Secure Storage Access With Private Endpoint

Portfolio Lab By THATO KGOLE
Date: November 2025
Cloud Platform: Microsoft Azure

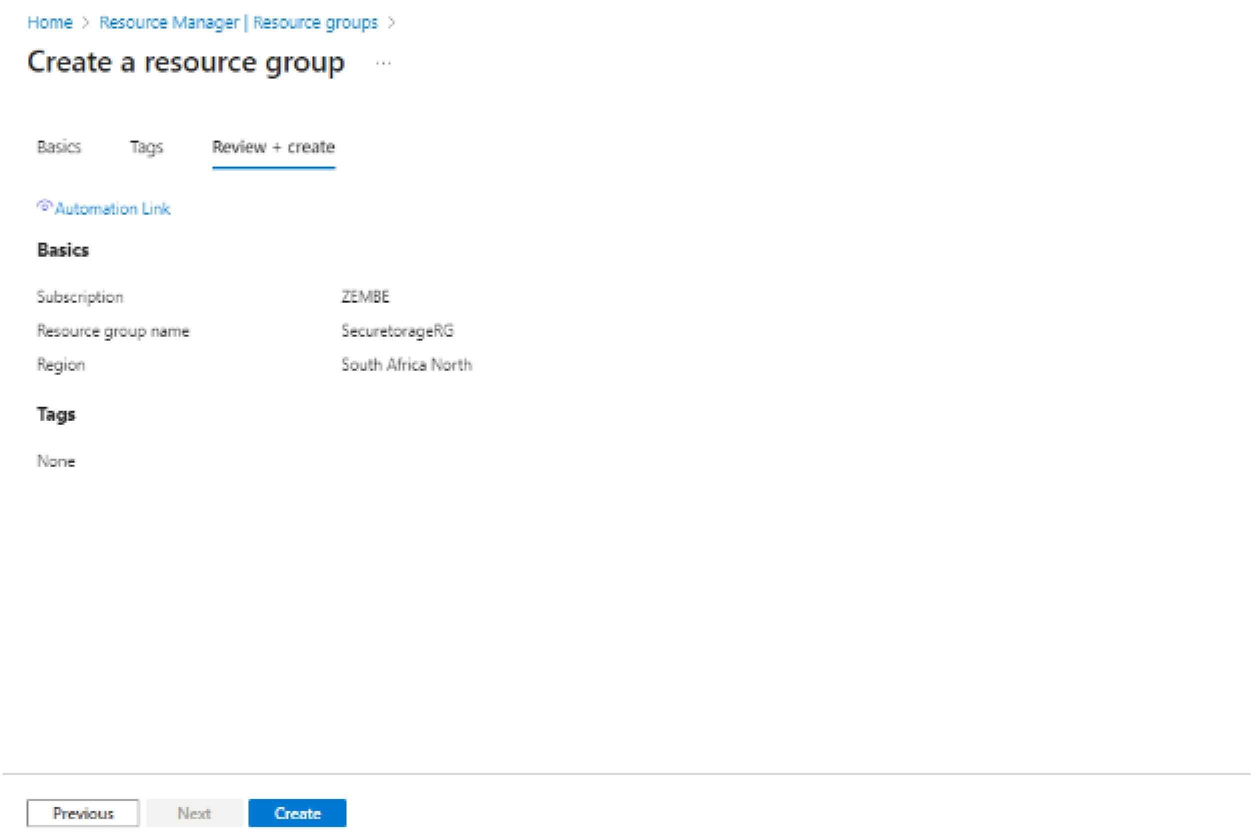
OVERVIEW

Designed and implemented a secure, private connection to an Azure Storage Account using a Private Endpoint.
The goal was to ensure all data traffic stays within Azure's private network, completely blocking internet access to the storage resource.
This demonstrates my understanding of network isolation, identity-based access, and Zero -Trust principles in Azure.

PROBLEM STATEMENT

Many organizations store critical data in Azure Storage, but by default, it's publicly accessible over the internet.
This introduces a risk of unauthorized access or data leaks.
To comply with security and governance standards, companies need a way to:
>Remove public endpoints,
>Enforce private, internal-only connections,
>Maintain network visibility and access control.

