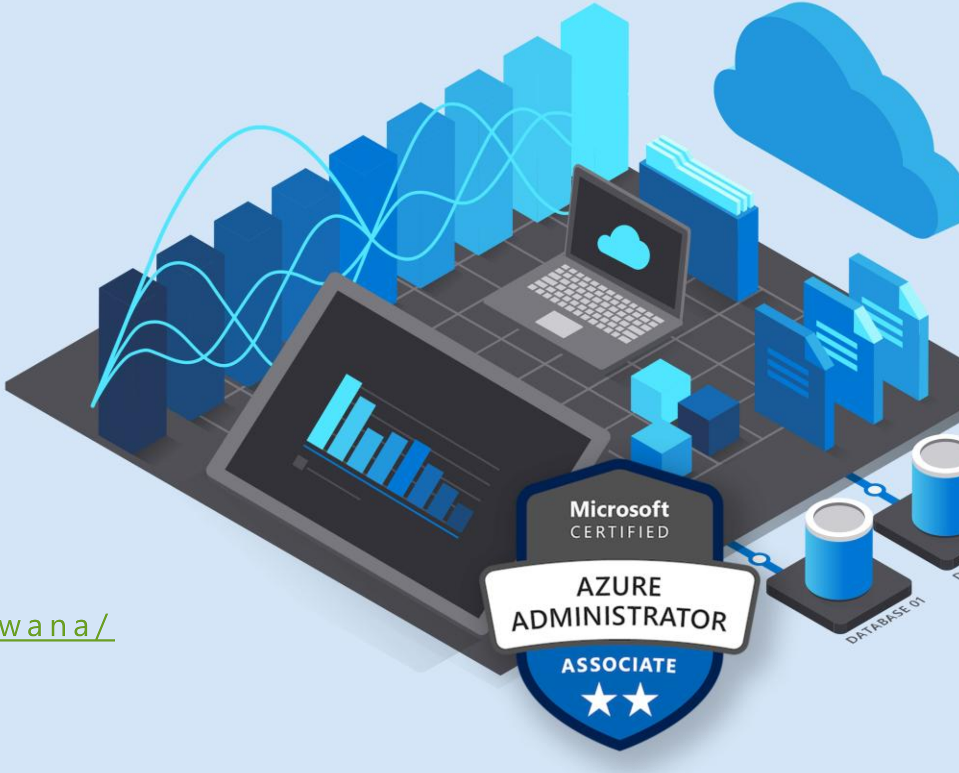
Microsoft
Azure Administrator



Maruti Makwana

MCT Corporate Trainer

https://www.linkedin.com/in/marutimakwana/

10th June 2025

Secure your Azure resources with Azure role-based access control (Azure RBAC)

Compare Azure RBAC Roles to Entra ID Roles

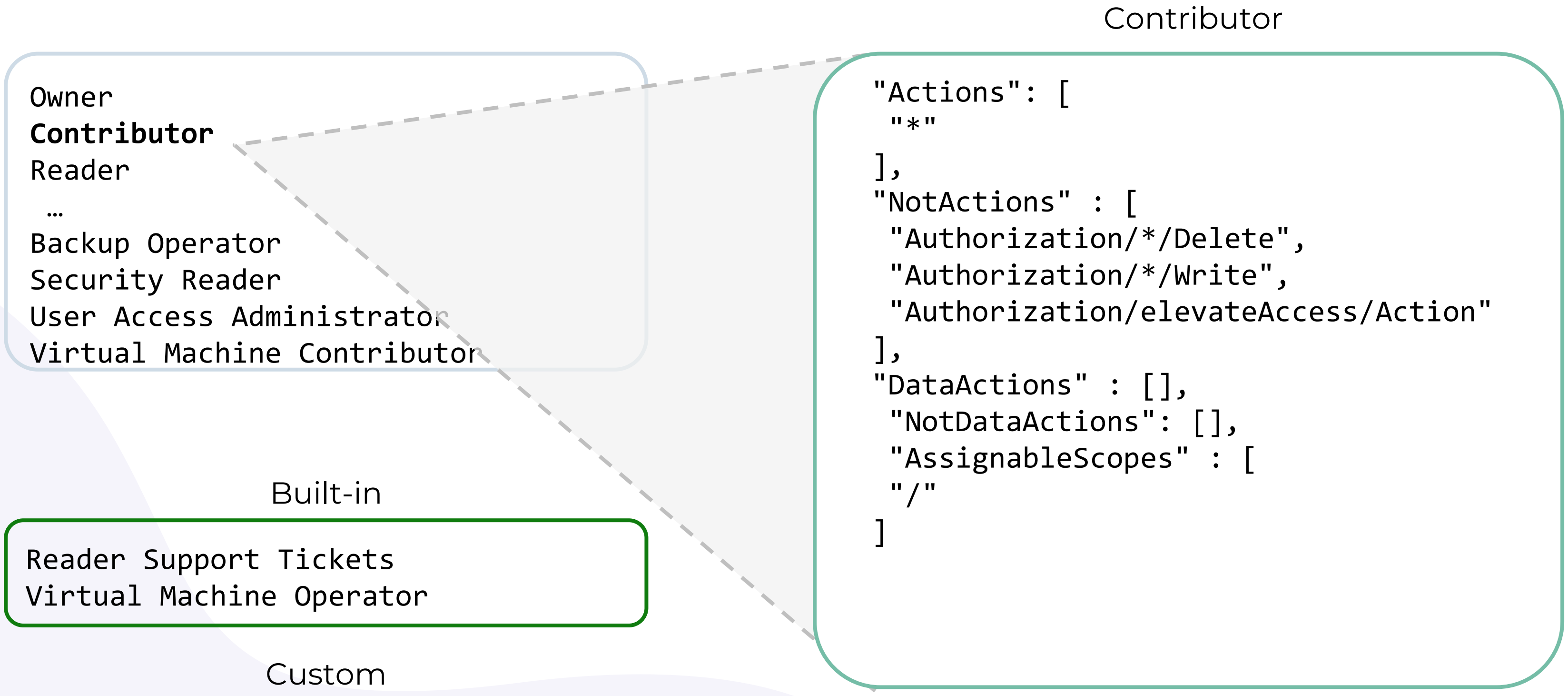
RBAC roles provide fine-grained access management

Azure RBAC roles	Entra ID roles
Manage access to Azure resources	Manage access to Entra ID objects
Scope can be specified at multiple levels	Scope is at the tenant level
Role information can be accessed in the Azure portal, Azure CLI, Azure PowerShell, Azure Resource Manager templates, REST API	Role information can be accessed in Azure portal, Microsoft 365 admin portal, Microsoft Graph PowerShell

