InsightScape

(Monitor and Back up Azure resources)

Manual By-

Purav Rawat

Date: 21 October 2024

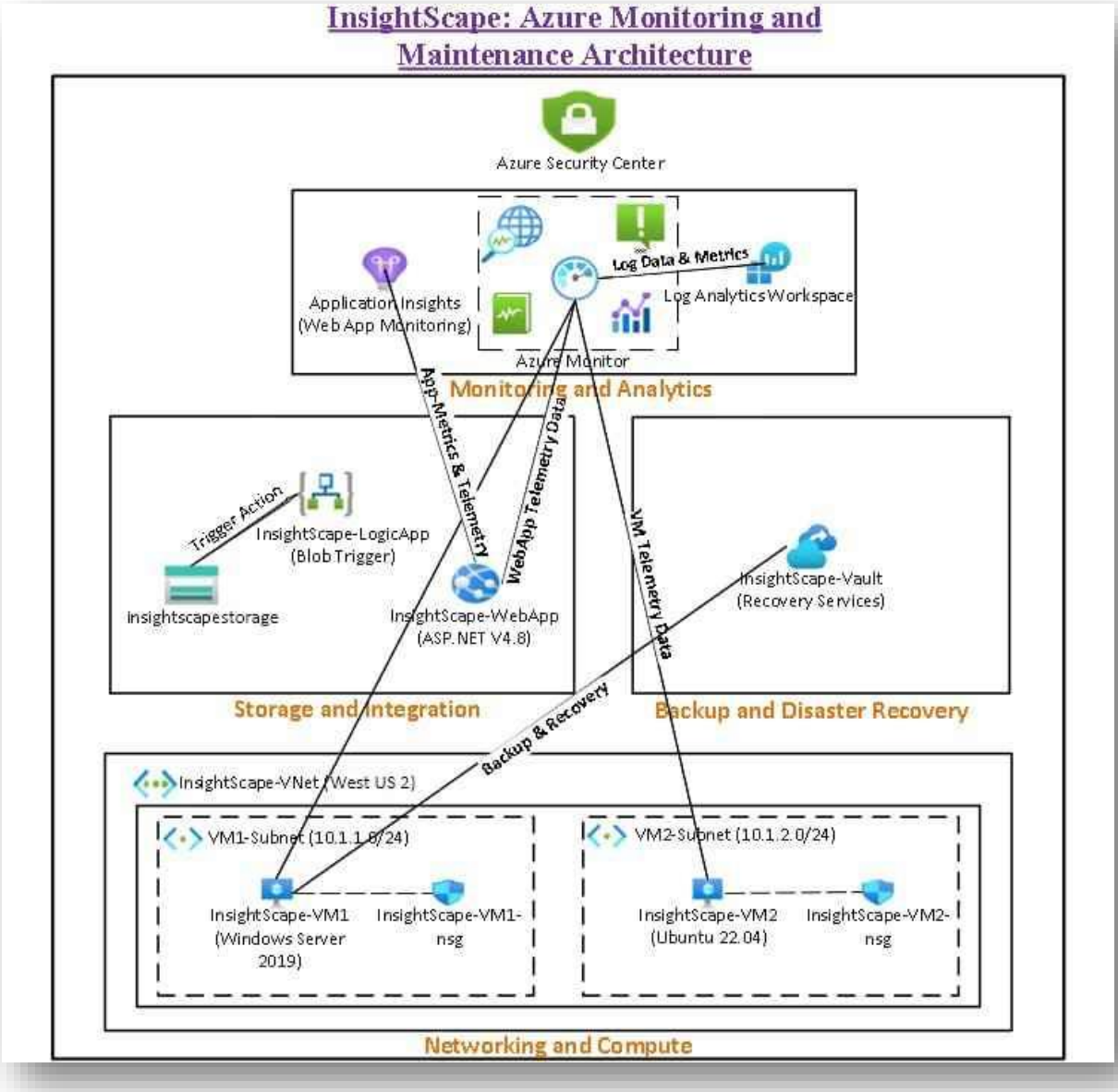
Contacts -

LinkedIn: https://www.linkedin.com/in/puravrawat/

GitHub: https://github.com/Puravcodes/InsightScape

Table of Contents

Project Architecture Diagram



Introduction

Project Overview:

Azure Monitoring and Maintenance project focuses on building a cohesive framework to monitor and maintain Azure resources using a variety of Microsoft Azure's monitoring, analytics, and security services. This project is designed to provide full visibility into the cloud environment, enhance security, and ensure performance optimization, leveraging Azure's robust tools for effective resource management.

Throughout the project, I implemented several Azure services, such as Azure Monitor, Log Analytics, Application Insights, Network Watcher, Azure Security Center, and Azure Backup. My objective was to establish a monitoring infrastructure that ensures cloud resources, including Virtual Machines, Virtual Networks, and a Web App, perform at peak efficiency. The project covers every stage, from initial setup to integrating monitoring and alerting capabilities, ensuring seamless operation and providing detailed insights into application performance, resource health, network security, and compliance management.

Purpose of this Documentation:

This document offers a detailed, step-by-step guide for recreating the InsightScape project, featuring clear instructions and screenshots to enhance understanding. It serves as a valuable resource for learning how to deploy monitoring and maintenance solutions for Azure resources, making it useful for both students and professionals alike.

The primary objective is to thoroughly document the project, highlighting my technical expertise, familiarity with Azure services, and overall approach. Additionally, it acts as a professional portfolio, showcasing my skills for potential employers and contributing to the broader tech community.

Prerequisites:

Before beginning this project, it's essential to have a foundational understanding of cloud computing, monitoring principles, and familiarity with the Azure portal. Additionally, ensure that the following prerequisites are in place:

1. **Azure Subscription**: A valid Azure subscription is required to deploy and manage resources.
2. **Basic Azure Knowledge**: Familiarity with Azure resources like Virtual Machines, Virtual Networks, and Network Security Groups (NSGs).
3. **Kusto Query Language (KQL) (Optional)**: While not mandatory, knowledge of KQL can be helpful for creating custom monitoring queries in Log Analytics.

This documentation, designed to demonstrate the completion of the InsightScape project, serves as a hands-on guide for setting up and managing a monitoring and maintenance framework in Azure. It provides valuable insights and best practices for replicating the project effectively.

Resources Setup

a) Resource Group and Virtual Networks

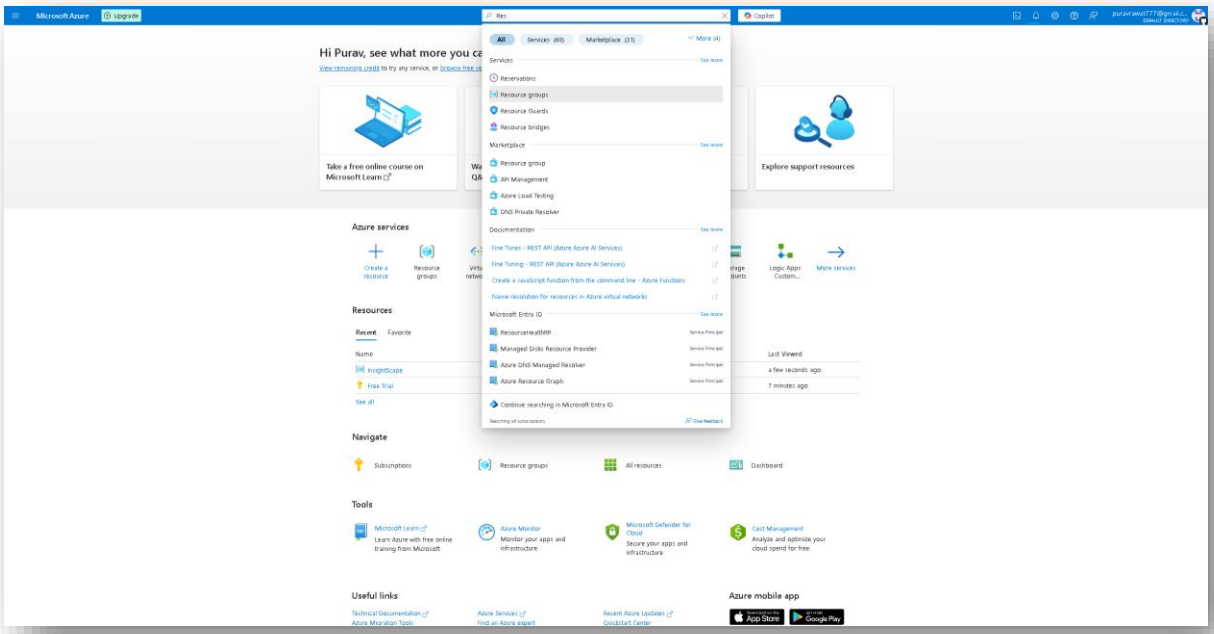
First, I created a Resource Group named **InsightScape-RG** in the West US 2 region, (You can create it in any region you want just make sure that the other resources you create are in the same region as your resource group) which I used to deploy the entire project. Next, I proceeded to create a Virtual Network:

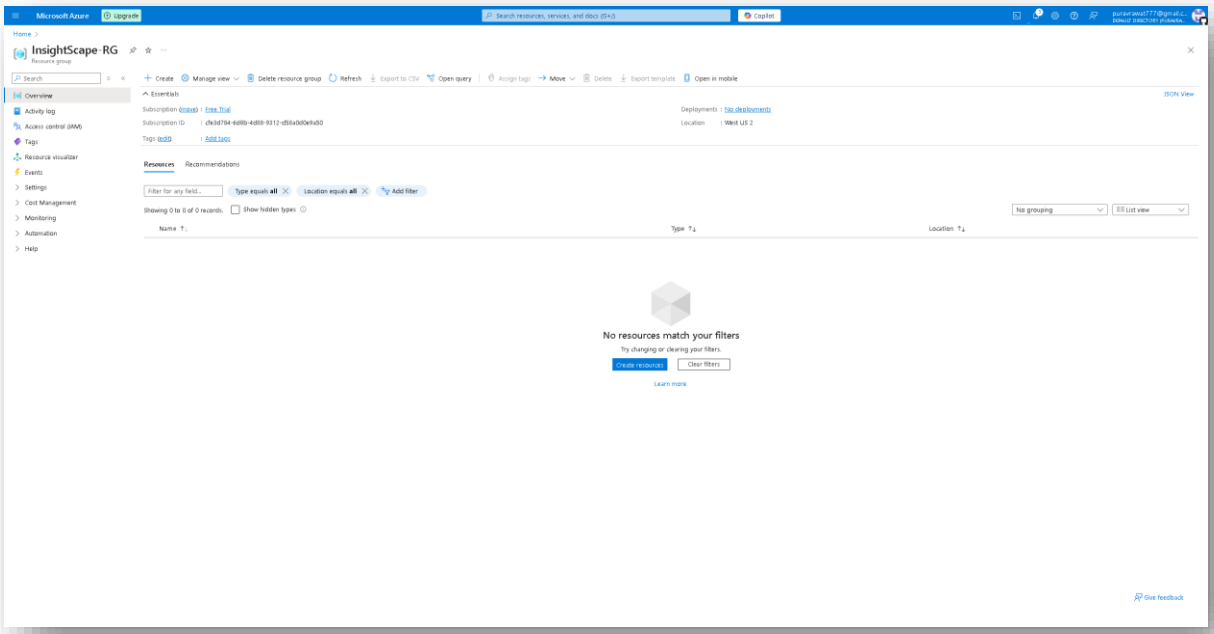
Virtual Network Creation:

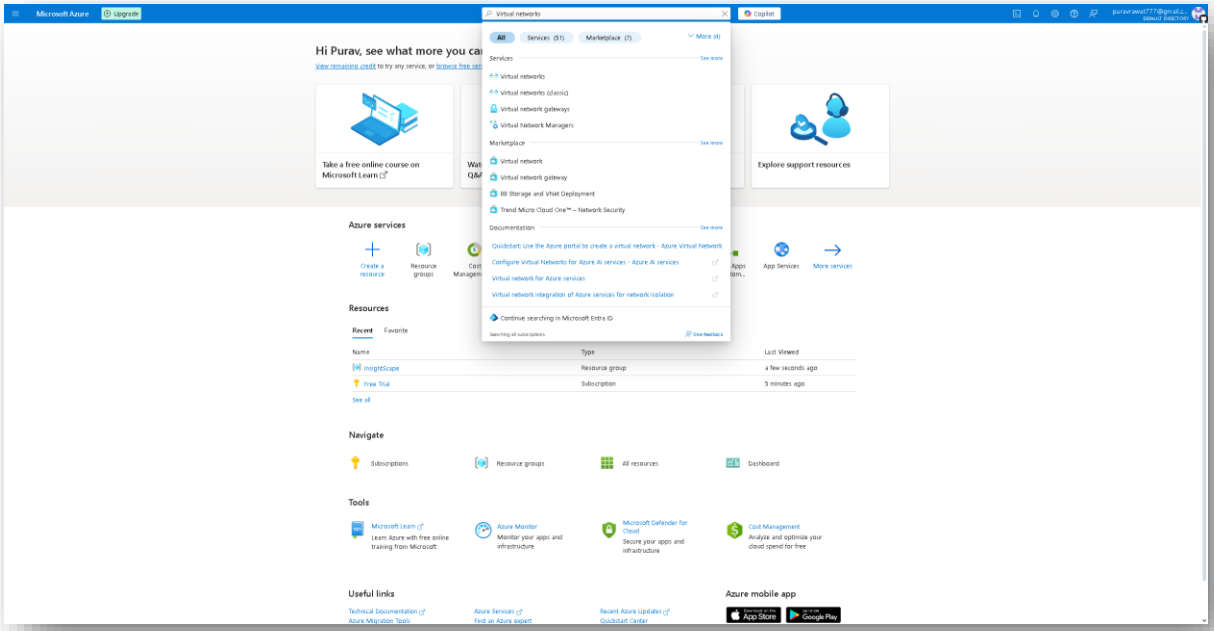
- Name**: InsightScape-VNet**
- Region: West US 2
- IP Addresses Configuration:
    1. Added a subnet named **VM1-Subnet**
        - IPv4 Address Range: 10.1.0.0/16
        - Starting Address: 10.1.1.0
        - Size: /24
    2. Added a second subnet named **VM2-Subnet**
        - IPv4 Address Range: 10.1.0.0/16
        - Starting Address: 10.1.2.0
        - Size: /24

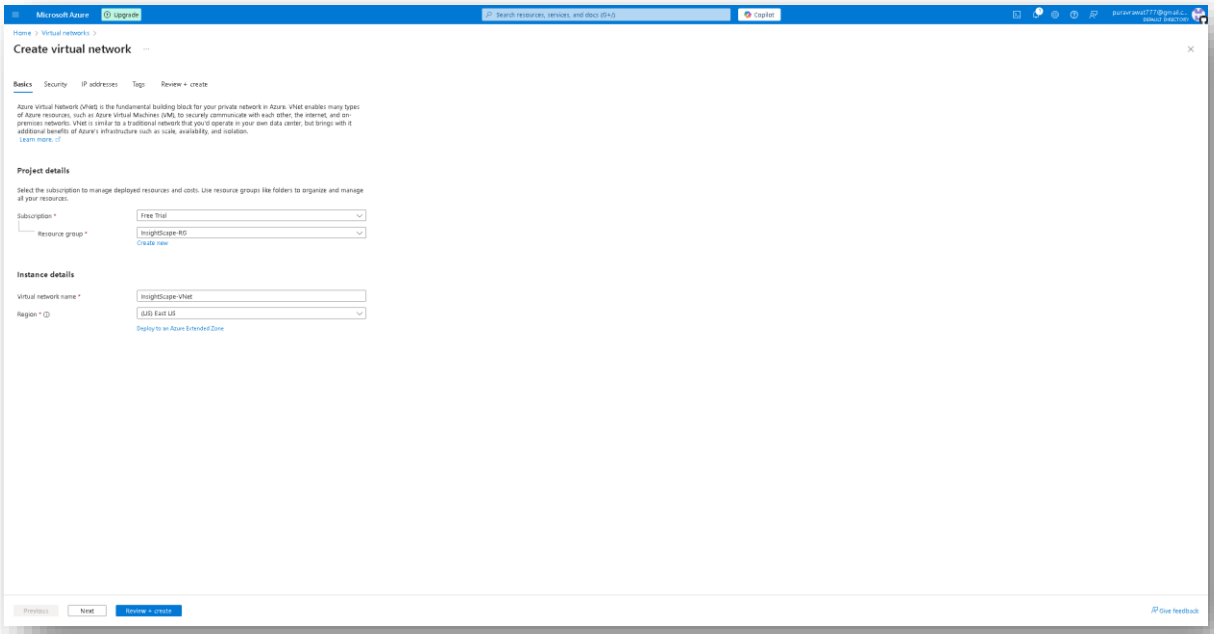
After completing these configurations, the InsightScape-VNet was successfully created.

