

Free Questions for SC-300

Shared by Maddox on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

SIMULATION

Task 10

You need to create a group named Audit. The solution must ensure that the members of Audit can activate the Security Reader role.

Options:

A- See the Explanation for the complete step by step solution

Answer:

A

Explanation:

To create a group named "Audit" and ensure that its members can activate the Security Reader role, follow these steps:

Open the Microsoft Entra admin center:

Sign in with an account that has the Security Administrator or Global Administrator role.

Navigate to Groups:

[Go to Teams & groups > Active teams and groups1.](#)

Create the security group:

Select Add a security group.

On the Set up the basics page, enter "Audit" as the group name.

[Add a description if necessary and choose Next1.](#)

Edit settings:

[On the Edit settings page, select whether you want Microsoft Entra roles to be assignable to this group and select Next1.](#)

Assign roles:

After creating the group, go to Roles > All roles.

Find and select the Security Reader role.

Under Assignments, choose Assign.

[Select the "Audit" group to assign the role to its members2.](#)

Review and finish:

Review the settings to ensure the "Audit" group is created with the ability for its members to activate the Security Reader role.

Finish the setup and save the changes.

By following these steps, you will have created the "Audit" group and enabled its members to activate the Security Reader role, which allows them to view security-related information without having permissions to change it. Remember to communicate the new group and role assignment to the relevant stakeholders in your organization.

Question 2

Question Type: MultipleChoice

SIMULATION

Task 9

You need to ensure that when users in the Sg-Operations group go to the My Apps portal a tab named Operations appears that contains only the following applications:

- * Unkedln

- * Box

Options:

A- See the Explanation for the complete step by step solution

Answer:

A

Explanation:

To ensure that users in the Sg-Operations group see a tab named "Operations" containing only LinkedIn and Box applications in the My Apps portal, you can create a collection with these specific applications. Here's how to do it:

Sign in to the Microsoft Entra admin center:

Make sure you have one of the following roles: Global Administrator, Cloud Application Administrator, Application Administrator, or owner of the service principal.

Navigate to App launchers:

Go to Identity > Applications > Enterprise applications.

Under Manage, select App launchers.

Create a new collection:

Click on New collection.

Enter "Operations" as the Name for the collection.

Provide a Description if necessary.

Add applications to the collection:

Select the Applications tab within the new collection.

Click on + Add application.

Search for and select LinkedIn and Box applications.

Click Add to include them in the collection.

Assign the collection to the Sg-Operations group:

Select the Users and groups tab.

Click on + Add users and groups.

Search for and select the Sg-Operations group.

Click Select to assign the collection to the group.

Review and create the collection:

Select Review + Create to check the configuration.

If everything is correct, click Create to finalize the collection.

By following these steps, when users in the Sg-Operations group visit the My Apps portal, they will see a new tab named "Operations" that contains only the LinkedIn and Box applications1.

Please note that to create collections on the My Apps portal, you need a Microsoft Entra ID P1 or P2 license1.

Question 3

Question Type: MultipleChoice

SIMULATION

Task 8

You need to prevent all users from using legacy authentication protocols when authenticating to Microsoft Entra ID.

Options:

A- See the Explanation for the complete step by step solution

Answer:

A

Explanation:

To prevent all users from using legacy authentication protocols when authenticating to Microsoft Entra ID, you can create a Conditional Access policy that blocks legacy authentication. Here's how to do it:

Sign in to the Microsoft Entra admin center:

Ensure you have the role of Global Administrator or Conditional Access Administrator.

Navigate to Conditional Access:

Go to Security > Conditional Access.

Create a new policy:

Select + New policy.

Give your policy a name that reflects its purpose, like "Block Legacy Auth".

Set users and groups:

Under Assignments, select Users or workload identities.

Under Include, select All users.

[Under Exclude, select Users and groups and choose any accounts that must maintain the ability to use legacy authentication. It's recommended to exclude at least one account to prevent lockout1.](#)

Target resources:

Under Cloud apps or actions, select All cloud apps.

Set conditions:

Under Conditions > Client apps, set Configure to Yes.

Check only the boxes for Exchange ActiveSync clients and Other clients.

Configure access controls:

Under Access controls > Grant, select Block access.

Enable policy:

Confirm your settings and set Enable policy to Report-only initially to understand the impact.

[After confirming the settings using report-only mode, you can move the Enable policy toggle from Report-only to On2.](#)

By following these steps, you will block legacy authentication protocols for all users, enhancing the security posture of your organization by requiring modern authentication methods. Remember to monitor the impact of this policy and adjust as necessary to ensure business continuity.

Question 4

Question Type: MultipleChoice

SIMULATION

Task 7

You need to lock out accounts for five minutes when they have 10 failed sign-in attempts.

Options:

A- See the Explanation for the complete step by step solution

Answer:

A

Explanation:

To configure the account lockout settings so that accounts are locked out for five minutes after 10 failed sign-in attempts, you can follow these steps:

Open the Microsoft Entra admin center:

Sign in with an account that has the Security Administrator or Global Administrator role.

