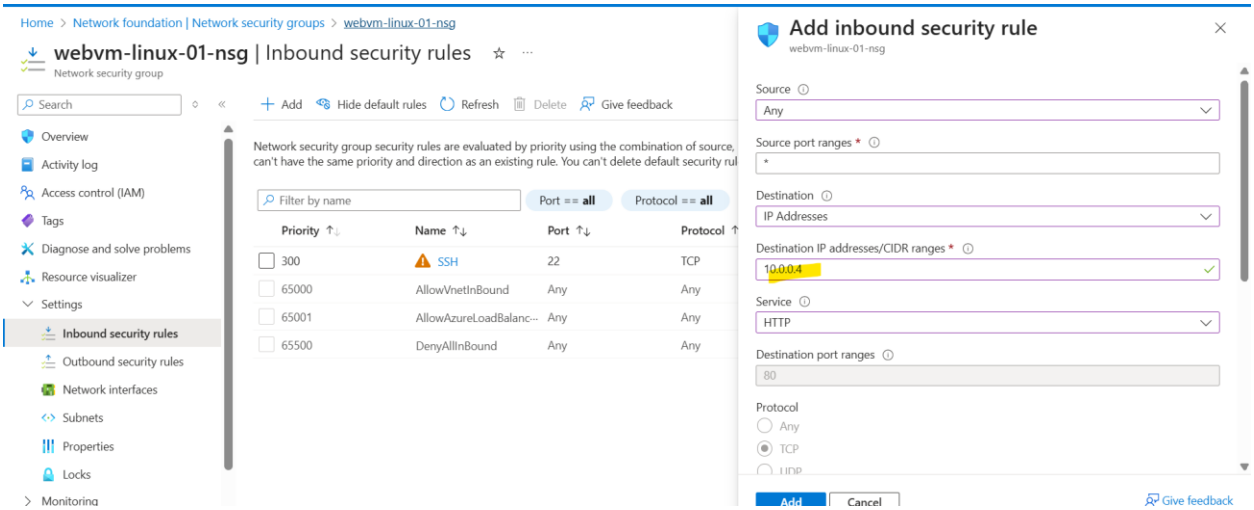
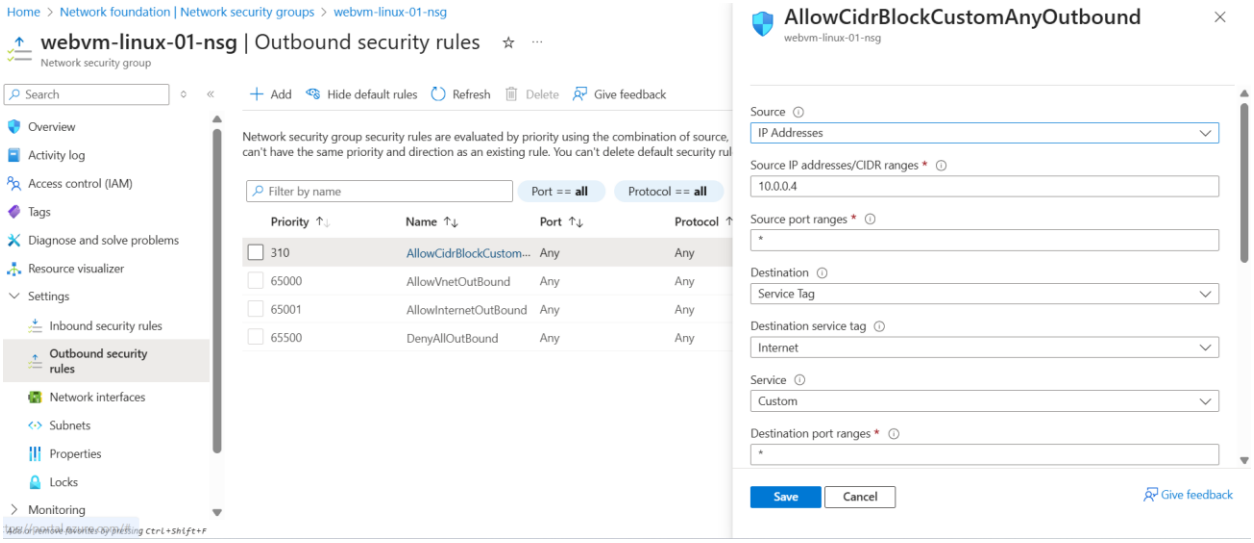
Network Security Groups - IP Address

Added rule for private ip for vm

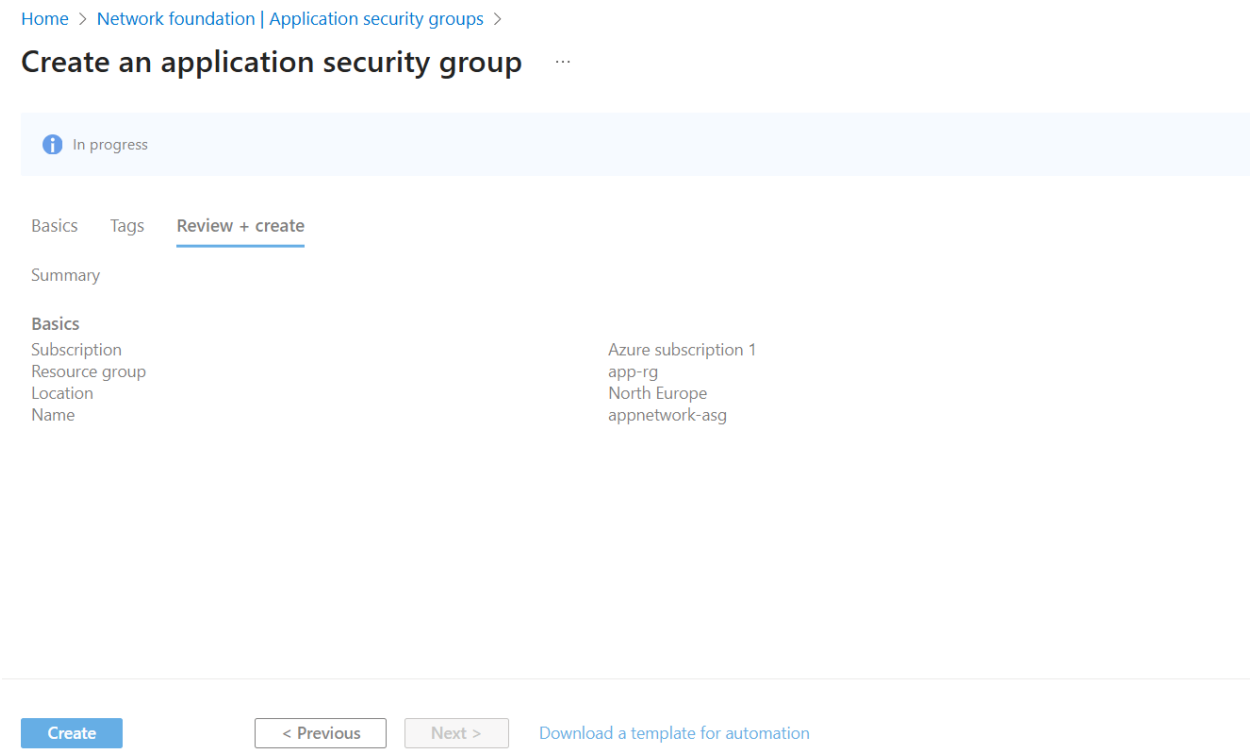


Network Security Groups - Outbound Rules

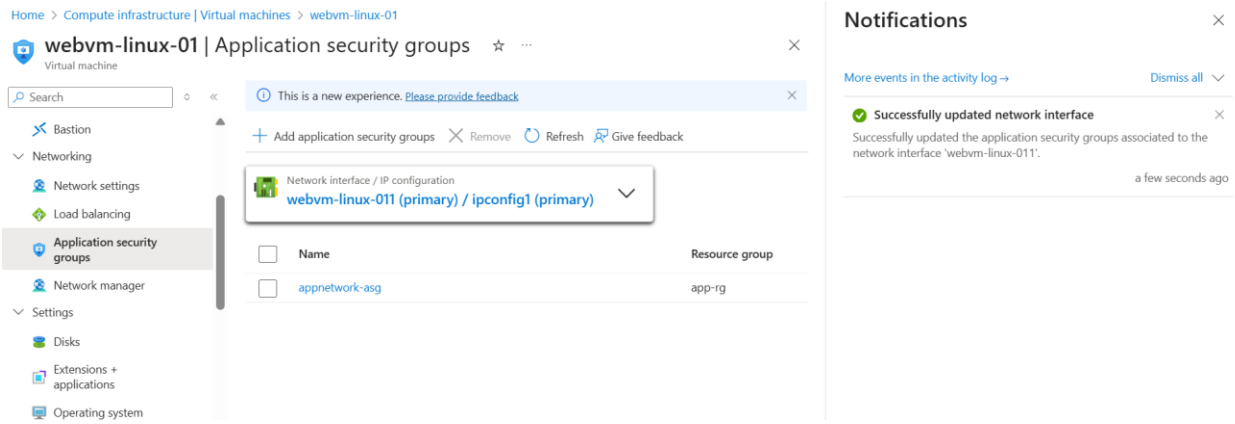
Outbound rule to deny all outbound traffic to internet