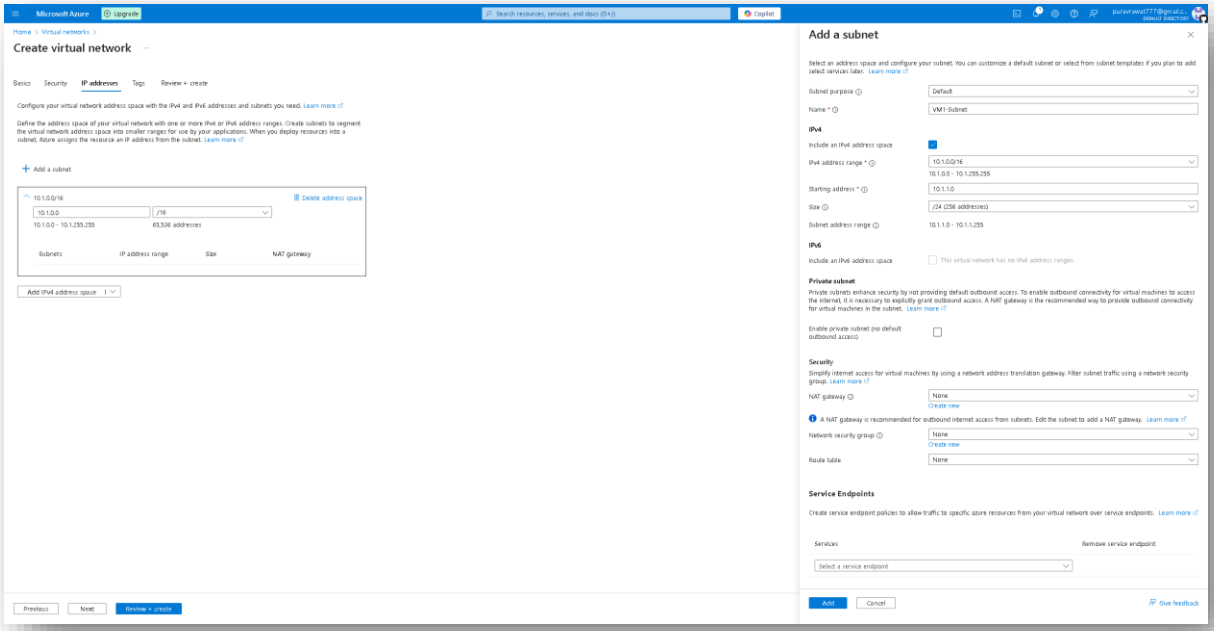
Screenshots -

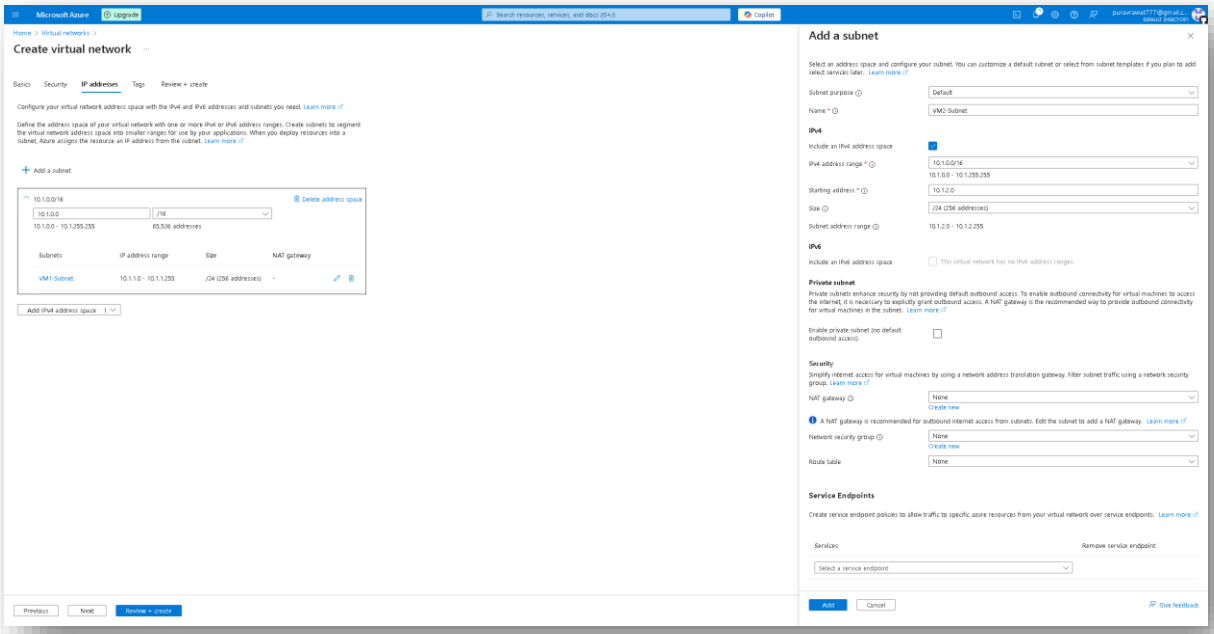


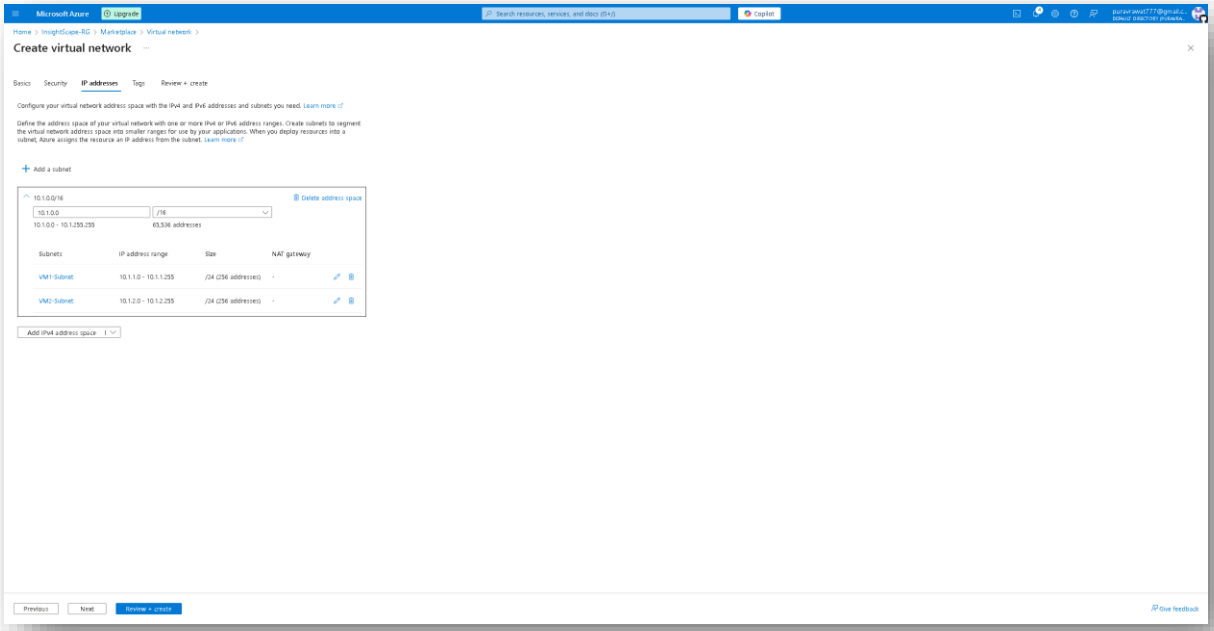


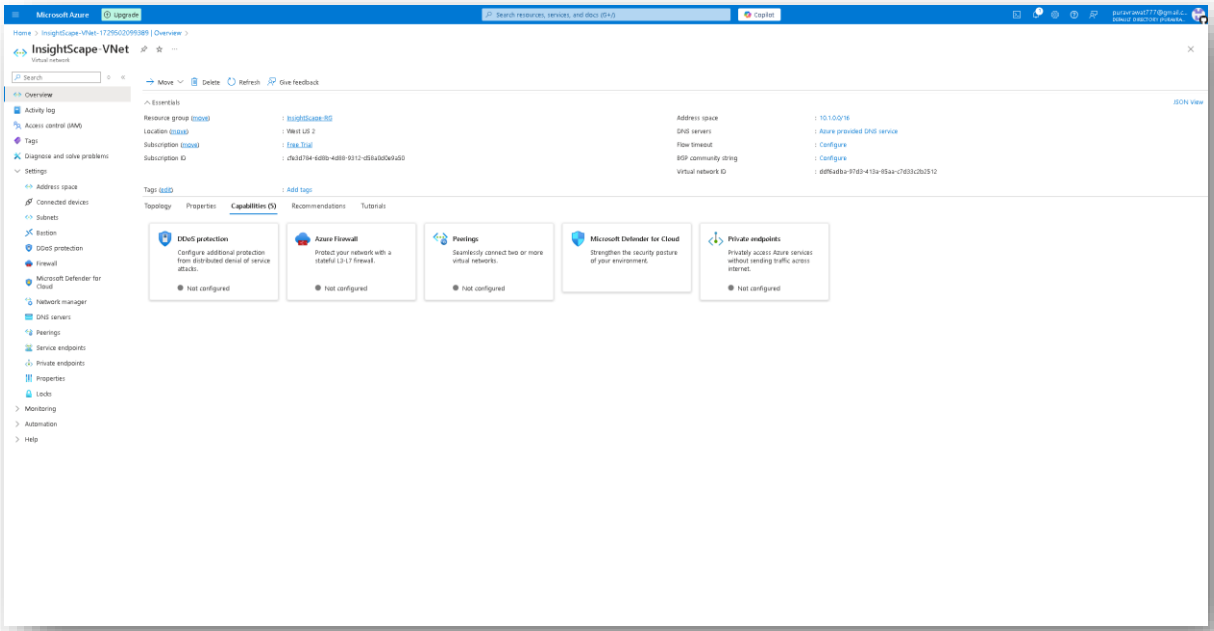

Microsoft Azure
Upgrade
Virtual networks
Copilot
Hi Purav, see what more you ca
Take a free online course on Microsoft Learn
Explore support resources
Azure services
Create a resource
Resource groups
App Services
More services
Resources
Recent
Favorite
Name
Type
Last Viewed
InsightScape
Resource group
a few seconds ago
Free Trial
Subscription
5 minutes ago
See all
Navigate
Subscriptions
Resource groups
All resources
Dashboard
Tools
Microsoft Learn
Learn Azure with free online training from Microsoft
Azure Monitor
Monitor your apps and infrastructure
Microsoft Defender for Cloud
Secure your apps and infrastructure
Cost Management
Analyze and optimize your cloud spend for free
Useful links
Technical Documentation
Azure Migration Tools
Azure Services
Find an Azure expert
Recent Azure Updates
Quickstart Center
Azure mobile app
App Store
Google Play


Microsoft Azure
Upgrade
Copilot
Home > Virtual networks >
Create virtual network
Basics
Security
IP addresses
Tags
Review + create
Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.
Learn more.
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
Free Trial
Resource group *
InsightScape-RG
Create new
Instance details
Virtual network name *
InsightScape-VNet
Region *
(US) East US
Deploy to an Azure Extended Zone
Previous
Next
Review + create
Give feedback


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Virtual networks >
Create virtual network
Basics
Security
IP addresses
Tags
Review + create
Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. Learn more
Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. Learn more
Add a subnet
10.1.0.0/16
10.1.0.0
/16
10.1.0.0 - 10.1.255.255
65,536 addresses
Delete address space
Subnets
IP address range
Size
NAT gateway
Add IPv4 address space
Previous
Next
Review + create
Add a subnet
Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. Learn more
Subnet purpose
Default
Name *
VM1-Subnet
IPv4
Include an IPv4 address space
IPv4 address range *
10.1.0.0/16
10.1.0.0 - 10.1.255.255
Starting address *
10.1.1.0
Size
/24 (256 addresses)
Subnet address range
10.1.1.0 - 10.1.1.255
IPv6
Include an IPv6 address space
This virtual network has no IPv6 address ranges.
Private subnet
Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. Learn more
Enable private subnet (no default outbound access)
Security
Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. Learn more
NAT gateway
None
Create new
A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. Learn more
Network security group
None
Create new
Route table
None
Service Endpoints
Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more
Services
Remove service endpoint
Select a service endpoint
Add
Cancel
Give feedback


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Virtual networks >
Create virtual network
Basics
Security
IP addresses
Tags
Review + create
Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. Learn more
Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. Learn more
Add a subnet
10.1.0.0/16
10.1.0.0
/16
10.1.0.0 - 10.1.255.255
65,536 addresses
Delete address space
Subnets
IP address range
Size
NAT gateway
VM1-Subnet
10.1.1.0 - 10.1.1.255
/24 (256 addresses)
-
Add IPv4 address space
Previous
Next
Review + create
Add a subnet
Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. Learn more
Subnet purpose
Default
Name *
VM2-Subnet
IPv4
Include an IPv4 address space
IPv4 address range *
10.1.0.0/16
10.1.0.0 - 10.1.255.255
Starting address *
10.1.2.0
Size
/24 (256 addresses)
Subnet address range
10.1.2.0 - 10.1.2.255
IPv6
Include an IPv6 address space
This virtual network has no IPv6 address ranges.
Private subnet
Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. Learn more
Enable private subnet (no default outbound access)
Security
Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. Learn more
NAT gateway
None
Create new
A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. Learn more
Network security group
None
Create new
Route table
None
Service Endpoints
Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more
Services
Remove service endpoint
Select a service endpoint
Add
Cancel
Give feedback


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > InsightScape-RG > Marketplace > Virtual network >
Create virtual network
Basics
Security
IP addresses
Tags
Review + create
Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. Learn more
Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. Learn more
Add a subnet
10.1.0.0/16
Delete address space
10.1.0.0
/16
10.1.0.0 - 10.1.255.255
65,536 addresses
Subnets
IP address range
Size
NAT gateway
VM1-Subnet
10.1.1.0 - 10.1.1.255
/24 (256 addresses)
VM2-Subnet
10.1.2.0 - 10.1.2.255
/24 (256 addresses)
Add IPv4 address space
Previous
Next
Review + create
Give feedback


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > InsightScape-VNet-1729602099389 | Overview >
InsightScape-VNet
Virtual network
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Address space
Connected devices
Subnets
Bastion
DDoS protection
Firewall
Microsoft Defender for Cloud
Network manager
DNS servers
Peerings
Service endpoints
Private endpoints
Properties
Locks
Monitoring
Automation
Help
Move
Delete
Refresh
Give feedback
Essentials
JSON View
Resource group (move) : InsightScape-RG
Location (move) : West US 2
Subscription (move) : Free Trial
Subscription ID : cfa3d784-6d0b-4d88-9312-d58a80d0e950
Address space : 10.1.0.0/16
DNS servers : Azure provided DNS service
Flow timeout : Configure
BGP community string : Configure
Virtual network ID : ddf6adba-97d3-413a-85aa-c7d33c2b2512
Tags (edit) : Add tags
Topology
Properties
Capabilities (5)
Recommendations
Tutorials
DDoS protection
Configure additional protection from distributed denial of service attacks.
Not configured
Azure Firewall
Protect your network with a stateful L3-L7 firewall.
Not configured
Peerings
Seamlessly connect two or more virtual networks.
Not configured
Microsoft Defender for Cloud
Strengthen the security posture of your environment.
Private endpoints
Privately access Azure services without sending traffic across internet.
Not configured

b) VMs and NSGs

Next, it was time to set up the Virtual Machines (VMs) and the Network Security Groups (NSGs):

1. Windows VM Creation (InsightScape-VM1):

    - Resource Group: InsightScape-RG
    - Virtual Machine Name: InsightScape-VM1
    - Region: West US 2
    - Availability Options: No infrastructure redundancy required
    - Security Type: Standard
    - Size: Standard B1s
    - Virtual Network: InsightScape-VNet
    - Subnet: VM1-Subnet (10.1.1.0/24)
    - Public IP: Created a new IP, named InsightScape-VM1-ip
    - NIC Network Security Group: Basic
    - Public Inbound Ports: RDP, HTTPS

2. Linux VM Creation (InsightScape-VM2):

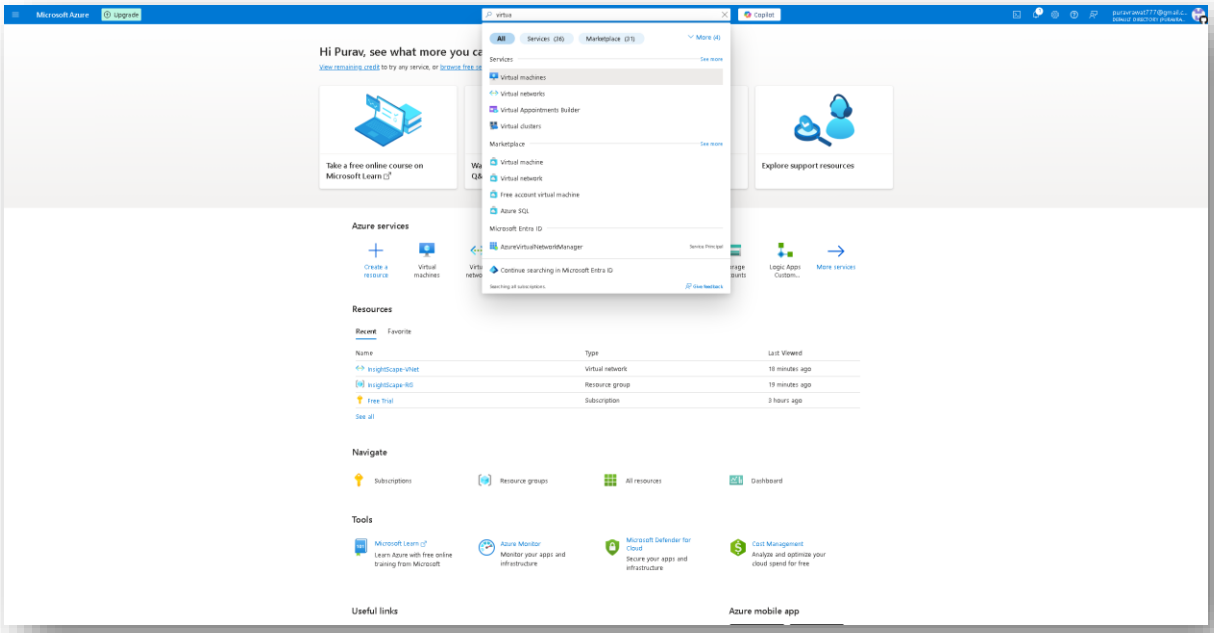
    - Resource Group: InsightScape-RG
    - Virtual Machine Name: InsightScape-VM2
    - Region: West US 2
    - Availability Options: No infrastructure redundancy required
    - Security Type: Standard
    - Size: Standard B1s
    - Authentication Type: Password
    - Username: InsightScape-User2
    - Virtual Network: InsightScape-VNet
    - Subnet: VM2-Subnet (10.1.2.0/24)
    - Public IP: Created a new IP, named InsightScape-VM2-ip
    - NIC Network Security Group: Basic
    - Public Inbound Ports: SSH, HTTPS, HTTP

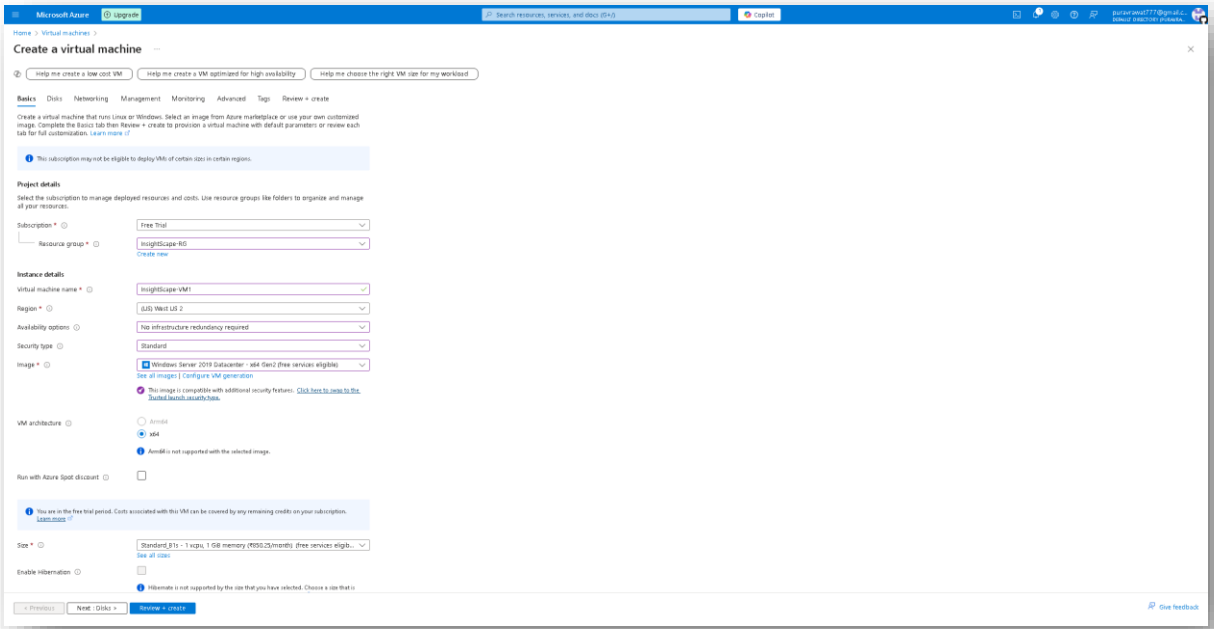
NSG Updates:

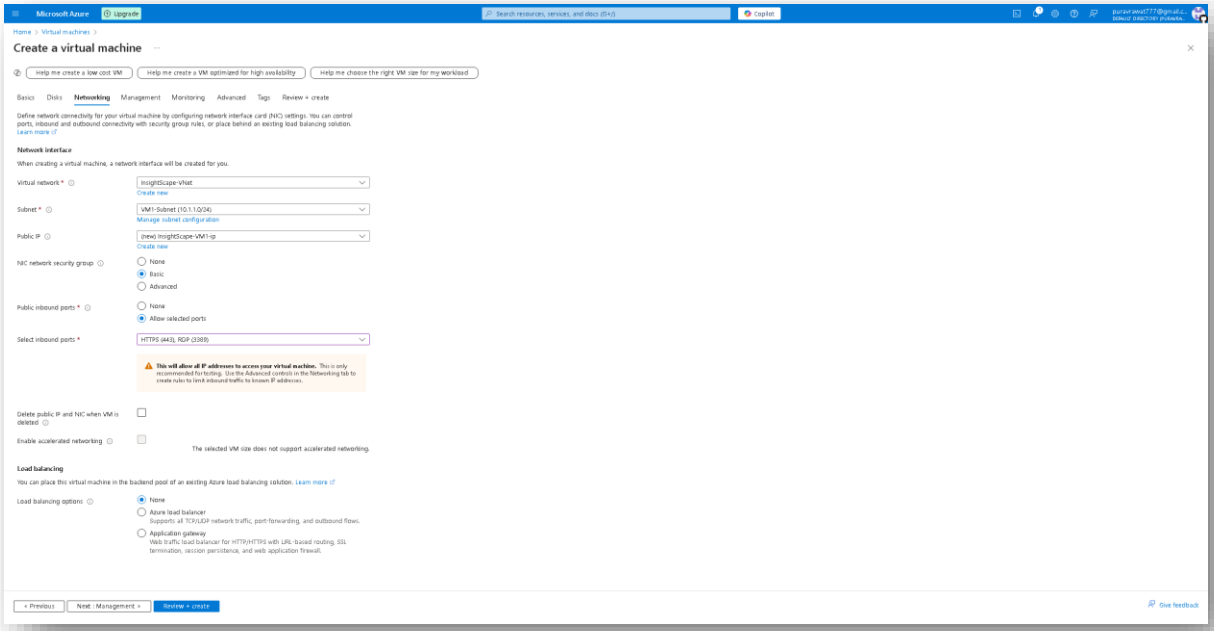
1. InsightScape-VM1-nsg:
    - Inbound Security Rule:
        - Source: Any
        - Source Port Ranges: *
        - Destination: Any
        - Service: HTTP
        - Destination Port Ranges: 80
        - Protocol: TCP
        - Action: Allow
    - Saved the security rule.

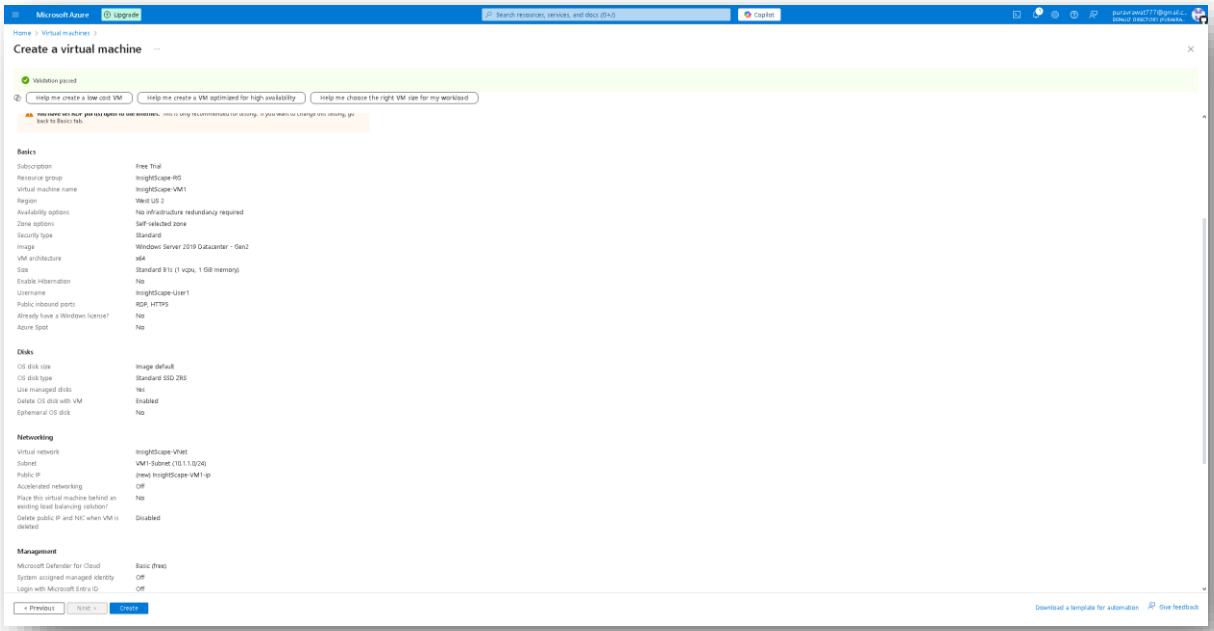
2. InsightScape-VM2-nsg:
    - No changes were made, as the default settings were sufficient.

