Project

DevOps Final Project

Name : Pithadiya Kirtan

CSI Student ID : CT_CSI_DV_3204

✨ Problem Statement ✨

Centralized connectivity and security management with hub and spoke:

“The hub and spoke model in Azure involves a central "hub" network connecting to multiple "spoke" networks, facilitating centralized connectivity, security enforcement, and traffic management, ideal for scalable and secure cloud infrastructures.”

1. Project Description

This project focuses on designing and implementing a secure and centralized network infrastructure in Microsoft Azure using the Hub-and-Spoke architecture model. The primary goal is to overcome the growing complexity and decentralized control faced by organizations with multiple virtual networks. The proposed solution enables controlled communication, centralized security management, and efficient resource sharing among cloud-hosted services. The Hub-and-Spoke model offers a scalable design approach that aligns with cloud best practices, promotes network isolation, and supports security and compliance needs.

By implementing Azure-native services like Virtual Network Peering, Azure Firewall, Azure Bastion, and User Defined Routes (UDRs), the architecture ensures that each environment or workload remains logically segmented while maintaining secure and efficient connectivity with centralized enforcement points. This facilitates a robust and scalable enterprise cloud network that is easier to manage, secure, and monitor.

2. Business Problem Statement

As an IT organization with multiple branch offices, remote teams, and increasing reliance on cloud-hosted resources, we are experiencing growing challenges in managing the connectivity, security, and operational consistency of our cloud network. Each workload or environment often ends up with isolated configurations, inconsistent access rules, and duplicated infrastructure components such as firewalls or VPNs.

This leads to several critical issues:

- Fragmented network visibility and management
- Increased security risks due to inconsistent enforcement
- Difficulty scaling with new workloads and services
- High operational costs and redundant resources

In the current setup, security auditing, centralized traffic control, and standardized connectivity are difficult to maintain, making it essential to adopt a more structured and unified network model.

3. Proposed Solution

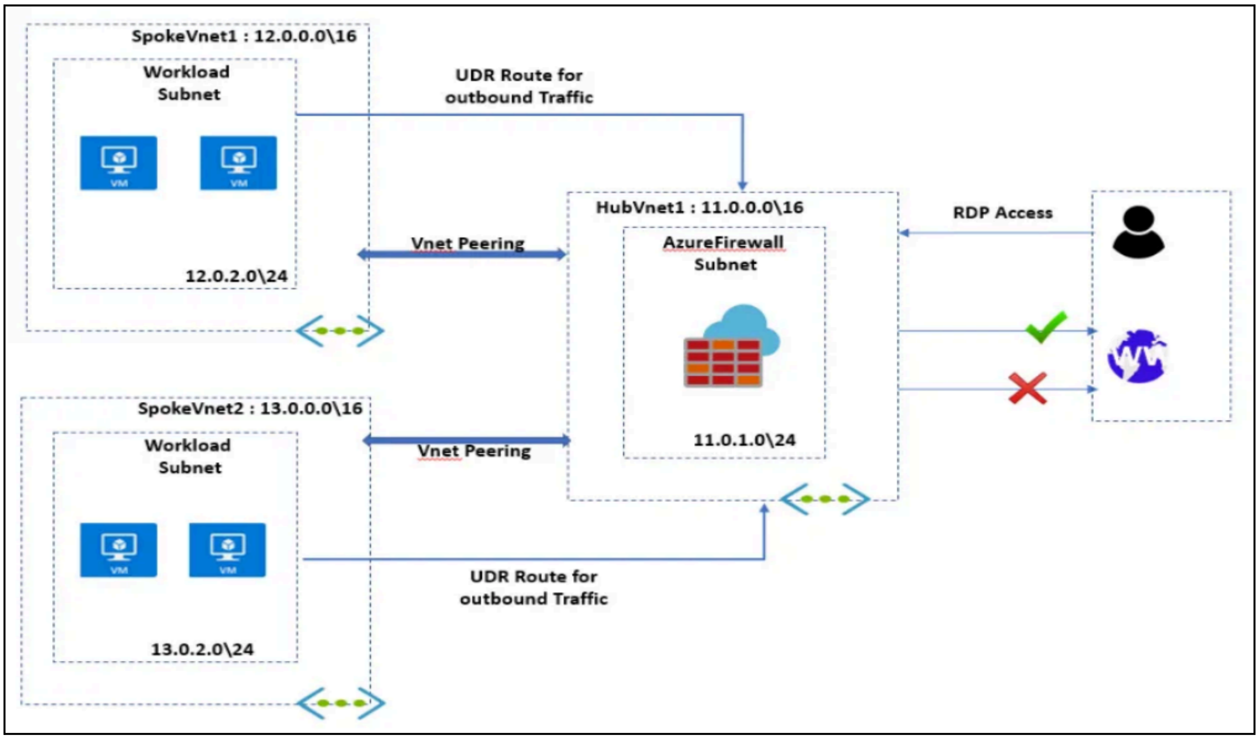
To address the above issues, the project adopts the Azure Hub-and-Spoke network architecture as the foundation for enterprise-grade cloud network design. This model ensures that all workloads across different VNets are connected through a centralized hub that manages traffic flow, security inspection, and access control.

Key Benefits of the Solution:

- **Centralized Security**: All outbound and inter-network traffic is routed through a centralized firewall deployed in the hub network, enabling uniform policy enforcement and inspection.
- **Efficient Connectivity**: Spoke networks (VNets) are connected only to the hub, minimizing direct peerings and simplifying routing logic.
- **Scalability**: New spokes can be added easily without disrupting the existing setup.
- **Cost Optimization**: Shared services like Bastion, monitoring tools, and firewalls are deployed once in the hub and used by all spokes.
- **Network Segmentation**: Different workloads or environments are logically and securely isolated in separate spoke VNets.

This solution not only improves network efficiency but also aligns with best practices in governance, compliance, and security.

High-Level Architecture:



4. Understanding the Hub-and-Spoke Architecture

The Hub-and-Spoke architecture is a popular network topology in Microsoft Azure that allows centralized connectivity between multiple virtual networks. In this model:

- The **Hub VNet** serves as the central point for connectivity and shared services.
- The **Spoke VNets** represent various workloads, environments, or departments, such as application servers, database systems, or Dev/Test/Prod environments.
- Each Spoke is connected to the Hub via **VNet Peering**.
- **Spokes do not connect to each other directly**; instead, they communicate through the Hub, enabling centralized inspection, logging, and security enforcement.

This model mirrors the traditional on-premises hub-and-branch topology and is highly effective in cloud environments where workload isolation, centralized governance, and efficient routing are crucial.

Core Components:

1. **Hub VNet**: Hosts centralized services such as Azure Firewall, Bastion, DNS servers, monitoring agents, or Active Directory.
2. **Spoke VNets**: Host workload-specific resources and remain isolated from each other for security and control.
3. **Azure Firewall**: Acts as the centralized security layer, providing NAT, network, and application-level filtering.
4. **Azure Bastion**: Enables secure, browser-based RDP/SSH access to virtual machines without exposing public IP addresses.
5. **User Defined Routes (UDRs)**: Redirects all spoke outbound traffic through the firewall, ensuring inspection and logging.

Advantages of Hub-and-Spoke Model:

- **Security**: Traffic inspection and access control are enforced centrally.
- **Manageability**: Common services are deployed once in the hub, reducing redundancy.
- **Compliance**: Easier to implement consistent policies across environments.
- **Scalability**: Seamlessly add or remove spokes without rearchitecting the network.
- **Performance**: Low-latency, private connections between hub and spokes.

The Azure Hub-and-Spoke architecture is ideal for organizations that aim to maintain control and visibility over a growing and distributed cloud environment. It supports the principles of zero trust, secure access, and workload segmentation, all of which are critical in modern enterprise networks.

✨ *Proposed Solution* ✨

🪐*Azure Portal Implementation*🪐

1. Hub Vnet

Hub Virtual Network (Hub-VNet) Design

The Hub Virtual Network (Hub-VNet) serves as the centralized backbone of the Hub-and-Spoke architecture, playing a critical role in managing connectivity, enforcing security policies, and hosting shared services for connected spoke VNets. It ensures a scalable and secure network topology by acting as the central point for inspecting and routing traffic across the entire environment.

To meet these goals, the Hub-VNet is logically divided into two key subnets:

1. AzureFirewallSubnet (`10.0.1.0/26`)

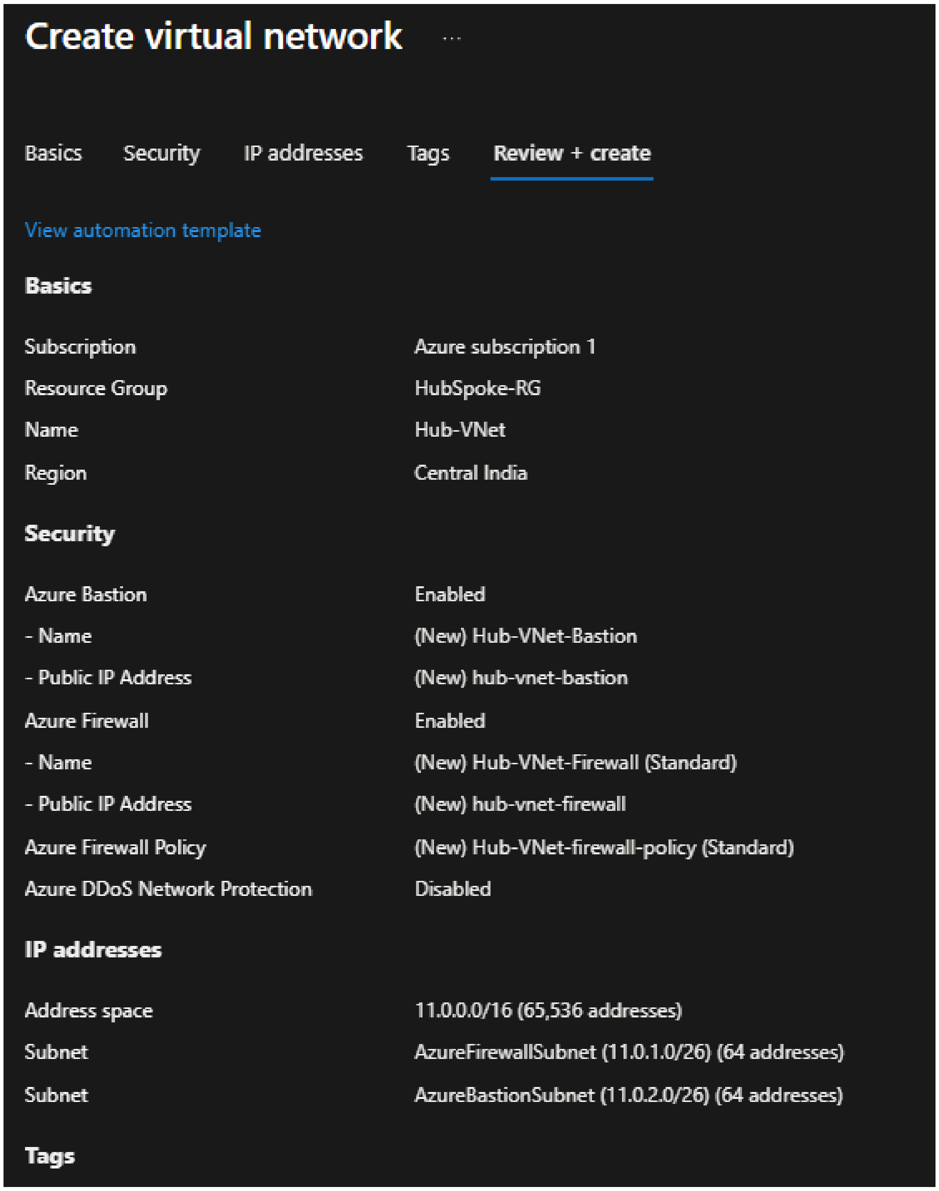
This subnet is dedicated to hosting the Azure Firewall, which provides centralized control over all network traffic entering or leaving the spoke VNets. It acts as the main security enforcement point, enabling the implementation of network and application-level filtering rules, NAT for external access, and routing control via User Defined Routes (UDRs). All outbound and inter-spoke traffic can be inspected through the firewall to meet enterprise-grade compliance and security requirements.

2. AzureBastionSubnet (`10.0.2.0/26`)

This subnet hosts the Azure Bastion service, which allows secure RDP/SSH access to virtual machines without exposing them to the public internet. By eliminating the need for public IP addresses on VMs, Azure Bastion reduces attack surfaces and prevents unauthorized access via port scanning or brute-force attacks. Administrators can securely connect to VMs directly through the Azure Portal using a browser, ensuring just-in-time access and enhancing the overall security posture.

Let’s create Hub-VNet with Two Subnet:

1. **AzureFirewallSubnet (11.0.1.0/26) (64 addresses)**
2. **AzureBastionSubnet (11.0.2.0/26) (64 addresses)**



Create virtual network ...

Basics

Subscription	Azure subscription 1
Resource Group	HubSpoke-RG
Name	Hub-VNet
Region	Central India

Security

Azure Bastion	Enabled
- Name	(New) Hub-VNet-Bastion
- Public IP Address	(New) hub-vnet-bastion
Azure Firewall	Enabled
- Name	(New) Hub-VNet-Firewall (Standard)
- Public IP Address	(New) hub-vnet-firewall
Azure Firewall Policy	(New) Hub-VNet-firewall-policy (Standard)
Azure DDoS Network Protection	Disabled

IP addresses

Address space	11.0.0.0/16 (65,536 addresses)
Subnet	AzureFirewallSubnet (11.0.1.0/26) (64 addresses)
Subnet	AzureBastionSubnet (11.0.2.0/26) (64 addresses)

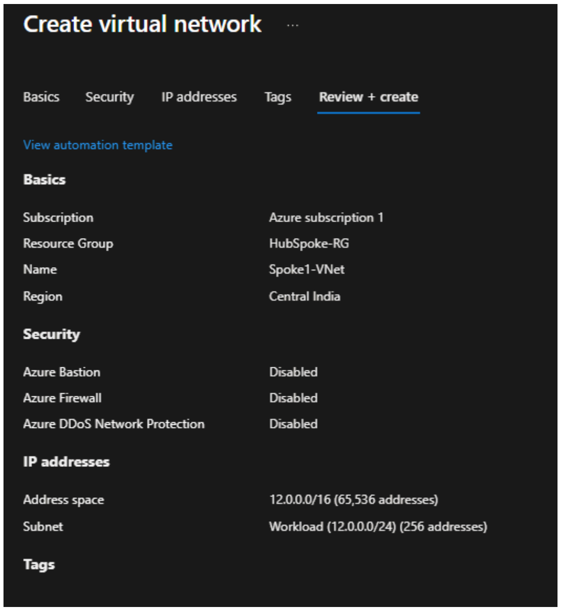
Tags

2. Spoke Vnet

The Spoke Virtual Networks are individual, isolated networks connected to the centralized Hub-VNet. Each spoke is designed to host a specific workload or environment, such as application servers, databases, or business services, and relies on the Hub for shared services and centralized security controls.

