader role at the "HRRG" level

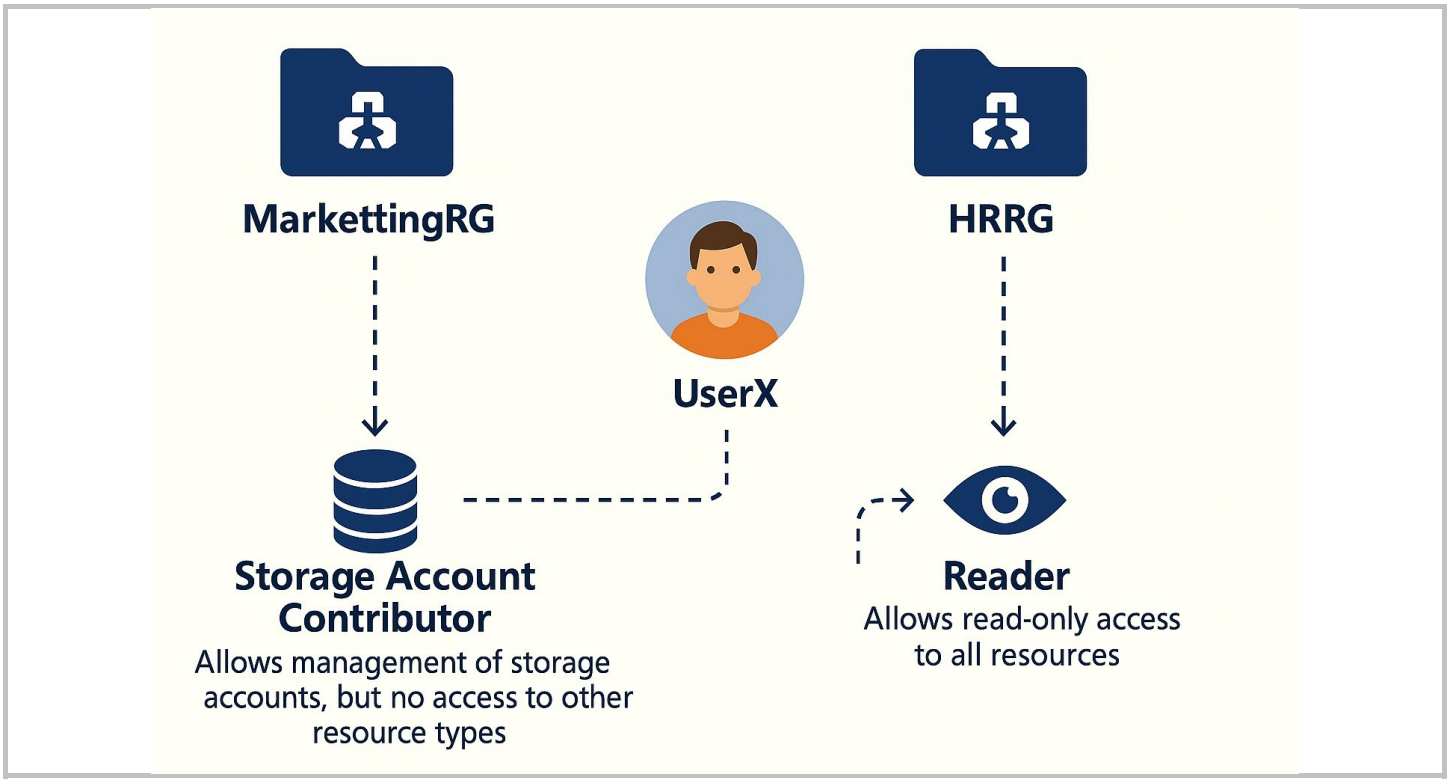
D. Assign Storage Blob Data Contributor role at the "MarketingRG" level and Reader role at the "HRRG" level wrong

Explanation:

Correct Answer: A

Option A is CORRECT because: Storage Account Contributor role allows the user to create, manage, and delete storage accounts within a scope, without giving access to other resource types like virtual machines or databases. Assigning this role at the MarketingRG level ensures that UserX's permissions are restricted only to storage services, satisfying the principle of least privilege.

Assigning the Reader role at the HRRG level enables read-only access to all resources in that resource group, fulfilling the secondary requirement of visibility without modification rights.



