

# EduPortal University – Secure Azure Production Architecture

Author: Alan Naqshbandi

Role: Azure Security Engineer (Portfolio Project)

Date: February 2026

## Executive Summary

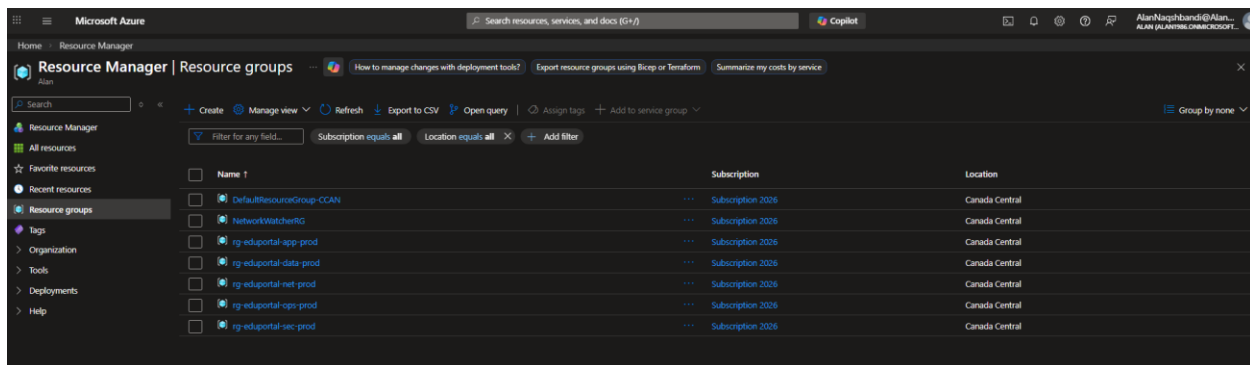
This document provides structured evidence of the secure deployment and validation of the EduPortal University Azure production architecture. It includes configuration snapshots and verification points demonstrating network segmentation, Private Endpoint implementation, identity-based access control, centralized monitoring, and production-level security controls.

## PHASE 0 – Resource Organization

### Purpose:

Ensure clean separation of workloads and enforce governance through tagging.

Resource Groups list:



The screenshot shows the Microsoft Azure portal's Resource Manager page. The 'Resource groups' section is active, displaying a table of resource groups. The table has columns for Name, Subscription, and Location. All resource groups are located in Canada Central and are associated with Subscription 2026.

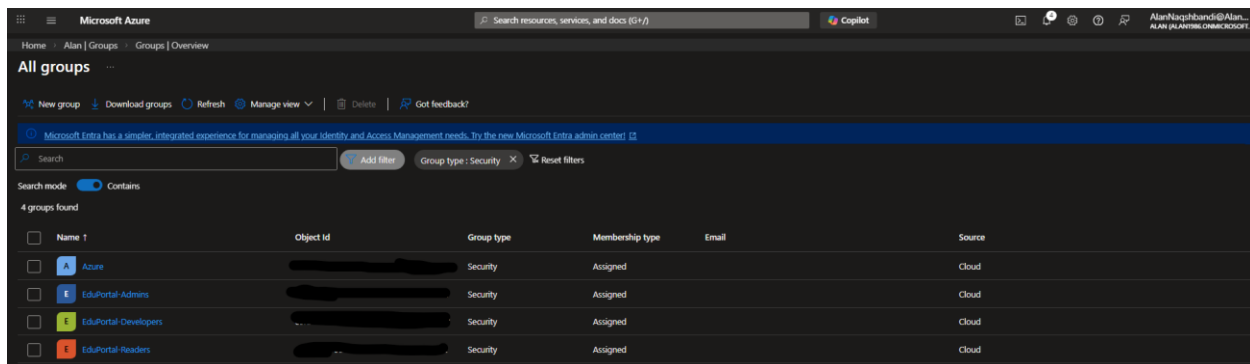
Name	Subscription	Location
DefaultResourceGroup-CCAN	Subscription 2026	Canada Central
NetworkWatcherRG	Subscription 2026	Canada Central
rg-eduportal-app-prod	Subscription 2026	Canada Central
rg-eduportal-data-prod	Subscription 2026	Canada Central
rg-eduportal-net-prod	Subscription 2026	Canada Central
rg-eduportal-ops-prod	Subscription 2026	Canada Central
rg-eduportal-sec-prod	Subscription 2026	Canada Central

## PHASE 1 – Identity & RBAC

### Purpose:

Implement group-based RBAC model enforcing least privilege and eliminating direct user assignments.

Groups:



The screenshot shows the Microsoft Azure portal's Identity page. The 'All groups' section is active, displaying a table of groups. The table has columns for Name, Object Id, Group type, Membership type, Email, and Source. All groups are of type Security and are assigned to the Cloud source.