Next up we will create 2 Spoke-VNet
Spoke-VNet-1

- **WorkLoad (12.0.0.0/24) (256 addresses)**



Basics

Subscription	Azure subscription 1
Resource Group	HubSpoke-RG
Name	Spoke1-VNet
Region	Central India

Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

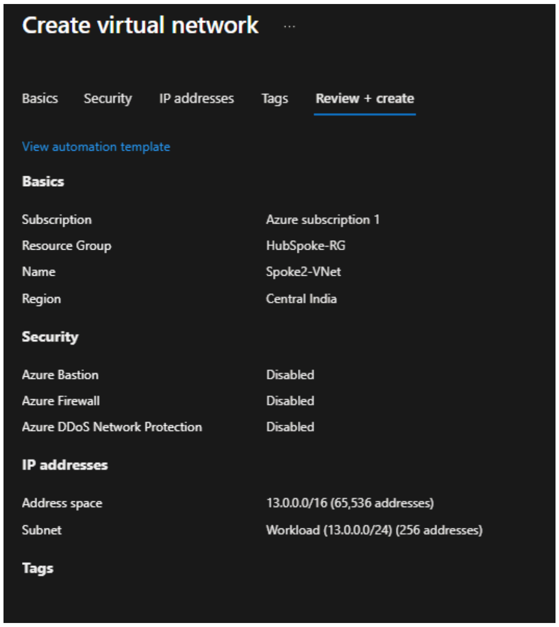
IP addresses

Address space	12.0.0.0/16 (65,536 addresses)
Subnet	Workload (12.0.0.0/24) (256 addresses)

Tags

Spoke-VNet-2

- **WorkLoad (13.0.0.0/24) (256 addresses)**



Basics

Subscription	Azure subscription 1
Resource Group	HubSpoke-RG
Name	Spoke2-VNet
Region	Central India

Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

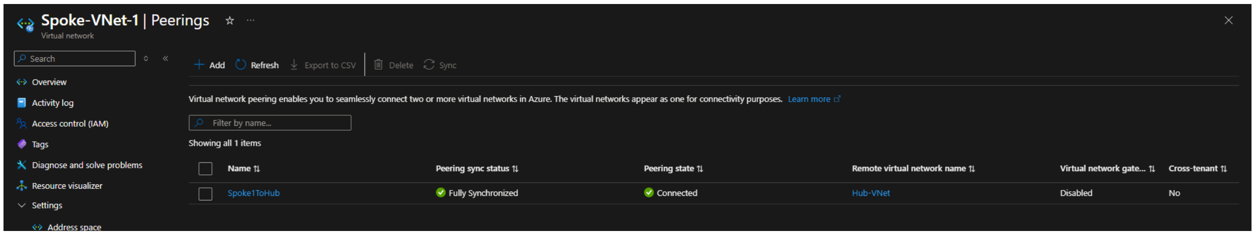
IP addresses

Address space	13.0.0.0/16 (65,536 addresses)
Subnet	Workload (13.0.0.0/24) (256 addresses)

Tags

Now let's add peering to all the Hub and Spoke Networks.

Spoke-1 To Hub

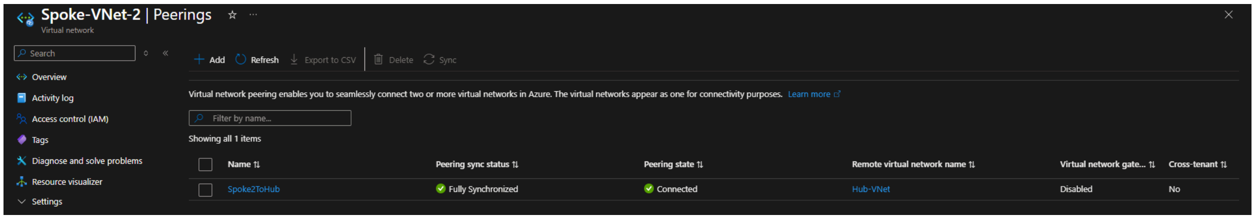


Virtual network peering enables you to seamlessly connect two or more virtual networks in Azure. The virtual networks appear as one for connectivity purposes. Learn more

Showing all 1 items

□	Name ⇅	Peering sync status ⇅	Peering state ⇅	Remote virtual network name ⇅	Virtual network gate... ⇅	Cross-tenant ⇅
□	Spoke1ToHub	✓ Fully Synchronized	✓ Connected	Hub-VNet	Disabled	No

Spoke-2 To Hub

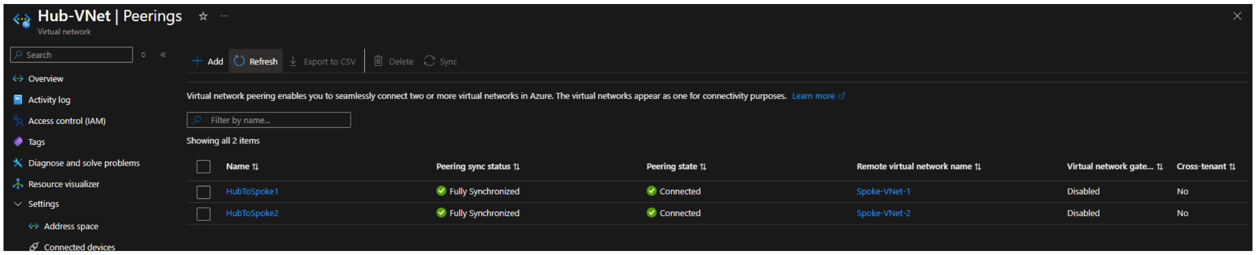


Virtual network peering enables you to seamlessly connect two or more virtual networks in Azure. The virtual networks appear as one for connectivity purposes. Learn more

Showing all 1 items

□	Name ⇅	Peering sync status ⇅	Peering state ⇅	Remote virtual network name ⇅	Virtual network gate... ⇅	Cross-tenant ⇅
□	Spoke2ToHub	✓ Fully Synchronized	✓ Connected	Hub-VNet	Disabled	No

Hub To Spoke-1 and Hub To Spoke-2



Virtual network peering enables you to seamlessly connect two or more virtual networks in Azure. The virtual networks appear as one for connectivity purposes. Learn more

Showing all 2 items

□	Name ⇅	Peering sync status ⇅	Peering state ⇅	Remote virtual network name ⇅	Virtual network gate... ⇅	Cross-tenant ⇅
□	HubToSpoke1	✓ Fully Synchronized	✓ Connected	Spoke-VNet-1	Disabled	No
□	HubToSpoke2	✓ Fully Synchronized	✓ Connected	Spoke-VNet-2	Disabled	No

All the peering and Connected and Running Successfully.

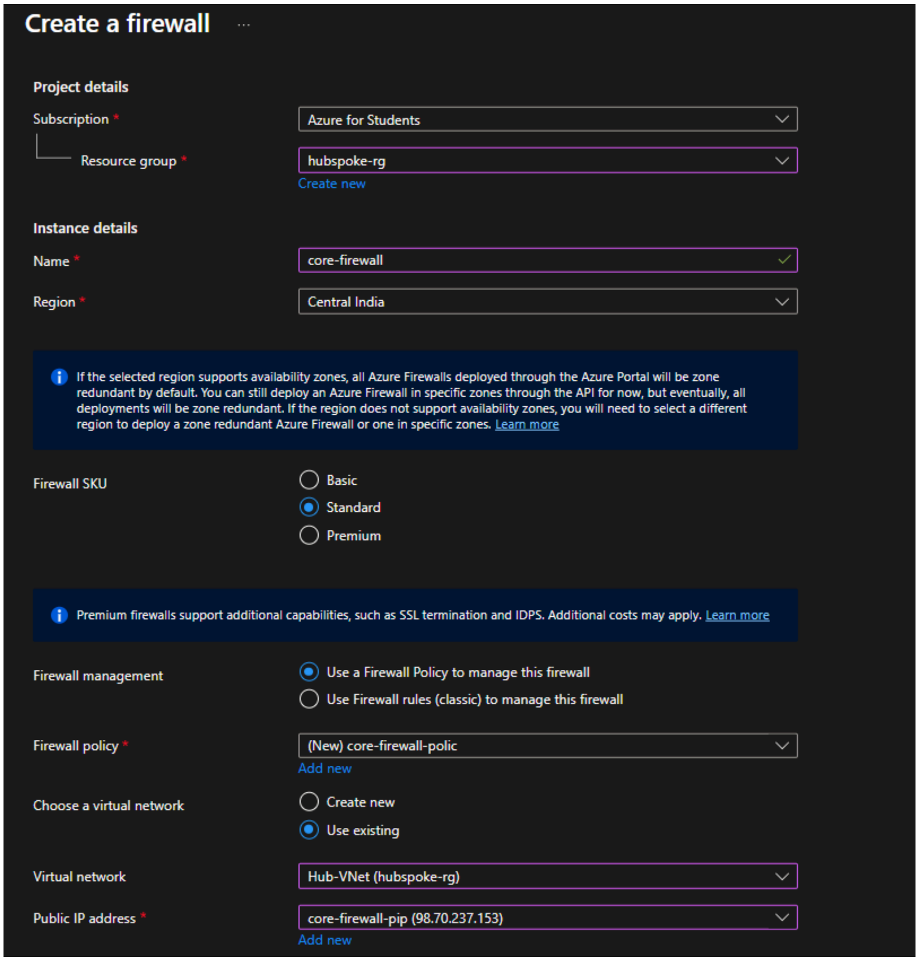
3. Azure Firewall

Azure Firewall is a cloud-native, fully managed network security service designed to protect Azure resources through centralized traffic filtering and monitoring. It allows organizations to enforce both network-level and application-level rules, enabling deep control over inbound, outbound, and lateral traffic across virtual networks.

In a Hub-and-Spoke architecture, Azure Firewall is deployed inside the Hub-VNet. Its main role is to inspect and control traffic that flows between spoke networks or from spokes to the internet. Instead of placing separate firewalls in every VNet, a single Azure Firewall in the Hub acts as the central security checkpoint.

This setup simplifies security management by applying a single set of rules across all spoke VNets. It also ensures that traffic from different workloads is consistently monitored and logged. Using User Defined Routes (UDRs), all spoke traffic can be directed through the firewall for inspection.

By centralizing security at the Hub, Azure Firewall helps enforce policies, reduce complexity, and maintain a strong, compliant, and scalable network architecture.



Create a firewall ...

Project details

Subscription * : Azure for Students

Resource group * : hubspoke-rg

Create new

Instance details

Name * : core-firewall ✓

Region * : Central India

If the selected region supports availability zones, all Azure Firewalls deployed through the Azure Portal will be zone redundant by default. You can still deploy an Azure Firewall in specific zones through the API for now, but eventually, all deployments will be zone redundant. If the region does not support availability zones, you will need to select a different region to deploy a zone redundant Azure Firewall or one in specific zones. Learn more

Firewall SKU: ○ Basic ● Standard ○ Premium

Premium firewalls support additional capabilities, such as SSL termination and IDPS. Additional costs may apply. Learn more

Firewall management: ● Use a Firewall Policy to manage this firewall ○ Use Firewall rules (classic) to manage this firewall

Firewall policy * : (New) core-firewall-polic

Add new

Choose a virtual network: ○ Create new ● Use existing

Virtual network: Hub-VNet (hubspoke-rg)

Public IP address * : core-firewall-pip (98.70.237.153)

Add new

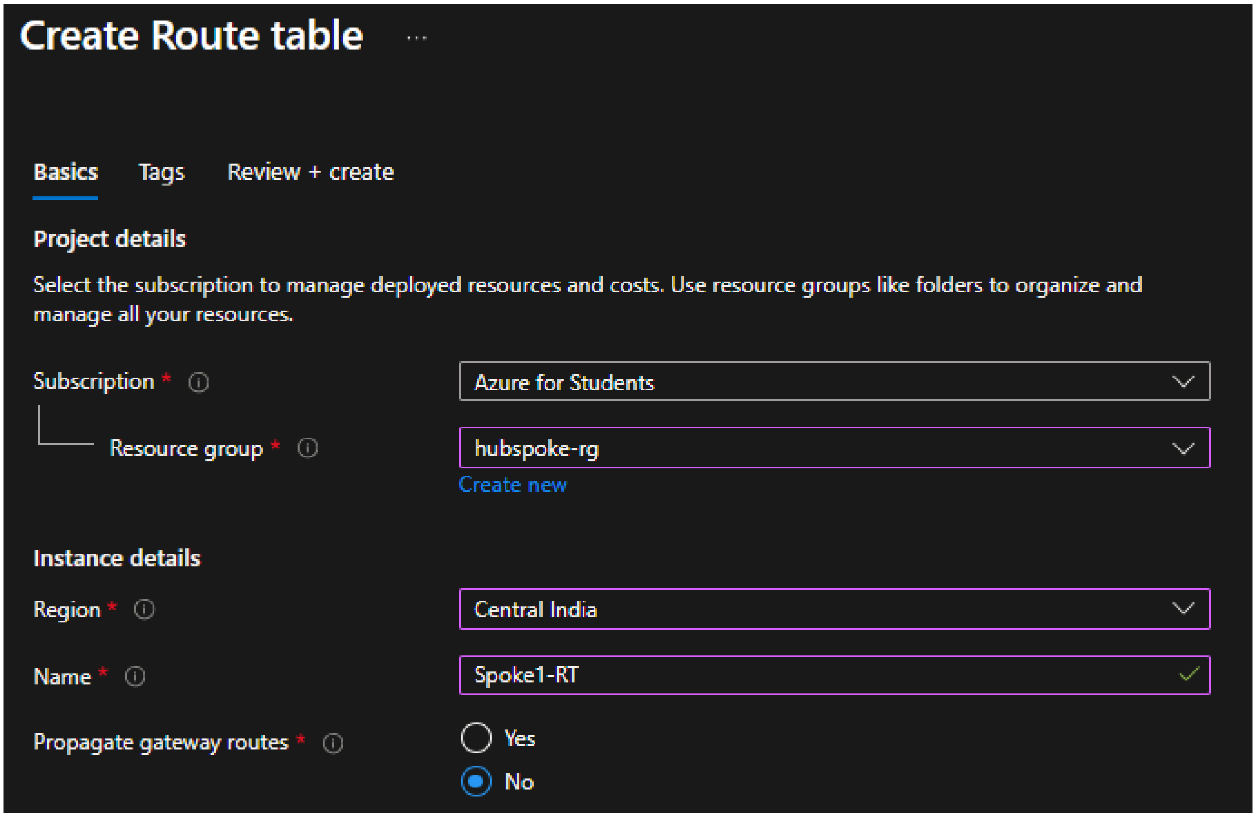
4. User Defined Routes (UDRs) in Spoke VNets

In a Hub-and-Spoke architecture, by default, Azure uses system routing tables which do not direct traffic through the Hub's security perimeter. To ensure all outbound and inter-spoke traffic is inspected by the Azure Firewall in the Hub, we implement User Defined Routes (UDRs) in each Spoke VNet.

A UDR allows us to manually define the traffic path, overriding Azure's default behavior and forcing packets to pass through the centralized firewall in the Hub before they leave the VNet. This is a core mechanism that enables centralized control and consistent security enforcement.

Step 1: Create a Route Table

- **A new route table named `Spoke1-RouteTable` is created in the same region and resource group as the spoke virtual network. This route table will hold custom routes that override Azure's default system routing.**



Create Route table ...

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Azure for Students

Resource group * : hubspoke-rg

Create new

Instance details

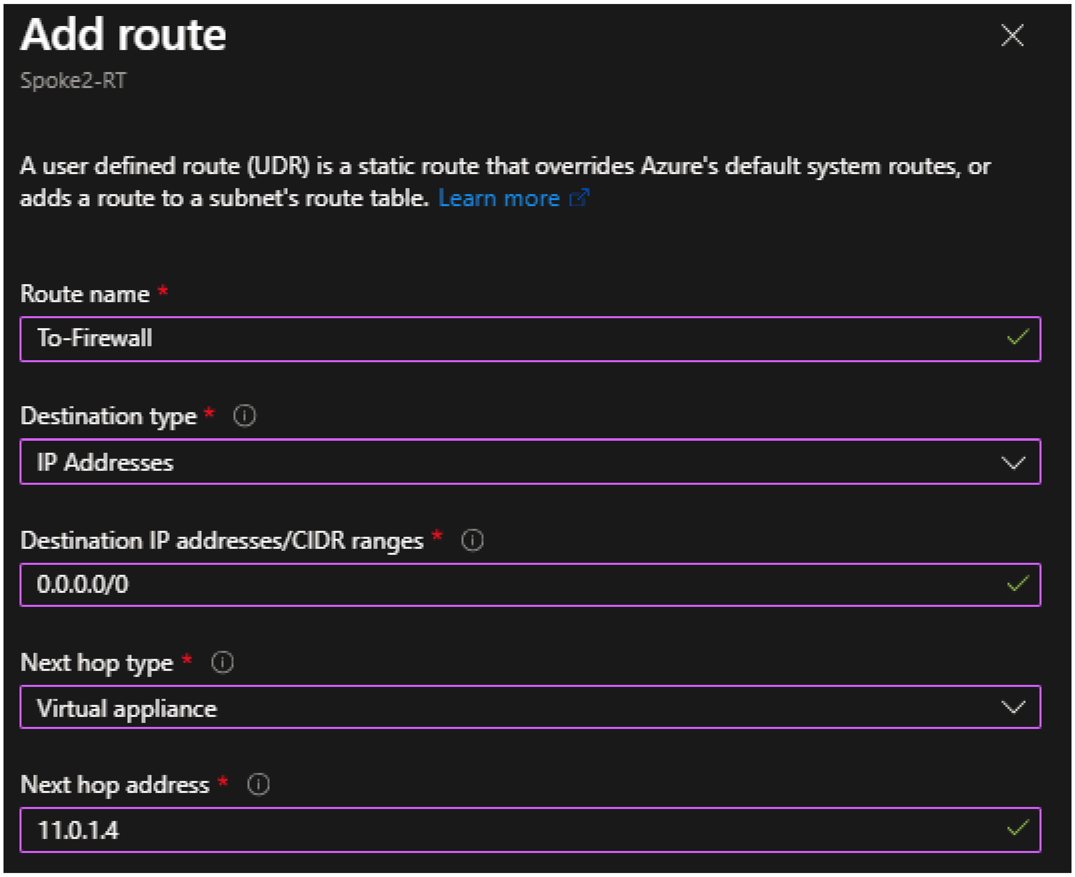
Region * : Central India

Name * : Spoke1-RT

Propagate gateway routes * : ○ Yes ● No

Step 2: Add a Custom Route

- A route is added to the newly created route table which targets all outbound traffic (`0.0.0.0/0`) and redirects it to the Azure Firewall's private IP in the Hub-VNet. This effectively forces all traffic to flow through the firewall for inspection.



