EduPortal University – Secure Azure Production Architecture
Author: Alan Naqshbandi
Role: Azure Security Engineer (Portfolio Project)
Date: February 2026

Executive Summary

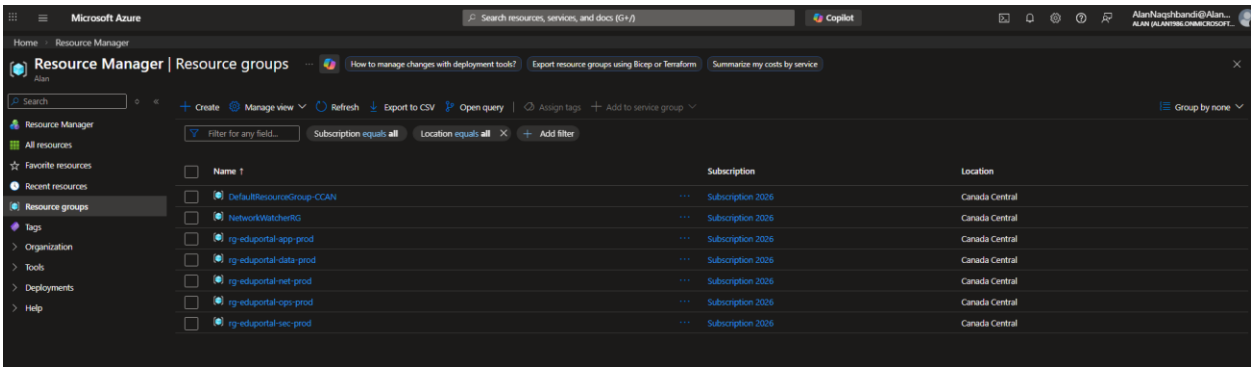
This document provides structured evidence of the secure deployment and validation of the EduPortal University Azure production architecture. It includes configuration snapshots and verification points demonstrating network segmentation, Private Endpoint implementation, identity-based access control,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

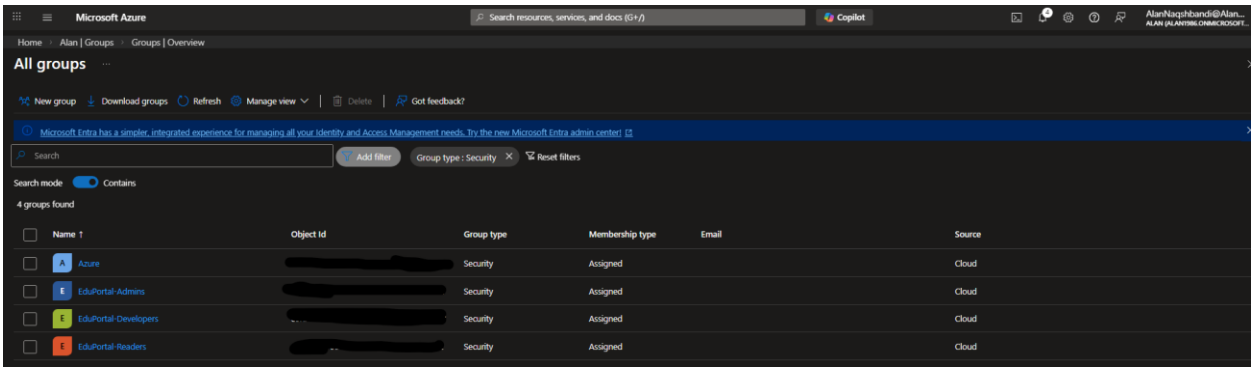


PHASE 1 – Identity & RBAC

Purpose:

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

Groups:

