

Azure Virtual Machine Provisioning using Terraform

- We will provision the Azure Virtual Machine using Terraform as an Infrastructure as Code.
 - We will deploy it in a custom Virtual Network for isolation.
 - We will SSH into the Virtual Machine, install the docker.
 - Then, we will deploy the Nginx Container and try accessing it on the Web Browser.
-

Prerequisites

1. Azure Account with Subscription.
 2. Terraform installed.
-

Write Terraform Configuration files

First we will write Terraform configuration files for AWS resources using predefined modules available on the internet.

Steps

1. Create the **virtual-machine-terraform** directory.
2. The folder structure for the above-created directory is as follows:

```
virtual-machine-terraform
├── .terraform.lock.hcl
├── locals.tf
├── main.tf
├── outputs.tf
├── providers.tf
├── terraform.tfstate
├── terraform.tfstate.backup
└── .terraform
```

We need to only create *providers.tf*, *main.tf*, *outputs.tf*, & *locals.tf* file. Other files are generated while initiating terraform.

3. Create a *providers.tf* file inside the above-created directory.
4. Inside it, define the following:
 - terraform
 - required_providers
 - provider
 - azurearm
5. Click [code](#) for reference.
6. The definition of *providers.tf* file is complete.

7. Now, create the *main.tf* file.
8. Inside *main.tf* file, we will use the following predefined modules:
 - module.resource-group
 - module.virtual-network
 - module.virtual-machine
9. Click [code](#) for reference.
10. The definition of *main.tf* file is complete.
11. Now we will create *outputs.tf* file.
12. Inside it, define the following outputs.
 - output.vm-public-ip
13. Click [code](#) for reference.
14. The definition of *outputs.tf* file is complete.
15. Now we will create *locals.tf* file.
16. Inside it, define the following variables:
 - local.resource-group-properties
 - local.virtual-network-properties
 - local.virtual-machine-properties
17. Click [code](#) for reference.
18. The definition of *locals.tf* file is complete.

Ensure you give the appropriate values to the variables defined in *locals.tf* file.

Provisioning the Infrastructure

Now we will provision the Azure infrastructure by applying the above-created configuration files.

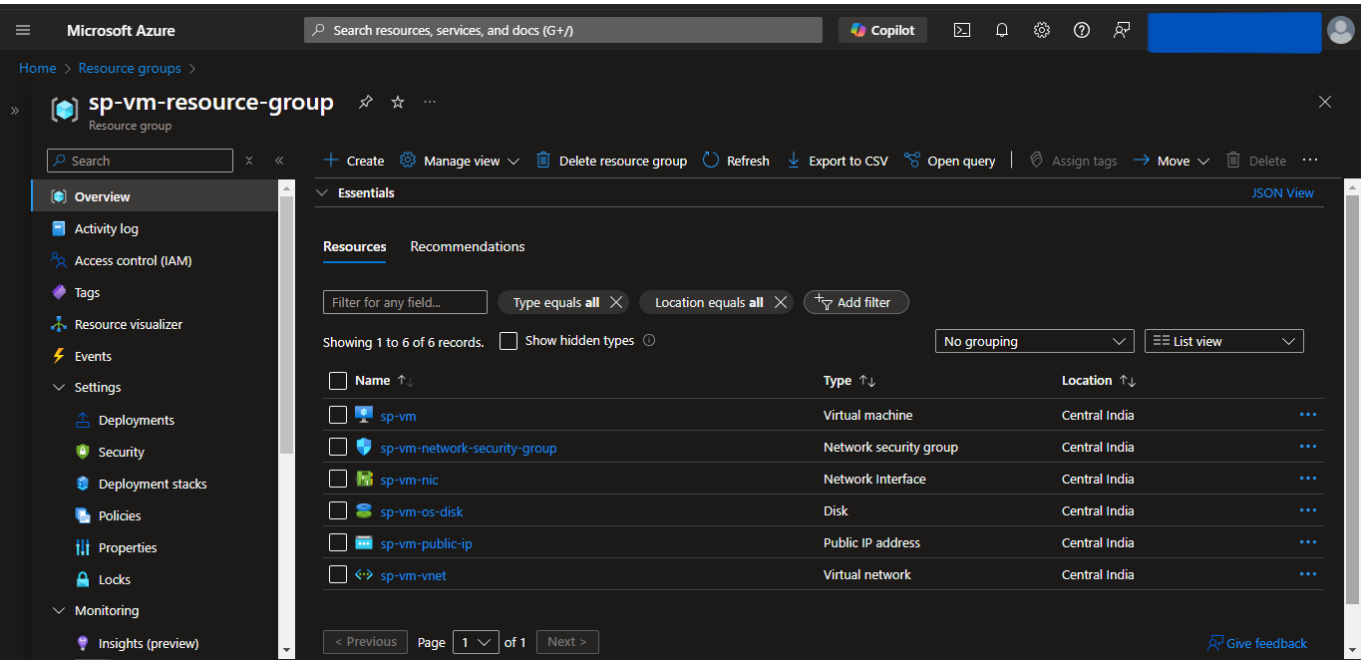
Ensure Azure CLI is configured with appropriate Azure Account credentials with enough permissions.

