Free Questions for SC-300

Shared by Merrill on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

SC-300 Mix Questions IN THIS CASE STUDY

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

The users have the devices shown in the following table.

You create the following two Conditional Access policies:

* Name: CAPolicy1

* Assignments

o Users or workload identities: Group 1

o Cloud apps or actions: Office 365 SharePoint Online

o Conditions

Filter for devices: Exclude filtered devices from the policy

Rule syntax: device.displayName -starts With "Device*"

o Access controls

Grant: Block access

Session: 0 controls selected

o Enable policy: On

* Name: CAPolicy2

* Assignments

o Users or workload identities: Group2

o Cloud apps or actions: Office 365 SharePoint Online

o Conditions: 0 conditions selected

* Access controls

o Grant: Grant access

Require multifactor authentication

o Session:

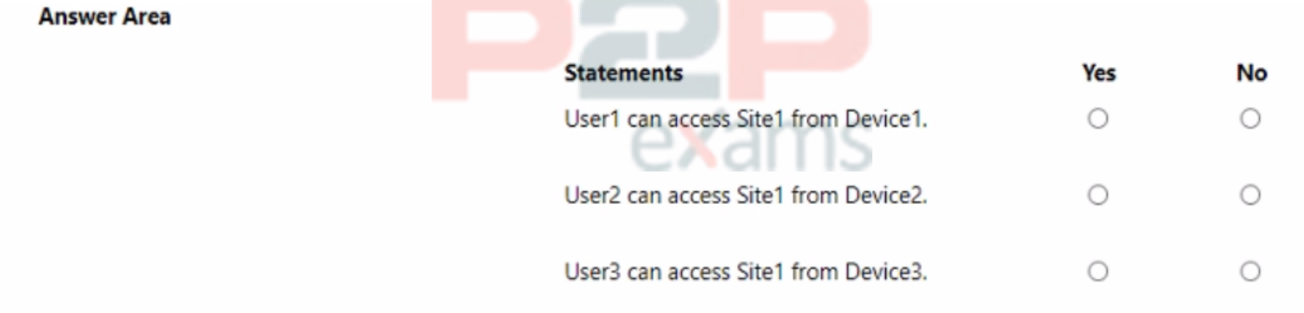
0 controls selected

* Enable policy: On

All users confirm that they can successfully authenticate using MFA.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User1 can access Site1 from Device1.	○	○
User2 can access Site1 from Device2.	○	○
User3 can access Site1 from Device3.	○	○

Answer:

See the Answer in the Premium Version!

Question 2

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

SC-300 Mix Questions IN THIS CASE STUDY

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:

D

Explanation:

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

Question 3

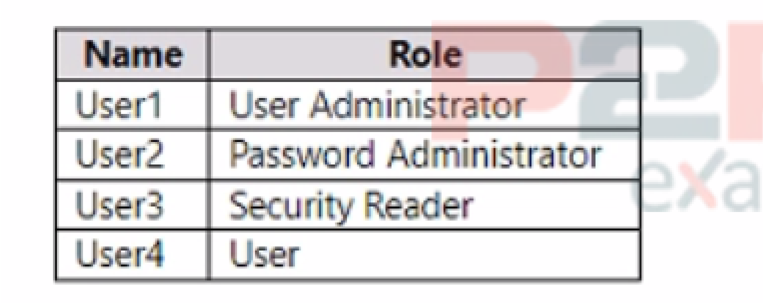
Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

SC-300 Mix Questions IN THIS CASE STUDY

You have an Azure AD tenant that contains the users shown in The following table.



Name	Role
User1	User Administrator
User2	Password Administrator
User3	Security Reader
User4	User

You enable self-service password reset (SSPR) for all the users and configure SSPR to require security questions as the only authentication method.

Which users must use security questions when resetting their password?

Options:

A- User4 only

B- User3and User4only

C- User1 and User4only

D- User1, User3, and User4 only

E- User1, User2, User3. and User4

Answer:

B

Question 4

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

SC-300 Mix Questions IN THIS CASE STUDY

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 5

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

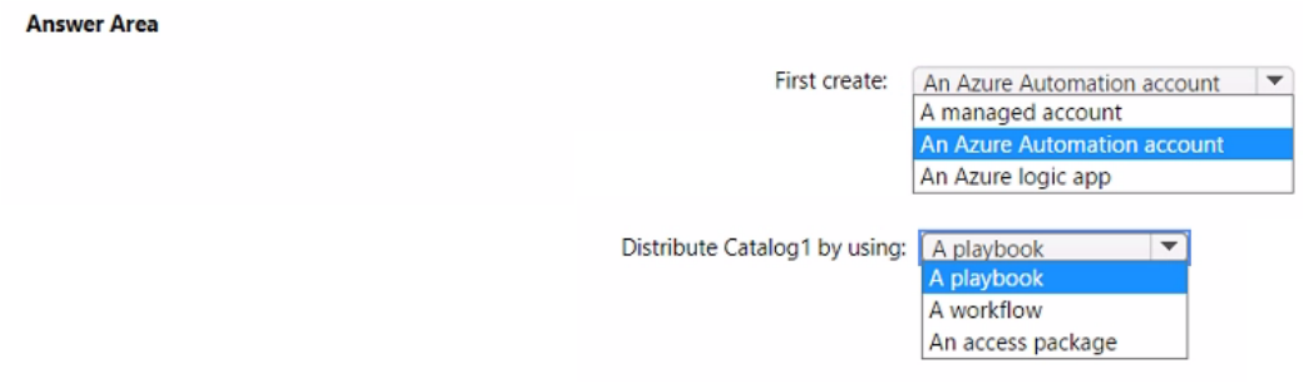
SC-300 Mix Questions IN THIS CASE STUDY

You have an Azure subscription.

From Entitlement management, you plan to create a catalog named Catalog1 that will contain a custom extension.

What should you create first and what should you use to distribute Catalog1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

First create: An Azure Automation account
- A managed account
- An Azure Automation account
- An Azure logic app

Distribute Catalog1 by using: A playbook
- A playbook
- A workflow
- An access package

Answer:

See the Answer in the Premium Version!

Question 6

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

SC-300 Mix Questions IN THIS CASE STUDY

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 7

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

SC-300 Mix Questions IN THIS CASE STUDY

You have an Azure Active Directory (Azure AD) tenant.

You need to review the Azure AD sign-in logs to investigate sign-ins that occurred in the past.

For how long does Azure AD store events in the sign-in logs?

Options:

A- 14 days
B- 30 days
C- 90 days
D- 365 days

Answer:

B

Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-dataretention#

how-long-does-azure-ad-store-the-data

Question 8

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

SC-300 Mix Questions IN THIS CASE STUDY

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 9

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

SC-300 Mix Questions IN THIS CASE STUDY

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 10

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

SC-300 Mix Questions IN THIS CASE STUDY

You have an Azure subscription that contains a virtual machine named VM1 and an Azure key vault named Vault1. VM1 has a system-assigned managed identity. You need to ensure that VM1 can retrieve the values of secrets stored in Vault 1. The solution must minimize administrative effort. What should you do first?

Options:

A- Configure the Resource access settings for Vault1.
B- Configure the permissions model for Vault1
C- Add a user-assigned managed identity to VM1.
D- Assign an Azure role to VM1.

Answer:

D

Question 11

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

SC-300 Mix Questions IN THIS CASE STUDY

You have a Microsoft Entra tenant.

You need to ensure that only users from specific external domains can be invited as guests to the tenant.

Which settings should you configure?

Options:

A- Cross-tenant access settings

B- External collaboration settings

C- Linked subscriptions

D- All identity providers

Answer:

B