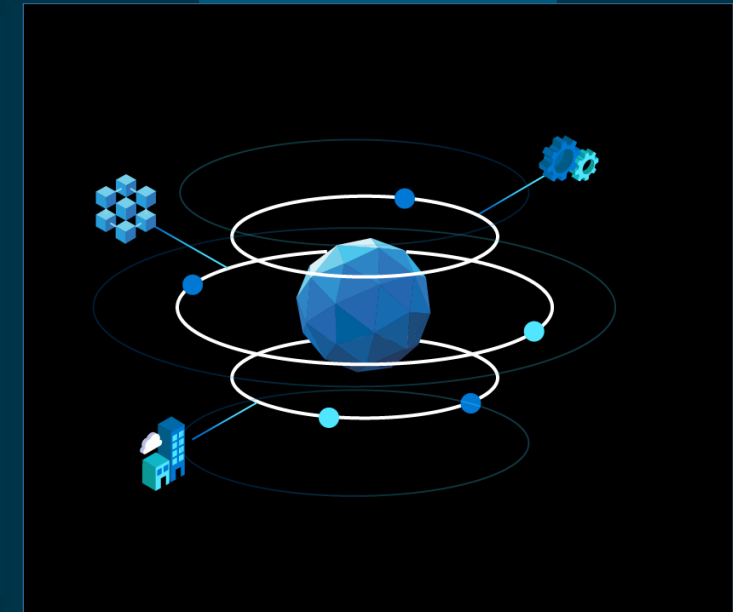


# Enterprise Readiness

*Prepared by Yeliz Kilinc, 16/6/2022*



# Azure Machine Learning Resources Overview

## Associated Resources



Storage



Key Vault



Container  
Registry



App Insights

## Model Inference Resources



AKS Cluster



ACI

## Model Training Resources



Compute  
Instance



Compute  
Cluster

## Data Stores



Storage



Data Lake



SQL

# Azure Machine Learning Security

Authentication  
&  
Authorization

Network  
Security

Data  
Protection

Policy  
&  
Monitoring

# Authentication

Authentication to AML workspace is based on Azure Active Directory.

## Authentication Workflows:

- 1- **Interactive** authentication enables you to control access to resources per user basis.
- 2- **Service Principle** is used when you need automated process to authenticate to the service without requiring user interactions. For ex CI/CD script to train&test the model.
- 3- **Managed Identity** allows various services to interact with AML without requiring admin keys or storing credentials in the code.

# Authorization

AzureML provides granular RBAC for multiple roles.

**Built-in roles:** Owner, Contributor, Reader and AML Data Scientist

## Custom roles :

### ML Flow Data Scientist

Perform all MLflow AzureML supported operations except Creation of compute, Deploying models to a production AKS cluster, Deploying a pipeline endpoint in production

### Workspace Admin

Allows you to perform all operations within the scope of a workspace, except: Creating a new workspace, Assigning subscription or workspace level quotas