Add route

Spoke2-RT

A user defined route (UDR) is a static route that overrides Azure's default system routes, or adds a route to a subnet's route table. Learn more

Route name * : To-Firewall

Destination type * : IP Addresses

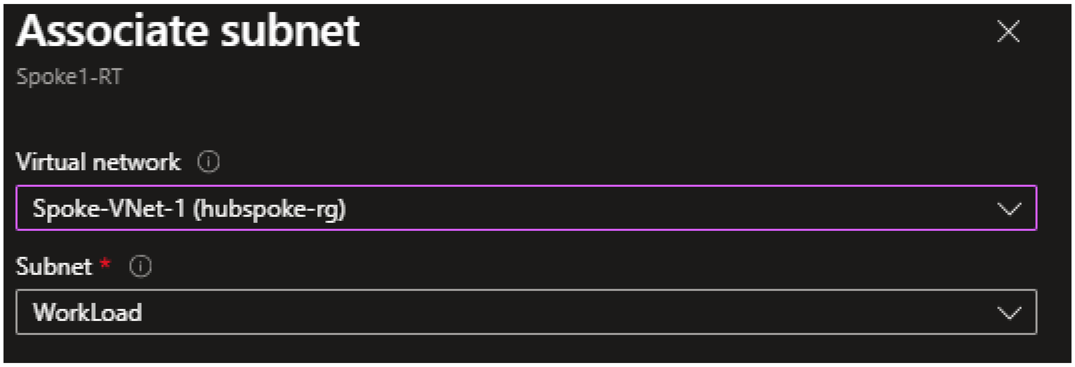
Destination IP addresses/CIDR ranges * : 0.0.0.0/0

Next hop type * : Virtual appliance

Next hop address * : 11.0.1.4

Step 3: Associate the Route Table with the Subnet

- The route table is then associated with the Workload subnet in `Spoke-VNet-1`. This binds the custom route logic to that subnet, enabling controlled egress through the central firewall.



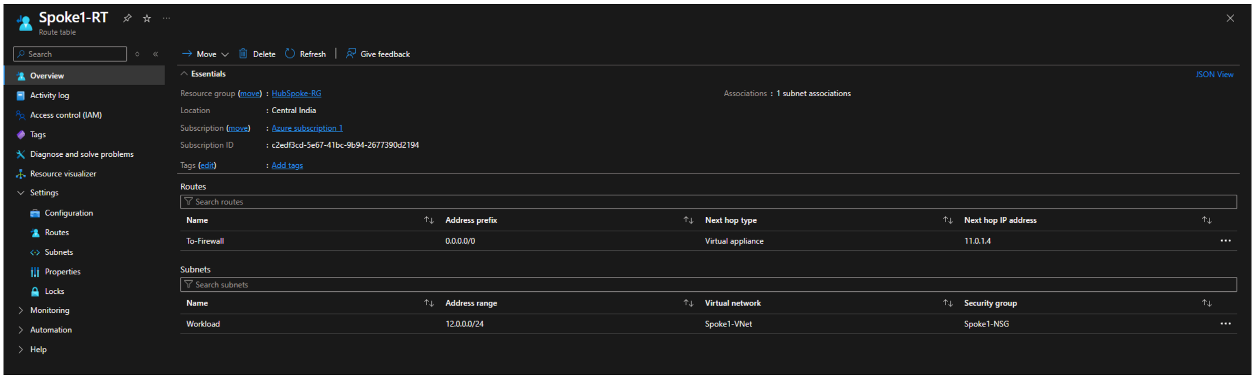
Associate subnet

Spoke1-RT

Virtual network : Spoke-VNet-1 (hubspoke-rg)

Subnet * : WorkLoad

Finally the Routing Table for the Spoke 1 is created.



Resource group (move) : HubSpoke-RG
Location : Central India
Subscription (move) : Azure subscription 1
Subscription ID : c2edf3cd-5e67-41bc-9b94-2677390d2194
Tags (edit) : Add tags
Associations : 1 subnet associations

Routes

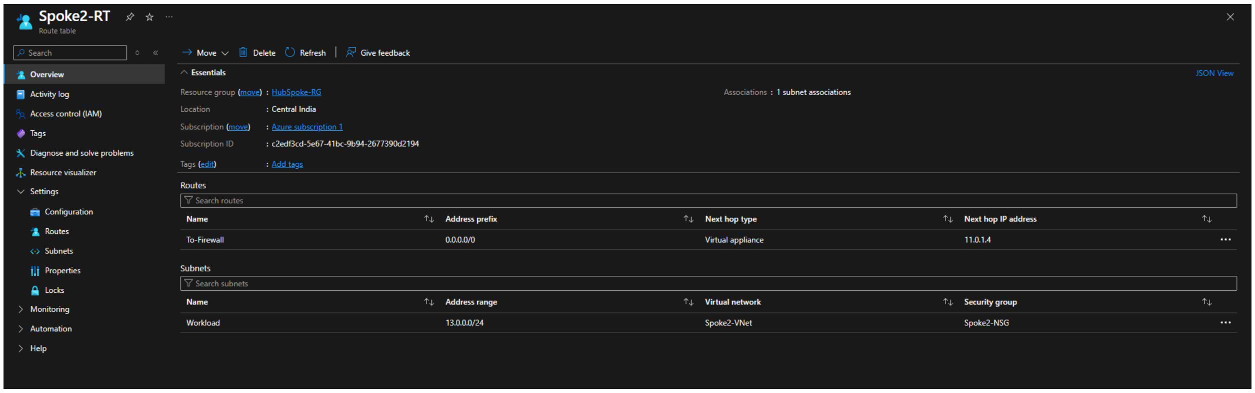
Name	Address prefix	Next hop type	Next hop IP address
To-Firewall	0.0.0.0/0	Virtual appliance	11.0.1.4

Subnets

Name	Address range	Virtual network	Security group
Workload	12.0.0.0/24	Spoke1-VNet	Spoke1-NSG

Now repeat the same process for the Spoke 2.

Finally the Routing Table for the Spoke 2 is created.



Resource group (move) : HubSpoke-RG
Location : Central India
Subscription (move) : Azure subscription 1
Subscription ID : c2edf3cd-5e67-41bc-9b94-2677390d2194
Tags (edit) : Add tags
Associations : 1 subnet associations

Routes

Name	Address prefix	Next hop type	Next hop IP address
To-Firewall	0.0.0.0/0	Virtual appliance	11.0.1.4

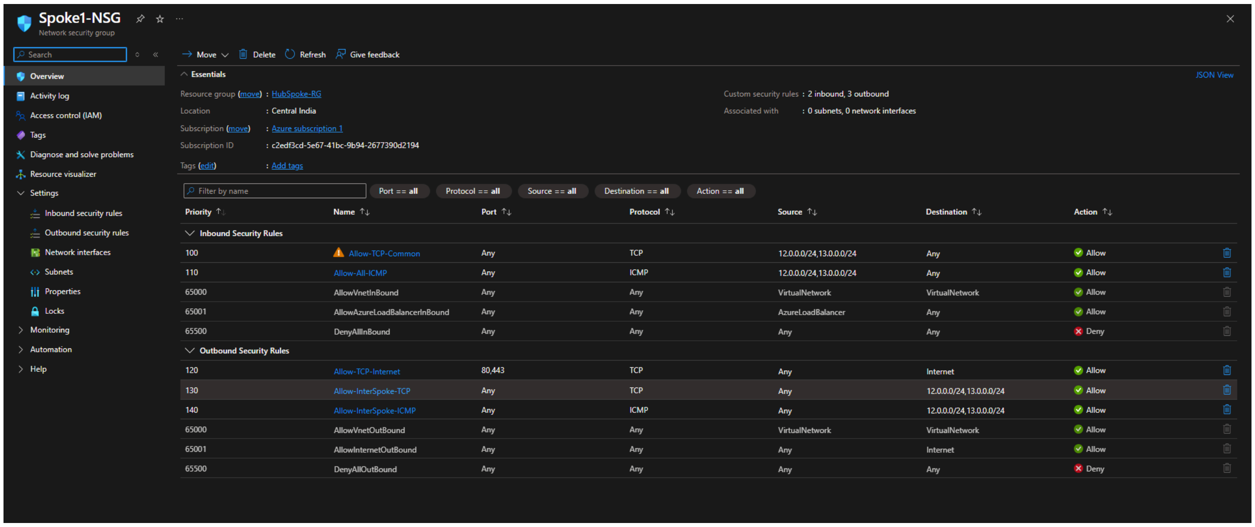
Subnets

Name	Address range	Virtual network	Security group
Workload	13.0.0.0/24	Spoke2-VNet	Spoke2-NSG

5. NSG Configuration

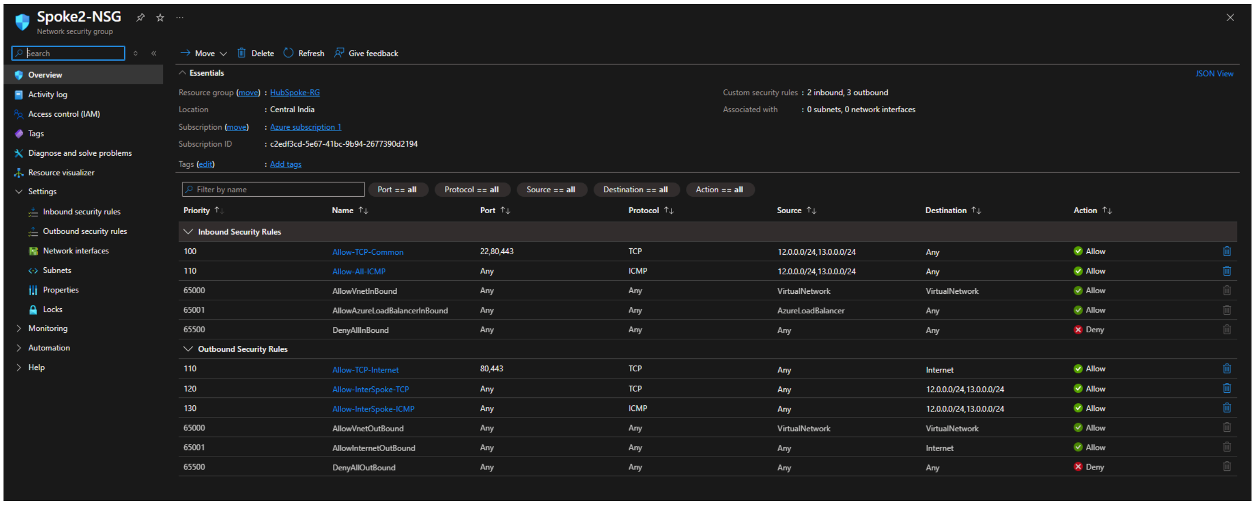
Here, in our Hub-and-Spoke Azure network architecture, we have used Network Security Groups (NSGs) to control traffic flow to and from the virtual machines deployed inside the Spoke1 and Spoke2 subnets. NSG acts like a virtual firewall that allows or denies traffic based on rules we define. It is essential for protecting our resources and ensuring only trusted communication happens across the network.

We created separate NSGs for both spokes — Spoke1-NSG and Spoke2-NSG — and associated them directly with their respective subnets. This means any virtual machine placed in those subnets automatically follows the NSG rules, ensuring centralized and consistent security.



Resource group (move) : HubSpoke-RG
Location : Central India
Subscription (move) : Azure subscription 1
Subscription ID : c2edf3cd-5e67-41bc-9b94-2677390d2194
Tags (edit) : Add tags
Custom security rules : 2 inbound, 3 outbound
Associated with : 0 subnets, 0 network interfaces

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
100	⚠ Allow-TCP-Common	Any	TCP	12.0.0.0/24,13.0.0.0/24	Any	✓ Allow
110	Allow-All-ICMP	Any	ICMP	12.0.0.0/24,13.0.0.0/24	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny
Outbound Security Rules						
120	Allow-TCP-Internet	80,443	TCP	Any	Internet	✓ Allow
130	Allow-InterSpoke-TCP	Any	TCP	Any	12.0.0.0/24,13.0.0.0/24	✓ Allow
140	Allow-InterSpoke-ICMP	Any	ICMP	Any	12.0.0.0/24,13.0.0.0/24	✓ Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny



Resource group (move) : HubSpoke-RG
Location : Central India
Subscription (move) : Azure subscription 1
Subscription ID : c2edf3cd-5e67-41bc-9b94-2677390d2194
Tags (edit) : Add tags
Custom security rules : 2 inbound, 3 outbound
Associated with : 0 subnets, 0 network interfaces

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
100	Allow-TCP-Common	22,80,443	TCP	12.0.0.0/24,13.0.0.0/24	Any	✓ Allow
110	Allow-All-ICMP	Any	ICMP	12.0.0.0/24,13.0.0.0/24	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny
Outbound Security Rules						
110	Allow-TCP-Internet	80,443	TCP	Any	Internet	✓ Allow
120	Allow-InterSpoke-TCP	Any	TCP	Any	12.0.0.0/24,13.0.0.0/24	✓ Allow
130	Allow-InterSpoke-ICMP	Any	ICMP	Any	12.0.0.0/24,13.0.0.0/24	✓ Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny

Allows inbound traffic for essential services:

- **SSH (port 22), HTTP (80), HTTPS (443) from trusted IP ranges (Spoke1 and Spoke2)**
- **ICMP (ping) for network testing between VMs**

Allows outbound traffic to:

- **The Internet (ports 80 and 443) so VMs can access websites**
- **Other VMs in the peer spoke subnet for inter-VM communication**
- **Firewall and DNS for name resolution and routing**

Blocks all other traffic by default to follow the Zero Trust model, where only what's needed is allowed, and everything else is denied for safety

6. Azure Firewall Rule Configuration

Once the Hub-and-Spoke architecture was established and all traffic from the spoke VNets was routed through the Azure Firewall in the Hub-VNet, it became necessary to define explicit firewall rules to allow essential traffic. Azure Firewall, by default, blocks all inbound and outbound traffic, so carefully crafted Network Rules and Application Rules were implemented to allow only legitimate communication.