Step 1: Create Resource Group
To group all related content



Create a resource group

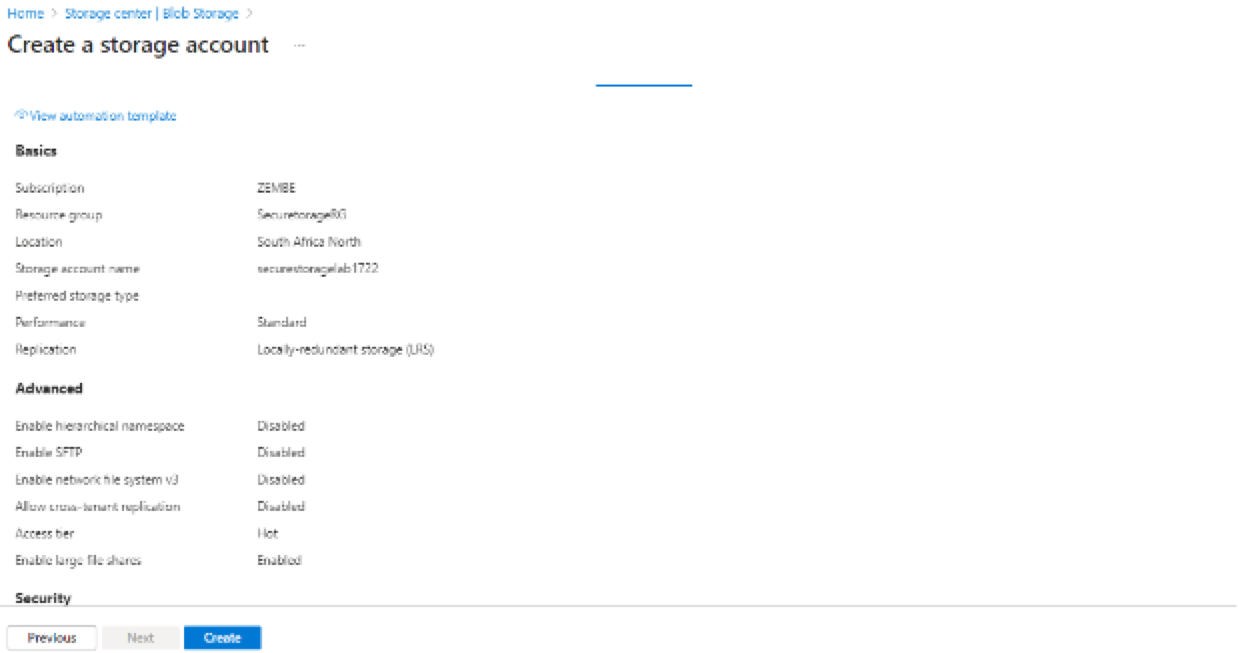
Basics

Subscription	ZEMBE
Resource group name	SecuretorageRG
Region	South Africa North

Tags

None

Step 2: Create Azure Storage Account
To store files and data



Create a storage account

Basics

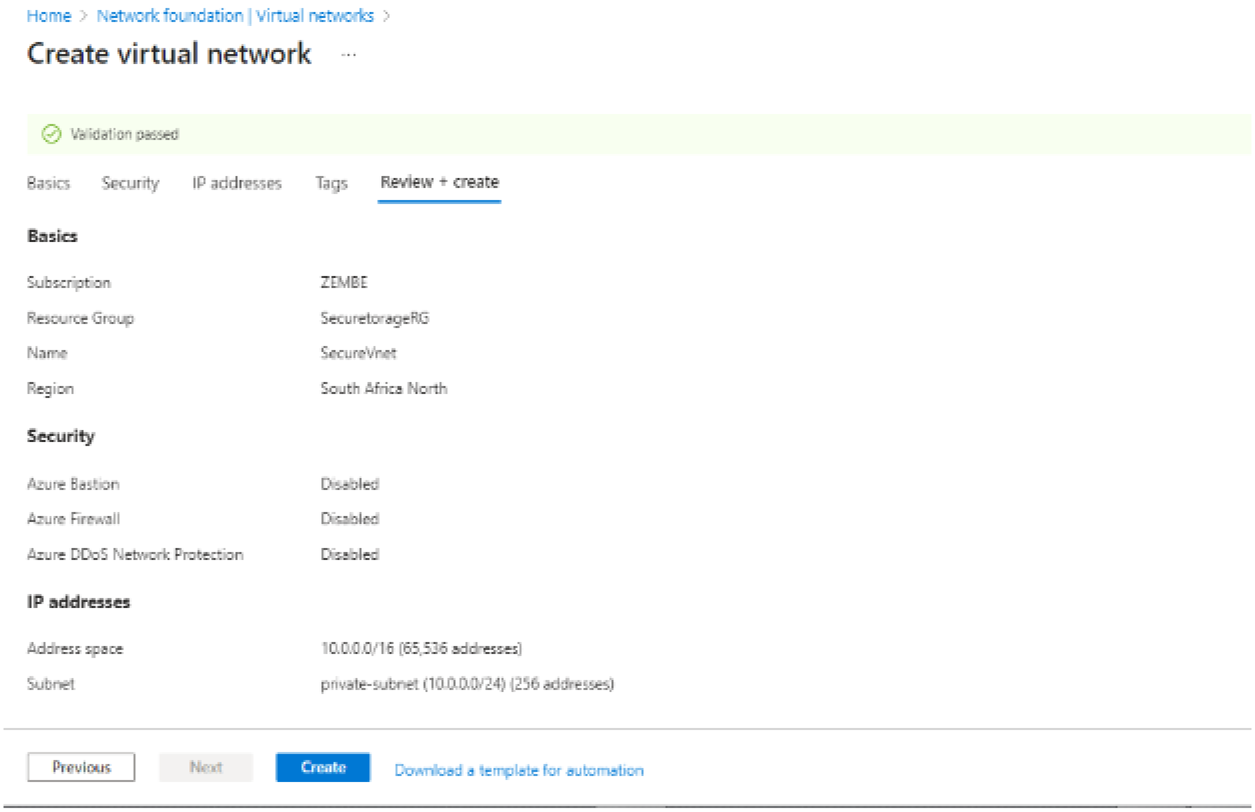
Subscription	ZEMBE
Resource group	SecuretorageRG
Location	South Africa North
Storage account name	securestoragelab1722
Preferred storage type	
Performance	Standard
Replication	Locally-redundant storage (LRS)

Advanced

Enable hierarchical namespace	Disabled
Enable SFTP	Disabled
Enable network file system v3	Disabled
Allow cross-tenant replication	Disabled
Access tier	Hot
Enable large file shares	Enabled

Security

Step 3: Create Virtual Network and subnet
To host private communication channels for internal traffic.



Home > Network foundation | Virtual networks >

Create virtual network ···

Validation passed

Basics Security IP addresses Tags Review + create

Basics

Subscription	ZEMBE
Resource Group	SecuretorageRG
Name	SecureVnet
Region	South Africa North