Steps:

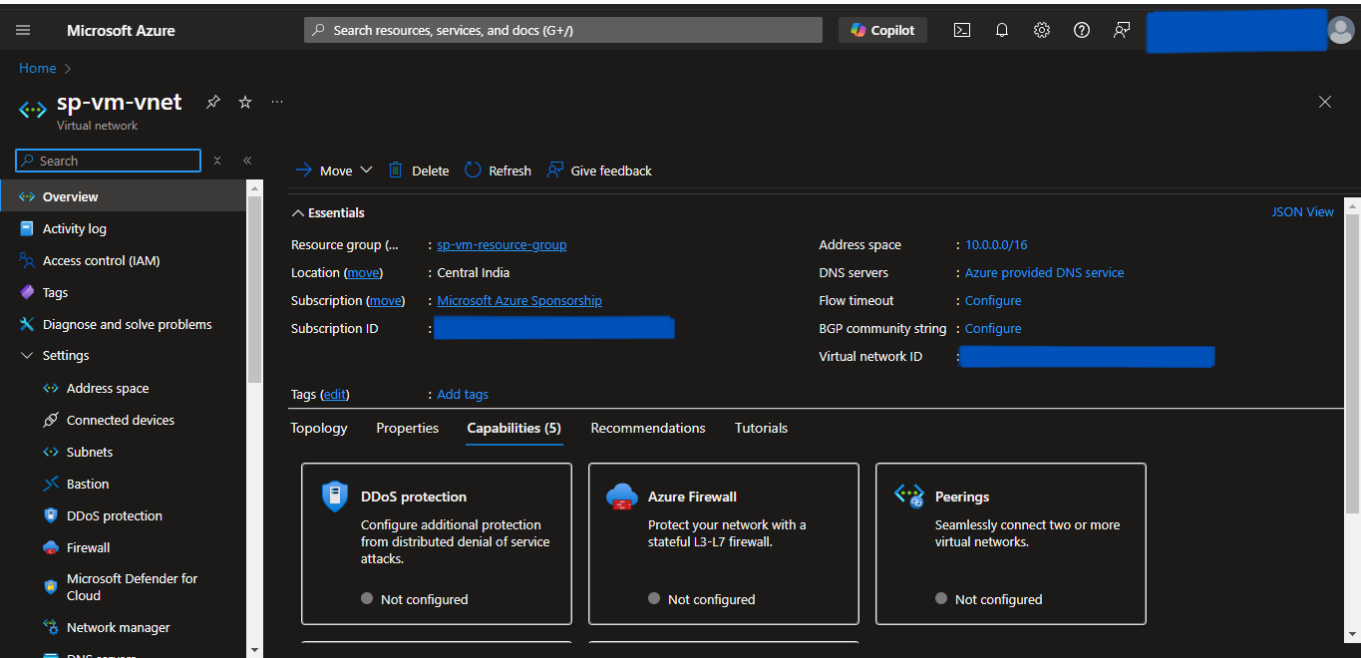
1. Open the PowerShell Window.
 2. Change the directory to the above-created **virtual-machine-terraform** directory using the **cd** command.
 3. Run the **terraform fmt -recursive** command to format the syntax of the files.
 4. Run the **terraform init** command to initialize the *terraform*.
 5. Run the **terraform validate** command to validate the configuration files.
 6. Run the **terraform plan** command to plan the resources to be created.
 7. Run the **terraform apply** command and if prompted, type **yes** to provision the infrastructure.
 8. Run the **terraform output** command to get the values of defined variables in *outputs.tf* file.
 9. Head to the Azure Console, and verify the created resources.
-

