

Portfolio Lab By THATO KGOLE

Date: November 2025

Cloud Platform: Microsoft Azure

OVERVIEW

This project demonstrates the end-to-end deployment of a secure, scalable, and well-structured cloud infrastructure in Microsoft Azure.

It focuses on core AZ-104 Administrator skills, including resource management, networking, security, storage, identity, and cost optimization.

PROBLEM STATEMENT

A growing startup wants to migrate its internal application to Azure.

They need an infrastructure that:

- >Is secure and segmented.*
- >Allows controlled public access to the web app but keeps databases private.*
- >Has identity-based access instead of hardcoded credentials.*
- >Supports monitoring, cost control, and compliance.*

As an Azure Administrator, Your goal was to design and deploy a secure, cost-efficient, and manageable cloud environment that fulfills these requirements.

SOLUTIONS

Step 1: Create Resource Group

To group all related resources together

Home > Resource Manager | Resource groups >

Create a resource group

Basics Tags Review + create

Automation Link

Basics

Subscription	Azure subscription 1
Resource group name	RG-az104
Region	South Africa North

Tags

None

Previous Next Create



The screenshot shows a Microsoft Azure 'Create a resource group' wizard. The 'Review + create' tab is selected. It displays basic information: Subscription (Azure subscription 1), Resource group name (RG-az104), and Region (South Africa North). The 'Tags' section shows 'None'. At the bottom, there are 'Previous' and 'Next' buttons, and a prominent blue 'Create' button. Below the buttons is a taskbar with icons for various Microsoft services like File Explorer, Task View, and Edge.

Step 2: Create Virtual Network

Configure address space

Add Subnets

Web subnet (10.0.0.0/24)

DB subnet (10.0.1.0/24)

Home > Network foundation | Virtual networks >

Create virtual network

 Validation passed

Basics Security IP addresses Tags **Review + create**

[View automation template](#)

Basics

Subscription	Azure subscription 1
Resource Group	RG-az104
Name	vnet-az104
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	subnet1 (10.0.0.0/24) (256 addresses)
Subnet	subnet2 (10.0.1.0/24) (256 addresses)

Tags

[Previous](#) [Next](#) **Create** [Download a template for automation](#)

Step 4: Deploy Virtual Machine

Web VM (public IP)

DB VM (private subnet)

Home > Compute infrastructure | Virtual machines >

Create a virtual machine

Help me create a VM optimized for high availability Help me create a low cost VM Help me choose the right VM size for my workload

Validation passed

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Basics

Subscription	Azure subscription 1
Resource group	RG-az104
Virtual machine name	vm-web
Region	South Africa North
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows Server 2019 Datacenter - Gen2
VM architecture	x64
Size	Standard B1s (1 vcpu, 1 GiB memory)
Enable Hibernation	No
Username	zembe1722
Already have a Windows license?	No
Azure Spot	No