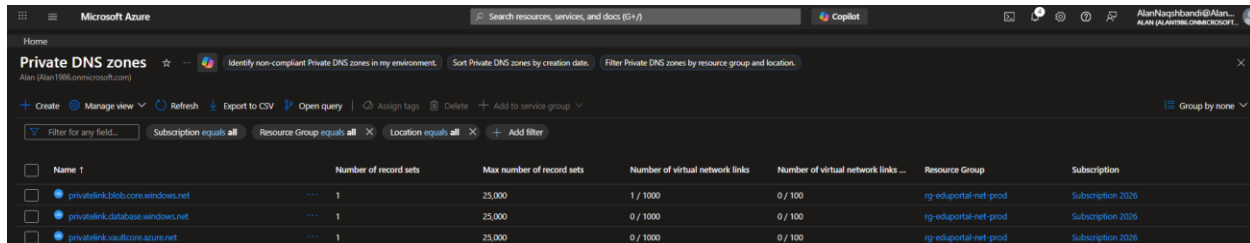
Name	Object Id	Group type	Membership type	Email	Source
Azure	[REDACTED]	Security	Assigned		Cloud
EduPortal-Admins	[REDACTED]	Security	Assigned		Cloud
EduPortal-Developers	[REDACTED]	Security	Assigned		Cloud
EduPortal-Readers	[REDACTED]	Security	Assigned		Cloud

## PHASE 2 – Networking

### Purpose:

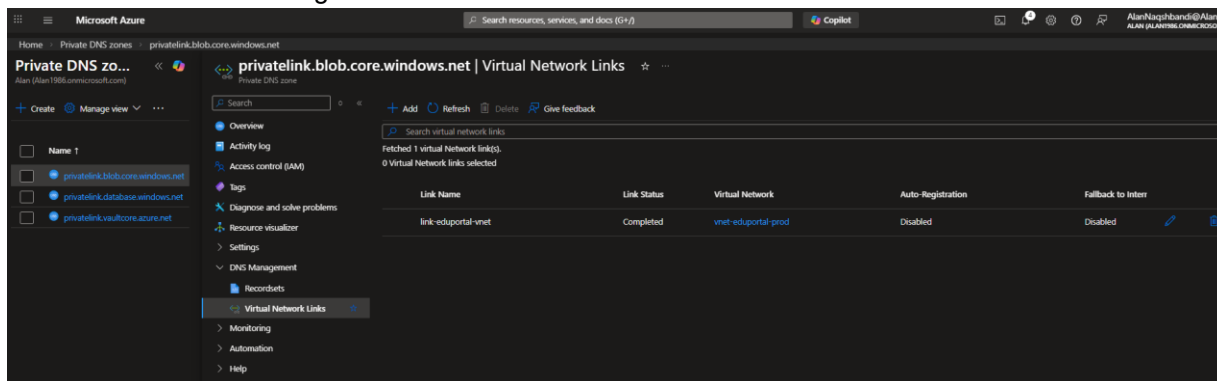
Establish network segmentation and private DNS integration to enforce private backend communication.

### Private DNS Zones



Name	Number of record sets	Max number of record sets	Number of virtual network links	Number of virtual network links...	Resource Group	Subscription
privatelink.blob.core.windows.net	1	25,000	1 / 1000	0 / 100	rg-eduportal-net-prod	Subscription 2026
privatelink.database.windows.net	1	25,000	0 / 1000	0 / 100	rg-eduportal-net-prod	Subscription 2026
privatelink.vaultcore.azure.net	1	25,000	0 / 1000	0 / 100	rg-eduportal-net-prod	Subscription 2026

### Virtual Network Link Configuration



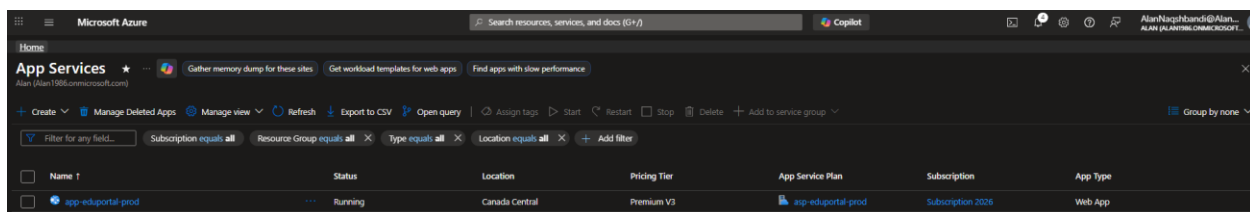
Link Name	Link Status	Virtual Network	Auto-Registration	Fallback to Internet
link-eduportal-vnet	Completed	vnet-eduportal-prod	Disabled	Disabled

