Microsoft Azure

Implementing Virtual Networking

AZ-104 Microsoft Azure Administrator — Lab 04

Nicolas Portilla Gomez
2-9-2026

Table of Contents

EXECUTIVE SUMMARY

This lab evaluated how virtual networking components are designed, deployed, and managed within Microsoft Azure to support secure and scalable cloud communication. The objective was to demonstrate how Azure Virtual Networks (VNets), subnets, network security groups (NSGs), and routing configurations enable controlled network segmentation, secure traffic flow, and connectivity between Azure resources.

During the lab, Azure virtual networking resources were created and configured to establish network boundaries and enforce traffic control policies. VNets and subnets were provisioned to segment resources logically, while network security groups were applied to regulate inbound and outbound traffic based on defined security rules. Additional configurations validated network connectivity and demonstrated how Azure networking constructs support isolation, security enforcement, and efficient resource communication. This approach illustrates how Azure virtual networking provides a foundational layer for secure cloud architecture and supports scalable, policy-driven network management.

Key Outcomes

- Azure Virtual Networks enable logical isolation and structured network design for cloud resources.
- Subnetting improves network organization and supports layered security architectures.
- Network Security Groups enforce traffic control through rule-based filtering at the subnet and resource level.
- Proper virtual network configuration strengthens security posture and supports scalable, enterprise-grade cloud networking.

METHODOLOGY

1. Review Azure virtual networking concepts, including virtual networks (VNets), subnets, and network security groups (NSGs), to understand their role in securing and organizing cloud network infrastructure.
2. Examine the structure and configuration of Azure virtual networks and subnets to understand how network segmentation and address space planning are implemented within Azure.
3. Deploy and configure Azure virtual networking resources to establish logical network boundaries and enable controlled communication between cloud resources.
4. Apply network security groups to subnets and resources to enforce inbound and outbound traffic rules based on defined security requirements.
5. Validate network configuration and connectivity through the Azure portal to confirm correct resource deployment, traffic flow behavior, and enforcement of network security rules.

SYSTEMS IN SCOPE

System	Type	Purpose
Azure Subscription	Cloud Control Plane	Provides the administrative scope for deploying and managing Azure virtual networking resources and enforcing subscription-level policies.
Resource Group	Logical Container	Hosts virtual networking resources deployed during the lab and defines management and lifecycle boundaries.
Virtual Network (VNet)	Network Infrastructure	Provides logical network isolation and enables secure communication between Azure resources.
Subnet	Network Segmentation	Divides the virtual network into smaller address spaces to support organization, security, and traffic control.

System	Type	Purpose
Network Security Group (NSG)	Security Control	Enforces inbound and outbound traffic rules to regulate network access at the subnet or resource level.
Azure Virtual Machines	Compute Resource	Acts as network endpoints used to validate connectivity and security rule enforcement within the virtual network.

TECHNICAL FINDINGS

Finding 1: Secure Network Traffic Control Was Implemented Using NSGs and ASGs

Description:

Network traffic control was implemented using a combination of Network Security Groups (NSGs) and an Application Security Group (ASG). The ASG logically grouped web-facing resources, while the NSG enforced inbound and outbound traffic filtering at the subnet level. A custom inbound rule allowed only HTTP and HTTPS traffic from the ASG, and a custom outbound rule denied all internet-bound traffic. Default NSG rules were retained for internal virtual network communication.

Evidence:

Figure 1 - Figure 6

Impact:

This configuration enforces least-privilege network access, reduces attack surface, and strengthens network security through centralized, role-based traffic control.

Finding 2: Virtual Networks and Subnets Were Deployed Using Infrastructure-as-Code

Description:

Virtual networks were deployed using Azure Resource Manager (ARM) templates to ensure consistent and repeatable infrastructure provisioning. The templates defined address spaces, subnet configurations, and locations declaratively. Existing virtual networks

were exported as ARM templates, parameterized, and reused to support standardized deployments across environments.

Evidence:
Figure 7 - Figure 9

Impact:
Infrastructure-as-code improves deployment consistency, minimizes configuration errors, and supports scalable cloud operations.

Finding 3: Network Segmentation Was Successfully Implemented

Description:
Virtual networks were configured with defined address spaces and multiple subnets to separate workloads such as shared services and databases. Subnet segmentation enabled logical isolation and supported layered security design within the network architecture.

Evidence:
Figure 10

Impact:
Subnet segmentation improves network organization, supports defense-in-depth strategies, and simplifies traffic management.