Screenshots of Provisioned Infrastructure

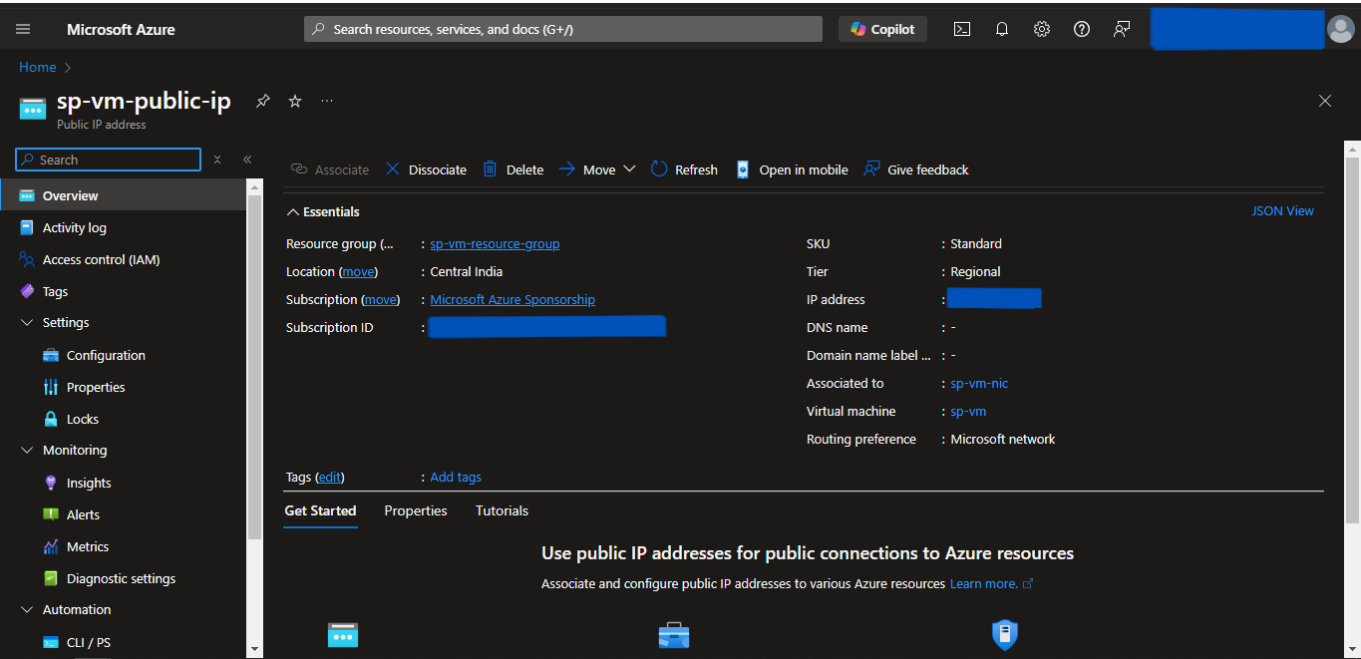
Resource Group Image



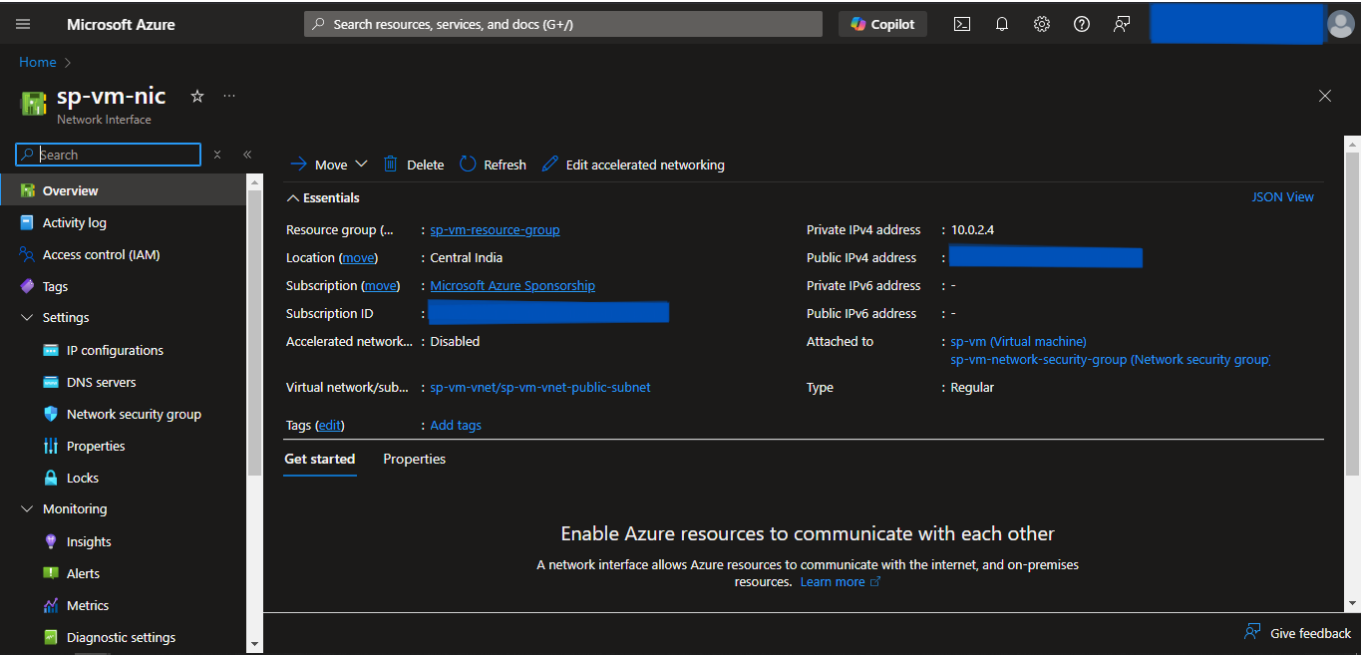
Virtual Network Image



Public IP Image



Network Interface Card Image



Network Security Group Image

Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

Home > sp-vm-nic >

sp-vm-network-security-group

Network security group

✦ ☆ ...

✕

Search

✕

«

→ Move

🗑 Delete

🔄 Refresh

💬 Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnostic settings

Essentials

JSON View

Resource group (move) : sp-vm-resource-group

Location : Central India

Subscription (move) : Microsoft Azure Sponsorship

Subscription ID :

Tags (edit) : Add tags

Custom security rules : 3 inbound, 0 outbound

Associated with : 0 subnets, 1 network interfaces

Filter by name

Port == all

Protocol == all

Source == all

Destination == all

Action == all

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
Inbound Security Rules						
100	ssh-inbound	22	Tcp	Any	Any	Allow
200	http-inbound	80	Tcp	Any	Any	Allow
300	https-inbound	443	Tcp	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Virtual Machine Image

Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

Home >

sp-vm

Virtual machine

✦ ☆ ...

✕

Search

✕

«

🔗 Help me copy this VM in any region

🔗 Connect

▶ Start

↺ Restart

⏏ Stop

⌌ Hibernate

📷 Capture

🗑 Delete

🔄 Refresh

📱 Open in mobile

💬 Feedback

🔗 CU / PS

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Networking

Network settings

Load balancing

Application security groups

Network manager

Settings

Disks

Essentials

JSON View

Resource group (move) : SP-VM-RESOURCE-GROUP

Status : Running

Location : Central India

Subscription (move) : Microsoft Azure Sponsorship

Subscription ID :

Operating system : Linux (ubuntu 22.04)

Size : Standard DS1 v2 (1 vcpu, 3.5 GiB memory)

