MICROSOFT SC-300

Microsoft Identity and Access Administrator Certification Questions & Answers

Exam Summary – Syllabus –Questions

SC-300
Microsoft Certified - Identity and Access Administrator Associate
40-60 Questions Exam – 700 / 1000 Cut Score – Duration of 120 minutes

Table of Contents:

Know Your SC-300 Certification Well:

The SC-300 is best suitable for candidates who want to gain knowledge in the Microsoft Security Compliance and Identity. Before you start your SC-300 preparation you may struggle to get all the crucial Identity and Access Administrator materials like SC-300 syllabus, sample questions, study guide.

But don't worry the SC-300 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the SC-300 syllabus?
- How many questions are there in the SC-300 exam?
- Which Practice test would help me to pass the SC-300 exam at the first attempt?

Passing the SC-300 exam makes you Microsoft Certified - Identity and Access Administrator Associate. Having the Identity and Access Administrator certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Microsoft SC-300 Identity and Access Administrator Certification Details:

Exam Name	Microsoft Certified - Identity and Access Administrator Associate
Exam Code	SC-300
Exam Price	$165 (USD)
Duration	120 mins
Number of Questions	40-60
Passing Score	700 / 1000
Books / Training	**Course SC-300T00: Microsoft Identity and Access Administrator**
Schedule Exam	**Pearson VUE**
Sample Questions	**Microsoft Identity and Access Administrator Sample Questions**
Practice Exam	**Microsoft SC-300 Certification Practice Exam**

SC-300 Syllabus:

Topic	Details
Implement an Identity Management Solution (25-30%)	
Implement initial configuration of Azure Active Directory	- configure and manage Azure AD directory roles - configure and manage custom domains - configure and manage device registration options - configure delegation by using administrative units - configure tenant-wide settings
Create, configure and manage identities	- create, configure and manage users - create, configure and manage groups - manage licenses
Implement and manage external identities	- manage external collaboration settings in Azure Active Directory - invite external users (individually or in bulk) - manage external user accounts in Azure Active Directory - configure identity providers (social and SAML/WS-fed)
Implement and manage hybrid identity	- implement and manage Azure Active Directory Connect (AADC) - implement and manage Azure AD Connect cloud sync - implement and manage Password Hash Synchronization (PHS) - implement and manage Pass-Through Authentication (PTA) - implement and manage seamless Single Sign-On (SSO) - implement and manage Federation (excluding manual ADFS deployments) - implement and manage Azure Active Directory Connect Health - troubleshoot synchronization errors
Implement an Authentication and Access Management Solution (25-30%)	
Plan and implement Azure Multifactor Authentication (MFA)	- plan Azure MFA deployment (excluding MFA Server) - implement and manage Azure MFA settings - manage MFA settings for users

Topic	Details
Manage user authentication	- administer authentication methods (FIDO2 / Passwordless) - implement an authentication solution based on Windows Hello for Business - configure and deploy self-service password reset - deploy and manage password protection - configure smart lockout thresholds - implement and manage tenant restrictions
Plan, implement and administer conditional access	- plan and implement security defaults - plan conditional access policies - implement conditional access policy controls and assignments (targeting, applications, and conditions) - testing and troubleshooting conditional access policies - implement application controls - implement session management
Manage Azure AD Identity Protection	- implement and manage a user risk policy - implement and manage sign-in risk policy - implement and manage MFA registration policy - monitor, investigate and remediate elevated risky users
Implement Access Management for Apps (10-15%)	
Plan, implement, and monitor the integration of Enterprise Apps for SSO	- implement and configure consent settings - discover apps by using MCAS or ADFS app report - design and implement access management for apps - design and implement app management roles - monitor and audit access / Sign-ins to Azure Active Directory integrated enterprise applications - integrate on-premises apps by using Azure AD application proxy - integrate custom SaaS apps for SSO - configure pre-integrated (gallery) SaaS apps - implement application user provisioning
Implement app registrations	- plan your line of business application registration strategy - implement application registrations - configure application permissions

Topic	Details
	- implement application authorization - plan and configure multi-tier application permissions
Plan and Implement an Identity Governance Strategy (25-30%)	
Plan and implement entitlement management	- define catalogs - define access packages - plan, implement and manage entitlements - implement and manage terms of use - manage the lifecycle of external users in Azure AD Identity Governance settings
Plan, implement and manage access reviews	- plan for access reviews - create access reviews for groups and apps - monitor access review findings - manage licenses for access reviews - automate access review management tasks - configure recurring access reviews
Plan and implement privileged access	- define a privileged access strategy for administrative users (resources, roles, approvals, thresholds) - configure Privileged Identity Management for Azure AD roles - configure Privileged Identity Management for Azure resources - assign roles - manage PIM requests - analyze PIM audit history and reports - create and manage break-glass accounts
Monitor and maintain Azure Active Directory	- analyze and investigate sign-in logs to troubleshoot access issues - review and monitor Azure AD audit logs - enable and integrate Azure AD diagnostic logs with Log Analytics / Azure Sentinel - export sign-in and audit logs to a third-party SIEM - review Azure AD activity by using Log Analytics / Azure Sentinel, excluding KQL use

Topic	Details
	- analyze Azure Active Directory workbooks / reporting - configure notifications

Microsoft SC-300 Sample Questions:

Question: 1

You have an Azure Active Directory (Azure AD) tenant named contoso.com. You implement entitlement management to provide resource access to users at a company named Fabrikam, Inc. Fabrikam uses a domain named fabrikam.com.