✓ There are many built-in roles, or you can create your own custom role

Create a Role Definition

Collection of permissions that lists the operations that can be performed



```
Owner
Contributor
Reader
 …
Backup Operator
Security Reader
User Access Administrator
Virtual Machine Contributor
```

Built-in

```
Reader Support Tickets
Virtual Machine Operator
```

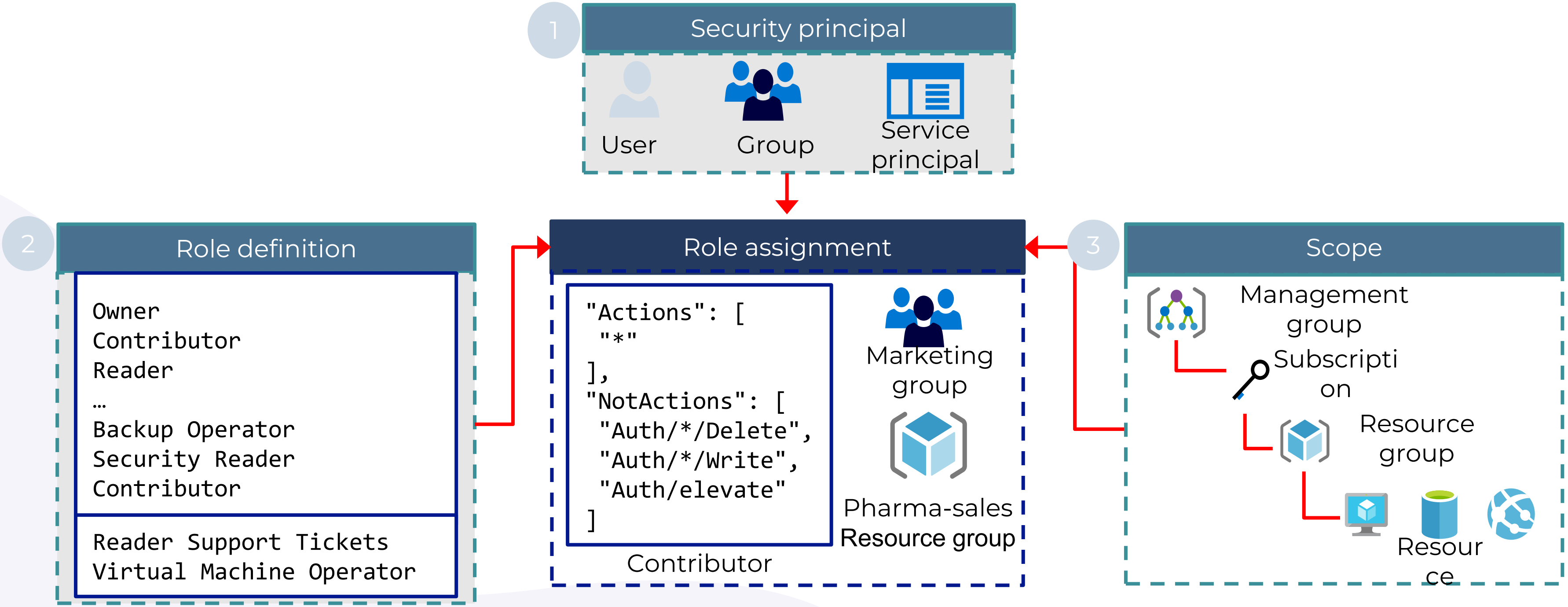
Custom

Contributor

```
"Actions": [
 "*"
],
"NotActions" : [
 "Authorization/*/Delete",
 "Authorization/*/Write",
 "Authorization/elevateAccess/Action"
],
"DataActions" : [],
 "NotDataActions": [],
 "AssignableScopes" : [
 "/"
]
```

Create a Role Assignment

Process of binding a role definition to a user, group, or service principal at a scope for the purpose of granting access



1 Security principal

User

Group

Service principal

2 Role definition

Owner
Contributor
Reader
…
Backup Operator
Security Reader
Contributor

Reader Support Tickets
Virtual Machine Operator

Role assignment

```
"Actions": [
  "*"
],
"NotActions": [
  "Auth/*/Delete",
  "Auth/*/Write",
  "Auth/elevate"
]
```