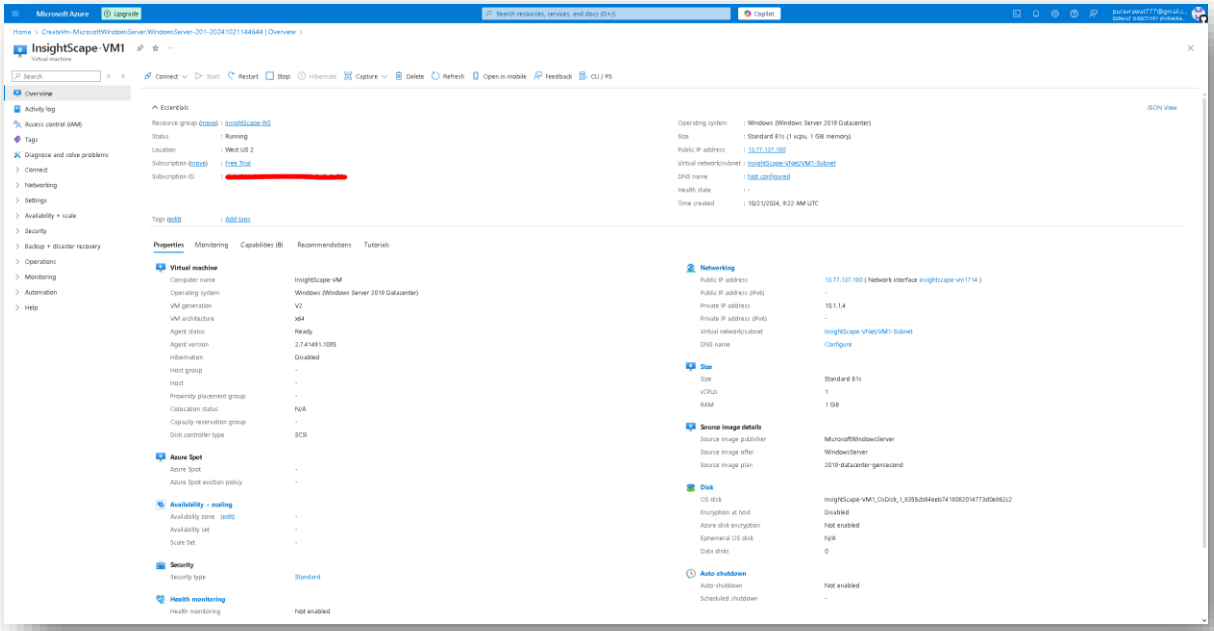
Screenshots –

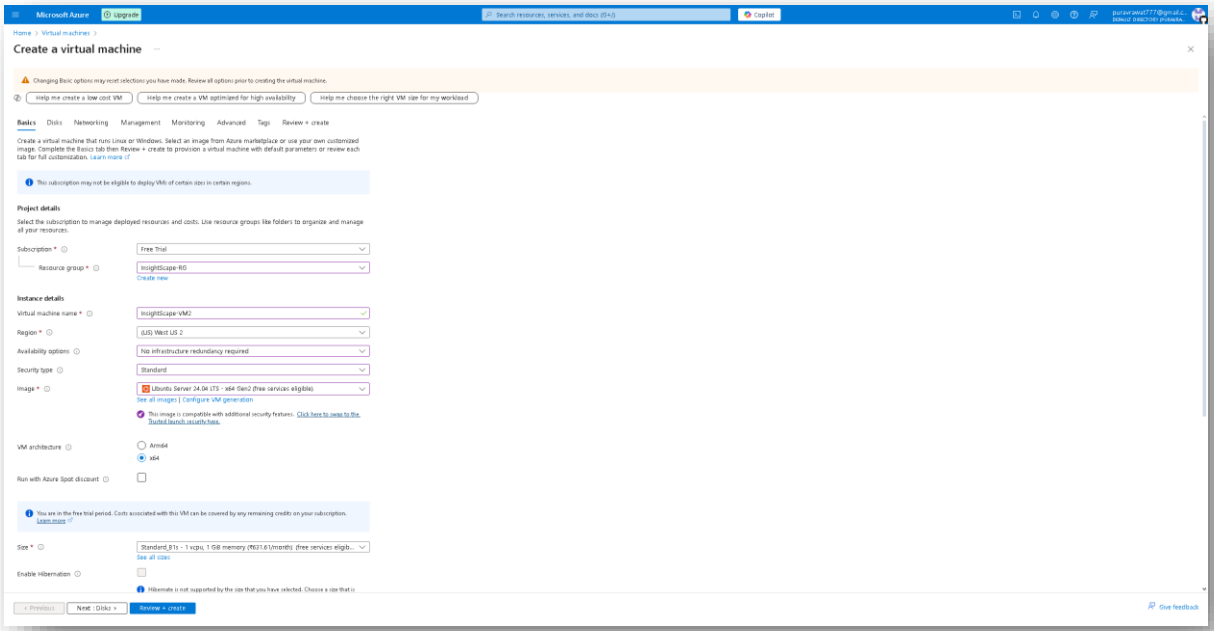


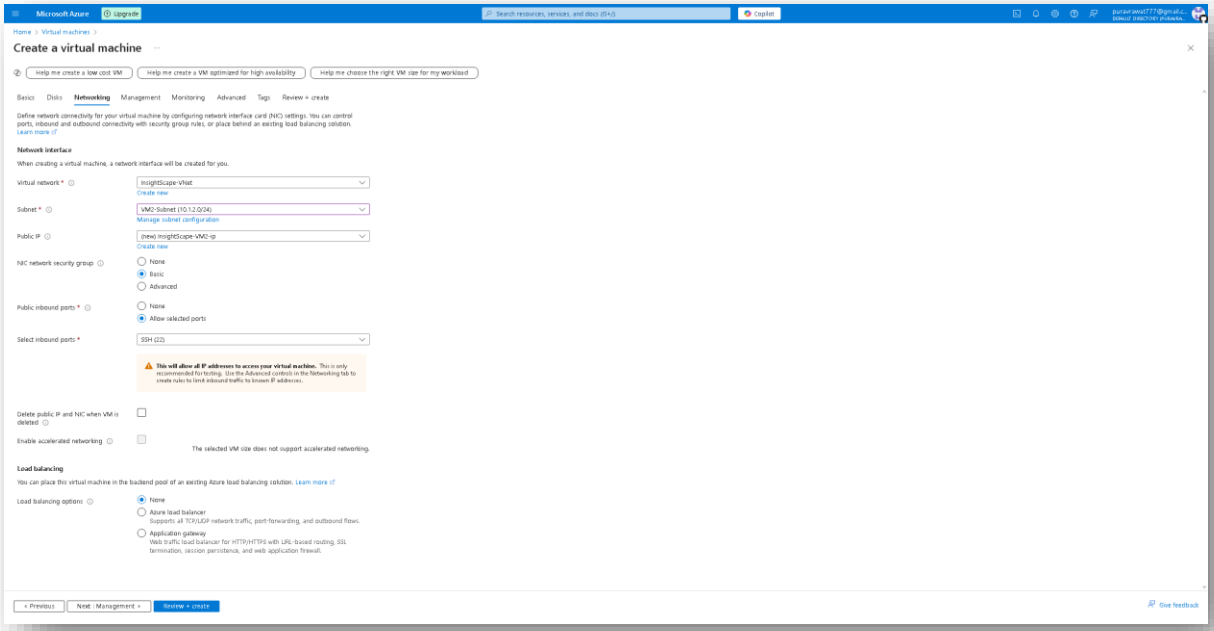


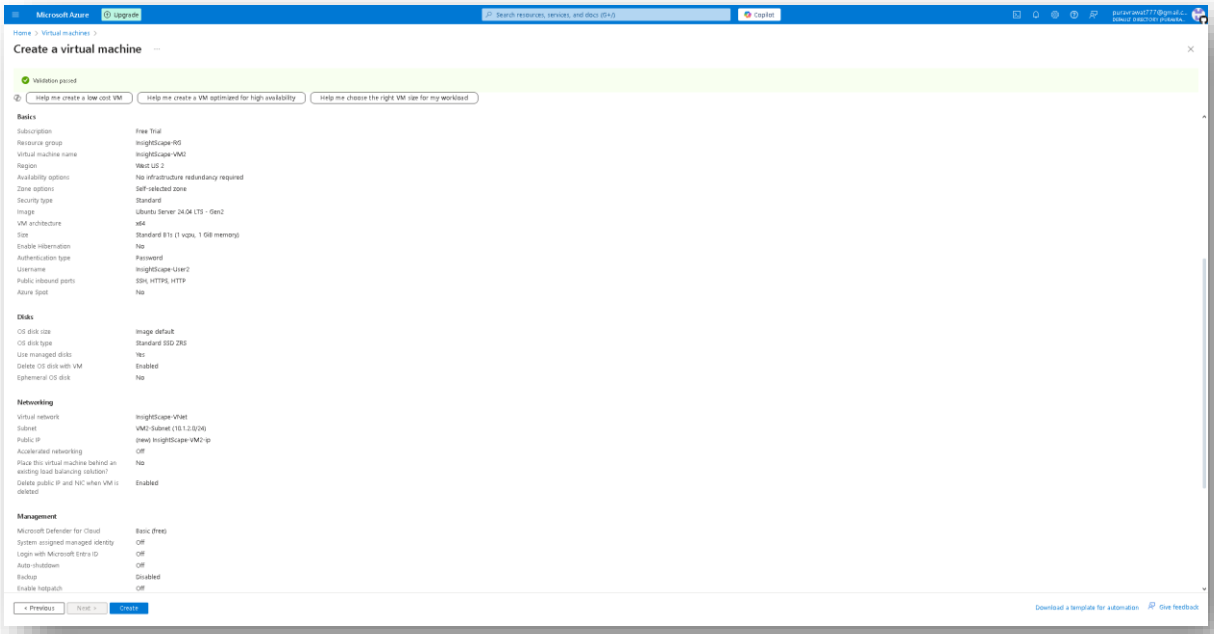

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Virtual machines >
Create a virtual machine
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics Disks Networking Management Monitoring Advanced Tags Review + create
Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
Learn more
Network interface
When creating a virtual machine, a network interface will be created for you.
Virtual network *
InsightScape-VNet
Create new
Subnet *
VM1-Subnet (10.1.1.0/24)
Manage subnet configuration
Public IP
(new) InsightScape-VM1-ip
Create new
NIC network security group
None
Basic
Advanced
Public inbound ports *
None
Allow selected ports
Select inbound ports *
HTTPS (443), RDP (3389)
This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.
Delete public IP and NIC when VM is deleted
Enable accelerated networking
The selected VM size does not support accelerated networking.
Load balancing
You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more
Load balancing options
None
Azure load balancer
Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.
Application gateway
Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL termination, session persistence, and web application firewall.
< Previous
Next : Management >
Review + create
Give feedback

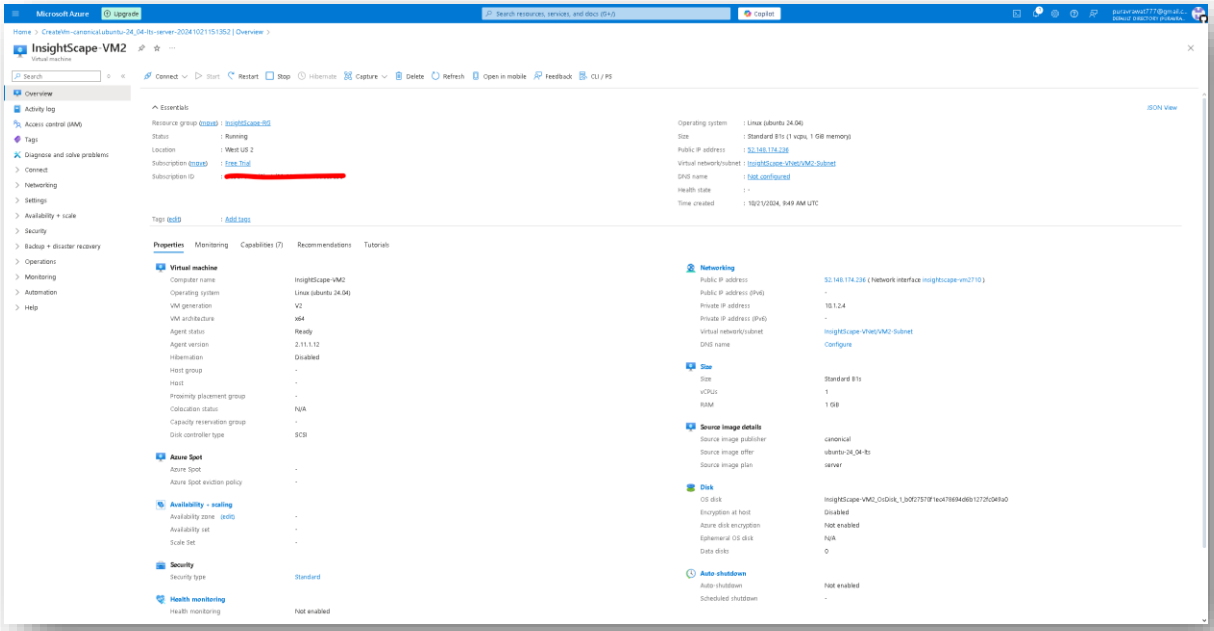

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Virtual machines >
Create a virtual machine
Validation passed
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Subscription Free Trial
Resource group InsightScape-RG
Virtual machine name InsightScape-VM1
Region West US 2
Availability options No infrastructure redundancy required
Zone options Self-selected zone
Security type Standard
Image Windows Server 2019 Datacenter - Gen2
VM architecture x64
Size Standard B1s (1 vcpu, 1 GiB memory)
Enable Hibernation No
Username InsightScape-User1
Public inbound ports RDP, HTTPS
Already have a Windows license? No
Azure Spot No
Disks
OS disk size Image default
OS disk type Standard SSD ZRS
Use managed disks Yes
Delete OS disk with VM Enabled
Ephemeral OS disk No
Networking
Virtual network InsightScape-VNet
Subnet VM1-Subnet (10.1.1.0/24)
Public IP (new) InsightScape-VM1-ip
Accelerated networking Off
Place this virtual machine behind an existing load balancing solution? No
Delete public IP and NIC when VM is deleted Disabled
Management
Microsoft Defender for Cloud Basic (free)
System assigned managed identity Off
Login with Microsoft Entra ID Off
< Previous
Next >
Create
Download a template for automation
Give feedback

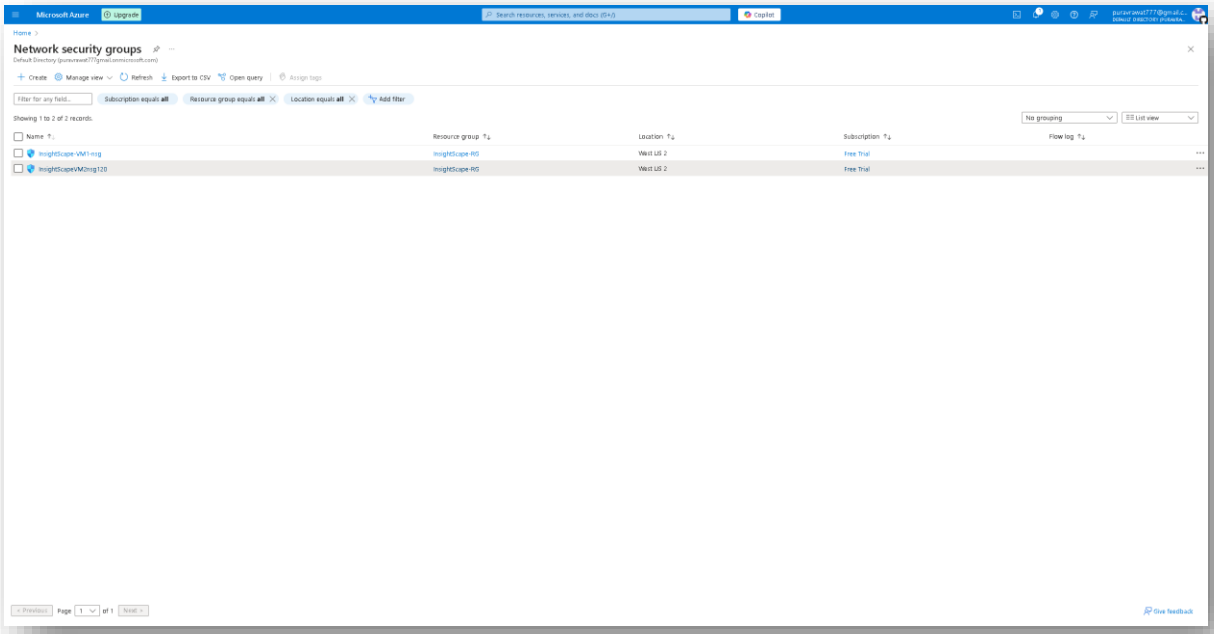

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > CreateVm-MicrosoftWindowsServer.WindowsServer-201-20241021144644 | Overview >
InsightScape-VM1
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Connect
Networking
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Automation
Help
Connect
Start
Restart
Stop
Hibernate
Capture
Delete
Refresh
Open in mobile
Feedback
CLI / PS
Essentials
JSON View
Resource group (move) : InsightScape-RG
Status : Running
Location : West US 2
Subscription (move) : Free Trial
Subscription ID :
Operating system : Windows (Windows Server 2019 Datacenter)
Size : Standard B1s (1 vcpu, 1 GiB memory)
Public IP address : 13.77.137.180
Virtual network/subnet : InsightScape-VNet/VM1-Subnet
DNS name : Not configured
Health state : -
Time created : 10/21/2024, 9:22 AM UTC
Tags (edit) : Add tags
Properties
Monitoring
Capabilities (8)
Recommendations
Tutorials
Virtual machine
Computer name InsightScape-VM
Operating system Windows (Windows Server 2019 Datacenter)
VM generation V2
VM architecture x64
Agent status Ready
Agent version 2.7.41491.1095
Hibernation Disabled
Host group -
Host -
Proximity placement group -
Colocation status N/A
Capacity reservation group -
Disk controller type SCSI
Azure Spot
Azure Spot eviction policy -
Availability + scaling
Availability zone (edit) -
Availability set -
Scale Set -
Security
Security type Standard
Health monitoring
Health monitoring Not enabled
Networking
Public IP address 13.77.137.180 (Network interface insightscape-vm1714)
Public IP address (IPv6) -
Private IP address 10.1.1.4
Private IP address (IPv6) -
Virtual network/subnet InsightScape-VNet/VM1-Subnet
DNS name Configure
Size
Size Standard B1s
vCPUs 1
RAM 1 GiB
Source image details
Source image publisher MicrosoftWindowsServer
Source image offer WindowsServer
Source image plan 2019-datacenter-gensecond
Disk
OS disk InsightScape-VM1_OsDisk_1_835cbb4eeb7418082014773d0e862c2
Encryption at host Disabled
Azure disk encryption Not enabled
Ephemeral OS disk N/A
Data disks 0
Auto-shutdown
Auto-shutdown Not enabled
Scheduled shutdown -

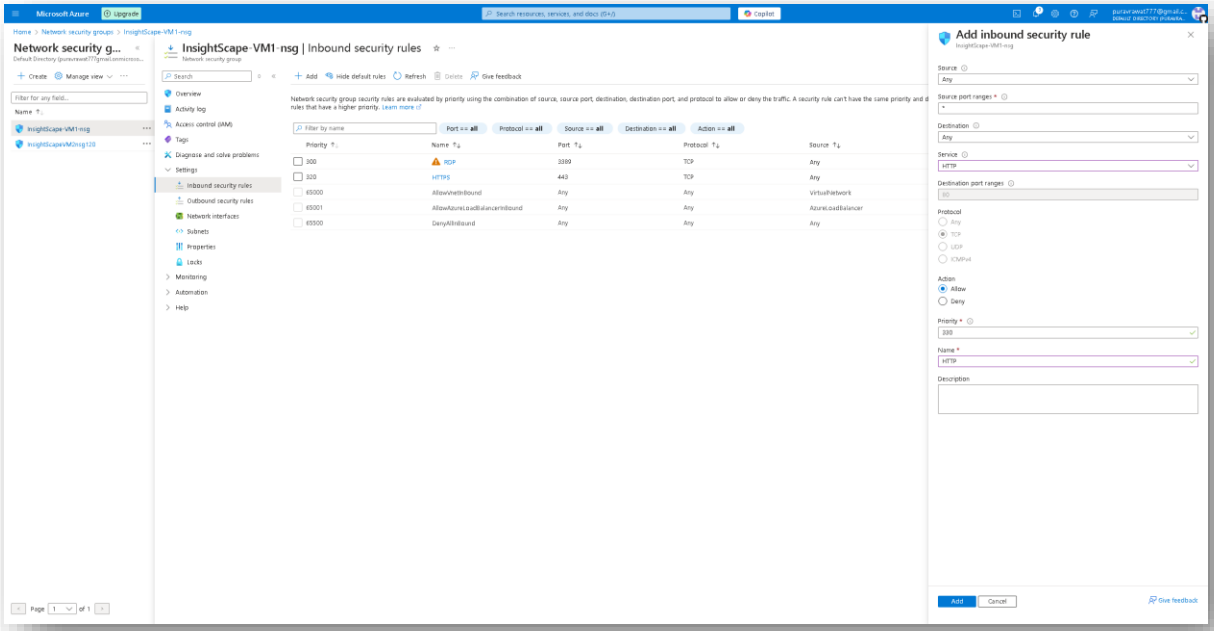

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Virtual machines >
Create a virtual machine
Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create
Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more
This subscription may not be eligible to deploy VMs of certain sizes in certain regions.
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription * Free Trial
Resource group * InsightScape-RG
Create new
Instance details
Virtual machine name * InsightScape-VM2
Region * (US) West US 2
Availability options No infrastructure redundancy required
Security type Standard
Image * Ubuntu Server 24.04 LTS - x64 Gen2 (free services eligible)
See all images | Configure VM generation
This image is compatible with additional security features. Click here to swap to the Trusted launch security type.
VM architecture Arm64
x64
Run with Azure Spot discount
You are in the free trial period. Costs associated with this VM can be covered by any remaining credits on your subscription.
Learn more
Size * Standard_B1s - 1 vcpu, 1 GiB memory (₹631.61/month) (free services eligib...
See all sizes
Enable Hibernation
Hibernate is not supported by the size that you have selected. Choose a size that is
< Previous
Next : Disks >
Review + create
Give feedback