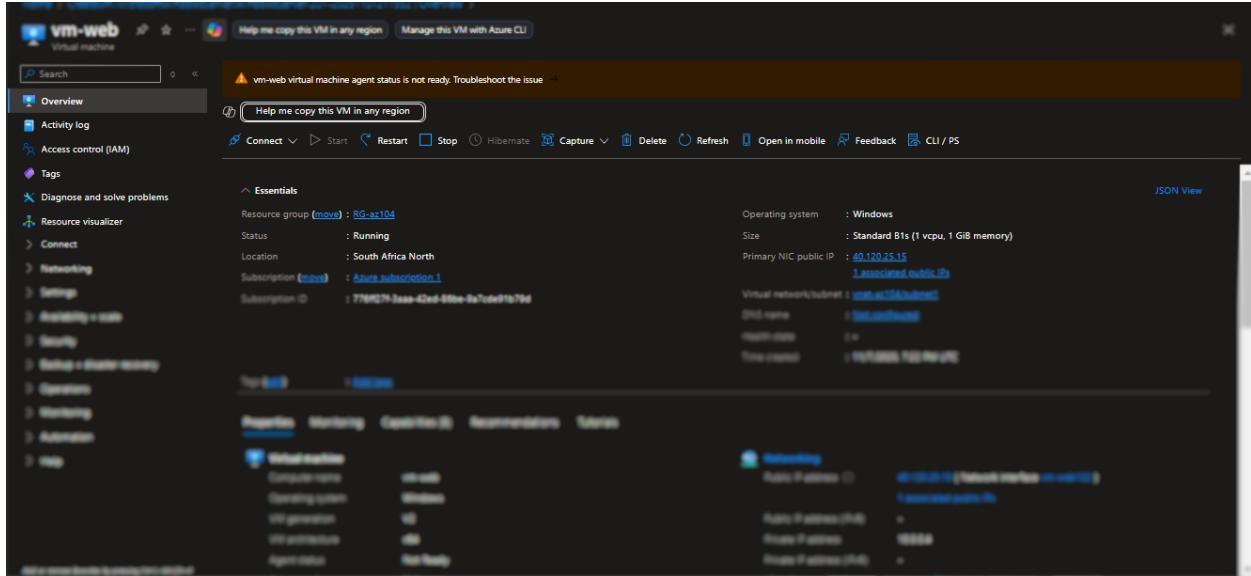
Disk

OS disk size Image default

< Previous Next > Create

Networking

Virtual network	vnet-az104
Subnet	subnet1
Public IP	(new) vm-web-ip
NIC network security group	None
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No
Delete public IP and NIC when VM is deleted	Disabled



DB VM

Home > Compute Infrastructure | Virtual machines >

Create a virtual machine

Validation passed

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Basics

Subscription	Azure subscription 1
Resource group	RG-az104
Virtual machine name	vm-db
Region	South Africa North
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows Server 2019 Datacenter - Gen2
VM architecture	x64
Size	Standard B1s (1 vcpu, 1 GiB memory)
Enable Hibernation	No
Username	zembe1722
Public inbound ports	RDP
Already have a Windows license?	No
Azure Spot	No

Disks

< Previous Next > Create

Networking

Virtual network	vnet-az104
Subnet	subnet2
Public IP	None
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No
Delete NIC when VM is deleted	Disabled

Home > CreateVm-MicrosoftWindowsServer.WindowsServer-201-20251107212054 | Overview >

vm-db Virtual machine

Help me copy this VM in any region Manage this VM with Azure CLI

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Connect

Networking

Settings

Availability + scale

Security

Backup + disaster recovery

Operations

Monitoring

Automation

Help

Your VM has a default outbound IP which is insecure and will no longer be assigned by default for new subnets after March 2026. To secure your VM and subnets and ensure future compatibility, follow guidance to add an explicit method of outbound and set your subnets to private.

Help me copy this VM in any region

Connect Start Restart Stop Hibernate Capture Delete Refresh Open in mobile Feedback CLI / PS

Essentials

Resource group (move) : RG-az104

Status : Running

Location : South Africa North

Subscription (move) : Azure subscription 1

Subscription ID : 776ff27f-3aaa-42ed-86be-9a7cde91b79d

Operating system : Windows

Size : Standard B1s (1 vcpu, 1 GiB memory)

Primary NIC public IP : [Public IP](#)

Virtual network/subnet : [vmdb-az104-subnet2](#)

DNS name : [vmdb-az104-subnet2](#)

Health state : [OK](#)

Time created : 14/09/2025 10:57:49 UTC

Properties Monitoring Capabilities Recommendations Status

VM details

Computer name : vm-db

Operating system : Windows

VM generation : V2

VM architecture : x64

Agent status : Ready

Network interface

Public IP address : [Public IP](#)

Private IP address (IPv4) : [Private IP](#)

Private IP address (IPv6) : [Private IP](#)

Private IP address (MAC) : [Private IP](#)

Virtual network interface : [vmdb-az104-subnet2](#)

JSON View

Step 5: Configure NSG Rules

Allow RDP only from your IP

Home > CreateNetworkSecurityGroupBladeV2-20251107210433 | Overview > nsg-web

nsg-web | Inbound security rules

Network security group

Search

Add Hide default rules Refresh Delete Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Automation

Help

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name Port = all Protocol = all Source = all Destination = all

Priority ↑	Name ↑	Port ↑	Protocol ↑	Action ↑
100	subnet	3389	TCP	Allow
65000	AllowVnetInBound	Any	Any	Virt
65001	AllowAzureLoadBalancerInBo...	Any	Any	Az
65500	DenyAllInBound	Any	Any	Deny