Contributor

Marketing group

Pharma-sales Resource group

3 Scope

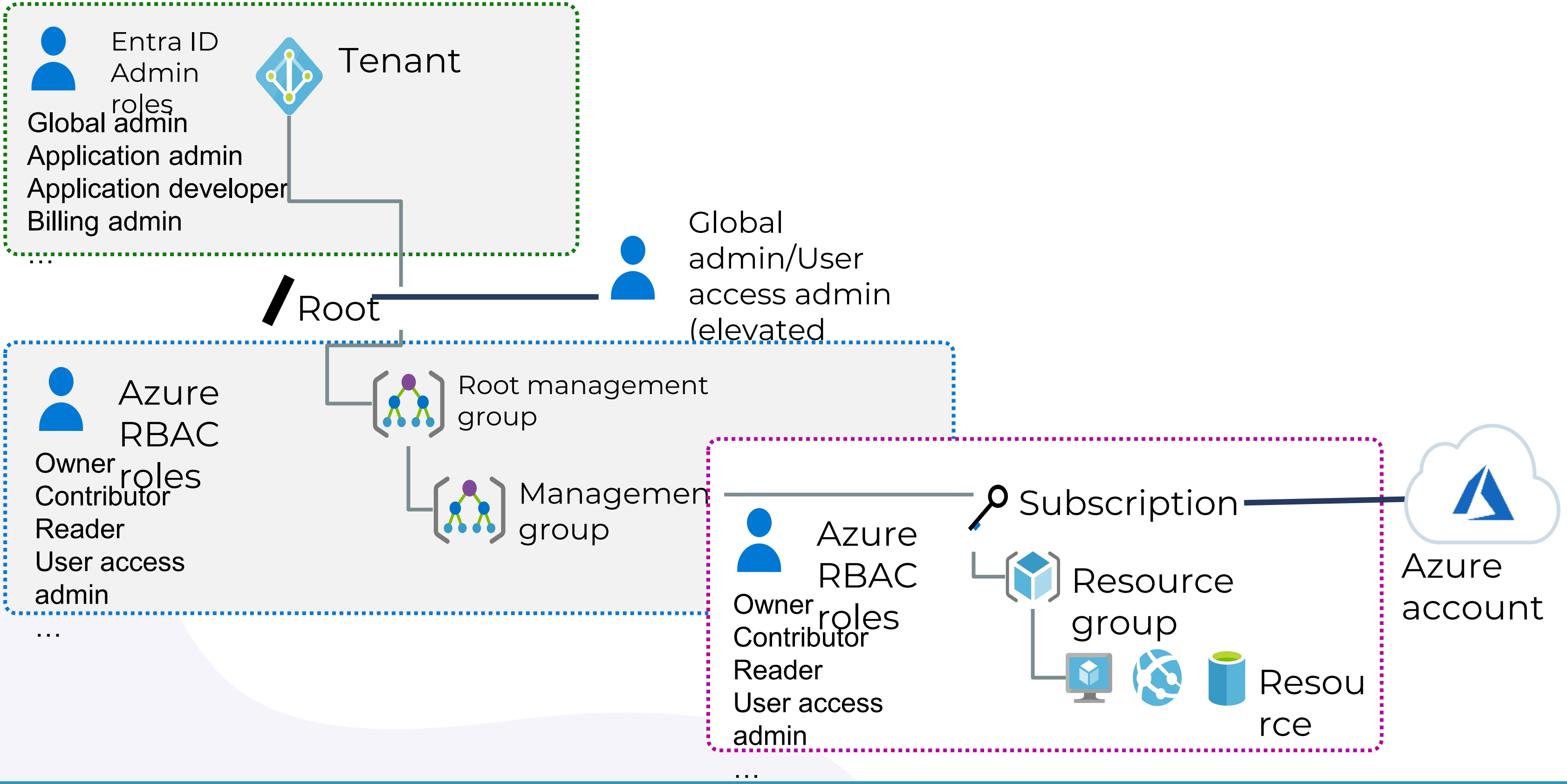
Management group

Subscripti on

Resource group

Resour ce

Apply RBAC Authentication



Entra ID Admin roles

Global admin
Application admin
Application developer
Billing admin
…

Tenant

/ Root

Global admin/User access admin (elevated

Azure RBAC roles

Owner
Contributor
Reader
User access admin
…

Root management group

Managemen group

Subscription

Azure account

Azure RBAC roles

Owner
Contributor
Reader
User access admin
…

Resource group

Resou rce

Azure Policy Initiatives

Implement Azure Policies

A service to create, assign, and manage policies

Runs evaluations and scans for non-compliant resources

Advantages:

- Enforcement and compliance
- Apply policies at scale
- Remediation

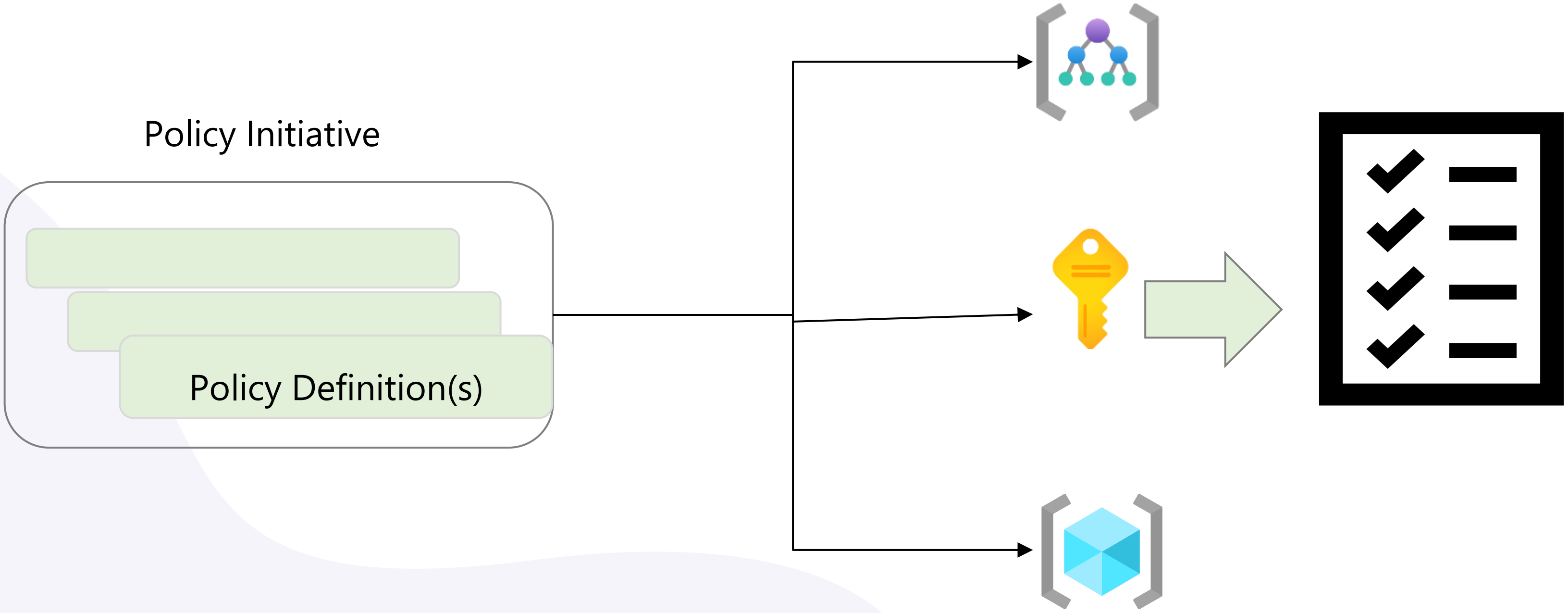
Usage Cases
Allowed resource types – Specify the resource types that your organization can deploy
Allowed virtual machine SKUs – Specify a set of virtual machine SKUs that your organization can deploy
Allowed locations – Restrict the locations your organization can specify when deploying resources
Require tag and its value – Enforces a required tag and its value
Azure Backup should be enabled for Virtual Machines – Audit if Azure Backup service is enabled for all Virtual machines