Navigate to the lockout settings:

Go to Security > Authentication methods > Password protection.

Adjust the Smart Lockout settings:

Set the Lockout threshold to 10 failed sign-in attempts.

Set the Lockout duration (in minutes) to 5.

Please note that by default, smart lockout locks an account from sign-in after 10 failed attempts in Azure Public and Microsoft Azure operated by 21Vianet tenants¹. The lockout period is one minute at first, and longer in subsequent attempts. However, you can customize these settings to meet your organization's requirements if you have Microsoft Entra ID P1 or higher licenses for your users¹.

Question 5

Question Type: MultipleChoice

SIMULATION

Task 6

You need to implement additional security checks before the members of the Sg-Executive can access any company apps. The members must meet one of the following conditions:

* Connect by using a device that is marked as compliant by Microsoft Intune.

* Connect by using client apps that are protected by app protection policies.

Options:

A- See the Explanation for the complete step by step solution

Answer:

A

Explanation:

To implement additional security checks for the Sg-Executive group members before they can access any company apps, you can use Conditional Access policies in Microsoft Entra

a. Here's a step-by-step guide:

Sign in to the Microsoft Entra admin center:

Ensure you have the role of Global Administrator or Security Administrator.

Navigate to Conditional Access:

Go to Security > Conditional Access.

Create a new policy:

Select + New policy.

Name the policy appropriately, such as "Sg-Executive Security Checks".

Assign the policy to the Sg-Executive group:

Under Assignments, select Users and groups.

Choose Select users and groups and then Groups.

Search for and select the Sg-Executive group.

Define the application control conditions:

Under Cloud apps or actions, select All cloud apps to apply the policy to any company app.

Set the device compliance requirement:

Under Conditions > Device state, configure the policy to include devices marked as compliant by Microsoft Intune.

Set the app protection policy requirement:

Under Conditions > Client apps, configure the policy to include client apps that are protected by app protection policies.

Configure the access controls:

Under Access controls > Grant, select Grant access.

Choose Require device to be marked as compliant and Require approved client app.

Ensure that the option Require one of the selected controls is enabled.

Enable the policy:

Set Enable policy to On.

Review and save the policy:

Review all settings to ensure they meet the requirements.

Click Create to save and implement the policy.

By following these steps, you will ensure that the Sg-Executive group members can only access company apps if they meet one of the specified conditions, either by using a compliant device or a protected client app. This enhances the security posture of your organization by enforcing stricter access controls for executive-level users.

Question 6

Question Type: MultipleChoice

SIMULATION

Task 5

You need to assign a Windows 10/11 Enterprise E3 license to the Sg-Retail group.

Options:

A- See the Explanation for the complete step by step solution

Answer:

A

Explanation:

To assign a Windows 10/11 Enterprise E3 license to the Sg-Retail group, you can follow these steps:

Sign in to the Microsoft Entra admin center:

Make sure you have the role of Global Administrator or License Administrator.

Navigate to the licensing page:

[Go to Billing > Licenses1.](#)

Find the Windows 10/11 Enterprise E3 license:

Look for the Windows 10/11 Enterprise E3 license in the list of available products.

Assign licenses to the group:

Select the license and then choose Assign licenses.

Search for and select the Sg-Retail group.

Confirm the assignment and make sure that the correct number of licenses is available for the group.

Review and confirm the assignment:

Ensure that the licenses have been properly assigned to the Sg-Retail group without affecting other groups or users.

Monitor the license status:

Check the license usage and status to ensure that the Sg-Retail group members can utilize the Windows 10/11 Enterprise E3 features.

By following these steps, the Sg-Retail group should now have the Windows 10/11 Enterprise E3 licenses assigned to them.

Question 7

Question Type: MultipleChoice

SIMULATION

Task 4

You need to ensure that all users can consent to apps that require permission to read their user profile. Users must be prevented from consenting to apps that require any other permissions.

Options:

A- See the Explanation for the complete step by step solution

Answer:

A

Explanation:

To ensure that all users can consent to apps that require permission to read their user profile and prevent them from consenting to apps that require any other permissions, you can configure the user consent settings in the Microsoft Entra admin center. Here's how you can do it:

Sign in as a Global Administrator:

Access the Microsoft Entra admin center with Global Administrator privileges.

Navigate to user consent settings:

[Go to Identity > Applications > Enterprise applications > Consent and permissions > User consent settings1.](#)

Configure the consent settings:

Under User consent for applications, select the option that allows users to consent to apps that only require permission to read their user profile.

[Ensure that all other permissions are set to require administrator consent, thus preventing users from consenting to apps that require additional permissions1.](#)

Save the settings:

After configuring the consent settings, select Save to apply the changes.

By following these steps, you will have configured the system to allow user consent for apps that need to read the user profile while blocking consent for apps that require additional permissions. This setup helps maintain user autonomy where appropriate while safeguarding against unauthorized access to broader permissions.