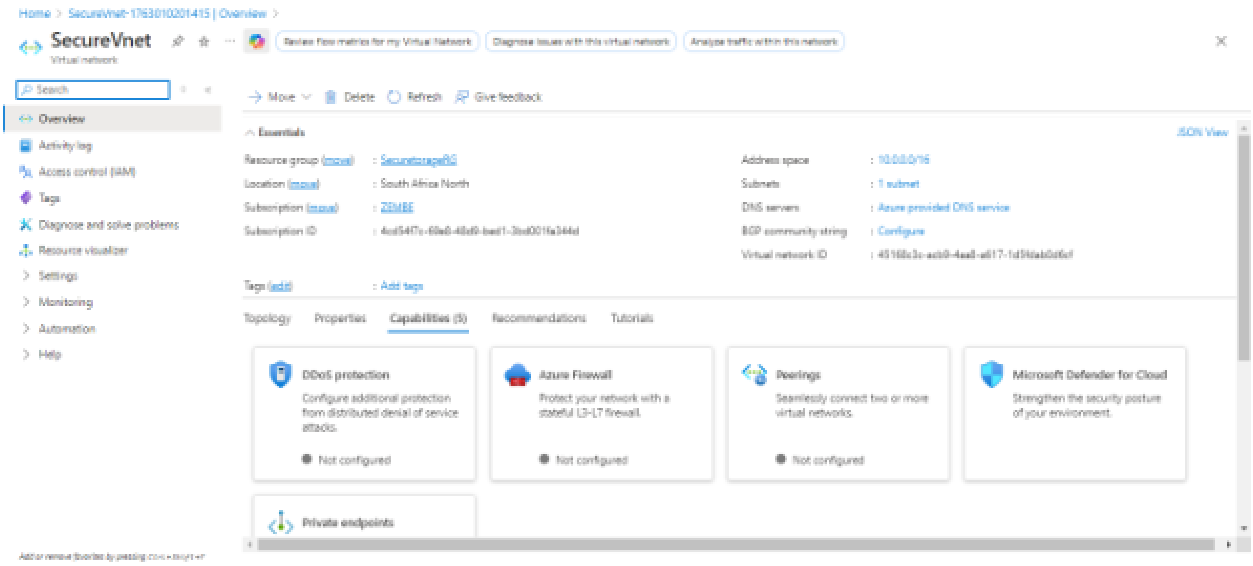
Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

IP addresses

Address space	10.0.0.0/16 (65,536 addresses)
Subnet	private-subnet (10.0.0.0/24) (256 addresses)

Previous
Next
Create
Download a template for automation



Home > SecureVnet-1763010201415 | Overview >

SecureVnet
Virtual network

Review flow metrics for my Virtual Network
Diagnose issues with this virtual network
Analyze traffic within this network
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Monitoring
Automation
Help
Move
Delete
Refresh
Give feedback
JSON View

Essentials

Resource group (move)	: SecuretorageRG	Address space	: 10.0.0.0/16
Location (move)	: South Africa North	Subnets	: 1 subnet
Subscription (move)	: ZEMBE	DNS servers	: Azure provided DNS service
Subscription ID	: 4cd5417c-60e8-48d9-bed1-3bd001fa344d	BGP community string	: Configure
		Virtual network ID	: 45168c3c-acb9-4ea8-a617-1d5fdab0d6f
Tags (add)	: Add tags		

DDoS protection
Configure additional protection from distributed denial of service attacks.
● Not configured

Azure Firewall
Protect your network with a stateful L3-L7 firewall.
● Not configured

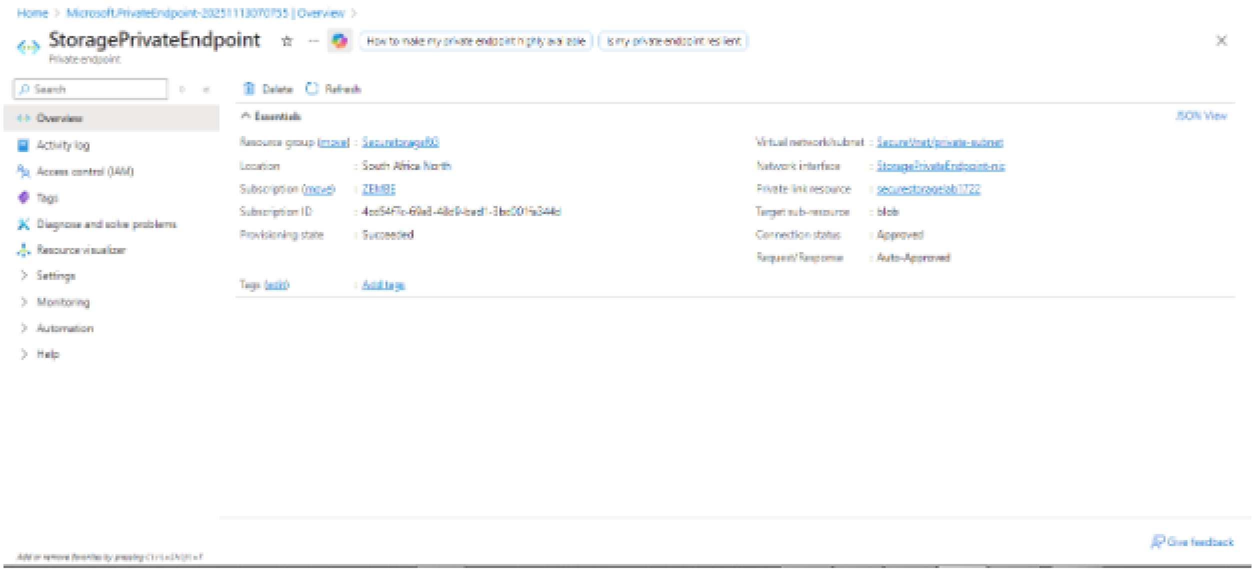
Peerings
Seamlessly connect two or more virtual networks.
● Not configured

