LAB BT THATO KGOLE
DATE : 17 - 18 NOVEMBER 2025
CLOUD PLATFORM : MICROSOFT AZURE

Secure Virtual Machine Access Using JIT-Style Authentication Without Bastion

OVERVIEW

This project demonstrates how to secure an Azure Virtual Machine (Windows Server) without exposing RDP to the internet, using a JIT-style (just in time) access workflow built entirely with free tier services

Instead of Azure Bastion or Defender for Cloud JIT (both paid), the project implements:
. A locked-down Network Security Group
. Time-bound access controlled manually
. NSG change detection
. Real-time email alerts using Azure Monitor

PROBLEM STATEMENT

Virtual Machines exposed to the internet through RDP (port 3389) are vulnerable to:
. Brute-force attacks
. Port scanning
. Credential stuffing
. Persistent attack probing

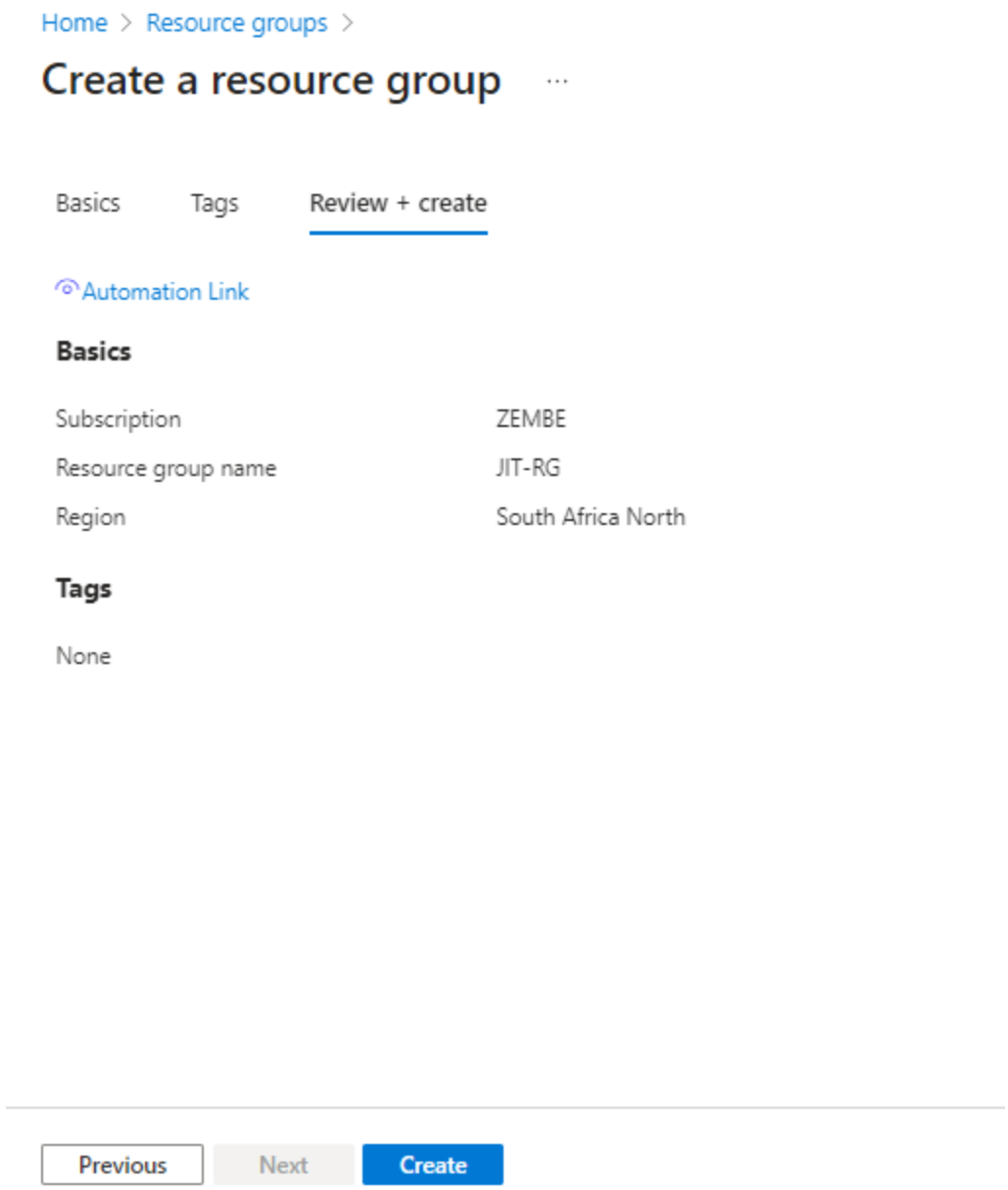
Organizations often use Bastion or paid JIT features - but these require higher subscription tiers.