Question 8

Question Type: MultipleChoice

SIMULATION

Task 3

You need to add the LinkedIn application as a resource to the Sales and Marketing access package. The solution must NOT remove any other resources from the access package.

Options:

A- See the Explanation for the complete step by step solution

Answer:

A

Explanation:

To add the LinkedIn application as a resource to the Sales and Marketing access package without removing any other resources, you can follow these steps:

Sign in to the Microsoft Entra admin center:

Ensure you have the role of Global Administrator or Identity Governance Administrator.

Navigate to Entitlement Management:

[Go to identity governance > Entitlement management > Access packages1.](#)

Select the Sales and Marketing access package:

Find and select the Sales and Marketing access package to modify it.

Add a new resource:

Within the access package details, select Resources.

Click on + Add resource.

Search for and select the LinkedIn application from the list of available resources.

Configure the resource role:

Assign the appropriate role for the LinkedIn application that users in the Sales and Marketing access package will have.

Review and update the access package:

Ensure that the LinkedIn application has been added as a resource.

Confirm that no other resources have been removed from the access package.

Save the changes:

After reviewing, save the changes to the access package.

Communicate the update:

Notify the relevant users about the addition of the LinkedIn application to their access package.

By following these steps, you will successfully add the LinkedIn application to the Sales and Marketing access package without affecting the other resources.

Question 9

Question Type: MultipleChoice

SIMULATION

Task 2

You need to implement a process to review guest users who have access to the Salesforce app. The review must meet the following requirements:

- * The reviews must occur monthly.
- * The manager of each guest user must review the access.
- * If the reviews are NOT completed within five days, access must be removed.
- * If the guest user does not have a manager, Megan Bowen must review the access.

Options:

A- See the Explanation for the complete step by step solution

Answer:

A

Explanation:

To implement a process for reviewing guest users' access to the Salesforce app with the specified requirements, you can use Microsoft Entra's Identity Governance access reviews feature. Here's a step-by-step guide:

Assign the appropriate role:

[Ensure you have one of the following roles: Global Administrator, User Administrator, or Identity Governance Administrator1.](#)

Navigate to Identity Governance:

Sign in to the Microsoft Entra admin center.

[Go to Identity governance > Access reviews1.](#)

Create a new access review:

Select New access review.

Choose the Salesforce app to review guest user access¹.

Configure the review settings:

Set the frequency of the review to monthly.

Define the duration of the review period to 5 days¹.

Determine the reviewers:

Assign the manager of each guest user as the reviewer.

If a guest user does not have a manager, assign Megan Bowen as the reviewer¹.

Automate the removal process:

Configure settings to automatically remove access if the review is not completed within the specified time frame¹.

Monitor and enforce compliance:

Regularly check the access review results to ensure compliance with the review policy¹.

Communicate the process:

Inform all stakeholders about the new review process and provide guidance on how to complete the reviews.

By following these steps, you can ensure that guest users' access to the Salesforce app is reviewed monthly, with managers being responsible for the review, and access is removed if the review is not completed in time.

Question 10

Question Type: MultipleChoice

SIMULATION

Task 1

You need to deploy multi factor authentication (MFA). The solution must meet the following requirements:

- * Require MFA registration only for members of the Sg-Finance group.
- * Exclude Debra Berger from having to register for MFA.
- * Implement the solution without using a Conditional Access policy.

Options:

A- See the Explanation for the complete step by step solution

Answer:

A

Explanation:

To deploy Multi-Factor Authentication (MFA) for only the members of the Sg-Finance group, excluding Debra Berger, and without using a Conditional Access policy, you can follow these steps:

Open the Microsoft Entra admin center:

Sign in as a Security Administrator or Global Administrator.

Navigate to MFA settings:

Go to Users > Active users.

On the Active users page, select Multi-factor authentication.

Manage user settings:

Find and select the Sg-Finance group.

Enable MFA for this group by setting the requirement status to Enabled.

Exclude a user from MFA:

In the Multi-factor authentication page, search for Debra Berger.

Set her MFA status to Disabled to exclude her from MFA registration.

Verify the configuration:

Ensure that all members of the Sg-Finance group have MFA enabled except for Debra Berger.

Communicate the change:

Inform the Sg-Finance group members about the MFA requirement and provide instructions on how to register for MFA.

Monitor the setup:

Check the sign-in logs to confirm that MFA is being prompted for the Sg-Finance group members and not for Debra Berger.

Question 11

Question Type: MultipleChoice

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 have an Active Directory forest that syncs to a Microsoft Entra tenant.

You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Microsoft Entra for up to 30 minutes.

You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Microsoft Entra.

Solution: You configure Microsoft Entra Password Protection.

Does this meet the goal?

Options:

A- Yes

B- No

Answer:

B

Explanation:

Topic 5,

SIMULATIONS and TASK

To Get Premium Files for SC-300 Visit

<https://www.p2pexams.com/products/sc-300>

For More Free Questions Visit

<https://www.p2pexams.com/microsoft/pdf/sc-300>

