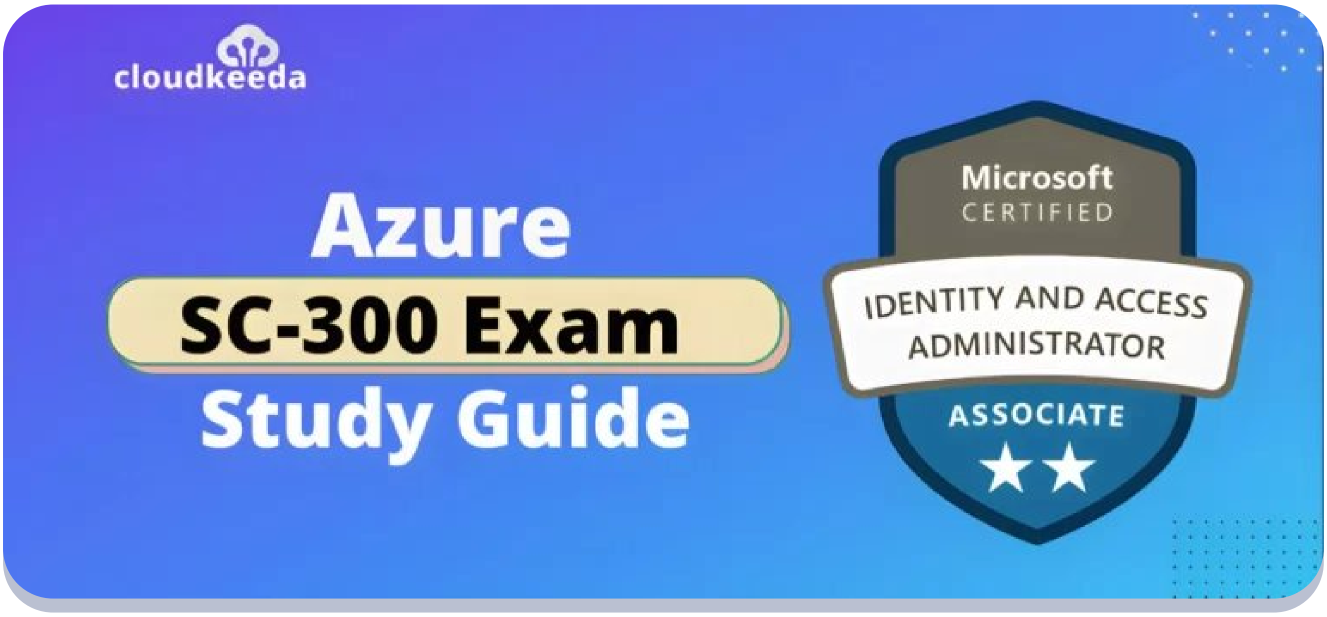


SC-300: Microsoft Certified Identity and Access Administrator Associate Exam Study Guide

March 17, 2023 by Sonali Jain

★★★★★ 5/5 - (27 votes)

The Microsoft SC-300 certification is designed to test and validate your skills and knowledge for implementing identity management and access solutions in Azure and 365.

The Identity and Access Administrator is responsible for designing and implementing security solutions across various Microsoft platforms for proper user authentication, authorization, and access management.

The certificate provides an excellent overview of identity and access infrastructure securely in this certification. Additionally, you'll learn how to use Identity Governance and Lifecycle, Conditional Access, Multi-Factor Authentication (MFA), and Identity Protection.

You will be more competitive in the job market and may receive a higher salary if you have the SC-300 certification.

Table of Contents

- SC-300 Certification Overview?
- Who Is Microsoft Identity and Access Administrator?
- Who This Certification Is For?
- Why SC-300 Certification
- Microsoft Identity and Access Administrator Responsibilities
- SC-300 Exam Details
- SC-300 Exam Skills Measured
- How to Register for SC 300 Certification Exam
- Prerequisite for SC-300 Certification
- SC-300 Study Guide
- SC-300 Exam Retake Policy
- Conclusion
- FAQs

SC-300 Certification Overview?