Finding 4: Private DNS Resolution Was Configured and Linked to Virtual Networks

Description:
A private DNS zone (*private.contoso2.com*) was created to support internal name resolution. Custom A records were added, and the zone

was linked to the Manufacturing virtual network. Auto-registration was disabled to maintain controlled DNS record management.

Evidence:
Figure 1, Figure 11

Impact:
Private DNS zones enable secure internal name resolution without exposing internal records to the public internet.

Finding 5: Public DNS Resolution Was Configured and Validated

Description:
A public DNS zone (*contoso2.com*) was configured to support external name resolution. DNS resolution was validated using the nslookup utility, confirming that public DNS records resolved to the expected IP address through Azure DNS.

Evidence:
Figure 2

Impact:
Public DNS configuration enables reliable external access to Azure-hosted services and confirms correct DNS publishing.

Finding 6: Separation of Public and Private DNS Was Maintained

Description:
The environment maintained a clear separation between private DNS zones for internal resolution and public DNS zones for external access.

This design prevents internal DNS records from being exposed publicly while still supporting external name resolution.

Evidence:
Figure 1, Figure 2, Figure 11

Impact:
Separating DNS scopes supports security best practices and reduces the risk of unintended information disclosure.

SCREENSHOTS & EVIDENCE

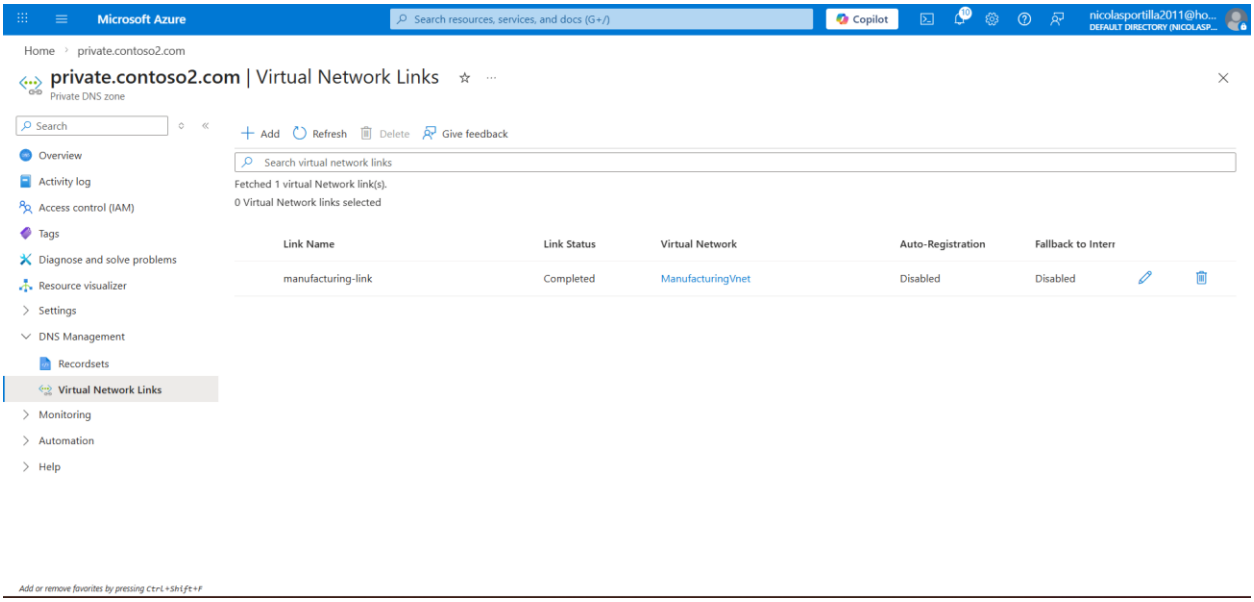

Figure 1: Private DNS zone private.contoso2.com linked to ManufacturingVnet with link status Completed and Auto-registration Disabled, enabling controlled private DNS resolution within the VNet.

