Secure Azure Virtual Network using Network security Groups

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

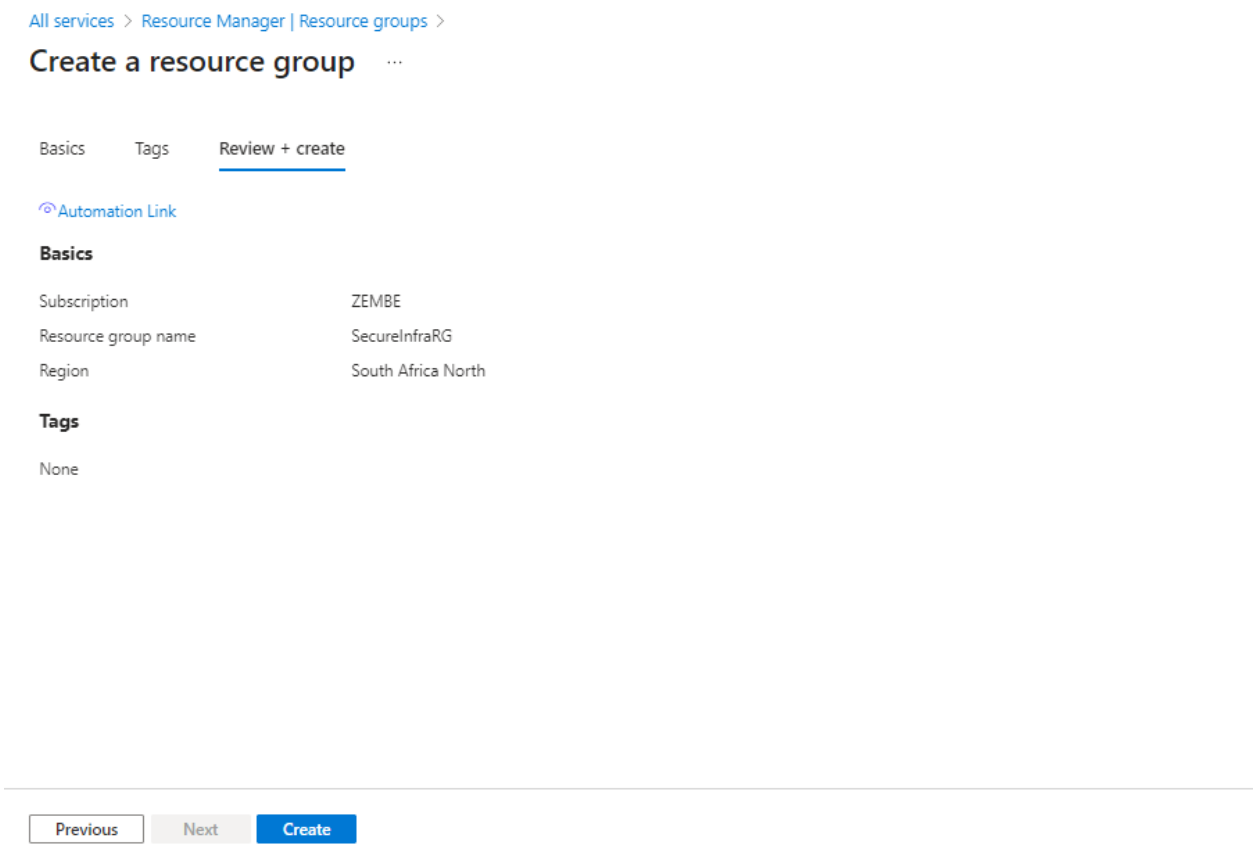
Overview

This project demonstrates how to secure an Azure Virtual Machine using Network Security Groups.
We'll create and configure an NSG to control inbound and outbound network traffic-applying Zero Trust principles at the network layer.

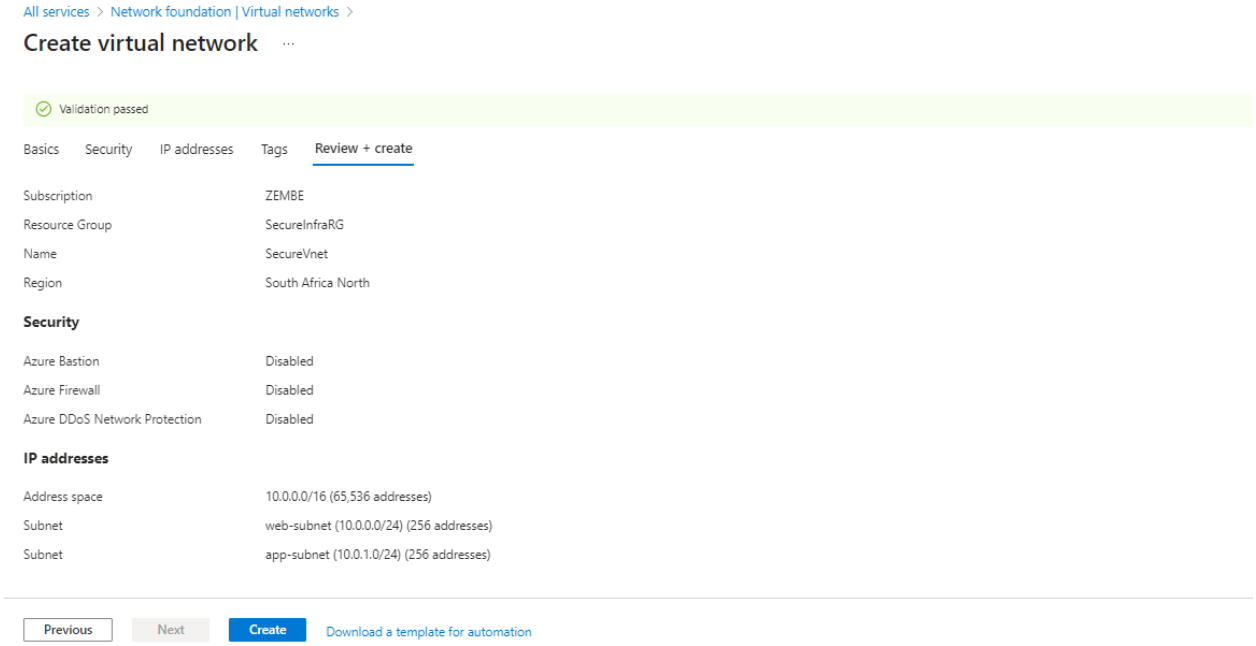
Problem Statement

Organizations deploy VMs and applications in Azure, but without network segmentation and access controls, these resources are vulnerable to external attacks.
The challenge is to secure cloud-based servers from unwanted traffic while allowing authorized access for applications and administrators.

Step 1: Create a Resource Group
To group all related content for easy management.

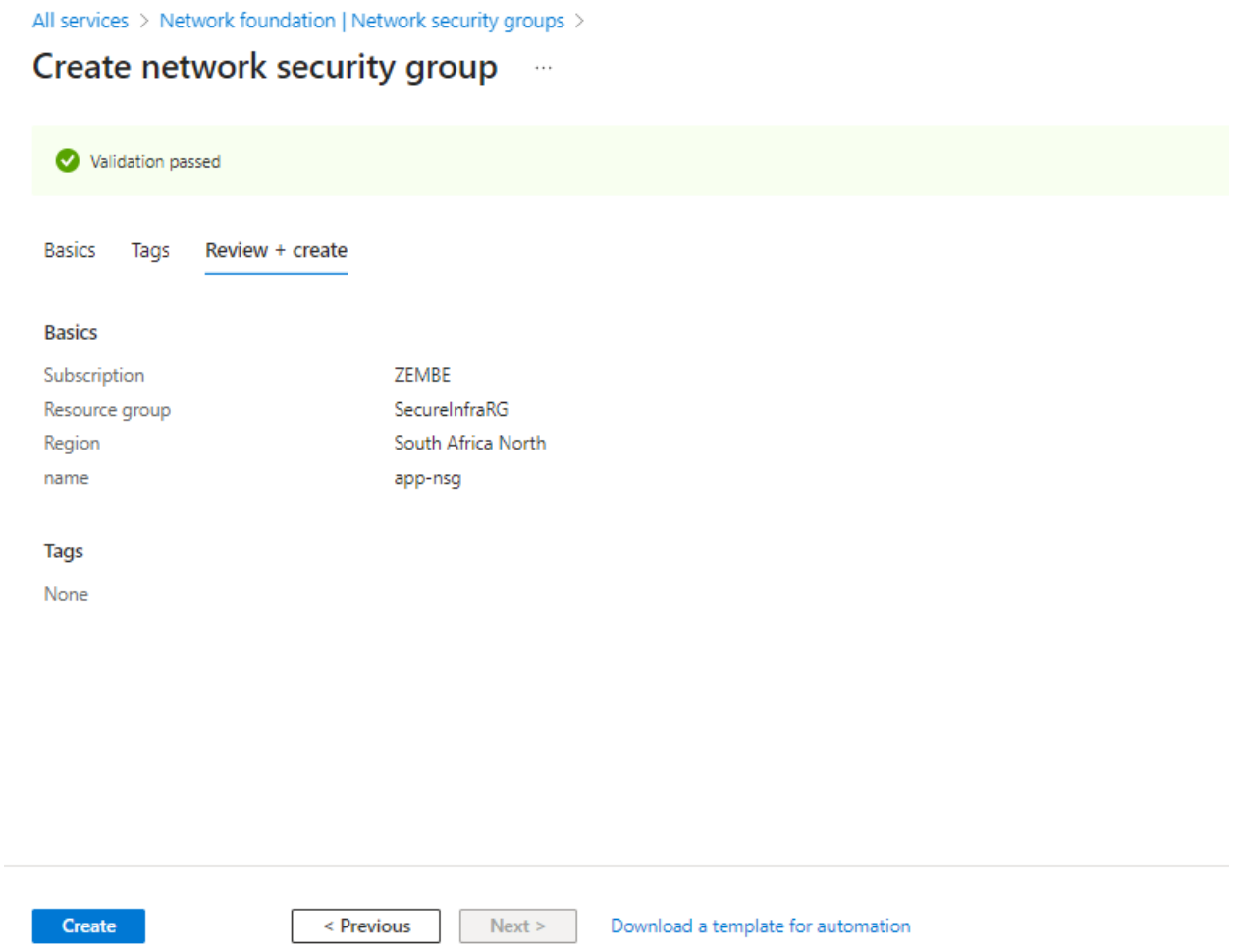


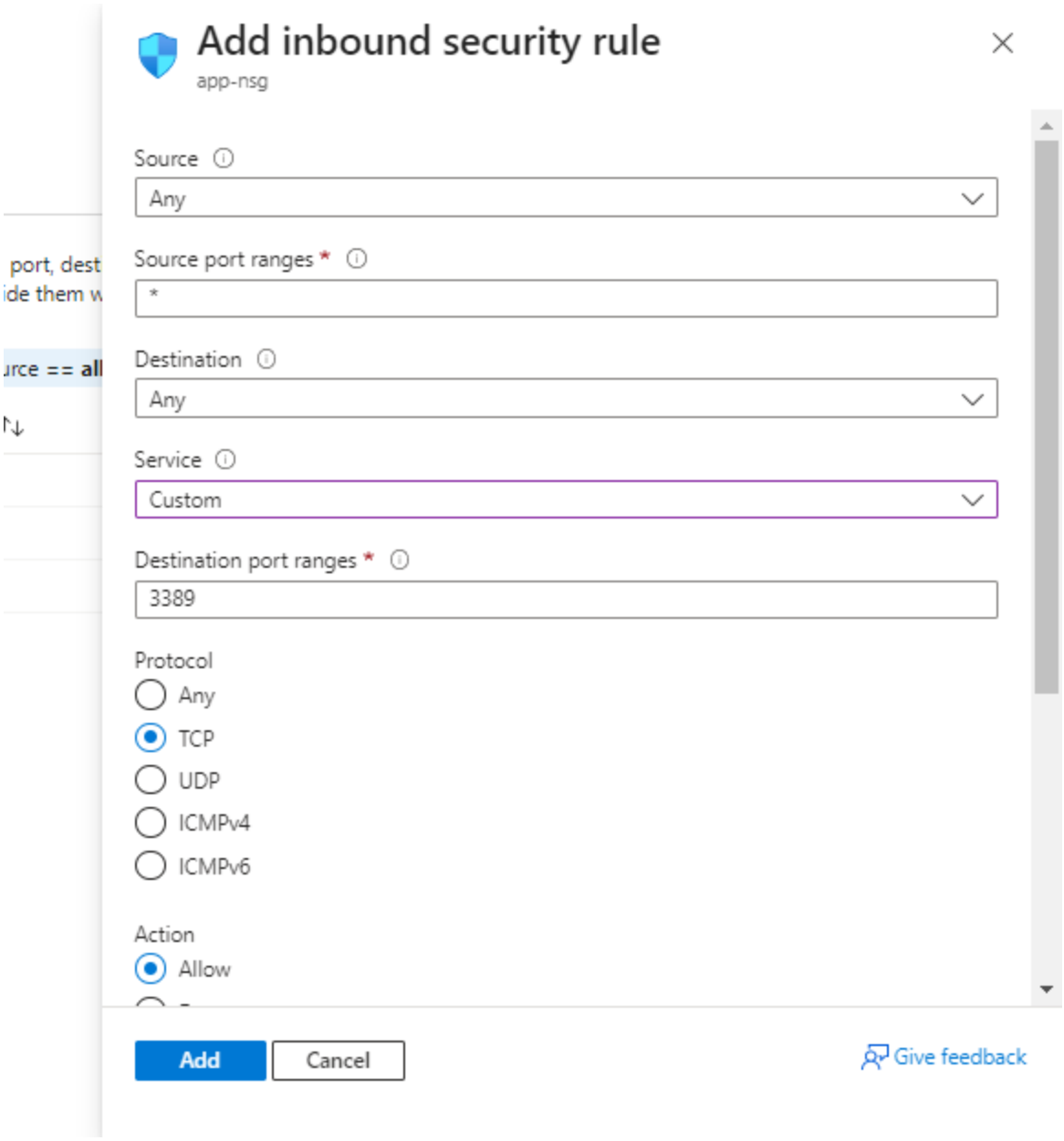
Step 2:Create a Virtual Network
It provides an isolated private network environment for your resources
Add 2 subnets one for public and one for private



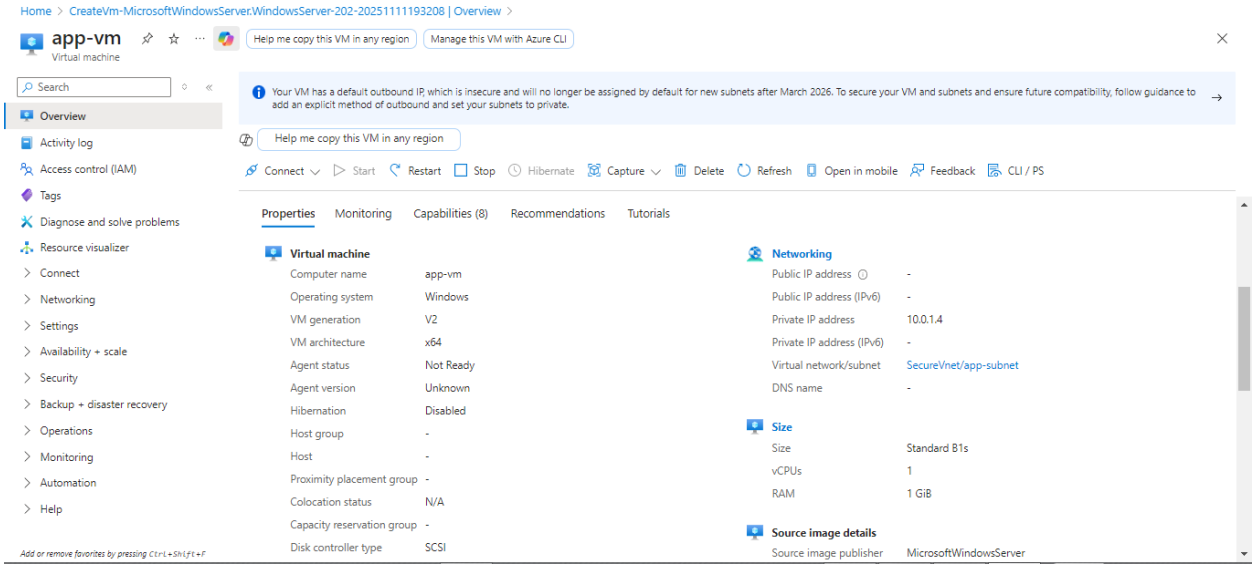
Step 3: Create Network Security Group

To control traffic

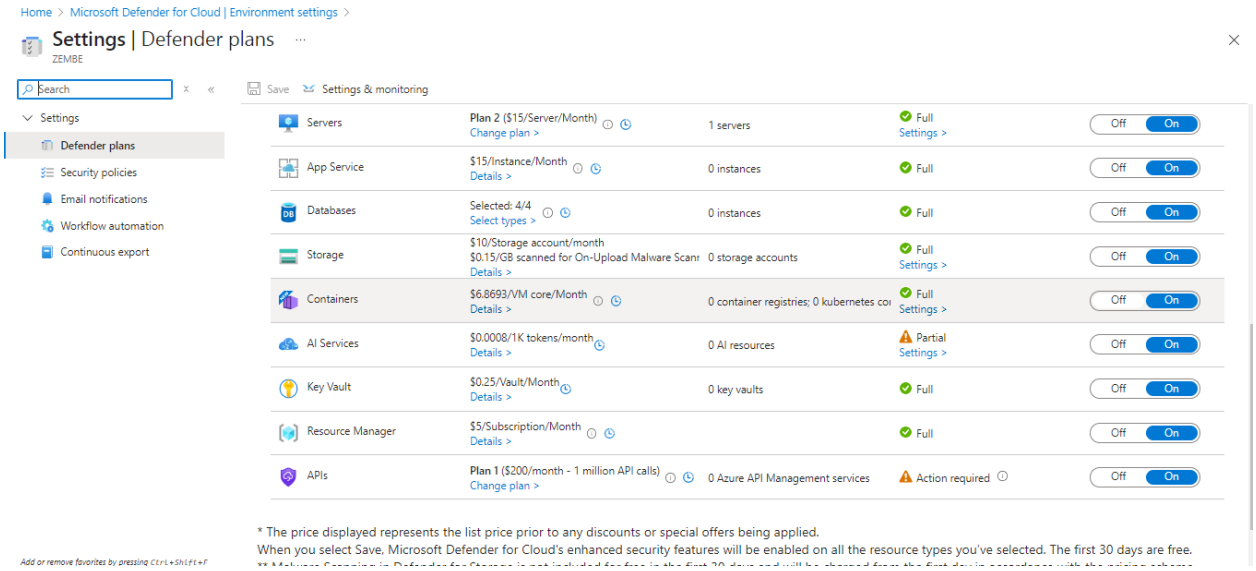




Step 3: Create Virtual Machine without Public IP

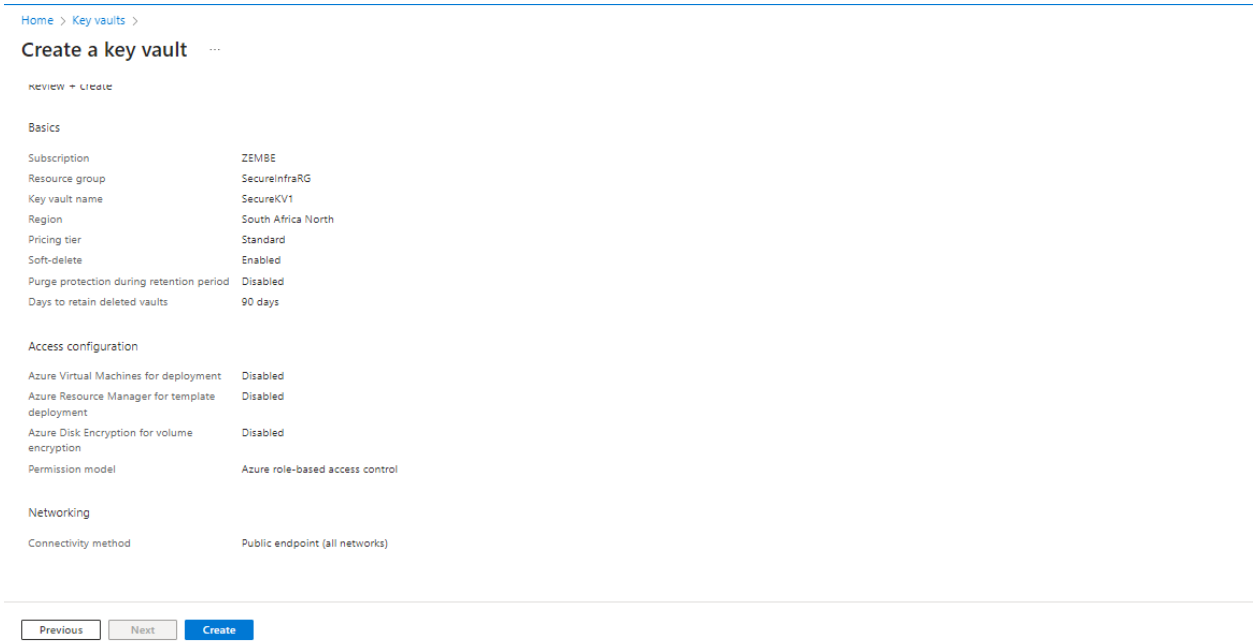


Step 4: Enable Azure Defender For Cloud
It provides security recommendations and threat detection

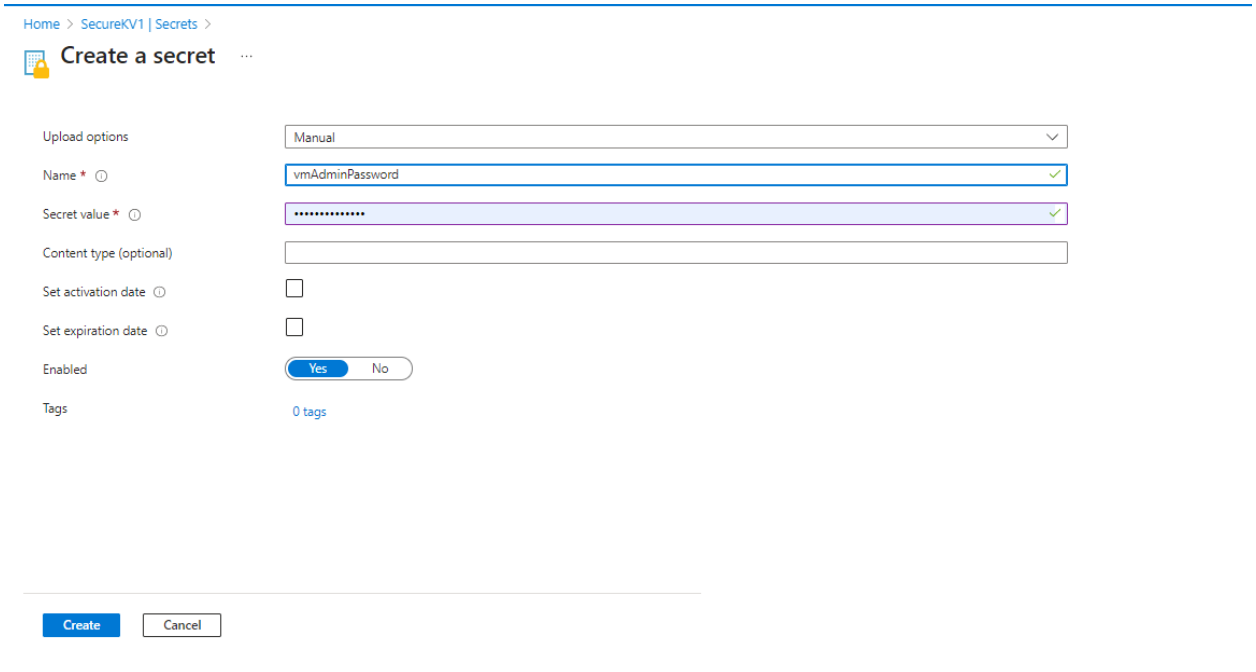


Step 5: Configure Just-In-Time
To reduce the time ports are open
>Defender for cloud – VM (app-vm) –Enable
>Configure allowed ports (RDP)

Step 6: Create Azure Key Vault
To store VM admin secret

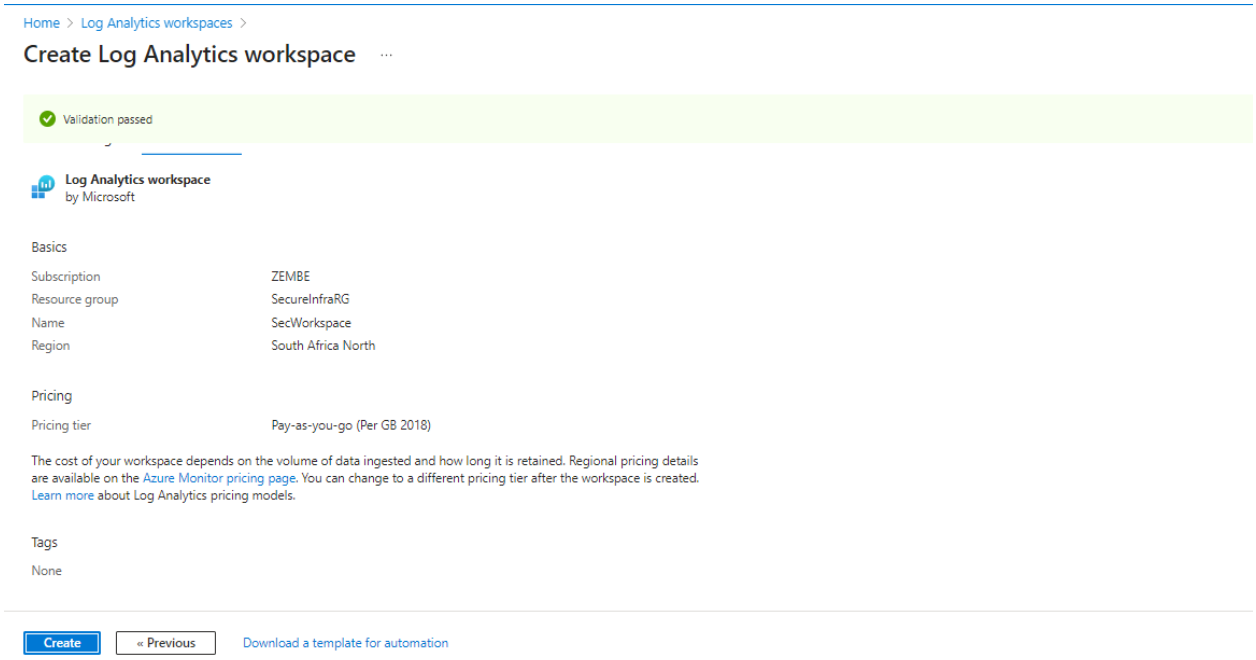


Step 7:Enable Disk Encryption
Ensures VM disks are encrypted at rest.
>>Encrypted by default



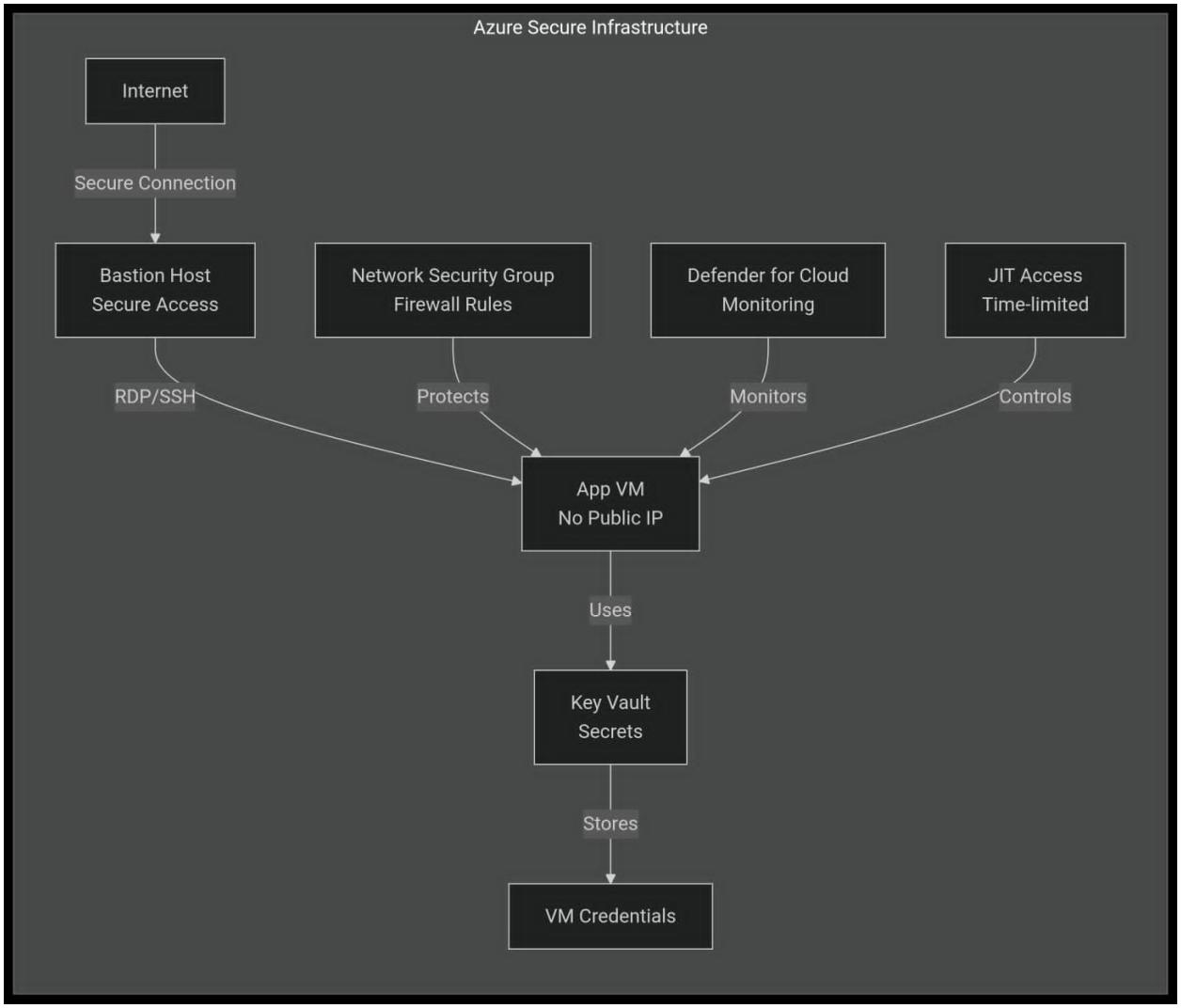
Step 8: Attach Key Vault To VM
To avoid storing credentials on the VM, let access Key Vault securely
>VM – Identity – System assigned – On –Save
>Key Vault – Access policies – Add Access Policy –VM's system identity – Add –Save

Step 9: Verify logging & monitoring
Ensures you can see security events–



Follow to complete
>Defender for cloud – setting – connect the subscription / resource to this workspace
>VM – Monitoring – Diagnostic settings – Send quest-level logs/events to Log Analytics (selectWorkspace)

DIAGRAM


Azure Secure Infrastructure
Internet
Secure Connection
Bastion Host
Secure Access
Network Security Group
Firewall Rules
Defender for Cloud
Monitoring
JIT Access
Time-limited
RDP/SSH
Protects
Monitors
Controls
App VM
No Public IP
Uses
Key Vault
Secrets
Stores
VM Credentials