Public IP address :

Virtual network/subnet : sp-vm-vnet/sp-vm-vnet-public-subnet

DNS name : Not configured

Health state : -

Time created : 1/9/2025, 3:48 AM UTC

Tags (edit) : Add tags

Properties

Monitoring

Capabilities (7)

Recommendations

Tutorials

Virtual machine

Computer name : sp-vm

Operating system : Linux (ubuntu 22.04)

Networking

Public IP address : (Network interface sp-vm-nic)

Public IP address (IPv6) : -

SSH Into EC2 Server

Now we will SSH into the Azure VM and configure the it for Nginx container deployment.

Steps

1. Open the Powershell Window.
2. Run the following command to SSH into Azure VM and substitute the *<admin-username>* with the value provided in locals.tf file under *<virtual-machine-properties>* section and *<vm-public-ip>* with the Azure VM public IP received from **terraform output** command:

```
ssh -o StrictHostKeyChecking=no admin-username@<*vm-public-ip*>
```

3. It will prompt for password, enter the *<admin_password>* provided in the *locals.tf* file under *<virtual-machine-properties>* section.
4. Once you enter the server, run the following commands to install the necessary dependencies for deployment and run the nginx container:

```
sudo apt update
sudo apt install -y docker.io
sudo docker run -d -p 80:80 nginx
```

9. Try accessing it on the browser using *<vm-public-ip>* received from **terraform output** command.

Nginx Image

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

Destroy the provisioned infrastructure

Lastly, we will destroy the above-created resources by Terraform configuration files for Azure.

Steps

1. To destroy infrastructure, open the Powershell Window and change the directory to the above-created **virtual-machine-terraform** directory using the **cd** command.
 2. Run **terraform destroy** & if prompted, type **yes**.
 3. Infrastructure will be destroyed.
-