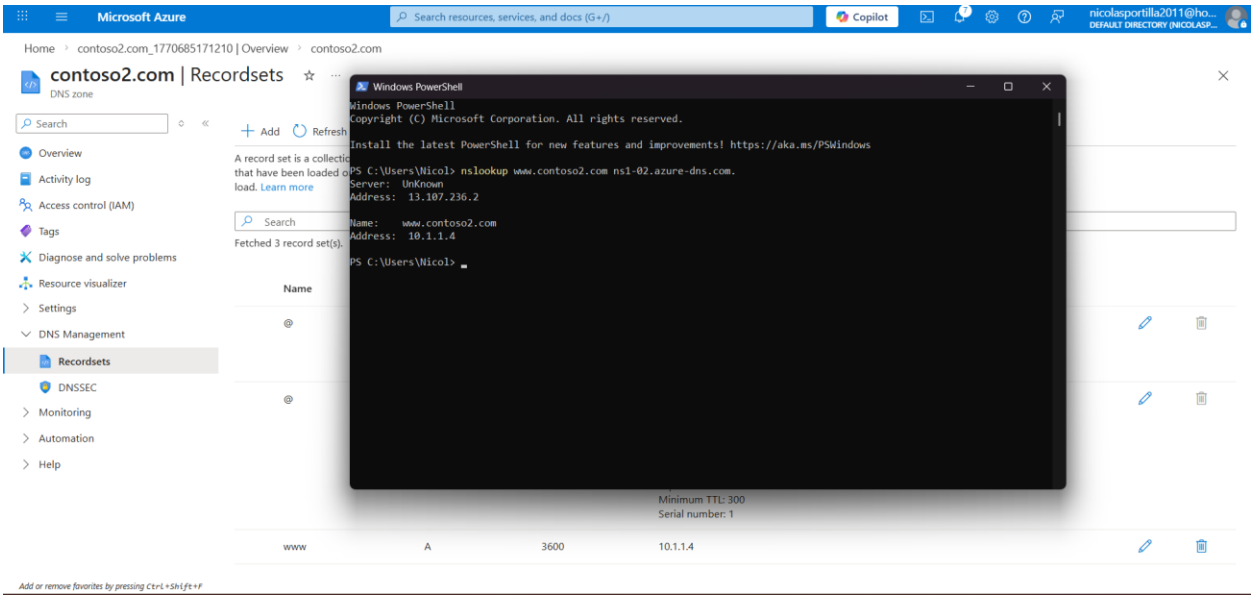

*Figure 2: nslookup test confirming **www.contoso2.com** resolves successfully (via Azure DNS) to the expected IP address, validating DNS record configuration and name resolution.*