GOAL

Secure a VM without Bastion, Defender for Cloud, or any paid features while maintaining operational access.

IMPLEMENTATION STEPS

Step 1: Create Resource Group
Logical container for all resources



Step 2: Create Virtual Network + Subnet
Private network environment for the VM.

Create virtual network ...

Validation passed

Basics Security IP addresses Tags Review + create

Subscription	ZEMBE
Resource Group	JIT-RG
Name	Jit-Vnet
Region	South Africa North

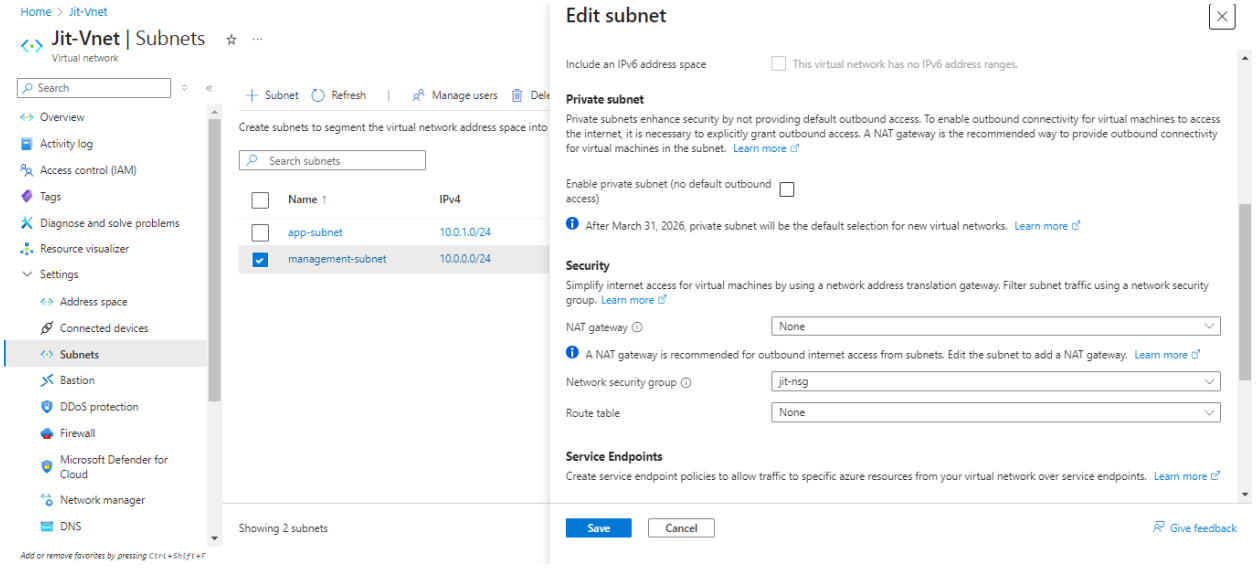
Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