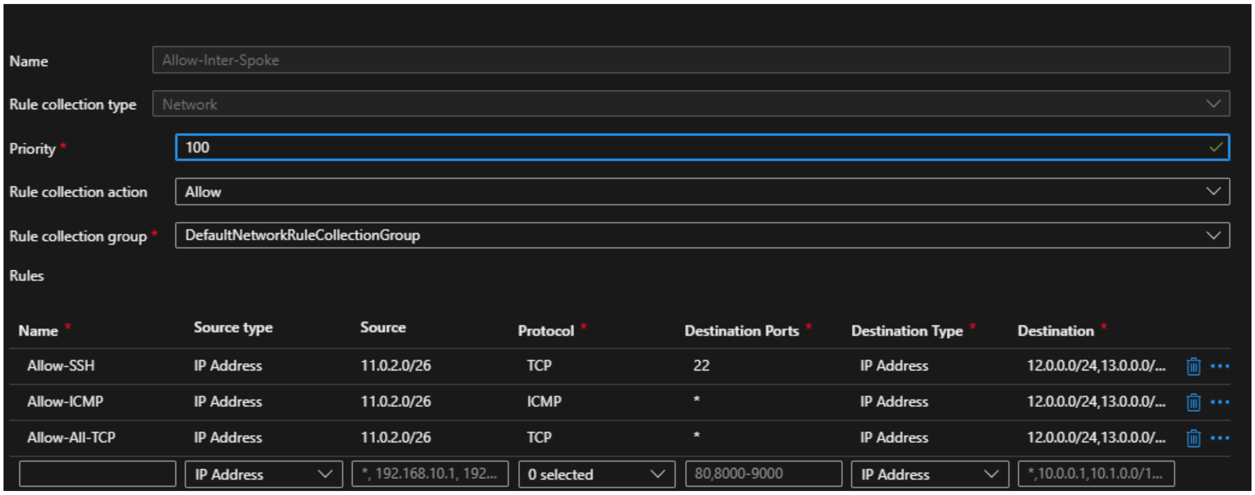
Network Rule Configuration – `Allow-Inter-Spoke`

To enable secure remote access via Azure Bastion, a Network Rule Collection named `Allow-Inter-Spoke` was configured in the Firewall Policy.

- Source Subnet:
  - `11.0.0.0/24` (Hub-VNet – AzureBastionSubnet)
- Destination Subnets:
  - `12.0.0.0/24` (Spoke-VNet-1 – Workload Subnet)
  - `13.0.0.0/24` (Spoke-VNet-2 – Workload Subnet)
- Protocol:
  - `TCP Port 22`– Required for SSH

This rule allows Azure Bastion to initiate browser-based SSH sessions to VMs in spoke networks without assigning public IPs to the VMs, eliminating exposure to the public internet and preventing common threats like brute-force or port scanning attacks.

Also allowed ICMP for the inter communication to test using PIng.



Name	Allow-Inter-Spoke
Rule collection type	Network
Priority *	100
Rule collection action	Allow
Rule collection group *	DefaultNetworkRuleCollectionGroup

Rules

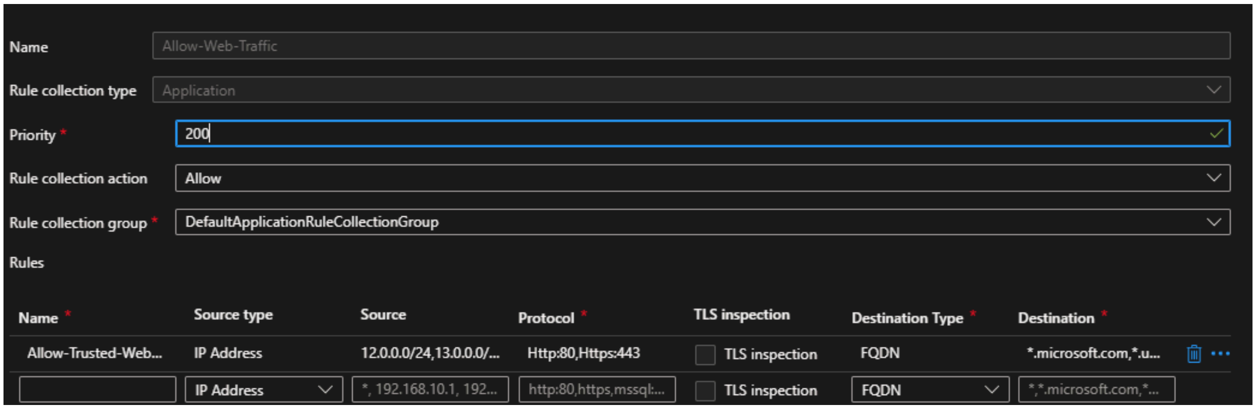
Name *	Source type	Source	Protocol *	Destination Ports *	Destination Type *	Destination *
Allow-SSH	IP Address	11.0.2.0/26	TCP	22	IP Address	12.0.0.0/24,13.0.0.0/...
Allow-ICMP	IP Address	11.0.2.0/26	ICMP	*	IP Address	12.0.0.0/24,13.0.0.0/...
Allow-All-TCP	IP Address	11.0.2.0/26	TCP	*	IP Address	12.0.0.0/24,13.0.0.0/...
	IP Address	*, 192.168.10.1, 192...	0 selected	80,8000-9000	IP Address	*,10.0.0.1,10.1.0.0/1...

Application Rule Configuration – `Allow-Web-Traffic`

To permit outbound internet access from the spoke VNets while maintaining strict control, an Application Rule Collection named `Allow-Web-Traffic` was created in the Azure Firewall Policy.

- **Source Subnets:**
  - `12.0.0.0/24` **(Spoke-VNet-1 – Workload Subnet)**
  - `13.0.0.0/24` **(Spoke-VNet-2 – Workload Subnet)**
- **Allowed Protocols:**
  - `HTTP (Port 80)`
  - `HTTPS (Port 443)`
- **Destination FQDNs (Fully Qualified Domain Names):**
  - `*.microsoft.com` **– For Azure and Microsoft services**
  - `*.ubuntu.com` **– For Linux package updates**
  - `*.github.com` **– For source code access and version control**
  - `google.com` **– For internet access**

This rule ensures that only trusted websites can be accessed by VMs, while all other outbound traffic is blocked, aligning with best practices for security and governance.

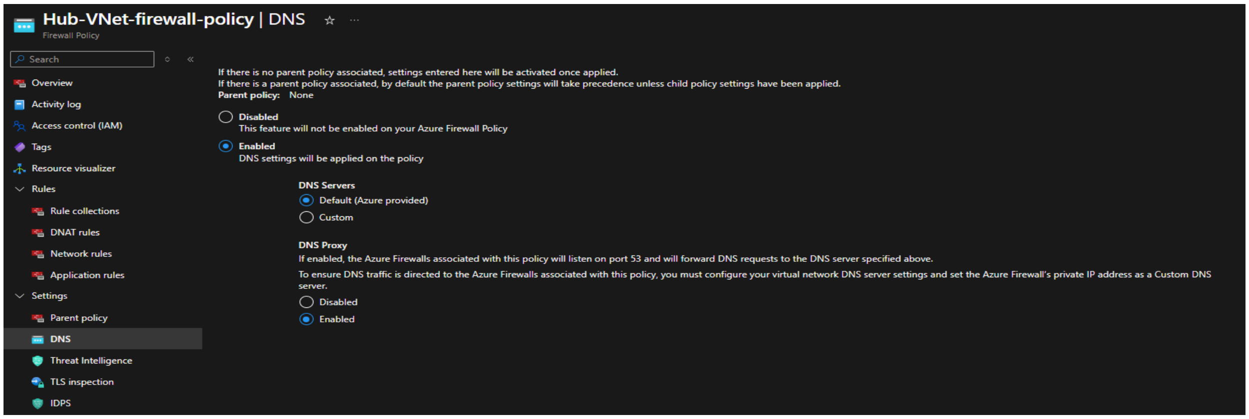


Name	Allow-Web-Traffic
Rule collection type	Application
Priority *	200
Rule collection action	Allow
Rule collection group *	DefaultApplicationRuleCollectionGroup

Rules

Name *	Source type	Source	Protocol *	TLS inspection	Destination Type *	Destination
Allow-Trusted-Web...	IP Address	12.0.0.0/24,13.0.0.0/...	Http:80,Https:443	□ TLS inspection	FQDN	*.microsoft.com,*.u...
	IP Address	*, 192.168.10.1, 192...	http:80,https,mssql:...	□ TLS inspection	FQDN	*,*.microsoft.com,*...

We have also enabled DNS Service on our Firewall Policy.



Hub-VNet-firewall-policy | DNS

Firewall Policy

If there is no parent policy associated, settings entered here will be activated once applied.
If there is a parent policy associated, by default the parent policy settings will take precedence unless child policy settings have been applied.
Parent policy: None

○ **Disabled**
This feature will not be enabled on your Azure Firewall Policy

● **Enabled**
DNS settings will be applied on the policy

DNS Servers

● Default (Azure provided)
○ Custom

DNS Proxy

If enabled, the Azure Firewalls associated with this policy will listen on port 53 and will forward DNS requests to the DNS server specified above.

To ensure DNS traffic is directed to the Azure Firewalls associated with this policy, you must configure your virtual network DNS server settings and set the Azure Firewall's private IP address as a Custom DNS server.

○ Disabled
● Enabled

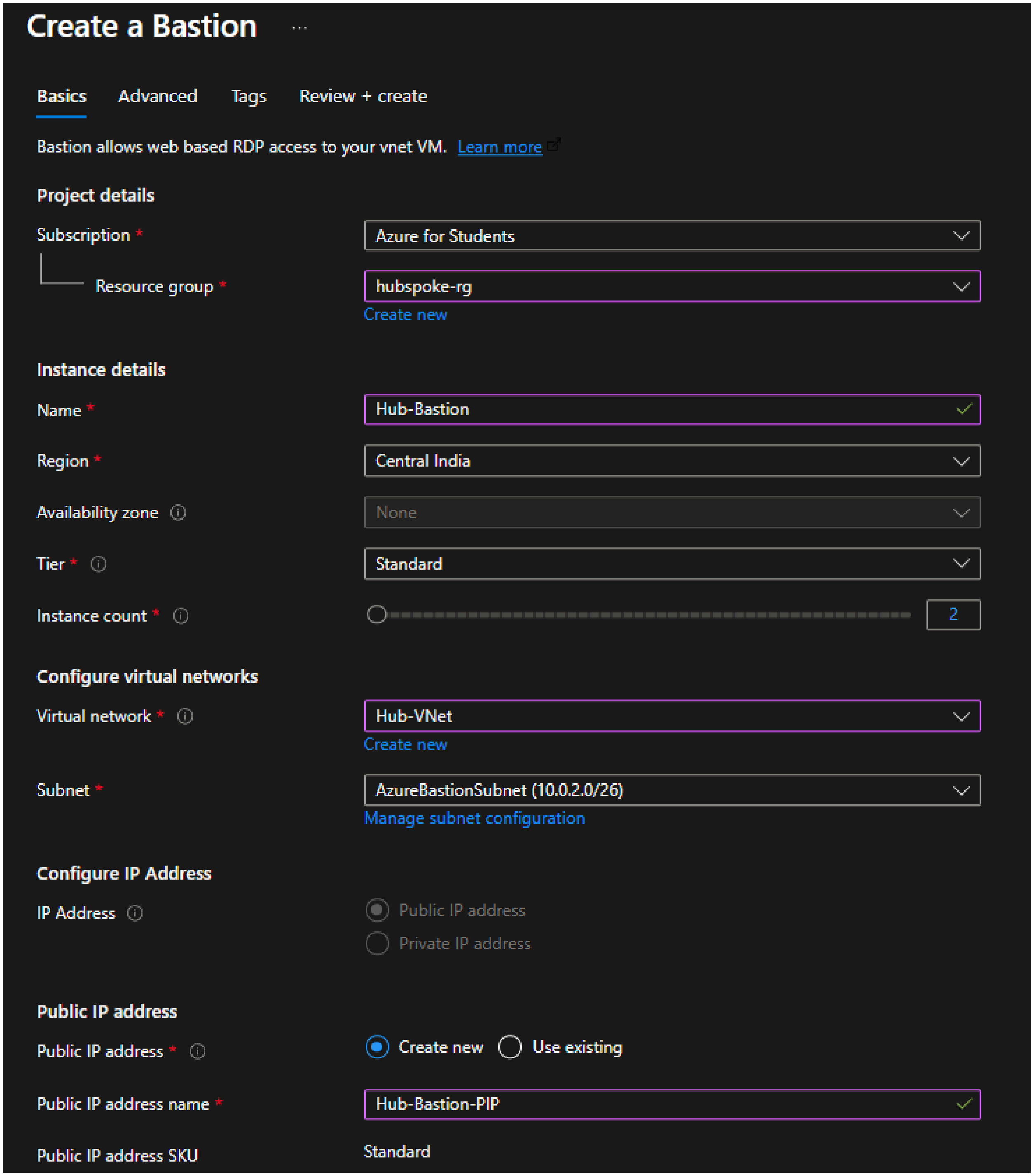
7. Azure Bastion Configuration

Azure Bastion is a secure and fully managed service that allows you to connect to virtual machines (VMs) using RDP or SSH directly from the Azure Portal, without exposing the VMs to the public internet. It removes the need for public IPs on VMs, reducing the risk of attacks like port scanning and brute-force attempts.

Why we are using Azure Bastion:

- Secure Remote Access
  Azure Bastion allows administrators to connect to virtual machines in both spoke networks using private IP addresses, eliminating the need for public IPs. This significantly reduces exposure to internet-based threats.
- Follows Zero Trust Principles
  By removing public access and enforcing controlled connections, Azure Bastion aligns with the Zero Trust security model, which is essential for enterprise-grade network protection.
- Centralized Management
  Since Bastion is deployed in the Hub-VNet, it provides a centralized way to securely access virtual machines across all peered spoke VNets. This simplifies remote access management and enhances operational efficiency.
- Works with Azure Firewall
  A network rule has been configured in Azure Firewall to allow RDP traffic from the Bastion subnet (10.0.2.0/26) to the workload subnets in the spokes. This ensures that all remote access traffic is inspected and securely routed.

Let’s create Bastion.



Create a Bastion ···

Basics | Advanced | Tags | Review + create

Bastion allows web based RDP access to your vnet VM. Learn more

Project details

Subscription * : Azure for Students

Resource group * : hubspoke-rg

Create new

Instance details

Name * : Hub-Bastion ✓

Region * : Central India

Availability zone ⓘ : None

Tier * ⓘ : Standard

Instance count * ⓘ : 2

Configure virtual networks

Virtual network * ⓘ : Hub-VNet

Create new

Subnet * : AzureBastionSubnet (10.0.2.0/26)

Manage subnet configuration

Configure IP Address

IP Address ⓘ : ● Public IP address ○ Private IP address

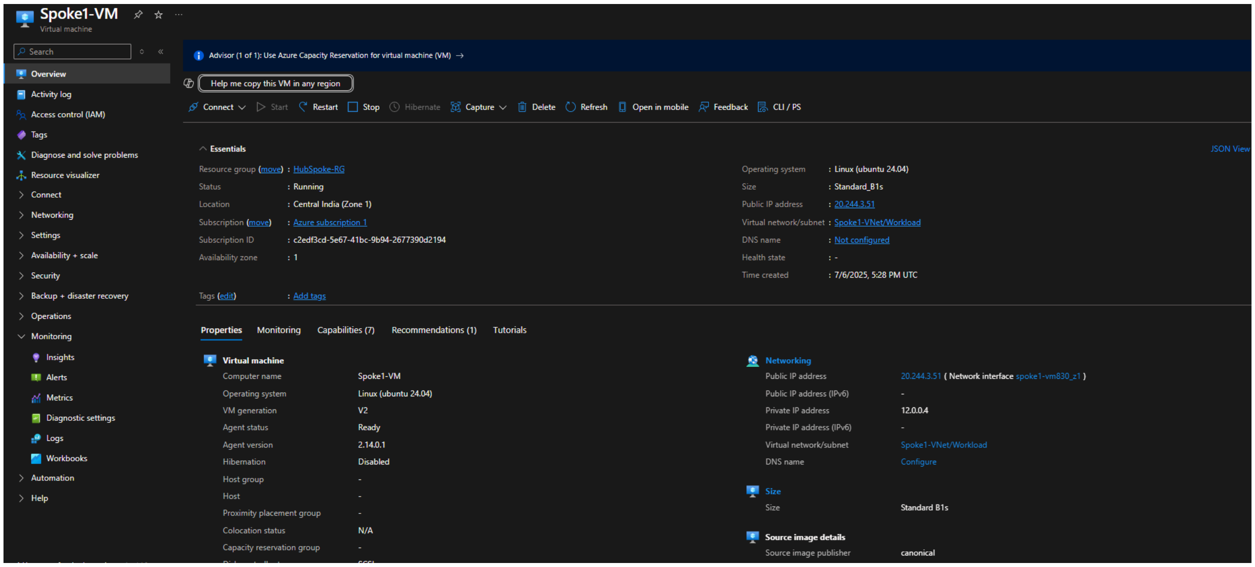
Public IP address

Public IP address * ⓘ : ● Create new ○ Use existing

Public IP address name * : Hub-Bastion-PIP ✓

Public IP address SKU : Standard

Spoke1-VM



Advisor (1 of 1): Use Azure Capacity Reservation for virtual machine (VM) →

Essentials

Resource group (move)	: HubSpoke-RG
Status	: Running
Location	: Central India (Zone 1)
Subscription (move)	: Azure subscription 1
Subscription ID	: c2edf3cd-5e67-41bc-9b94-2677390d2194
Availability zone	: 1
Tags (edit)	: Add tags