## PHASE 3 – App Service

### Purpose:

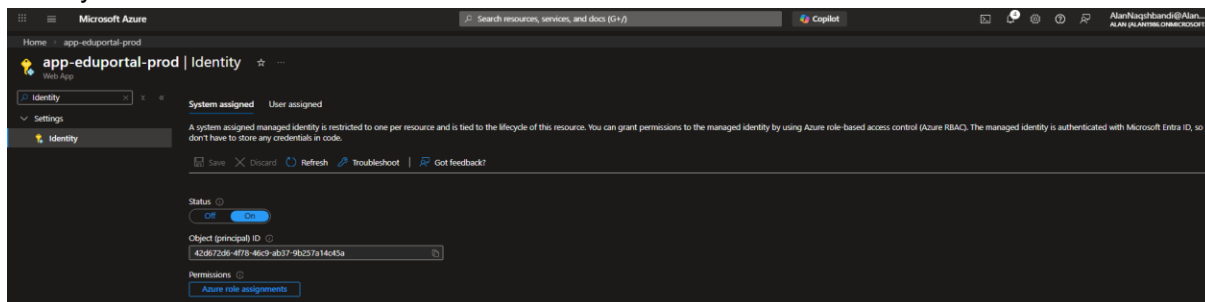
Deploy secure application layer integrated with Managed Identity and private networking.

### WebApp



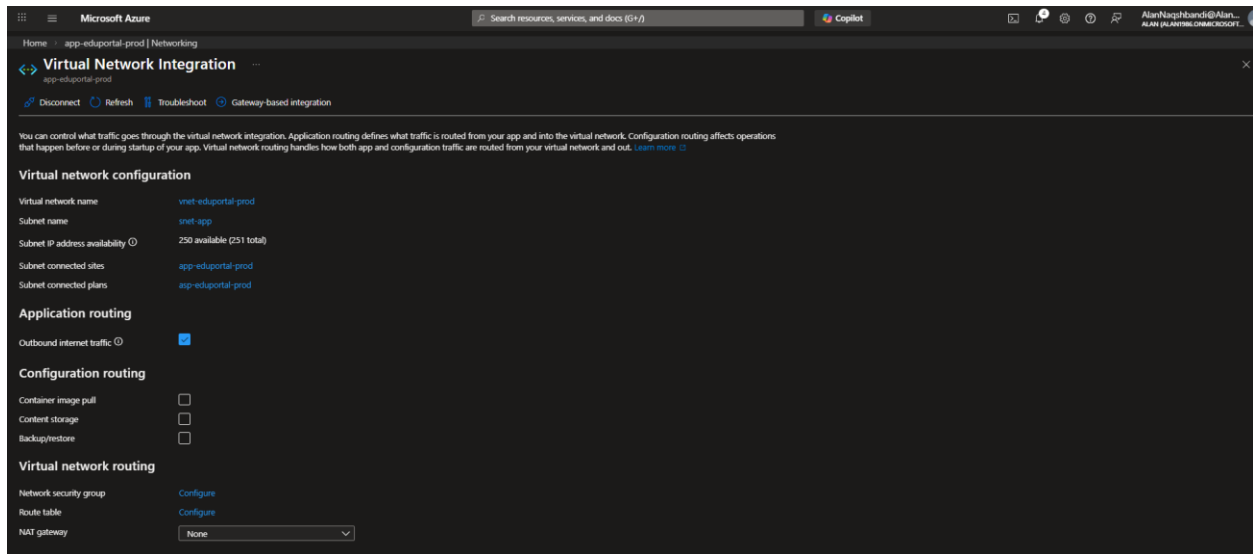
Name	Status	Location	Pricing Tier	App Service Plan	Subscription	App Type
app-eduportal-prod	Running	Canada Central	Premium V3	app-eduportal-prod	Subscription 2026	Web App

### Identity



System assigned	User assigned
<div><div><div>Identity</div><div>Settings</div><div>Identity</div></div><div><div>Save</div><div>Discard</div><div>Refresh</div><div>Troubleshoot</div><div>Got feedback?</div></div></div> <div><div>Status</div><div>On</div><div>Object (principal) ID</div><div>42087236-4778-46c9-ab37-9b237a14c43a</div><div>Permissions</div><div>Azure role assignments</div></div>	