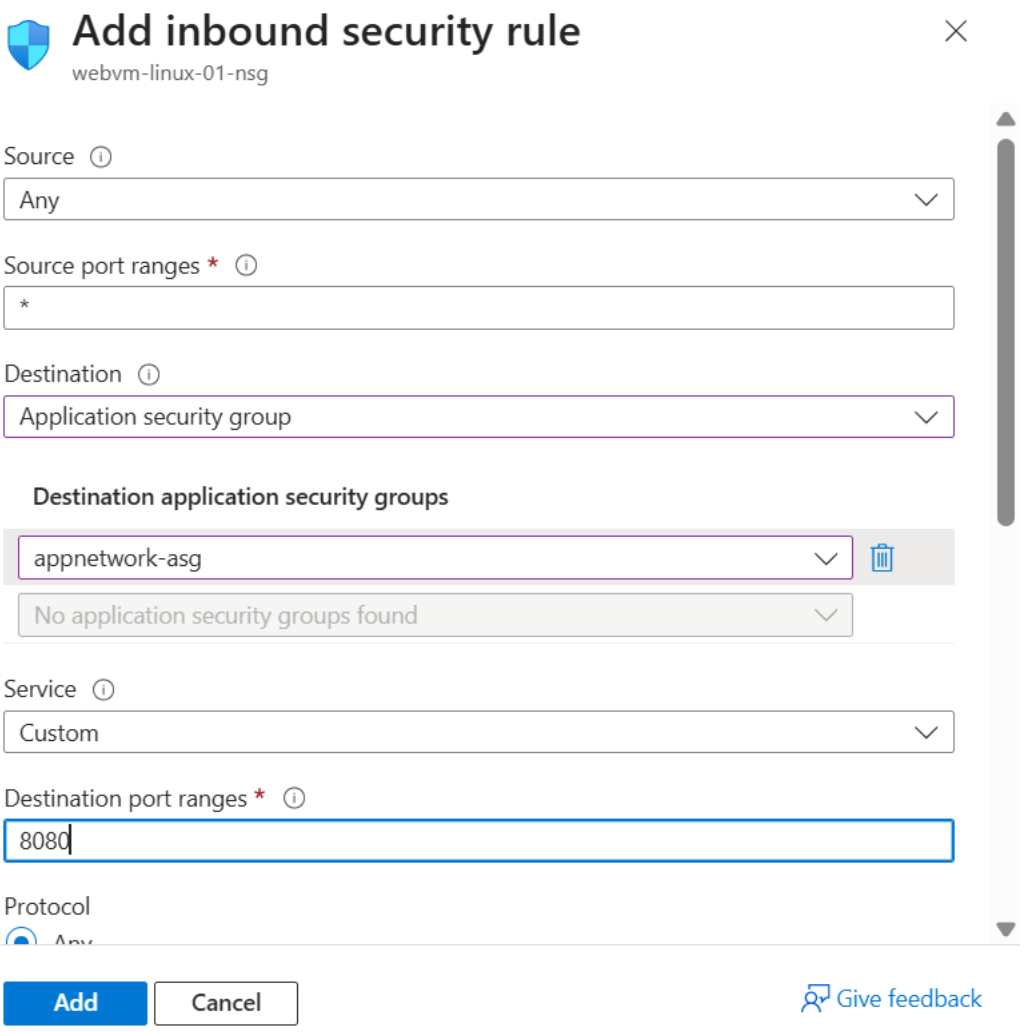


Application security group



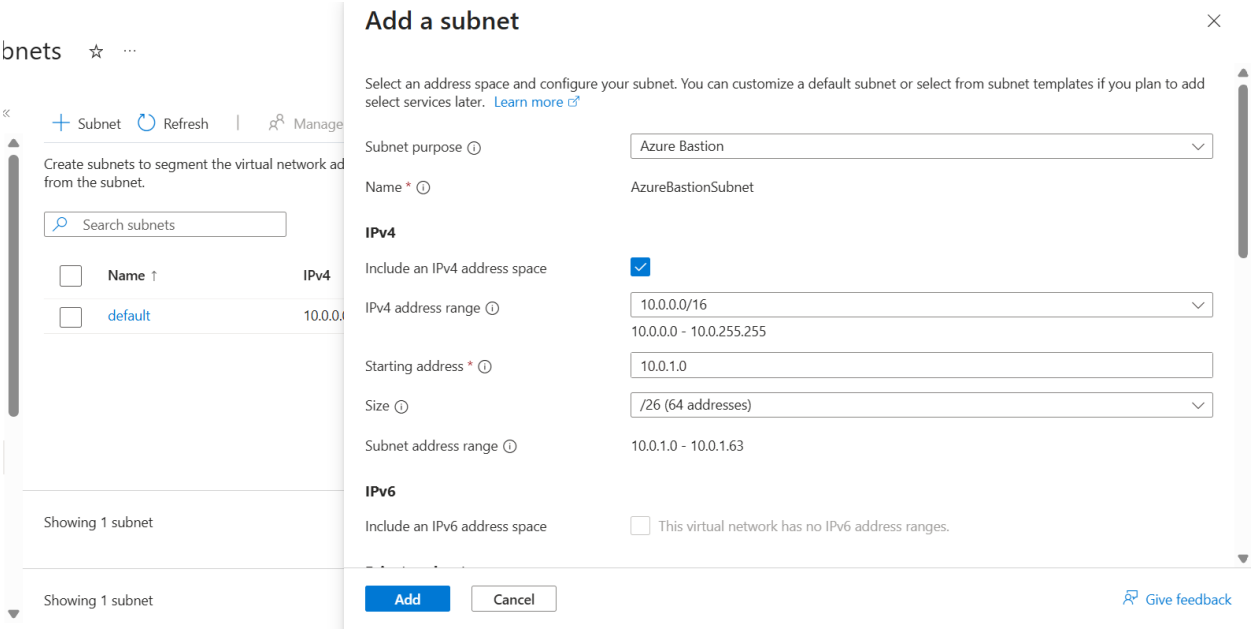
Updating security group

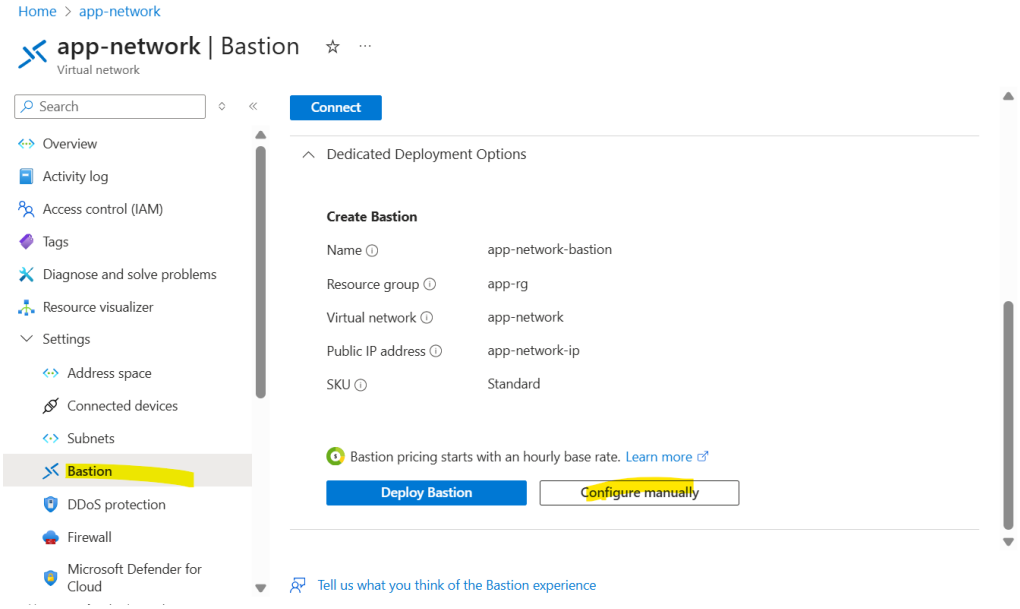



Add inbound security rule
webvm-linux-01-nsg
Source
Any
Source port ranges *
*
Destination
Application security group
Destination application security groups
appnetwork-asg
No application security groups found
Service
Custom
Destination port ranges *
8080
Protocol
Add
Cancel
Give feedback

Azure Bastion

Secure communication to vm without need of machines needing to have public ip address





Configure manually

Create a Bastion ...

Validation passed

Basics Advanced Tags **Review + create**

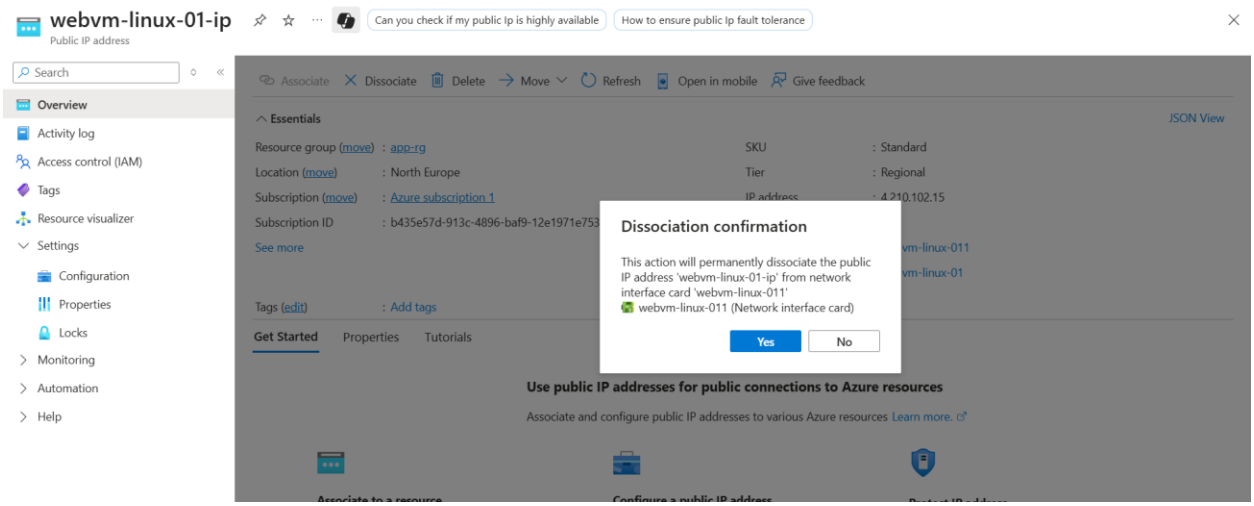
Summary

Basics

Name	app-bastion
Subscription	Azure subscription 1
Resource group	app-rg
Region	North Europe
Availability zone	None
Virtual network	app-network
Tier	Basic
Subnets	AzureBastionSubnet
Public IP address	app-network-ip
Instance count	2
Copy and paste	Enabled
IP-based connection	Disabled
Kerberos authentication	Disabled
Shareable Link	Disabled
Session recording	Disabled
Native client support	Disabled