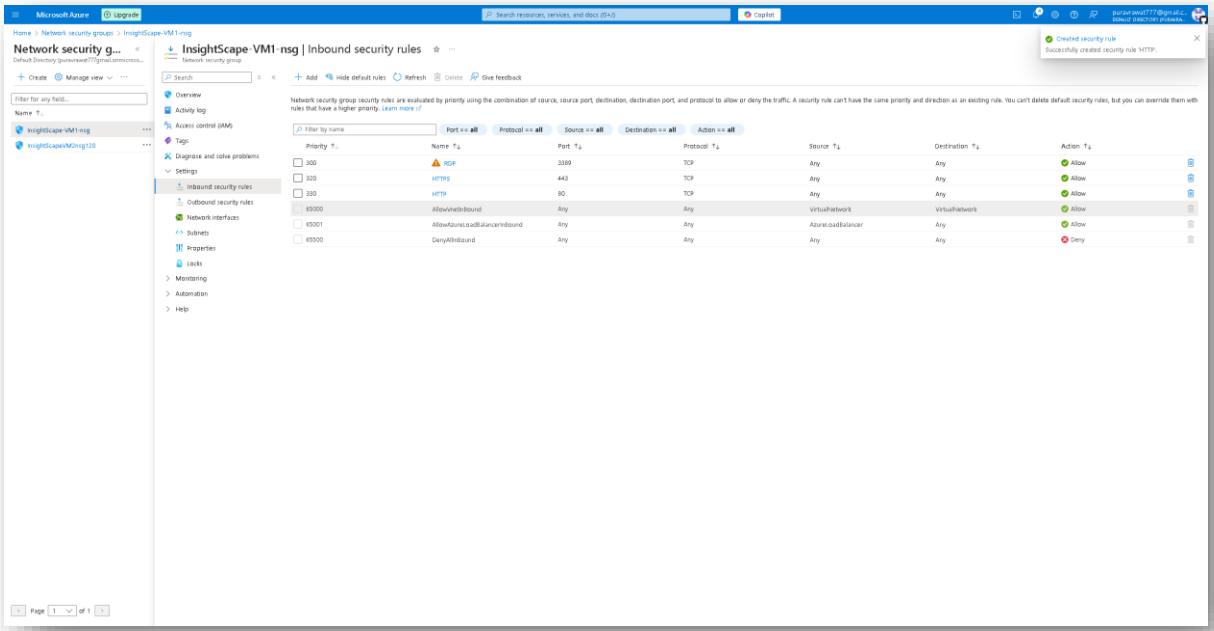

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Virtual machines >
Create a virtual machine
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics Disks Networking Management Monitoring Advanced Tags Review + create
Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
Learn more
Network interface
When creating a virtual machine, a network interface will be created for you.
Virtual network *
InsightScape-VNet
Create new
Subnet *
VM2-Subnet (10.1.2.0/24)
Manage subnet configuration
Public IP
(new) InsightScape-VM2-ip
Create new
NIC network security group
None
Basic
Advanced
Public inbound ports *
None
Allow selected ports
Select inbound ports *
SSH (22)
This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.
Delete public IP and NIC when VM is deleted
Enable accelerated networking
The selected VM size does not support accelerated networking.
Load balancing
You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more
Load balancing options
None
Azure load balancer
Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.
Application gateway
Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL termination, session persistence, and web application firewall.
< Previous
Next : Management >
Review + create
Give feedback

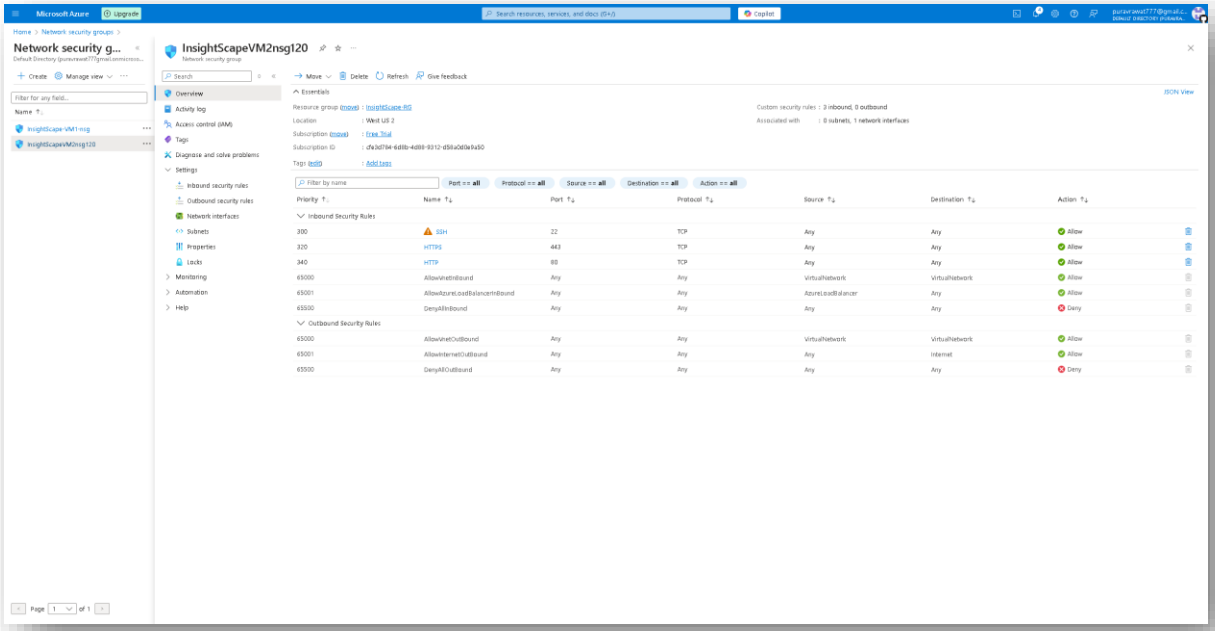

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Virtual machines >
Create a virtual machine
Validation passed
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Subscription Free Trial
Resource group InsightScape-RG
Virtual machine name InsightScape-VM2
Region West US 2
Availability options No infrastructure redundancy required
Zone options Self-selected zone
Security type Standard
Image Ubuntu Server 24.04 LTS - Gen2
VM architecture x64
Size Standard B1s (1 vcpu, 1 GiB memory)
Enable Hibernation No
Authentication type Password
Username InsightScape-User2
Public inbound ports SSH, HTTPS, HTTP
Azure Spot No
Disks
OS disk size Image default
OS disk type Standard SSD ZRS
Use managed disks Yes
Delete OS disk with VM Enabled
Ephemeral OS disk No
Networking
Virtual network InsightScape-VNet
Subnet VM2-Subnet (10.1.2.0/24)
Public IP (new) InsightScape-VM2-ip
Accelerated networking Off
Place this virtual machine behind an existing load balancing solution? No
Delete public IP and NIC when VM is deleted Enabled
Management
Microsoft Defender for Cloud Basic (free)
System assigned managed identity Off
Login with Microsoft Entra ID Off
Auto-shutdown Off
Backup Disabled
Enable hotpatch Off
< Previous
Next >
Create
Download a template for automation
Give feedback


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > CreateVm-canonical.ubuntu-24_04-lts-server-20241021151352 | Overview >
InsightScape-VM2
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Connect
Networking
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Automation
Help
Connect
Start
Restart
Stop
Hibernate
Capture
Delete
Refresh
Open in mobile
Feedback
CLI / PS
Essentials
JSON View
Resource group (move) : InsightScape-RG
Status : Running
Location : West US 2
Subscription (move) : Free Trial
Subscription ID : [redacted]
Tags (edit) : Add tags
Operating system : Linux (ubuntu 24.04)
Size : Standard B1s (1 vcpu, 1 GiB memory)
Public IP address : 52.148.174.236
Virtual network/subnet : InsightScape-VNet/VM2-Subnet
DNS name : Not configured
Health state : -
Time created : 10/21/2024, 9:49 AM UTC
Properties
Monitoring
Capabilities (7)
Recommendations
Tutorials
Virtual machine
Computer name InsightScape-VM2
Operating system Linux (ubuntu 24.04)
VM generation V2
VM architecture x64
Agent status Ready
Agent version 2.11.1.12
Hibernation Disabled
Host group -
Host -
Proximity placement group -
Colocation status N/A
Capacity reservation group -
Disk controller type SCSI
Azure Spot
Azure Spot -
Azure Spot eviction policy -
Availability + scaling
Availability zone (edit) -
Availability set -
Scale Set -
Security
Security type Standard
Health monitoring
Health monitoring Not enabled
Networking
Public IP address 52.148.174.236 (Network interface insightscape-vm2710)
Public IP address (IPv6) -
Private IP address 10.1.2.4
Private IP address (IPv6) -
Virtual network/subnet InsightScape-VNet/VM2-Subnet
DNS name Configure
Size
Size Standard B1s
vCPUs 1
RAM 1 GiB
Source image details
Source image publisher canonical
Source image offer ubuntu-24_04-lts
Source image plan server
Disk
OS disk InsightScape-VM2_OsDisk_1_b0f27507f1ec47869d6b1272fc041a0
Encryption at host Disabled
Azure disk encryption Not enabled
Ephemeral OS disk N/A
Data disks 0
Auto-shutdown
Auto-shutdown Not enabled
Scheduled shutdown -


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home >
Network security groups
Default Directory (punavrawat777gmail.onmicrosoft.com)
Create
Manage view
Refresh
Export to CSV
Open query
Assign tags
Filter for any field...
Subscription equals all
Resource group equals all
Location equals all
Add filter
Showing 1 to 2 of 2 records.
No grouping
List view
Name
Resource group
Location
Subscription
Flow log
InsightScape-VM1-nsg
InsightScape-RG
West US 2
Free Trial
InsightScapeVM2nsg120
InsightScape-RG
West US 2
Free Trial
< Previous
Page 1 of 1
Next >
Give feedback


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Network security groups > InsightScape-VM1-nsg
Network security g...
InsightScape-VM1-nsg | Inbound security rules
Network security group
Create
Manage view
Filter for any field...
Name
InsightScape-VM1-nsg
InsightScapeVM2nsg120
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Monitoring
Automation
Help
Add
Hide default rules
Refresh
Delete
Give feedback
Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and d
rules that have a higher priority. Learn more
Filter by name
Port == all
Protocol == all
Source == all
Destination == all
Action == all
Priority
Name
Port
Protocol
Source
300
RDP
3389
TCP
Any
320
HTTPS
443
TCP
Any
65000
AllowVnetInBound
Any
Any
VirtualNetwork
65001
AllowAzureLoadBalancerInBound
Any
Any
AzureLoadBalancer
65500
DenyAllInBound
Any
Any
Any
Page 1 of 1
Add inbound security rule
InsightScape-VM1-nsg
Source
Any
Source port ranges *
*
Destination
Any
Service
HTTP
Destination port ranges
80
Protocol
Any
TCP
UDP
ICMPv4
Action
Allow
Deny
Priority *
300
Name *
HTTP
Description
Add
Cancel
Give feedback


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Network security groups > InsightScape-VM1-nsg
Network security g...
InsightScape-VM1-nsg | Inbound security rules
Network security group
Create
Manage view
Filter for any field...
Name
InsightScape-VM1-nsg
InsightScapeVM2nsg120
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Monitoring
Automation
Help
Add
Hide default rules
Refresh
Delete
Give feedback
Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with
rules that have a higher priority. Learn more
Filter by name
Port == all
Protocol == all
Source == all
Destination == all
Action == all
Priority
Name
Port
Protocol
Source
Destination
Action
300
RDP
3389
TCP
Any
Any
Allow
320
HTTPS
443
TCP
Any
Any
Allow
330
HTTP
80
TCP
Any
Any
Allow
65000
AllowVnetInBound
Any
Any
VirtualNetwork
VirtualNetwork
Allow
65001
AllowAzureLoadBalancerInBound
Any
Any
AzureLoadBalancer
Any
Allow
65500
DenyAllInBound
Any
Any
Any
Any
Deny
Page 1 of 1
Created security rule
Successfully created security rule 'HTTP'.


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Network security groups >
Network security g...
Create
Manage view
Filter for any field...
Name
InsightScape-VM1-nsg
InsightScapeVM2nsg120
InsightScapeVM2nsg120
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
Automation
Help
Essentials
JSON View
Resource group (move) : InsightScape-RG
Location : West US 2
Subscription (move) : Free Trial
Subscription ID : d9d3d784-6d8b-4d88-9312-d58a0d0a9a50
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
300 SSH 22 TCP Any Any Allow
320 HTTPS 443 TCP Any Any Allow
340 HTTP 80 TCP Any 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
65000 AllowVnetOutBound Any Any VirtualNetwork VirtualNetwork Allow
65001 AllowInternetOutBound Any Any Any Internet Allow
65500 DenyAllOutBound Any Any Any Any Deny
Page 1 of 1

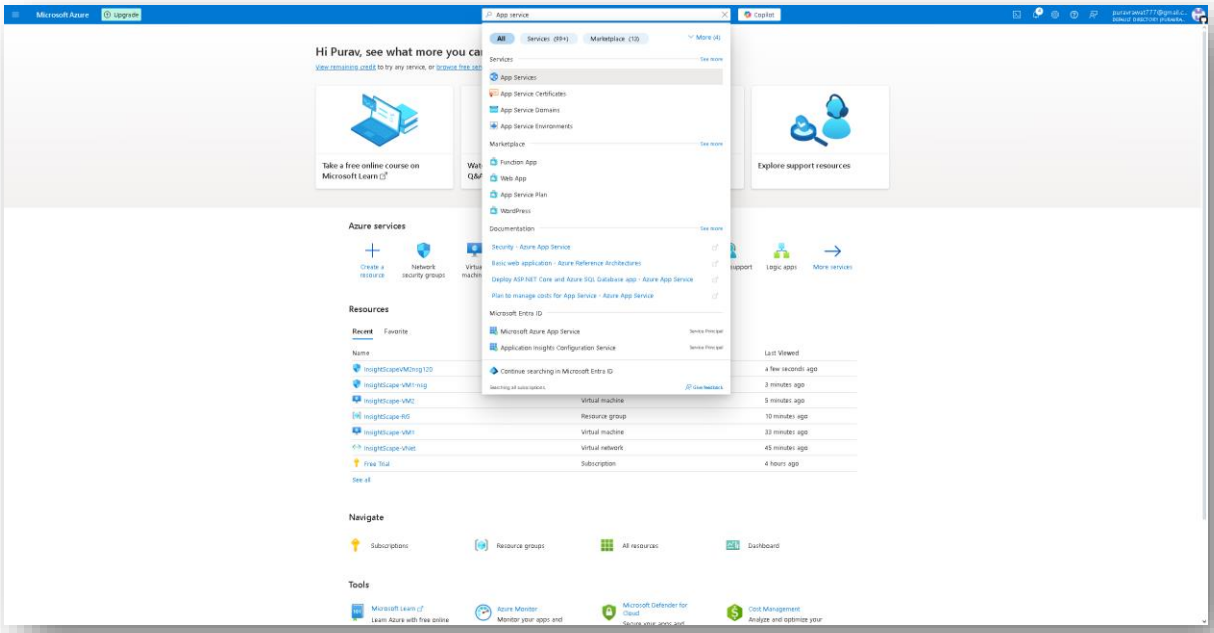
c) Web App

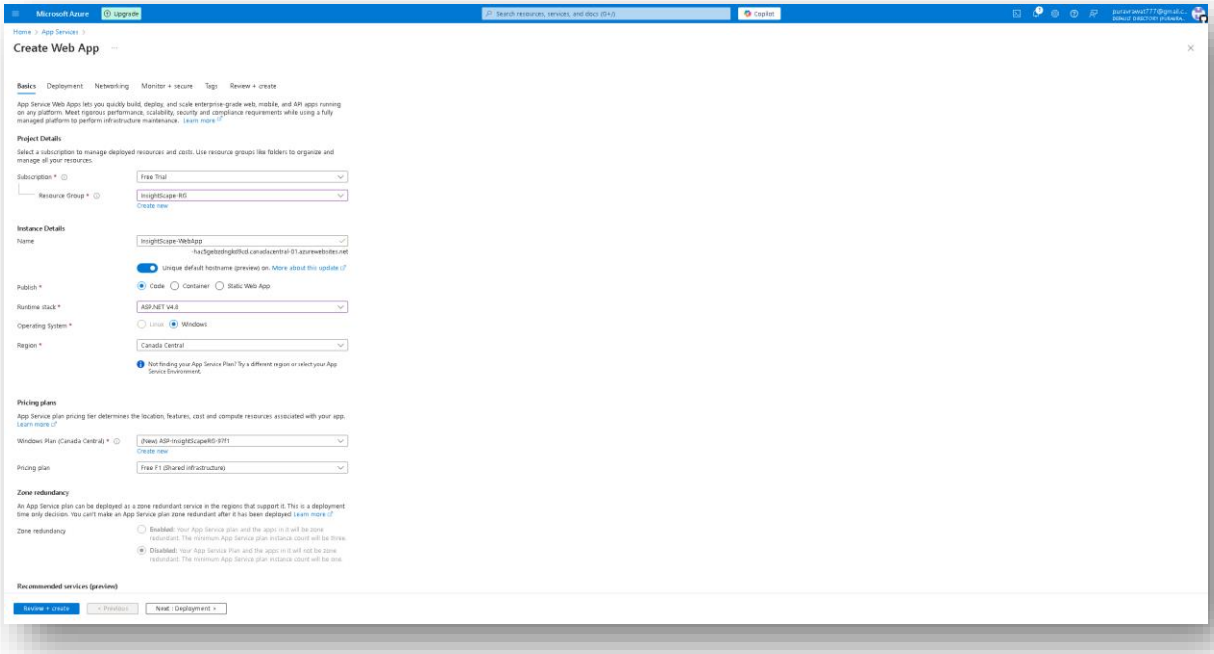
After the VM setup, it was time to create the Web App:

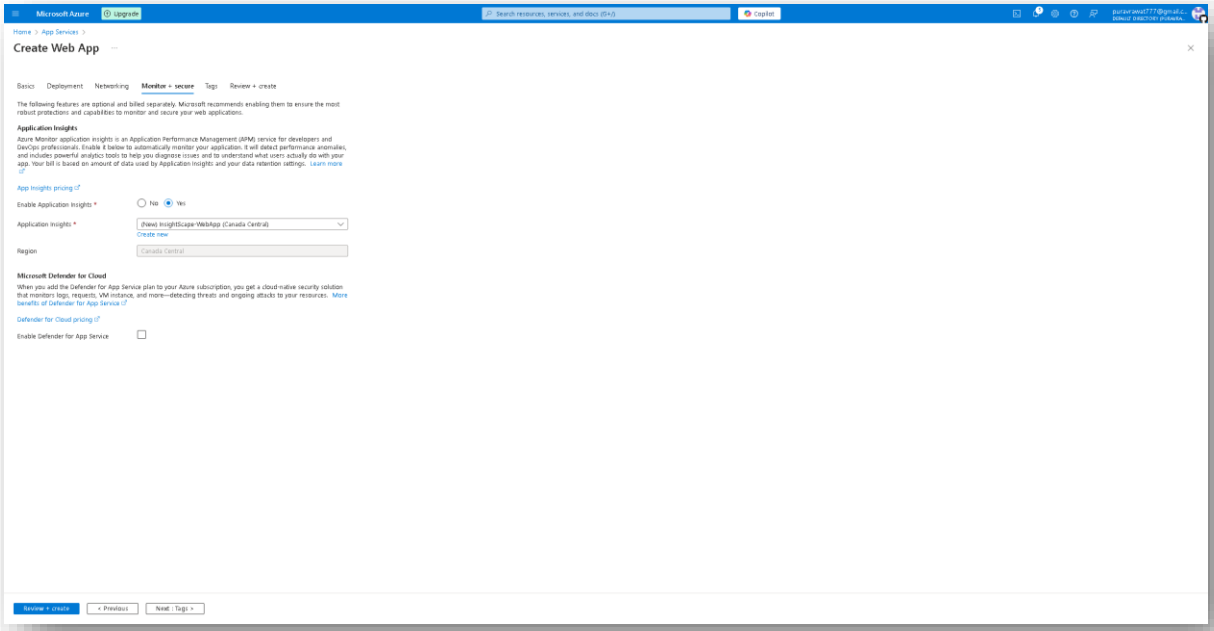
1. Web App Creation:
    - Resource Group: InsightScape-RG
    - Name: InsightScape-WebApp
    - Publish: Code
    - Runtime Stack: ASP.NET V4.8
    - Operating System: Windows
    - App Service Plan: InsightScape-Plan (B1:1)
2. Monitor + Secure Tab:
    - Enable Application Insights: Yes
    - Application Insights: Created a new instance named InsightScape-WebApp (Canada Central)
3. Deployment of Sample App:
    - Forked an ASP.NET sample app from GitHub ("MyDemoApp" repository).
    - Deployment:
        - Accessed the Deployment Centre tab in the InsightScape-WebApp.
        - Selected GitHub as the source.
        - Signed in with GitHub credentials.
        - Selected "MyDemoApp" as the repository and "main" as the branch.
        - Saved the configuration.
    - Verified successful deployment by checking the deployment logs and the default domain URL

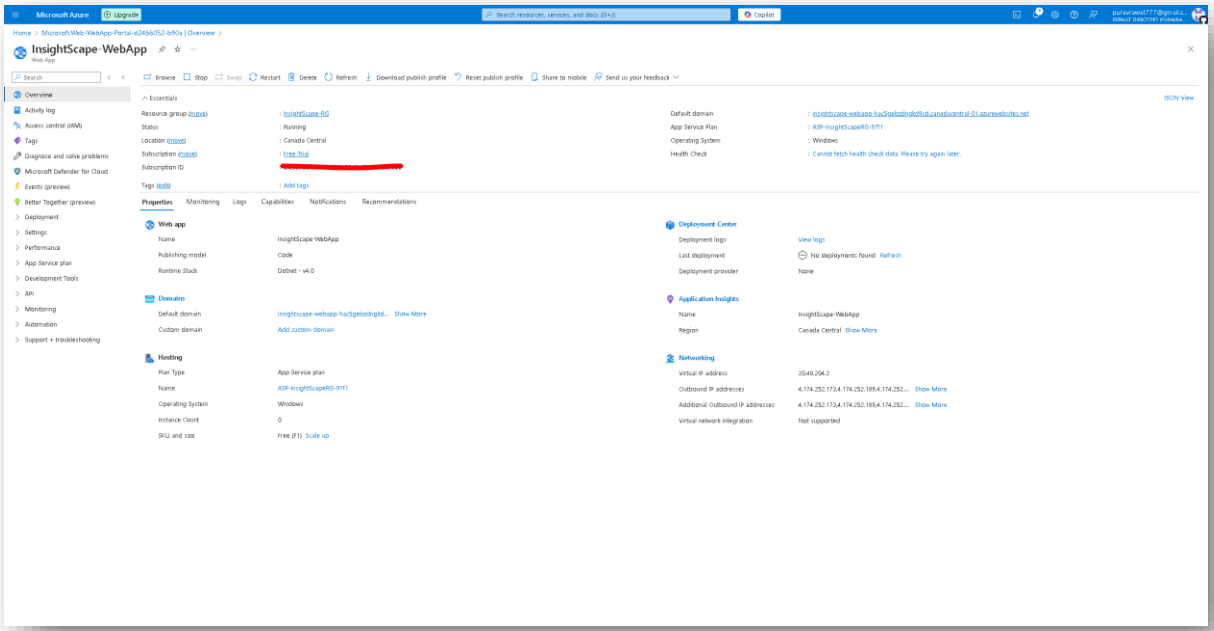
Quick Note: During the project, I deployed my Web App in the Canada Central region, as deployment in the West US 2 region was unavailable due to limitations associated with my Free Trial subscription. Certain regions restrict resource deployment for Free Tier accounts, which is why I opted for Canada Central as an alternative.

