email : techcenter@trainocate.com.my
contact : +603-2281-1111

SC-5008: Configure and govern entitlement with Microsoft Entra ID

Course Code: SC-5008
Duration: 1 day
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

Use Microsoft Entra to manage access by using entitlements, access reviews, privileged access tools, and monitor access events.

SKILLS COVERED

- Plan and implement entitlement management
- Plan, implement, and manage access review
- Monitor and maintain Microsoft Entra ID
- Plan and implement privileged access
- Explore the many features of Microsoft Entra Permissions Management

WHO SHOULD ATTEND?

- Administrator

PREREQUISITES

- Basic Azure administration knowledge.
- Ability to create users and groups using Microsoft Entra.

MODULES

Module 1: Plan and implement entitlement management

When new users or external users join your site, quickly assigning them access to Azure solutions is a must. Explore how to entitle users to access your site and resources.

Learning objectives

By the end of this module, you will be able to:

- Define catalogs.
- Define access packages.
- Plan, implement and manage entitlements.
- Implement and manage terms of use.
- Manage the lifecycle of external users in Microsoft Entra Identity Governance settings.

Module 2: 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.

Learning objectives

By the end of this module, you will be able to:

- Plan for access reviews
- Create access reviews for groups and apps
- Monitor the access review findings
- Manage licenses for access reviews
- Automate management tasks for access review
- Configure recurring access reviews

Module 3: Monitor and maintain Microsoft Entra ID

Audit and diagnostic logs within Microsoft Entra ID provide a rich view into how users are accessing your Azure solution. Learn to monitor, troubleshoot, and analyze sign-in data.

Learning objectives

By the end of this module, you'll be able to:

- Analyze and investigate sign in logs to troubleshoot access issues
- Review and monitor Microsoft Entra audit logs
- Enable and integrate Microsoft Entra diagnostic logs with Log Analytics / Azure Sentinel
- Export sign in and audit logs to a third-party SIEM (security information and event management)
- Review Microsoft Entra activity by using Log Analytics / Azure Sentinel, excluding KQL (Kusto Query Language) use
- Analyze Microsoft Entra workbooks / reporting
- Configure notifications

Module 4: Plan and implement privileged access

Ensuring that administrative roles are protected and managed to increase your Azure solution security is a must. Explore how to use PIM to protect your data and resources.

Learning objectives

By the end of this module, you will be able to:

- Define a privileged access strategy for administrative users (resources, roles, approvals, and thresholds)
- Configure Privileged Identity Management for Microsoft Entra roles
- Configure Privileged Identity Management for Azure resources
- Assign roles
- Manage PIM requests
- Analyze PIM audit history and reports
- Create and manage emergency access accounts

Module 5: Explore the many features of Microsoft Entra Permissions Management

While diving deeper into the features of Microsoft Entra Permissions Management, we use the framework of discover, remediate, monitor as a guide to help walkthrough how the Permissions Management features set can benefit your organization.

Learning objectives

By the end of this module, you'll be able to:

- Understand the features of Microsoft Entra Permissions Management
- Learn more specifics about how Permissions Management allows you to discover, remediate, and monitor identities, permissions, and resources
- Get real-world views of the data and analytics Permissions Management provides

END OF PAGE