Learn

Implement security through a pipeline using Azure DevOps

Course AZ-2001: 1 day; Intermediate; Instructor-Led

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.

Note: You need an Azure subscription to complete the exercises. If you don't have an Azure subscription, create a free account and add a subscription before you begin. If you're a student, you can take advantage of the Azure for students offer.

Prerequisites

- 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 Outline

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.

In this module, you practice how 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.
- Prerequisites
- Basic knowledge of Azure DevOps to manage projects and repositories.
- Basic knowledge of security concepts for project repositories.

Lessons

- Organize project and repository structure
- Configure secure projects and repositories
- Lab - Configure a project and repository structure to support secure pipelines

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.

In this module, you practice how 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.

Prerequisites
- Basic knowledge of Azure DevOps to manage agents and service connections.
- Basic knowledge of security concepts like secret variables and secure files.

Lessons
- 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

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.

In this module, you practice how 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.

Prerequisites
- Basic knowledge of Azure DevOps to manage agents and service connections.
- Basic knowledge of security concepts like agent identities and managed identity.
- Experience using the Azure portal to create managed identities.

Lessons
- 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

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.

In this module, you practice how to:
- Configure and validate user permissions.
- Configure and validate pipeline permissions.
- Configure and validate approval and branch checks.
- Manage and audit permissions in Azure DevOps.
- Prerequisites
- Basic knowledge of Azure DevOps to manage branches.
- Basic knowledge of security concepts like user and pipeline permissions.

Lessons
- 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

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.

In this module, you practice how 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.

Prerequisites

- Basic knowledge of Azure Pipelines and YAML.
- Basic knowledge of security concepts for pipelines.
- Experience with application logs and troubleshooting.

Lessons

- 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

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.

In this module, you practice how 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.

Prerequisites

- Basic knowledge of Azure Pipelines and YAML.
- Basic knowledge of security concepts like Azure Key Vault and permissions.

Lessons

- 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

Module 7: Configure pipelines to securely use variables and parameters

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.

In this module, you practice how 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.

Prerequisites

- Basic knowledge of Azure Pipelines and YAML.

Lessons

- 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