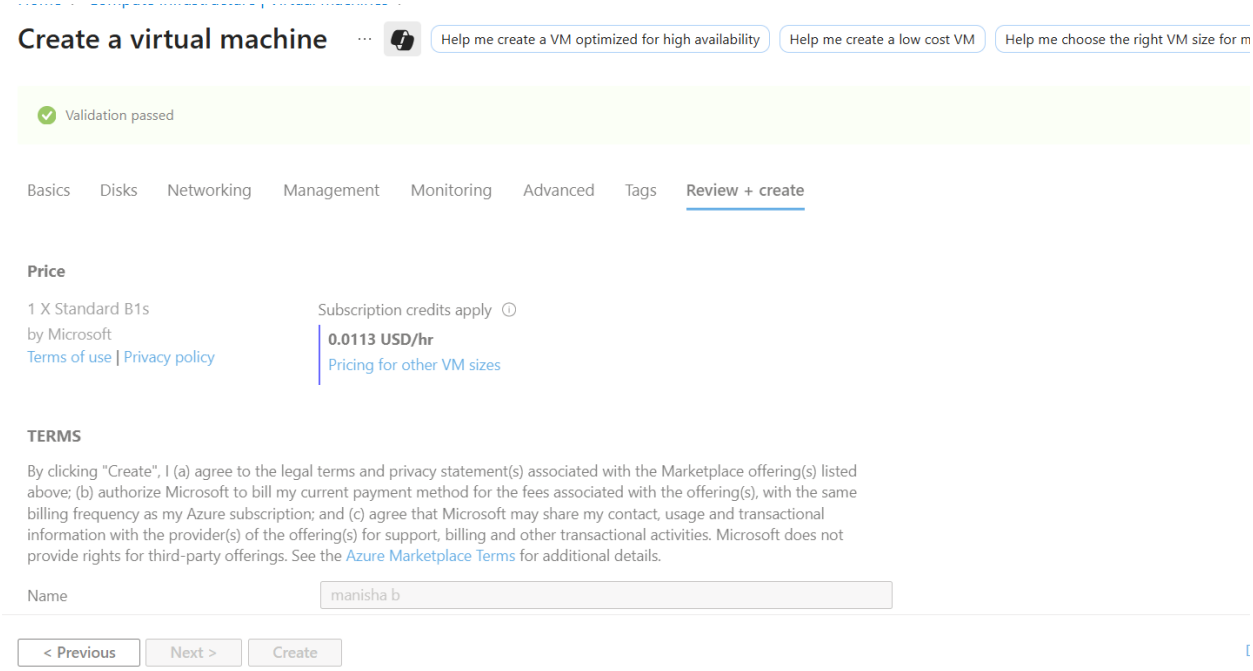
Create Previous Next Download a template for automation