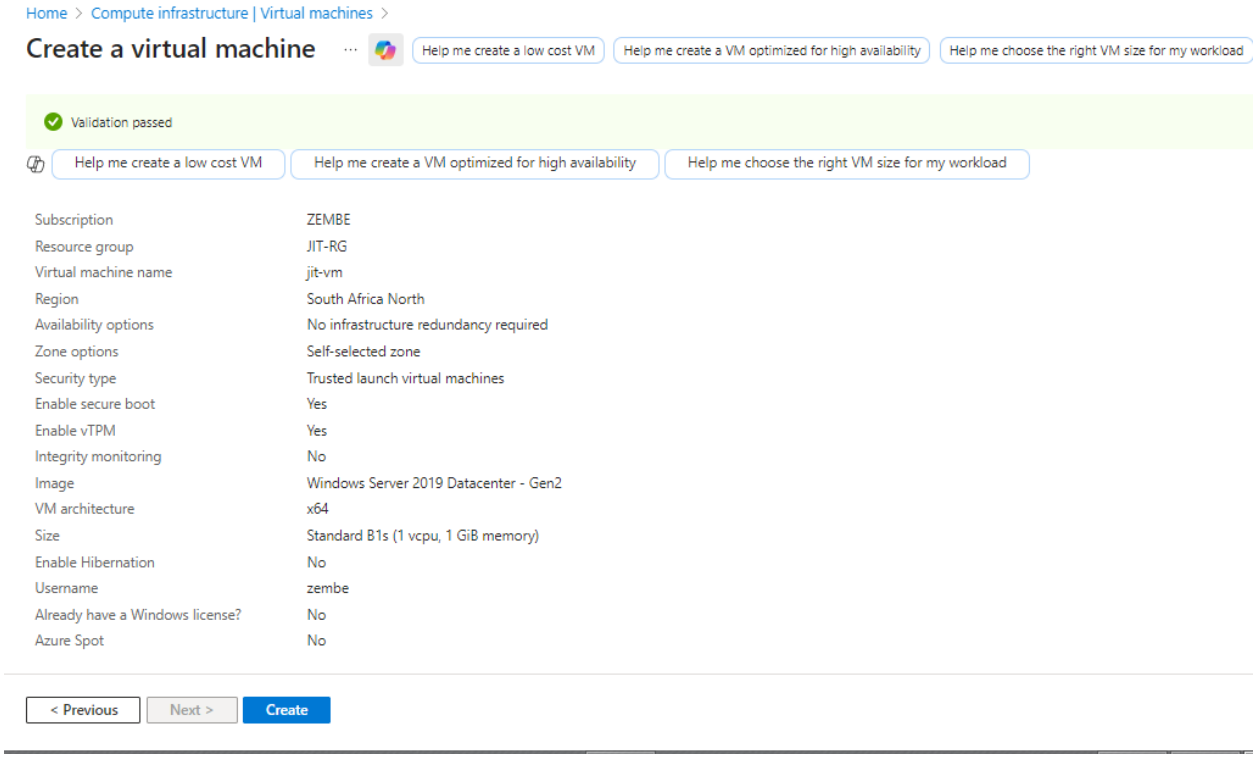
IP addresses

Address space	10.0.0.0/16 (65,536 addresses)
Subnet	management-subnet (10.0.0.0/24) (256 addresses)
Subnet	app-subnet (10.0.1.0/24) (256 addresses)

Previous Next Create Download a template for automation



Step 3: Deploy Windows VM (No Public Access)
A VM that cannot be accessed by default.



Disks

OS disk size	Image default
OS disk type	Standard SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

Networking

Virtual network	Jit-Vnet
Subnet	app-subnet
Public IP	None
NIC network security group	None
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No
Delete NIC when VM is deleted	Enabled

< Previous | Next > | Create

Step 4: Lock Down the Network Security Group

Home > Network foundation | Network security groups >

Create network security group ...