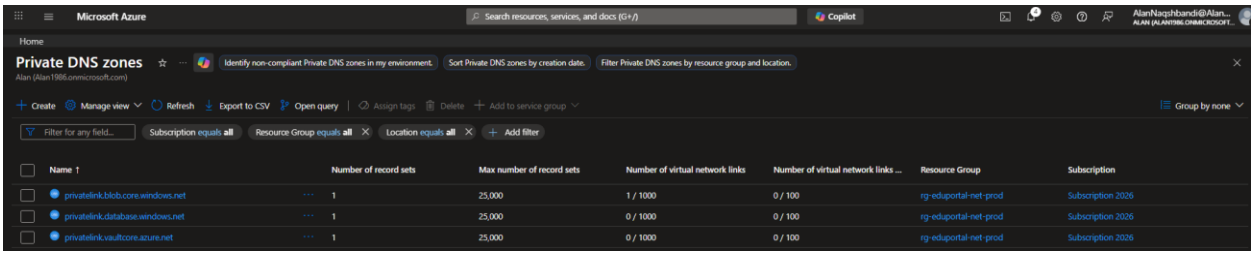


PHASE 2 – Networking

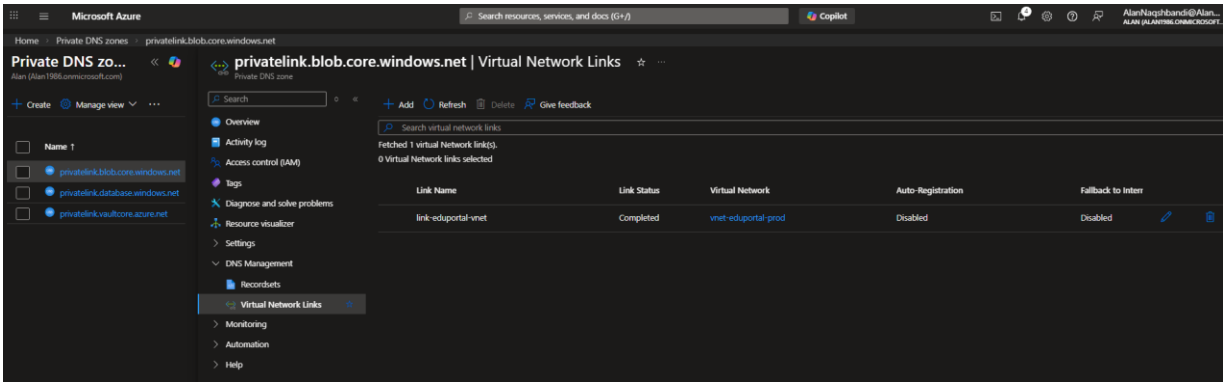
Purpose:

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

Private DNS Zones



Virtual Network Link Configuration

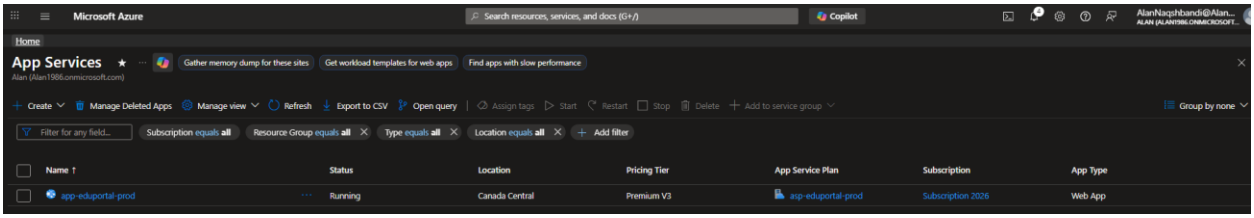


PHASE 3 – App Service

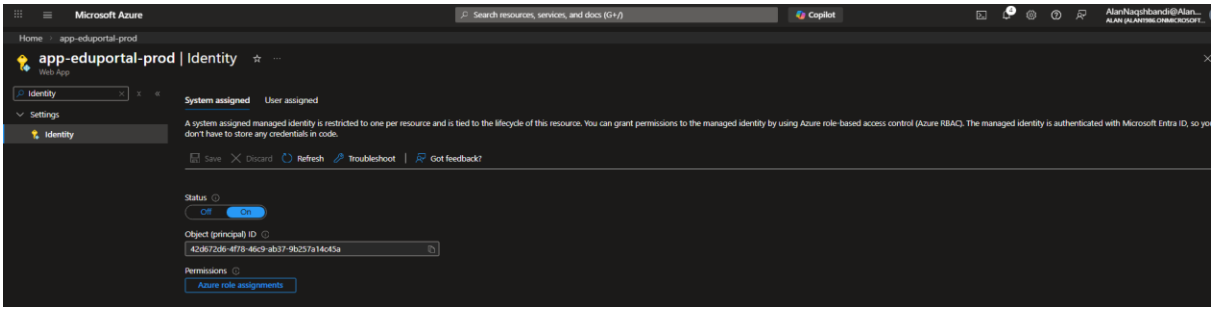
Purpose:

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

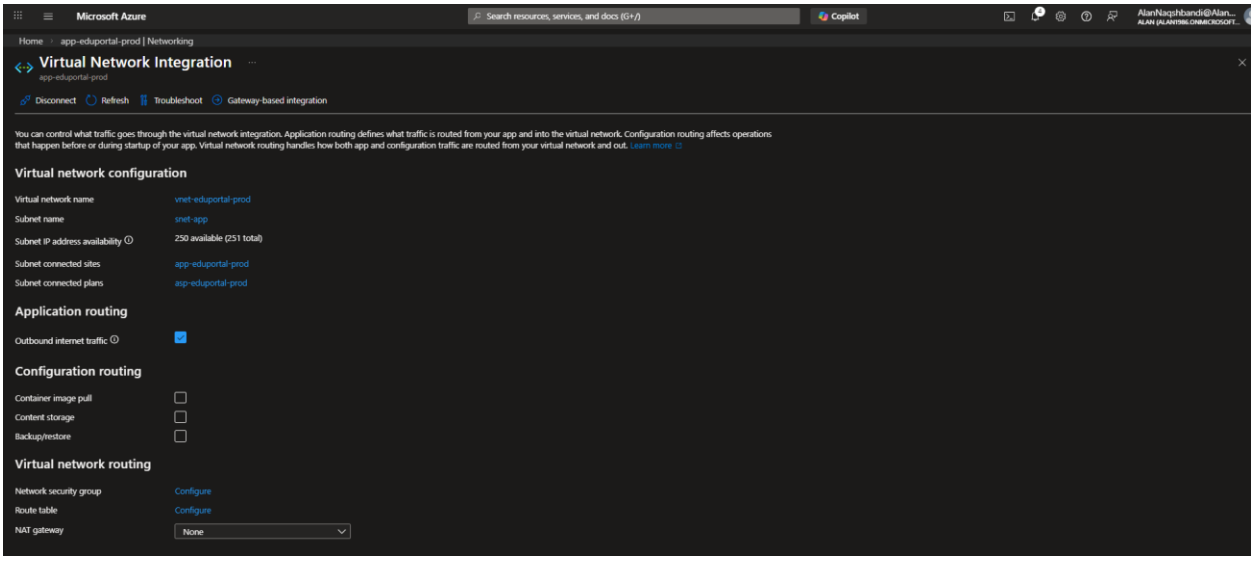
WebApp



Identity



VNet Integration

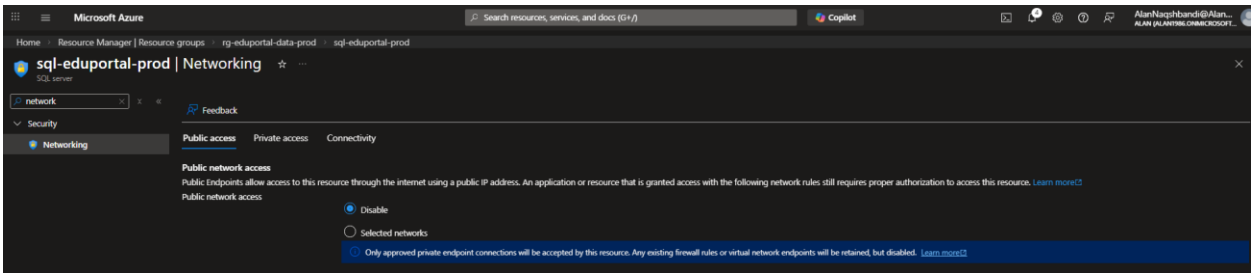


PHASE 4 – Azure SQL

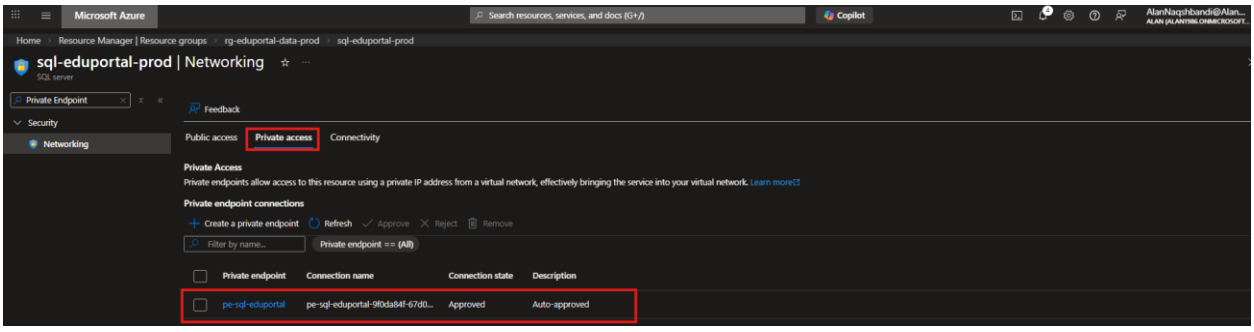
Purpose:

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

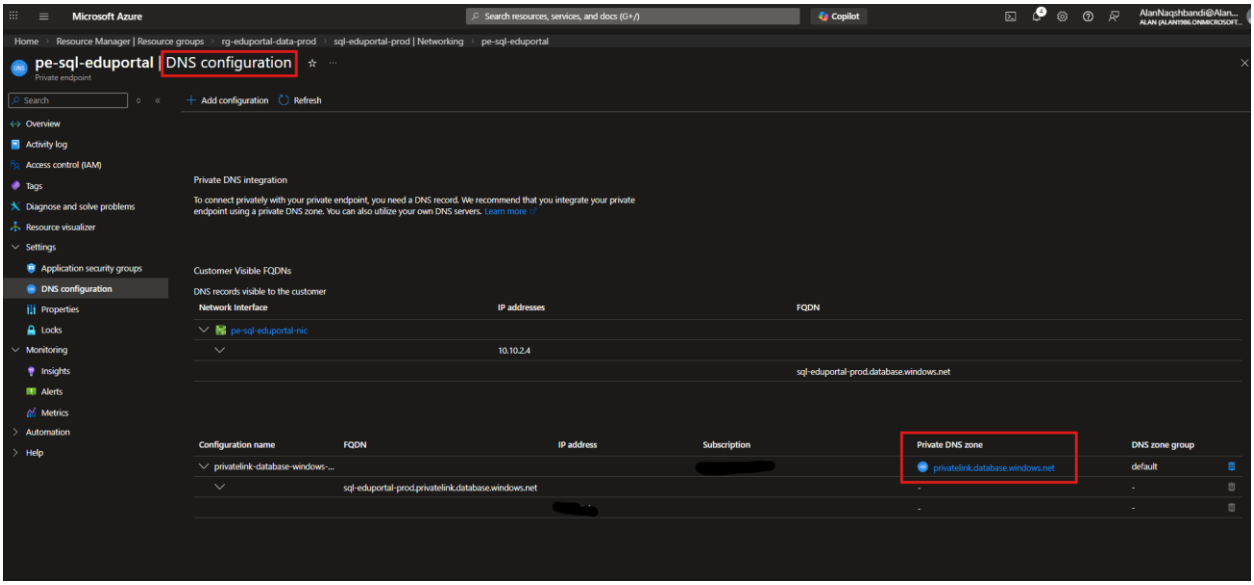
SQL Server Networking:



Private Endpoint overview



DNS zone attached

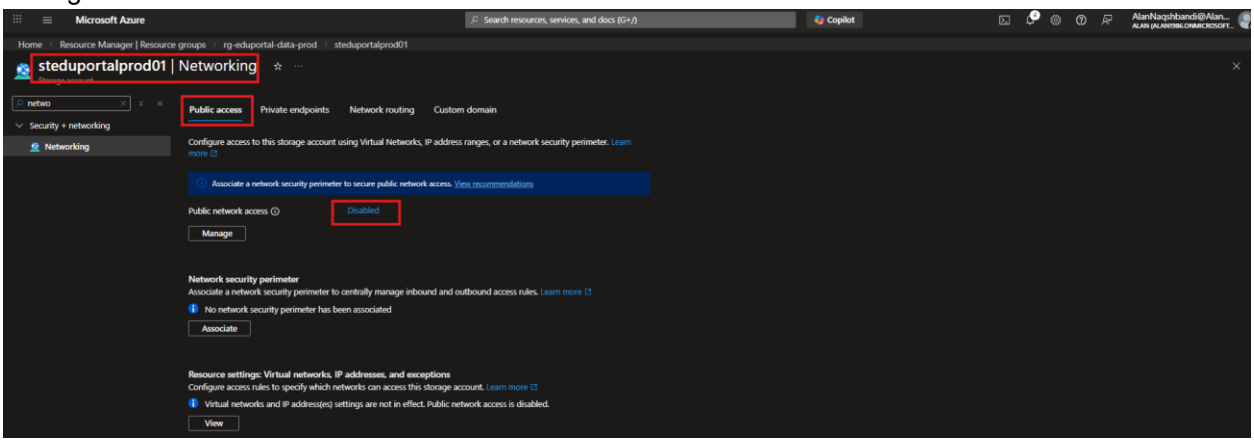


PHASE 5 – Storage Account

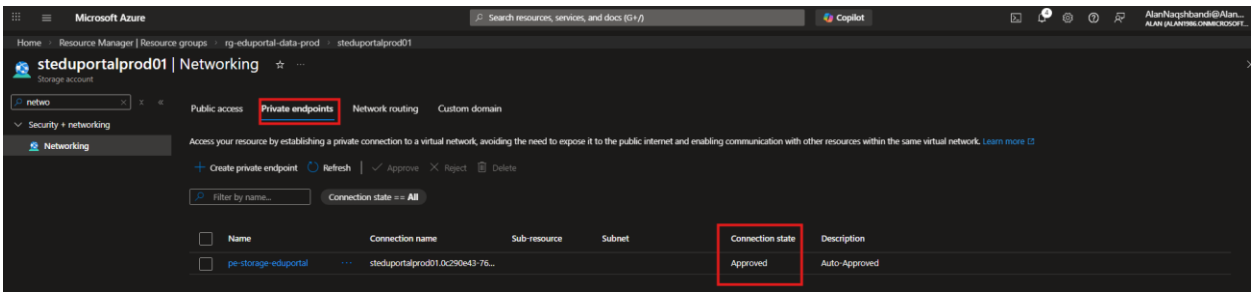
Purpose:

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

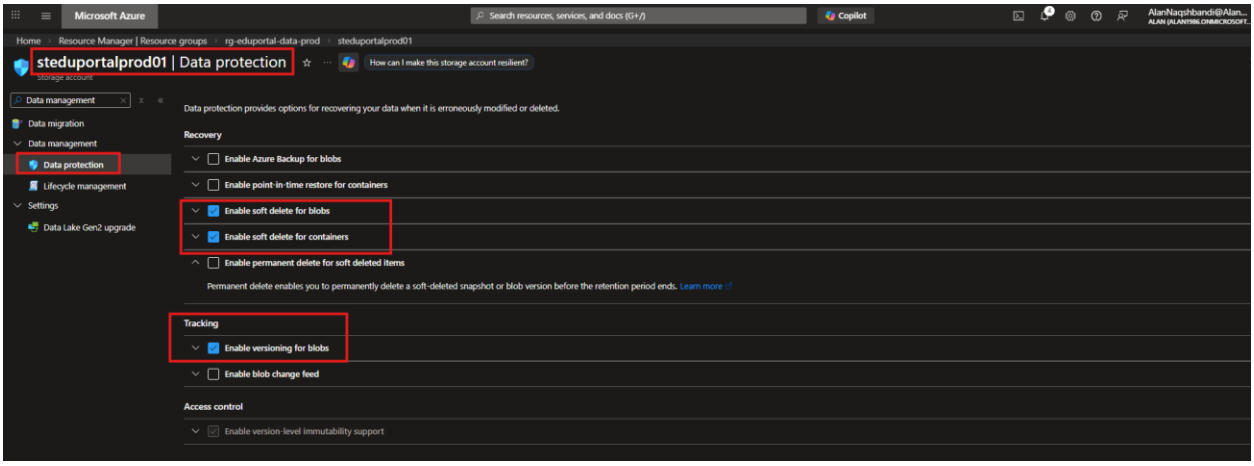
Storage



Private endpoint connected



Blob Service Data Protection Settings

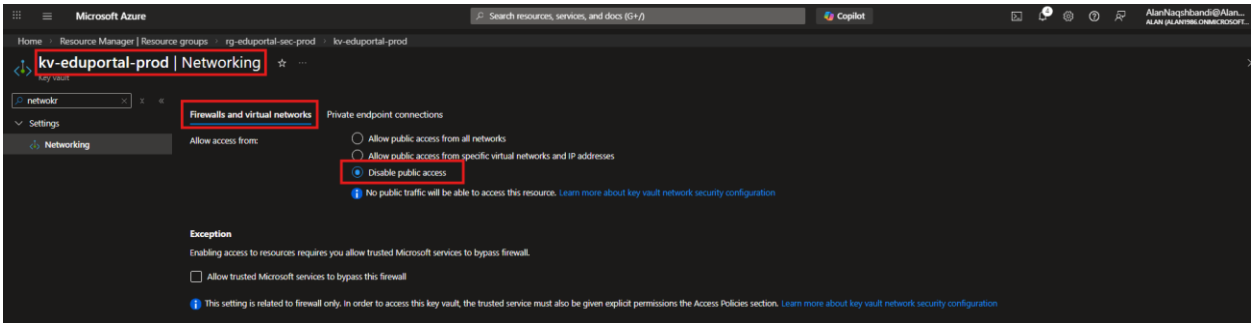


PHASE 6 – Key Vault

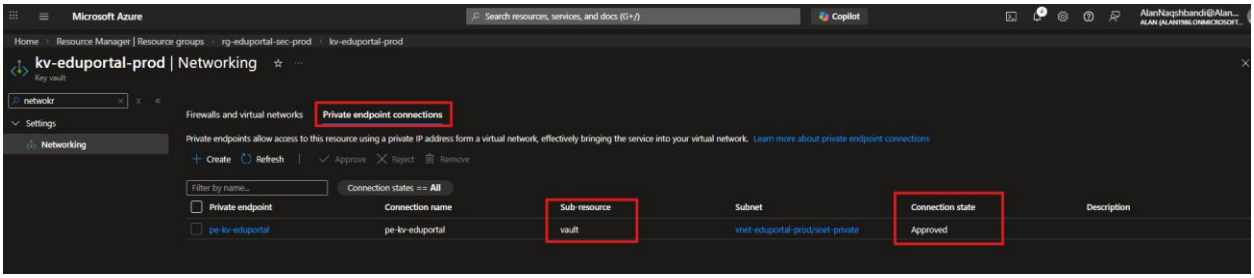
Purpose:

Implement secure secret management using RBAC and Managed Identity authentication.

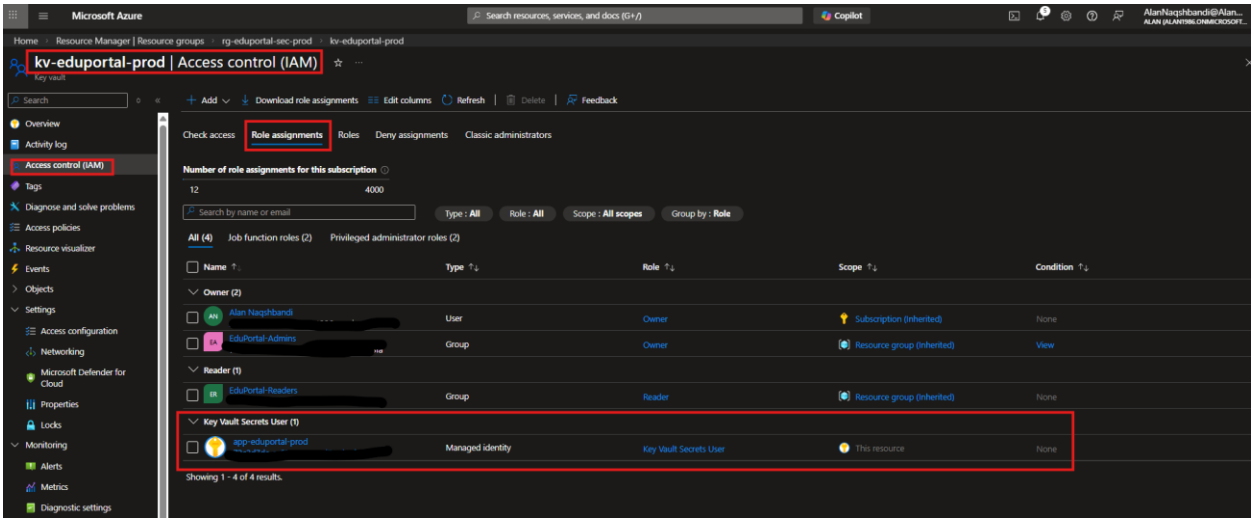
Key Vault → Networking



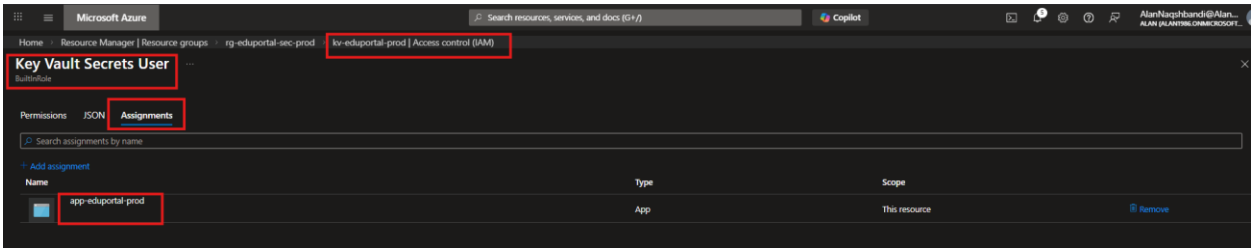
Private endpoint



Key Vault → Access control (IAM)