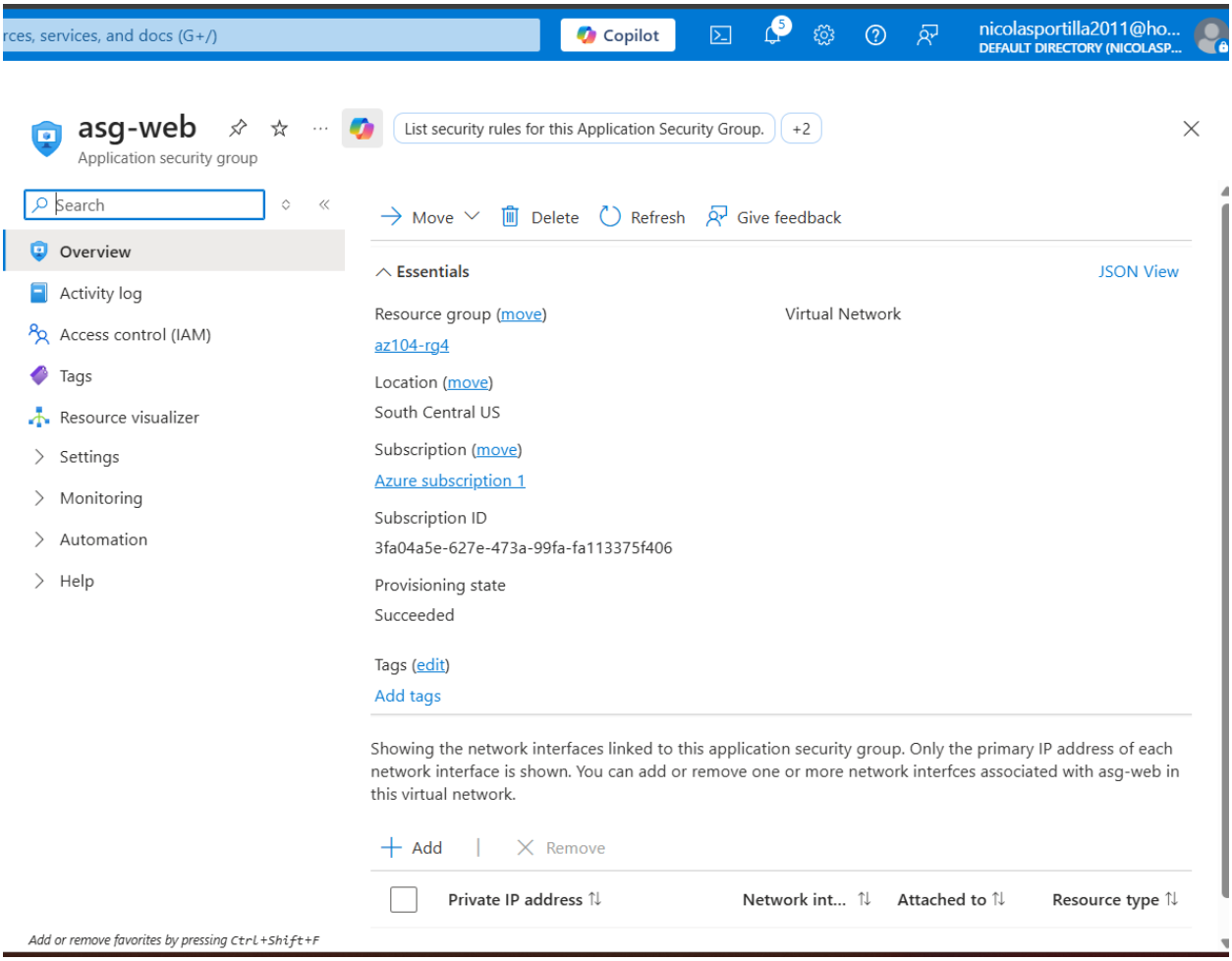

Figure 3: Application Security Group asg-web created successfully in resource group az104-rg4, providing an application-based grouping mechanism for NSG rules.

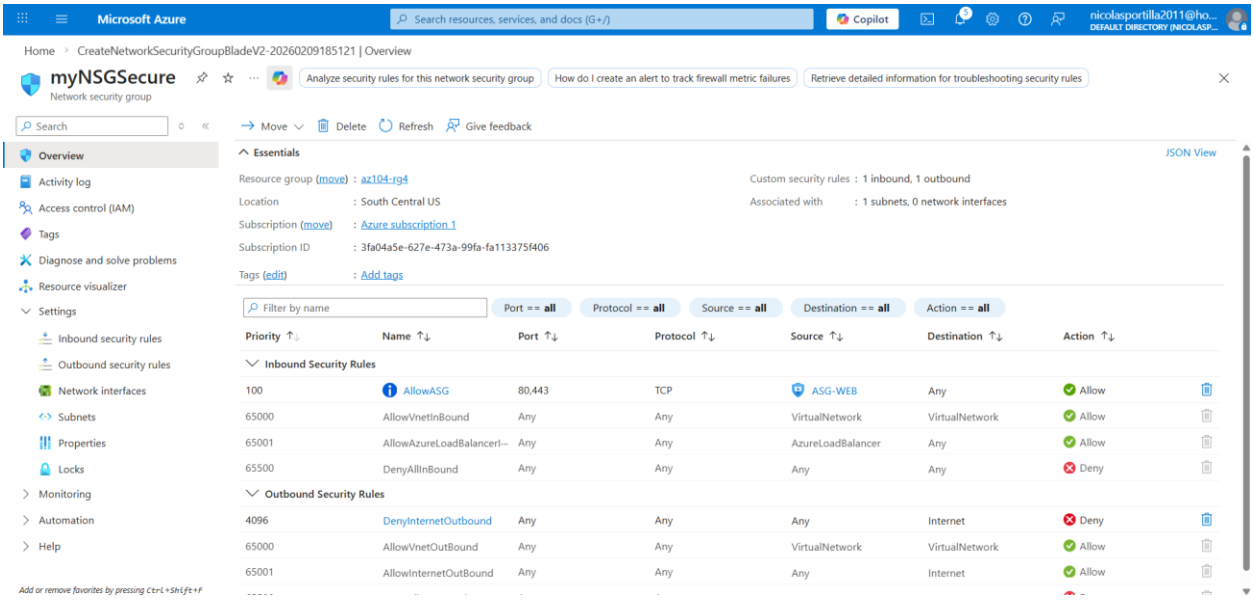

Figure 4: Network Security Group myNSGSecure showing custom rules (1 inbound, 1 outbound) and association with 1 subnet, confirming NSG deployment and scope.