Validation passed

Basics | Tags | Review + create

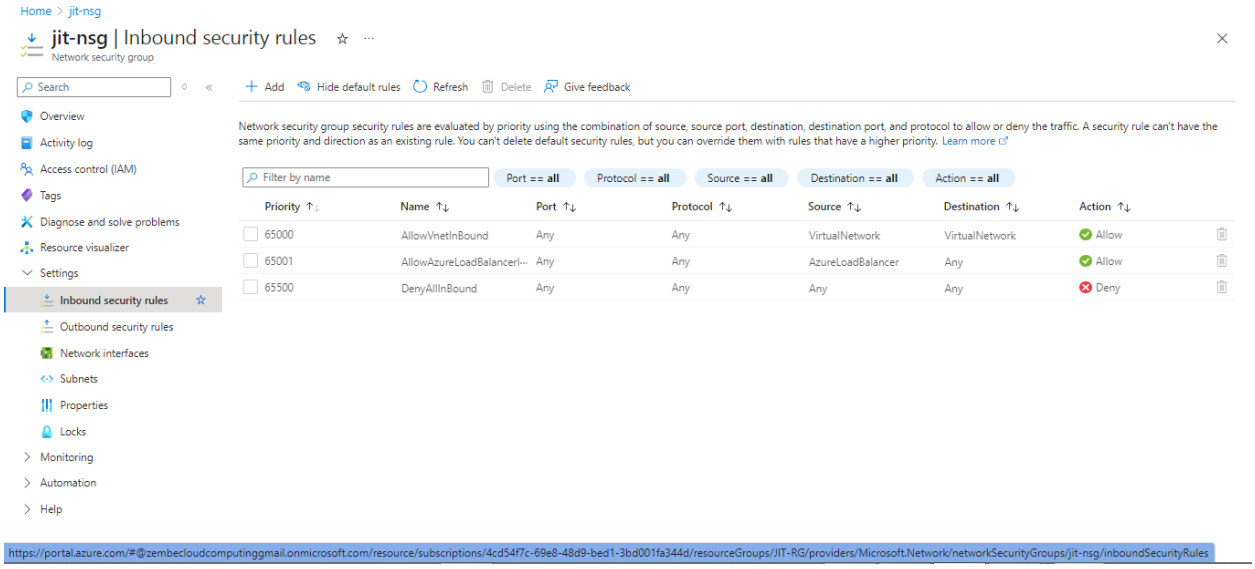
Basics

Subscription	ZEMBE
Resource group	JIT-RG
Region	South Africa North
name	jit-nsg

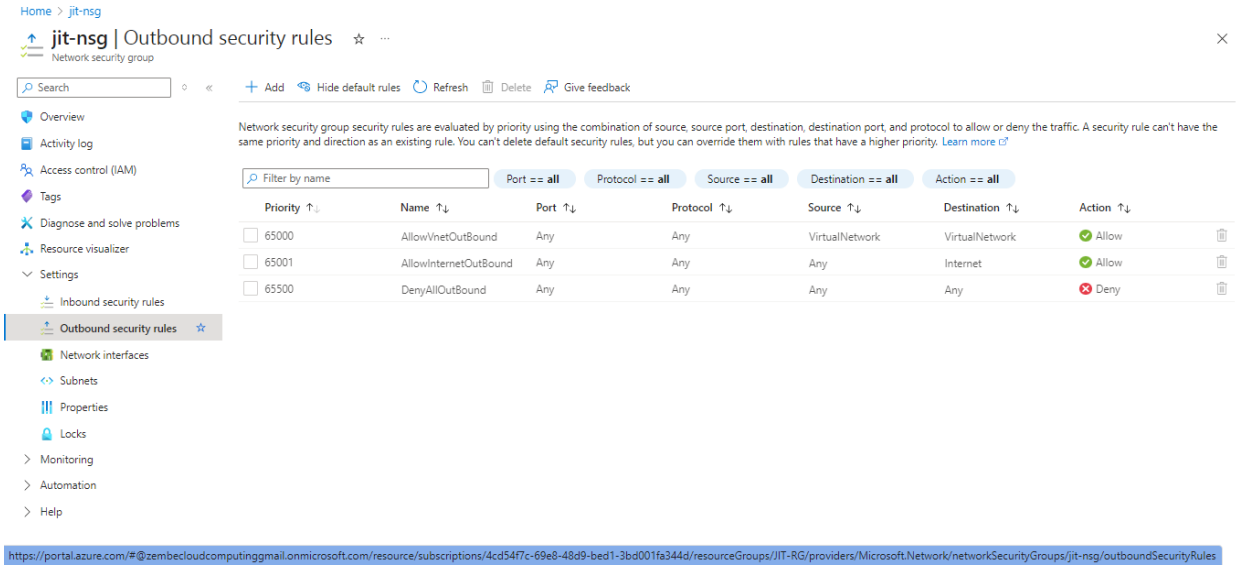
Tags

None

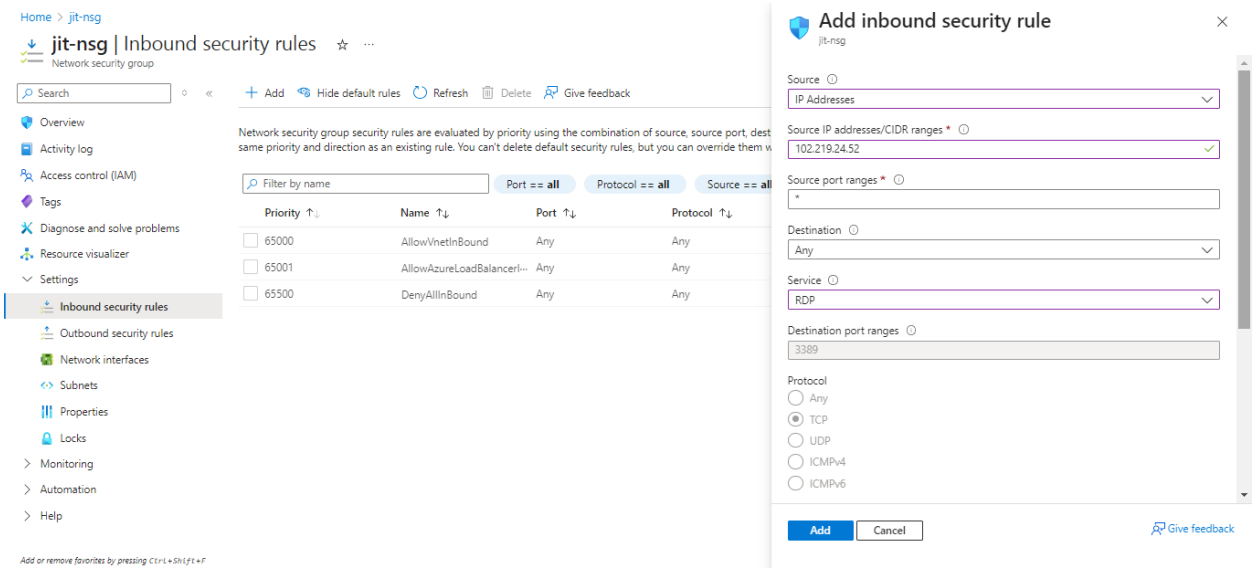