Operating system	: Linux (ubuntu 24.04)
Size	: Standard_B1s
Public IP address	: 20.244.3.51
Virtual network/subnet	: Spoke1-VNet/Workload
DNS name	: Not configured
Health state	: -
Time created	: 7/6/2025, 5:28 PM UTC

Virtual machine

Computer name	Spoke1-VM
Operating system	Linux (ubuntu 24.04)
VM generation	V2
Agent status	Ready
Agent version	2.14.0.1
Hibernation	Disabled
Host group	-
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-

Networking

Public IP address	20.244.3.51 (Network interface spoke1-vm830_z1)
Public IP address (IPv6)	-
Private IP address	12.0.0.4
Private IP address (IPv6)	-
Virtual network/subnet	Spoke1-VNet/Workload
DNS name	Configure

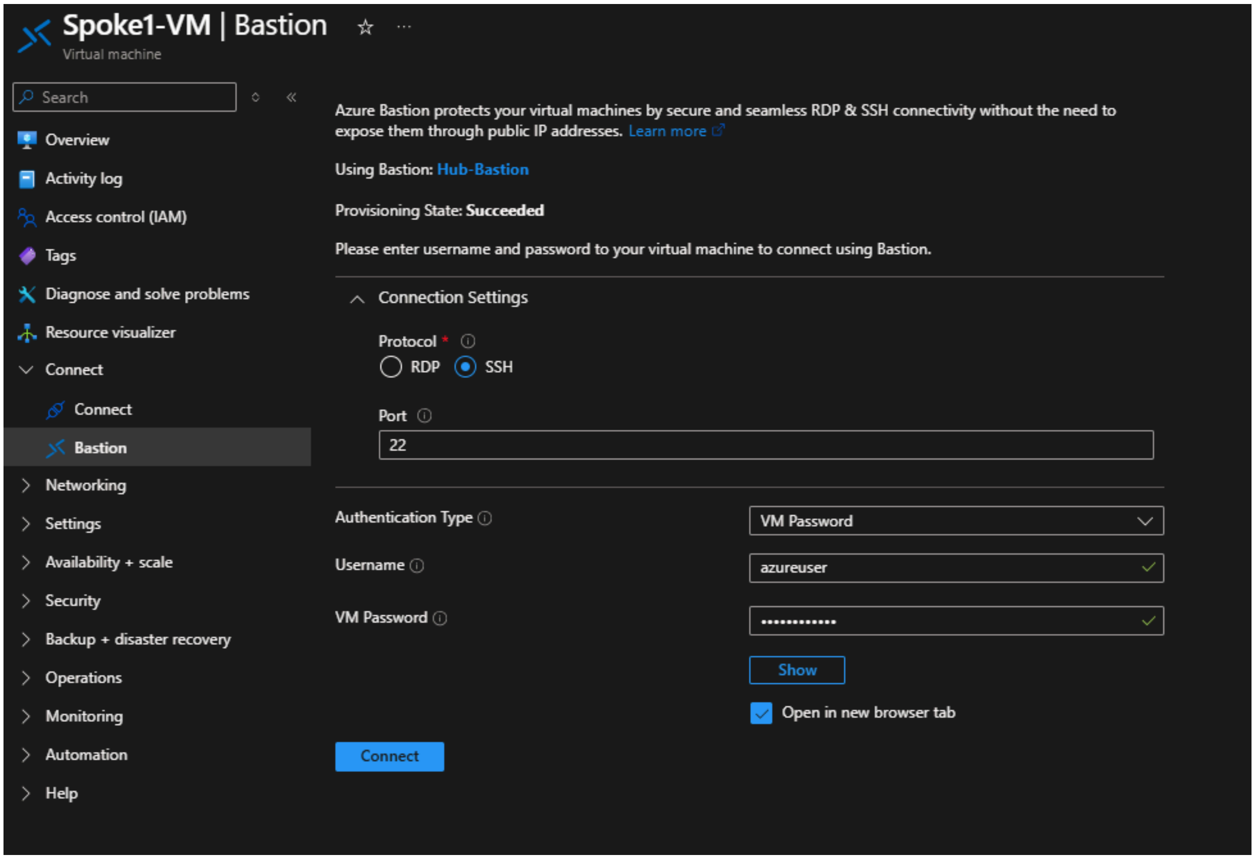
Size

Size	Standard B1s

Source image details

Source image publisher	canonical

Connect via Bastion



Azure Bastion protects your virtual machines by secure and seamless RDP & SSH connectivity without the need to expose them through public IP addresses. Learn more

Using Bastion: Hub-Bastion

Provisioning State: Succeeded

Please enter username and password to your virtual machine to connect using Bastion.

Connection Settings

Protocol * ○ RDP ● SSH

Port: 22

Authentication Type: VM Password

Username: azureuser

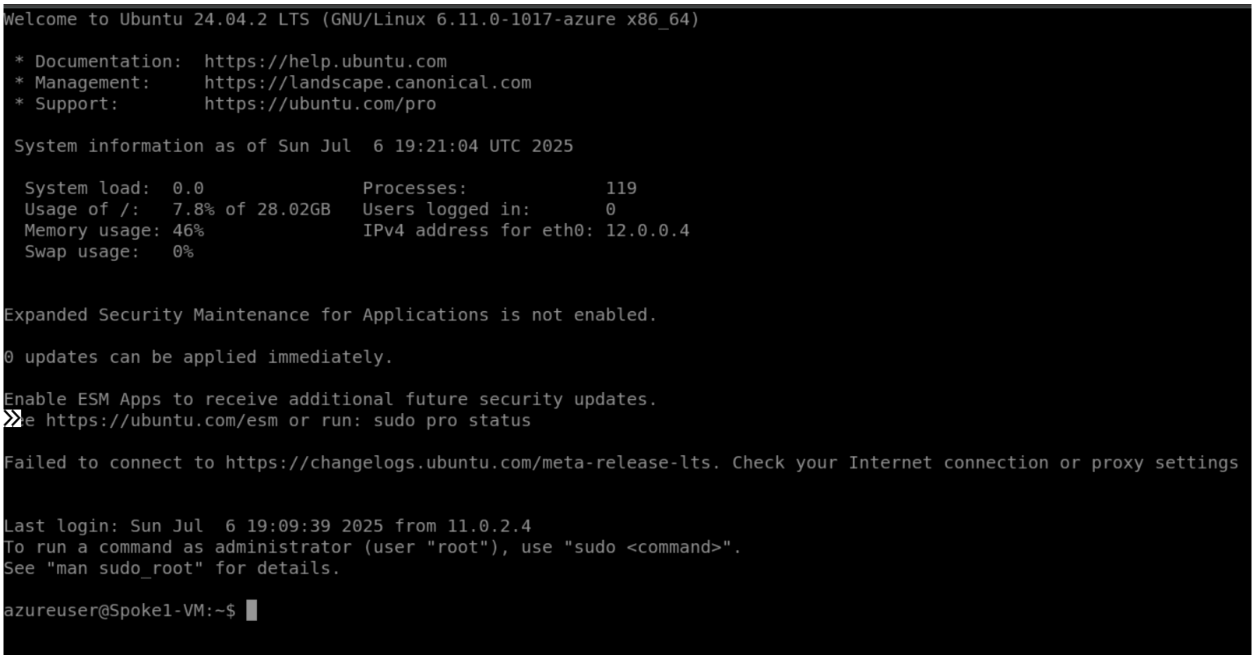
VM Password: ••••••••••••

☑ Open in new browser tab

Connect to VM using Bastion

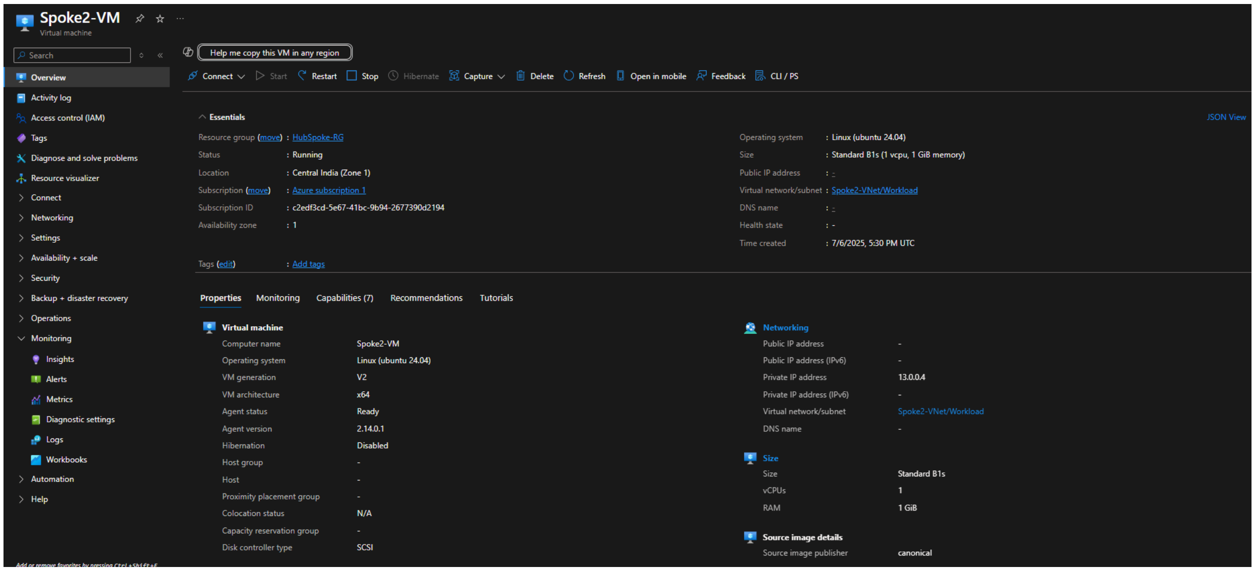
On the Bastion connection panel we have to provide the Username and Password which we have set during VM creation.

Connected to VM Successfully.



```
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-1017-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Jul  6 19:21:04 UTC 2025

  System load:  0.0               Processes:             119
  Usage of /:   7.8% of 28.02GB   Users logged in:       0
  Memory usage: 46%               IPv4 address for eth0: 12.0.0.4
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
 e https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Sun Jul  6 19:09:39 2025 from 11.0.2.4
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

azureuser@Spoke1-VM:~$ 
```

Spoke2-VM



Essentials

Resource group (move) : HubSpoke-RG
Status : Running
Location : Central India (Zone 1)
Subscription (move) : Azure subscription 1
Subscription ID : c2edf3cd-5e67-41bc-9b94-2677390d2194
Availability zone : 1

Tags (edit) : Add tags

Operating system : Linux (ubuntu 24.04)
Size : Standard B1s (1 vcpu, 1 GiB memory)
Public IP address : -
Virtual network/subnet : Spoke2-VNet/Workload
DNS name : -
Health state : -
Time created : 7/6/2025, 5:30 PM UTC

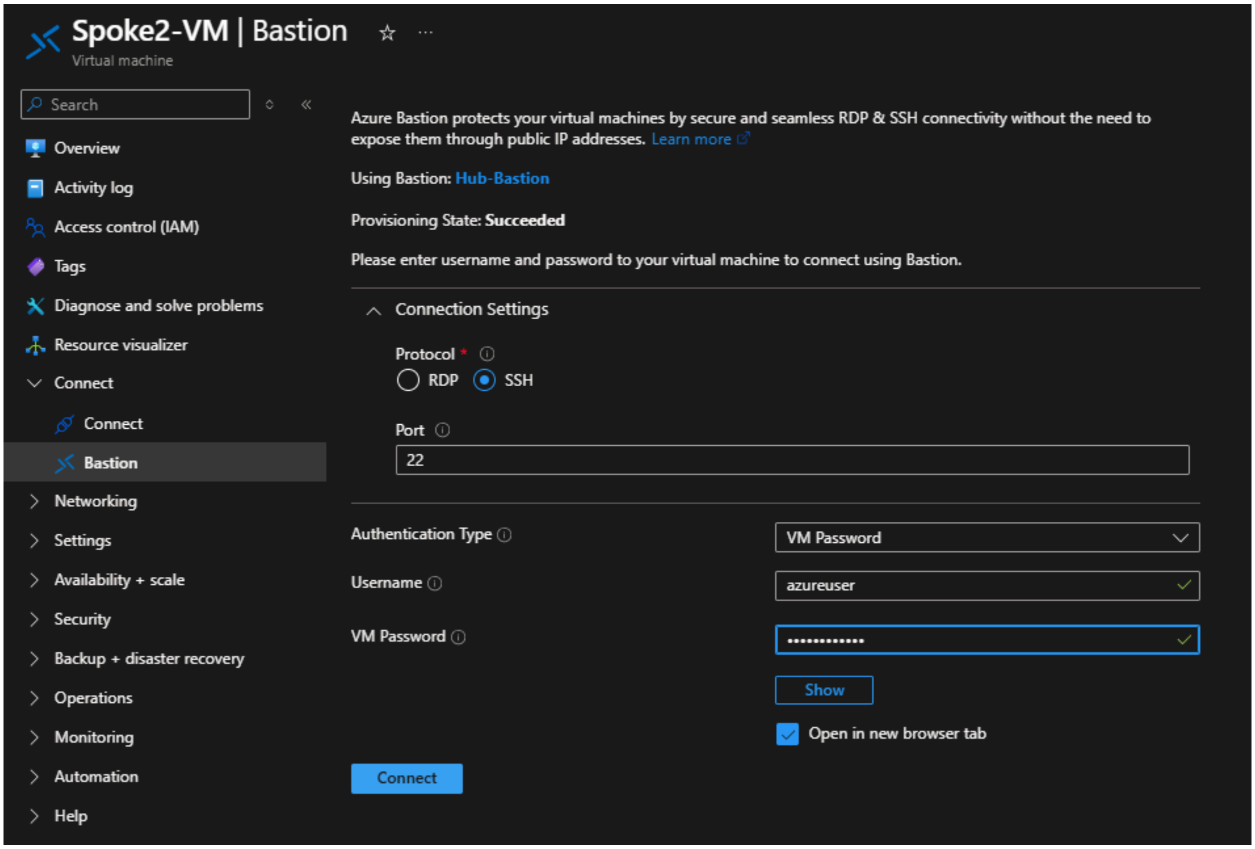
Virtual machine	
Computer name	Spoke2-VM
Operating system	Linux (ubuntu 24.04)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.14.0.1
Hibernation	Disabled
Host group	-
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-
Disk controller type	SCSI

Networking	
Public IP address	-
Public IP address (IPv6)	-
Private IP address	13.0.0.4
Private IP address (IPv6)	-
Virtual network/subnet	Spoke2-VNet/Workload
DNS name	-

Size	
Size	Standard B1s
vCPUs	1
RAM	1 GiB

Source image details	
Source image publisher	canonical

Connect via Bastion



Azure Bastion protects your virtual machines by secure and seamless RDP & SSH connectivity without the need to expose them through public IP addresses. Learn more

Using Bastion: Hub-Bastion

Provisioning State: **Succeeded**

Please enter username and password to your virtual machine to connect using Bastion.

