

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 Azure Resource Manager - Resource groups page. The left sidebar has 'Resource groups' selected. The main area lists 10 resource groups under 'Subscription' (Subscription 2026) and 'Location' (Canada Central). The groups are: DefaultResourceGroup-CCAN, NetworkWatcherRG, rg-eduportal-app-prod, rg-eduportal-data-prod, rg-eduportal-net-prod, rg-eduportal-ops-prod, and rg-eduportal-sec-prod. There are also three system resource groups: 'Name 1', 'Subscription 2026', and 'Subscription 2026'.

Name	Subscription	Location
Name 1	Subscription 2026	Canada Central
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 Azure Groups - Overview page. The left sidebar has 'Groups' selected. The main area lists four groups under 'Group type: Security'. The groups are: Azure, EduPortal-Admins, EduPortal-Developers, and EduPortal-Readers. All groups have 'Source' listed as 'Cloud' and 'Membership type' as 'Assigned'.

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

The screenshot shows the Microsoft Azure Private DNS zones page. It lists four entries under the 'Name' column: 'privatelink.blob.core.windows.net', 'privatelink.database.windows.net', 'privatelink.vaultcore.azure.net', and 'privatelink.core.windows.net'. Each entry has a status of 'Active' (indicated by a blue dot) and a value of '1' under 'Number of record sets'. The 'Max number of record sets' column shows values of 25,000 for all entries. The 'Number of virtual network links' column shows values of 1/1000 for all entries. The 'Resource Group' column shows 'rg-eduportal-net-prod' for the first three and 'Subscription 2026' for the fourth. The 'Subscription' column shows 'Subscription 2026' for all entries.

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

Virtual Network Link Configuration

The screenshot shows the Microsoft Azure Private DNS zone details page for 'privatelink.blob.core.windows.net'. Under the 'Virtual Network Links' section, there is one entry: 'link-eduportal-vnet'. The 'Link Status' is 'Completed', 'Virtual Network' is 'vnet-eduportal-prod', 'Auto-registration' is 'Disabled', and 'Fallback to Internet' is 'Disabled'.

PHASE 3 – App Service

Purpose:

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

WebApp

The screenshot shows the Microsoft Azure App Services page. It lists one entry: 'app-eduportal-prod'. The 'Status' is 'Running', 'Location' is 'Canada Central', 'Pricing Tier' is 'Premium V3', 'App Service Plan' is 'asp-eduportal-prod', 'Subscription' is 'Subscription 2026', and 'App Type' is 'Web App'.

Identity

The screenshot shows the Microsoft Azure App Service identity settings page for 'app-eduportal-prod'. Under the 'Identity' tab, it shows 'System assigned' and 'User assigned' identities. A note states: 'A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. You can grant permissions to the managed identity by using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Microsoft Entra ID, so you don't have to store any credentials in code.' The 'Status' is set to 'On'. The 'Object (principal) ID' is listed as '42de7206-4f76-46c9-ab37-9b257a14c45a'. Under 'Permissions', it says 'Azure role assignments'.

VNet Integration

The screenshot shows the 'Virtual Network Integration' blade for the 'app-eduportal-prod' application. It includes sections for 'Virtual network configuration', 'Application routing', 'Configuration routing', and 'Virtual network routing'. Under 'Virtual network configuration', it lists the virtual network name as 'vnet-eduportal-prod', subnet name as 'snet-app', and subnet IP address availability as '250 available (251 total)'. Under 'Application routing', 'Outbound internet traffic' is checked. Under 'Configuration routing', 'Container image pull', 'Content storage', and 'Backup/restore' are listed with checkboxes. Under 'Virtual network routing', there are options for 'Network security group', 'Route table', and 'NAT gateway'.