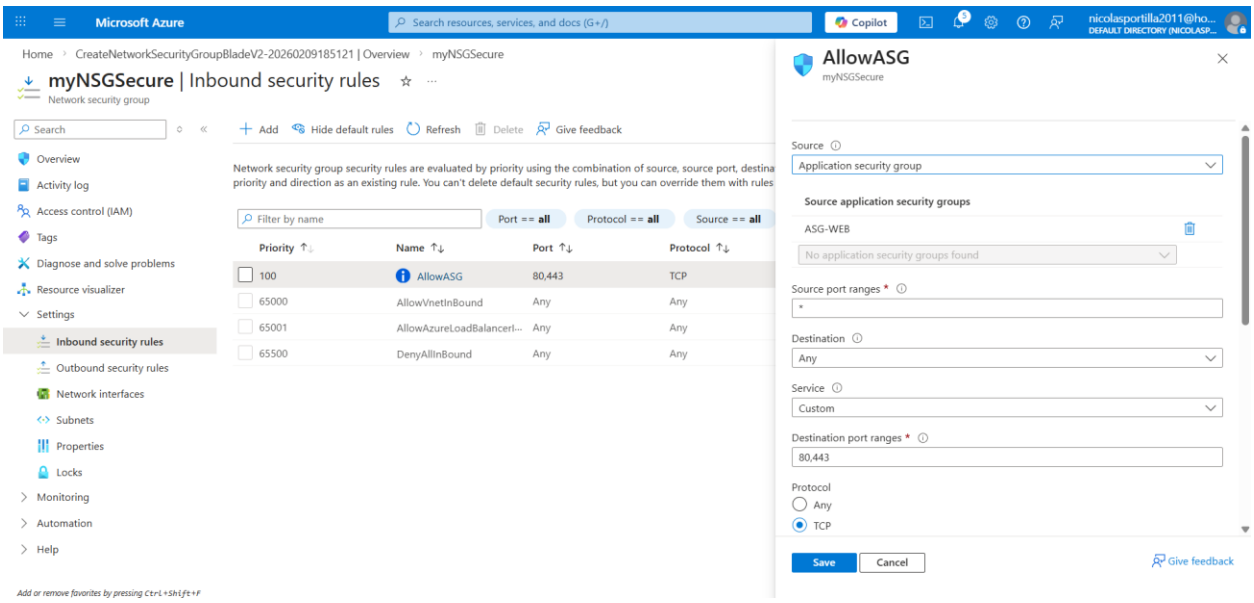

Figure 5: Inbound NSG rule AllowASG configured to allow TCP ports 80 and 443 using ASG-WEB as the source, restricting web access to approved application resources.

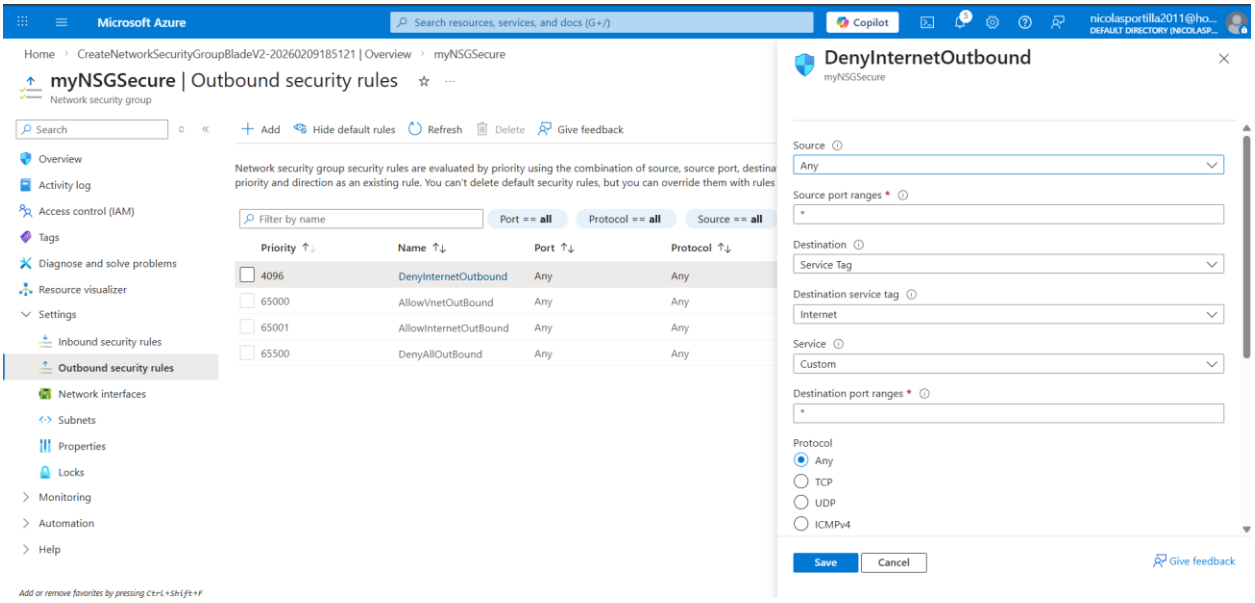

Figure 6: Outbound NSG rule DenyInternetOutbound configured to deny traffic to the Internet service tag, limiting outbound connectivity and enforcing controlled egress.

