TEMARIO

Course SC-300T00-A: Microsoft Identity and Access Administrator

CompuEducación®

Course (4 days)

About this course

This course provides IT Identity and Access Professional, along with IT Security Professional, with the knowledge and skills needed to implement identity management solutions based on Microsoft Azure AD, and it connected identity technologies. This course includes identity content for Azure AD, enterprise application registration, conditional access, identity governance, and other identity tools.

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.

Job role: Administrator, Identity And Access Administrator, Security Engineer
Preparation for exam: SC-300
Features: none

Skills gained

- Implement an identity management solution
- Implement an authentication and access management solutions
- Implement access management for apps
- Plan and implement an identity governancy strategy

Prerequisites

Successful learners will have prior knowledge and 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.

Prerequisite courses (or equivalent knowledge and hands-on experience):

This free online training will give you the experience you need to be successful in this course.

- SC-900 part 1: Describe the concepts of security, compliance, and identity - Learn | Microsoft Docs
- SC-900 part 2: Describe the capabilities of Microsoft Identity and access management solutions - Learn | Microsoft Docs
- SC-900 part 3: Describe the capabilities of Microsoft security solutions - Learn | Microsoft Docs
- SC-900 part 4: Describe the capabilities of Microsoft compliance solutions - Learn | Microsoft Docs
- AZ-104: Manage identities and governance in Azure - Learn | Microsoft Docs

TEMARIO

Module 1: 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.

Lessons

- Implement Initial configuration of Azure AD
- Create, configure, and manage identities
- Implement and manage external identities
- Implement and manage hybrid identity

Lab : Manage user roles

Lab : Setting tenant-wide properties

Lab : Assign licenses to users

Lab : Restore or remove deleted users

Lab : Add groups in Azure AD

Lab : Change group license assignments

Lab : Configure external collaboration

Lab : Add guest users to the directory

Lab : Explore dynamic groups

After completing this module, students will be able to:

- Deploy an initail Azure AD with custom settings
- Manage both internal and external identities
- Implement a hybrid identity solution

Module 2: 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.

Lessons

- Secure Azure AD user with MFA
- Manage user authentication
- Plan, implement, and administer conditional access
- Manage Azure AD identity protection

Lab : Enable Azure AD MFA

Lab : Configure and deploy self-service password reset (SSPR)

Lab : Work with security defaults

Lab : Implement conditional access policies, roles, and assignments

Lab : Configure authentication session controls

Lab : Manage Azure AD smart lockout values

Lab : Enable sign-in risk policy

Lab : Configure Azure AD MFA authentication registration policy

After completing this module, students will be able to:

- Configure and manage user authentication including MFA
- Control access to resources using conditional access
- Use Azure AD Identity Protection to protect your organization

Module 3: Mitigate threats using Azure Defender

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

Lessons

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

Lab : Implement access management for apps

Lab : Create a custom role to management app registration

Lab : Register an application

Lab : Grant tenant-wide admin consent to an application

Lab : Add app roles to applications and recieve tokens

After completing this module, students will be able to:

- Register a new application to your Azure AD
- Plan and implement SSO for enterprise application
- Monitor and maintain enterprise applications

Module 4: Plan and implement an identity governancy strategy

Design and implement identity governance for your identity solution using entitlement, access reviews, privileged access, and monitoring your Azure Active Directory (Azure AD).

Lessons

- Plan and implement entitlement management
- Plan, implement, and manage access reviews
- Plan and implement privileged access
- Monitor and maintain Azure AD

Lab : Creat and manage a resource catalog with Azure AD entitlement

Lab : Add terms of use acceptance report

Lab : Manage the lifecycle of external users with Azure AD identity governance

Lab : Create access reviews for groups and apps

Lab : Configure PIM for Azure AD roles

Lab : Assign Azure AD role in PIM

Lab : Assign Azure resource roles in PIM

Lab : Connect data from Azure AD to Azure

Use Azure Defender integrated with Azure Security Center, for Azure, hybrid cloud, and on-premises workload protection and security. Learn the purpose of Azure Defender, Azure Defender's relationship to Azure Security Center, and how to enable Azure Defender. You will also learn about the protections and detections provided by Azure Defender for each cloud workload. Learn how you can add Azure Defender capabilities to your hybrid environment.