The Microsoft SC-300 certification exam measures candidates' ability to implement identity management solutions, acquire access management for apps, plan identity governance strategies, etc.

This course teaches students about how to manage access to data, services, apps, and infrastructure securely, as well as how to use Identity Governance &

Lifecycle, Conditional Access, Multi-Factor Authentication (MFA), Identity Protection, and more.

For anyone considering a career in IAM solutions, this course provides a great overview. This course demonstrates how to define and implement robust access control solutions, plan and implement a security strategy, and understand the fundamentals of Microsoft IAM.

This course will prepare students to set up and troubleshoot Microsoft IAM solutions in the cloud and develop and implement IAM security policies.

Are you new to Azure Cloud? Do check out our blog post on the Azure Certification Path 2023 and choose the best certification for you.

Who Is Microsoft Identity and Access Administrator?

Microsoft Identity and Access Administrator implement, manage, and access solutions in Microsoft Azure and Microsoft 365.

As Identity and Access Administrators, they are responsible for designing and implementing security solutions that ensure proper user authentication, authorization, and access management across various Microsoft platforms.

Azure Active Directory, Azure AD Connect, Microsoft 365, and other

Microsoft identity and access technologies fall under this category.

Who This Certification Is For?

Those who are planning to take the associated certification exam, or who perform identity and access administration tasks in their day-to-day jobs, should take this course.

Why SC-300 Certification

SC-300 certification offers the following advantages:

- With the SC-300 certification, you can manage identity and access solutions in complex enterprise environments.
- It validates your skills and expertise using Microsoft identity and access technologies, like Azure Active Directory, Azure AD Connect, and Microsoft 365.
- You will be more competitive in the job market with the certification. Additionally, it can lead to higher salaries.

Check Out: TOP 60+ Azure Interview Questions and Answers

Microsoft Identity and Access Administrator Responsibilities

Microsoft identity and access administrators have the following responsibilities:

- An identity and access administrator designs, implements, and maintains an organisation's identity and access management systems using Microsoft Azure Active Directory (Azure AD).

- Their responsibility is to configure and manage identities for Azure resources, applications, and devices.

- They offer seamless experiences and self-service management capabilities.

- To comply with Zero Trust principles, they verify identities explicitly.

- Using PowerShell, they automate Azure AD management and analyse events with Kusto Query Language.

- They're also responsible for troubleshooting, monitoring, and reporting.

- Managing identity solutions, implementing hybrid identity solutions, and implementing identity governance are all responsibilities of identity and access administrators.