Diassociated public ip of vm

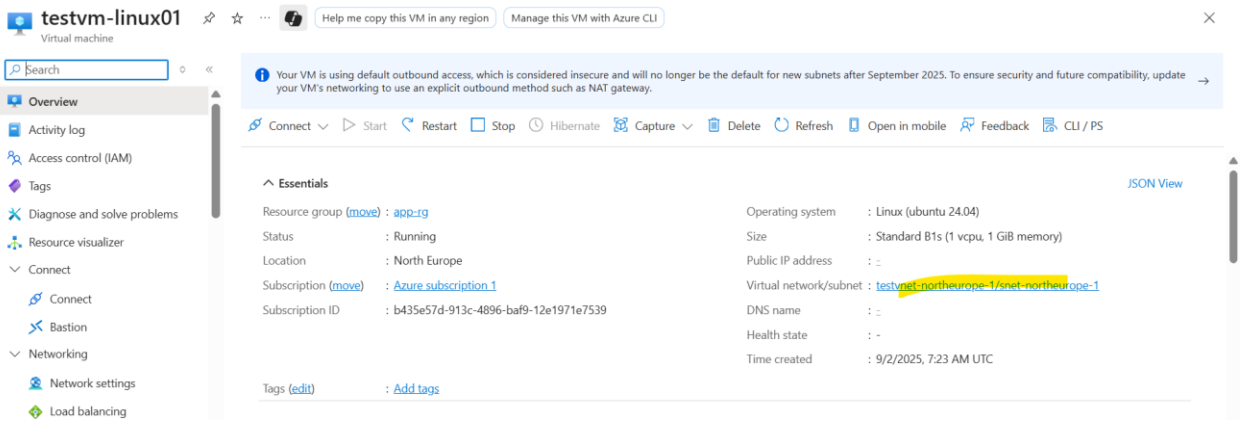


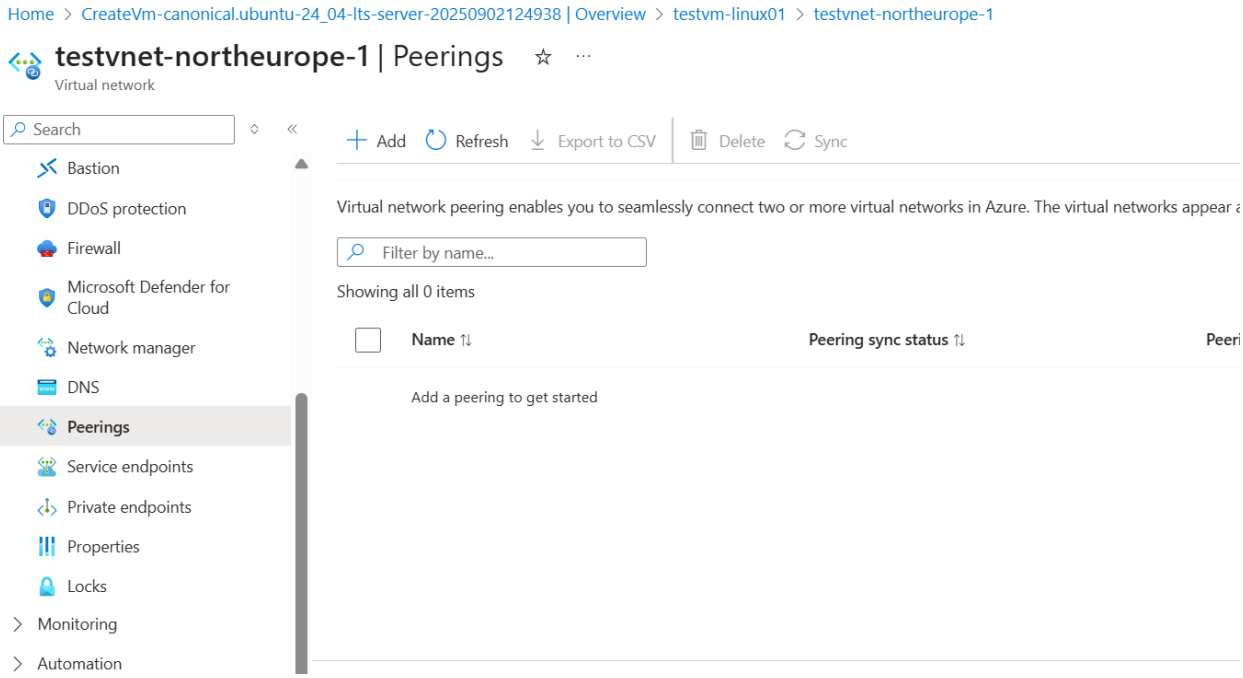
Peering

Create vm

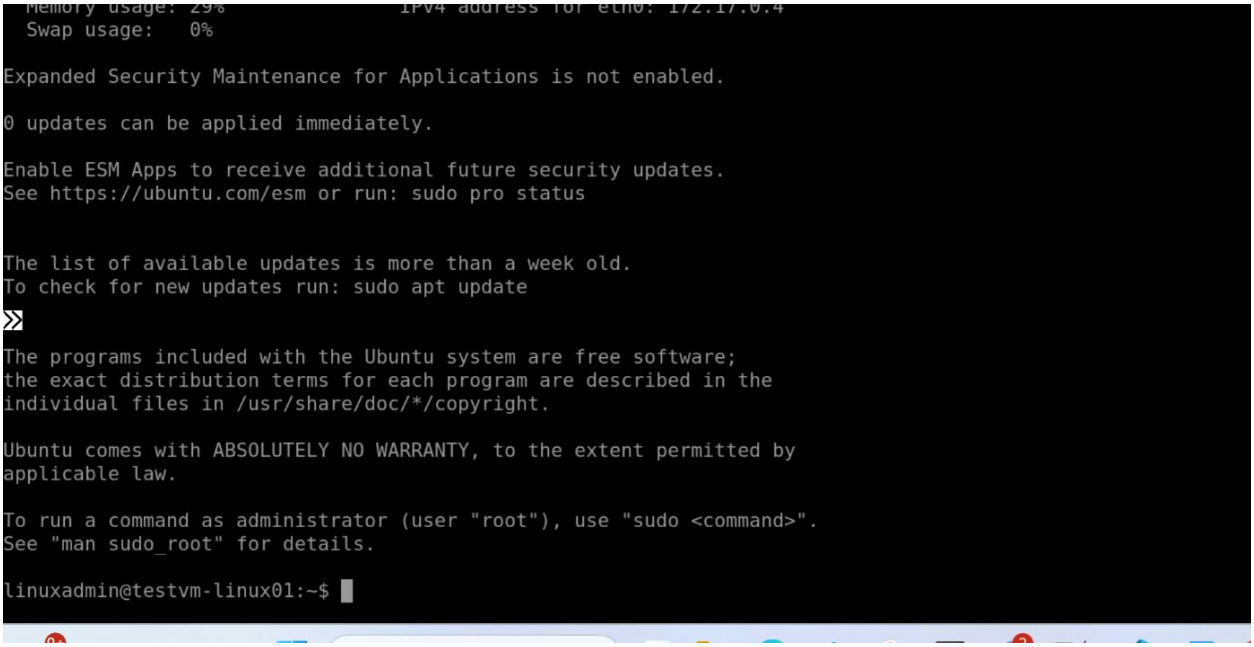


Got vnet -> go to peering and add perring connections

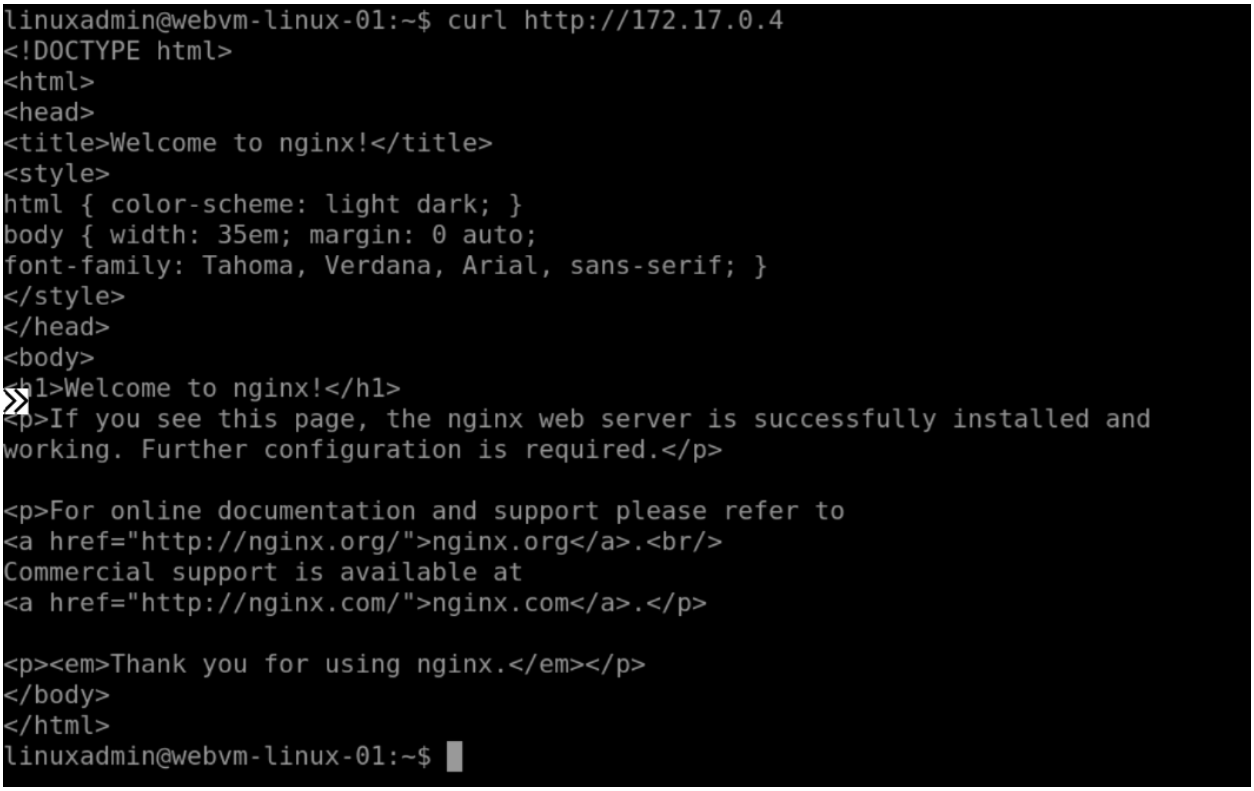

testvm-linux01
Virtual machine
Help me copy this VM in any region
Manage this VM with Azure CLI
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Connect
Bastion
Networking
Network settings
Load balancing
Your VM is using default outbound access, which is considered insecure and will no longer be the default for new subnets after September 2025. To ensure security and future compatibility, update your VM's networking to use an explicit outbound method such as NAT gateway.
Connect
Start
Restart
Stop
Hibernate
Capture
Delete
Refresh
Open in mobile
Feedback
CLI / PS
Essentials
JSON View
Resource group (move) : app-rg
Status : Running
Location : North Europe
Subscription (move) : Azure subscription 1
Subscription ID : b435e57d-913c-4896-baf9-12e1971e7539
Operating system : Linux (ubuntu 24.04)
Size : Standard B1s (1 vcpu, 1 GiB memory)
Public IP address : -
Virtual network/subnet : testvnet-northeurope-1/snet-northeurope-1
DNS name : -
Health state : -
Time created : 9/2/2025, 7:23 AM UTC
Tags (edit) : Add tags


Home > CreateVm-canonical.ubuntu-24_04-lts-server-20250902124938 | Overview > testvm-linux01 > testvnet-northeurope-1
testvnet-northeurope-1 | Peerings
Virtual network
Search
Bastion
DDoS protection
Firewall
Microsoft Defender for Cloud
Network manager
DNS
Peerings
Service endpoints
Private endpoints
Properties
Locks
Monitoring
Automation
Add
Refresh
Export to CSV
Delete
Sync
Virtual network peering enables you to seamlessly connect two or more virtual networks in Azure. The virtual networks appear a
Filter by name...
Showing all 0 items
Name
Peering sync status
Peeri
Add a peering to get started

Login to via Bastion



Login to another vm check connection with vm using private ip



Routes

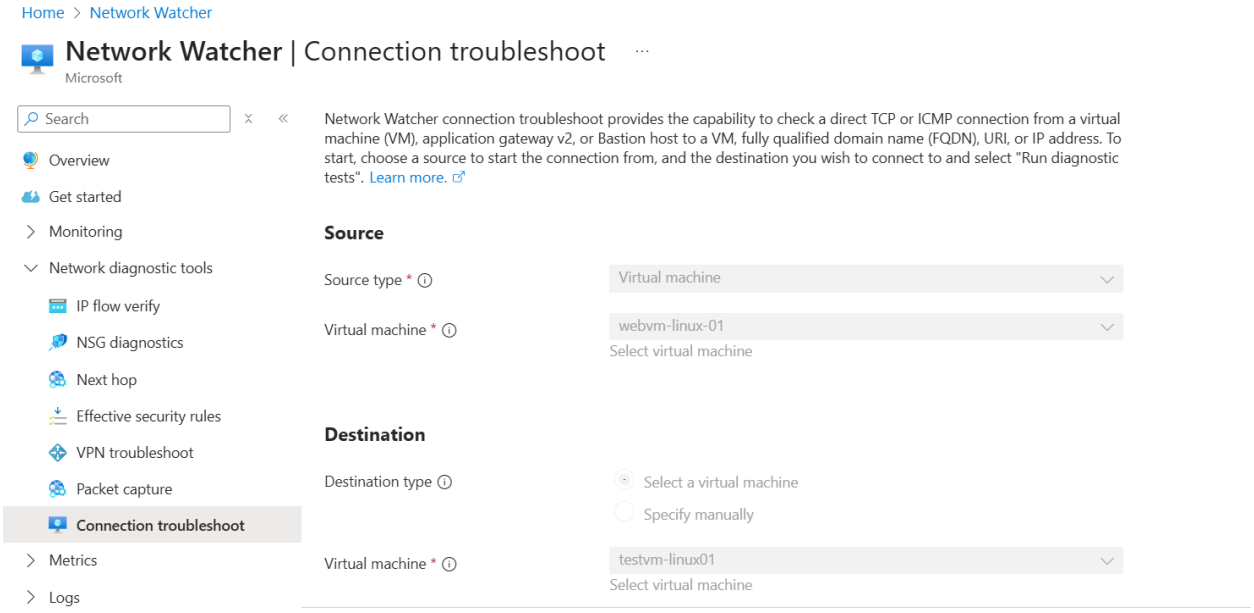
By default there are system routes in place which ensures the traffic is routed correctly across subnets is a virtual network

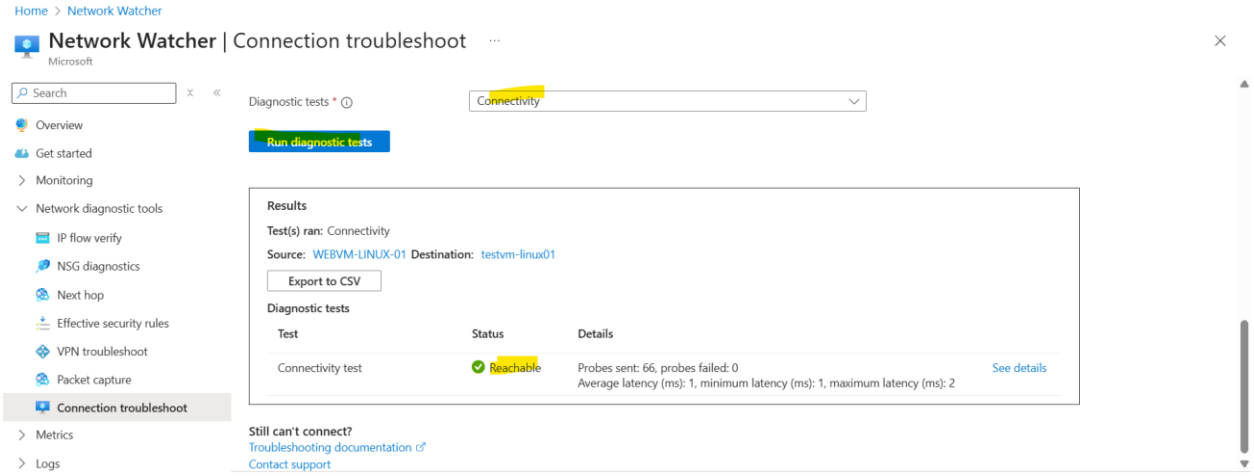
Eg. Lets say company has a virtual machine that is hosting a virtual appliance – Firewall

And all traffic in the virtual network needs to be route through the virtual appliance

We can define a user-defined route that makes sure all traffic is routed through the firewall appliance device

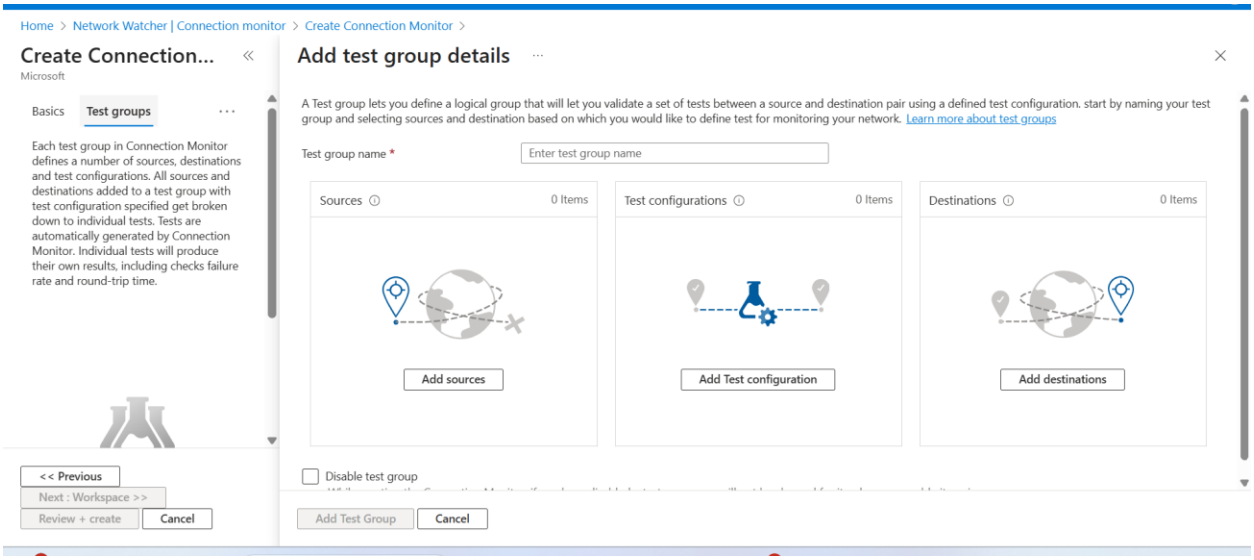
Network watcher





Network monitor

End to end connection monitoring



Add Sources

Azure endpoints | ARC endpoints | Recent endpoint

Select from a list of Azure VMs with Network Watcher extension installed. Group by, search and filter on Subscriptions, Resource Groups, VNETs and Subnets.

