

AZ-2001: Implement security through a pipeline using Azure DevOps

Course Description

This learning path helps you prepare for the Implement security through a pipeline assessment using Azure DevOps. Learn how to configure and secure Azure Pipelines. You'll also get opportunities to practice hands-on skills. These skills include configuring secure access to pipeline resources, configuring, and validating permissions, configuring a project and repository structure, extending a pipeline, configuring pipelines to use variables and parameters securely, and managing identity for projects, pipelines, and agents.

Course Duration

1 day

Prerequisites

- Basic knowledge of Azure DevOps.
- Basic knowledge of security concepts like identities and permissions.
- Experience using the Azure portal to create resources like Azure Key Vault and set permissions.

Course Outline

1 - Configure a project and repository structure to support secure pipelines

- Organize project and repository structure
- Configure secure projects and repositories

2 - Manage identity for projects, pipelines, and agents

- Configure a Microsoft-hosted pool
- Configure agents for projects
- Configure agent identities
- Configure the scope of a service connection
- Understand and convert to a Managed Identity

3 - Configure secure access to pipeline resources

- Configure agent pools
- Use secret variables and variable groups
- Understand secure files
- Configure service connections
- Manage environments
- Secure repositories

4 - Configure and validate permissions

- Configure and validate user permissions
- Configure and validate pipeline permissions
- Configure and validate approval and branch checks
- Manage and audit permissions

5 - Extend a pipeline to use multiple templates

- Create a nested template
- Rewrite the main deployment pipeline

- Configure the pipeline and the application to use tokenization
- Remove plain text secrets
- Restrict agent logging
- Identify and conditionally remove script tasks

6 - Configure secure access to Azure Repos from pipelines

- Configure pipeline access to packages
- Configure pipeline access to credential secrets
- Configure pipeline access to secrets for services
- Use Azure Key Vault to secure secrets
- Explore and secure log files

7 - Configure pipelines to securely use variables and parameters

- Ensure parameter and variable types
- Identify and restrict insecure use of parameters and variables
- Move parameters into a YAML file
- Limit queue time variables
- Validate mandatory variables

Who Should Attend

- Administrator
- Developer
- DevOps Engineer
- Security Engineer
- Security Operations Analyst
- Solution Architect
- Student
- Support Engineer