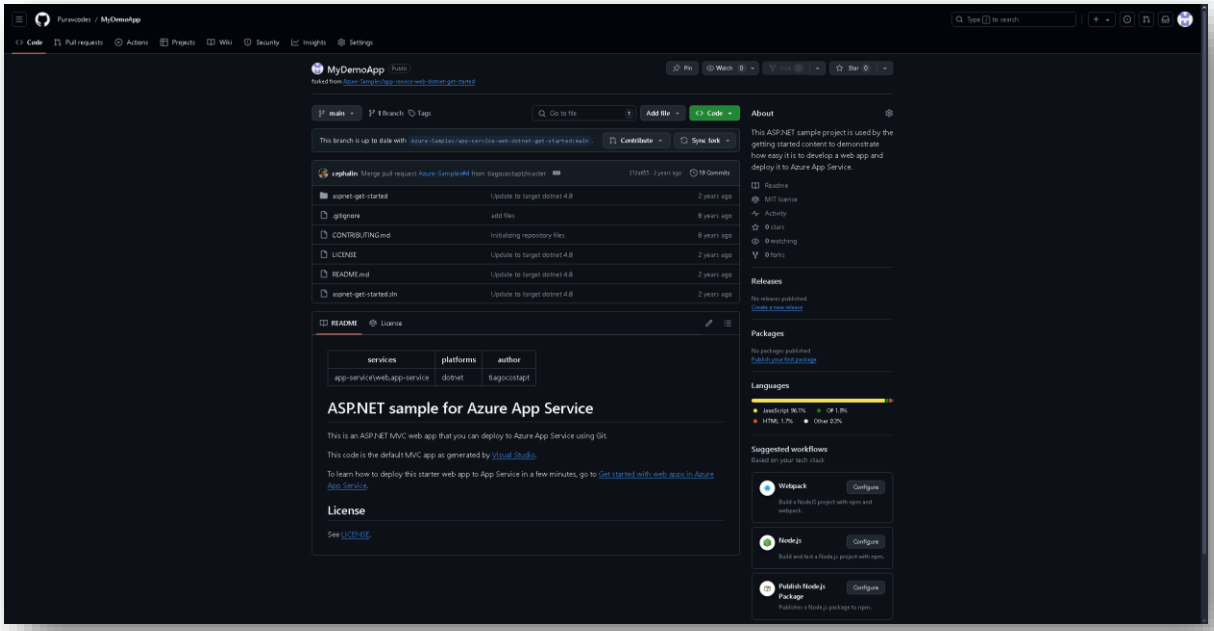
Screenshots -

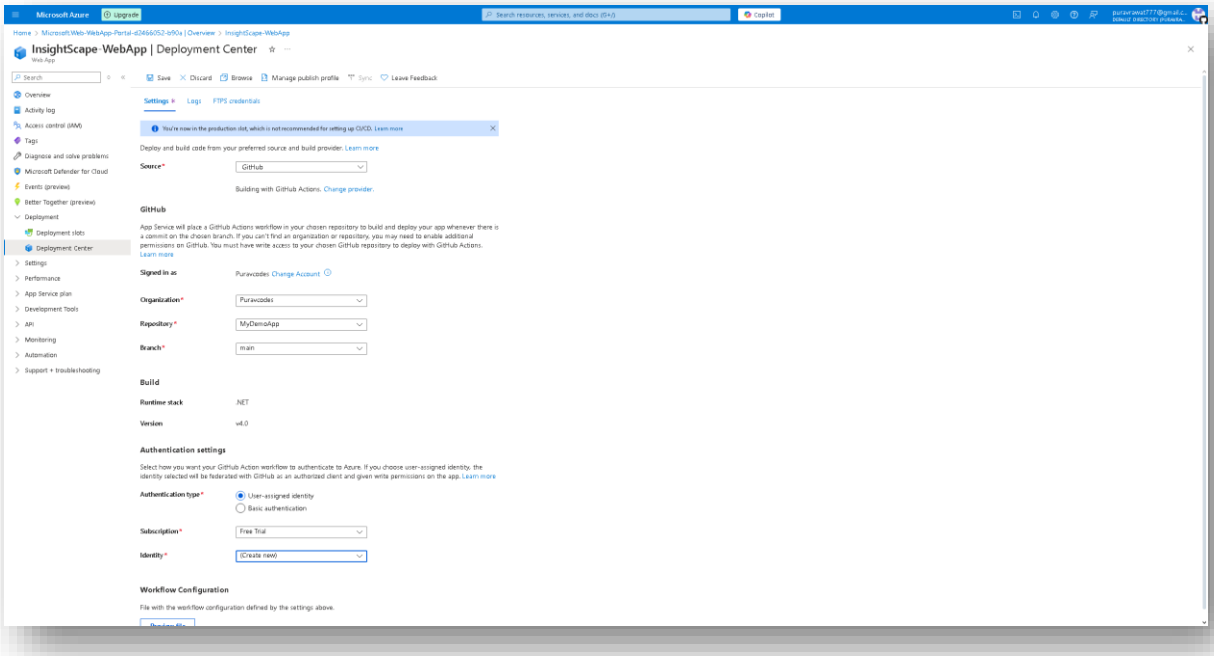


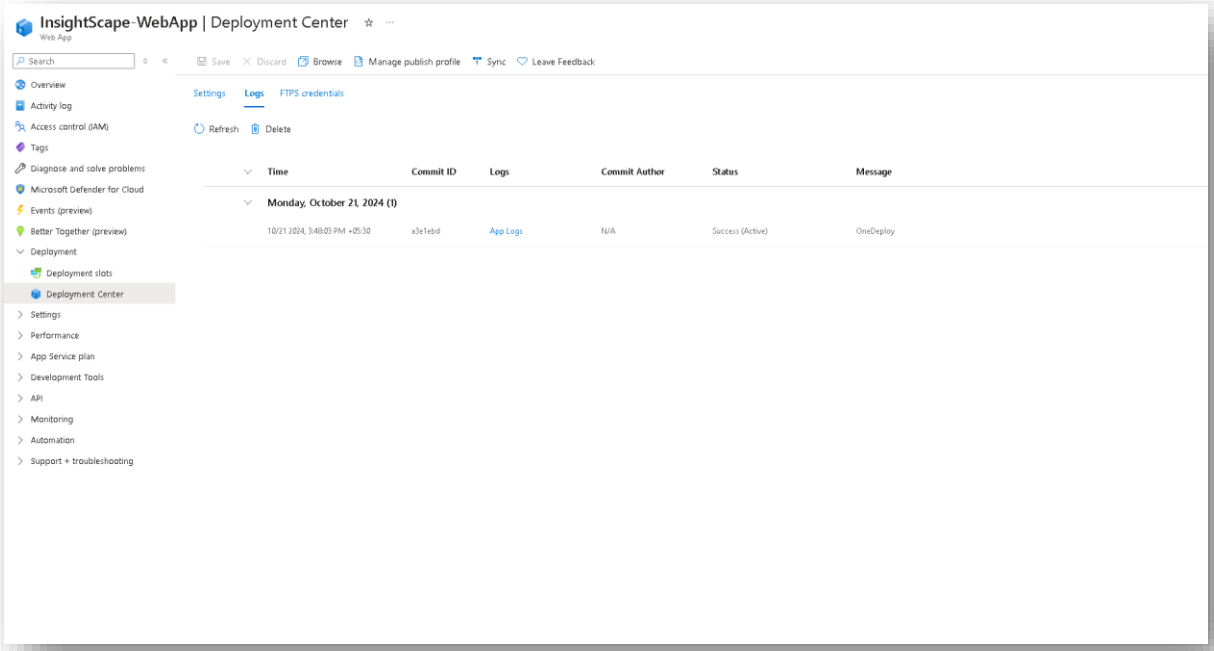


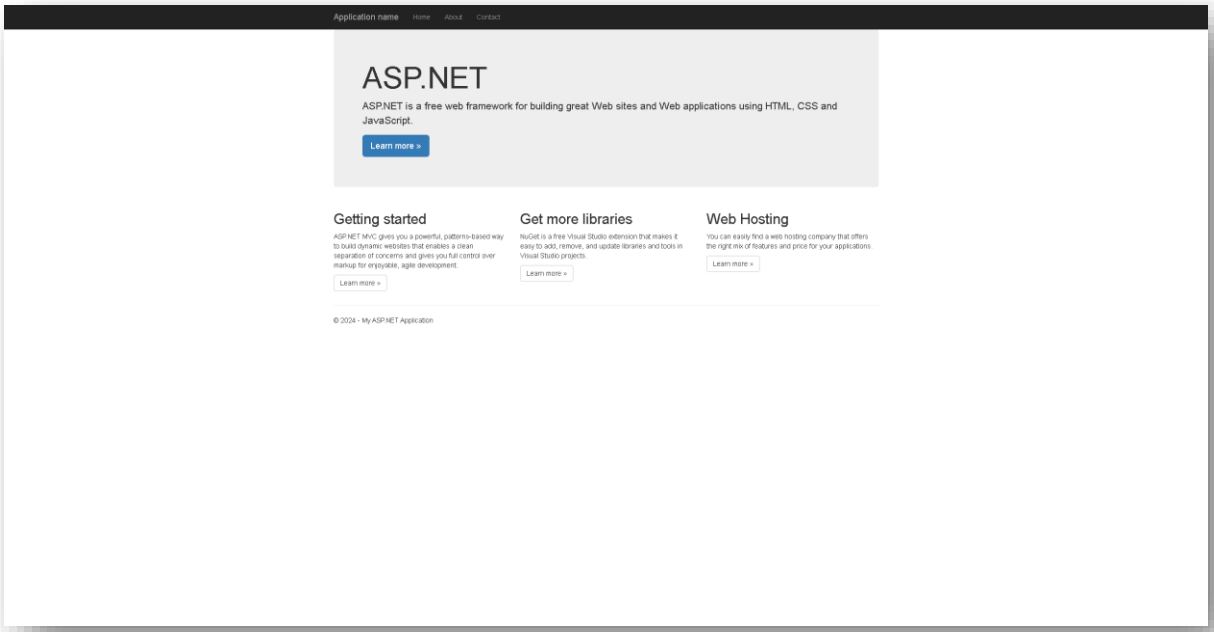

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > App Services >
Create Web App
Basics
Deployment
Networking
Monitor + secure
Tags
Review + create
The following features are optional and billed separately. Microsoft recommends enabling them to ensure the most robust protections and capabilities to monitor and secure your web applications.
Application Insights
Azure Monitor application insights is an Application Performance Management (APM) service for developers and DevOps professionals. Enable it below to automatically monitor your application. It will detect performance anomalies, and includes powerful analytics tools to help you diagnose issues and to understand what users actually do with your app. Your bill is based on amount of data used by Application Insights and your data retention settings. Learn more
App Insights pricing
Enable Application Insights *
No
Yes
Application Insights *
(New) InsightScape-WebApp (Canada Central)
Create new
Region
Canada Central
Microsoft Defender for Cloud
When you add the Defender for App Service plan to your Azure subscription, you get a cloud-native security solution that monitors logs, requests, VM instance, and more—detecting threats and ongoing attacks to your resources. More benefits of Defender for App Service
Defender for Cloud pricing
Enable Defender for App Service
Review + create
< Previous
Next : Tags >


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft.Web-WebApp-Portal-d2466052-b90a | Overview >
InsightScape-WebApp
Web App
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Microsoft Defender for Cloud
Events (preview)
Better Together (preview)
Deployment
Settings
Performance
App Service plan
Development Tools
API
Monitoring
Automation
Support + troubleshooting
Browse
Stop
Swap
Restart
Delete
Refresh
Download publish profile
Reset publish profile
Share to mobile
Send us your feedback
Essentials
JSON View
Resource group (move) : InsightScape-RG
Status : Running
Location (move) : Canada Central
Subscription (move) : Free Trial
Subscription ID
Tags (edit) : Add tags
Default domain : insightscape-webapp-hac5gebzdngkd9cd.canadacentral-01.azurewebsites.net
App Service Plan : ASP-InsightScapeRG-97f1
Operating System : Windows
Health Check : Cannot fetch health check data. Please try again later.
Properties
Monitoring
Logs
Capabilities
Notifications
Recommendations
Web app
Name InsightScape-WebApp
Publishing model Code
Runtime Stack Dotnet - v4.0
Deployment Center
Deployment logs View logs
Last deployment No deployments found Refresh
Deployment provider None
Domains
Default domain insightscape-webapp-hac5gebzdngkd... Show More
Custom domain Add custom domain
Application Insights
Name InsightScape-WebApp
Region Canada Central Show More
Hosting
Plan Type App Service plan
Name ASP-InsightScapeRG-97f1
Operating System Windows
Instance Count 0
SKU and size Free (F1) Scale up
Networking
Virtual IP address 20.48.204.2
Outbound IP addresses 4.174.252.173,4.174.252.189,4.174.252.... Show More
Additional Outbound IP addresses 4.174.252.173,4.174.252.189,4.174.252.... Show More
Virtual network integration Not supported


Puravcodes / MyDemoApp
Code
Pull requests
Actions
Projects
Wiki
Security
Insights
Settings
MyDemoApp
Public
Forked from Azure-Samples/app-service-web-dotnet-get-started
Pin
Watch 0
Star 0
main
1 Branch
0 Tags
Go to file
Add file
Code
This branch is up to date with Azure-Samples/app-service-web-dotnet-get-started:main.
Contribute
Sync fork
cephalin Merge pull request Azure-Samples#4 from tiagocostajpt/master
21b4851 · 2 years ago
10 Commits
aspnet-get-started
Update to target dotnet 4.8
2 years ago
.gitignore
add files
8 years ago
CONTRIBUTING.md
Initializing repository files.
8 years ago
LICENSE
Update to target dotnet 4.8
2 years ago
README.md
Update to target dotnet 4.8
2 years ago
aspnet-get-started.sln
Update to target dotnet 4.8
2 years ago
README
License
services
platforms
author
app-service\web.app-service
dotnet
tiagocostajpt
ASP.NET sample for Azure App Service
This is an ASP.NET MVC web app that you can deploy to Azure App Service using Git.
This code is the default MVC app as generated by Visual Studio.
To learn how to deploy this starter web app to App Service in a few minutes, go to Get started with web apps in Azure App Service.
License
See LICENSE.
About
This ASP.NET sample project is used by the getting started content to demonstrate how easy it is to develop a web app and deploy it to Azure App Service.
Readme
MIT license
Activity
0 stars
0 watching
0 forks
Releases
No releases published
Create a new release
Packages
No packages published
Publish your first package
Languages
JavaScript 96.9%
C# 1.9%
HTML 1.1%
Other 0.1%
Suggested workflows
Based on your tech stack
Webpack
Configure
Node.js
Configure
Publish Node.js Package
Configure


Microsoft Azure
Upgrade
Copilot
Home > Microsoft.Web-WebApp-Portal-d2466052-b90a | Overview > InsightScape-WebApp
InsightScape-WebApp | Deployment Center
Web App
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Microsoft Defender for Cloud
Events (preview)
Better Together (preview)
Deployment
Deployment slots
Deployment Center
Settings
Performance
App Service plan
Development Tools
API
Monitoring
Automation
Support + troubleshooting
Save
Discard
Browse
Manage publish profile
Sync
Leave Feedback
Settings
Logs
FTPS credentials
You're now in the production slot, which is not recommended for setting up CI/CD. Learn more
Deploy and build code from your preferred source and build provider. Learn more
Source*
GitHub
Building with GitHub Actions. Change provider.
GitHub
App Service will place a GitHub Actions workflow in your chosen repository to build and deploy your app whenever there is a commit on the chosen branch. If you can't find an organization or repository, you may need to enable additional permissions on GitHub. You must have write access to your chosen GitHub repository to deploy with GitHub Actions. Learn more
Signed in as
Puravcodes Change Account
Organization*
Puravcodes
Repository*
MyDemoApp
Branch*
main
Build
Runtime stack
.NET
Version
v6.0
Authentication settings
Select how you want your GitHub Action workflow to authenticate to Azure. If you choose user-assigned identity, the identity selected will be federated with GitHub as an authorized client and given write permissions on the app. Learn more
Authentication type*
User-assigned identity
Basic authentication
Subscription*
Free Trial
Identity*
(Create new)
Workflow Configuration
File with the workflow configuration defined by the settings above.


InsightScape-WebApp | Deployment Center
Web App
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Microsoft Defender for Cloud
Events (preview)
Better Together (preview)
Deployment
Deployment slots
Deployment Center
Settings
Performance
App Service plan
Development Tools
API
Monitoring
Automation
Support + troubleshooting
Save
Discard
Browse
Manage publish profile
Sync
Leave Feedback
Settings
Logs
FTPS credentials
Refresh
Delete
Time
Commit ID
Logs
Commit Author
Status
Message
Monday, October 21, 2024 (1)
10/21 2024, 3:48:03 PM +05:30
a3e1ebd
App Logs
N/A
Success (Active)
OneDeploy


Application name
Home
About
Contact
ASP.NET
ASP.NET is a free web framework for building great Web sites and Web applications using HTML, CSS and JavaScript.
Learn more »
Getting started
ASP.NET MVC gives you a powerful, patterns-based way to build dynamic websites that enables a clean separation of concerns and gives you full control over markup for enjoyable, agile development.
Learn more »
Get more libraries
NuGet is a free Visual Studio extension that makes it easy to add, remove, and update libraries and tools in Visual Studio projects.
Learn more »
Web Hosting
You can easily find a web hosting company that offers the right mix of features and price for your applications.
Learn more »
© 2024 - My ASP.NET Application

d) Blob Storage and Logic App

After setting up the Web App, it was time to create the Blob Storage and Logic App.

1. Storage Account Creation:

- Name: insightscapestorage
- Resource Group: InsightScape-RG
- Region:West US 2
- Primary Service: Azure Blob Storage or Azure Data Lake Storage Gen 2
- Performance: Standard o Redundancy: Locally-redundant storage (LRS)
- Account Kind: StorageV2 (general purpose v2)
- Other Configurations: Used default settings for remaining configurations

After setting these configurations, I clicked "Create" to deploy the storage account.

Once the deployment was successful, I proceeded to:

- Navigate to the Containers tab under Data Storage in the insightscapestorage storage account.
- Create a container named "files".

2. Logic App Setup:

- Hosting Option: Consumption (Multi-tenant)
- Resource Group: InsightScape-RG
- Name: InsightScape-LogicApp
- Region: West US 2
- Enable Log Analytics: No

After setting the configurations above, I clicked on "Review + Create". Once the Logic App was successfully deployed, I followed these steps:

- Trigger Setup in Logic App Designer:
  - I accessed the Logic App Designer under the Development Tools in the InsightScape-LogicApp.
  - For the trigger, I selected "When a blob is added or modified (properties only) (V2)".
  - To authenticate the Logic App connection, I went to the Access keys of the insightscapestorage storage account and copied the access keys.
  - Create Connection in Trigger:
    - Connection Name: InsightScapeBlobConnection
    - Authentication Type: Access Key
    - Azure Storage Account Name or Blob Endpoint: insightscapestorage
    - Azure Storage Account Access Key: (The access key from the storage account)

    After providing these details, I clicked on "Create new".