Create Azure Policies

Define and create

Scope and assign

Assess compliance

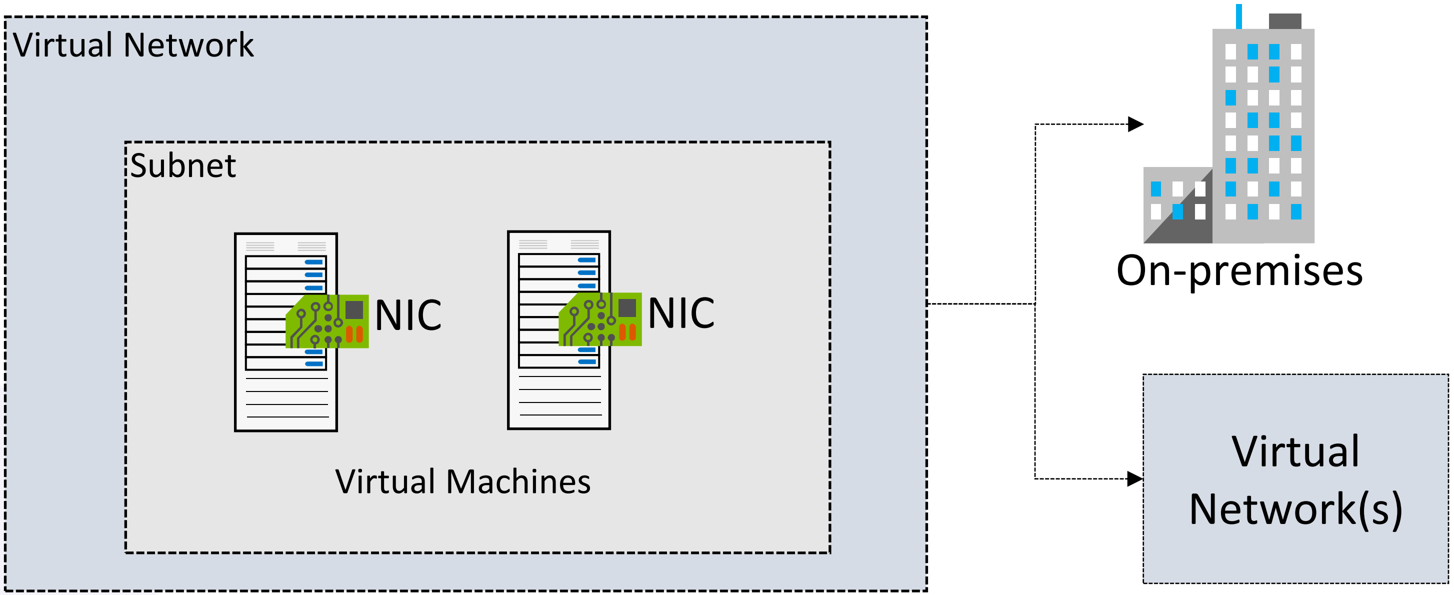


Policy Initiative

Policy Definition(s)

Configure Virtual Networks

Plan Virtual Networks



Logical representation of your own network

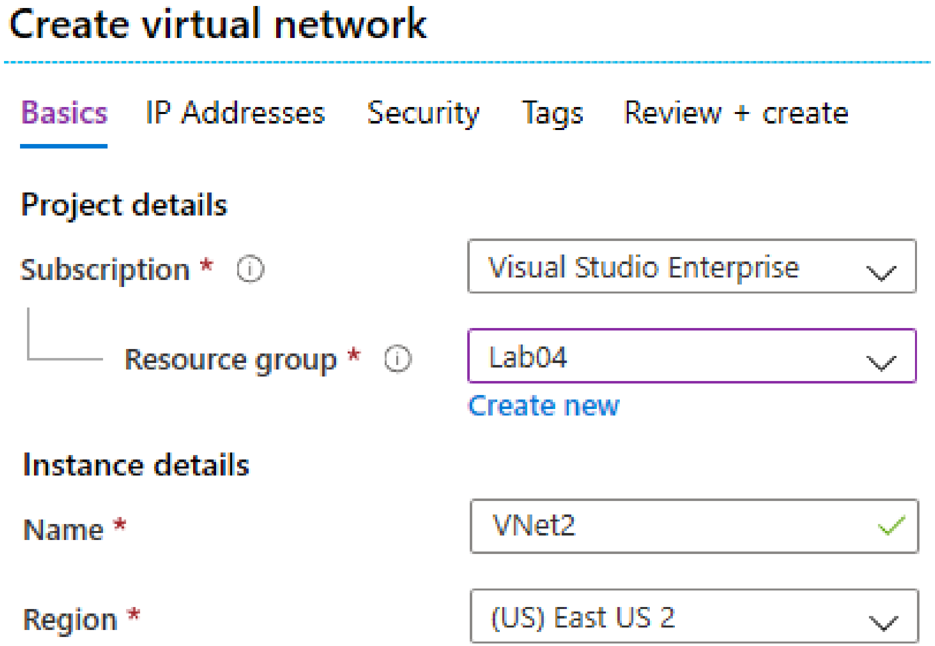
Create a dedicated private cloud-only virtual network

Securely extend your datacenter with virtual networks

Enable hybrid cloud scenarios

Create Virtual Networks

- Create new virtual networks at any time
- Add virtual networks when you create a virtual machine
- Define the address space, and at least one subnet
- Check for overlapping address spaces



Create virtual network

Project details

Subscription * : Visual Studio Enterprise

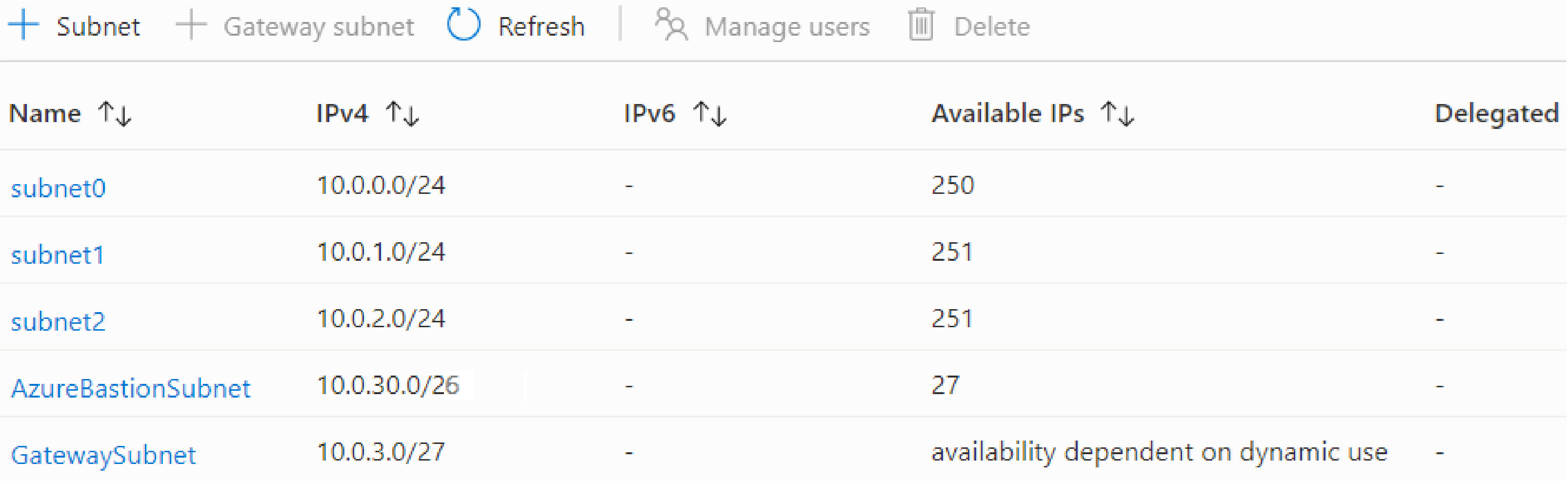
Resource group * : Lab04

Instance details

Name * : VNet2

Region * : (US) East US 2

Create Subnets



Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated
subnet0	10.0.0.0/24	-	250	-
subnet1	10.0.1.0/24	-	251	-
subnet2	10.0.2.0/24	-	251	-
AzureBastionSubnet	10.0.30.0/26	-	27	-
GatewaySubnet	10.0.3.0/27	-	availability dependent on dynamic use	-