Connection Settings

Protocol *

○ RDP ● SSH

Port: 22

Authentication Type: VM Password

Username: azureuser

VM Password: ••••••••••••

Show

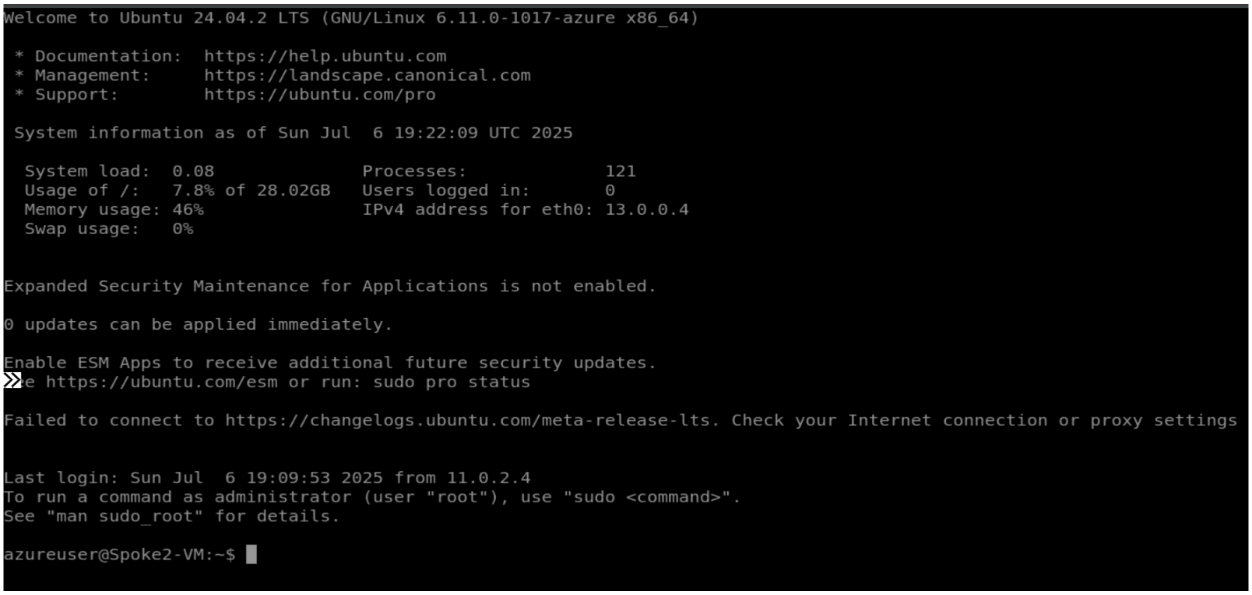
☑ Open in new browser tab

Connect

Connect to VM using Bastion

On the Bastion connection panel we have to provide the Username and Password which we have set during VM creation.

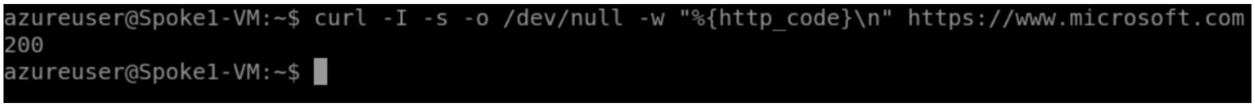
Connected to VM Successfully.



```
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-1017-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Jul  6 19:22:09 UTC 2025

  System load:  0.08              Processes:             121
  Usage of /:   7.8% of 28.02GB   Users logged in:       0
  Memory usage: 46%               IPv4 address for eth0: 13.0.0.4
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Sun Jul  6 19:09:53 2025 from 11.0.2.4
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

azureuser@Spoke2-VM:~$ █
```

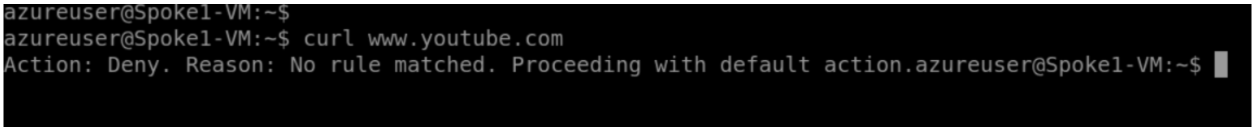
8. Test Traffic

We have allowed traffic from some site like *.microsoft.com, *.windowsupdate.com, *.ubuntu.com, *.github.com



```
azureuser@Spoke1-VM:~$ curl -I -s -o /dev/null -w "%{http_code}\n" https://www.microsoft.com
200
azureuser@Spoke1-VM:~$ 
```

Now if we try other than this traffic it will not allow us to do so because we have blocked all the traffic from outside.

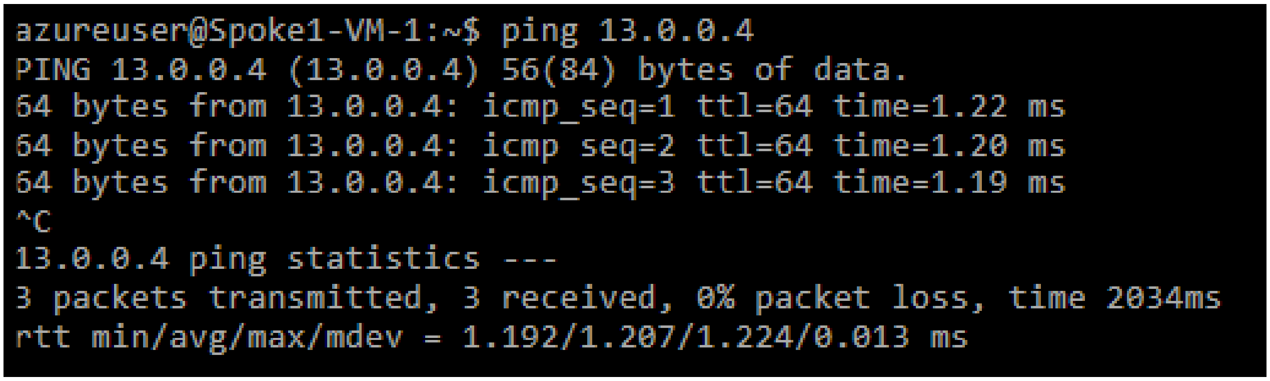


```
azureuser@Spoke1-VM:~$
azureuser@Spoke1-VM:~$ curl www.youtube.com
Action: Deny. Reason: No rule matched. Proceeding with default action.azureuser@Spoke1-VM:~$ 
```

As we can see Action: Deny. Reason: No rule matched. Means it is not allowing other traffic then which is allowed.

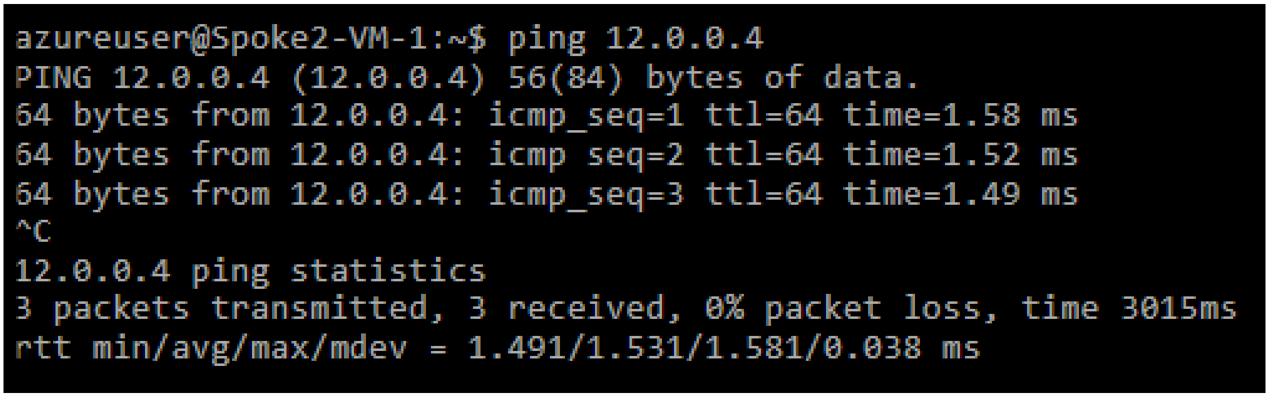
We also have tested this ping from one Subnet 1 VM to Subnet 2 VM and Vice Versa which is working perfectly.

Spoke 1



```
azureuser@Spoke1-VM-1:~$ ping 13.0.0.4
PING 13.0.0.4 (13.0.0.4) 56(84) bytes of data.
64 bytes from 13.0.0.4: icmp_seq=1 ttl=64 time=1.22 ms
64 bytes from 13.0.0.4: icmp seq=2 ttl=64 time=1.20 ms
64 bytes from 13.0.0.4: icmp_seq=3 ttl=64 time=1.19 ms
^C
13.0.0.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2034ms
rtt min/avg/max/mdev = 1.192/1.207/1.224/0.013 ms
```

Spoke 2



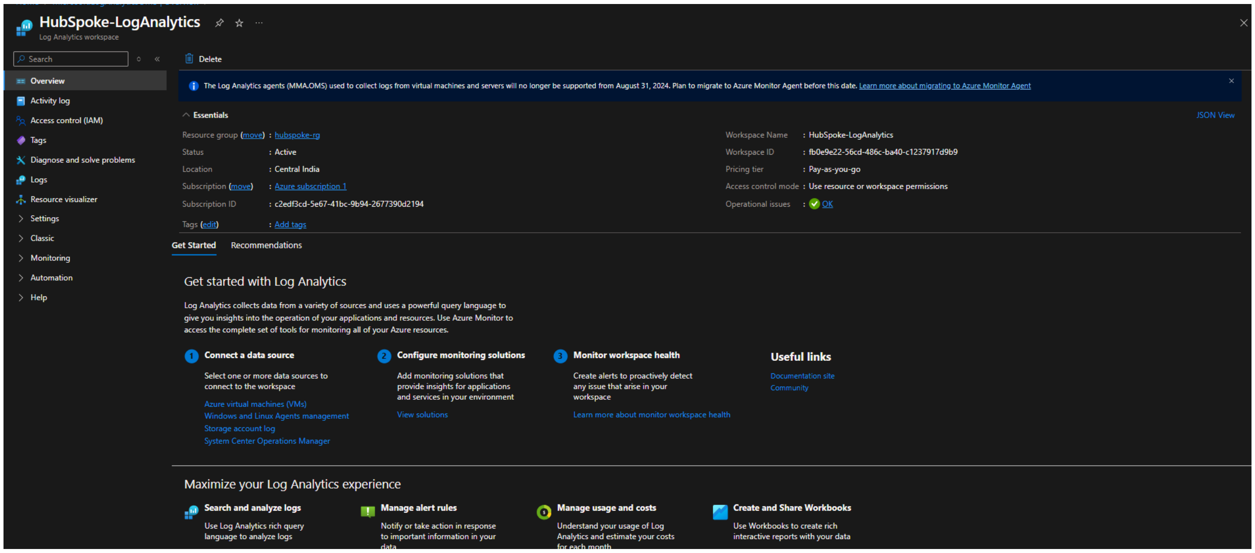
```
azureuser@Spoke2-VM-1:~$ ping 12.0.0.4
PING 12.0.0.4 (12.0.0.4) 56(84) bytes of data.
64 bytes from 12.0.0.4: icmp_seq=1 ttl=64 time=1.58 ms
64 bytes from 12.0.0.4: icmp seq=2 ttl=64 time=1.52 ms
64 bytes from 12.0.0.4: icmp_seq=3 ttl=64 time=1.49 ms
^C
12.0.0.4 ping statistics
3 packets transmitted, 3 received, 0% packet loss, time 3015ms
rtt min/avg/max/mdev = 1.491/1.531/1.581/0.038 ms
```

9. Logs and Analysis

To ensure complete visibility, monitoring, and troubleshooting across our Hub-and-Spoke architecture, we have implemented a centralized logging and monitoring system using Azure Log Analytics, NSG Flow Logs, Traffic Analytics, and VM Insights.

Log Analytics Workspace (LAW)

We created a centralized Log Analytics Workspace named `HubSpoke-LogAnalytics` to collect and analyze logs from all critical Azure resources. This workspace is the backbone for storing diagnostic and performance data.



The Log Analytics agents (MMA.OMS) used to collect logs from virtual machines and servers will no longer be supported from August 31, 2024. Plan to migrate to Azure Monitor Agent before this date. Learn more about migrating to Azure Monitor Agent

Essentials

Resource group (move)	: hubspoke-rg	Workspace Name	: HubSpoke-LogAnalytics
Status	: Active	Workspace ID	: fb0e9e22-56cd-486c-ba40-c1237917d9b9
Location	: Central India	Pricing tier	: Pay-as-you-go
Subscription (move)	: Azure subscription 1	Access control mode	: Use resource or workspace permissions
Subscription ID	: c2edf3cd-5e67-41bc-9b94-2677390d2194	Operational issues	: ✓ OK
Tags (edit)	: Add tags		

Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

1 Connect a data source

Select one or more data sources to connect to the workspace

Azure virtual machines (VMs)
Windows and Linux Agents management
Storage account log
System Center Operations Manager

2 Configure monitoring solutions

Add monitoring solutions that provide insights for applications and services in your environment

View solutions

3 Monitor workspace health

Create alerts to proactively detect any issue that arise in your workspace

Learn more about monitor workspace health

Useful links

Documentation site
Community

Maximize your Log Analytics experience

Search and analyze logs

Use Log Analytics rich query language to analyze logs

Manage alert rules

Notify or take action in response to important information in your data

Manage usage and costs

Understand your usage of Log Analytics and estimate your costs for each month

Create and Share Workbooks

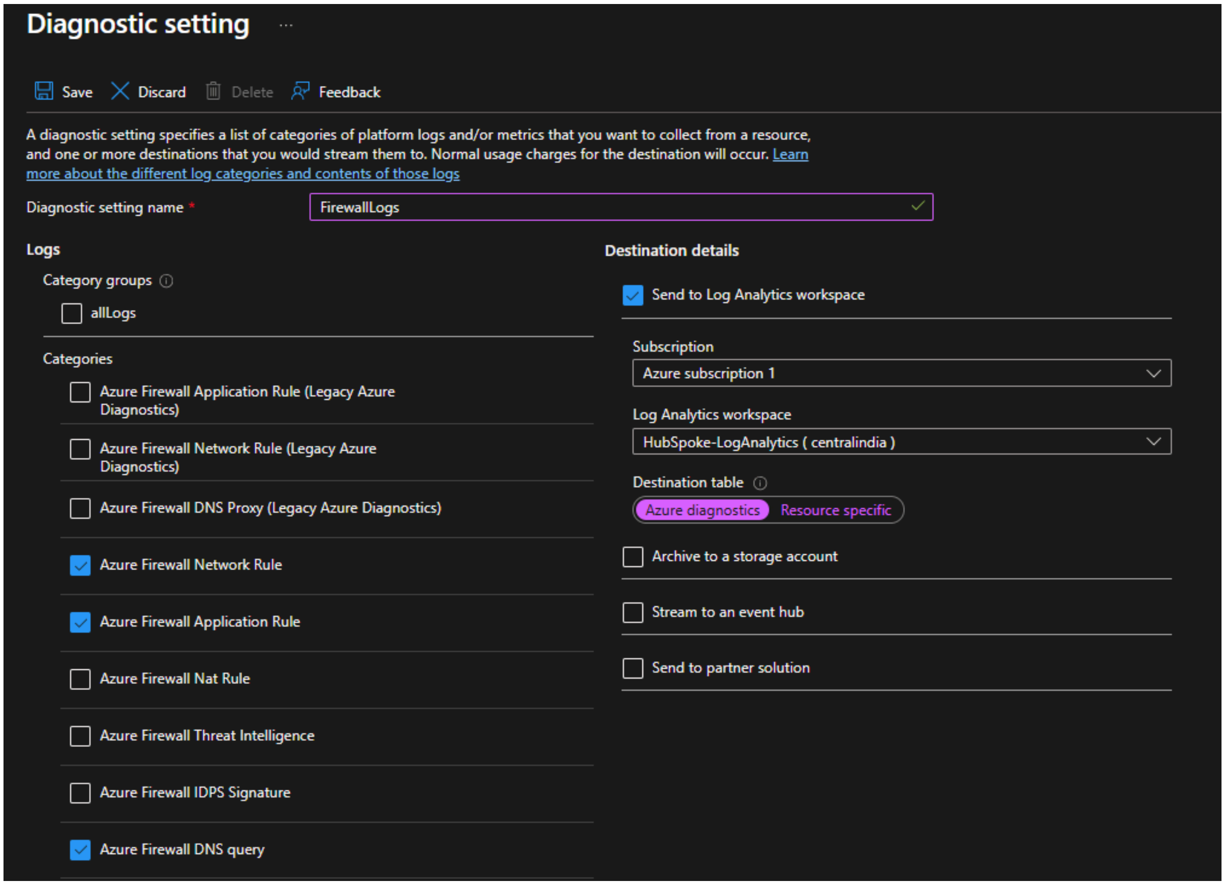
Use Workbooks to create rich interactive reports with your data

Azure Firewall Diagnostic Logs

We enabled diagnostic logging on the Azure Firewall and connected it to the Log Analytics Workspace. The following logs and metrics were configured:

- **Network Rule Logs – to track IP-based rule matches**
- **Application Rule Logs – to track FQDN/URL-based rule matches**
- **DNS Proxy Logs – to monitor name resolution requests**
- **Firewall Metrics – to gather traffic statistics and health metrics**

This helps us inspect what traffic is being allowed/denied and verify if the firewall is correctly enforcing security policies.