Microsoft Defender for Cloud
Strengthen the security posture of your environment.

Private endpoints

Step 4: Create a Private Endpoint

To securely link the storage account into your private VNet, ensuring no public traffic can reach it.

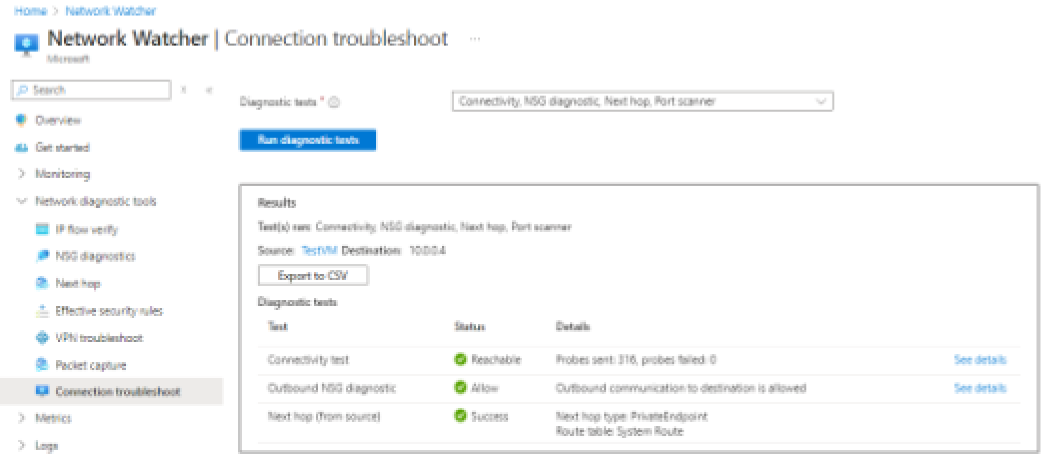


Resource group (move) : SecurestorageRG
Location : South Africa North
Subscription (move) : ZEMBE
Subscription ID : 4cd54f7c-69a8-48d9-bad1-3bc001fa344d
Provisioning state : Succeeded
Tags (edit) : Add tags

Virtual network/subnet : SecureVnet/private-subnet
Network interface : StoragePrivateEndpoint-nic
Private link resource : securestoragelab1722
Target sub-resource : blob
Connection status : Approved
Request/Response : Auto-Approved

Step 5: Test Secure Connectivity

To prove that the storage account is only reachable inside the private network.