Create | < Previous | Next > | Download a template for automation



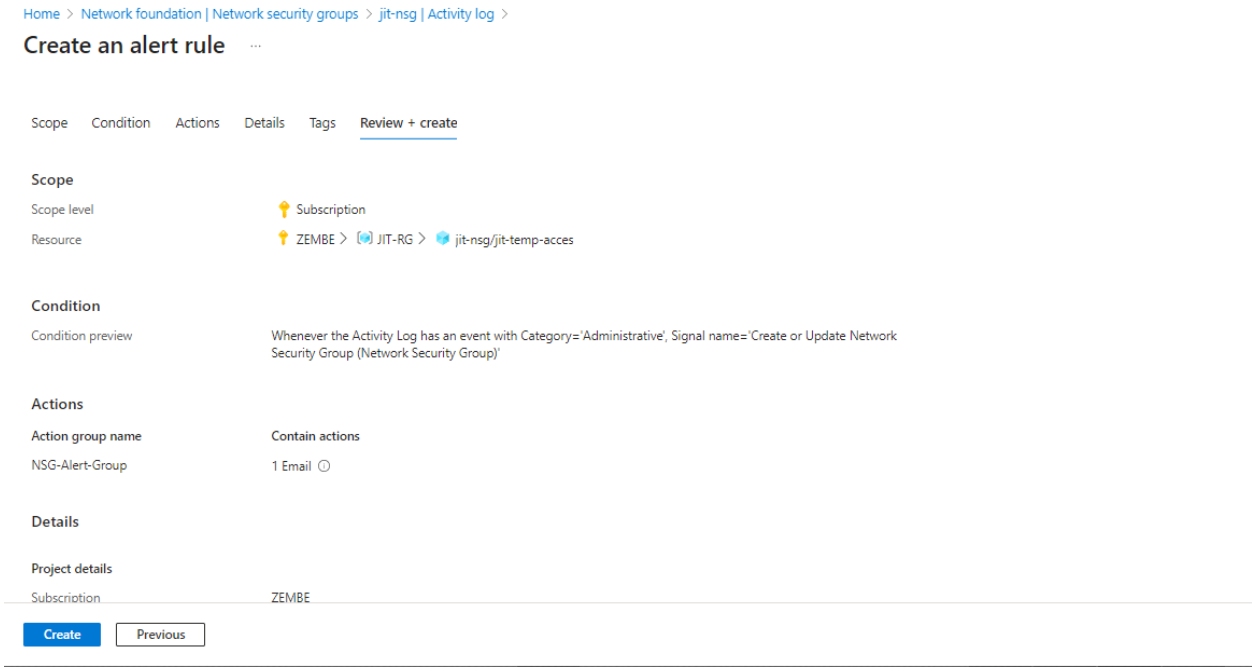
https://portal.azure.com/#@zembecloudcomputinggmail.onmicrosoft.com/resource/subscriptions/4cd54f7c-69e8-48d9-bed1-3bd001fa344d/resourceGroups/JIT-RG/providers/Microsoft.Network/networkSecurityGroups/jit-nsg/inboundSecurityRules