Lessons

- Plan for cloud workload protections using Azure Defender
- Explain cloud workload protections in Azure Defender
- Connect Azure assets to Azure Defender
- Connect non-Azure resources to Azure Defender
- Remediate security alerts using Azure Defender

Lab : Mitigate threats using Azure Defender

- Deploy Azure Defender
- Mitigate Attacks with Azure Defender

After completing this module, students will be able to:

- Describe Azure Defender features
- Explain Azure Security Center features
- Explain which workloads are protected by Azure Defender
- Explain how Azure Defender protections function
- Configure auto-provisioning in Azure Defender
- Describe manual provisioning in Azure Defender
- Connect non-Azure machines to Azure Defender
- Describe alerts in Azure Defender
- Remediate alerts in Azure Defender
- Automate responses in Azure Defender

Module 4: Create queries for Azure Sentinel using Kusto Query Language (KQL)

Write Kusto Query Language (KQL) statements to query log data to perform detections, analysis, and reporting in Azure Sentinel. This module will focus on the most used operators. The example KQL statements will showcase security related table queries. KQL is the query language used to perform analysis on data to create analytics, workbooks, and perform hunting in Azure Sentinel. Learn how basic KQL statement structure provides the foundation to build more complex statements. Learn how to summarize and visualize data with a KQL statement provides the foundation to build detections in Azure Sentinel. Learn how to use the Kusto Query Language (KQL) to manipulate string data ingested from log sources.

Lessons

- Construct KQL statements for Azure Sentinel
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with data in Azure Sentinel using Kusto Query Language

Lab : Create queries for Azure Sentinel using Kusto Query Language (KQL)

- Construct Basic KQL Statements
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with string data using KQL statements

After completing this module, students will be able to:

- Construct KQL statements
- Search log files for security events using KQL
- Filter searches based on event time, severity, domain, and other relevant data using KQL
- Summarize data using KQL statements
- Render visualizations using KQL statements
- Extract data from unstructured string fields using KQL
- Extract data from structured string data using KQL
- Create Functions using KQL

Module 5: Configure your Azure Sentinel environment

Get started with Azure Sentinel by properly configuring the Azure Sentinel workspace. Traditional security information and event management (SIEM) systems typically take a long time to set up and configure. They're also not necessarily designed with cloud workloads in mind. Azure Sentinel enables you to start getting valuable security insights from your cloud and on-premises data quickly. This module helps you get started. Learn about the architecture of Azure Sentinel workspaces to ensure you configure your system to meet your organization's security operations requirements. As a Security Operations Analyst, you must understand the tables, fields, and data ingested in your workspace. Learn how to query the most used data tables in Azure Sentinel.

Lessons

- Introduction to Azure Sentinel
- Create and manage Azure Sentinel workspaces
- Query logs in Azure Sentinel
- Use watchlists in Azure Sentinel
- Utilize threat intelligence in Azure Sentinel

Lab : Configure your Azure Sentinel environment

- Create an Azure Sentinel Workspace
- Create a Watchlist
- Create a Threat Indicator

After completing this module, students will be able to:

- Identify the various components and functionality of Azure Sentinel.
- Identify use cases where Azure Sentinel would be a good solution.
- Describe Azure Sentinel workspace architecture
- Install Azure Sentinel workspace
- Manage an Azure Sentinel workspace
- Create a watchlist in Azure Sentinel
- Use KQL to access the watchlist in Azure Sentinel
- Manage threat indicators in Azure Sentinel
- Use KQL to access threat indicators in Azure Sentinel

Module 6: Connect logs to Azure Sentinel

Connect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds to Azure Sentinel. The primary approach to connect log data is using the Azure Sentinel provided data connectors. This module provides an overview of the available data connectors. You will get to learn about the configuration options and data provided by Azure Sentinel connectors for Microsoft 365 Defender.