PHASE 4 – Azure SQL

Purpose:

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

SQL Server Networking:

The screenshot shows the 'Networking' blade for the 'sql-eduportal-prod' SQL server. It has tabs for 'Public access', 'Private access', and 'Connectivity'. The 'Public access' tab is selected, showing the 'Public network access' section where 'Public endpoints allow access to this resource through the internet using a public IP address'. A radio button for 'Disable' is selected. Below it, a note says 'Only approved private endpoint connections will be accepted by this resource. Any existing firewall rules or virtual network endpoints will be retained, but disabled.' A 'Selected networks' option is also present.

Private Endpoint overview

The screenshot shows the 'Private Endpoint' blade for the 'sql-eduportal-prod' SQL server. It has tabs for 'Public access' (selected), 'Private access', and 'Connectivity'. The 'Private access' tab shows the 'Private endpoints' section, which allows access to the resource using a private IP address from a virtual network. It includes a 'Create a private endpoint' button and a table for managing private endpoint connections. One connection is listed: 'pe-sql-eduportal' with connection name 'pe-sql-eduportal-9f0da84f-67d0...', state 'Approved', and description 'Auto-approved'. This row is highlighted with a red border.

DNS zone attached

pe-sql-eduportal | DNS configuration

Customer Visible FQDNs

Network Interface	IP addresses	FQDN
pe-sql-eduportal-nic	10.10.2.4	sql-eduportal-prod.database.windows.net

Configuration name FQDN IP address Subscription Private DNS zone DNS zone group

privatelink-database-windows...	sql-eduportal-prod.privatelink.database.windows.net	[REDACTED]	privatelink-database.windows.net	default
---------------------------------	---	------------	----------------------------------	---------

PHASE 5 – Storage Account

Purpose:

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

Storage

steduportalprod01 | Networking

Public access

Associate a network security perimeter to secure public network access. [View recommendations](#)

Public network access: Disabled

Manage

Network security perimeter

Associate a network security perimeter to centrally manage inbound and outbound access rules. [Learn more](#)

No network security perimeter has been associated

Associate

Resource settings: Virtual networks, IP addresses, and exceptions

Configure access rules to specify which networks can access this storage account. [Learn more](#)

Virtual networks and IP address(es) settings are not in effect. Public network access is disabled.

View

Private endpoint connected

steduportalprod01 | Networking

Storage account

Private endpoints

Create private endpoint Refresh Approve Reject Delete

Filter by name... Connection state == All

Name	Connection name	Sub-resource	Subnet	Connection state	Description
pe-storage-eduportal	steduportalprod01.0c290e43-76...			Approved	Auto-Approved

Blob Service Data Protection Settings

The screenshot shows the 'Data protection' section of the Blob Service Data Protection Settings. It includes options for 'Enable Azure Backup for blobs', 'Enable point in time restore for containers', 'Enable soft delete for blobs' (which is checked), 'Enable soft delete for containers' (which is checked), and 'Enable permanent delete for soft deleted items'. Below this, a note states: 'Permanent delete enables you to permanently delete a soft-deleted snapshot or blob version before the retention period ends.' Under the 'Tracking' section, 'Enable versioning for blobs' is checked. The 'Access control' section has 'Enable version-level immutability support' checked.

PHASE 6 – Key Vault

Purpose:

Implement secure secret management using RBAC and Managed Identity authentication.

Key Vault → Networking

The screenshot shows the 'Networking' settings for the Key Vault 'kv-eduportal-prod'. In the 'Firewalls and virtual networks' tab, the 'Allow access from:' section has 'Disable public access' selected (radio button highlighted). A note below states: 'No public traffic will be able to access this resource.'

Private endpoint

The screenshot shows the 'Networking' settings for the Key Vault 'kv-eduportal-prod'. In the 'Private endpoint connections' tab, it lists a connection named 'pe-kv-eduportal' with a 'Sub-resource' of 'vault' and a 'Connection state' of 'Approved' (highlighted with a red box).