Destination : Any

Service : RDP

Destination port ranges : 3389

Protocol : TCP

Action : Allow

Priority : 100

Name : subnet

Description :

Save Cancel Give feedback

Home > CreateNetworkSecurityGroupBladeV2-20251107210433 | Overview > nsg-web

nsg-web | Subnets

Network security group

Associate

Search subnets

Name	Address range	Virtual network
subnet1	10.0.0.0/24	vnet-az104

Give feedback

Add or remove favorites by pressing **Ctrl+Shift+F**

Step 6: Enable Managed Identity

Assign identity to both VMs

Microsoft Azure

Compute infrastructure | Virtual machines > vm-web

vm-web | Identity

Virtual machine

Search

System assigned User assigned

You are viewing a new version of Browse experience. Click here to access the old experience.

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.

Save Discard Refresh Got feedback?

Status: Off On

Identity

- Microsoft Defender for Cloud
- Backup + disaster recovery
- Operations
- Monitoring
- Automation
- Help

Add or remove favorites by pressing **Ctrl+Shift+F**

Step 7: Create Storage Account

Use for logs/backups

Microsoft Azure

Home > Storage center | Blob Storage >

Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review + create

[View automation template](#)

Basics

Subscription	Azure subscription 1
Resource group	RG-VM-LAB
Location	South Africa North
Storage account name	storage104
Preferred storage type	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

Secure transfer	Enabled
-----------------	---------

Previous Next Create

Microsoft Azure

Home > storage104_1762544324296 | Overview >

storage104

Storage account

Search

Upload Open in Explorer Delete Move Refresh Open in mobile CLI / PS Feedback

Improve data protection for this storage account Enhance the security of this storage account Analyze connectivity to this storage account

Overview

Essentials

Resource group (mow)	: RG-VM-LAB	Performance	: Standard
Location	: southafricanorth	Replication	: Locally-redundant storage (LRS)
Subscription (mow)	: Azure subscription 1	Account kind	: StorageV2 (general purpose v2)
Subscription ID	: 776f127f-3aaa-42ed-80be-9a7cde91b79d	Provisioning state	: Succeeded
Disk state	: Available	Created	: 11/7/2025, 9:43:46 PM
Tags (e)	: Add tags		

Properties Monitoring Capabilities (7) Recommendations (0) Tutorials Tools + SDKs

Blob service

Hierarchical namespace	Disabled	Require secure transfer for REST API operations	Enabled
Default access tier	Hot	Storage account key access	Enabled
Blob anonymous access	Disabled	Minimum TLS version	Version 1.2
Blob soft delete	Enabled (7 days)	Infrastructure encryption	Disabled
Container soft delete	Enabled (7 days)		
Versioning	Disabled		
Change feed	Disabled		
NFS v3	Disabled		
Allow cross-tenant replication	Disabled		
Storage tasks assignments	None		

Security

Require secure transfer for REST API operations	Enabled
Storage account key access	Enabled
Minimum TLS version	Version 1.2
Infrastructure encryption	Disabled

Networking

Public network access	Enabled
Public network access scope	Enable from all networks
Private endpoint connections	0
Network routing	Microsoft network routing
Endpoint type	Standard

Add or remove favorites by pressing Ctrl+Shift+F+F

File service

The screenshot shows the Azure Storage Access Control (IAM) interface for the storage104 account. The left sidebar includes options like Overview, Activity log, Tags, Diagnose and solve problems, and Access Control (IAM). The main area displays a table of role assignments:

Name	Type	Role	Scope	Condition
vm-web	Managed identity	Storage Blob Data Contributor	This resource	

Showing 1 - 1 of 1 results.

Step 8: Assign RBAC Role “Storage Blob Contributor” to Managed Identity

The screenshot shows the 'Add role assignment' wizard in the Microsoft Azure portal. The steps are:

- Role: Storage Blob Data Contributor
- Scope: /subscriptions/776ff27f-3aaa-42ed-86be-9a7cd91b79d/resourcegroups/RG-VM-LAB/providers/Microsoft.Storage/storageAccounts/storage104
- Members:

Name	Object ID	Type
vm-web	c11728ce-9f65-44b5-adb4-7f6d171da625	Virtual machine
- Description: No description
- Condition: None

At the bottom, there are 'Review + assign', 'Previous', and 'Next' buttons.