Lessons

- Connect data to Azure Sentinel using data connectors
- Connect Microsoft services to Azure Sentinel
- Connect Microsoft 365 Defender to Azure Sentinel
- Connect Windows hosts to Azure Sentinel
- Connect Common Event Format logs to Azure Sentinel
- Connect syslog data sources to Azure Sentinel
- Connect threat indicators to Azure Sentinel

Lab : Connect logs to Azure Sentinel

- Connect Microsoft services to Azure Sentinel
- Connect Windows hosts to Azure Sentinel
- Connect Linux hosts to Azure Sentinel
- Connect Threat intelligence to Azure Sentinel

After completing this module, students will be able to:

- Explain the use of data connectors in Azure Sentinel
- Explain the Common Event Format and Syslog connector differences in Azure Sentinel
- Connect Microsoft service connectors
- Explain how connectors auto-create incidents in Azure Sentinel
- Activate the Microsoft 365 Defender connector in Azure Sentinel
- Connect Azure Windows Virtual Machines to Azure Sentinel
- Connect non-Azure Windows hosts to Azure Sentinel
- Configure Log Analytics agent to collect Sysmon events
- Explain the Common Event Format connector deployment options in Azure Sentinel
- Configure the TAXII connector in Azure Sentinel
- View threat indicators in Azure Sentinel

Module 7: Create detections and perform investigations using Azure Sentinel

Detect previously uncovered threats and rapidly remediate threats with built-in orchestration and automation in Azure Sentinel. You will learn how to create Azure Sentinel playbooks to respond to security threats. You'll investigate Azure Sentinel incident management, learn about Azure Sentinel events and entities, and discover ways to resolve incidents. You will also learn how to query, visualize, and monitor data in Azure Sentinel.

Lessons

- Threat detection with Azure Sentinel analytics
- Threat response with Azure Sentinel playbooks
- Security incident management in Azure Sentinel
- Use entity behavior analytics in Azure Sentinel
- Query, visualize, and monitor data in Azure Sentinel

Lab : Create detections and perform investigations using Azure Sentinel

- Create Analytical Rules
- Model Attacks to Define Rule Logic
- Mitigate Attacks using Azure Sentinel
- Create Workbooks in Azure Sentinel

After completing this module, students will be able to:

- Explain the importance of Azure Sentinel Analytics.
- Create rules from templates.
- Manage rules with modifications.
- Explain Azure Sentinel SOAR capabilities.
- Create a playbook to automate an incident response.
- Investigate and manage incident resolution.
- Explain User and Entity Behavior Analytics in Azure Sentinel
- Explore entities in Azure Sentinel
- Visualize security data using Azure Sentinel Workbooks.

Module 8: Perform threat hunting in Azure Sentinel

In this module, you'll learn to proactively identify threat behaviors by using Azure Sentinel queries. You'll also learn to use bookmarks and livestream to hunt threats. You will also learn how to use notebooks in Azure Sentinel for advanced hunting.

Lessons

- Threat hunting with Azure Sentinel
- Hunt for threats using notebooks in Azure Sentinel

Lab : Threat hunting in Azure Sentinel

- Threat Hunting in Azure Sentinel
- Threat Hunting using Notebooks

After completing this module, students will be able to:

- Describe threat hunting concepts for use with Azure Sentinel
- Define a threat hunting hypothesis for use in Azure Sentinel
- Use queries to hunt for threats.
- Observe threats over time with livestream.
- Explore API libraries for advanced threat hunting in Azure Sentinel
- Create and use notebooks in Azure Sentinel