## VNet Integration

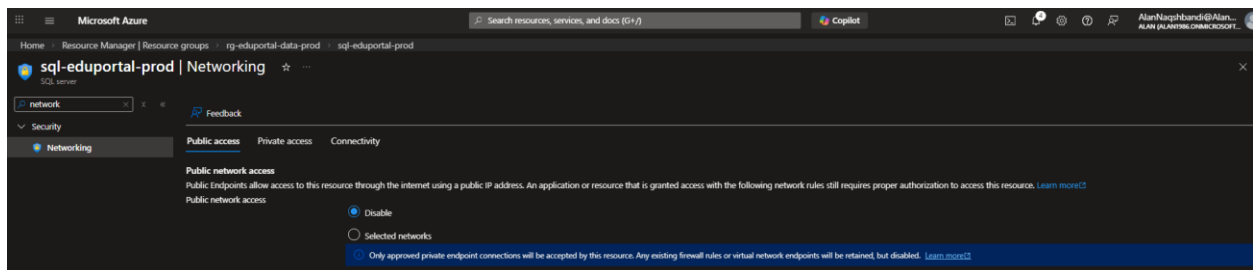


## PHASE 4 – Azure SQL

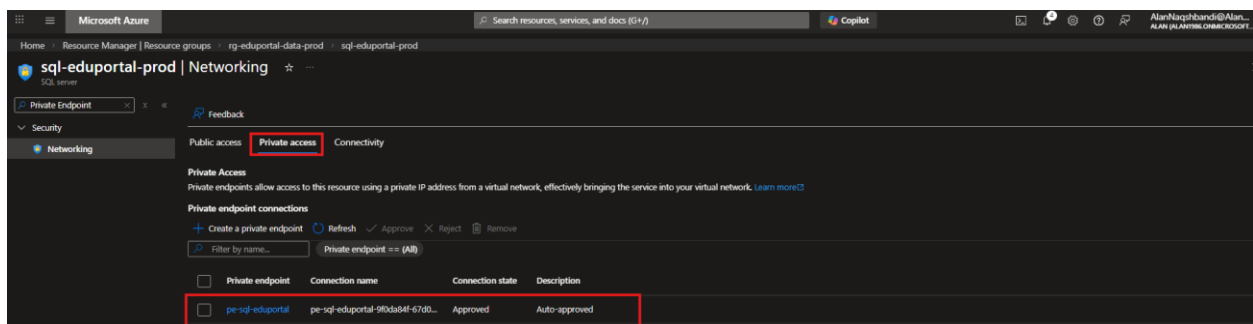
### Purpose:

Deploy database layer with zero public exposure and private endpoint connectivity.

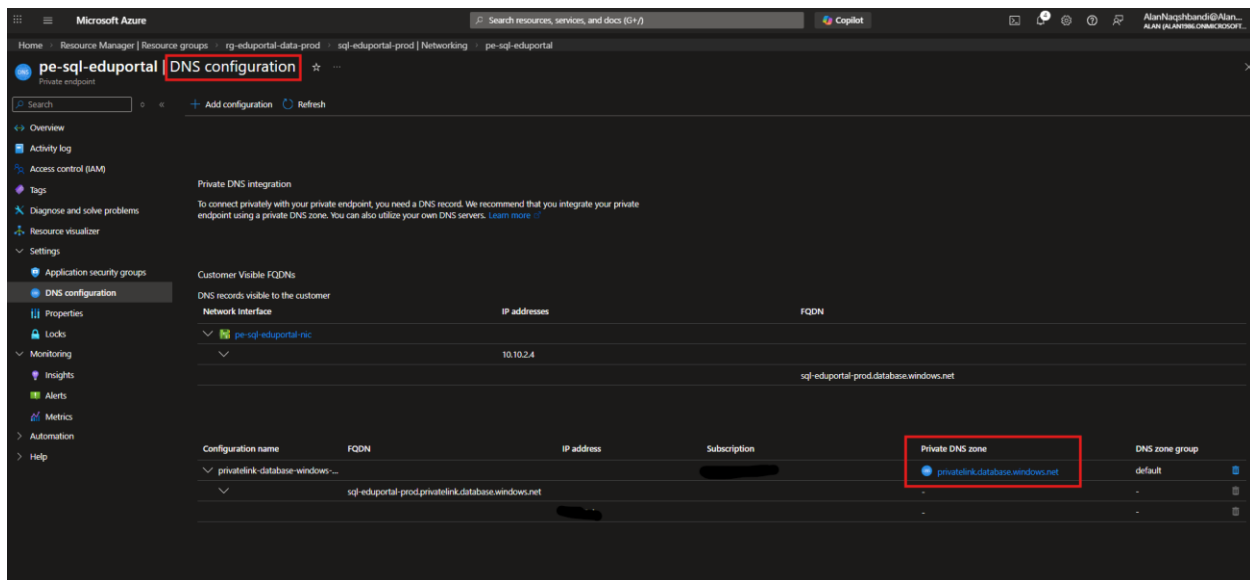
SQL Server Networking:



### Private Endpoint overview



DNS zone attached

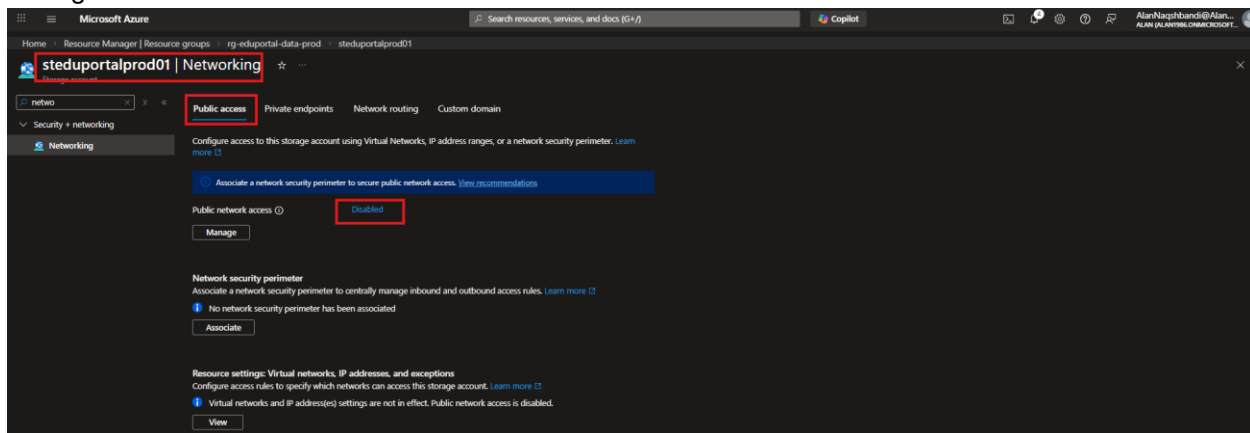


## PHASE 5 – Storage Account

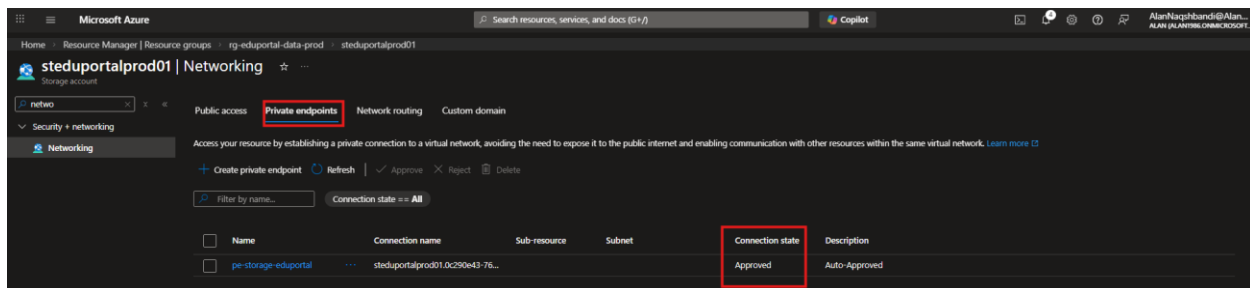
### Purpose:

Ensure secure storage configuration with private access and data protection controls.