Fabrikam users must be removed automatically from the tenant when access is no longer required. You need to configure the following settings:

- Block external user from signing in to this directory: No

- Remove external user: Yes

- Number of days before removing external user from this directory: 90

What should you configure on the Identity Governance blade?

a) Access packages
b) Settings
c) Terms of use
d) Access reviews

Answer: b

Question: 2

Reference Scenario: **click here**

You have an Azure Active Directory (Azure AD) tenant. You open the risk detections report. Which risk detection type is classified as a user risk?

a) impossible travel
b) anonymous IP address
c) atypical travel
d) leaked credentials

Answer: d

Question: 3

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?

a) Modify the Diagnostics settings for Azure A
b) Run the Get-AzureADAuditDirectoryLogs cmdlet
c) Run the Set-AzureADTenantDetail cmdlet
d) Create an Azure AD workbook

Answer: a

Question: 4

You have an Azure Active Directory (Azure AD) tenant. You need to review the Azure AD sign-ins log to investigate sign ins that occurred in the past.
For how long does Azure AD store events in the sign-in log?

a) 30 days
b) 14 days
c) 90 days
d) 365 days

Answer: a

Question: 5

You have an Azure Active Directory (Azure AD) tenant. You configure self-service password reset (SSPR) by using the following settings:

- Require users to register when signing in: Yes

- Number of methods required to reset: 1

What is a valid authentication method available to users?

a) a mobile app code
b) mobile app notification
c) an email to an address in your organization
d) home prison

Answer: d

Question: 6

Your company recently implemented Azure Active Directory (Azure AD) Privileged Identity Management (PIM). While you review the roles in PIM, you discover that all 15 users in the IT department at the company have permanent security administrator rights.
You need to ensure that the IT department users only have access to the Security administrator role when required. What should you configure for the Security administrator role assignment?

a) Expire eligible assignments after from the Role settings details
b) Expire active assignments after from the Role settings details
c) Assignment type to Active
d) Assignment type to Eligible

Answer: d

Question: 7

You have a Microsoft 365 tenant. In Azure Active Directory (Azure AD), you configure the terms of use. You need to ensure that only users who accept the terms of use can access the resources in the tenant. Other users must be denied access.
What should you zzconfigure?

a) an access policy in Microsoft Cloud App Security
b) Terms and conditions in Microsoft Endpoint Manager
c) a conditional access policy in Azure AD
d) a compliance policy in Microsoft Endpoint Manager

Answer: c

Question: 8

Reference Scenario: **click here**

You configure a new Microsoft 365 tenant to use a default domain name of contoso.com. You need to ensure that you can control access to Microsoft 365 resources by using conditional access policies.

What should you do first?

a) Disable the User consent settings
b) Disable Security defaults
c) Configure a multi-factor authentication (MFA) registration policy
d) Configure password protection for Windows Server Active Directory

Answer: b

Question: 9

You have an Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The on-premises network contains a VPN server that authenticates to the on-premises Active Directory domain.

The VPN server does NOT support Azure Multi-Factor Authentication (MFA). You need to recommend a solution to provide Azure MFA for VPN connections.

What should you include in the recommendation?

a) Azure AD Application Proxy
b) an Azure AD Password Protection proxy
c) Network Policy Server (NPS)
d) a pass-through authentication proxy

Answer: c

Question: 10

Reference Scenario: **click here**

You have an Azure Active Directory (Azure AD) tenant named contoso.com. All users who run applications registered in Azure AD are subject to conditional access policies.

You need to prevent the users from using legacy authentication. What should you include in the conditional access policies to filter out legacy authentication attempts?

a) a cloud apps or actions condition
b) a user risk condition
c) a client apps condition
d) a sign-in risk condition

Answer: c

Study Guide to Crack Microsoft Identity and Access Administrator SC-300 Exam:

- Getting details of the SC-300 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the SC-300 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Microsoft provided training for SC-300 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the SC-300 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on SC-300 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for SC-300 Certification

Make EduSum.com your best friend during your Microsoft Identity and Access Administrator exam preparation. We provide authentic practice tests for the SC-300 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual SC-300 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don’t bother if you don’t get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the SC-300 exam.

Start Online Practice of SC-300 Exam by visiting URL
https://www.edusum.com/microsoft/sc-300-microsoft-identity-and-access-administrator