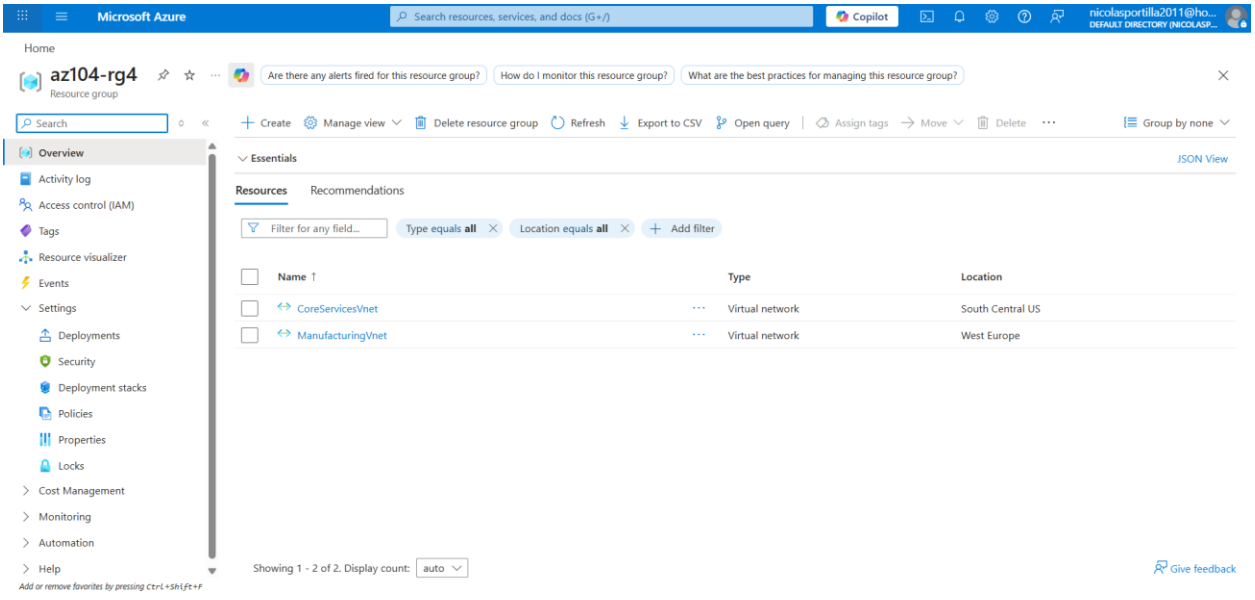

Figure 7: ARM template file showing declarative configuration for ManufacturingVnet, including address space definitions and subnet resources.