Key Vault → Access control (IAM)

Microsoft Azure

Home > Resource Manager | Resource groups > rg-eduportal-sec-prod > kv-eduportal-prod

kv-eduportal-prod | Access control (IAM)

Key vault

Search: Add Download role assignments Edit columns Refresh Delete Feedback

Check access Role assignments Roles Deny assignments Classic administrators

Number of role assignments for this subscription: 12 / 4000

All (4) Job function roles (2) Privileged administrator roles (2)

Name	Type	Role	Scope	Condition
Owner (2)	User	Owner	Subscription (Inherited)	None
AN [Alan Naspibandi]	User	Owner	Resource group (Inherited)	View
EduPortal-Admins	Group	Owner	Resource group (Inherited)	View
Reader (1)	Group	Reader	Resource group (Inherited)	None
EduPortal-Readers	Group	Reader	This resource	None
Key Vault Secrets User (1)	Managed identity	Key Vault Secrets User	This resource	None
app-eduportal-prod	Managed identity	Key Vault Secrets User	This resource	None

Showing 1 - 4 of 4 results.

Role: Key Vault

Microsoft Azure

Home > Resource Manager | Resource groups > rg-eduportal-sec-prod > kv-eduportal-prod | Access control (IAM)

Key Vault Secrets User

Permissions JSON Assignments

+ Add assignment

Name	Type	Scope
app-eduportal-prod	App	This resource

Remove

PHASE 7 – Monitoring

Purpose:

Enable centralized logging and operational alerting for production visibility.

Log Analytics Workspace overview

Microsoft Azure

Home > Resource Manager | Resource groups > rg-eduportal-ops-prod > law-eduportal-prod | Log Analytics workspace

law-eduportal-prod

How do I troubleshoot issues with this Log Analytics workspace? Show me records exported metrics for this Log Analytics workspace. Show me bytes exported metrics for this Log Analytics workspace.

Search: Delete

Azure Monitor will enforce TLS versions 1.2 and above starting March 1, 2026. To avoid data loss and service disruption please upgrade to AMA and ensure your OS supports TLS 1.2 or higher. Learn More About TLS. Learn More About Agents.

Essentials

Resource group (Inherited): rg-eduportal-ops-prod	Workspace Name: law-eduportal-prod
Status: Active	Workspace ID: [REDACTED]
Location: Canada Central	Pricing tier: Pay-as-you-go
Subscription (Inherited): [REDACTED]	Access control mode: Use resource or workspace permissions
Subscription ID: [REDACTED]	Operational issues: Ok
Tags (edit): Add tags	

Get Started Recommendations

Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

1 Connect a data source
Select one or more data sources to connect to the workspace
Azure virtual machines (VMs)
Windows and Linux Agents management

2 Configure monitoring solutions
Add monitoring solutions that provide insights for applications and services in your environment
View solutions

3 Monitor workspace health
Create alerts to proactively detect any issue that arise in your workspace
Learn more about monitor workspace health

Useful links
Documentation site
Community

Diagnostic Settings

The screenshot shows the Microsoft Azure Diagnostic settings page. A diagnostic setting named "diag-sql-to-law" is selected. It is configured to send logs to a Log Analytics workspace named "st-eduportal-prod". Other options like Storage account and Event hub are listed but not selected.

