Free Questions for SC-300 by go4braindumps

Shared by Mcclain on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You have an Azure Active Directory Premium P2 tenant.

You create a Log Analytics workspace.

You need to ensure that you can view Azure Active Directory (Azure AD) audit log information by using Azure Monitor.

What should you do first?

Options:

A- Run the Set-AzureADTenantDetail cmdlet.

B- Create an Azure AD workbook.

C- Modify the Diagnostics settings for Azure AD.

D- Run the Get-AzureADAuditDirectoryLogs cmdlet.

Answer:

C

Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics

Question 2

Question Type: MultipleChoice

You have an Azure Active Directory (Azure AD) tenant that contains cloud-based enterprise apps.

You need to group related apps into categories in the My Apps portal.

What should you create?

Options:

A- tags

B- collections

C- naming policies

D- dynamic groups

Answer:

B

Explanation:

https://support.microsoft.com/en-us/account-billing/customize-app-collections-in-the-my-apps-portal-2dae6b8a-d8b0-4a16-9a5d-71ed4d6a6c1d

Question 3

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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

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

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

Solution: From Azure AD, you modify the Diagnostics settings.

Does this meet the goal?

Options:

A- Yes

B- No

Answer:

A

Question 4

Question Type: **MultipleChoice**

You have a Microsoft 365 tenant.

All users have mobile phones and laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

Options:

A- a notification through the Microsoft Authenticator app

B- email

C- security questions

D- a verification code from the Microsoft Authenticator app

Answer:

D

Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app#verification-code-from-mobile-app

Question 5

Question Type: MultipleChoice

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure AD Identity Protection policies enforced.

You create an Azure Sentinel instance and configure the Azure Active Directory connector.

You need to ensure that Azure Sentinel can generate incidents based on the risk alerts raised by Azure AD Identity Protection.

What should you do first?

Options:

A- Add an Azure Sentinel data connector.

B- Configure the Notify settings in Azure AD Identity Protection.

C- Create an Azure Sentinel playbook.

D- Modify the Diagnostics settings in Azure AD.

Answer:

A

Explanation:

https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-ad-identity-protection

Question 6

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 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?

Options:

A- Yes

B- No

Answer:

B

Explanation:

You need to configure the fraud alert settings.

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