

MS-AZ2001: IMPLEMENT SECURITY THROUGH A PIPELINE USING AZURE DEVOPS



DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
1 Day	Intermediate	Azure	Instructor Led	NA

INTRODUCTION

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.

AUDIENCE PROFILE

This course is designed for individuals who want to enhance their skills in securing Azure Pipelines. The primary audience for this course includes:

- Administrators: Those responsible for managing and securing IT infrastructure and pipelines.
- DevOps Engineers: Professionals who focus on the development and operations of software and need to implement secure pipelines.
- Security Engineers: Individuals tasked with ensuring the security of applications and infrastructure within Azure environments.
- IT Professionals: Those with a basic understanding of Azure DevOps and security concepts who want to deepen their knowledge and skills in these areas.

PREREQUISITES

Before attending this course, delegates must have:

- An Azure Subscription. You need to bring your own subscription.
- 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 OBJECTIVES

After completion of this course, delegates will be able to:

- Configure secure access to pipeline resources: Ensure that only authorized users and systems can access pipeline resources.
- Configure and validate permissions: Set up and verify permissions to maintain security and compliance.
- Configure a project and repository structure to support secure pipelines: Organize projects and repositories in a way that enhances security.
- Extend a pipeline to use multiple templates: Utilize templates to streamline and secure pipeline configurations.
- Manage identity for projects, pipelines, and agents: Handle identities and permissions for various components within Azure DevOps.

COURSE CONTENT

Module 1: Configure a project and repository structure to support secure pipelines

This module is designed to help learners understand the importance of configuring a secure project and repository

structure to support pipelines in Azure DevOps. The module covers fundamental concepts and best practices for organizing the

project and repository structure and moving the security repository away from the application project.

Lessons

- Introduction.
- Organize project and repository structure.
- Configure secure projects and repositories.
- Lab - Configure a project and repository structure to support secure pipelines.
- Knowledge check.

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

- Separate a project into team projects and repositories.
- Separate secure files between projects.
- Move the security repository away from a project.
- Assign project and repository permissions.
- Organize a project and repository structure.

Module 2: Configure secure access to pipeline resources

This module is designed to help learners understand the importance of pipeline security and how to secure pipeline resources using Azure DevOps. The module covers fundamental concepts and best practices for secure agent pools, secret variables, files and storage, service connections, environments, and repositories.

Lessons

- Introduction.
- Configure agent pools.
- Use secret variables and variable groups.
- Understand secure files.
- Configure service connections.
- Manage environments.
- Secure repositories.
- Lab - Configure agents and agent pools for secure pipelines.
- Knowledge check.

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

- Identify and mitigate common security threats.
- Configure pipeline access to specific agent pools.
- Manage secret variables and variable groups.
- Secure files and storage.
- Configure service connections.
- Manage environments.
- Secure repositories.

Module 3: Manage identity for projects, pipelines, and agents

This module is designed to help learners understand the importance of managing identity for projects, pipelines, and agents in Azure DevOps. The module covers fundamental concepts and best practices for configuring a Microsoft-hosted pool, configuring agents for projects, configuring agent identities, configuring the scope of a service connection, and converting to a managed identity.

Lessons

- Introduction.
- 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.
- Lab - Manage identity for projects and pipelines.
- Knowledge check.

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

- Configure a Microsoft-hosted pool.
- Configure agents for projects.
- Configure agent identities.
- Configure the scope of a service connection.
- Convert to a managed identity in Azure DevOps.

Module 4: Configure and validate permissions

This module covers fundamental concepts and best practices for configuring and validating user permissions, pipeline permissions, approval and branch checks, and auditing and managing permissions.

Lessons

- Introduction.
- Configure and validate user permissions.
- Configure and validate pipeline permissions.
- Configure and validate approval and branch checks.
- Manage and audit permissions.
- Lab - Configure and validate permissions.
- Knowledge check.

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

- Configure and validate pipeline permissions.

- Configure and validate approval and branch checks.
- Manage and audit permissions in Azure DevOps.

Module 5: Extend a pipeline to use multiple templates

This module is designed to help learners understand the importance of extending a pipeline to multiple templates and how to do it using Azure DevOps. The module covers fundamental concepts and best practices for creating nested templates, rewriting the main deployment pipeline, configuring the pipeline and the application to use tokenization, removing plain text secrets, restricting agent logging, and identifying and conditionally removing script tasks.

Lessons

- Introduction.
- 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.
- Lab - Extend a pipeline to use multiple templates.
- Knowledge check.

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

- Create nested templates.
- 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 in Azure DevOps.

Module 6: Configure secure access to Azure Repos from pipelines

This module is designed to help learners understand the importance of securing access to Azure Repos from pipelines and how to do it using Azure DevOps. The module covers fundamental concepts and best practices for securing access to packages, credential secrets, secrets for services, and Azure Key Vault.

Lessons

- Introduction.

- 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.
- Lab - Integrate Azure Key Vault with Azure Pipelines.
- Knowledge check.

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

- Configure pipeline access to packages.
- Configure credential secrets, and secrets for services.
- Ensure that the secrets are in the Azure Key Vault.
- Ensure that secrets aren't in the logs.

Module 7: Configure pipelines to securely use variables and parameters Kubernetes Service

This module is designed to help learners understand the importance of configuring pipelines to use variables and parameters securely in Azure DevOps. The module covers fundamental concepts and best practices for ensuring that parameters and variables retain their type, identifying and restricting insecure use of parameters and variables, moving parameters into a YAML file that protects their type, limiting variables that can be set at queue time, and validating that mandatory variables are present and set correctly.

Lessons

- Introduction.
- 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.
- Lab - Configure pipelines to securely use variables and parameters.
- Knowledge check.

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

- Ensure that parameters and variables retain their type.
- Identify and restrict insecure use of parameters and variables.
- Move parameters into a YAML file that protects their type.
- Limit variables that can be set at queue time.
- Validate that mandatory variables are present and set correctly in Azure DevOps.

ASSOCIATED CERTIFICATIONS & EXAM

There is no Associated certification & Exam for this course, however, there is an assessment to achieve your Applied Skills credential. ([Assessment Link](#))