Type * Virtual Machines

Subscription | Resource group | VNET | Subnet

Subscription * Azure subscription 1

Region North Europe

Filter by name

Name	IP	Subscription	Resource gro...	Subnet	Network Wat...
vnet-north		Azure subscription...	app-rg		Not Enabled
testvnet-n.		Azure subscription...	app-rg		Not Enabled
app-netw..		Azure subscription...	app-rg		Enabled
defaul	10.0.0.0/24	Azure subscription...	app-rg		Enabled
w.	Any	Azure subscription...	app-rg	default	Enabled

Selected sources (1 Azure endpoints)

Add endpoints | Cancel

Destinations 1 Items

Azure endpoints	Extension Statu
testvm-linux01(app-rg) *Subscription : Azure subscription 1* *Resource group: app-rg* Edit	Enable

Add Test configuration

New configuration | Choose existing

Test configuration name *

testwebmonitor

Protocol

HTTP

Create TCP test configuration

Destination port *

80

Test Frequency

Every minute

HTTP Configuration

Method

GET

Path

Eg: /

Request headers

Add Test configuration | Cancel

Create Connection Monitor

Microsoft

Basics | Test groups | Workspace | Create alert | Review + create

You can use this section to setup granular control over where you wish to store all the monitoring data generated as part of monitoring tests. Learn more

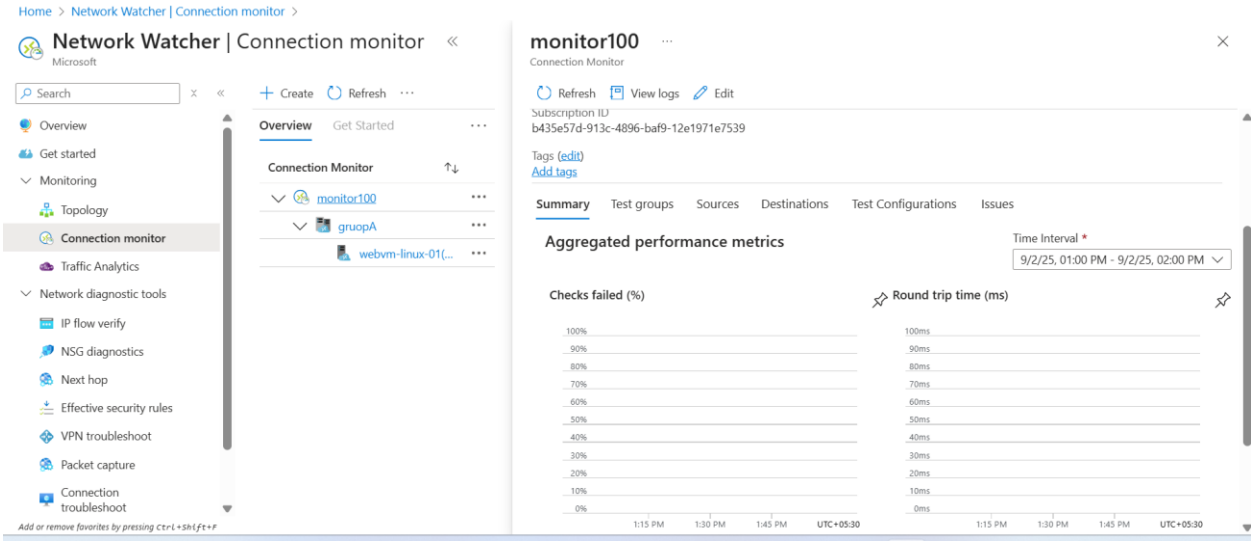
Workspace *

- (•) Default (Recommended)
- ( ) Custom Workspace

Workspace configuration

Workspace

DefaultWorkspace-b435e57d-913c-4896-baf9-12e1971e753...
Azure subscription 1 in northeurope (system generated)


Home > Network Watcher | Connection monitor >
Network Watcher | Connection monitor
Microsoft
Search
Overview
Get started
Monitoring
Topology
Connection monitor
Traffic Analytics
Network diagnostic tools
IP flow verify
NSG diagnostics
Next hop
Effective security rules
VPN troubleshoot
Packet capture
Connection troubleshoot
Add or remove favorites by pressing Ctrl+Shift+F
Create
Refresh
Overview
Get Started
Connection Monitor
monitor100
gruopA
webvm-linux-01(...
monitor100
Connection Monitor
Refresh
View logs
Edit
Subscription ID
b435e57d-913c-4896-baf9-12e1971e7539
Tags (edit)
Add tags
Summary
Test groups
Sources
Destinations
Test Configurations
Issues
Aggregated performance metrics
Time Interval *
9/2/25, 01:00 PM - 9/2/25, 02:00 PM
Checks failed (%)
Round trip time (ms)
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
100ms
90ms
80ms
70ms
60ms
50ms
40ms
30ms
20ms
10ms
0ms
1:15 PM
1:30 PM
1:45 PM
UTC+05:30

Azure load balancer

A load balancer is used to distribute the incoming network traffic across a set of backend servers

Frondend ip configuration – this is entry point for clients onto the load balancer this can contain apublic ip address that is associated with the load balancer

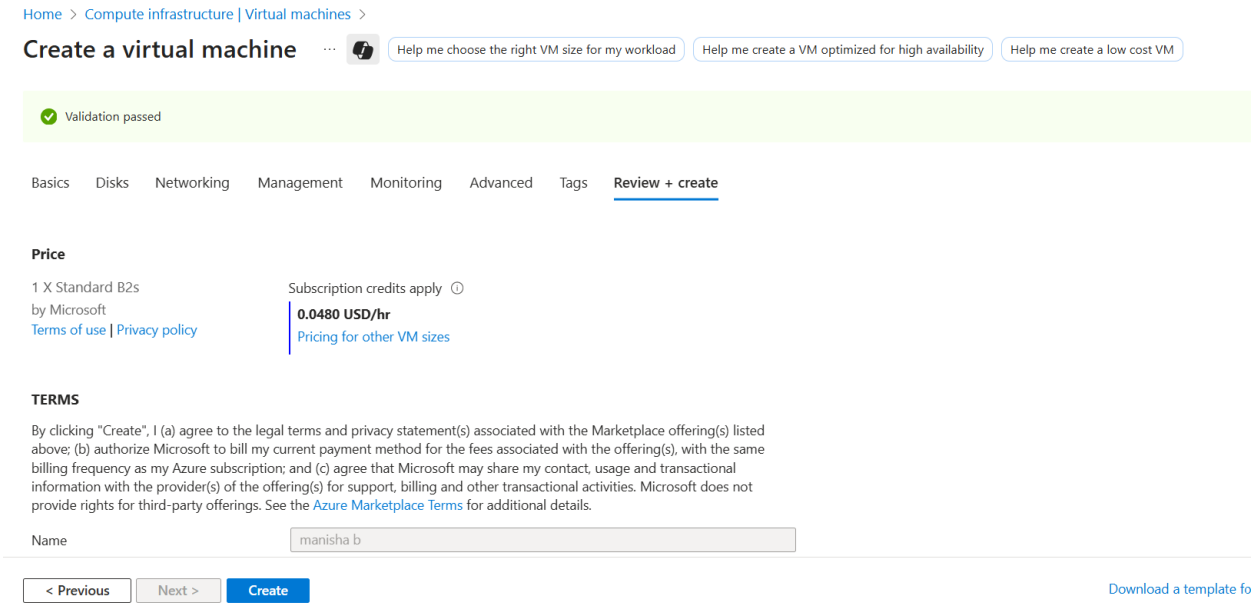
Bakendpool – backend vm that will be use to serve the client requests

Health probe – used to determine if the backend machines are healthy or not

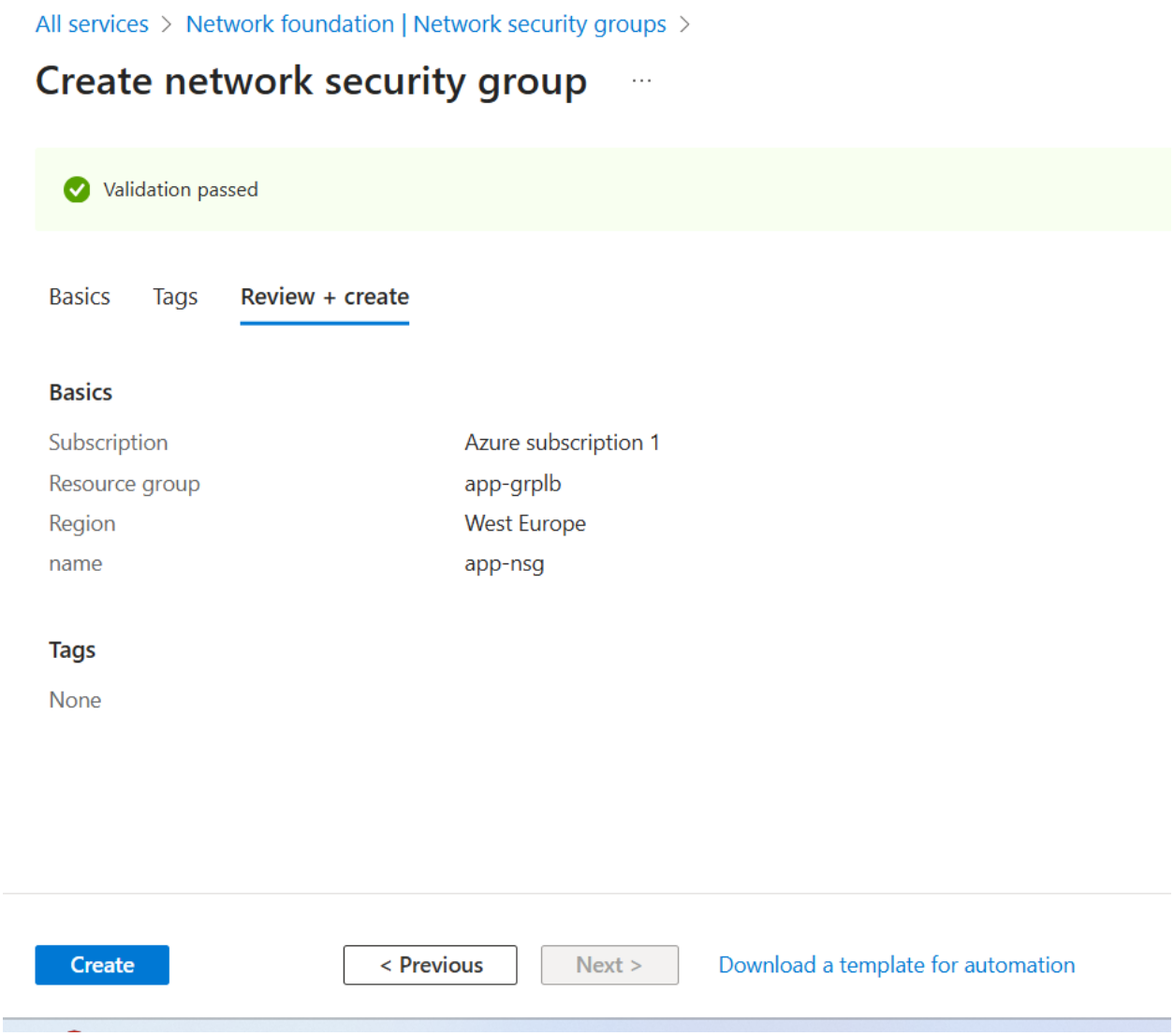
Load balancer rules – used to determine how the requests from the clients are routed to the backend instance