Diagnostic setting ...

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs

Diagnostic setting name * FirewallLogs

Logs

Category groups

□ allLogs

Categories

□ Azure Firewall Application Rule (Legacy Azure Diagnostics)

□ Azure Firewall Network Rule (Legacy Azure Diagnostics)

□ Azure Firewall DNS Proxy (Legacy Azure Diagnostics)

☑ Azure Firewall Network Rule

☑ Azure Firewall Application Rule

□ Azure Firewall Nat Rule

□ Azure Firewall Threat Intelligence

□ Azure Firewall IDPS Signature

☑ Azure Firewall DNS query

Destination details

☑ Send to Log Analytics workspace

Subscription: Azure subscription 1

Log Analytics workspace: HubSpoke-LogAnalytics (centralindia)

Destination table: [✓ Azure diagnostics] Resource specific

□ Archive to a storage account

□ Stream to an event hub

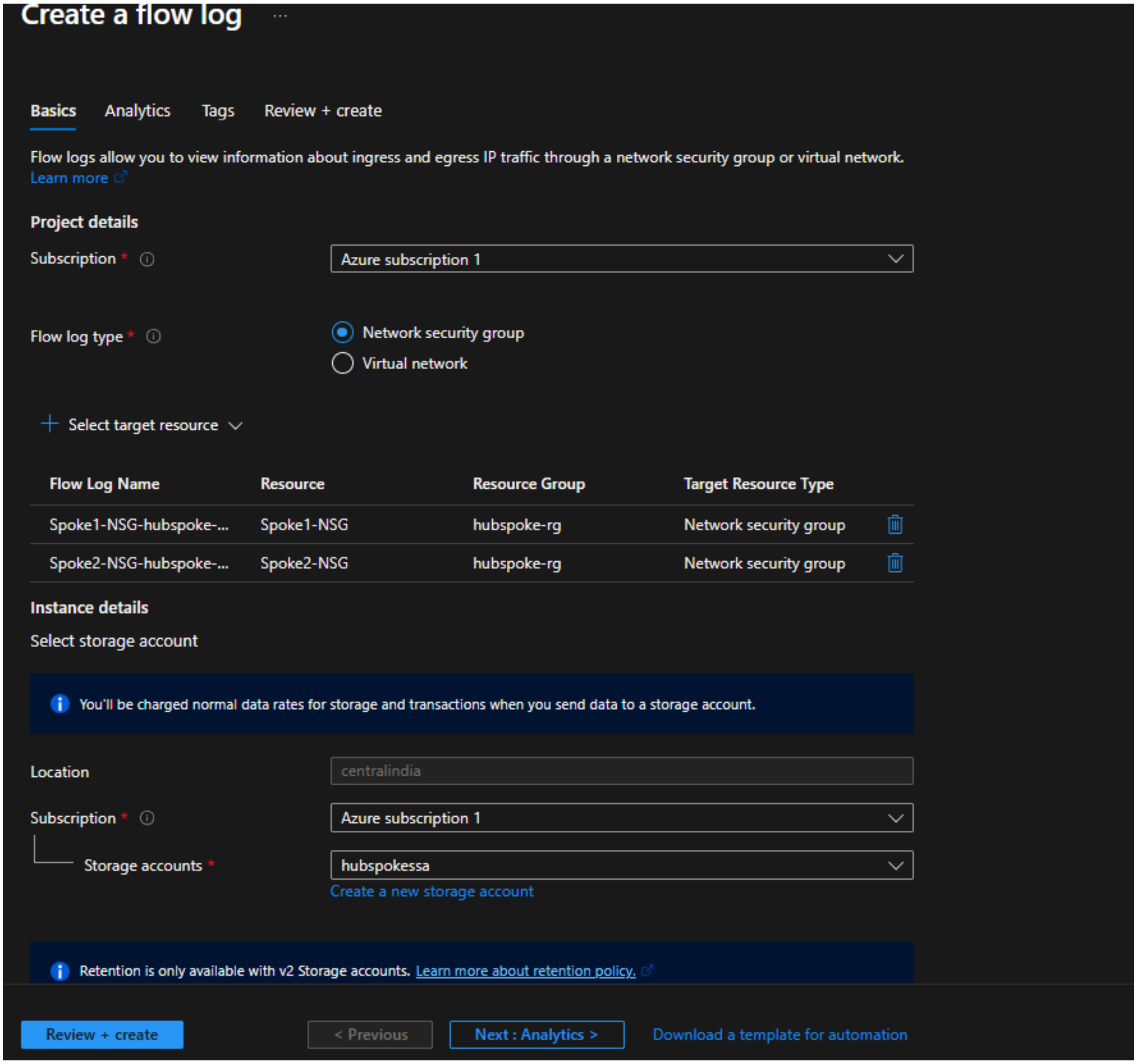
□ Send to partner solution

NSG Flow Logs

To monitor traffic flowing through the Spoke1-NSG and Spoke2-NSG, we enabled NSG Flow Logs (version 2):

- **A Storage Account named `hubspokestorageacc` was created as required for storing raw flow logs.**
- **Flow logs were enabled for both NSGs associated with the Spoke subnets.**
- **We also enabled Traffic Analytics, which provides summarized insights into top talkers, traffic trends, allowed/denied flows, and more.**

This ensures complete visibility into which traffic is passing through or being blocked by our NSGs.



Create a flow log

Flow logs allow you to view information about ingress and egress IP traffic through a network security group or virtual network. Learn more

Project details

Subscription * : Azure subscription 1

Flow log type * : ● Network security group ○ Virtual network

Flow Log Name	Resource	Resource Group	Target Resource Type
Spoke1-NSG-hubspoke-...	Spoke1-NSG	hubspoke-rg	Network security group
Spoke2-NSG-hubspoke-...	Spoke2-NSG	hubspoke-rg	Network security group

Instance details

Select storage account

You'll be charged normal data rates for storage and transactions when you send data to a storage account.

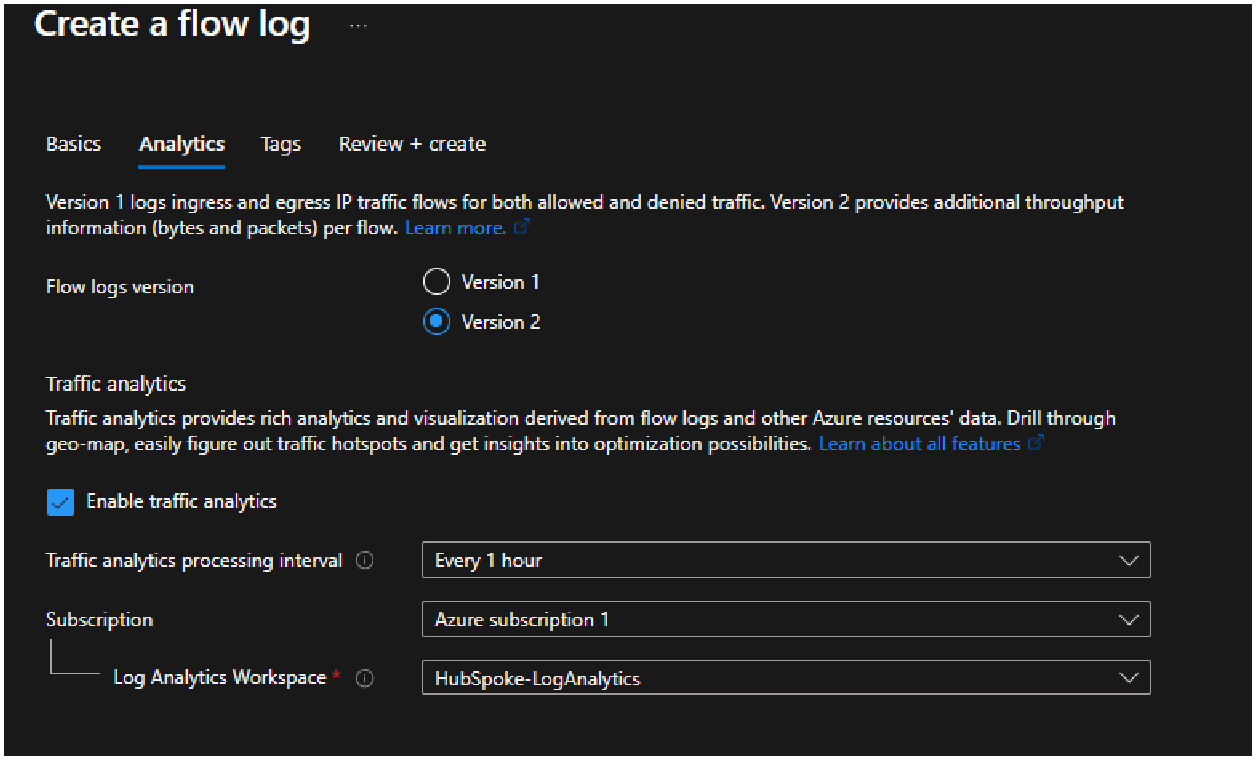
Location: centralindia

Subscription * : Azure subscription 1

Storage accounts * : hubspokessa

Create a new storage account

Retention is only available with v2 Storage accounts. Learn more about retention policy.



Create a flow log ···

Version 1 logs ingress and egress IP traffic flows for both allowed and denied traffic. Version 2 provides additional throughput information (bytes and packets) per flow. Learn more.

Flow logs version

○ Version 1

● Version 2

Traffic analytics

Traffic analytics provides rich analytics and visualization derived from flow logs and other Azure resources' data. Drill through geo-map, easily figure out traffic hotspots and get insights into optimization possibilities. Learn about all features

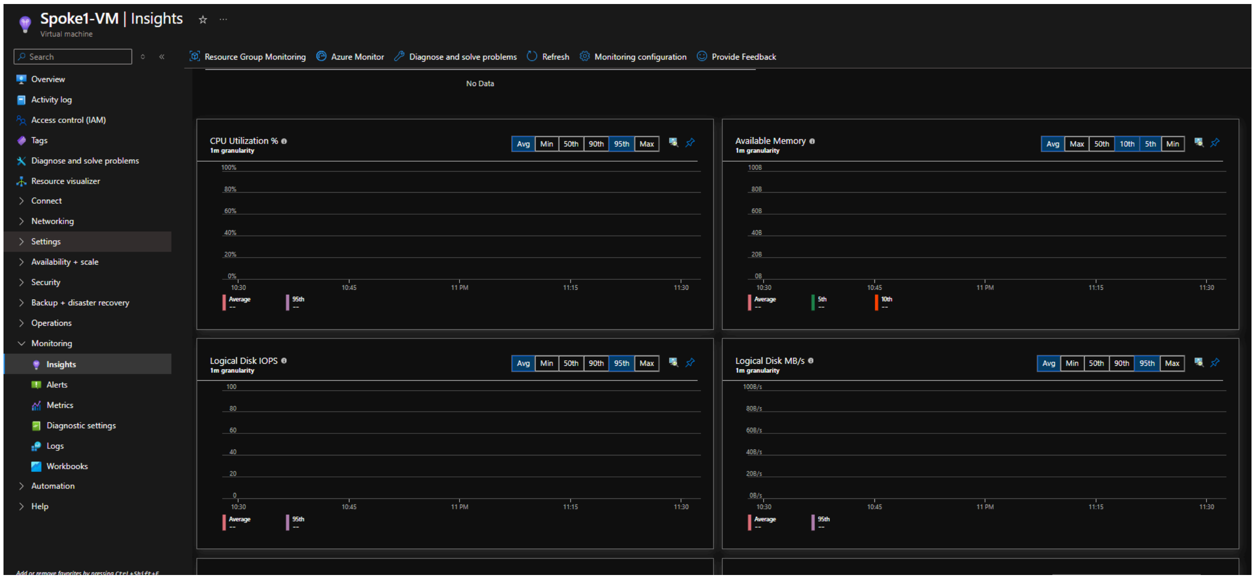
☑ Enable traffic analytics

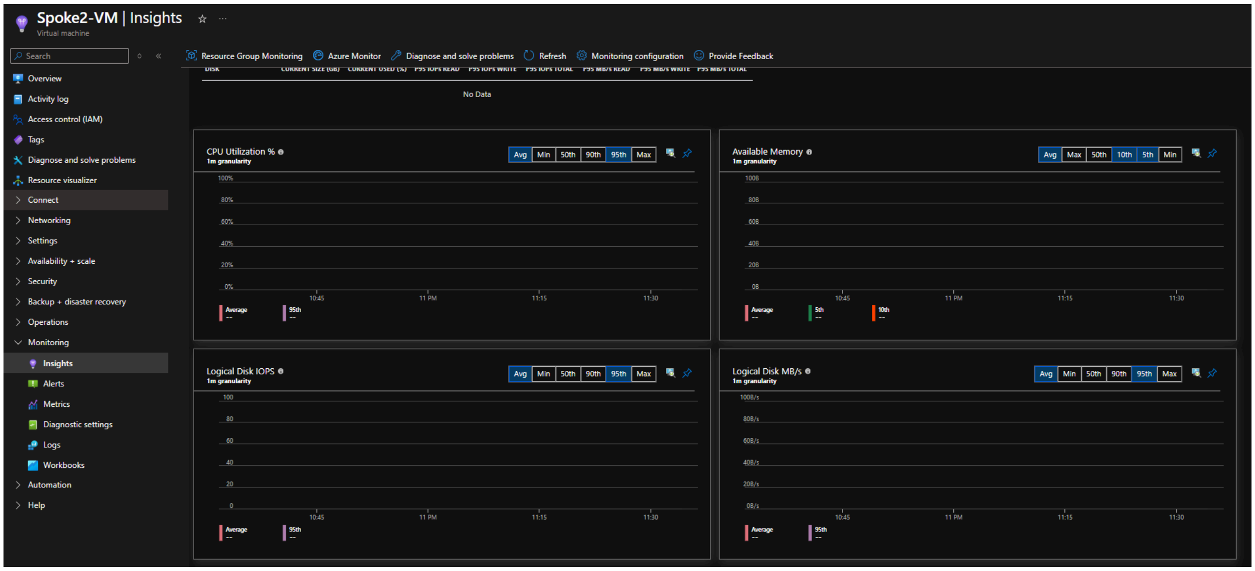
Traffic analytics processing interval ⓘ	Every 1 hour
Subscription	Azure subscription 1
Log Analytics Workspace * ⓘ	HubSpoke-LogAnalytics

VM Insights (Performance Monitoring)

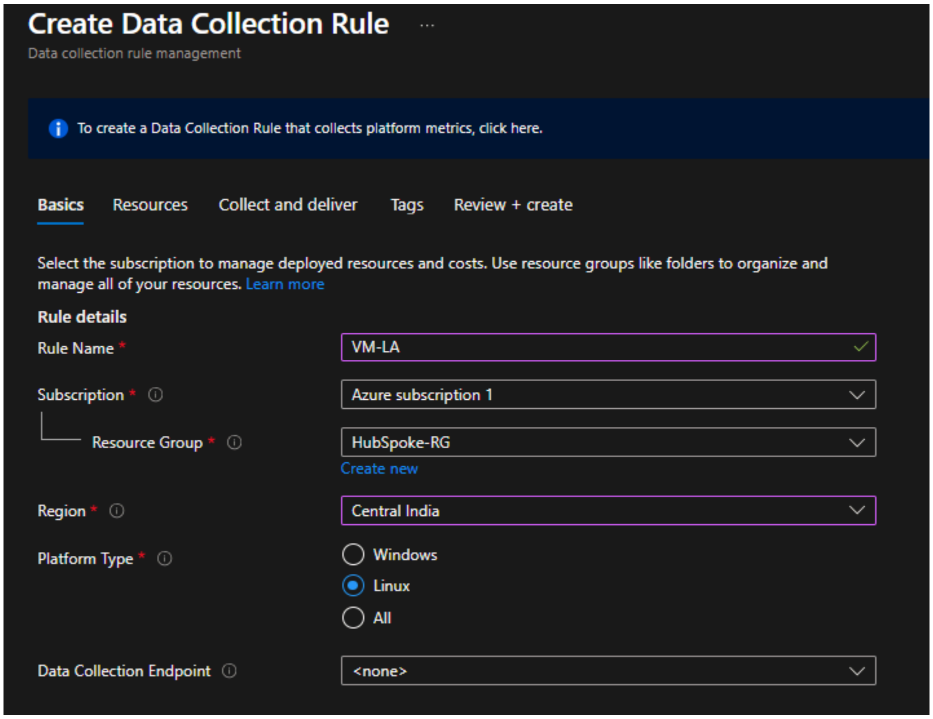
I have enabled VM Insights for both virtual machines (`Spoke1-VM` and `Spoke2-VM`) and connected them to the Log Analytics Workspace:

- **This allows monitoring of CPU, memory, disk, and network performance.**
- **Helps detect bottlenecks, track usage trends, and ensure optimal VM operation.**
- **Performance counters and logs are collected continuously for deeper analysis.**





Inside the LogAnalytics i have added both the VM to analyze.