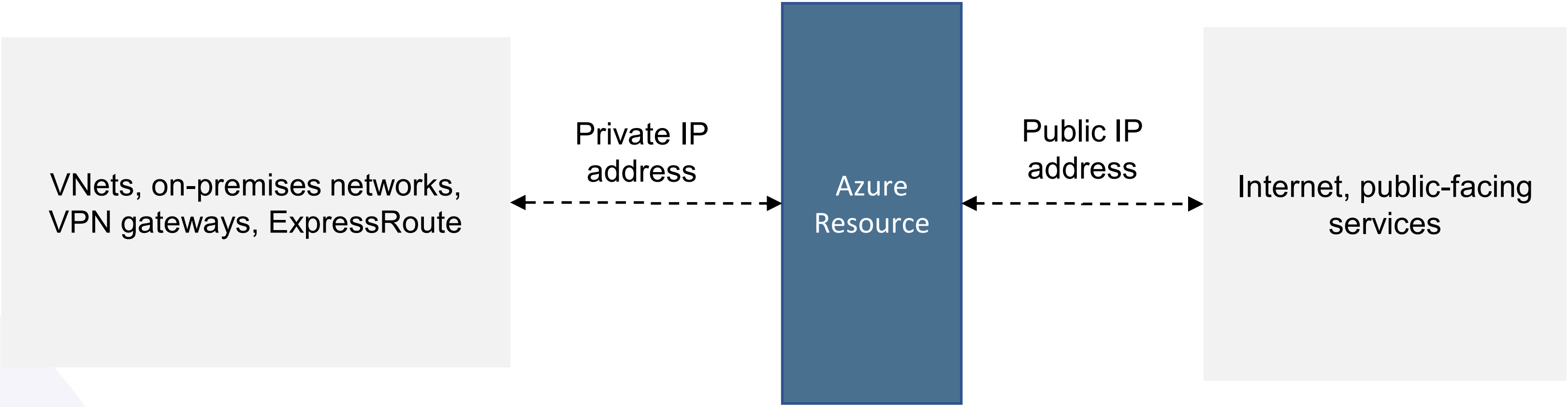
A virtual network can be segmented into one or more subnets

Subnets provide logical divisions within your network

Subnets can help improve security, increase performance, and make it easier to manage the network

Each subnet must have a unique address range – cannot overlap with other subnets in the vnet in the subscription

Plan IP Addressing



VNets, on-premises networks, VPN gateways, ExpressRoute

Private IP address

Azure Resource

Public IP address

Internet, public-facing services

Private IP addresses - used within an Azure virtual network (VNet), and your on-premises network, when you use a VPN gateway or ExpressRoute circuit to extend your network to Azure

Public IP addresses - used for communication with the Internet, including Azure public-facing services

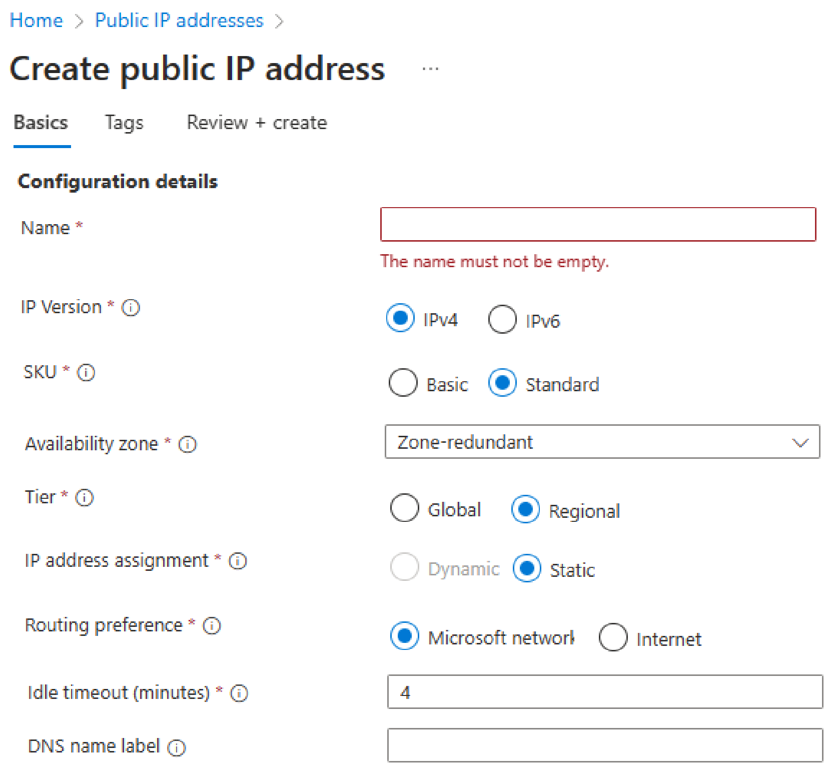
Create Public IP Addresses

Available in IPv4 or IPv6 or both

Basic vs Standard SKU

Dynamic vs Static

Microsoft vs. internet routing



Home > Public IP addresses >

Create public IP address ...

Basics | Tags | Review + create

Configuration details

Name *

The name must not be empty.

IP Version * ⓘ ● IPv4 ○ IPv6

SKU * ⓘ ○ Basic ● Standard

Availability zone * ⓘ Zone-redundant

Tier * ⓘ ○ Global ● Regional

IP address assignment * ⓘ ○ Dynamic ● Static

Routing preference * ⓘ ● Microsoft networl ○ Internet

Idle timeout (minutes) * ⓘ 4

DNS name label ⓘ

Associate Public IP Addresses

Public IP addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Load Balancer	Front-end configuration	Yes	Yes
VPN Gateway	Gateway IP configuration	Yes	Yes*
Application Gateway	Front-end configuration	Yes	Yes*

A public IP address resource can be associated with virtual machine network interfaces, internet-facing load balancers, VPN gateways, and application gateways

*Static IP addresses only available on certain SKUs.