Option B is INCORRECT because The Contributor role at the "MarketingRG" level would grant "UserX" broad access to manage all types of resources within the "MarketingRG" resource group, including virtual machines, databases, and networking components. This is not in line with the requirement to restrict access to only the storage accounts within "MarketingRG". The Reader role at the "HRRG" level is appropriate, but combining it with the Contributor role for the entire "MarketingRG" resource group would violate the intent of restricting "UserX's" permissions to just storage accounts.

Option C is INCORRECT because The Owner role grants full administrative permissions, including the ability to delete or modify any resources, not just storage accounts. "UserX" would be able to modify any resource type within the "MarketingRG" resource group, including virtual machines, databases, and networking resources, which is not required in this case. This violates the principle of least privilege, where users should only have the minimum permissions necessary for their tasks. While the Reader role at the "HRRG" level is correct, the Owner role at the "MarketingRG" level goes beyond the required permissions and grants unnecessary access.

Option D is INCORRECT because The Storage Blob Data Contributor role is more restrictive than the Storage Account Contributor role. It specifically allows the user to manage blob data (containers, blobs, etc.) but does not provide the necessary permissions to manage the storage account itself (such as creating or deleting storage accounts). "UserX" needs to manage the storage accounts themselves, not just blob data within those accounts. Thus, this role does not fully meet the requirement to manage all aspects of storage accounts. The Reader role at the "HRRG" level is correct, but the Storage Blob Data Contributor role does not provide sufficient

permissions for managing the storage accounts themselves.

References:

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

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

Ask our Experts

Did you like this **Question?**

Question 7 Incorrect

Domain: Manage Azure identities and governance

You are an Azure Administrator reviewing access permissions for an enterprise application (AppUser) that needs to read data from all storage accounts in a specific resource group named ResourceGroupA. However, individual storage accounts within this resource group have custom roles and deny assignments. You must apply the principle of least privilege and evaluate what the user can and cannot do.

Here is the access configuration for AppUser:

Assigned Reader role at the subscription level

Assigned Contributor role at the ResourceGroupA level

Assigned a custom role with only "read" permissions on StorageAccountB within ResourceGroupA

A Deny assignment exists on StorageAccountB, scoped directly to AppUser

Which TWO statements below are true about AppUser's effective access permissions? (Select 2)

- [ ] A. AppUser will be able to read data from all storage accounts within Resource Group A, regardless of individual role assignments wrong

