SC-300T00-A

Microsoft Identity and Access Administrator

32 horas | Microsoft 365 | Microsoft

INTRODUÇÃO

The Microsoft Identity and Access Administrator course explores how to design, implement, and operate an organization's identity and access management systems by using Azure AD. Learn to manage tasks such as providing secure authentication and authorization access to enterprise applications. You will also learn to provide seamless experiences and self-service management capabilities for all users. Finally, learn to create adaptive access and governance of your identity and access management solutions ensuring you can troubleshoot, monitor, and report on your environment. The Identity and Access Administrator may be a single individual or a member of a larger team. Learn how this role collaborates with many other roles in the organization to drive strategic identity projects. The end goal is to provide you knowledge to modernize identity solutions, to implement hybrid identity solutions, and to implement identity governance.

OBJETIVO DO CURSO

–

PÚBLICO-ALVO

Audience Profile

This course is for the Identity and Access Administrators who are planning to take the associated certification exam, or who are performing identity and access administration tasks in their day-to-day job. This course would also be helpful to an administrator or engineer that wants to specialize in providing identity solutions and access management systems for Azure-based solutions; playing an integral role in protecting an organization.

PRÉ-REQUISITOS

Prerequistes

Before attending this course, students should have understanding of:

• Security best practices and industry security requirements such as defense in depth, least privileged access, shared responsibility, and zero trust model.
• Be familiar with identity concepts such as authentication, authorization, and active directory.
• Have some experience deploying Azure workloads. This course does not cover the basics of Azure administration, instead the course content builds on that knowledge by adding security specific information.
• Some experience with Windows and Linux operating systems and scripting languages is helpful but not required. Course labs may use PowerShell and the CLI.

CONTEÚDO PROGRAMÁTICO

COURSE OUTLINE

Module 1: SC-300: Implement an identity management solution

Learn to create and manage your initial Azure Active Directory (Azure AD) implementation and configure the users, groups, and external identities you will use to run your solution. Aligned to SC-300 Exam.

• Implement initial configuration of Azure Active Directory
• Create, configure, and manage identities
• Implement and manage external identities
• Implement and manage hybrid identity

Module 2: SC-300: Implement an Authentication and Access Management solution

Implement and administer your access management using Azure AD. Use MFA, Conditional Access, and identity protection to manager your identity solution. Aligned to SC-300 exam.

• Secure Azure Active Directory users with Multi-Factor Authentication
• Manage user authentication
• Plan, implement, and administer Conditional Access
• Manage Azure AD Identity Protection
• Implement access management for Azure resources

Module 3: SC-300: Implement Access Management for Apps

Explore how applications can and should be added to your identity and access solution with application registration in Azure AD. Aligned to SC-300 Exam.

• Plan and design the integration of enterprise apps for SSO
• Implement and monitor the integration of enterprise apps for SSO
• Implement app registration

Module 4: SC-300: Plan and implement an identity governance strategy

Design and implement identity governance for your identity solution using entitlement, access reviews, privileged access, and monitoring your Azure Active Directory (Azure AD). Aligned to SC-300 exam.

• Plan and implement entitlement management
• Plan, implement, and manage access review
• Plan and implement privileged Access
• Monitor and maintain Azure Active Directory