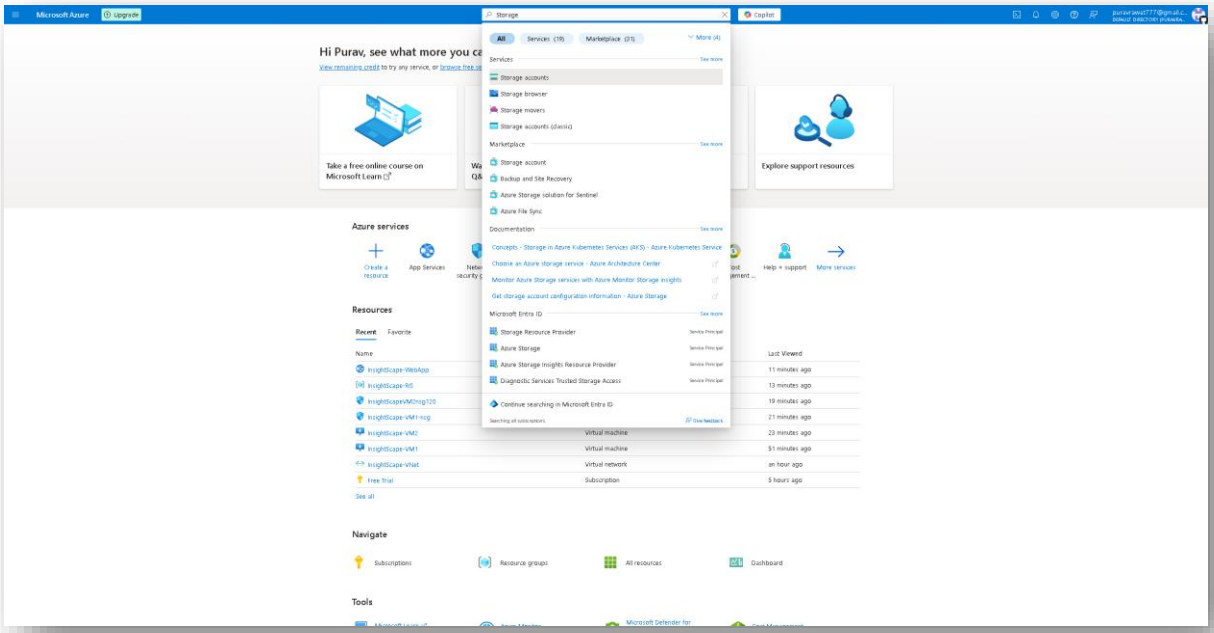
- Trigger Configurations:
  - Storage Account Name or Blob Endpoint: Use connection settings (insightscapestorage)
  - Container: /files
  - Number Of Blobs To Return: 10
- Action Setup After Trigger:
  - I created the same connection again with:
    - Connection Name: InsightScapeBlobConnection
    - Authentication Type: Access Key
    - Azure Storage Account Name or Blob Endpoint: insightscapestorage
    - Azure Storage Account Access Key: (The access key from the storage account)
  - Action: I chose "Get blob content (V2)".
- Action Parameters:
  - Storage Account Name or Blob Endpoint: Use connection settings (insightscapestorage)
  - Blob: List of Files Path (Dynamic Content)

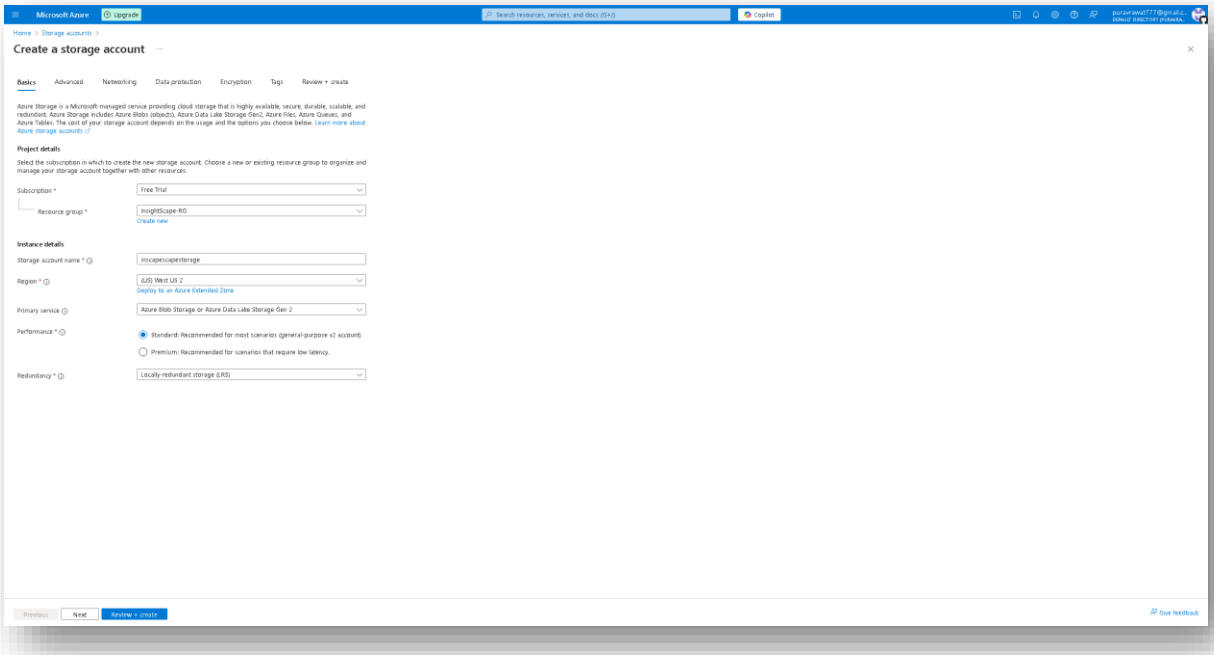
With this setup, the logic for the Logic App was ready.

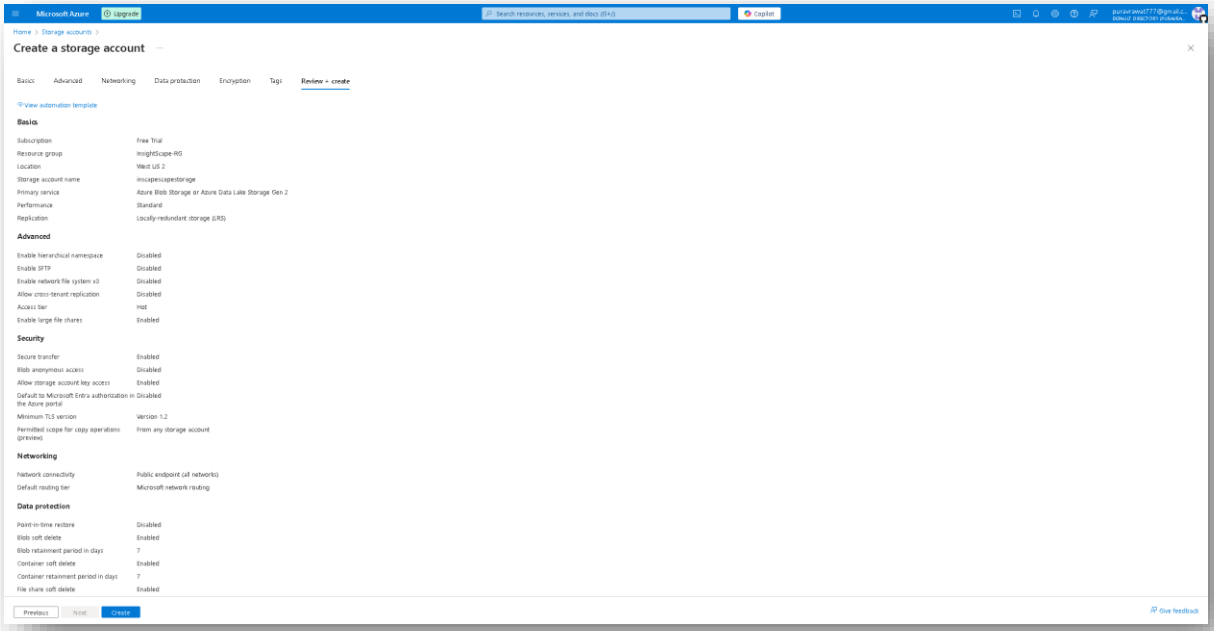
- Verification:
  - To verify that the Logic App was working perfectly, I uploaded two documents named "azure.png" and "SDLC.png" to the "files" container.
  - Immediately after, I went to the Run History tab in the InsightScapeLogicApp.
  - In the run history, I saw two successful runs. I clicked on one of the runs, and in the outputs, I could see the raw outputs of the blob content.

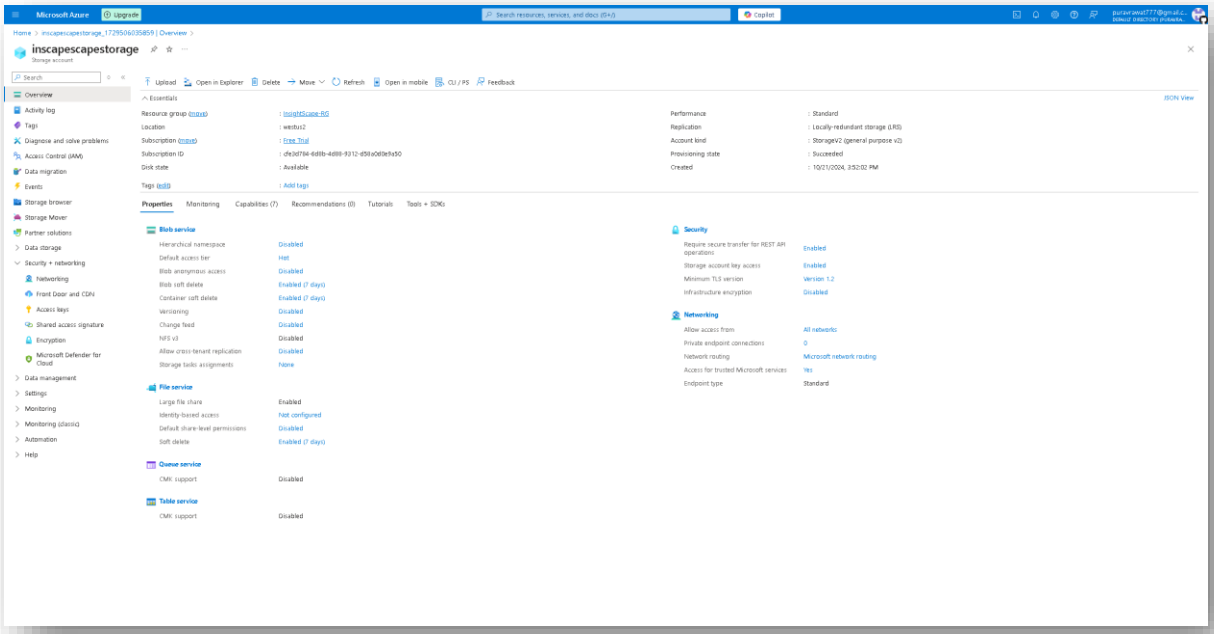
This entire process and its results confirmed that the Logic App was working successfully.

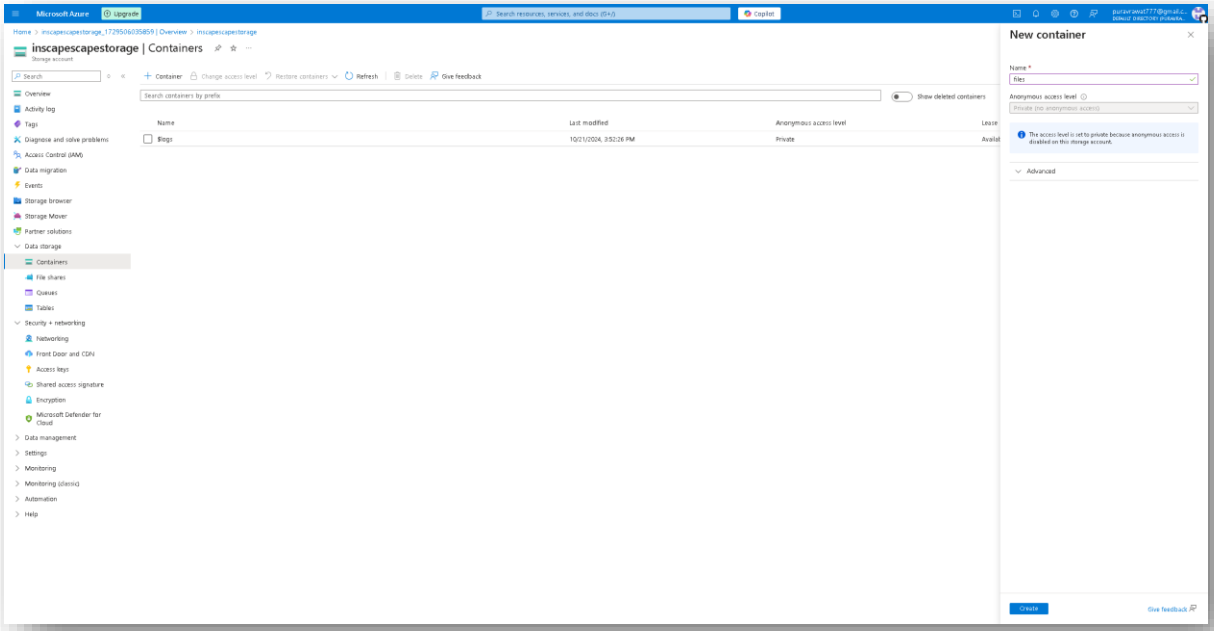
Screenshots –

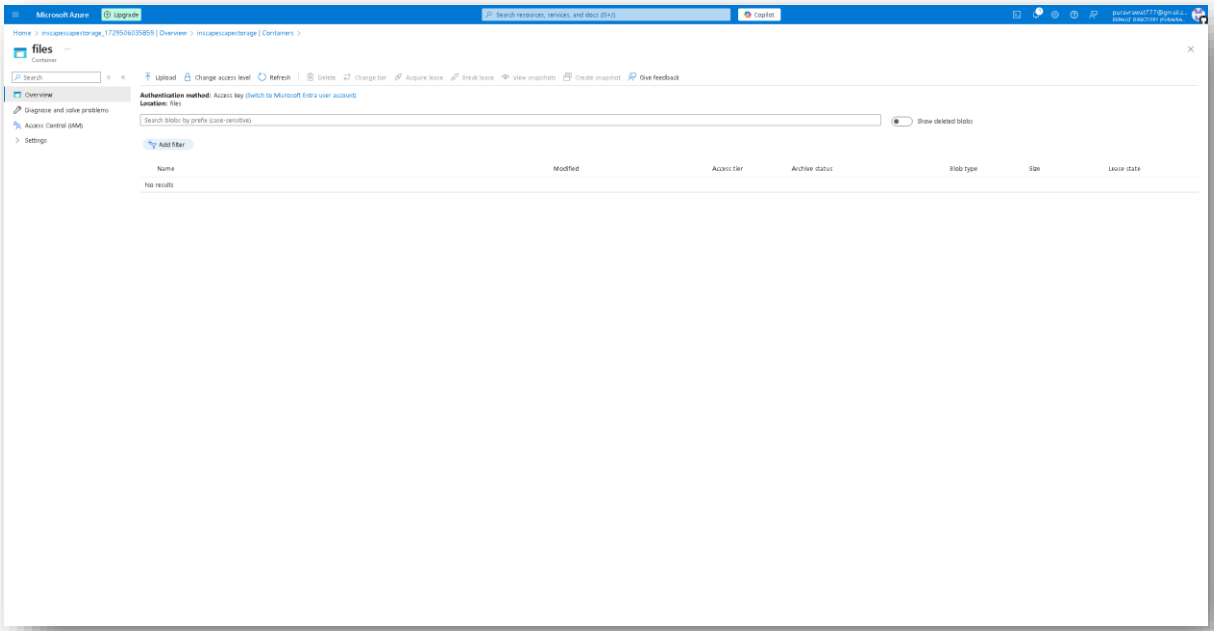


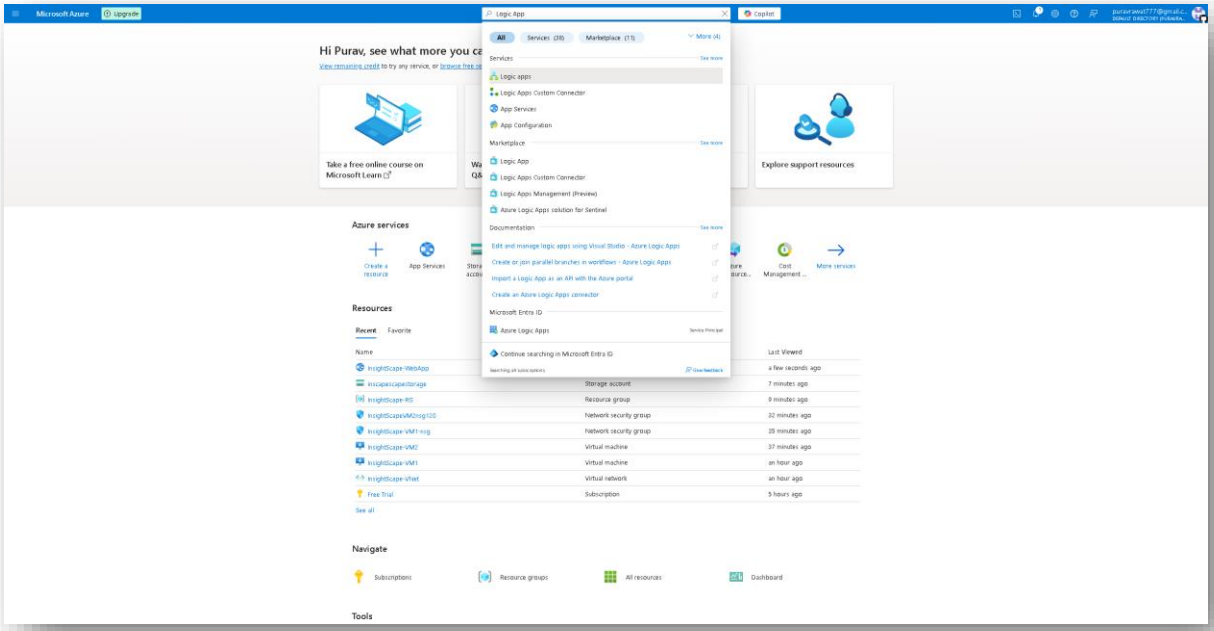


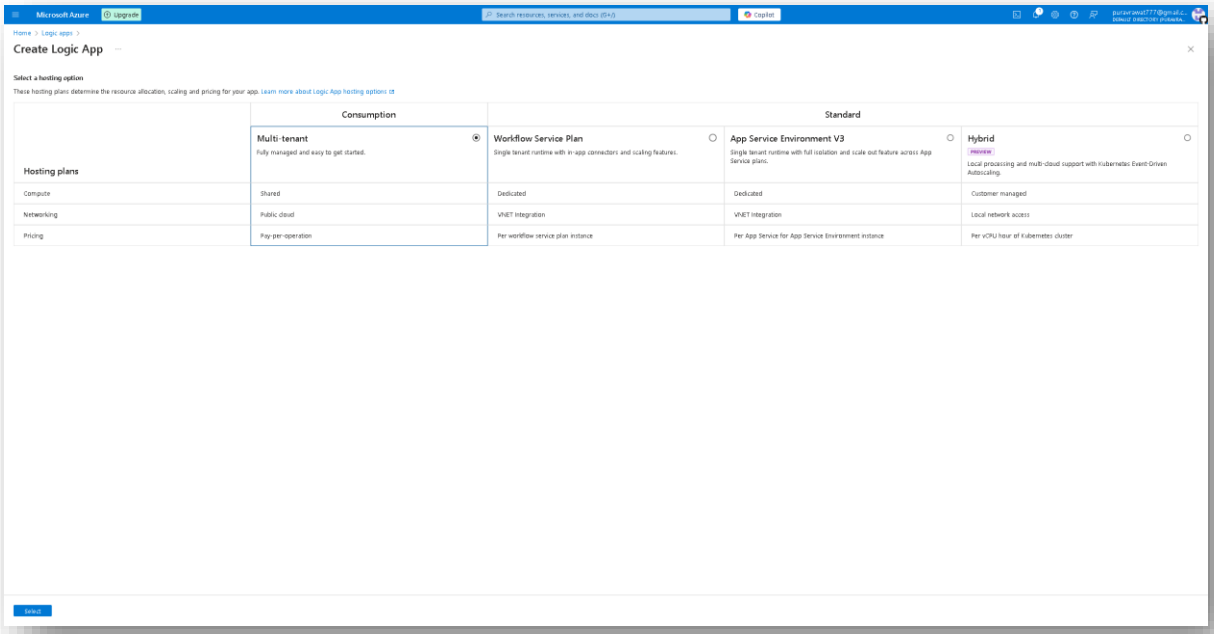

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Storage accounts >
Create a storage account
Basics
Advanced
Networking
Data protection
Encryption
Tags
Review + create
View automation template
Basics
Subscription Free Trial
Resource group InsightScape-RG
Location West US 2
Storage account name inscapescapestorage
Primary service Azure Blob Storage or Azure Data Lake Storage Gen 2
Performance Standard
Replication Locally-redundant storage (LRS)
Advanced
Enable hierarchical namespace Disabled
Enable SFTP Disabled
Enable network file system v3 Disabled
Allow cross-tenant replication Disabled
Access tier Hot
Enable large file shares Enabled
Security
Secure transfer Enabled
Blob anonymous access Disabled
Allow storage account key access Enabled
Default to Microsoft Entra authorization in the Azure portal Disabled
Minimum TLS version Version 1.2
Permitted scope for copy operations (preview) From any storage account
Networking
Network connectivity Public endpoint (all networks)
Default routing tier Microsoft network routing
Data protection
Point-in-time restore Disabled
Blob soft delete Enabled
Blob retainment period in days 7
Container soft delete Enabled
Container retainment period in days 7
File share soft delete Enabled
Previous
Next
Create
Give feedback