Basic Load Balancer

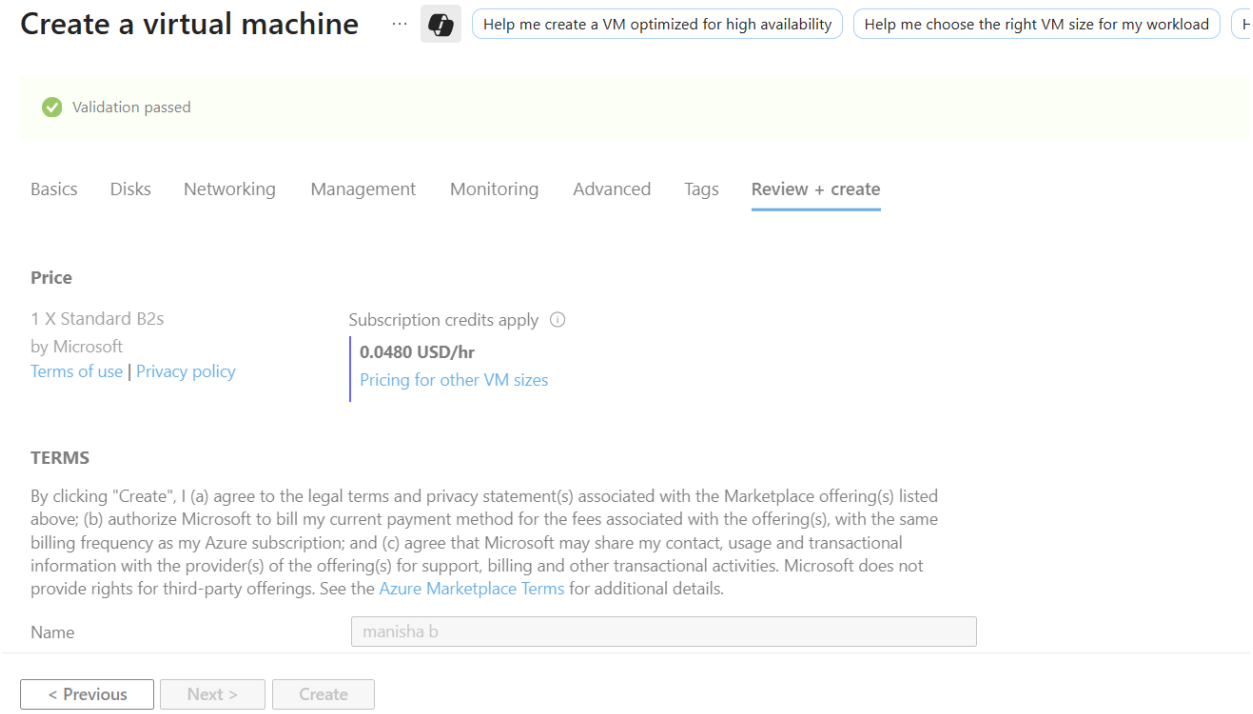
Create linux vm



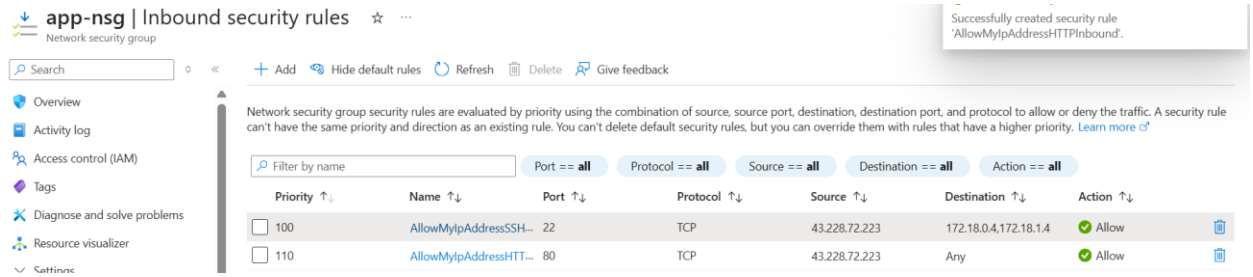
Create network security group

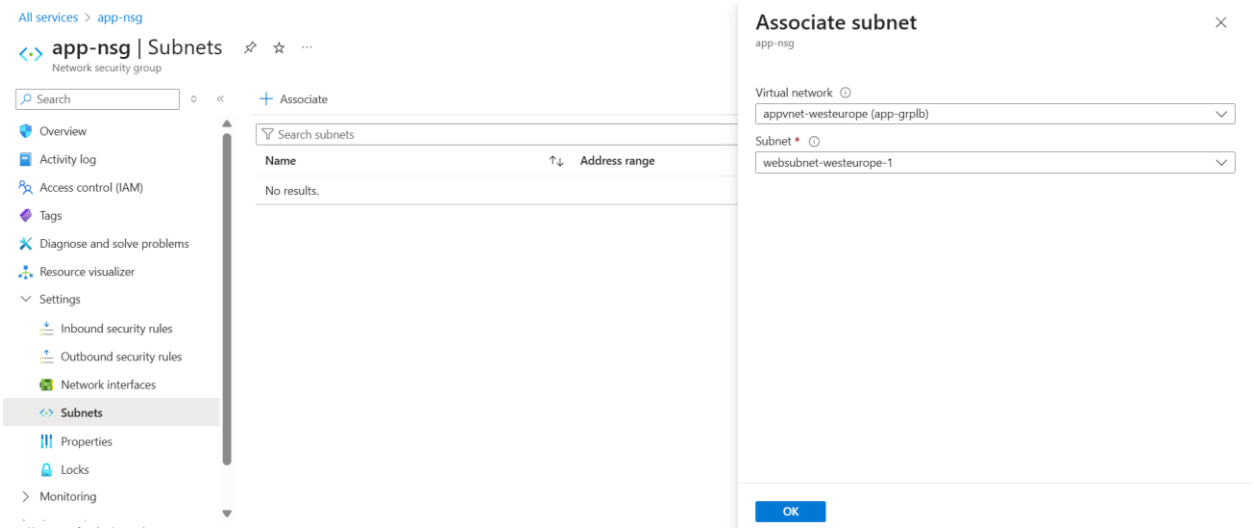


Create another vm



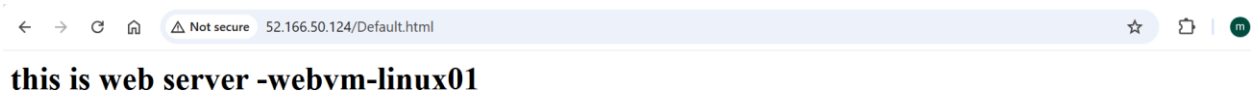
Goto nsg and inbound rule to allow traffic





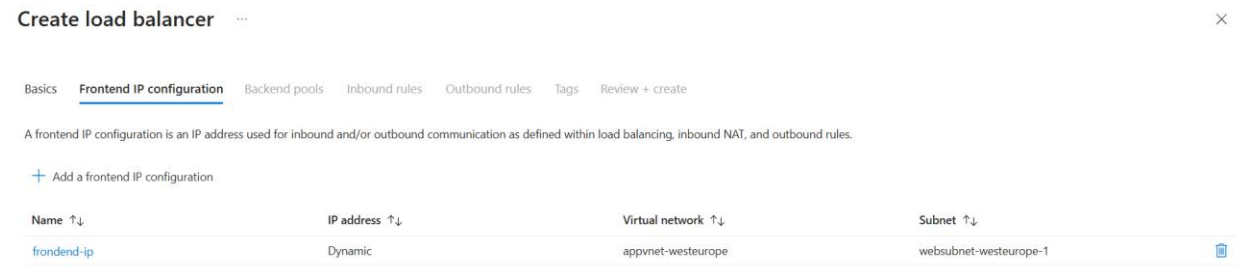
Connect to fist machine

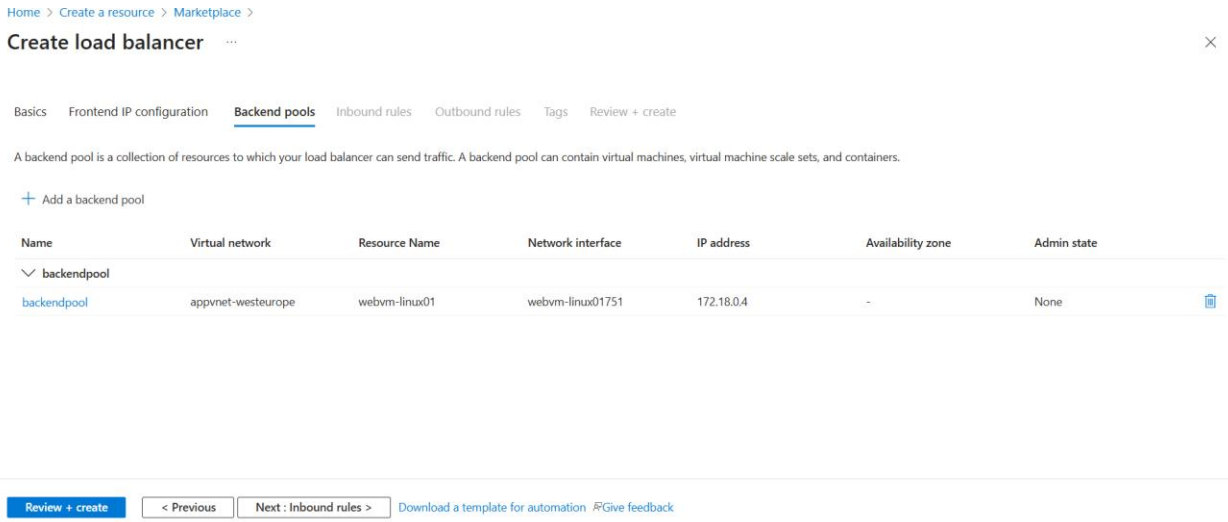
Install nginx and access to public ip



this is web server -webvm-linux01

Lab - Basic Load Balancer – Deployment





Create load balancer

Validation passed

Basics | Frontend IP configuration | Backend pools | Inbound rules | Outbound rules | Tags | **Review + create**

Basics

Subscription	Azure subscription 1
Resource group	app-grplb
Name	app-balancer
Region	West Europe
SKU	Standard
Tier	Regional
Type	Internal

Frontend IP configuration

Frontend IP configuration name	frondend-ip
Frontend IP configuration IP address	Dynamic

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

Home > CreateLoadBalancerBladeV2-20230902130610 | Overview > app-balancer | Health probes >

Add health probe

app-balancer

Health probes are used to check the status of a backend pool instance. If the health probe fails to get a response from a backend instance then no new connections will be sent to that backend instance until the health probe succeeds again.