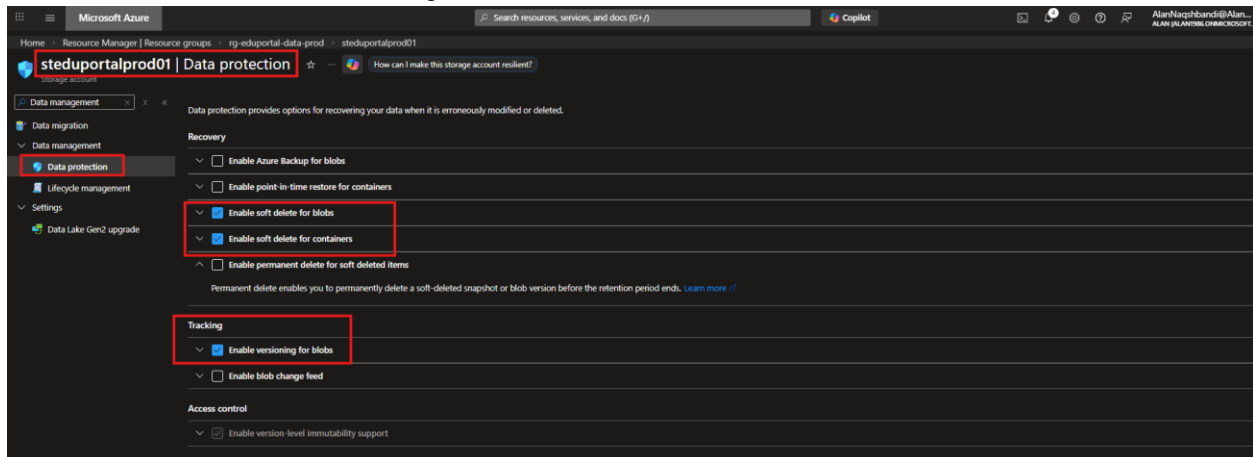
### Storage



### Private endpoint connected



## Blob Service Data Protection Settings

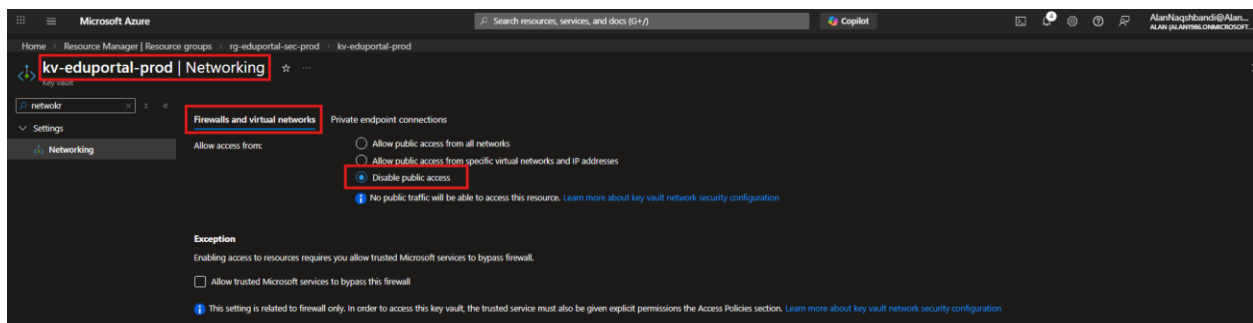


## PHASE 6 – Key Vault

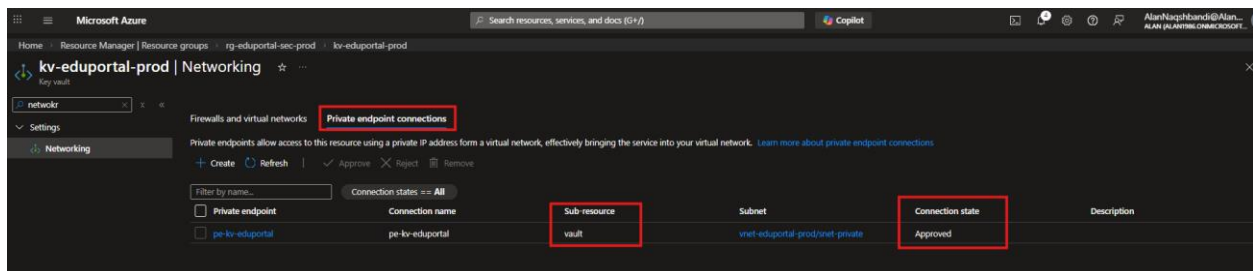
### Purpose:

Implement secure secret management using RBAC and Managed Identity authentication.

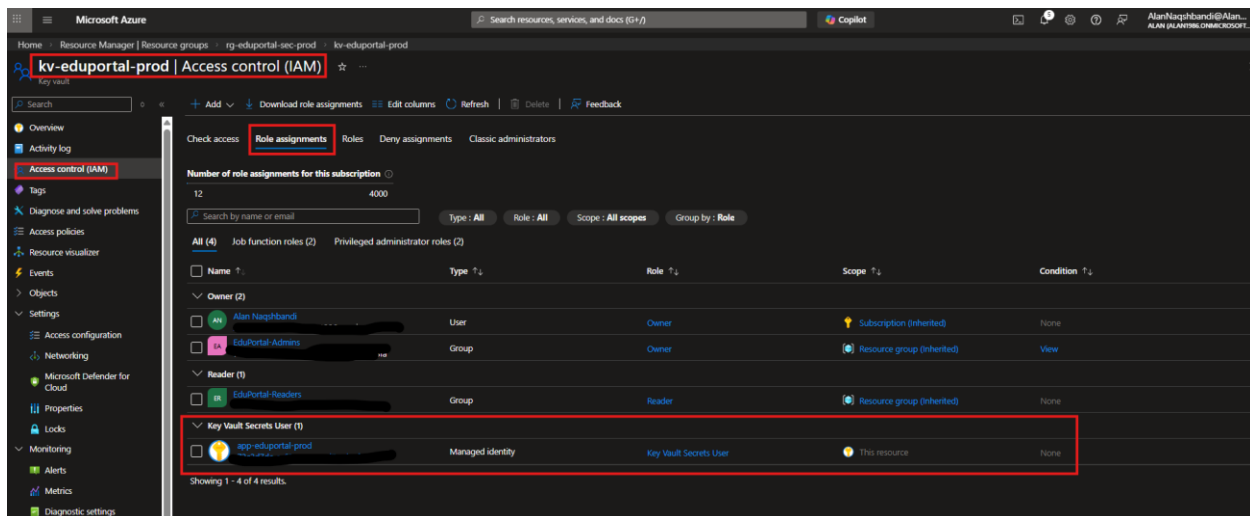
Key Vault → Networking



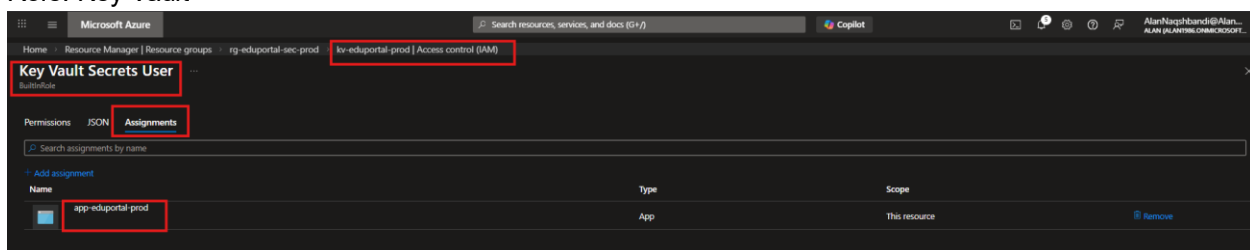
### Private endpoint



Key Vault → Access control (IAM)