SC-300 Exam Details

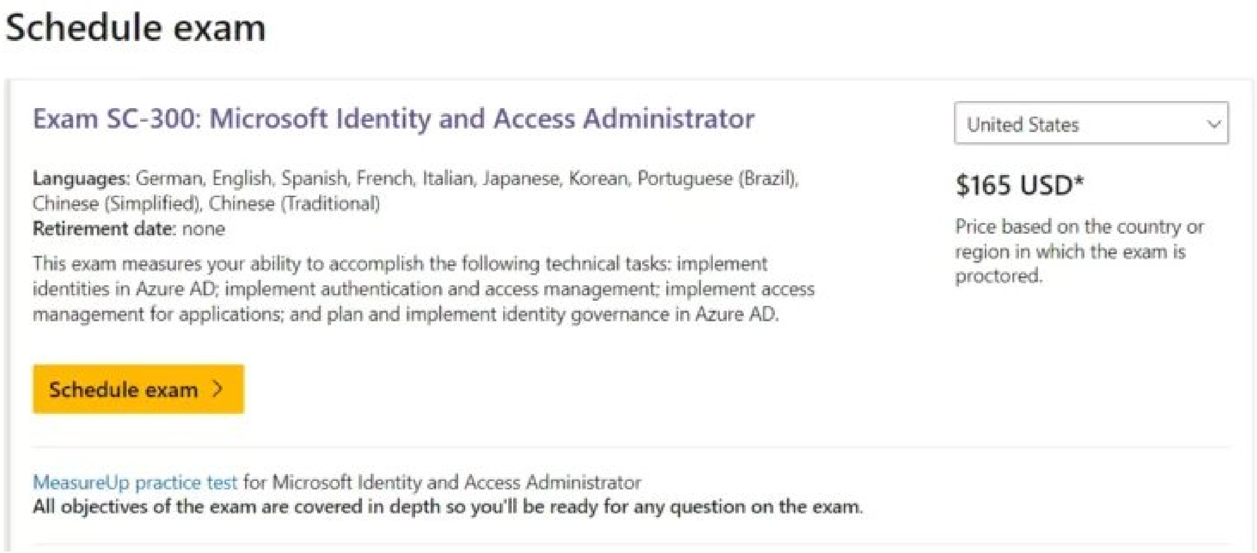
Exam Name SC-300: Microsoft Identity and Access Administrator	**Passing Marks** 700
Exam Fee $165	**Exam Duration** 180 Minutes
Exam Validity 1 Year	**Exam Languages** German, English, Spanish, French, Italian, Japanese, Korean, Portuguese (Brazil), Chinese (Simplified), Chinese (Traditional)
Total Questions 90-100 Questions	**Exam Type** Multiple-choice and Multiple response questions

SC-300 Exam Skills Measured

Implement identities in Azure AD	**20-25%**
Implement authentication and access management	**25-30%**
Implement access management for applications	**15-20%**
Plan and implement identity governance in Azure AD	**20–25%**

How to Register for SC 300 Certification Exam

You can register for the Microsoft Identity and Access Administrator Exam (SC-300) by going to the Official Microsoft Page.



Schedule exam

Exam SC-300: Microsoft Identity and Access Administrator

Languages: German, English, Spanish, French, Italian, Japanese, Korean, Portuguese (Brazil), Chinese (Simplified), Chinese (Traditional)
Retirement date: none

This exam measures your ability to accomplish the following technical tasks: implement identities in Azure AD; implement authentication and access management; implement access management for applications; and plan and implement identity governance in Azure AD.

MeasureUp practice test for Microsoft Identity and Access Administrator
All objectives of the exam are covered in depth so you'll be ready for any question on the exam.

$165 USD*

Price based on the country or region in which the exam is proctored.

How to Register for SC-300 Exam

Prerequisite for SC-300 Certification

The SC-300 prerequisites are as follows

- Microsoft Windows experience
- Worked with Microsoft Active Directory or related products
- Familiarity and understanding of networking concepts
- Basic understanding of security concepts

Also Check: Top 10 Microsoft Azure Security Best Practices

SC-300 Study Guide

Implement identities in Azure AD (20–25%)

Configure and manage an Azure AD tenant

- Configure and manage Azure AD roles
  - Assign Azure AD roles to users
- Configure delegation by using administrative units
  - Administrative units in Azure Active Directory
  - Configure delegation by using administrative units
- Analyze Azure AD role permissions
  - Azure AD built-in roles
- Configure and manage custom domains
  - Add custom domain name to Azure Active Directory
  - Configure and manage custom domains
- Configure tenant-wide settings
  - Configuration in a tenant
  - Configure tenant-wide setting

Create, configure, and manage Azure AD identities

- Create, configure, and manage users
  - Create, configure, and manage users
  - Create and manage users
- Create, configure, and manage groups

    - Create, configure, and manage groups
    - Create and manage groups
- Configure and manage device join and registration, including writeback
    - Azure AD Connect: Enabling device writeback
- Assign, modify, and report on licenses
    - Manage licenses