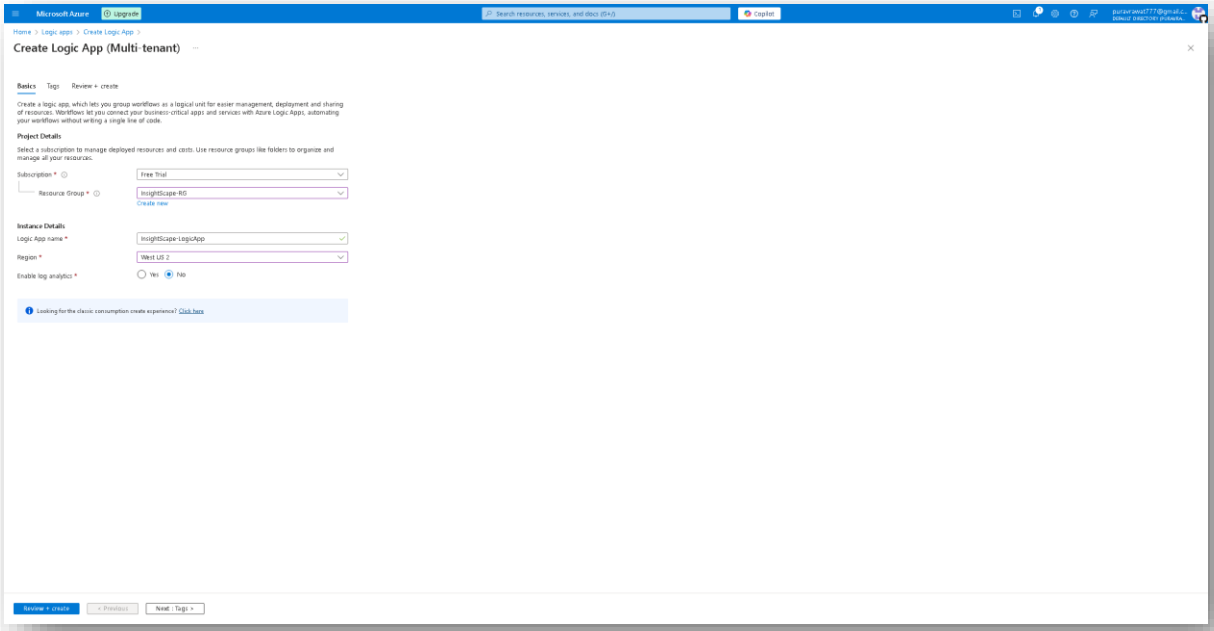

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > inscapescapestorage_1729506035859 | Overview >
inscapescapestorage
Storage account
Search
Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage browser
Storage Mover
Partner solutions
Data storage
Security + networking
Networking
Front Door and CDN
Access keys
Shared access signature
Encryption
Microsoft Defender for Cloud
Data management
Settings
Monitoring
Monitoring (classic)
Automation
Help
Upload
Open in Explorer
Delete
Move
Refresh
Open in mobile
CLI / PS
Feedback
Essentials
JSON View
Resource group (move) : InsightScape-RG
Location : westus2
Subscription (move) : Free Trial
Subscription ID : cfe3d784-6d8b-4d88-9312-d58a0d8e9a50
Disk state : Available
Tags (edit) : Add tags
Performance : Standard
Replication : Locally-redundant storage (LRS)
Account kind : StorageV2 (general purpose v2)
Provisioning state : Succeeded
Created : 10/21/2024, 3:52:02 PM
Properties
Monitoring
Capabilities (7)
Recommendations (0)
Tutorials
Tools + SDKs
Blob service
Hierarchical namespace Disabled
Default access tier Hot
Blob anonymous access Disabled
Blob soft delete Enabled (7 days)
Container soft delete Enabled (7 days)
Versioning Disabled
Change feed Disabled
NFS v3 Disabled
Allow cross-tenant replication Disabled
Storage tasks assignments None
File service
Large file share Enabled
Identity-based access Not configured
Default share-level permissions Disabled
Soft delete Enabled (7 days)
Queue service
CMK support Disabled
Table service
CMK support Disabled
Security
Require secure transfer for REST API operations Enabled
Storage account key access Enabled
Minimum TLS version Version 1.2
Infrastructure encryption Disabled
Networking
Allow access from All networks
Private endpoint connections 0
Network routing Microsoft network routing
Access for trusted Microsoft services Yes
Endpoint type Standard

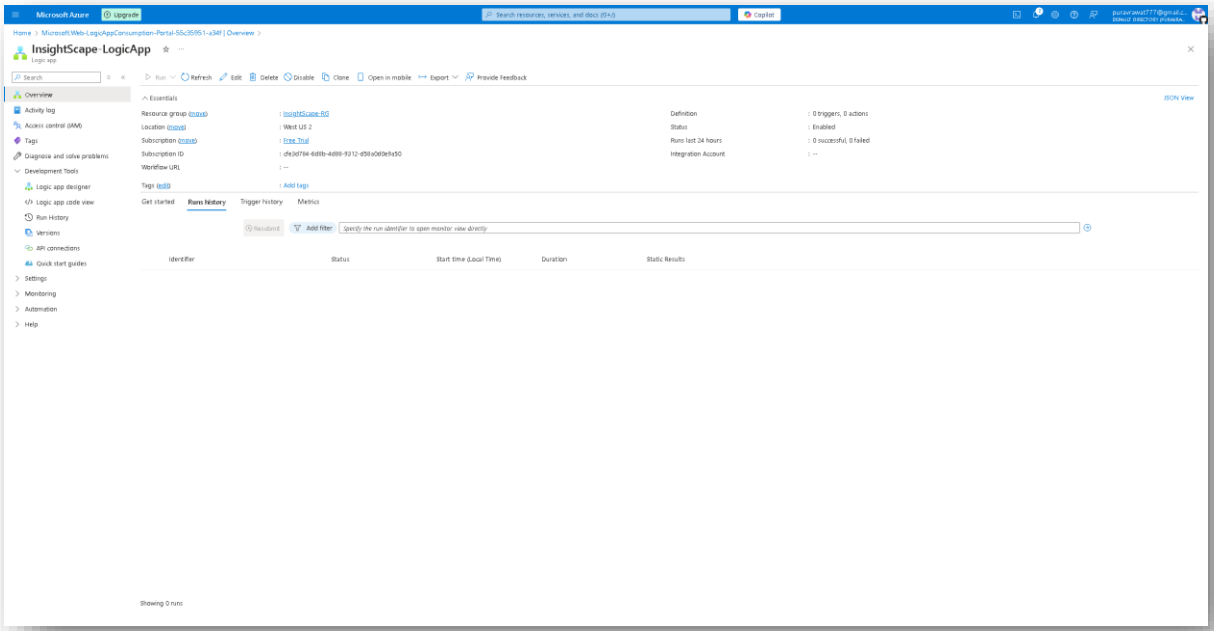

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > inscapecapestorage_1729506035859 | Overview > inscapecapestorage
inscapecapestorage | Containers
Storage account
Search
Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage browser
Storage Mover
Partner solutions
Data storage
Containers
File shares
Queues
Tables
Security + networking
Networking
Front Door and CDN
Access keys
Shared access signature
Encryption
Microsoft Defender for Cloud
Data management
Settings
Monitoring
Monitoring (classic)
Automation
Help
Container
Change access level
Restore containers
Refresh
Delete
Give feedback
Search containers by prefix
Show deleted containers
Name
Last modified
Anonymous access level
Lease
Blogs
10/21/2024, 3:52:26 PM
Private
New container
Name *
files
Anonymous access level
Private (no anonymous access)
The access level is set to private because anonymous access is disabled on this storage account.
Advanced
Create
Give feedback

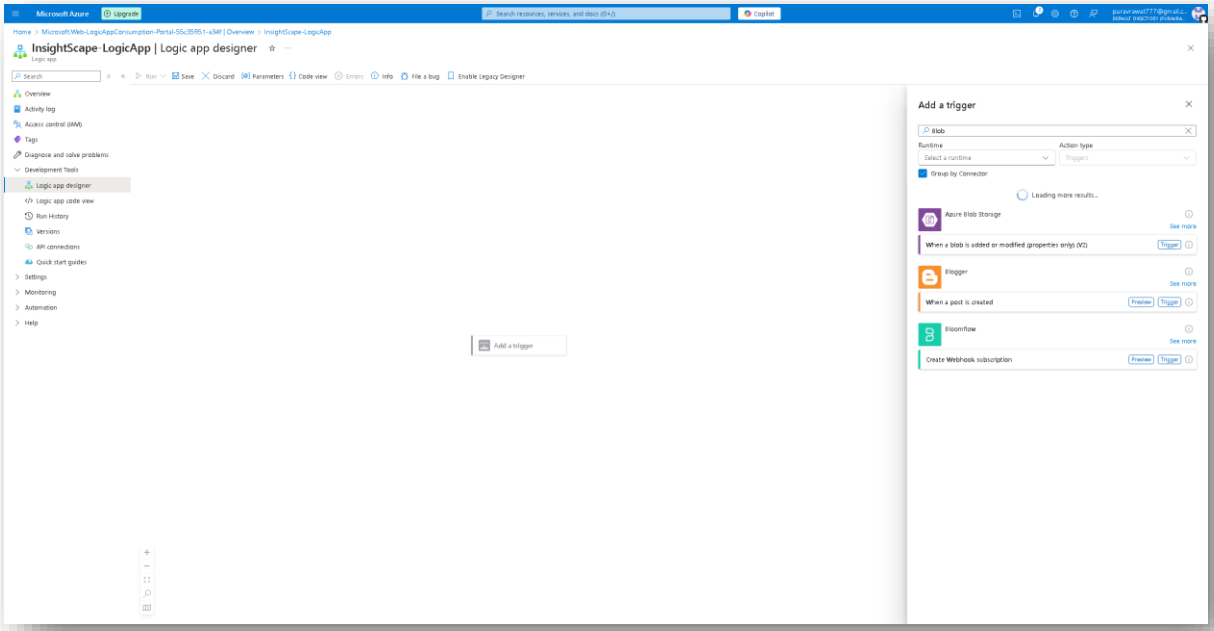

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > inscapecapestorage_1729506035859 | Overview > inscapecapestorage | Containers >
files
Container
Search
Overview
Diagnose and solve problems
Access Control (IAM)
Settings
Upload
Change access level
Refresh
Delete
Change tier
Acquire lease
Break lease
View snapshots
Create snapshot
Give feedback
Authentication method: Access key (Switch to Microsoft Entra user account)
Location: files
Search blobs by prefix (case-sensitive)
Show deleted blobs
Add filter
Name
Modified
Access tier
Archive status
Blob type
Size
Lease state
No results

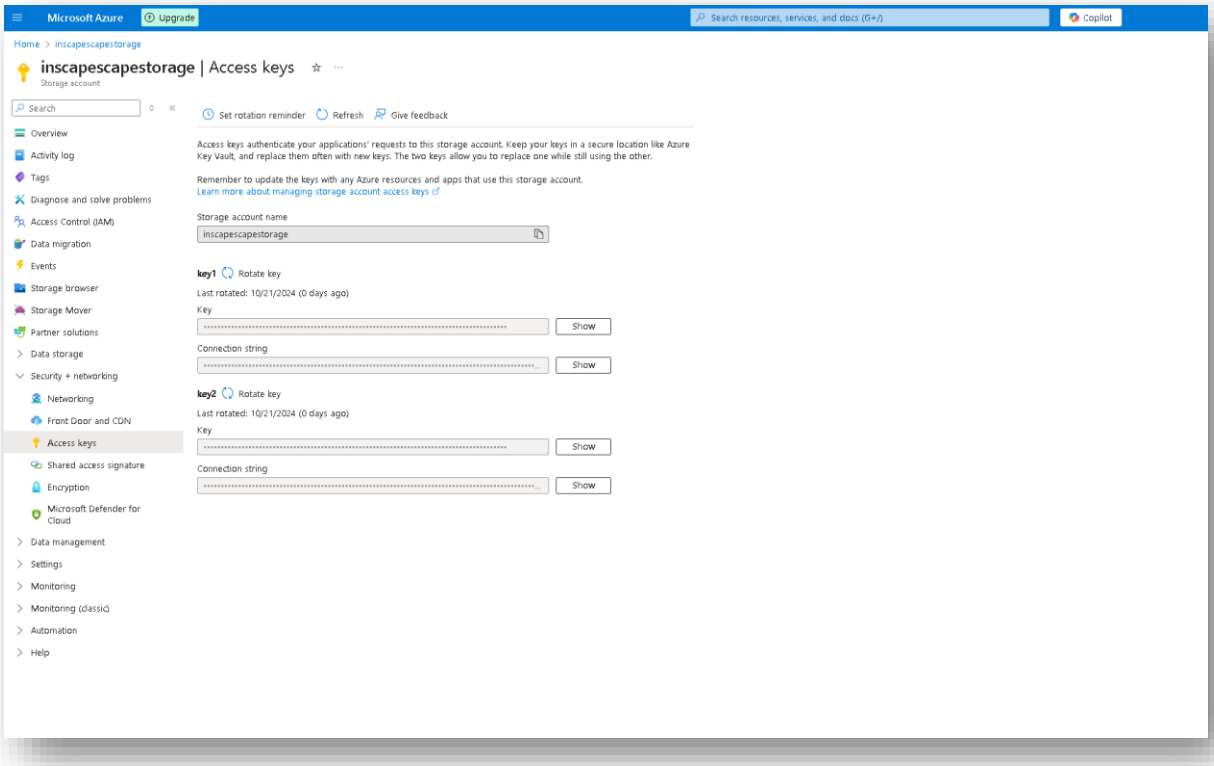

Microsoft Azure
Upgrade
Logic App
Copilot
Hi Purav, see what more you ca
Take a free online course on Microsoft Learn
Explore support resources
Azure services
Create a resource
App Services
Cost Management ...
More services
Resources
Recent
Favorite
Name
Last Viewed
Navigate
Subscriptions
Resource groups
All resources
Dashboard
Tools

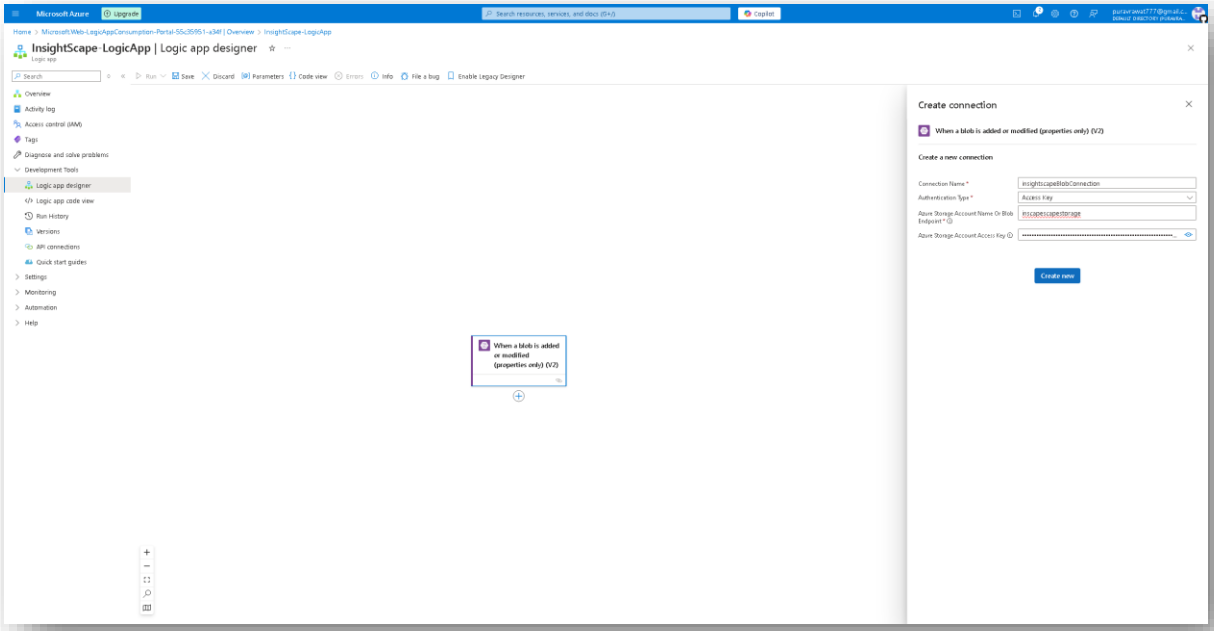

Microsoft Azure
Upgrade
Copilot
Home > Logic apps >
Create Logic App
Select a hosting option
These hosting plans determine the resource allocation, scaling and pricing for your app. Learn more about Logic App hosting options
Consumption
Standard
Hosting plans
Multi-tenant
Fully managed and easy to get started.
Workflow Service Plan
Single tenant runtime with in-app connectors and scaling features.
App Service Environment V3
Single tenant runtime with full isolation and scale out feature across App Service plans.
Hybrid
Preview
Local processing and multi-cloud support with Kubernetes Event-Driven Autoscaling.
Compute
Shared
Dedicated
Dedicated
Customer managed
Networking
Public cloud
VNET Integration
VNET Integration
Local network access
Pricing
Pay-per-operation
Per workflow service plan instance
Per App Service for App Service Environment instance
Per vCPU hour of Kubernetes cluster
Select

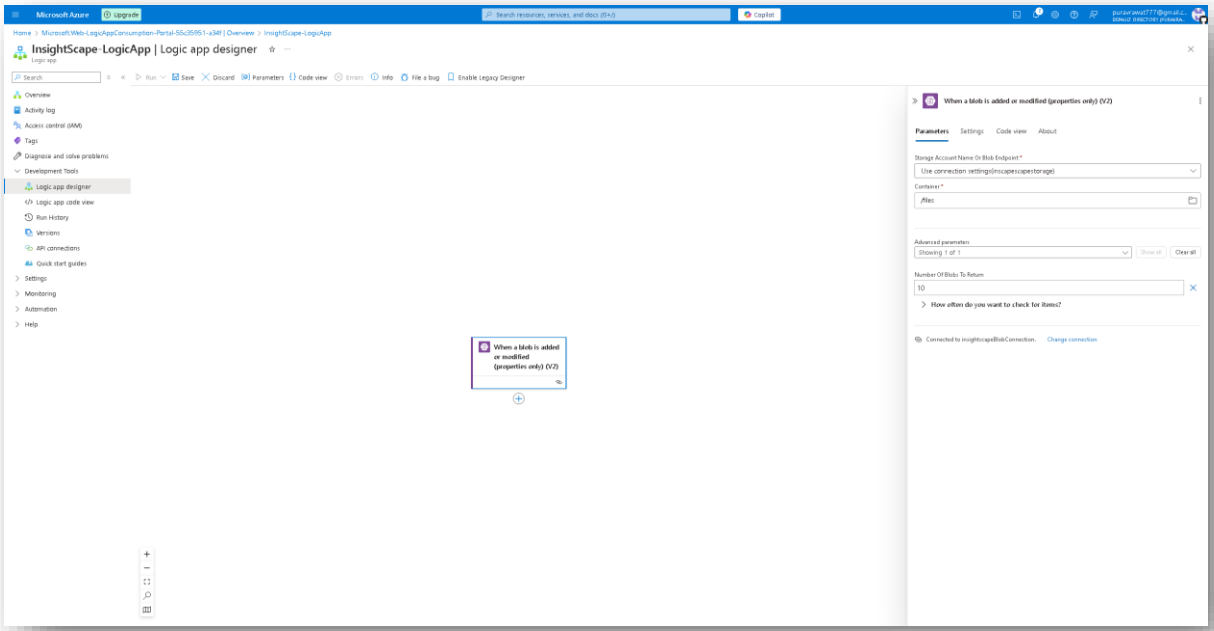

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Logic apps > Create Logic App >
Create Logic App (Multi-tenant)
Basics
Tags
Review + create
Create a logic app, which lets you group workflows as a logical unit for easier management, deployment and sharing of resources. Workflows let you connect your business-critical apps and services with Azure Logic Apps, automating your workflows without writing a single line of code.
Project Details
Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
Free Trial
Resource Group *
InsightScape-RG
Create new
Instance Details
Logic App name *
InsightScape-LogicApp
Region *
West US 2
Enable log analytics *
Yes
No
Looking for the classic consumption create experience? Click here
Review + create
< Previous
Next : Tags >