## Role: Key Vault

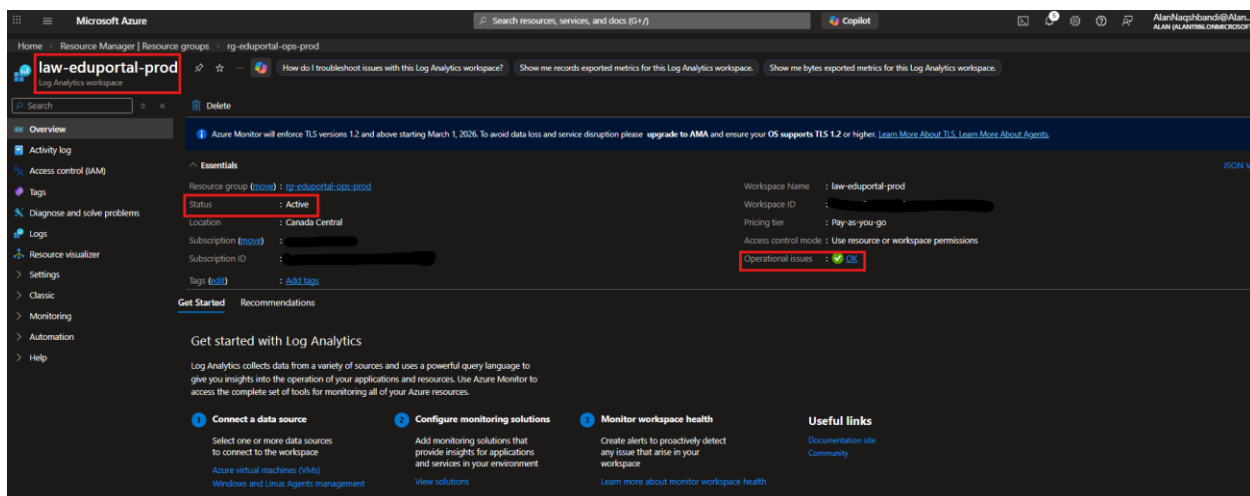


## PHASE 7 – Monitoring

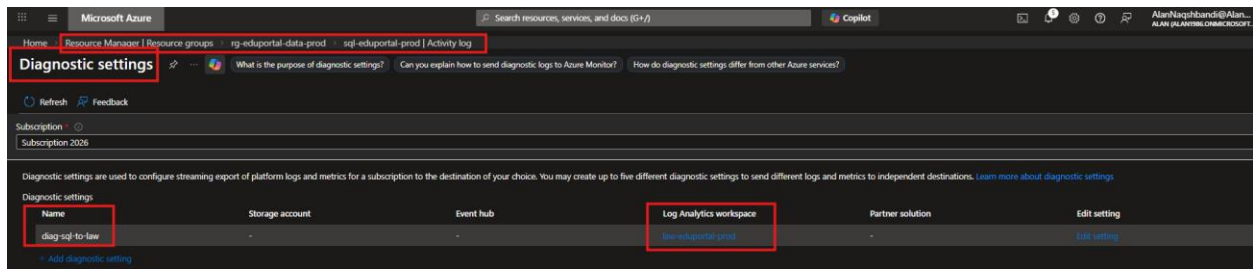
### Purpose:

Enable centralized logging and operational alerting for production visibility.