Implement and manage external identities

- Manage external collaboration settings in Azure AD
    - Manage external collaboration
    - Manage external collaboration settings in Azure Active Directory
- Invite external users, individually or in bulk
    - Invite external users – individually and in bulk
    - Invite guest users in bulk
    - Demo – manage guest users in Azure Active Directory
- Manage external user accounts in Azure AD
    - Manage external user accounts in Azure Active Directory
- Configure identity providers, including SAML or WS-fed
    - Configure identity providers

Implement and manage hybrid identity

- Implement and manage Azure AD Connect
    - Plan, design, and implement Azure Active Directory Connect
    - Get started with Azure AD Connect by using express settings
- Implement and manage Azure AD Connect cloud sync
    - What is Azure AD Connect cloud sync?
- Implement and manage Password Hash Synchronization (PHS)
    - What is password hash synchronization with Azure AD?
    - Implement manage password hash synchronization (PHS)
- Implement and manage Pass-Through Authentication (PTA)

    - What is Azure Active Directory Pass-through Authentication?
    - Implement manage pass-through authentication (PTA)
- Implement and manage seamless Single Sign-On (SSO)
    - Azure Active Directory Seamless single sign-on
    - Demo – Manage pass-through authentication and seamless single sign-on (SSO)
- Implement and manage Federation, excluding manual AD FS deployments
    - Implement and manage federation
- Implement and manage Azure AD Connect Health
    - Implement Azure Active Directory Connect Health
    - Manage Azure Active Directory Connect Health
- Troubleshoot synchronization errors
    - Trouble-shoot synchronization errors

Implement authentication and access management (25–30%)

Plan, implement, and manage Azure Multifactor Authentication (MFA) and self-service password reset

- Plan Azure MFA deployment, excluding MFA Server
    - What is Azure AD Multi-Factor Authentication?
    - Plan your multi-factor authentication deployment
- Configure and deploy self-service password reset
    - Let users reset their own passwords
- Implement and manage Azure MFA settings
    - Configure Azure AD Multi-Factor Authentication settings
- Manage MFA settings for users
    - Manage user authentication methods for Azure AD Multi-Factor Authentication
- Extend Azure AD MFA to third party and on-premises devices
    - Plan an Azure Active Directory Multi-Factor Authentication deployment

- Monitor Azure AD MFA activity
    - Use the sign-ins report to review Azure AD Multi-Factor Authentication events

Plan, implement, and manage Azure AD user authentication

- Plan for authentication
    - Plan an Azure Active Directory Multi-Factor Authentication deployment
- Implement and manage authentication methods
    - What authentication and verification methods are available in Azure Active Directory?
- Implement and manage Windows Hello for Business
    - Windows Hello for Business and Authentication
    - Implement an authentication solution based on Windows Hello for Business
- Implement and manage password protection and smart lockout
    - Protect user accounts from attacks with Azure Active Directory smart lockout
- Implement certificate-based authentication in Azure AD
    - How to configure Azure AD certificate-based authentication
- Configure Azure AD user authentication for Windows and Linux virtual machines on Azure
    - Log in to a Linux virtual machine in Azure by using Azure AD and OpenSSH

Plan, implement, and manage Azure AD conditional access

- Plan conditional access policies
    - Plan a Conditional Access deployment
- Implement conditional access policy assignments
    - Exercise – Implement Conditional Access policies roles and assignments

- Implement conditional access policy controls
    - Implement Conditional Access policies roles and assignments
- Test and troubleshoot conditional access policies
    - Test and troubleshoot Conditional Access policies
- Implement session management
    - Implement session management
- Implement device-enforced restrictions
    - Use app-enforced restrictions
- Implement continuous access evaluation
    - Continuous access evaluation
- Create a conditional access policy from a template
    - Conditional Access templates (Preview)

Manage Azure AD Identity Protection

- Implement and manage a user risk policy
    - Implement and manage user risk policy
    - Enable user risk policy
- Implement and manage sign-in risk policy
    - Enable user risk policy
- Implement and manage MFA registration policy
    - How To: Configure the Azure AD multifactor authentication registration policy
    - Exercise configure Azure Active Directory multi-factor authentication registration policy
- Monitor, investigate and remediate risky users
    - Monitor, investigate, and remediate elevated risky users
- Implement security for workload identities
    - Securing workload identities with Identity Protection