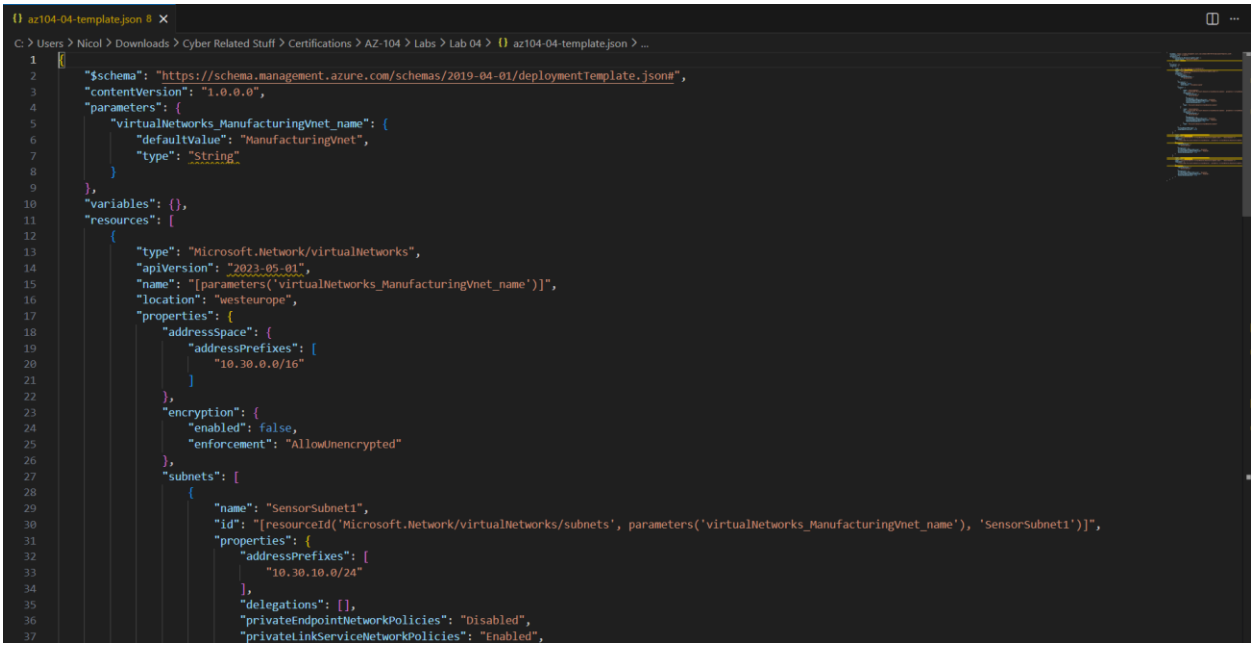

Figure 8: Downloaded ARM template edited locally to support customization and parameterized deployment, demonstrating infrastructure-as-code reuse.

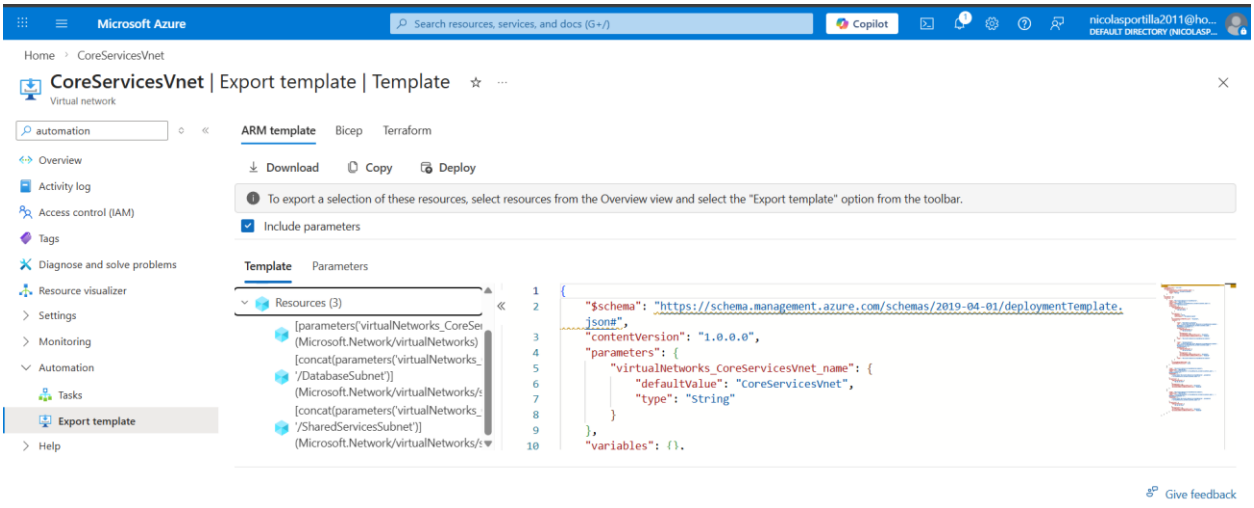

Figure 9: Azure portal Export template view for CoreServicesVnet with parameters included, supporting standardized redeployment.