Role: Key Vault

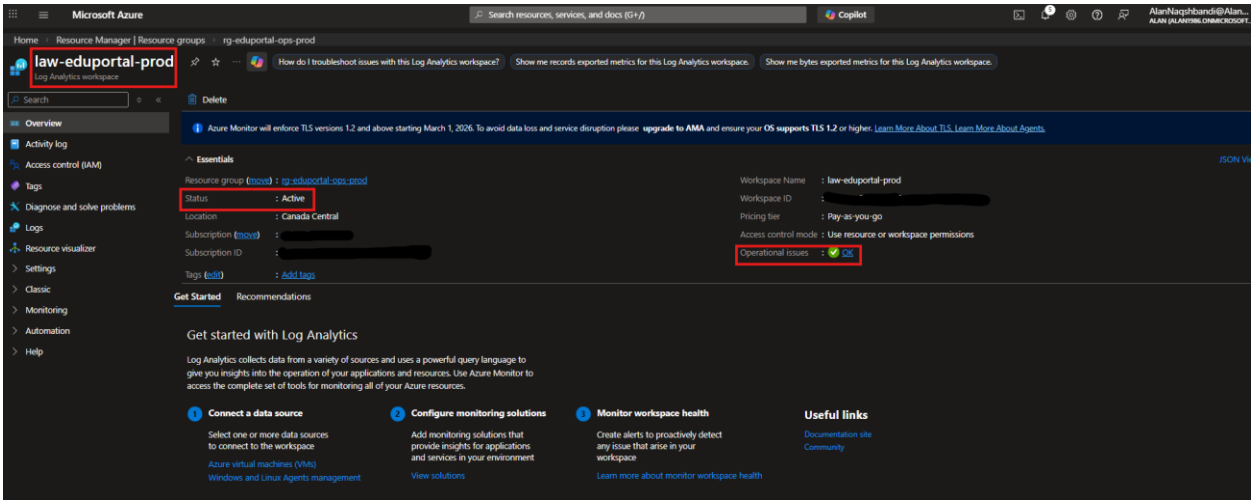


PHASE 7 – Monitoring

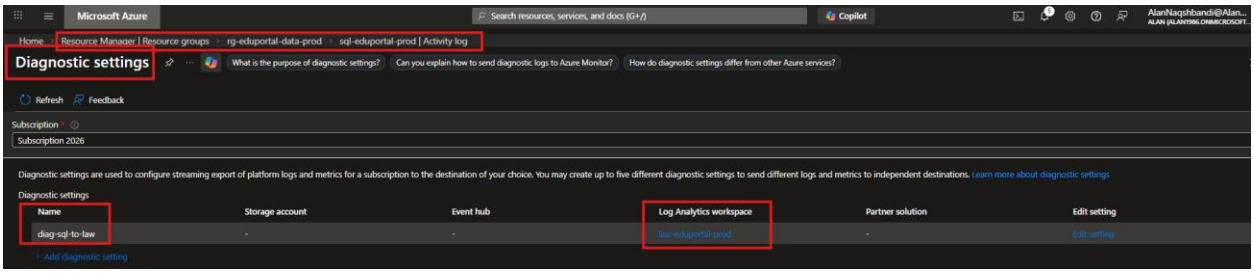
Purpose:

Enable centralized logging and operational alerting for production visibility.