Implement access management for Azure resources

- Assign Azure roles

    - Assign Azure roles using the Azure portal
- Configure custom Azure roles
    - Create and assign a custom role in Azure Active Directory
- Create and configure managed identities
    - What are managed identities for Azure resources?
- Use managed identities to access Azure resources
- Analyze Azure role permissions
    - Azure built-in roles
- Configure Azure Key Vault RBAC and policies
    - Provide access to Key Vault keys, certificates, and secrets with an Azure role-based access control

Implement access management for applications (15–20%)

Manage and monitor application access by using Microsoft Defender for Cloud Apps

- Discover and manage apps by using Microsoft Defender for Cloud Apps
    - Microsoft Defender for Cloud Apps overview
- Configure connectors to apps
    - Create a custom connector from scratch
- Implement application-enforced restrictions
    - Use app-enforced restrictions
- Configure conditional access app control
    - Deploy Conditional Access App Control for catalog apps with Azure AD
- Create access and session policies in Microsoft Defender for Cloud Apps
    - Session policies
- Implement and manage policies for OAUTH apps
    - Create policies to control OAuth apps

Plan, implement, and monitor the integration of Enterprise applications

- Configure and manage user and admin consent
  - Configure how users consent to applications
- Discover apps by using ADFS application activity reports
  - Review the application activity report
- Design and implement access management for apps
  - Manage access to an application
- Design and implement app management roles
  - Application roles
- Monitor and audit activity in enterprise applications
  - Audit logs in Azure Active Directory
- Design and implement integration for on-premises apps by using Azure AD Application Proxy
  - Remote access to on-premises applications through Azure AD Application Proxy
- Design and implement integration for SaaS apps
  - Tutorials for integrating SaaS applications with Azure Active Directory
- Provision and manage users, groups, and roles on Enterprise applications
  - Assign users and groups to an application
- Create and manage application collections
  - Create collections on the My Apps portal

Plan and implement application registrations

- Plan for application registrations
  - Implement application registration
  - Exercise register an application
- Implement application registrations
  - Implement application registration

- Configure application permissions
  - Configure application permission
- Implement application authorization
  - Implement application authorization
- Plan and configure multi-tier application permissions
  - Making your application multi-tenant
- Manage and monitor applications by using App governance
  - App governance add-on to Defender for Cloud Apps in Microsoft 365 Defender

Plan and implement identity governance in Azure AD (20–25%)

Plan and implement entitlement management

- Plan entitlements
  - Configure entitlement management
- Create and configure catalogs
  - Create and manage a catalog of resources in entitlement management
- Create and configure access packages
  - Define access packages
  - What are access packages and what resources can I manage with them?
- Manage access requests
  - Set up and manage access requests
- Implement and manage terms of use
  - Exercise add terms of use acceptance report
- Manage the lifecycle of external users in Azure AD Identity Governance settings
  - Exercise manage the lifecycle of external users with Azure AD identity governance
- Configure and manage connected organizations

    - Add a connected organization in entitlement management
- Review per-user entitlements by using Azure AD Entitlement management
    - What is entitlement management?

Plan, implement, and manage access reviews

- Plan for access reviews
    - Plan for access reviews
    - Plan a Microsoft Entra access reviews deployment
- Create and configure access reviews for groups and apps
    - Create access reviews for groups and apps
- Create and configure access review programs
    - Create an access review of groups and applications in Azure AD
- Monitor access review activity
    - What are access reviews?
- Respond to access review activity, including automated and manual responses
    - Review access to groups and applications in access reviews

Plan and implement privileged access

- Plan and manage Azure roles in Privileged Identity Management (PIM), including settings and assignments
    - What is Azure AD Privileged Identity Management?
- Plan and manage Azure resources in PIM, including settings and assignments
    - Plan a Privileged Identity Management deployment
- Plan and configure Privileged Access groups
- Manage PIM requests and approval process
    - Approve or deny requests for Azure AD roles in Privileged Identity Management
- Analyze PIM audit history and reports