Name *	helathprobA
Protocol *	TCP
Port *	80
Interval (seconds) *	5
Used by *	Not used

Save Cancel

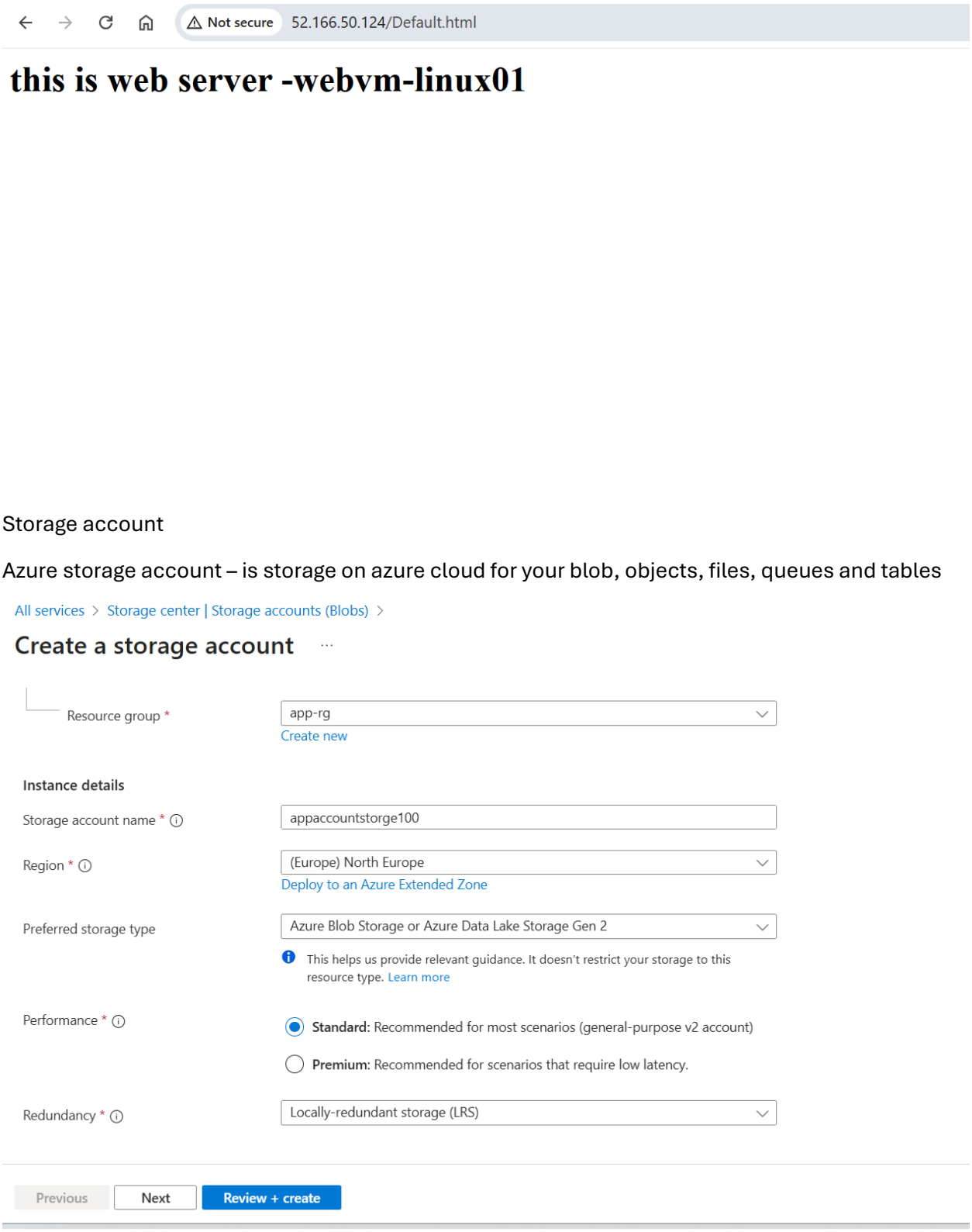
Add load balancing rule

app-balancer

A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic. Learn more.

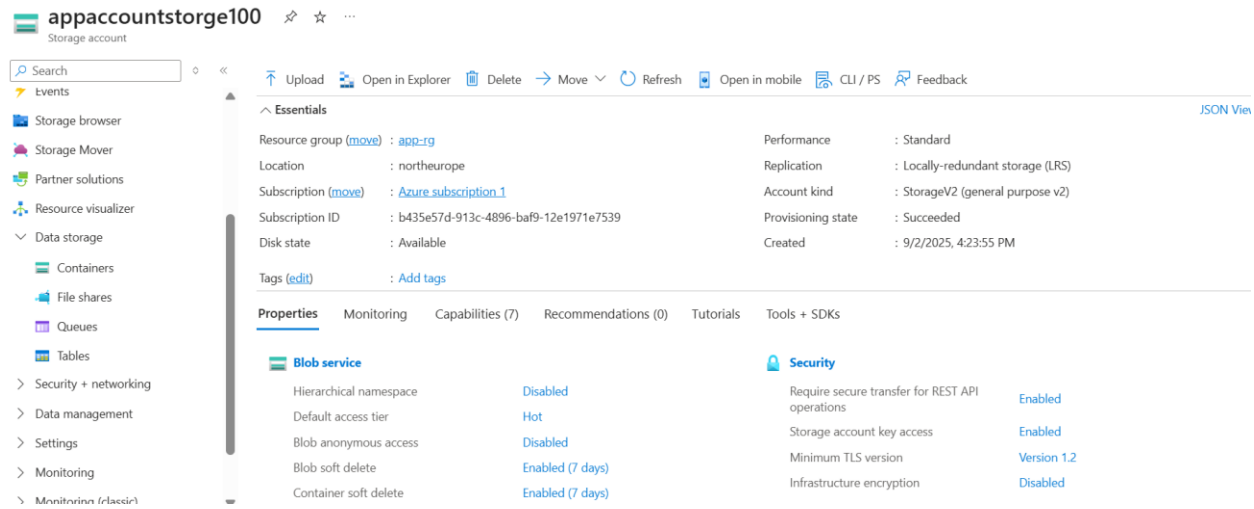
Name *	balncer-rule
IP version *	IPv4 / IPv6
Frontend IP address *	frondend-ip (172.18.0.5)
Backend pool *	backendpool
High availability ports	☐
Protocol	TCP / UDP