Step 9: Enable Azure Defender Security Center - Defender Plans

The screenshot shows the Microsoft Defender for Cloud Overview page. On the left, there's a navigation sidebar with sections like General, Setup, Recommendations, Attack path analysis, Security alerts, Inventory, Cloud Security Explorer, Workbooks, Community, Diagnose and solve problems, Cloud Security, and Management. A search bar is at the top. The main area has a dark header with 'Subscriptions' and 'What's new'. Below the header, it says 'You may be viewing limited information. To get tenant-wide visibility, click here →'. It displays metrics: 1 Azure subscription, 5 Assessed resources, 0 Attack paths, and 0 Security alerts. A large central box titled 'Security posture' shows 0 Critical recommendations, 0 Attack paths, and 0/0 Overdue recommendations. It also shows an environment risk and secure score with 4 recommendations: Critical 0, High 0, Medium 0, Low 0, and Not evaluated 4. A 'Total secure score' bar is at 0%. Below this, there are links for 'Explore your security posture >' and 'Click here to upgrade >'. To the right, there's a section titled 'Utilize the Permissions Management capability in Defender CSPM' which describes CIEM and its benefits. Another section below it is 'Upgrade to new Defender CSPM plan' with a link to upgrade.

Step 10: Create Recovery Service Vault

The screenshot shows the 'Create Recovery Services vault' wizard. At the top, there are two buttons: 'Help me create a vault' and 'Help me copy an existing vault settings'. Below them is a navigation bar with tabs: Basics, Redundancy, Encryption, Vault properties, Networking, Tags, and 'Review + create' (which is underlined). The 'Summary' step is selected. Under 'Basics', the configuration is as follows:

Subscription	Azure subscription 1
Resource group	RG-az104
Vault name	rsv-az104
Region	South Africa North

Under 'Redundancy', the settings are:

Backup Storage Redundancy	Geo-redundant
Cross Region Restore	Disable

Under 'Vault properties', the setting is:

Immutability	Disabled
--------------	----------

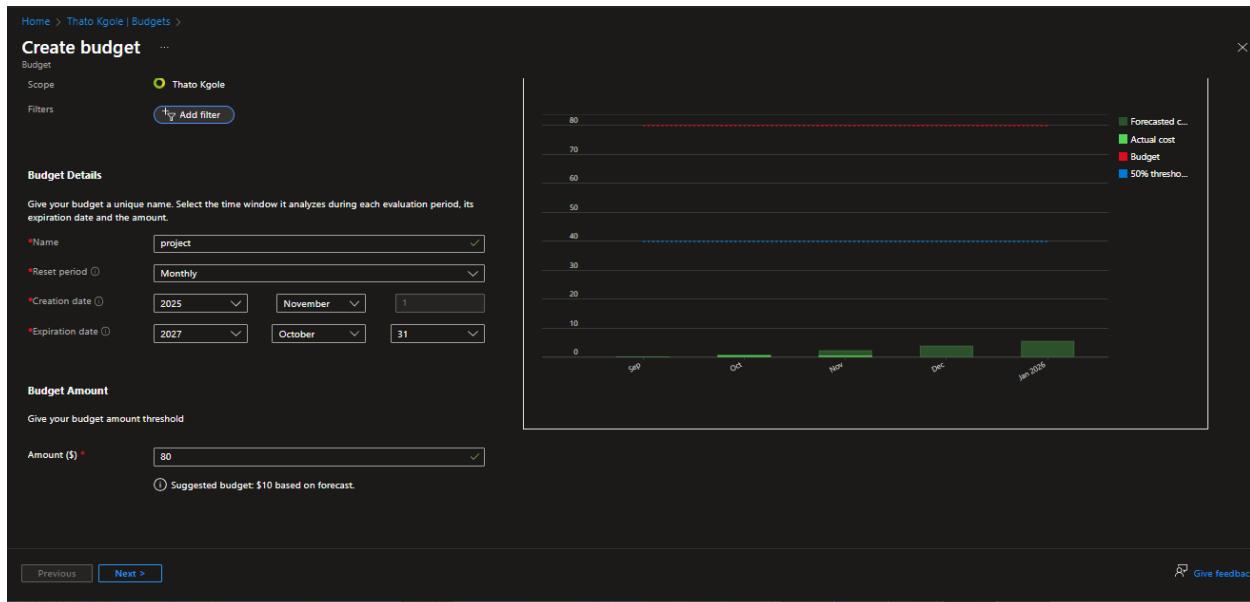
Under 'Networking', the setting is:

Connectivity method	Allow public access from all networks
---------------------	---------------------------------------

At the bottom, there are buttons for 'Create', 'Previous: Tags', 'Feedback', and 'Download a template for automation'.

Step 11: Set Budget & Alerts

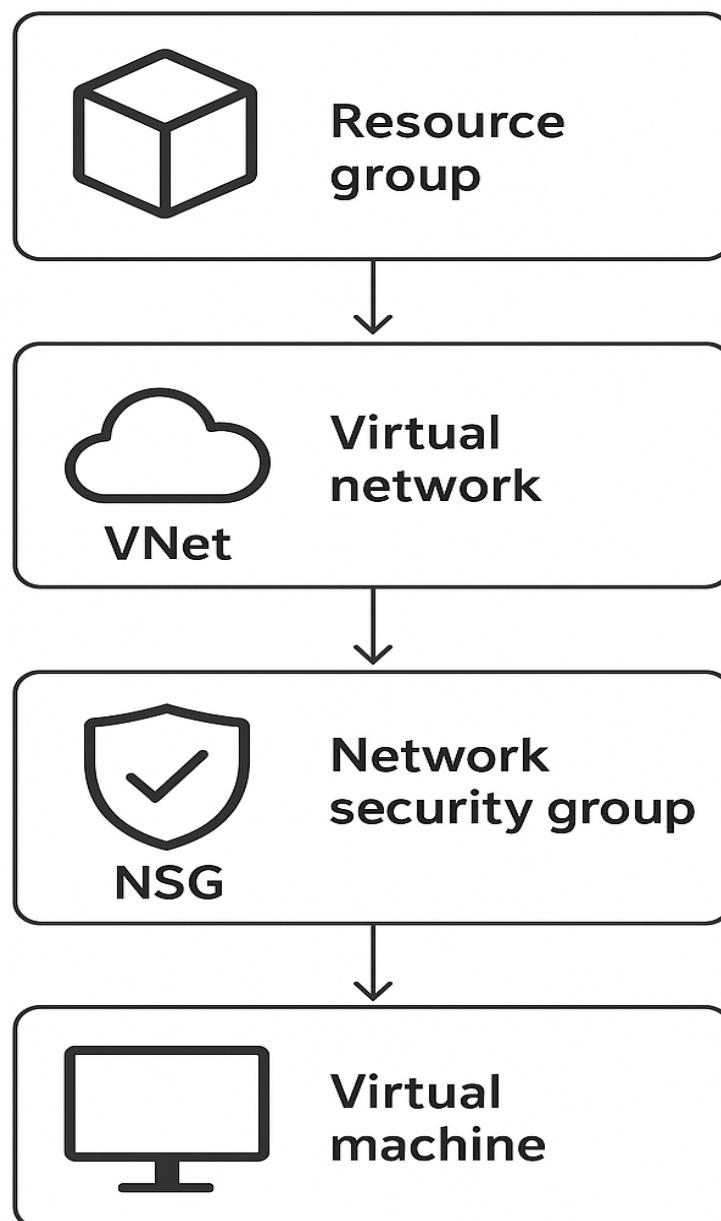
Configure monthly cost limit and email alert



Step 12: Resource Group showing All related content

Name	Type	Location
nsg-web	Network security group	South Africa North
rsv-az104	Recovery Services vault	South Africa North
vm-db	Virtual machine	South Africa North
vm-db-nsg	Network security group	South Africa North
vm-db90	Network Interface	South Africa North
vm-db_OsDisk_1_8335409aaebf45b8b3d2b790c5b	Disk	South Africa North
vm-web	Virtual machine	South Africa North
vm-web-ip	Public IP address	South Africa North
vm-web122	Network Interface	South Africa North
vm-web_OsDisk_1_d30bf287d6b440efaf0faf4f6c83	Disk	South Africa North
vnet-az104	Virtual network	South Africa North

DIAGRAM



LEARNING OUTCOME

.Deploy Azure Resources

.Understanding Networking, Security, Identity and cost control