B. The deny assignment on Storage Account B will override any role-based access assignments for AppUser right

C. AppUser's access to Storage Account B is governed by the custom role and is not affected by the deny assignment

D. AppUser will have full access to Resource Group A due to the Contributor role assignment

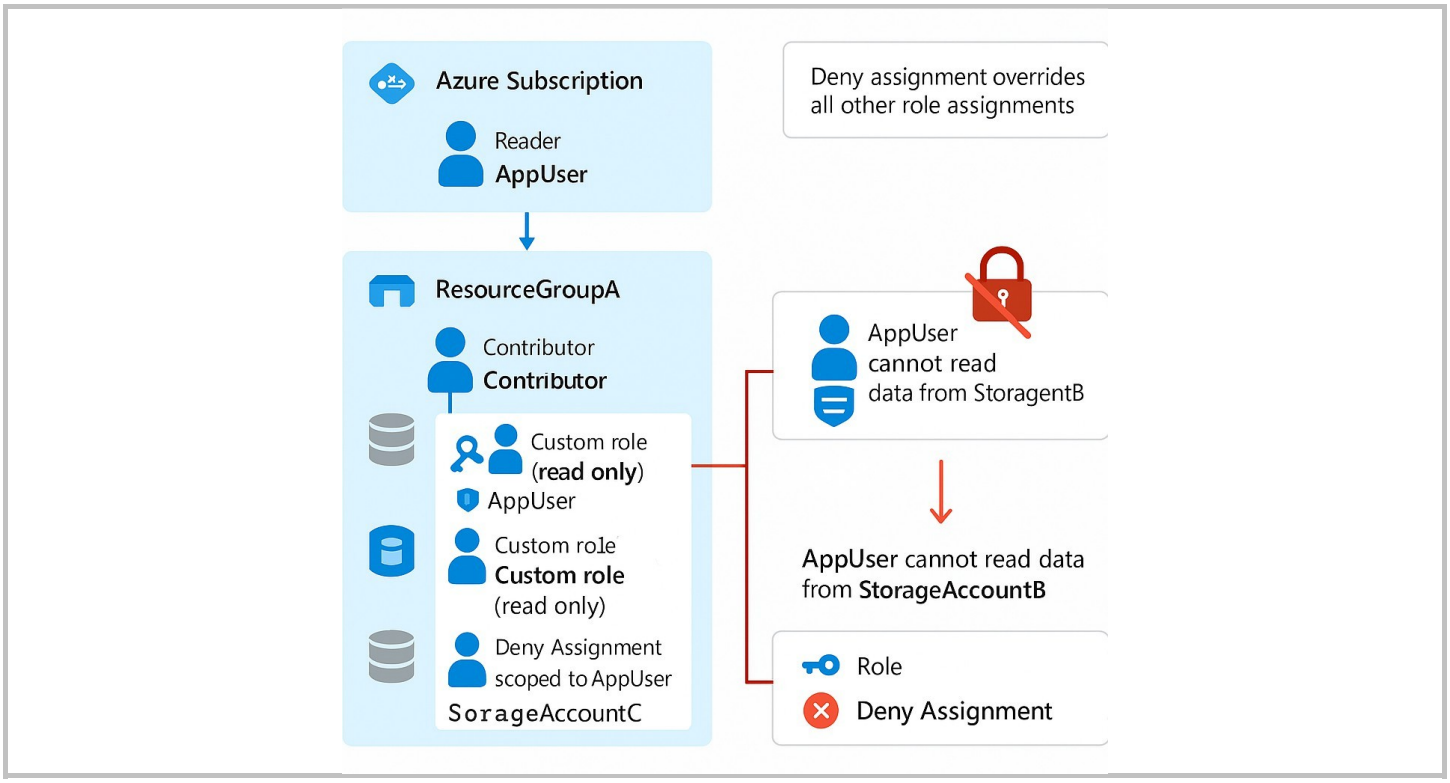
- [ ] E. AppUser will not be able to read data from Storage Account B due to the presence of a deny assignment, even though the custom role grants read access right

Explanation:

Correct Answers: B and E

Option B is CORRECT because Azure RBAC has a well-defined priority: deny assignments take precedence over role-based access (RBAC assignments). This means that even though AppUser has been assigned the Reader role at the subscription level and a custom read role on Storage Account B, the deny assignment on Storage Account B will prevent any access to that storage account. Deny assignments cannot be overridden by role assignments at lower scopes, ensuring that the principle of least privilege is enforced by denying access explicitly.

Option E is CORRECT because deny assignments take precedence over role-based access assignments in Azure. Even though AppUser is assigned a custom role that grants read permissions on Storage Account B, the deny assignment explicitly blocks any access to that storage account. Azure enforces this to prevent conflicts and ensures that deny overrides any role-based permission, regardless of what roles or assignments are in place.



Option A is INCORRECT because AppUser's ability to access resources is not solely determined by their Reader role at the subscription level. The Reader role allows read access to most resources, but role assignments and deny assignments at lower scopes (resource groups or individual resources like storage accounts) override this global access. The deny assignment on Storage Account B will prevent AppUser from accessing that particular storage account, regardless of the global Reader role.

Option C is INCORRECT because of the aforementioned priority of denying assignments. Even though the custom role grants read access to Storage Account B, the deny assignment on that specific resource will take precedence. Deny assignments effectively block any permissions, even if the user has roles that would typically allow access. Therefore, AppUser's access to Storage Account B is indeed affected by the deny assignment, and the custom role cannot grant read access in this case.

Option D is INCORRECT because the Contributor role does grant permissions to modify resources at the Resource Group A level, but it does not inherently provide full access. The Contributor role allows for creating and managing resources, but it does not grant the ability to read resources (since Reader would be needed for that). Furthermore, Contributor role access applies at the Resource Group A level and does not extend to individual resources like Storage Account B, especially considering the deny assignment at the storage account level. Thus, AppUser will have management capabilities within Resource Group A but will not have access to the specific resources (like Storage Account B) if there is a deny assignment.

References:

What is Azure role-based access control (Azure RBAC)?

Azure deny assignments

Ask our Experts

Did you like this **Question?**

Finish Review