Save Cancel

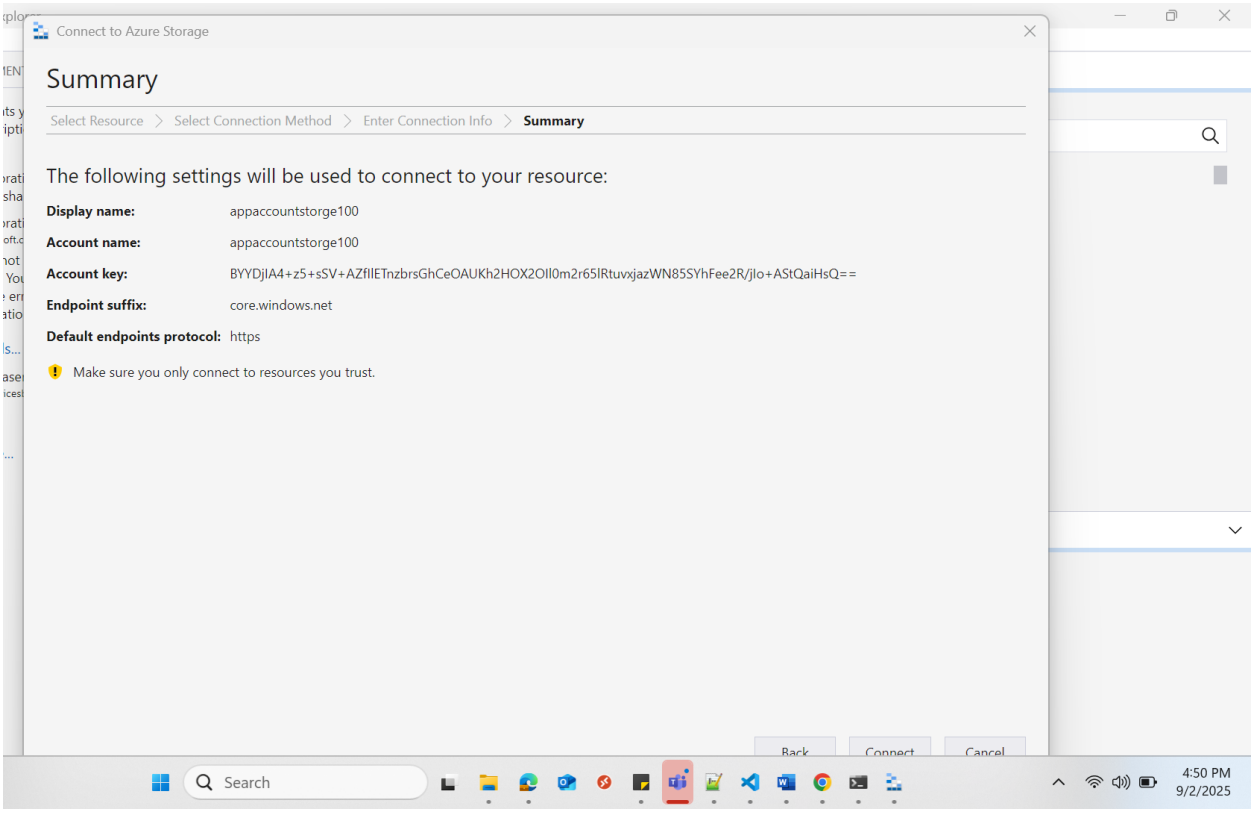


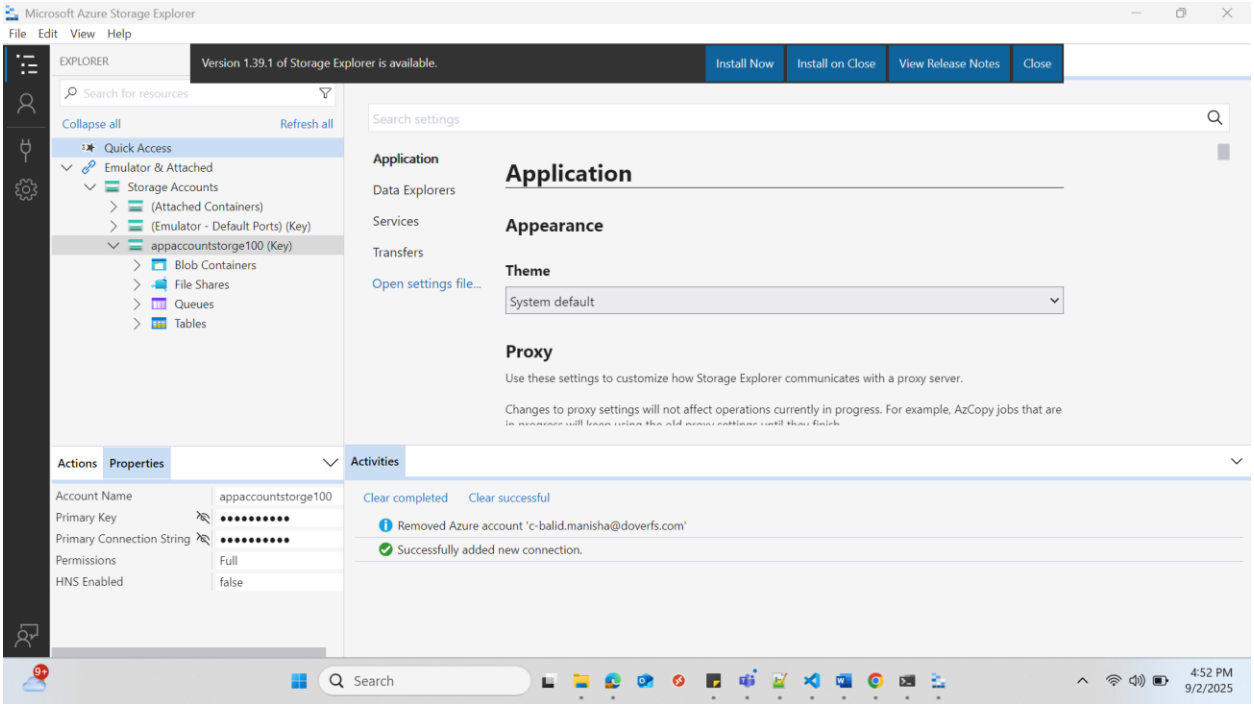
Storage account

Azure storage account – is storage on azure cloud for your blob, objects, files, queues and tables

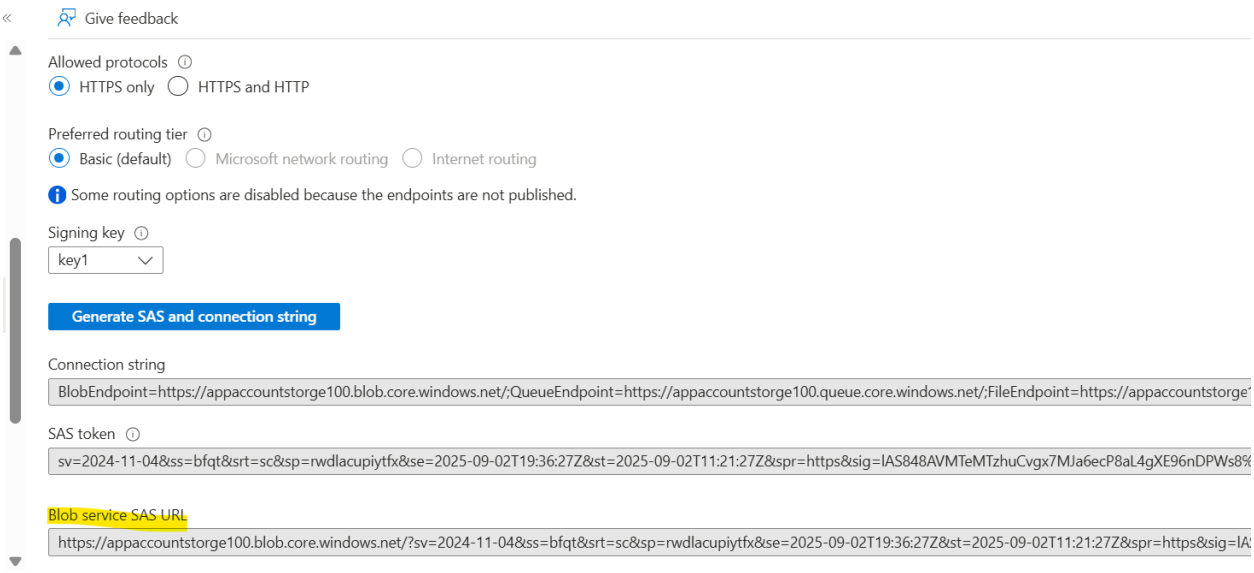


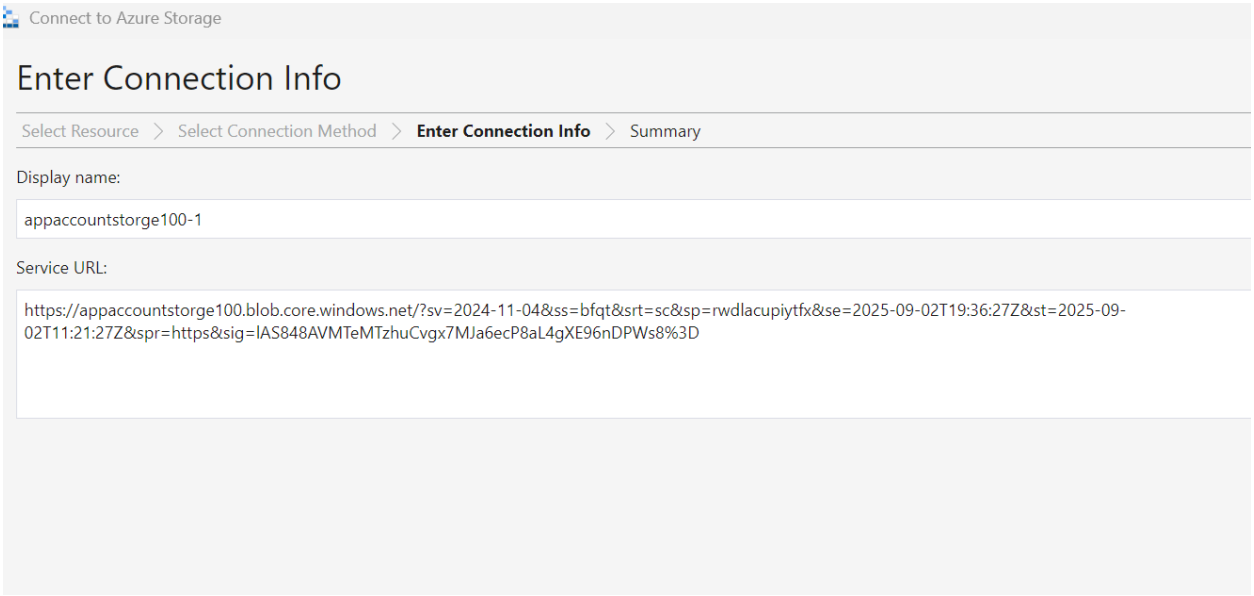
Using access key





Shared Access Signatures - At the Storage Account Level


Give feedback
Allowed protocols
HTTPS only
HTTPS and HTTP
Preferred routing tier
Basic (default)
Microsoft network routing
Internet routing
Some routing options are disabled because the endpoints are not published.
Signing key
key1
Generate SAS and connection string
Connection string
BlobEndpoint=https://appaccountstorge100.blob.core.windows.net/;QueueEndpoint=https://appaccountstorge100.queue.core.windows.net/;FileEndpoint=https://appaccountstorge
SAS token
sv=2024-11-04&ss=bfqt&srt=sc&sp=rwdlacupiytfx&se=2025-09-02T19:36:27Z&st=2025-09-02T11:21:27Z&spr=https&sig=lAS848AVMTeMTzhuCvgx7MJa6ecP8aL4gXE96nDPWs8%
Blob service SAS URL
https://appaccountstorge100.blob.core.windows.net/?sv=2024-11-04&ss=bfqt&srt=sc&sp=rwdlacupiytfx&se=2025-09-02T19:36:27Z&st=2025-09-02T11:21:27Z&spr=https&sig=lA


Connect to Azure Storage
Enter Connection Info
Select Resource
Select Connection Method
Enter Connection Info
Summary
Display name:
appaccountstorge100-1
Service URL:
https://appaccountstorge100.blob.core.windows.net/?sv=2024-11-04&ss=bfqt&srt=sc&sp=rwdlacupiytfx&se=2025-09-02T19:36:27Z&st=2025-09-02T11:21:27Z&spr=https&sig=lAS848AVMTeMTzhuCvgx7MJa6ecP8aL4gXE96nDPWs8%3D

Summary

Select Resource > Select Connection Method > Enter Connection Info > **Summary**

The following settings will be used to connect to your resource:

Display name:	appaccountstorge100-1
Account name:	appaccountstorge100
Blob endpoint:	https://appaccountstorge100.blob.core.windows.net/
File endpoint:	https://appaccountstorge100.file.core.windows.net/
Queue endpoint:	https://appaccountstorge100.queue.core.windows.net/
Table endpoint:	https://appaccountstorge100.table.core.windows.net/
SAS:	sv=2024-11-04&ss=bfqt&srt=sc&sp=rwdlacupiytfx&se=2025-09-02T19:36:27Z&st=2025-09-02T11:21:27Z&spr=https&sig=lAS848AVMTeMTzhuCvgx7MJa6ecP8aL4gXE96nDPWs8%3D
Service access:	Blob, File, Queue, Table
Resource type access:	Service, Container
Permissions:	Read, Write, Delete, List, Add, Create, Update, Process, Set immutability policy, Permanent delete, Tag, Filter, Delete version

Make sure you only connect to resources you trust.