    - Analyze Privileged Identity Management audit history and reports
    - View audit history for Azure AD roles in Privileged Identity Management
- Create and manage break-glass accounts
    - Create and manage emergency access accounts
    - Manage emergency access accounts in Azure AD

Monitor Azure AD

- Design a strategy for monitoring Azure AD
    - Azure Active Directory reporting and monitoring deployment dependencies
- Review and analyze sign-in, audit, and provisioning logs by using the Azure Active Directory admin center
    - Analyze Azure AD activity logs with Azure Monitor logs
- Configure diagnostic settings, including Log Analytics, storage accounts, and Event Hub
    - Diagnostic settings in Azure Monitor
- Monitor Azure AD by using Log Analytics, including KQL queries
    - Get started with log queries in Azure Monitor
- Analyze Azure AD by using workbooks and reporting in the Azure Active Directory admin center
    - How to use Azure Monitor workbooks for Azure Active Directory
- Monitor and improve the security posture by using the Identity Secure Score
    - What is the identity secure score in Azure Active Directory?

SC-300 Exam Retake Policy

Retake policies for the Microsoft Exam SC-300 are as follows:

- A candidate who fails the first time must wait at least 24 hours before retaking the test.

- Candidates who don't pass the test the second time have to wait at least 14 days before retaking it.
- Also, there's a 14-day waiting period for the fourth and fifth retakes.

Conclusion

To conclude, Microsoft gives you a study guide, online courses, and practice tests so you can prepare for the SC-300 exam. It's a good idea if you have experience with Microsoft Windows, Active Directory, and networking concepts, and a basic understanding of security concepts. SC-300 has 40-60 questions and lasts 2 hours.

For those interested in a career in IAM solutions, the SC-300 certification offers many benefits.

You will be responsible for designing and implementing user authentication, authorization, and access management solutions across various Microsoft platforms.

With the right resources, you can succeed and validate your expertise in Microsoft identity and access technologies.

FAQs

Q1. How long is the SC 300 exam?

The SC 300 exam is 2 hours long.

Q2. Does SC-300 expire?

Within 6 months of passing the first SC-300 exam, you will be eligible to take the renewal exam, and you must renew the certification within 12 months.

Q3. How to prepare for the SC-300 exam?

Start by reviewing the exam objectives provided by Microsoft. This will give you a clear idea of the topics and skills that will be covered in the exam. Microsoft offers official study materials for the SC-300 exam, including a study guide, online courses, and practice tests. Preparing for the SC-300 exam can seem like a daunting task, but with a structured approach and the right resources, you can succeed.

Q4. How many questions is SC 300?

There are 40-60 questions in the SC-300 exam

Related Articles

- SC-200 Exam Study Guide
- AI-102 Exam Study Guide
- AZ-305 Exam Study Guide
- AZ-400 Exam Study Guide
- DP-900 Exam Study Guide

Sonali Jain

Sonali Jain is a highly accomplished Microsoft Certified Trainer, with over 6 certifications to her name. With 4 years of experience at Microsoft, she brings a wealth of expertise and knowledge to her role. She is a dynamic and engaging presenter, always seeking new ways to connect with her audience and make complex concepts accessible to all.