### ML Ops Service Principal

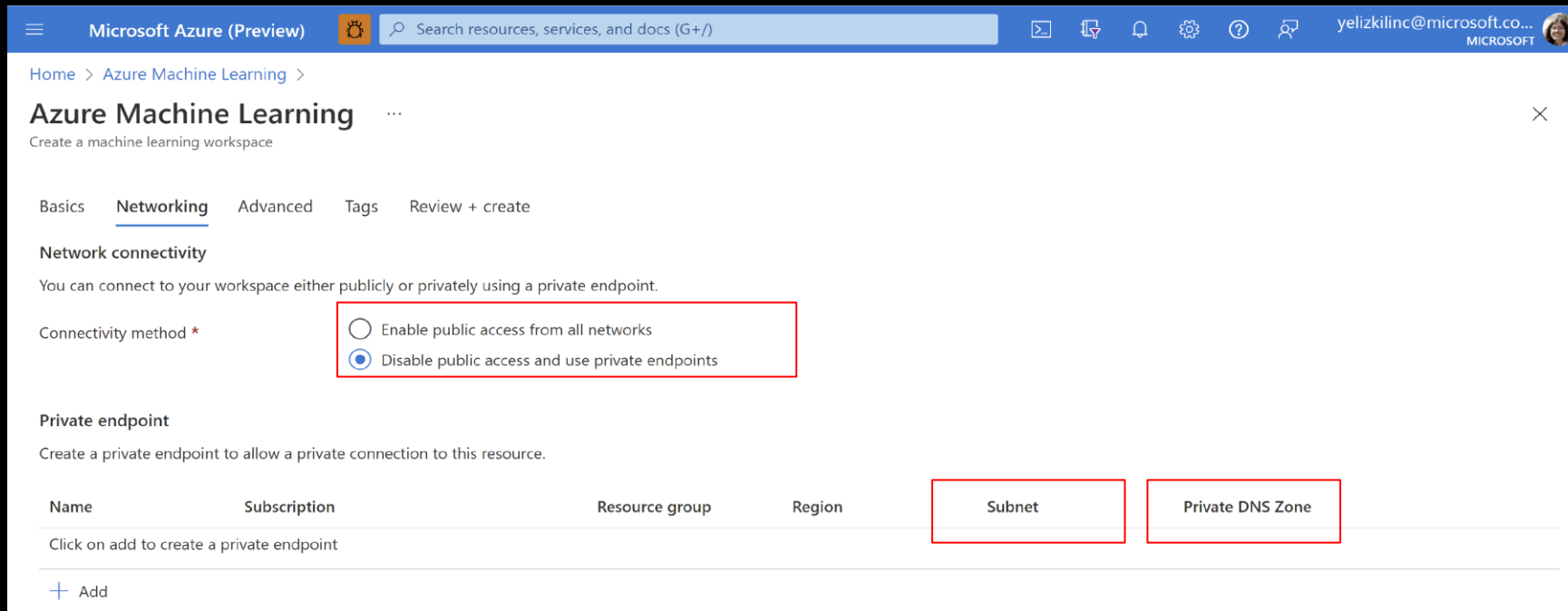
Can only trigger published pipeline runs

# Network Security

**Vnet** is an isolated network within the Microsoft Azure cloud.

**Private endpoint** is a network interface that uses a private IP address from your virtual network.

Traffic between your virtual network and the service travels the Microsoft backbone network with no exposure to the internet.



The screenshot shows the 'Networking' tab of the Azure Machine Learning workspace configuration. The 'Connectivity method' section has two radio buttons: 'Enable public access from all networks' (unselected) and 'Disable public access and use private endpoints' (selected). The 'Private endpoint' section includes a table with columns: Name, Subscription, Resource group, Region, Subnet, and Private DNS Zone. The 'Subnet' and 'Private DNS Zone' columns are highlighted with red boxes. Below the table is a '+ Add' button.

Name	Subscription	Resource group	Region	Subnet	Private DNS Zone
Click on add to create a private endpoint					



