COURSE OVERVIEW

Course Name:
(SC-300) Microsoft Identity and Access Administrator

COURSE DURATION: 4 Days

Gauteng:
3rd Floor, 34 Whitely Road
Melrose Arch
Johannesburg
2196

Gauteng:
192 on Bram
192 Bram Fischer Drive
Ferndale, Randburg
Johannesburg
2160

Cape Town:
3rd Floor, Thomas Pattullo Building
19 Jan Smuts St
Cape Town
8000

Durban:
9 Mountview Close
Broadlands
Mount Edgecombe
Durban
4302

087 941 5764
sales@impactful.co.za
impactful.co.za

INTRODUCTION

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.

DELIVERY METHOD

Our courses have flexible delivery options:

- In-person classroom training at the Impactful training facilities
  - Johannesburg, Durban, Cape Town
- Virtual instructor-led training
- Nationally: on-site at the client

IMPACTFUL
Powered by LRMG

INTENDED AUDIENCE

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.

PREREQUISITES

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.

COURSE CONTENT

Explore identity and Azure AD

This module will cover definitions and available services for identity provided in Azure AD to Microsoft 365. You start with authentication, authorization, and access tokens then build into full identity solutions.

Implement initial configuration of Azure Active Directory

Learn to create an initial Azure Active Directory configuration to ensure all the identity solutions available in Azure are ready to use. This module explores how to build and configure an Azure AD system.

Create, configure, and manage identities

Access to cloud-based workloads needs to be controlled centrally by providing a definitive identity for each user and resource. You can ensure employees and vendors have just-enough access to do their job.

Implement and manage external identities

Inviting external users to use company Azure resources is a great benefit, but you want to do it in a secure way. Explore how to enable secure external collaboration.

Implement and manage hybrid identity

Creating a hybrid-identity solution to use your on-premises active directory can be challenging. Explore how to implement a secure hybrid-identity solution.

Secure Azure Active Directory users with Multi-Factor Authentication

Learn how to use multi-factor authentication with Azure AD to harden your user accounts.

Manage user authentication

There are multiple options for authentication in Azure AD. Learn how to implement and manage the right authentications for users based on business needs.

Plan, implement, and administer Conditional Access

Conditional Access gives a fine granularity of control over which users can do specific activities, access which resources, and how to ensure data and systems are safe.

Manage Azure AD Identity Protection

Protecting a user's identity by monitoring their usage and sign-in patterns will ensure a secure cloud solution. Explore how to design and implement Azure AD Identity protection.

Implement access management for Azure resources

Explore how to use built-in Azure roles, managed identities, and RBAC-policy to control access to Azure resources.

Plan and design the integration of enterprise apps for SSO

Enterprise app deployment enables control over which users can access the apps, easily log into apps with single-sign-on, and provide integrated usage reports.

Implement and monitor the integration of enterprise apps for SSO

Deploying and monitoring enterprise applications to Azure solutions can ensure security. Explore how to deploy on-premises and cloud based apps to users.

Implement app registration

Line of business developed in-house need registration in Azure AD and assigned to users for a secure Azure solution. Explore how to implement app registration.

Plan, implement, and manage access review

Once identity is deployed, proper governance using access reviews is necessary for a secure solution. Explore how to plan for and implement access reviews.

Monitor and maintain Azure Active Directory

Azure AD audit and diagnostic logs provide a rich view into how users are accessing your Azure solution. Learn to monitor, troubleshoot, and analyze sign-in data.