Allocate or Assign Private IP Addresses

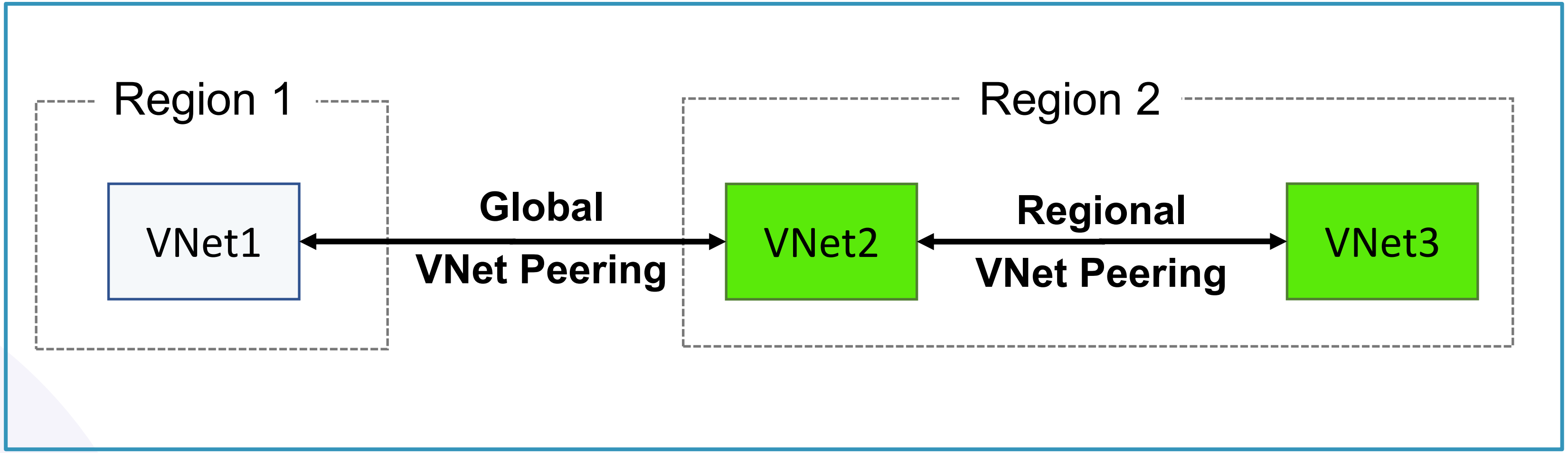
Private IP Addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Internal Load Balancer	Front-end configuration	Yes	Yes
Application Gateway	Front-end configuration	Yes	Yes

Dynamic (default). Azure assigns the next available unassigned or unreserved IP address in the subnet's address range

Static. You select and assign any unassigned or unreserved IP address in the subnet's address range

Configure VNet Peering

Determine VNet Peering Uses



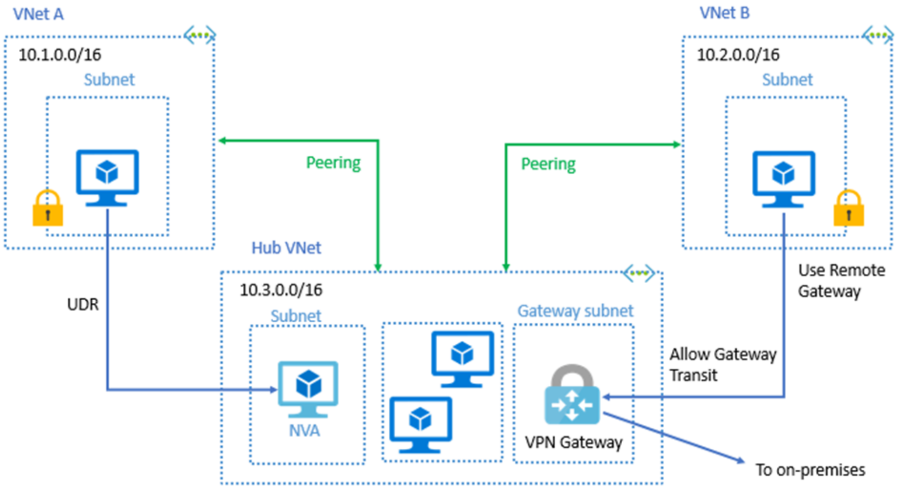
- Two types of peering: Global and Regional
- Connects two Azure virtual networks – you can peer across subscriptions and tenants
- Peered networks use the Azure backbone for privacy and isolation
- Easy to setup, seamless data transfer, and great performance

Determine Gateway Transit and Connectivity Needs

Gateway transit allows peered virtual networks to share the gateway and get access to resources

No VPN gateway is required in the peered spoke virtual network

Default VNet peering provides full connectivity



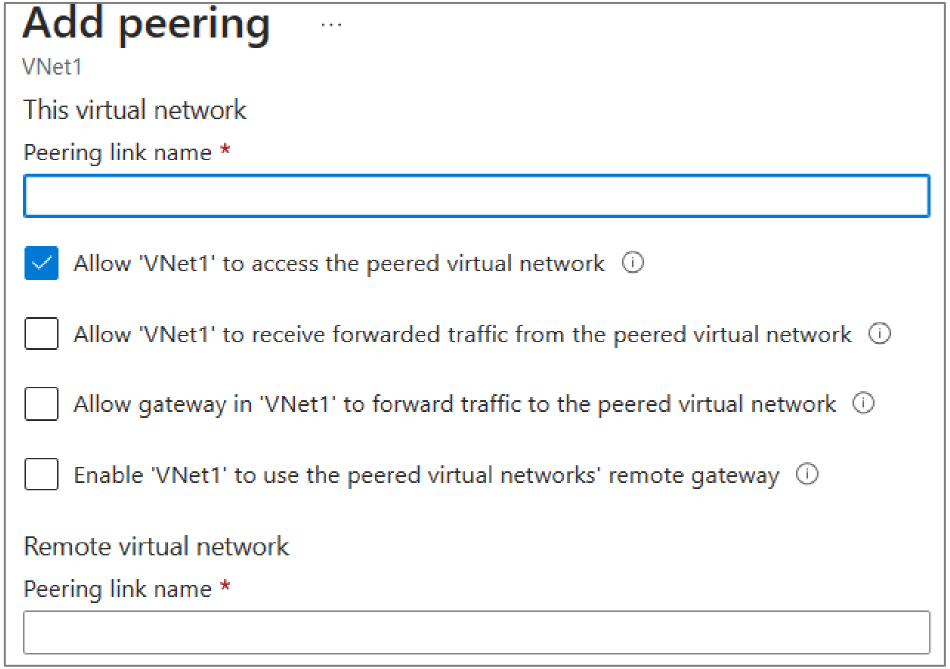
✓ IP address spaces of connected networks can't overlap