Azure Storage



Key Vault

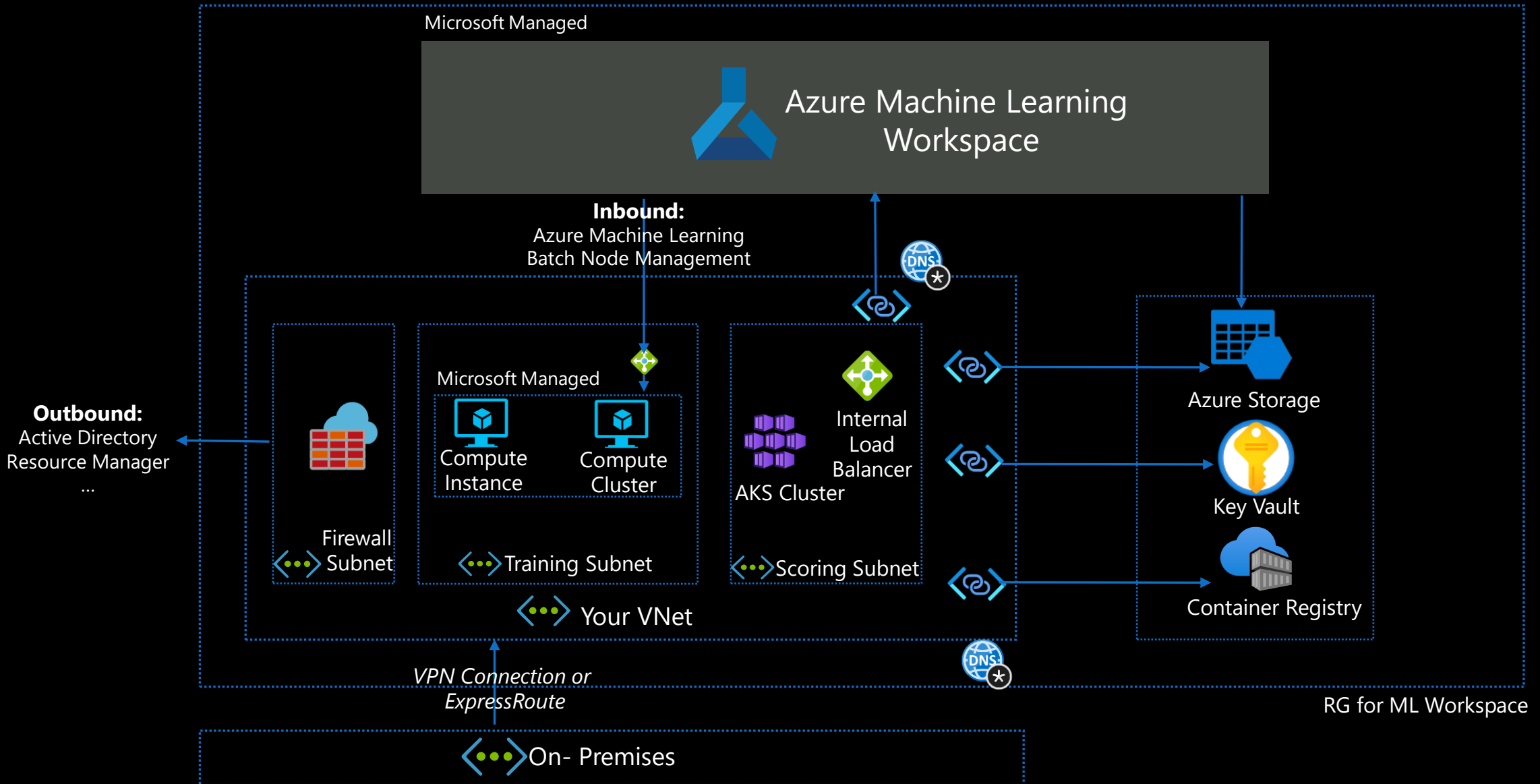


Container Registry

Learn more

[Overview doc](#) / [Configure Azure Private Link for AML](#)

# AML Recommended Network Security Architecture



# Data Protection



## At Rest

Home > New > Machine Learning >

### Machine learning

Create a machine learning workspace

Basics Networking **Advanced** Tags Review + create

#### Data encryption

Azure machine learning service stores metrics and metadata in an Azure Cosmos DB instance where all data is encrypted at rest. By default, the data is encrypted with Microsoft-managed keys. You may choose to bring your own (customer-managed) keys.

Encryption type

☒ Microsoft-managed keys

☐ Customer-managed keys

#### Data impact

If your workspace contains sensitive data, you can specify a high business impact workspace. This will control the amount of data Microsoft collects for diagnostic purposes and enables additional encryption in Microsoft managed environments.

High business impact workspace ☐

[Review + create](#) [< Previous](#) [Next : Tags](#)

- [Learn more](#)

## In Transit

- Azure Machine Learning uses TLS to secure internal communication between various AML microservices. All azure storage access also occurs over a secure channel.
- To secure external calls made to the scoring endpoint, Azure Machine Learning uses TLS.

# Policies and Governance

Recommended policies:



- Customer-managed key

- Enforce customer-managed key while creating workspaces.



- Private link/endpoint

- Enforce private endpoint to communicate between a virtual network and workspace.



- Authentication

- Disable non-Azure AD authentication such as SSH.



- Private DNS zone

- Enforce private DNS zones to use for the private link.



# Monitoring

- Set up diagnostic logging to a centralized Log Analytics workspace to **audit resource access and altering events** in the workspace.
- Use Azure Application Insights to collect the following data from an endpoint and send them to Azure Log Analytics:
  - Output data
  - Responses
  - Request rates, response times, and failure rates
  - Dependency rates, response times, and failure rates
  - Exceptions
- Set alerts on metrics, logs, and the activity log. For example; when a user creates or makes configuration changes to the virtual network.