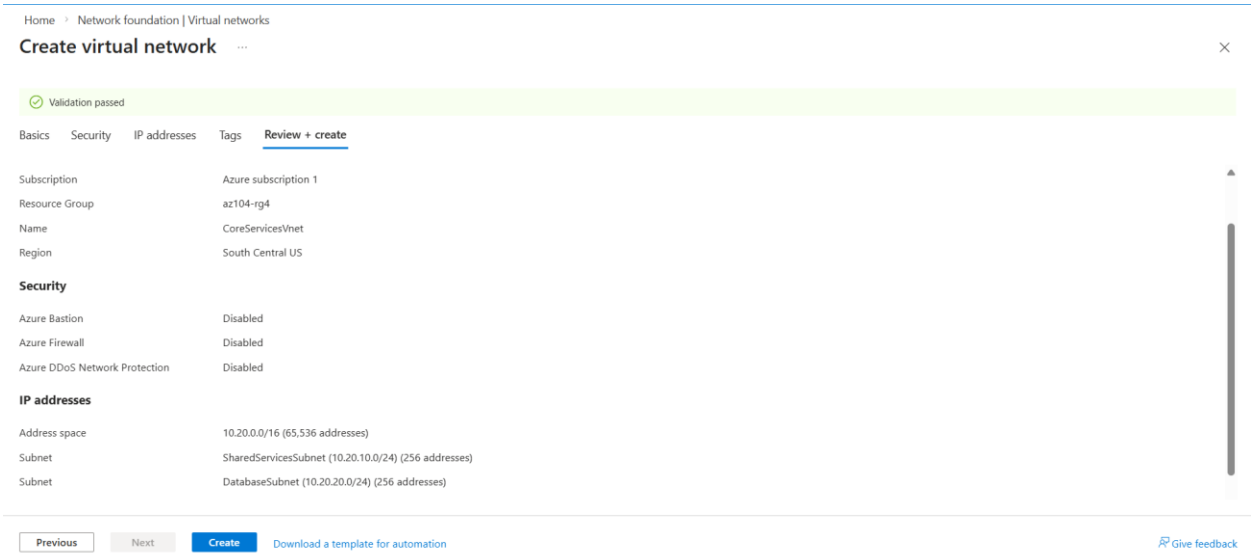

Figure 10: Virtual network creation summary displaying address space 10.20.0.0/16 and two subnets (SharedServicesSubnet and DatabaseSubnet), confirming subnet segmentation.

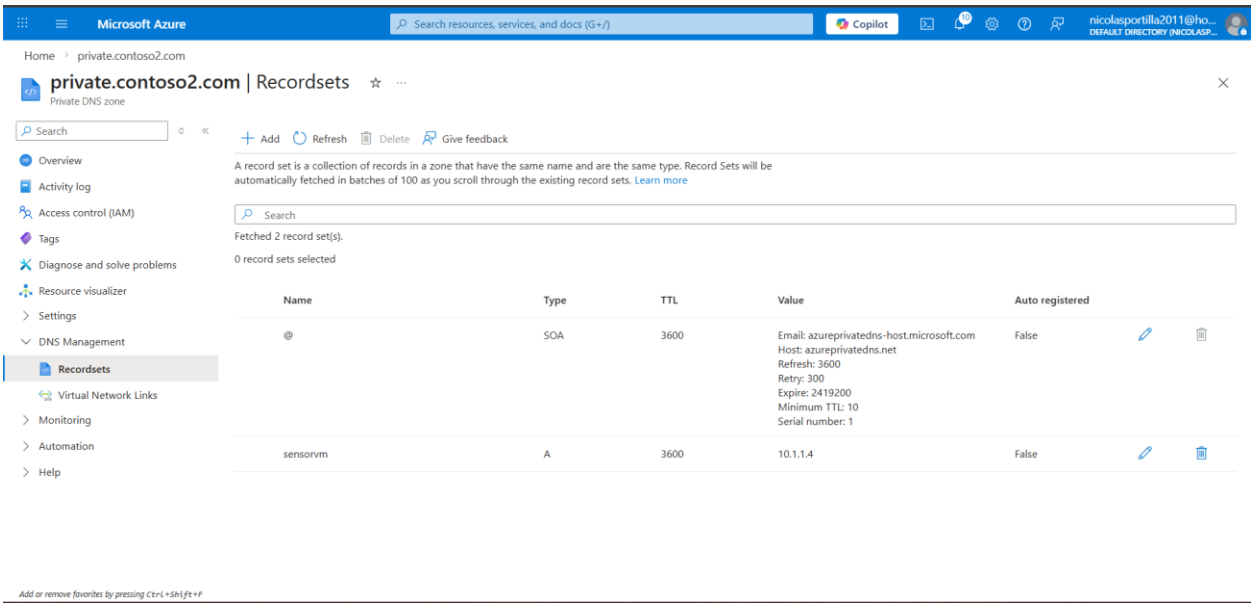

Figure 11: Private DNS zone private.contoso2.com recordsets showing default SOA record and custom A record (sensorvm) mapped to private IP 10.1.1.4, confirming internal DNS resolution.

APPENDICIES

REFER TO GITHUB FOR TEMPLATE.JSON AND PARAMETERS.JSON

REFERENCES

[1] Microsoft, "Microsoft Learning," 2025. [Online]. Available: https://microsoftlearning.github.io/AZ-104-MicrosoftAzureAdministrator/Instructions/Labs/LAB_04-Implement_Virtual_Networking.html. [Accessed 9 February 2026].