Create VNet Peering

Allow virtual network access settings

Configure forwarded traffic settings

Status should show “connected”



Add peering ···

VNet1

This virtual network

Peering link name *

☑ Allow 'VNet1' to access the peered virtual network ⓘ

□ Allow 'VNet1' to receive forwarded traffic from the peered virtual network ⓘ

□ Allow gateway in 'VNet1' to forward traffic to the peered virtual network ⓘ

□ Enable 'VNet1' to use the peered virtual networks' remote gateway ⓘ

Remote virtual network

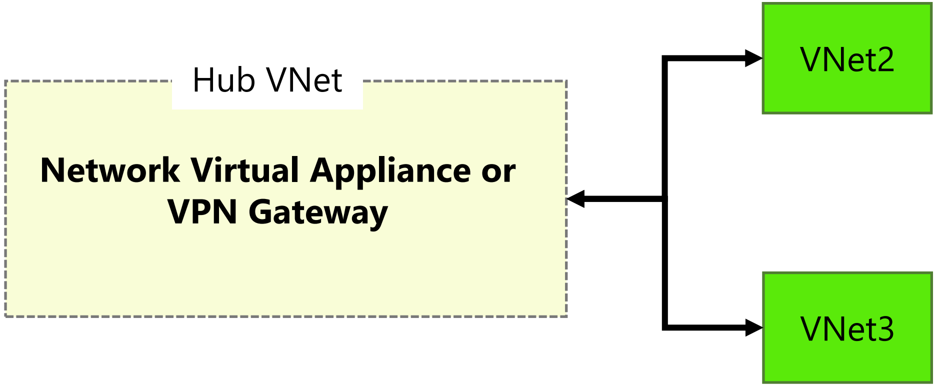
Peering link name *

Determine Service Chaining Uses

Leverage user-defined routes and service chaining to implement custom routing

Implement a VNet hub with a network virtual appliance or a VPN gateway

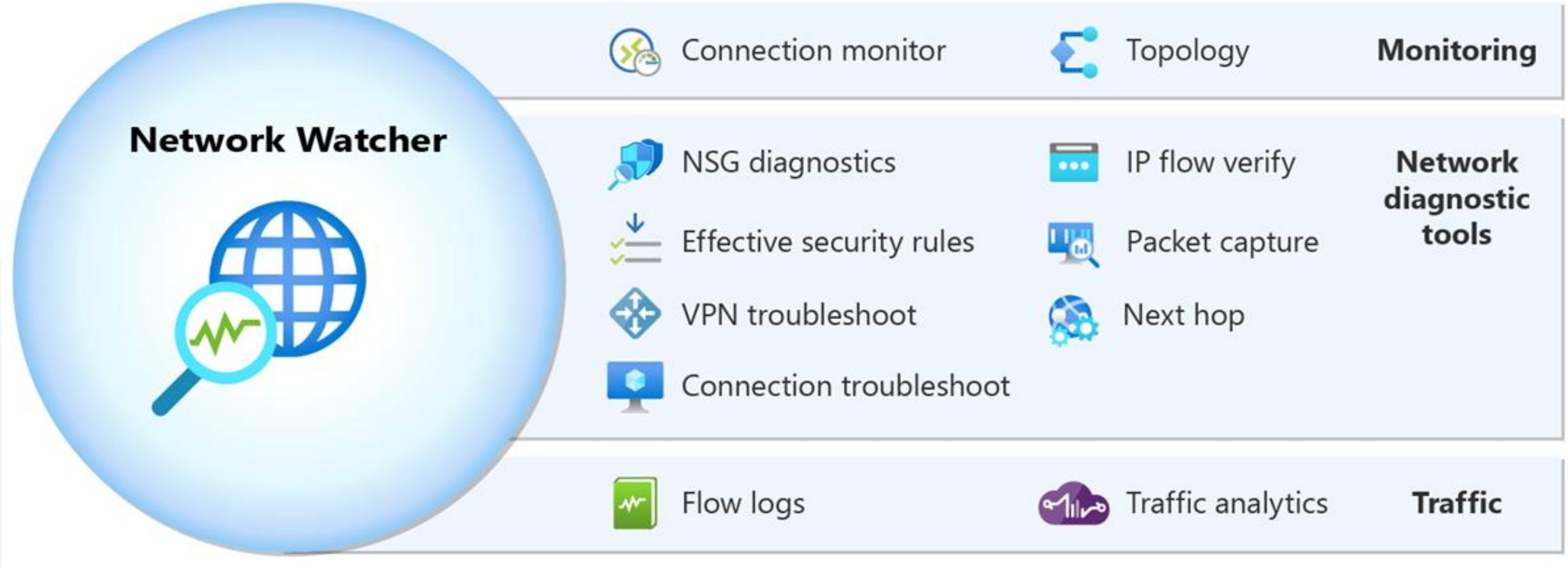
Service chaining enables you to direct traffic from one virtual network to a virtual appliance, or virtual network gateway,
in a peered virtual network, through user-defined routes