https://portal.azure.com/#@zembecloudcomputinggmail.onmicrosoft.com/resource/subscriptions/4cd54f7c-69e8-48d9-bed1-3bd001fa344d/resourceGroups/JIT-RG/providers/Microsoft.Network/networkSecurityGroups/jit-nsg/outboundSecurityRules



Step 5: Configure Azure Monitor Alert
To detect any time someone opens port 3389 - even for a moment



Home > Network foundation | Network security groups > jit-nsg | Activity log >

Create an alert rule ...

Condition

Condition preview	Whenever the Activity Log has an event with Category='Administrative', Signal name='Create or Update Network Security Group (Network Security Group)'

Actions

Action group name	Contain actions
NSG-Alert-Group	1 Email

Details

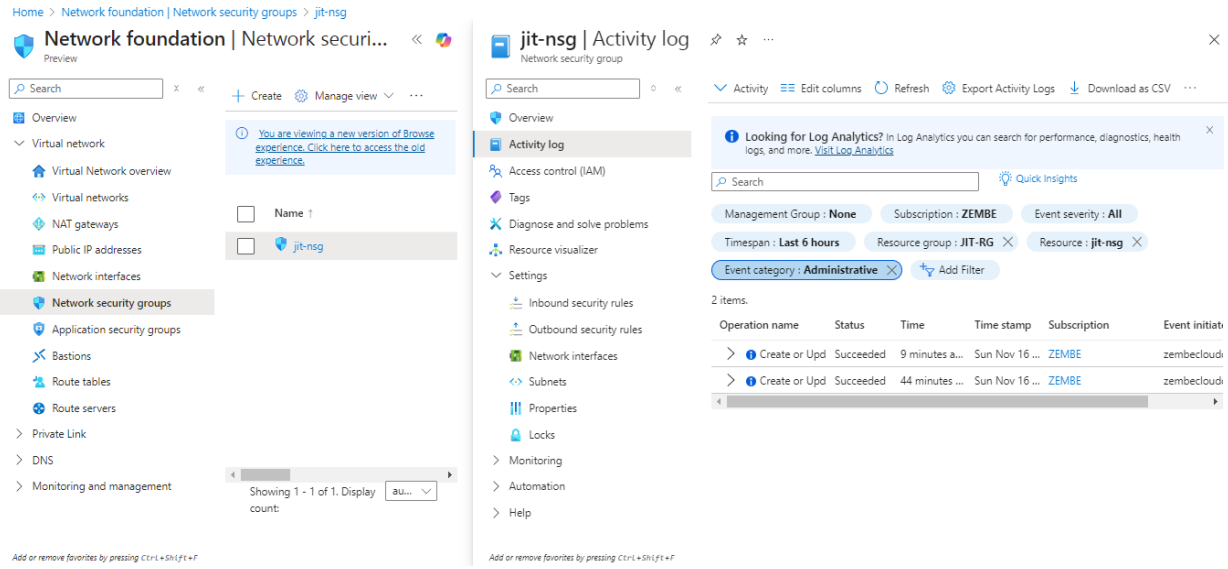
Project details

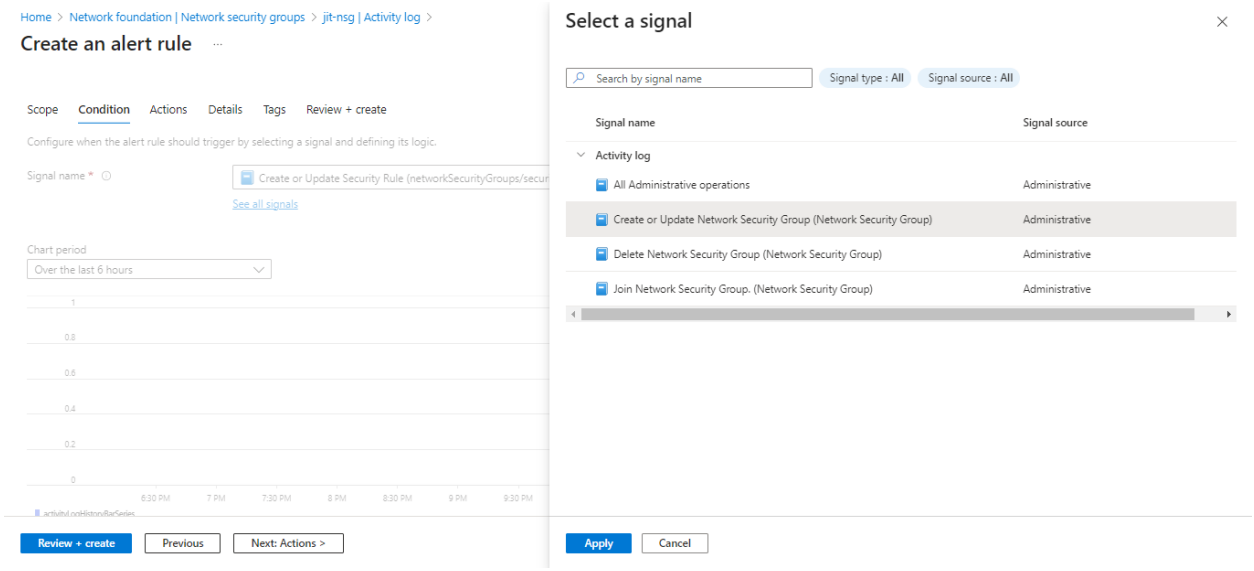
Subscription	ZEMBE