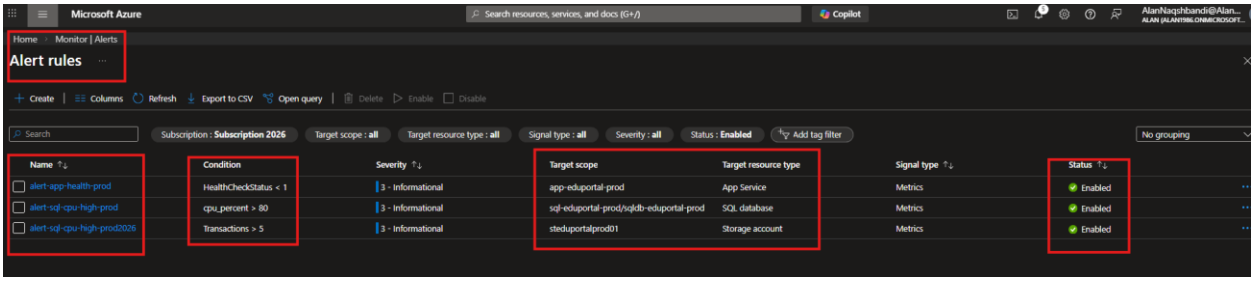
Log Analytics Workspace overview



Diagnostic Settings



Azure Monitor → Alert rules

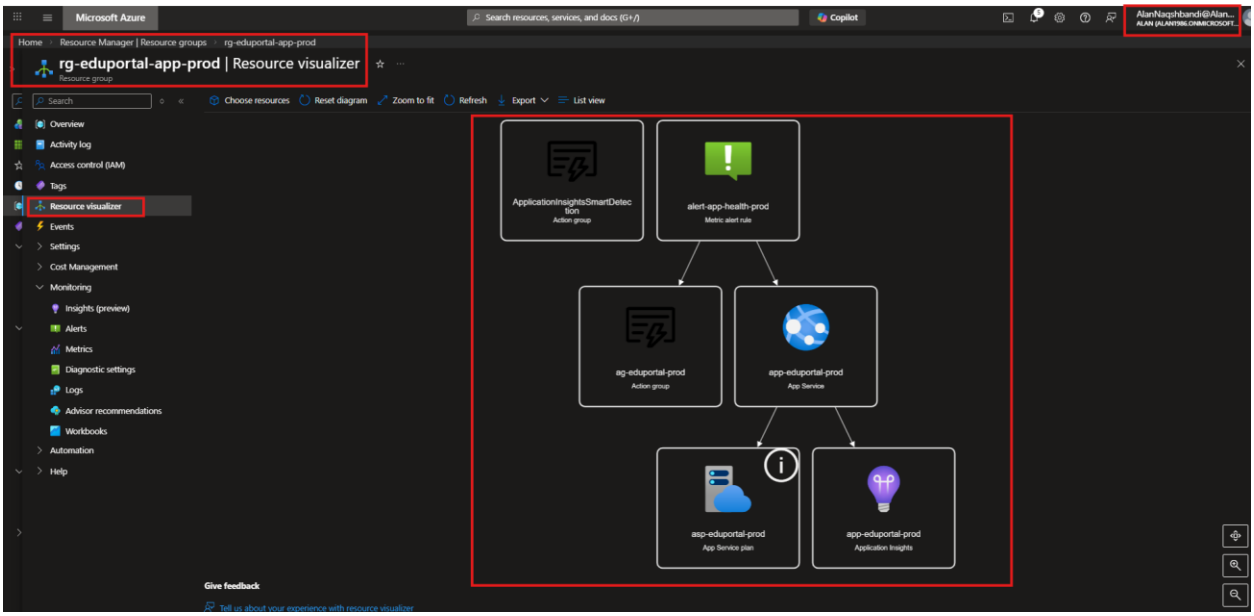


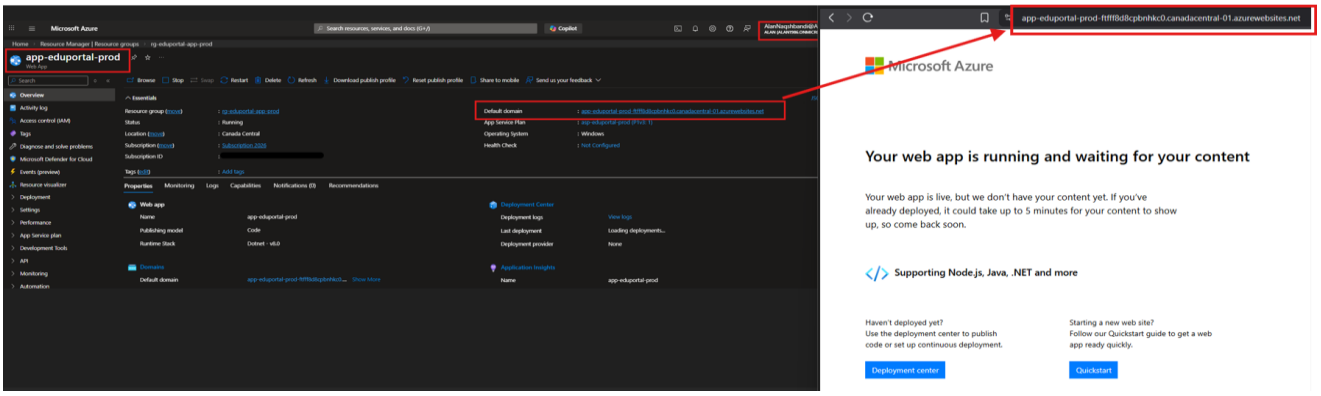
PHASE 8 – Production Validation

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.