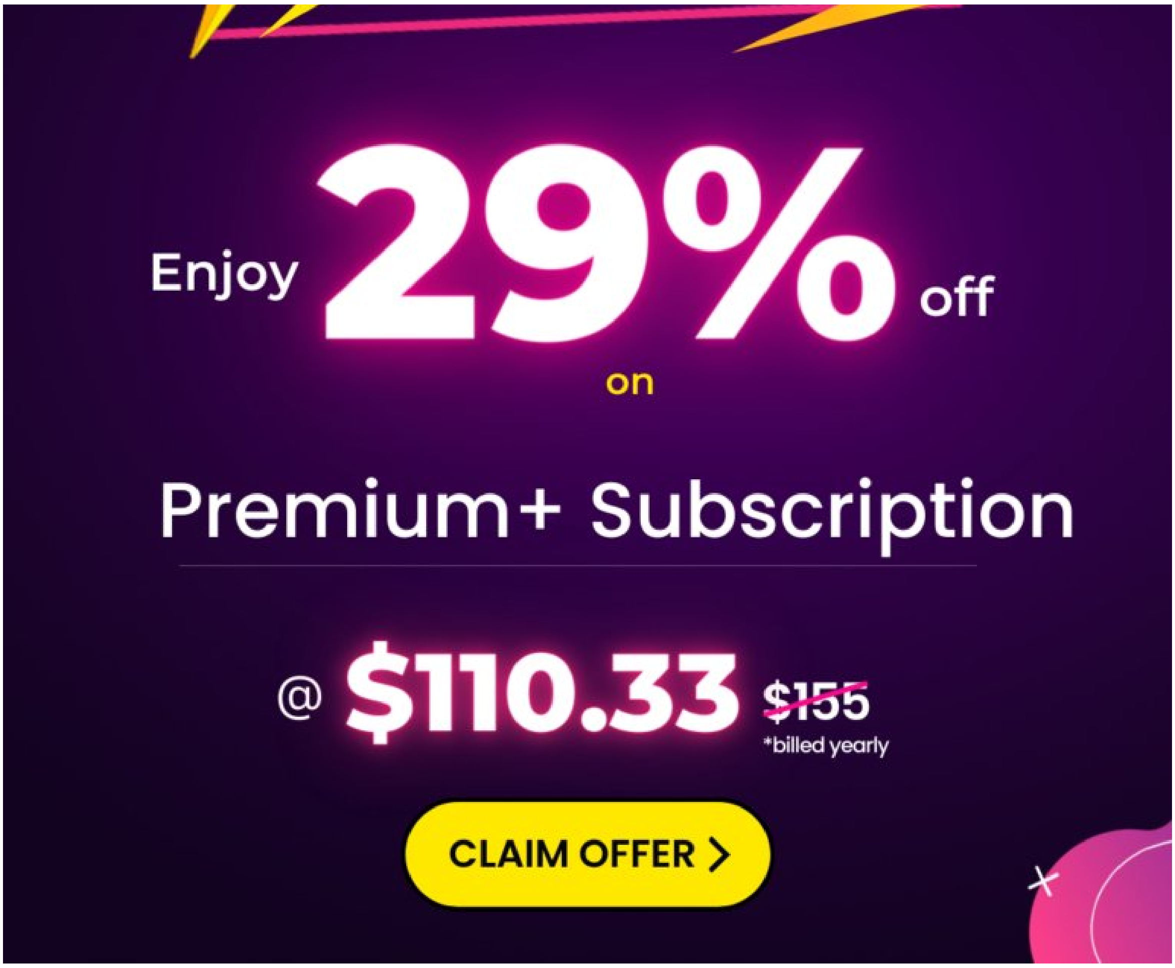
Leave a Comment

Name *

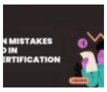
Email *

□ Save my name, email, and website in this browser for the next time I comment.

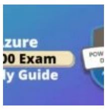
Post Comment



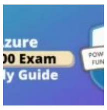
Recent Posts



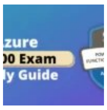
Common Mistakes to Avoid in Azure Certification Exams



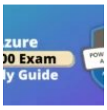
PL-400 Microsoft Power Platform Developer Exam Study Guide



PL-900 Microsoft Power Platform Fundamentals Exam Study Guide



PL-200 Microsoft Power Platform Functional Consultant Exam Study Guide



PL-100: Microsoft Power Platform App Maker Associate Exam Study Guide

Privacy Policy About HTML Sitemap