Resource group	JIT-RG
Region	global

Alert rule details

Alert rule name	NSG RDP Access Change Alert
Alert rule description	Triggers when any Network Security Group rule is created or updated, including opening RDP (3389). Helps detect unauthorized access.
Enable upon creation	☑

Create | Previous



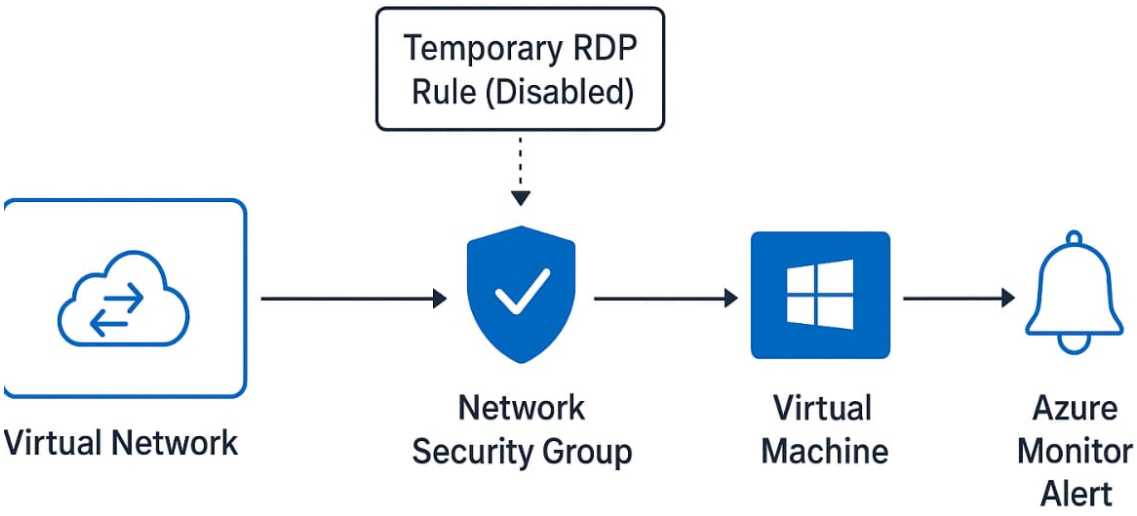


Step 6: Test Scenario (Documented)
> Modify the RDP rule to allow your public IP
> Save the rule
> Azure Monitor detects the change
> Action Group sends an email alert

Learning Outcome

. NSG firewall design
. Zero-Trust network access
. How to manually implement a free JIT-style model
. Monitoring NSG changes
. Creating alert rules & action groups
. Least privilege security governance
. Real - world security operations workflow

Diagram



Secure VM with JIT-Style Access (No Bastion)