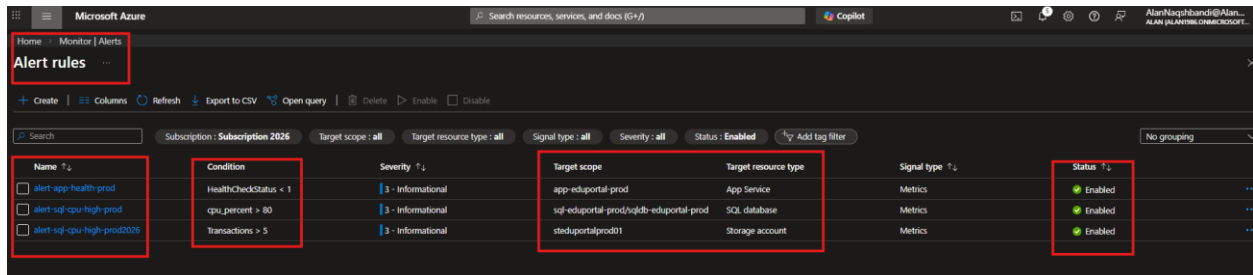
### Log Analytics Workspace overview



## Diagnostic Settings



Azure Monitor → Alert rules

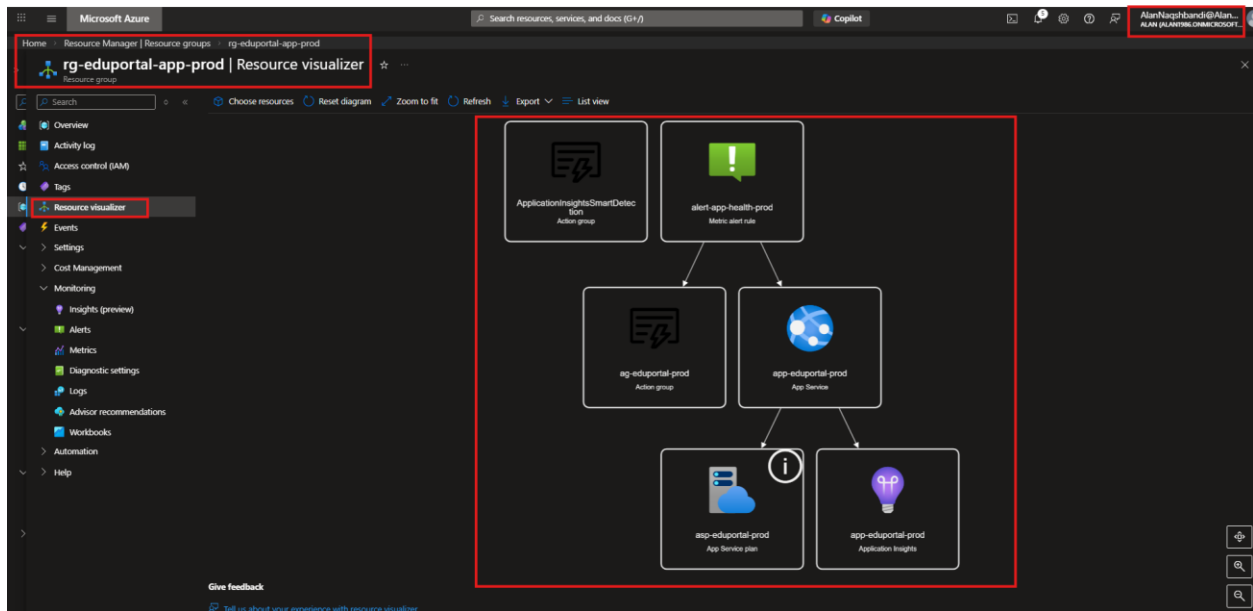


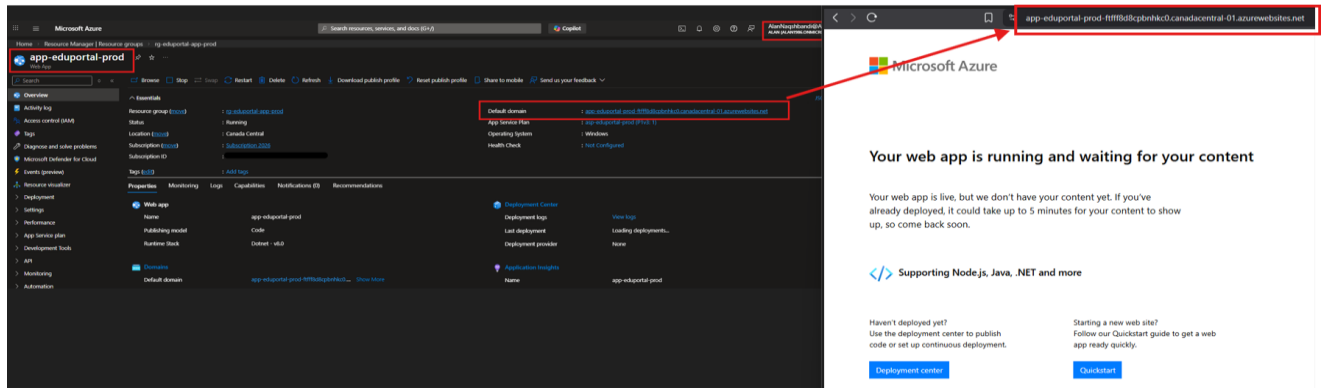
## PHASE 8 – Production Validation

### Purpose:

Validate architecture security posture and confirm enforcement of private connectivity.

Final architectural view





## Project Journey

This project demonstrates the end-to-end deployment of a secure, production-grade Azure environment. It implements structured resource organization, group-based RBAC, VNet segmentation, Private Endpoints, Managed Identity authentication, and centralized monitoring with Log Analytics and Azure Monitor. All backend services are private, access is identity-based, and operational visibility is enforced through diagnostic settings and alert rules. The architecture reflects practical Azure security engineering principles aligned with real-world production standards.