SC-300 Q&As

Microsoft Identity and Access Administrator

Pass Microsoft SC-300 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/sc-300.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

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 a Microsoft 365 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services. Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a

sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate. Solution: From the Azure portal, you configure the Notifications settings for multi-factor authentication (MFA). Does this meet the goal?

A. Yes

B. No

Correct Answer: B

You need to configure the fraud alert settings.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

QUESTION 2

You need to sync the ADatum users. The solution must meet the technical requirements. What should you do?

A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.

B. From PowerShell, run Set-ADSyncScheduler.

C. From PowerShell, run Start-ADSyncSyncCycle.

D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

Correct Answer: A

You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).

QUESTION 3

You have a Microsoft 365 tenant.

You have an Active Directory domain that syncs to the Azure Active Directory {Azure AD) tenant.

Users connect to the internet by using a hardware firewall at your company. The users authenticate to the firewall by using their Active Directory credentials.

You plan to manage access to external applications by using Azure AD.

You need to use the firewall logs to create a list of unmanaged external applications and the users who access them.

What should you use to gather the information?

A. Cloud App Discovery in Microsoft Defender for Cloud Apps

B. enterprise applications in Azure AD

C. access reviews in Azure AD

D. Application Insights in Azure Monitor

Correct Answer: A

QUESTION 4

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain.

Users connect to the internet by using a hardware firewall at your company. The users authenticate to the firewall by using their Active Directory credentials.

You plan to manage access to external applications by using Azure AD.

You need to use the firewall logs to create a list of unmanaged external applications and the users who access them.

What should you use to gather the information?

A. Application Insights in Azure Monitor

B. access reviews in Azure AD

C. Cloud App Discovery in Microsoft Cloud App Security

D. enterprise applications in Azure AD

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/cloud-app-security/create-snapshot-cloud-discovery-reports#using-traffic-logs-for-cloud-discovery

QUESTION 5

You have an Azure Active Directory (Azure AD) tenant that contains a user named SecAdmin1. SecAdmin1 is assigned the Security administrator role.

SecAdmin1 reports that she cannot reset passwords from the Azure AD Identity Protection portal.

You need to ensure that SecAdmin1 can manage passwords and invalidate sessions on behalf of non-administrative users. The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

A. Authentication administrator

B. Helpdesk administrator

C. Privileged authentication administrator

D. Security operator

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference