LAB BY THATO KGOLE
DATE : 15 - 16 NOVEMBER 2025
CLOUD PLATFORM : MICROSOFT AZURE

Secure Secret Management Using Azure Key Vault & Managed Identity

OVERVIEW

This project implements a secure method for storing and accessing secrets in Azure using key vault and Managed Identity. The system ensures Virtual Machines can securely retrieve secrets without using passwords, stored credentials, or environment variables, following zero-trust and least privilege security principles.

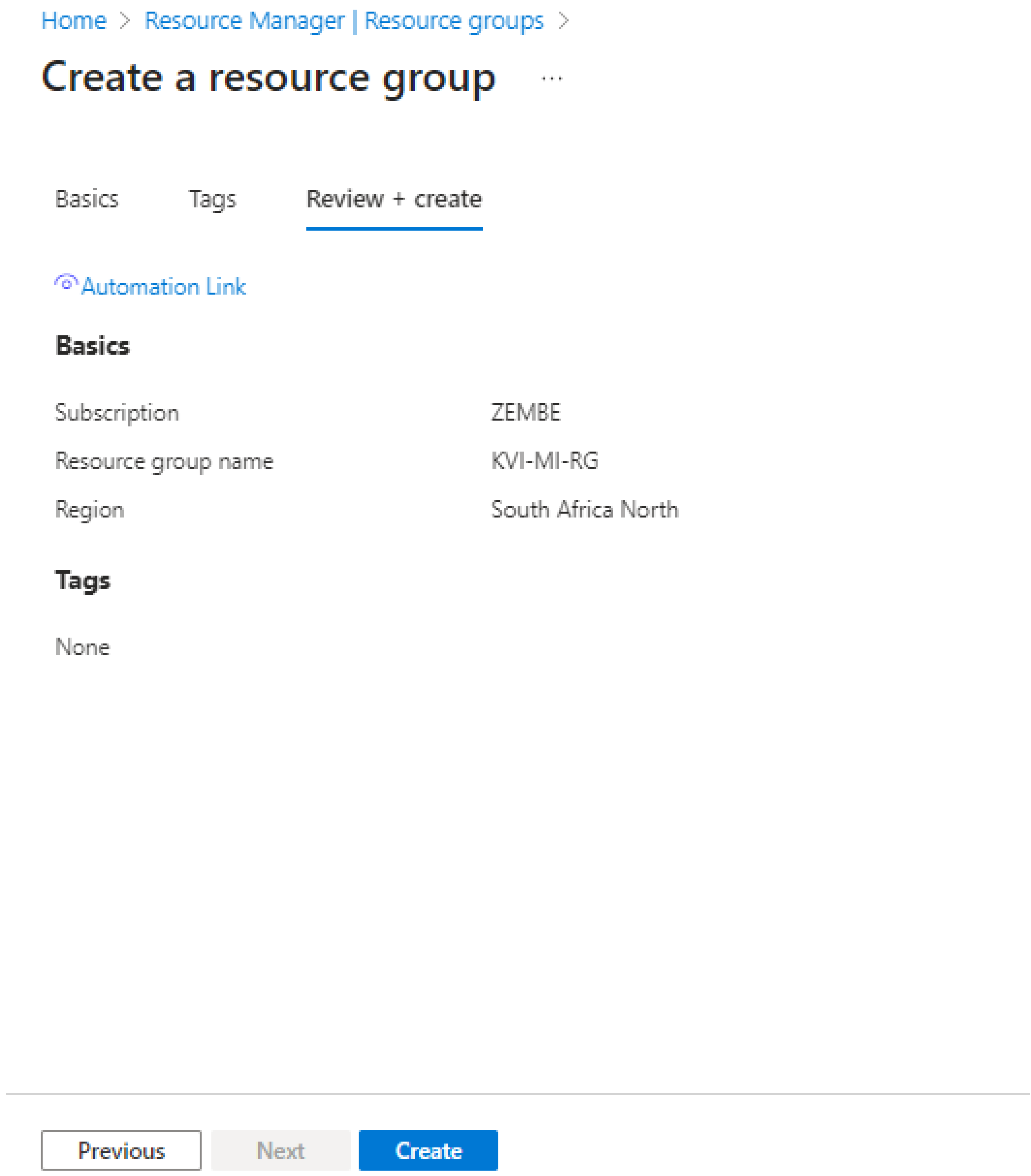
PROBLEM STATEMENT

Applications and workloads deployed in Azure often need sensitive values such as:
. Database passwords
. API Keys
. Connection strings

Storing these secrets directly onVMs or inside code is risky and violates security best practices. This project solves the problem by enabling a VM to securely retrieve a secret from Azure Key Vault using Managed Identity-meaning:
. No credentials are stored on the VM
. No hardcoded passwords
. Access is granted through RBAC
. Secrets stay protected inside Key Vault

IMPLEMENTATION STEPS

Step 1: Create Resource Group
To group all resources for the project



Create a resource group

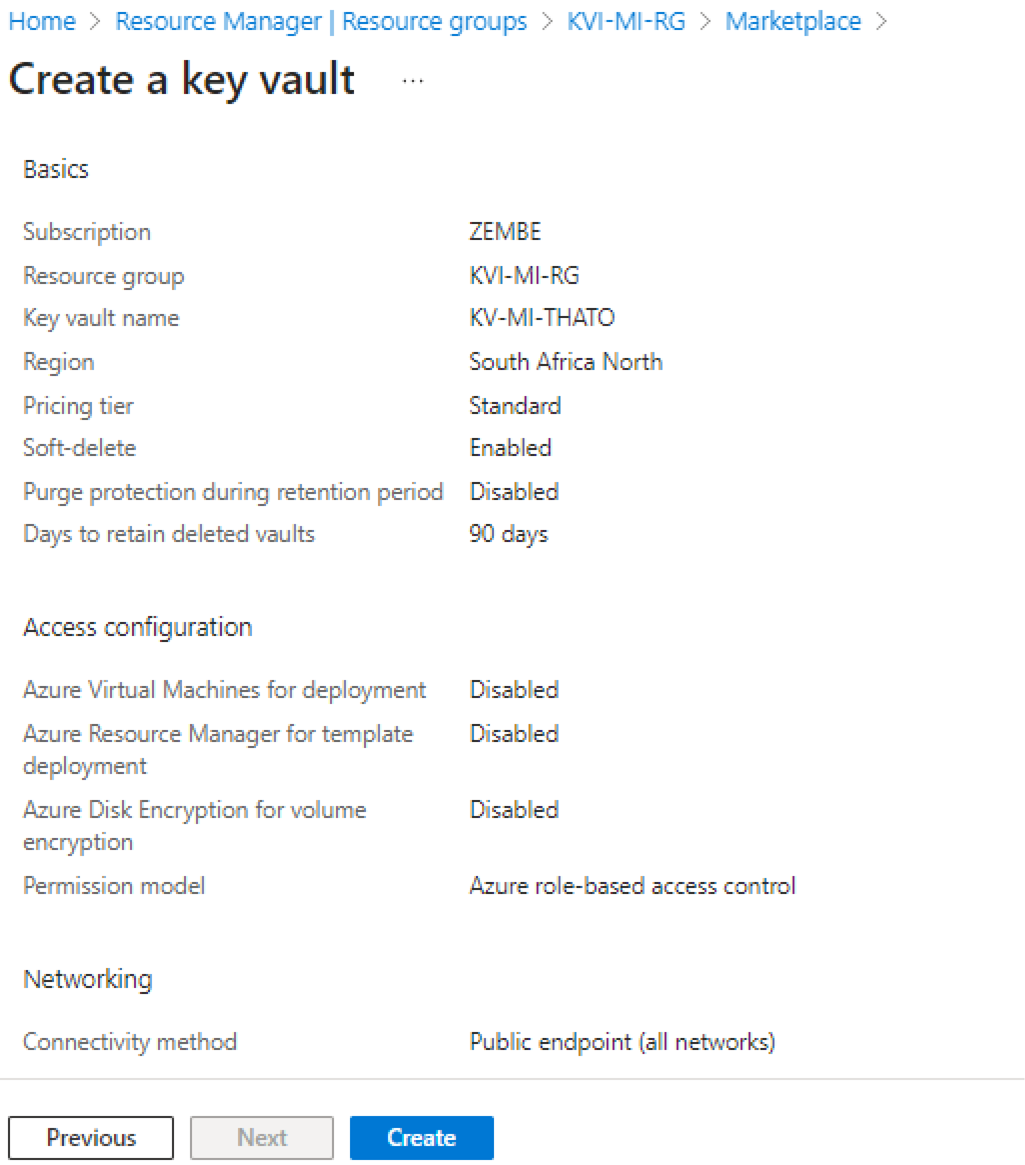
Basics

Subscription	ZEMBE
Resource group name	KVI-MI-RG
Region	South Africa North

Tags

None

Step 2: Deploy Azure Key Vault
To Store and Secure digital secrets


Home > Resource Manager | Resource groups > KVI-MI-RG > Marketplace >

Create a key vault

Basics

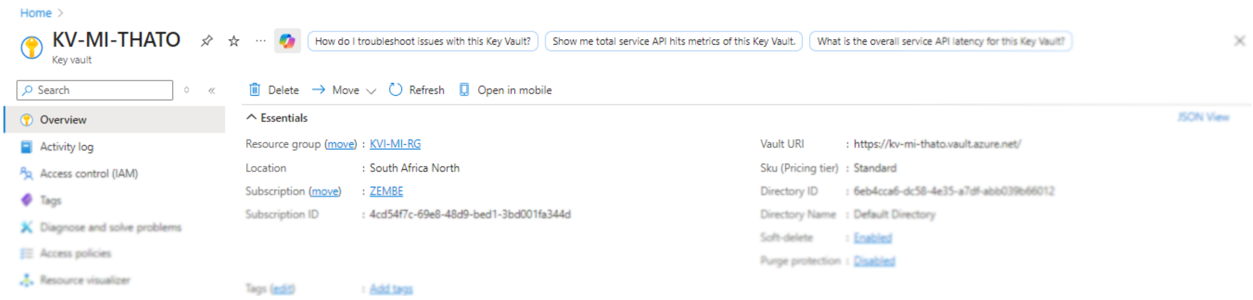
Subscription	ZEMBE
Resource group	KVI-MI-RG
Key vault name	KV-MI-THATO
Region	South Africa North
Pricing tier	Standard
Soft-delete	Enabled
Purge protection during retention period	Disabled
Days to retain deleted vaults	90 days

Access configuration

Azure Virtual Machines for deployment	Disabled
Azure Resource Manager for template deployment	Disabled
Azure Disk Encryption for volume encryption	Disabled
Permission model	Azure role-based access control

Networking

Connectivity method	Public endpoint (all networks)

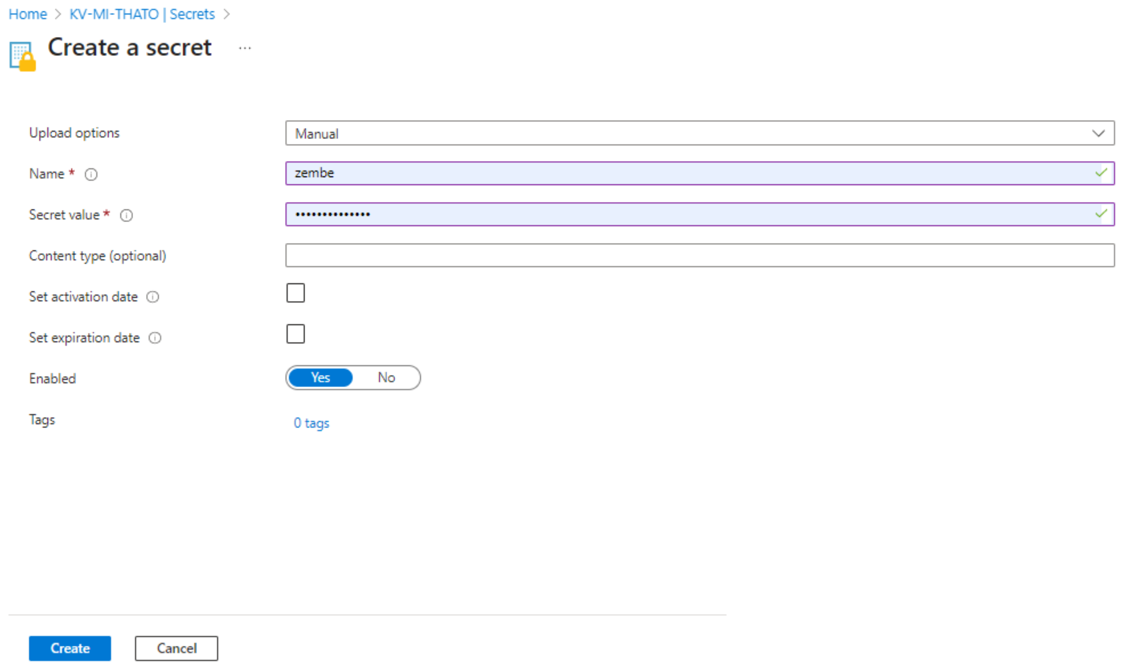

Home >
How do I troubleshoot issues with this Key Vault?
Show me total service API hits metrics of this Key Vault.
What is the overall service API latency for this Key Vault?
Search
Delete
Move
Refresh
Open in mobile
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Access policies
Resource visualizer
JSON View

KV-MI-THATO
Key vault

Essentials

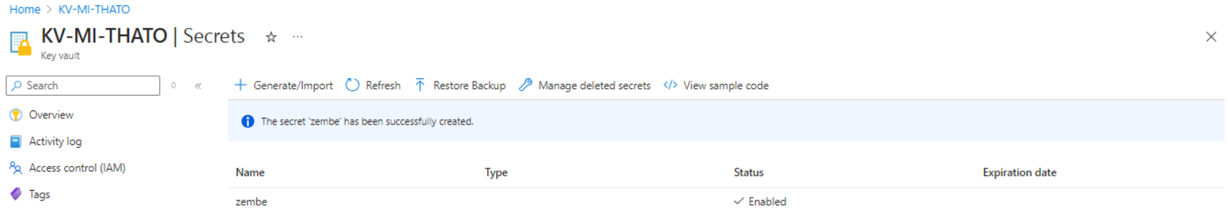
Resource group (move)	: KVI-MI-RG	Vault URI	: https://kv-mi-thato.vault.azure.net/
Location	: South Africa North	Sku (Pricing tier)	: Standard
Subscription (move)	: ZEMBE	Directory ID	: 6eb4cca6-dc58-4e35-a7df-abb039b66012
Subscription ID	: 4cd54f7c-69e8-48d9-bed1-3bd001fa344d	Directory Name	: Default Directory
		Soft-delete	: Enabled
		Purge protection	: Disabled
Tags (edit)	: Add tags		

Step 3: Add a Secret to Key Vault



Create a secret

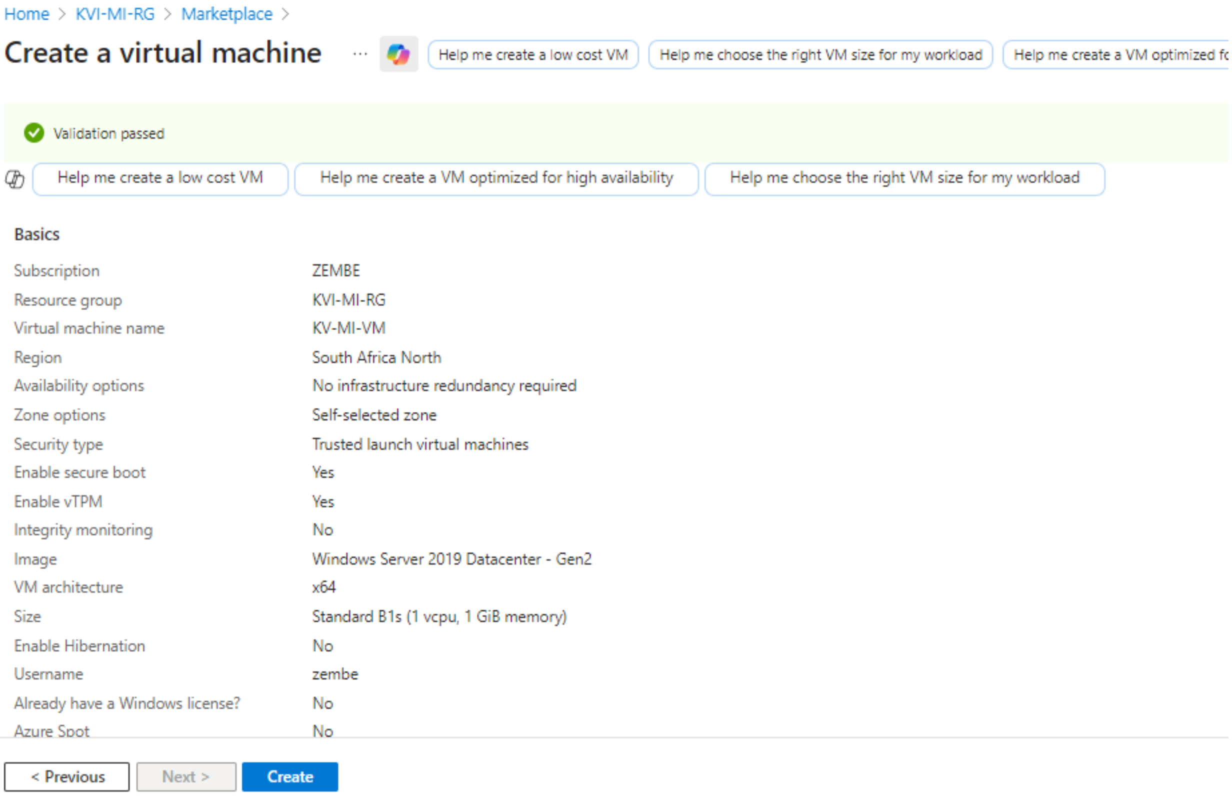
Upload options	Manual
Name *	zembe
Secret value *	••••••••••••••
Content type (optional)	
Set activation date	□
Set expiration date	□
Enabled	[✓ Yes] No
Tags	0 tags



The secret 'zembe' has been successfully created.

Name	Type	Status	Expiration date
zembe		✓ Enabled	

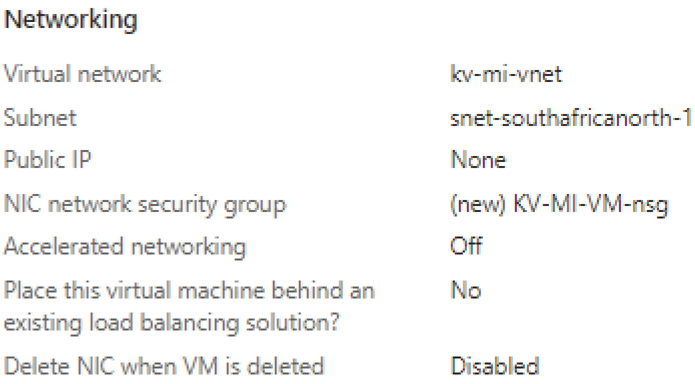
Step 4: Create Virtual Machine


Home > KVI-MI-RG > Marketplace >
Create a virtual machine
Help me create a low cost VM
Help me choose the right VM size for my workload
Help me create a VM optimized fc
Help me create a VM optimized for high availability
< Previous
Next >
Create

Validation passed

Basics

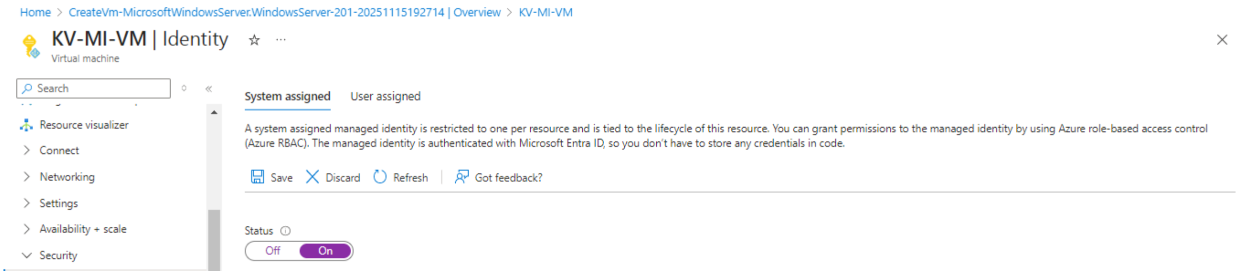
Subscription	ZEMBE
Resource group	KVI-MI-RG
Virtual machine name	KV-MI-VM
Region	South Africa North
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image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



Networking

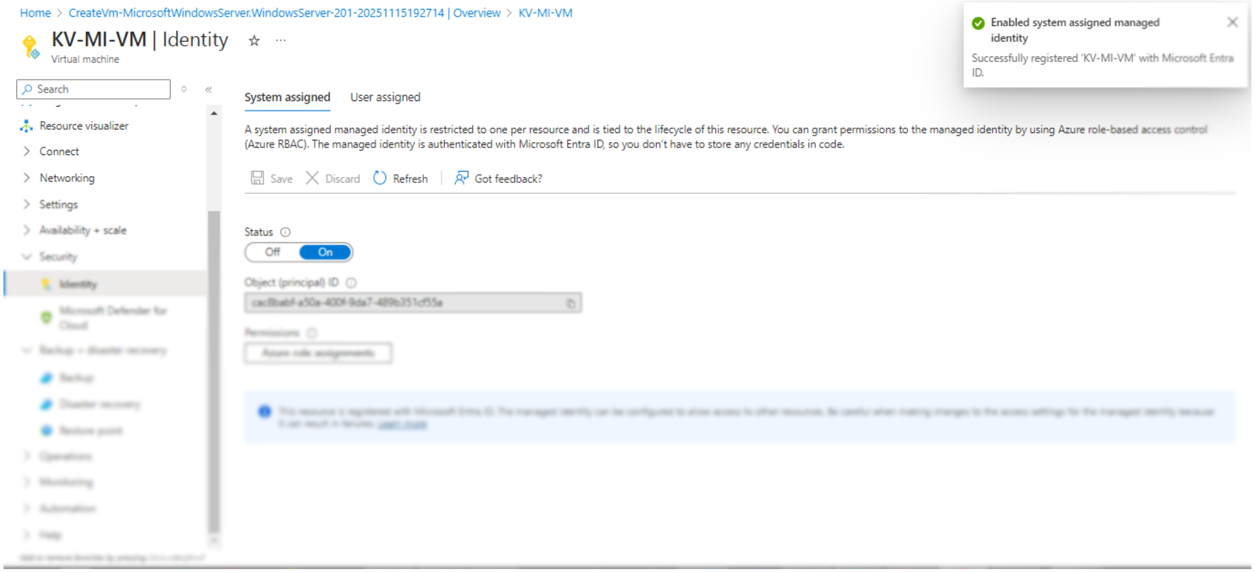
Virtual network	kv-mi-vnet
Subnet	snet-southafricanorth-1
Public IP	None
NIC network security group	(new) KV-MI-VM-nsg
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No
Delete NIC when VM is deleted	Disabled

Step 5: Enable Managed Identity



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.

Status: Off [✓ On]



Enabled system assigned managed identity

Successfully registered 'KV-MI-VM' with Microsoft Entra ID.

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.

Status: Off [✓ On]

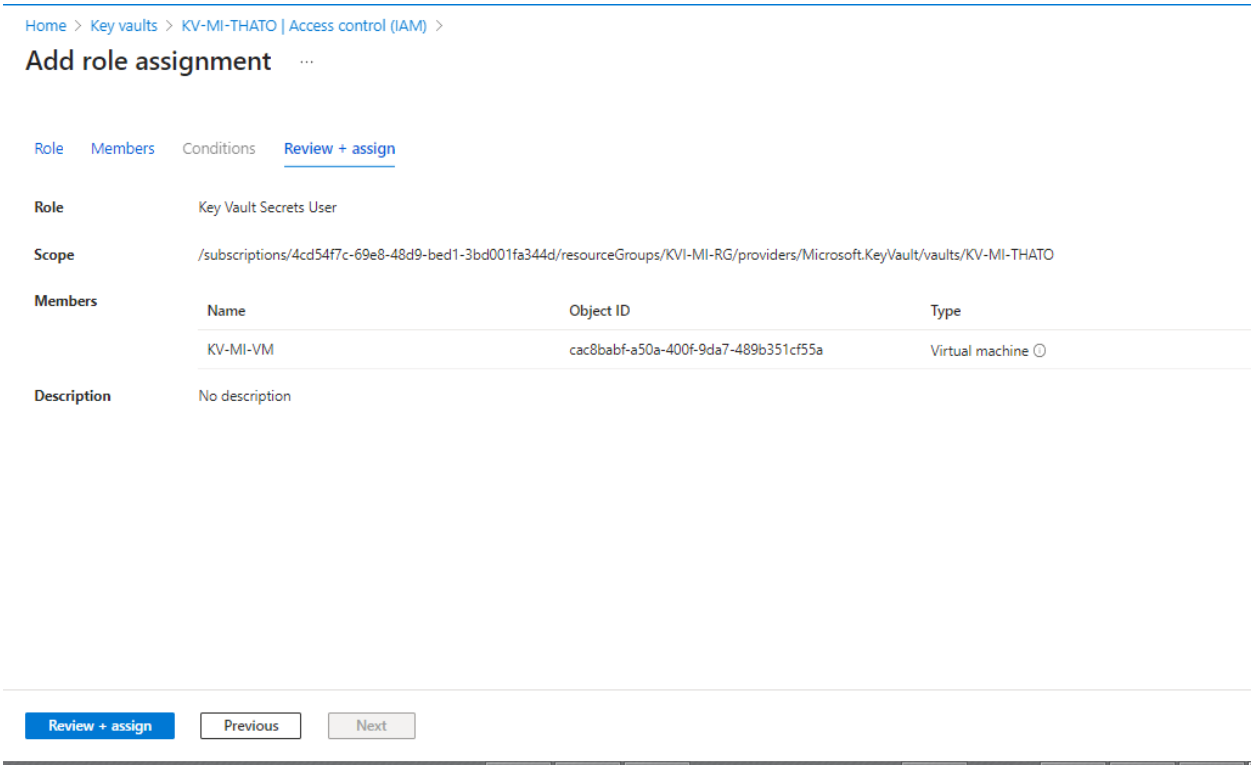
Object (principal) ID: cac8babf-a50a-400f-9da7-489b351cf55a

Permissions

This resource is registered with Microsoft Entra ID. The managed identity can be configured to allow access to other resources. Be careful when making changes to the access settings for the managed identity because it can result in failures. Learn more

Step 6: Assign RBAC Role to the VM

VM access Key



Add role assignment ...

Role Key Vault Secrets User

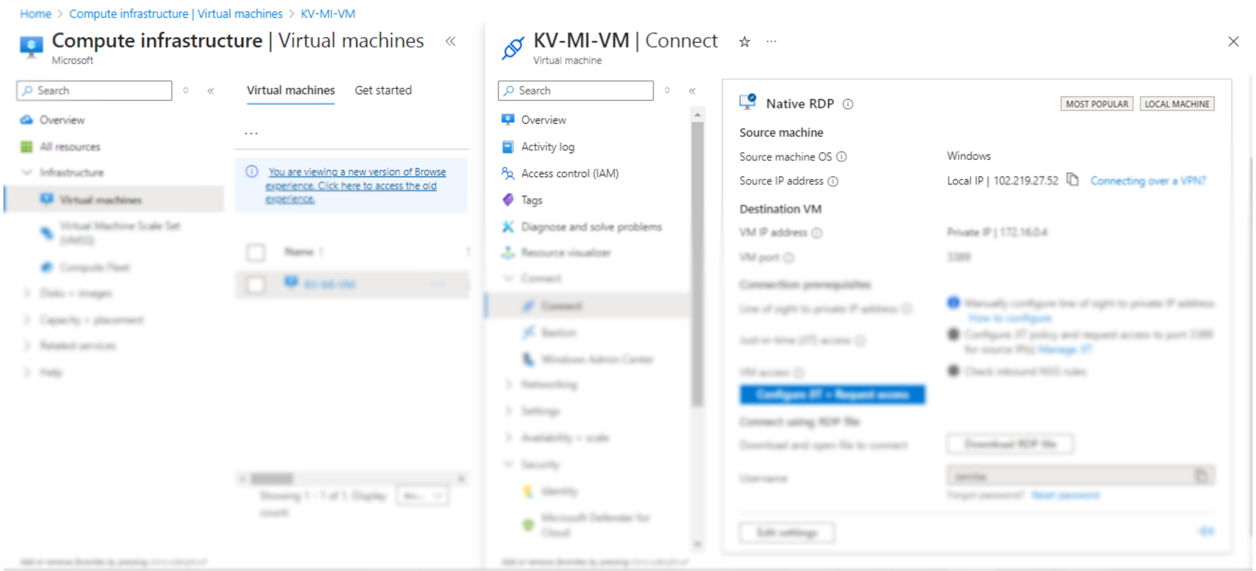
Scope /subscriptions/4cd54f7c-69e8-48d9-bed1-3bd001fa344d/resourceGroups/KVI-MI-RG/providers/Microsoft.KeyVault/vaults/KV-MI-THATO

Members

Name	Object ID	Type
KV-MI-VM	cac8babf-a50a-400f-9da7-489b351cf55a	Virtual machine ⓘ

Description No description

Step 7: Retrieve Secret From Key Vault



Home > Compute infrastructure | Virtual machines > KV-MI-VM
Compute infrastructure | Virtual machines
Microsoft
Search
Overview
All resources
Infrastructure
Virtual machines
Virtual Machine Scale Set (VMSS)
Compute Fleet
Disks + images
Capacity + placement
Related services
Help
Virtual machines
Get started
You are viewing a new version of Browse experience. Click here to access the old experience.
Name
KV-MI-VM
KV-MI-VM | Connect
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Connect
Bastion
Windows Admin Center
Networking
Settings
Availability + scale
Security
Identity
Microsoft Defender for Cloud
Native RDP ⓘ
MOST POPULAR
LOCAL MACHINE

Source machine

Source machine OS ⓘ Windows

Source IP address ⓘ Local IP | 102.219.27.52 Connecting over a VPN?

Destination VM

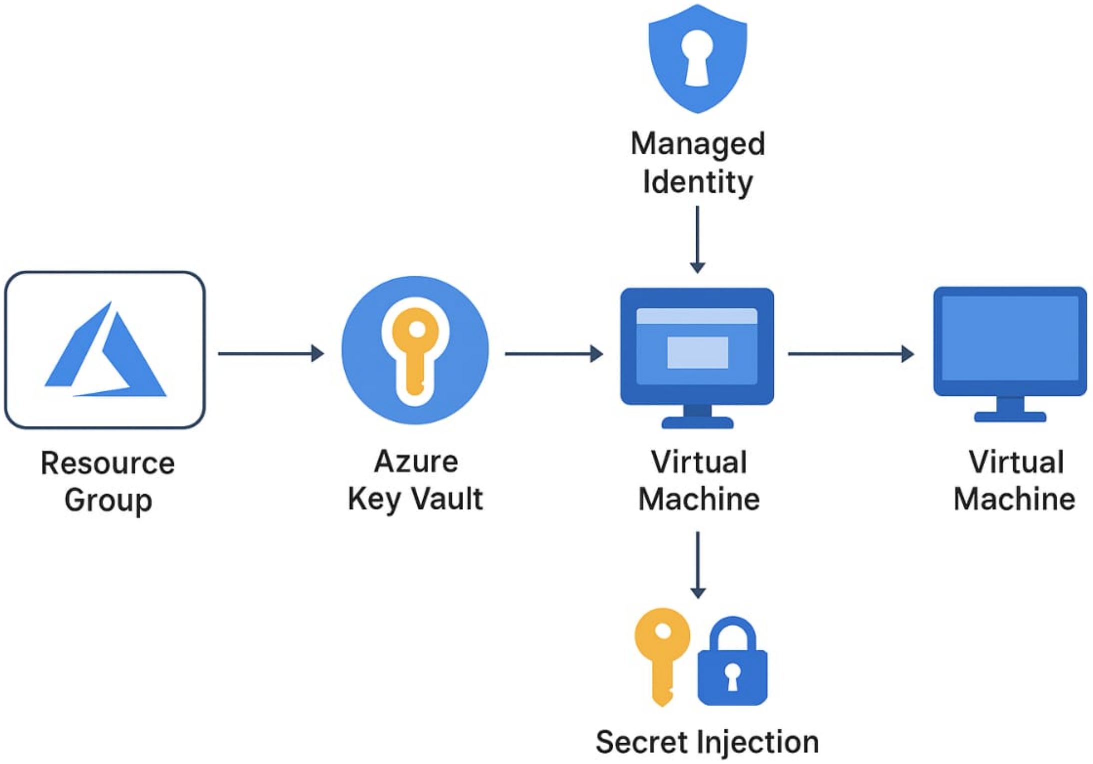
VM IP address ⓘ Private IP | 172.16.0.4

VM port ⓘ 3389

Connection prerequisites

Line of sight to private IP address ⓘ
Just-in-time (JIT) access ⓘ
VM access ⓘ
Manually configure line of sight to private IP address
How to configure
Configure JIT policy and request access to port 3389 for source IP(s) Manage JIT
Check inbound NSG rules
Configure JIT + Request access
Connect using RDP file
Download and open file to connect
Download RDP file
Username
Forgot password? Reset password
Edit settings

DIAGRAM


Managed Identity
Resource Group
Azure Key Vault
Virtual Machine
Virtual Machine
Secret Injection