Create Data Collection Rule

Data collection rule management

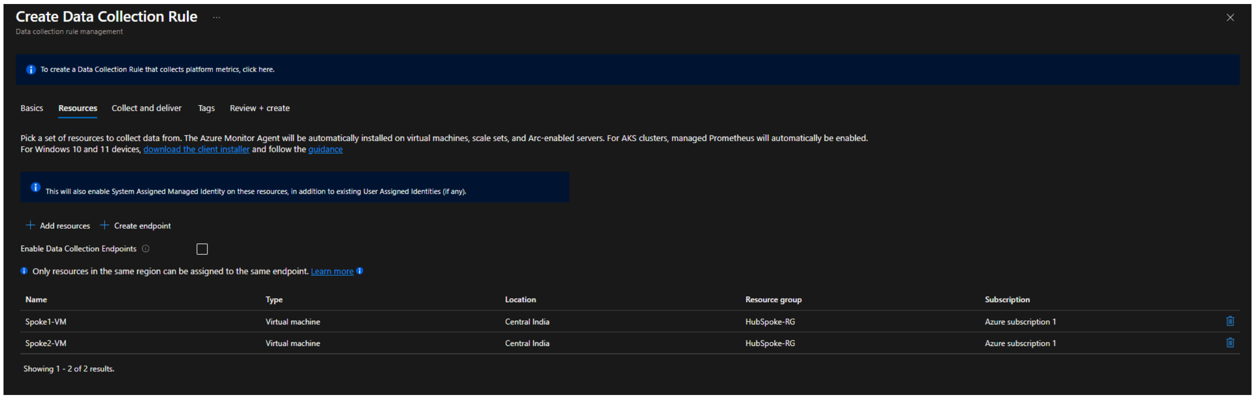
To create a Data Collection Rule that collects platform metrics, click here.

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources. Learn more

Rule details

Rule Name *	VM-LA
Subscription *	Azure subscription 1
Resource Group *	HubSpoke-RG Create new
Region *	Central India
Platform Type *	○ Windows ● Linux ○ All
Data Collection Endpoint	<none>

Associated VMs



Create Data Collection Rule

Data collection rule management

To create a Data Collection Rule that collects platform metrics, click here.

Pick a set of resources to collect data from. The Azure Monitor Agent will be automatically installed on virtual machines, scale sets, and Arc-enabled servers. For AKS clusters, managed Prometheus will automatically be enabled.
For Windows 10 and 11 devices, download the client installer and follow the guidance

This will also enable System Assigned Managed Identity on these resources, in addition to existing User Assigned Identities (if any).

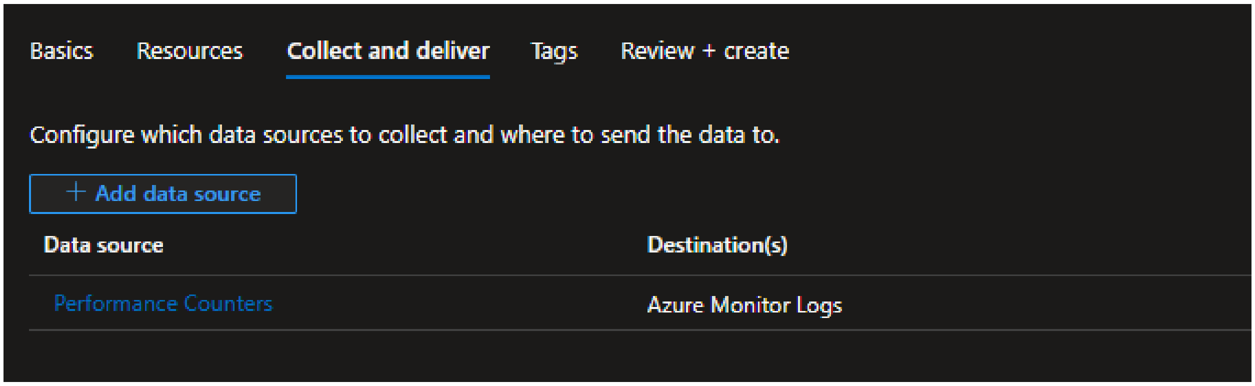
Enable Data Collection Endpoints □

Only resources in the same region can be assigned to the same endpoint. Learn more

Name	Type	Location	Resource group	Subscription
Spoke1-VM	Virtual machine	Central India	HubSpoke-RG	Azure subscription 1
Spoke2-VM	Virtual machine	Central India	HubSpoke-RG	Azure subscription 1

Showing 1 - 2 of 2 results.

Added collect and delivery for the performance counter

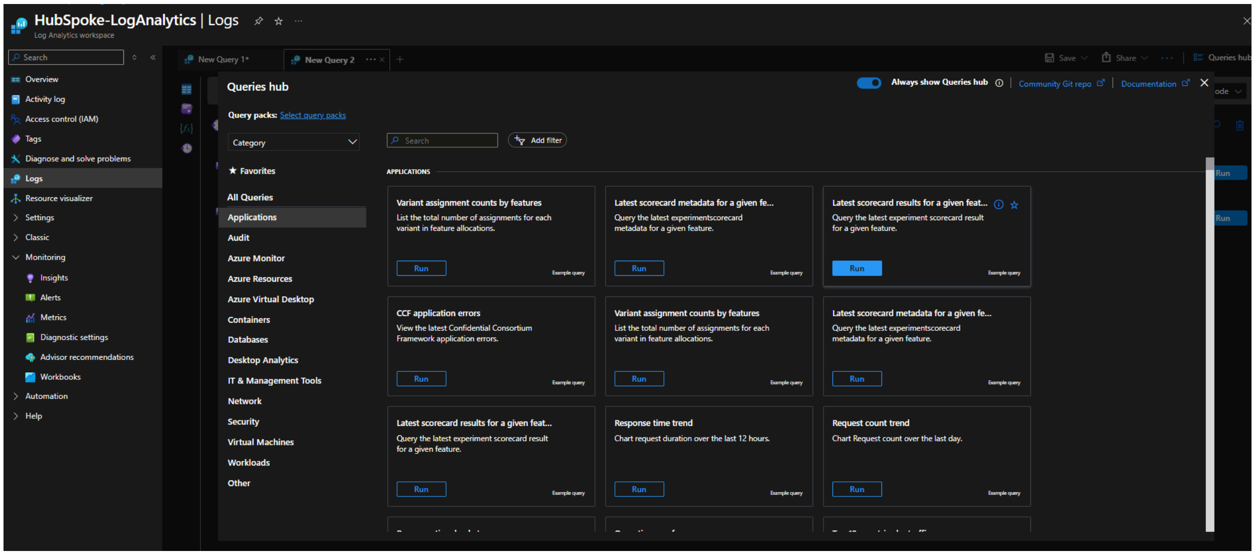


Configure which data sources to collect and where to send the data to.

Data source	Destination(s)
Performance Counters	Azure Monitor Logs

Within the Log Analytics workspace:

- Azure provides a set of predefined queries to quickly analyze different types of logs such as Firewall rule hits, NSG traffic flows, and VM performance.
- We can customize and apply filters to search for specific IPs, ports, or time frames — making the troubleshooting process faster and more efficient.



Queries hub

Query packs: Select query packs

APPLICATIONS

Variant assignment counts by features
List the total number of assignments for each variant in feature allocations.

Latest scorecard metadata for a given fe...
Query the latest experimentscorecard metadata for a given feature.

Latest scorecard results for a given feat...
Query the latest experiment scorecard result for a given feature.

CCF application errors
View the latest Confidential Consortium Framework application errors.

Variant assignment counts by features
List the total number of assignments for each variant in feature allocations.

Latest scorecard metadata for a given fe...
Query the latest experimentscorecard metadata for a given feature.

Latest scorecard results for a given feat...
Query the latest experiment scorecard result for a given feature.

Response time trend
Chart request duration over the last 12 hours.

Request count trend
Chart Request count over the last day.

Azure Monitor Dashboard

To visualize all logs and metrics in a single view, we can set up a custom Azure Monitor dashboard. This allows us to:

- Display charts for firewall hits, NSG traffic stats, VM CPU usage, etc.
- Monitor real-time activity and performance across the entire architecture.
- Quickly detect anomalies and security issues.

🌌*Azure CLI Implementation*🌌

Overview

In this project, I have designed and implemented a secure and scalable Hub-and-Spoke architecture in Microsoft Azure using CLI. The goal was to centralize control, ensure secure communication across workloads, and allow efficient resource sharing. The complete deployment was done step-by-step using Azure CLI to automate and standardize the setup process.

Throughout the project, I focused on aligning with best practices including workload isolation, zero trust principles, centralized security inspection, and performance monitoring. This document outlines everything I did during the project, from infrastructure provisioning to testing and verification.

Architecture Summary

- **Hub VNet (11.0.0.0/16)** with subnets:
  - AzureFirewallSubnet (11.0.1.0/26)
  - AzureBastionSubnet (11.0.2.0/26)
- **Spoke1 VNet (12.0.0.0/24)** and **Spoke2 VNet (13.0.0.0/24)**
- Peering between hub and each spoke
- Centralized Azure Firewall with custom rules (Firewall Private IP: **11.0.1.4**)
- Bastion access from browser without public IPs on VMs
- User Defined Routes in Spokes to redirect all traffic via firewall
- NSGs applied to spoke subnets for added control
- Ubuntu-based VMs deployed in each spoke (**12.0.1.4**, **13.0.1.4**)
- Centralized monitoring using Log Analytics

Step-by-Step CLI Implementation

1. Resource Group

```
az group create --name HubSpoke-RG --location centralindia
```

2. Hub Virtual Network with Subnets

```
az network vnet create \
  --resource-group HubSpoke-RG \
  --name Hub-VNet \
  --address-prefix 11.0.0.0/16 \
  --subnet-name AzureFirewallSubnet \
  --subnet-prefix 11.0.1.0/26

az network vnet subnet create \
  --resource-group HubSpoke-RG \
  --vnet-name Hub-VNet \
  --name AzureBastionSubnet \
  --address-prefix 11.0.2.0/26
```

3. Spoke VNets

```
az network vnet create \
  --resource-group HubSpoke-RG \
  --name Spoke1-VNet \
  --address-prefix 12.0.0.0/24 \
  --subnet-name Workload \
  --subnet-prefix 12.0.0.0/24

az network vnet create \
  --resource-group HubSpoke-RG \
  --name Spoke2-VNet \
  --address-prefix 13.0.0.0/24 \
  --subnet-name Workload \
  --subnet-prefix 13.0.0.0/24
```

4. VNet Peering

```
az network vnet peering create --name Spoke1ToHub --resource-group HubSpoke-RG
--vnet-name Spoke1-VNet --remote-vnet Hub-VNet --allow-vnet-access
az network vnet peering create --name HubToSpoke1 --resource-group HubSpoke-RG
--vnet-name Hub-VNet --remote-vnet Spoke1-VNet --allow-vnet-access

az network vnet peering create --name Spoke2ToHub --resource-group HubSpoke-RG
--vnet-name Spoke2-VNet --remote-vnet Hub-VNet --allow-vnet-access
az network vnet peering create --name HubToSpoke2 --resource-group HubSpoke-RG
--vnet-name Hub-VNet --remote-vnet Spoke2-VNet --allow-vnet-access
```

5. Azure Firewall Deployment

```
az network public-ip create --name FirewallPublicIP --resource-group HubSpoke-RG --sku
Standard --location centralindia --allocation-method Static

az network firewall create --name HubFirewall --resource-group HubSpoke-RG --location
centralindia

az network firewall ip-config create \
  --firewall-name HubFirewall \
  --name FWConfig \
  --public-ip-address FirewallPublicIP \
  --resource-group HubSpoke-RG \
  --vnet-name Hub-VNet
```

6. Firewall Private IP

11.0.1.4

7. User Defined Routes (UDRs)

Spoke1

```
az network route-table create --name Spoke1-RouteTable --resource-group HubSpoke-RG
--location centralindia
az network route-table route create --resource-group HubSpoke-RG --route-table-name
Spoke1-RouteTable --name RouteToFirewall --address-prefix 0.0.0.0/0 --next-hop-type
VirtualAppliance --next-hop-ip-address 11.0.1.4
az network vnet subnet update --resource-group HubSpoke-RG --vnet-name Spoke1-VNet
--name Workload --route-table Spoke1-RouteTable
```

Spoke2

```
az network route-table create --name Spoke2-RouteTable --resource-group HubSpoke-RG --location centralindia
az network route-table route create --resource-group HubSpoke-RG --route-table-name Spoke2-RouteTable --name RouteToFirewall --address-prefix 0.0.0.0/0 --next-hop-type VirtualAppliance --next-hop-ip-address 11.0.1.4
az network vnet subnet update --resource-group HubSpoke-RG --vnet-name Spoke2-VNet --name Workload --route-table Spoke2-RouteTable
```

8. NSGs

```
az network nsg create --resource-group HubSpoke-RG --name Spoke1-NSG --location centralindia
az network nsg create --resource-group HubSpoke-RG --name Spoke2-NSG --location centralindia

az network vnet subnet update --resource-group HubSpoke-RG --vnet-name Spoke1-VNet --name Workload --network-security-group Spoke1-NSG
az network vnet subnet update --resource-group HubSpoke-RG --vnet-name Spoke2-VNet --name Workload --network-security-group Spoke2-NSG
```

9. Bastion

```
az network public-ip create --name BastionPublicIP --resource-group HubSpoke-RG --sku Standard --location centralindia --allocation-method Static

az network bastion create \
  --name HubBastion \
  --public-ip-address BastionPublicIP \
  --resource-group HubSpoke-RG \
  --vnet-name Hub-VNet \
  --location centralindia
```

10. Virtual Machines

```
az vm create \
  --name Spoke1-VM \
  --resource-group HubSpoke-RG \
  --vnet-name Spoke1-VNet \
  --subnet Workload \
  --image UbuntuLTS \
  --admin-username azureuser \
  --authentication-type password \
  --admin-password 'Kirtan@12345' \
  --nsg Spoke1-NSG \
  --private-ip-address 12.0.1.4
```

```
az vm create \
  --name Spoke2-VM \
  --resource-group HubSpoke-RG \
  --vnet-name Spoke2-VNet \
  --subnet Workload \
  --image UbuntuLTS \
  --admin-username azureuser \
  --authentication-type password \
  --admin-password 'Kirtan@12345' \
  --nsg Spoke2-NSG \
  --private-ip-address 13.0.1.4
```

11. Firewall Rules

Created via portal:

- Allow SSH from 11.0.2.0/26 to 12.0.0.0/24 and 13.0.0.0/24 (TCP 22)
- Allow ICMP
- Application Rules for:
  - *.microsoft.com
  - *.ubuntu.com
  - *.github.com
  - google.com

12. Log Analytics Workspace

```
az monitor log-analytics workspace create --resource-group HubSpoke-RG --workspace-name HubSpoke-LogAnalytics --location centralindia
```

13. Enable Monitoring

Enabled from portal:

- VM Insights
- NSG Flow Logs
- Traffic Analytics