Introduction to Network Watcher

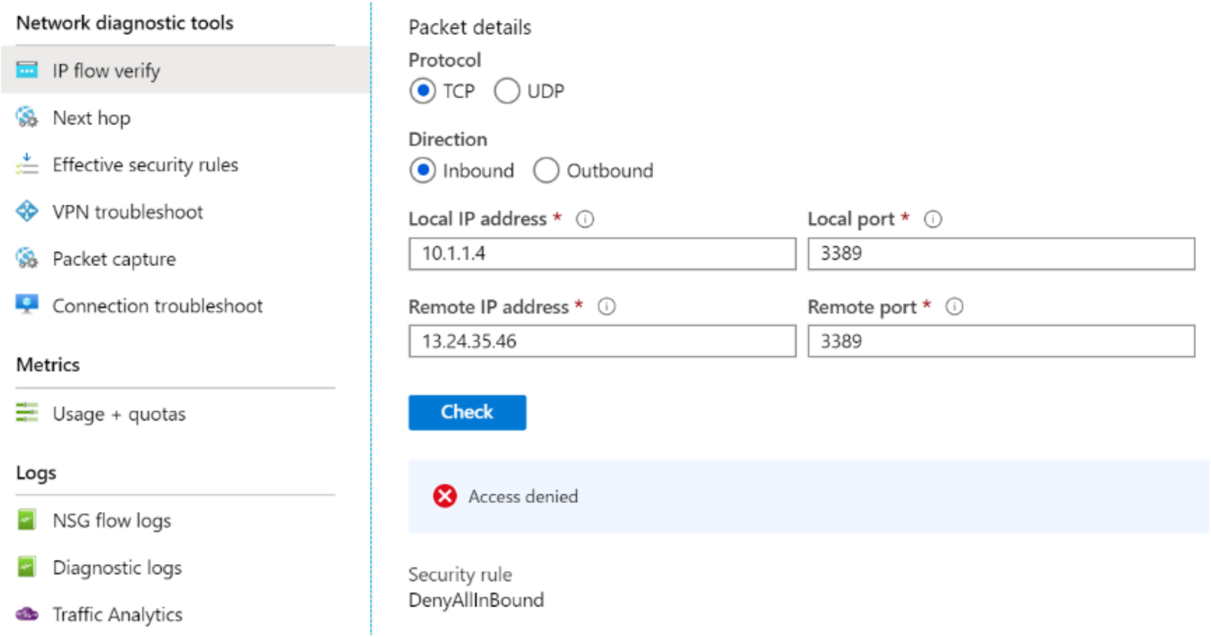
Describe Network Watcher Features

A regional service with various network diagnostics



Review IP Flow Verify Diagnostics

Checks if a packet is allowed or denied to or from a virtual machine



Packet details

Protocol

● TCP ○ UDP

Direction

● Inbound ○ Outbound

Local IP address * ⓘ 10.1.1.4

Local port * ⓘ 3389

Remote IP address * ⓘ 13.24.35.46

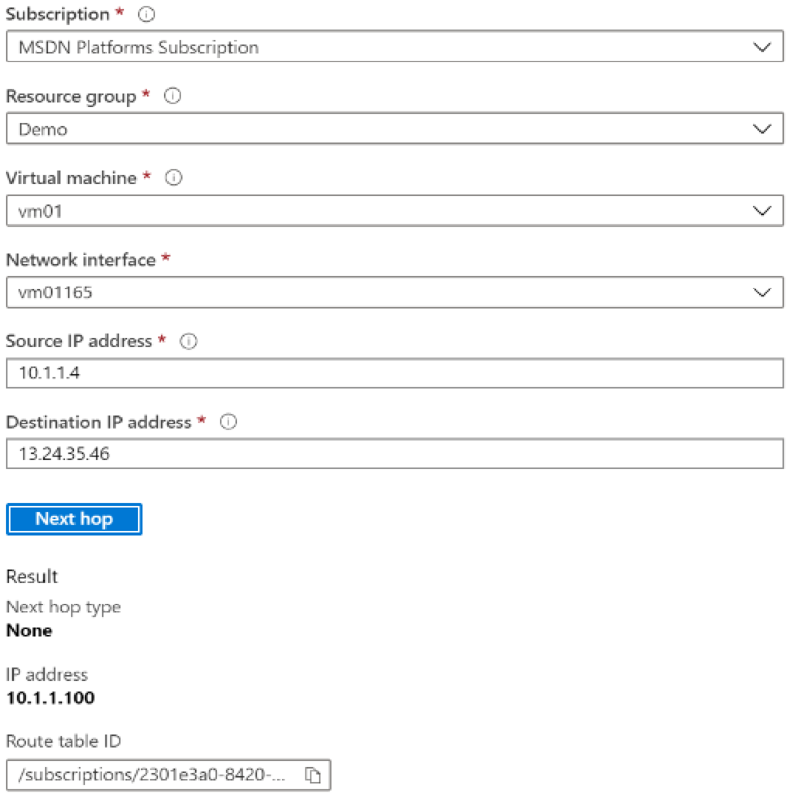
Remote port * ⓘ 3389

☒ Access denied

Security rule
DenyAllInBound

Review Next Hop Diagnostics

Helps with determining whether traffic is being directed to the intended destination by showing the next hop



Subscription *
MSDN Platforms Subscription

Resource group *
Demo

Virtual machine *
vm01

Network interface *
vm01165

Source IP address *
10.1.1.4

Destination IP address *
13.24.35.46

Result

Next hop type
None

IP address
10.1.1.100

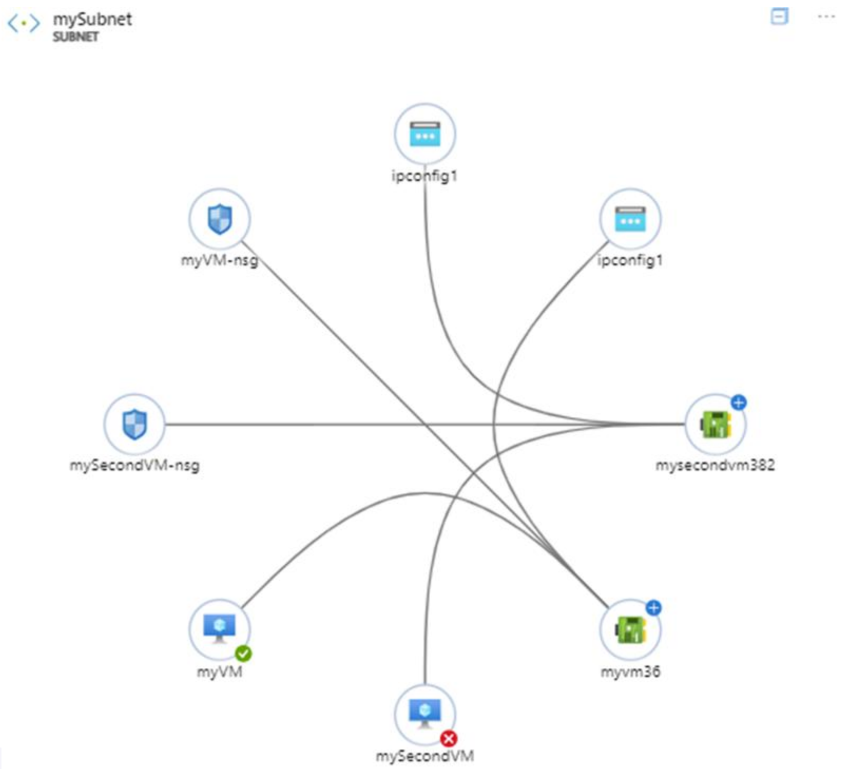
Route table ID
/subscriptions/2301e3a0-8420-...

Visualize the Network Topology

Provides a visual representation of your networking elements

View all the resources in a virtual network, resource to resource associations, and relationships between the resources

Locate the Network Watcher instance in the same region as the virtual network



mySubnet
SUBNET
ipconfig1
myVM-nsg
ipconfig1
mySecondVM-nsg
mysecondvm382
myVM
myvm36
mySecondVM