Diagnostic tests * : Connectivity, NSG diagnostic, Next hop, Port scanner

Results

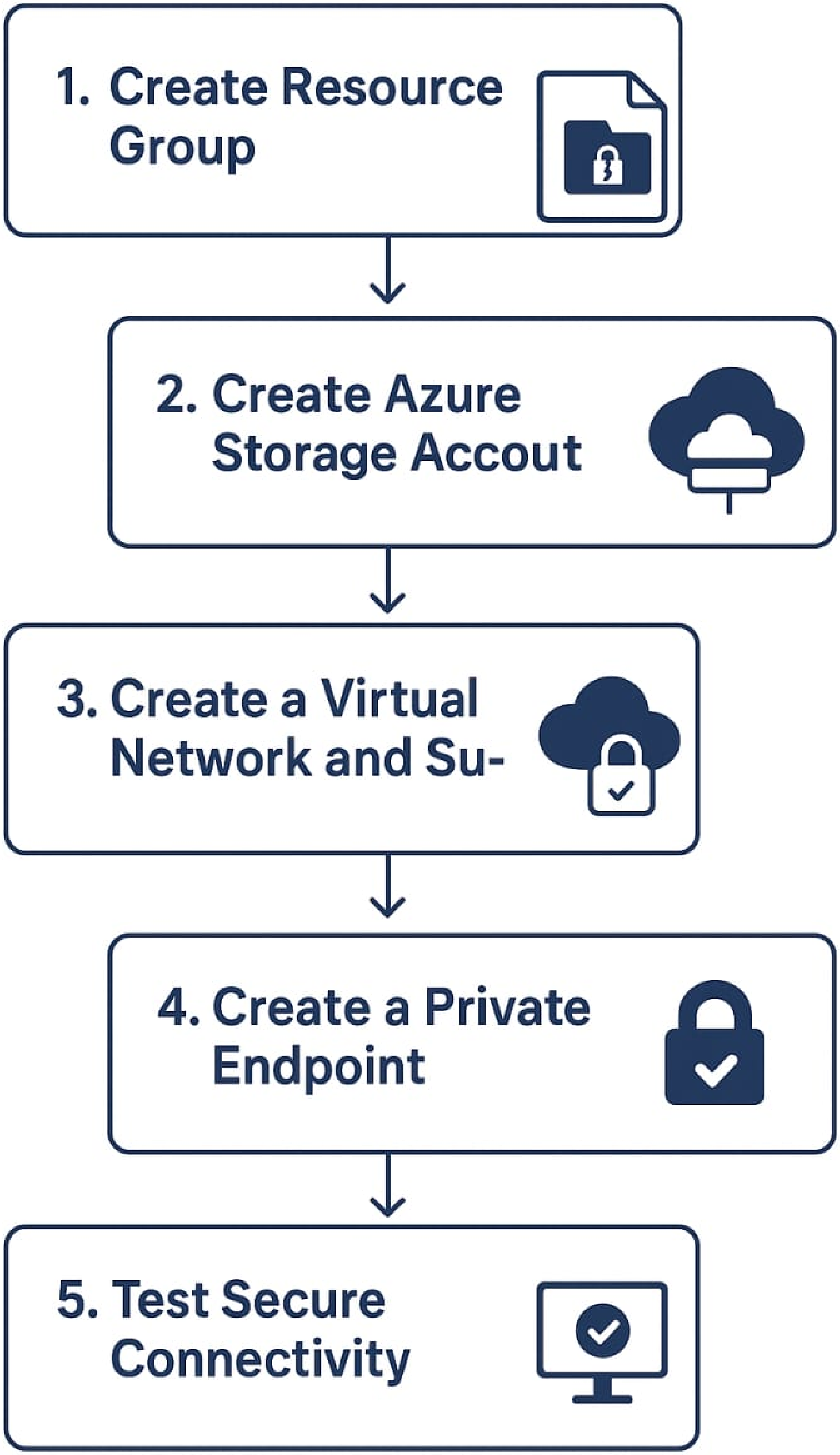
Test(s) ran: Connectivity, NSG diagnostic, Next hop, Port scanner

Source: TestVM Destination: 10.0.0.4

Diagnostic tests

Test	Status	Details	
Connectivity test	✓ Reachable	Probes sent: 316, probes failed: 0	See details
Outbound NSG diagnostic	✓ Allow	Outbound communication to destination is allowed	See details
Next hop (from source)	✓ Success	Next hop type: PrivateEndpoint Route table: System Route	

DIAGRAM



1. Create Resource Group
2. Create Azure Storage Accout
3. Create a Virtual Network and Su-
4. Create a Private Endpoint
5. Test Secure Connectivity

OVERALL KNOWLEDGE GAINED

.Azure Networking Fundamentals (VNets, Subnets)
.Private Endpoint Implementation
.Secure Storage Configuration
.Zero Trust Network Design
.Network Monitoring & Validation
.Professional Documentation & Presentation Skills