Azure Monitor → Alert rules

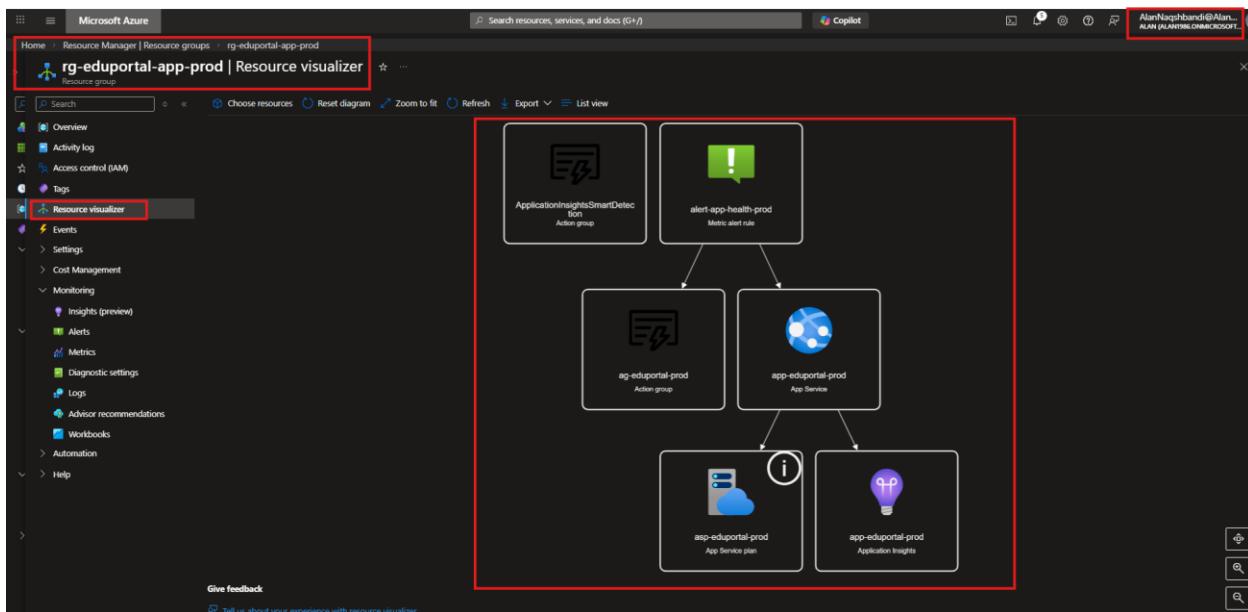
The screenshot shows the Microsoft Azure Alert rules page. Three alert rules are listed: "alert-app-health-prod", "alert-sql-cpu-high-prod", and "alert-sql-cpu-high-prod2026". Each rule has a condition section (e.g., HealthCheckStatus < 1, cpu_percent > 80, Transactions > 5) and a target scope section (e.g., app-eduportal-prod, sql-eduportal-prod/sqldb-eduportal-prod, st-eduportalprod01). The status column indicates that all three rules are enabled.

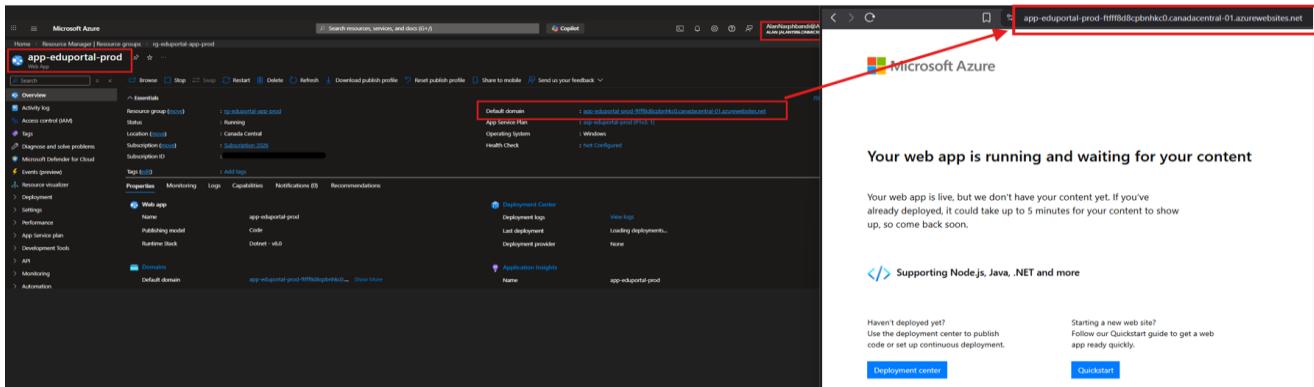
PHASE 8 – Production Validation

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.