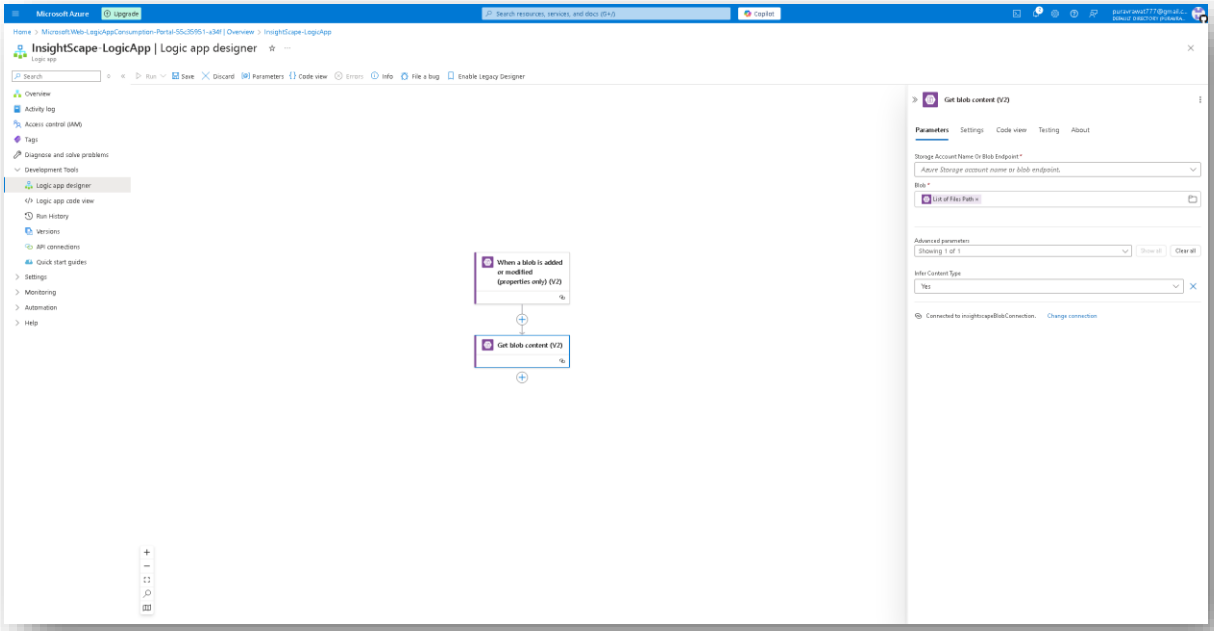

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft.Web-LogicAppConsumption-Portal-55c35951-a34f | Overview >
InsightScape-LogicApp
Logic app
Search
Run
Refresh
Edit
Delete
Disable
Clone
Open in mobile
Export
Provide Feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Run History
Versions
API connections
Quick start guides
Settings
Monitoring
Automation
Help
Essentials
JSON View
Resource group (move) : InsightScape-RG
Location (move) : West US 2
Subscription (move) : Free Trial
Subscription ID : cfe3d784-6d8b-4d88-9312-d58a0d8e9a50
Workflow URL : --
Tags (edit) : Add tags
Definition : 0 triggers, 0 actions
Status : Enabled
Runs last 24 hours : 0 successful, 0 failed
Integration Account : --
Get started
Runs history
Trigger history
Metrics
Resubmit
Add filter
Specify the run identifier to open monitor view directly
Identifier
Status
Start time (Local Time)
Duration
Static Results
Showing 0 runs

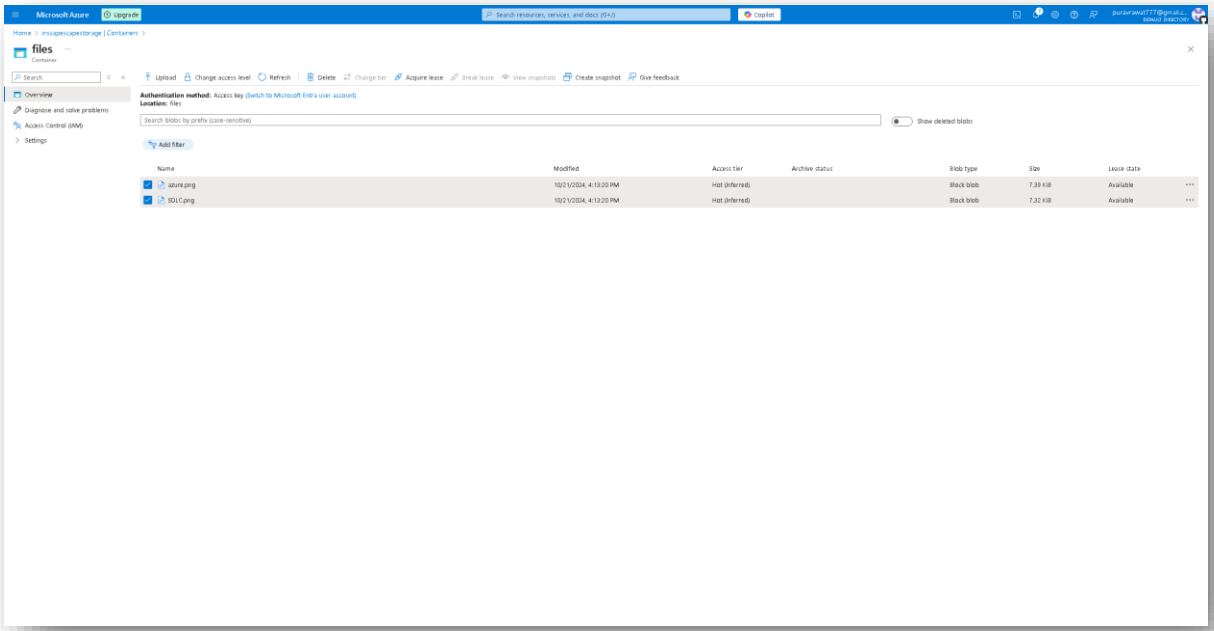

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
InsightScape-LogicApp | Logic app designer
Logic app
Search
Run
Save
Discard
Parameters
Code view
Errors
Info
File a bug
Enable Legacy Designer
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Run History
Versions
API connections
Quick start guides
Settings
Monitoring
Automation
Help
Add a trigger
Add a trigger
Blob
Runtime
Select a runtime
Action type
Triggers
Group by Connector
Loading more results...
Azure Blob Storage
See more
When a blob is added or modified (properties only) (V2)
Trigger
Blogger
See more
When a post is created
Preview
Trigger
Bloomflow
See more
Create Webhook subscription
Preview
Trigger

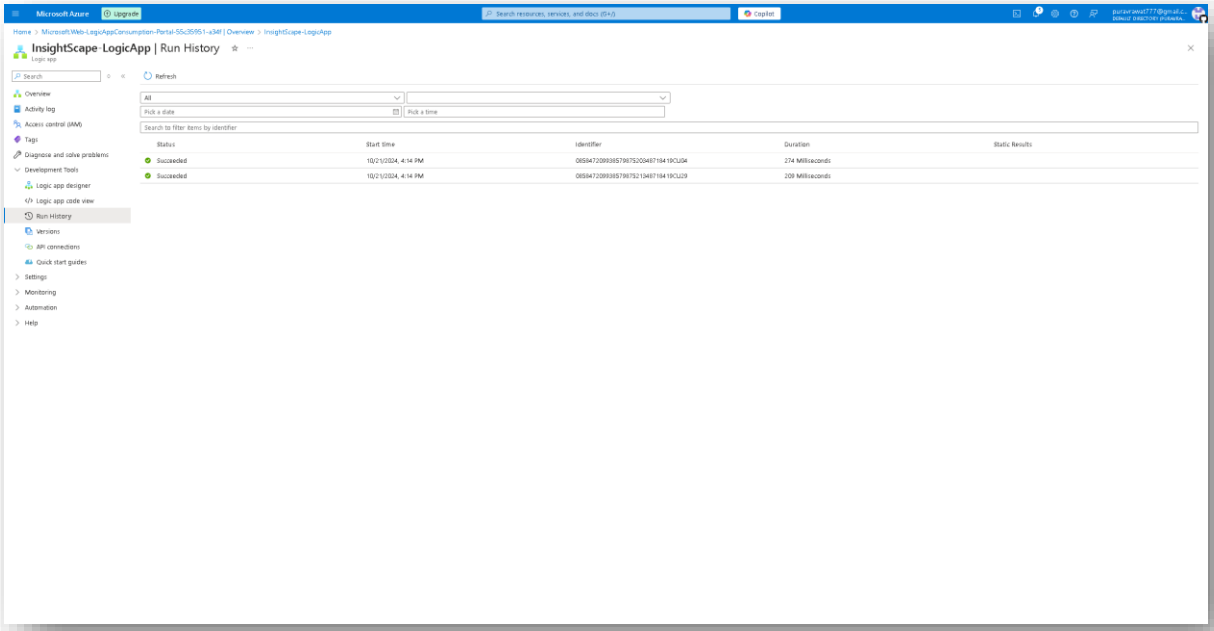

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home
inscapescapestorage
inscapescapestorage | Access keys
Storage account
Search
Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage browser
Storage Mover
Partner solutions
Data storage
Security + networking
Networking
Front Door and CDN
Access keys
Shared access signature
Encryption
Microsoft Defender for Cloud
Data management
Settings
Monitoring
Monitoring (classic)
Automation
Help
Set rotation reminder
Refresh
Give feedback
Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azure Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other.
Remember to update the keys with any Azure resources and apps that use this storage account.
Learn more about managing storage account access keys
Storage account name
inscapescapestorage
key1
Rotate key
Last rotated: 10/21/2024 (0 days ago)
Key
Show
Connection string
Show
key2
Rotate key
Last rotated: 10/21/2024 (0 days ago)
Key
Show
Connection string
Show

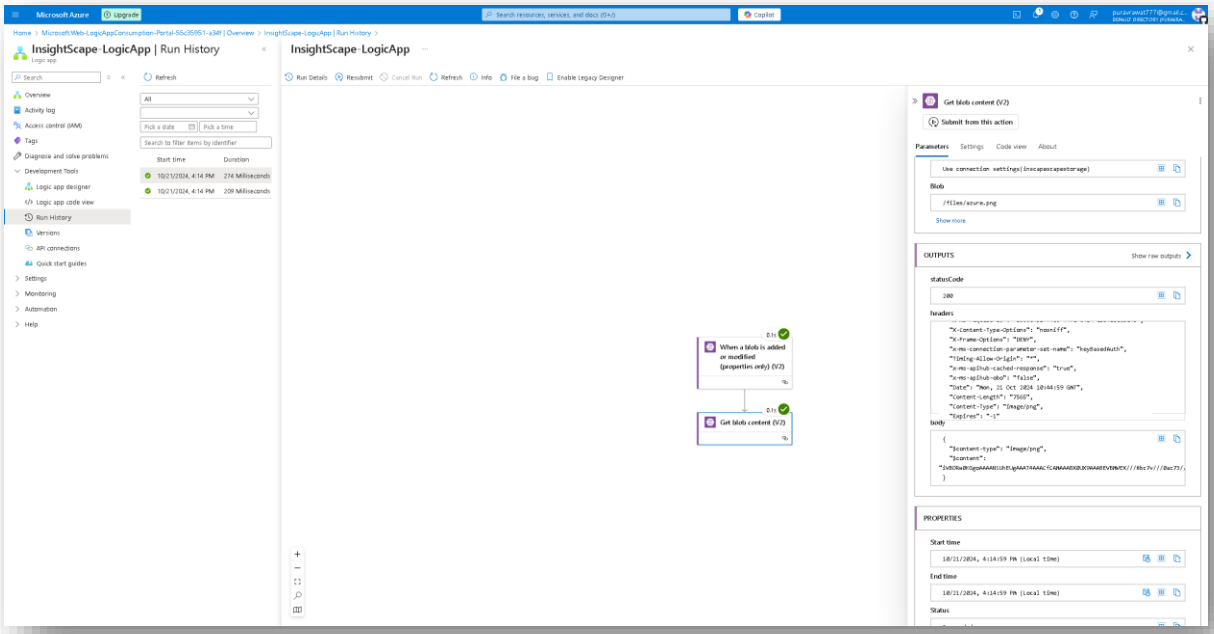

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft.Web-LogicAppConsumption-Portal-55c35951-a34f | Overview > InsightScape-LogicApp
InsightScape-LogicApp | Logic app designer
Logic app
Search
Run
Save
Discard
Parameters
Code view
Errors
Info
File a bug
Enable Legacy Designer
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Run History
Versions
API connections
Quick start guides
Settings
Monitoring
Automation
Help
When a blob is added or modified (properties only) (V2)
Create connection
When a blob is added or modified (properties only) (V2)
Create a new connection
Connection Name *
insightscapeBlobConnection
Authentication Type *
Access Key
Azure Storage Account Name Or Blob Endpoint *
nscapenscapestorage
Azure Storage Account Access Key
Create new


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft.Web-LogicAppConsumption-Portal-55c35951-a34f | Overview > InsightScape-LogicApp
InsightScape-LogicApp | Logic app designer
Logic app
Search
Run
Save
Discard
Parameters
Code view
Errors
Info
File a bug
Enable Legacy Designer
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Run History
Versions
API connections
Quick start guides
Settings
Monitoring
Automation
Help
When a blob is added or modified (properties only) (V2)
When a blob is added or modified (properties only) (V2)
Parameters
Settings
Code view
About
Storage Account Name Or Blob Endpoint *
Use connection settings(nscapescapestorage)
Container *
/files
Advanced parameters
Showing 1 of 1
Show all
Clear all
Number Of Blobs To Return
10
How often do you want to check for items?
Connected to insightscapeBlobConnection.
Change connection


Microsoft Azure
Upgrade
Copilot
InsightScape-LogicApp | Logic app designer
Logic app
Save
Discard
Parameters
Code view
Info
File a bug
Enable Legacy Designer
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Run History
Versions
API connections
Quick start guides
Settings
Monitoring
Automation
Help
When a blob is added or modified (properties only) (V2)
Get blob content (V2)
Get blob content (V2)
Parameters
Settings
Code view
Testing
About
Storage Account Name Or Blob Endpoint *
Azure Storage account name or blob endpoint.
Blob *
List of Files Path ×
Advanced parameters
Showing 1 of 1
Show all
Clear all
Infer Content Type
Yes
Connected to insightscapeBlobConnection.
Change connection


Microsoft Azure
Upgrade
Copilot
files
Container
Upload
Change access level
Refresh
Delete
Change tier
Acquire lease
Break lease
View snapshots
Create snapshot
Give feedback
Overview
Diagnose and solve problems
Access Control (IAM)
Settings
Authentication method: Access key (Switch to Microsoft Entra user account)
Location: files
Search blobs by prefix (case-sensitive)
Show deleted blobs
Add filter
Name
Modified
Access tier
Archive status
Blob type
Size
Lease state
azure.png
10/21/2024, 4:13:20 PM
Hot (inferred)
Block blob
7.39 KiB
Available
SDLC.png
10/21/2024, 4:13:20 PM
Hot (inferred)
Block blob
7.32 KiB
Available


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft.Web-LogicAppConsumption-Portal-55c35f95-1-a34f | Overview > InsightScape-LogicApp
InsightScape-LogicApp | Run History
Logic app
Search
Refresh
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Run History
Versions
API connections
Quick start guides
Settings
Monitoring
Automation
Help
All
Pick a date
Pick a time
Search to filter items by identifier
Status
Start time
Identifier
Duration
Static Results
Succeeded
10/21/2024, 4:14 PM
08584720893857987520948719419CU04
274 Milliseconds
Succeeded
10/21/2024, 4:14 PM
08584720893857987521348719419CU29
209 Milliseconds


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft.Web-LogicAppConsumption-Portal-55c35f95-1-a34f | Overview > InsightScape-LogicApp | Run History >
InsightScape-LogicApp | Run History
Logic app
InsightScape-LogicApp
Run Details
Resubmit
Cancel Run
Refresh
Info
File a bug
Enable Legacy Designer
Start time
Duration
10/21/2024, 4:14 PM
274 Milliseconds
209 Milliseconds
When a blob is added or modified (properties only) (V2)
Get blob content (V2)
Submit from this action
Parameters
Settings
Code view
About
Blob
/files/azure.png
Show more
OUTPUTS
Show raw outputs
statusCode
200
headers
body
PROPERTIES
Start time
10/21/2024, 4:14:59 PM (Local time)
End time
10/21/2024, 4:14:59 PM (Local time)
Status

e) Networking Resources

For setting up Networking Resources, I followed these steps:

1. Network Watcher Installation:

- I ensured that Network Watcher was installed and available for the West US 2 region.

2. Packet Capture Configuration:

- I navigated to the Packet Capture tab under Network Diagnostic Tools in the Network Watcher.
- Clicked on "Add" to set up the packet capture.

Packet Capture Configurations:

- Resource Group: InsightScape-RG
- Target Type: Virtual Machine
- Target Instance: InsightScape-VM1
- Packet Capture Name: InsightScape-VM1_Capture1
- Capture Location: Storage Account (insightscapestorage)
- Time Limit (seconds): 180
- Default settings were used for the remaining configurations.

After completing these configurations, I clicked on "Start packet capture".

- Verification:
  - To verify that the packet capture was successful, I navigated to the Containers tab in the insightscapestorage storage account and clicked on the "network-watcher-logs" container.
  - I was able to see the file named " packetcapture10_52_47_031.cap".
  - I downloaded the packetcapture10_52_47_031.cap file and opened it in Wireshark to view the captured packet details.

3. Connection Monitor Setup:

- After the packet capture, it was time to set up the Connection Monitor.
- I navigated to the Connection Monitor under the Monitoring tab in the Network Watcher and clicked on "+ Create".

Connection Monitor Configurations:

- Basics Tab:
  - Connection Monitor Name: VM1-to-VM2-Monitor
  - Region: East US 2
- Test Groups Tab:
  - Test Group Name: VM1-to-VM2-TestGrp

Sources:

- Azure Endpoints: VM1-Subnet
- Extension Status: Enabled

Test Configuration:

- Configuration Name: VM1-to-VM2-TestConfig
- Protocol: ICMP
- Test Frequency: Every 30 seconds

Success Threshold:

- Checks Failed (%): 50
- Round Trip Time (ms): 300

Destinations:

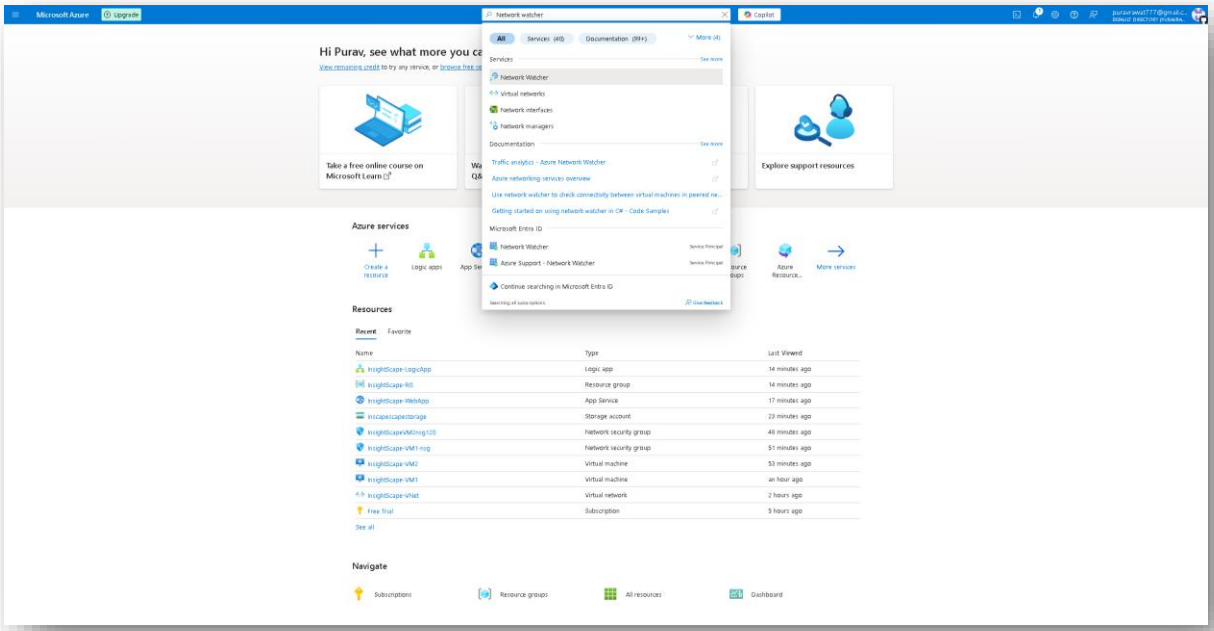
- Azure Endpoints: VM2-Subnet
- Extension Status: Enabled

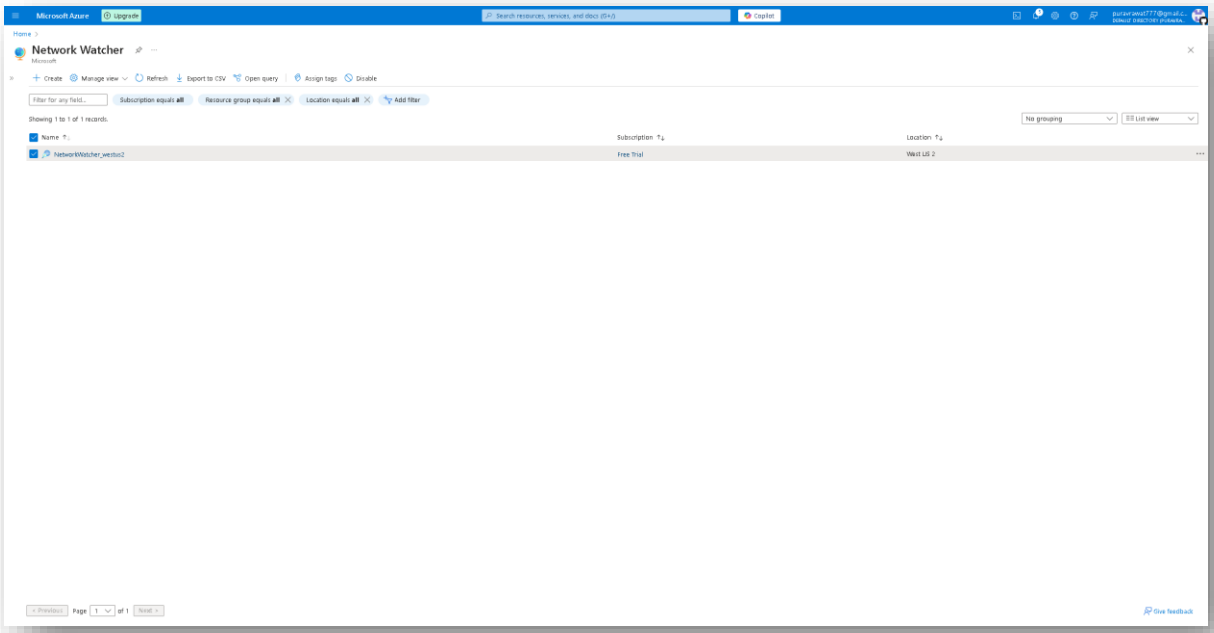
- After completing the test group details, I clicked on "Review + Create".

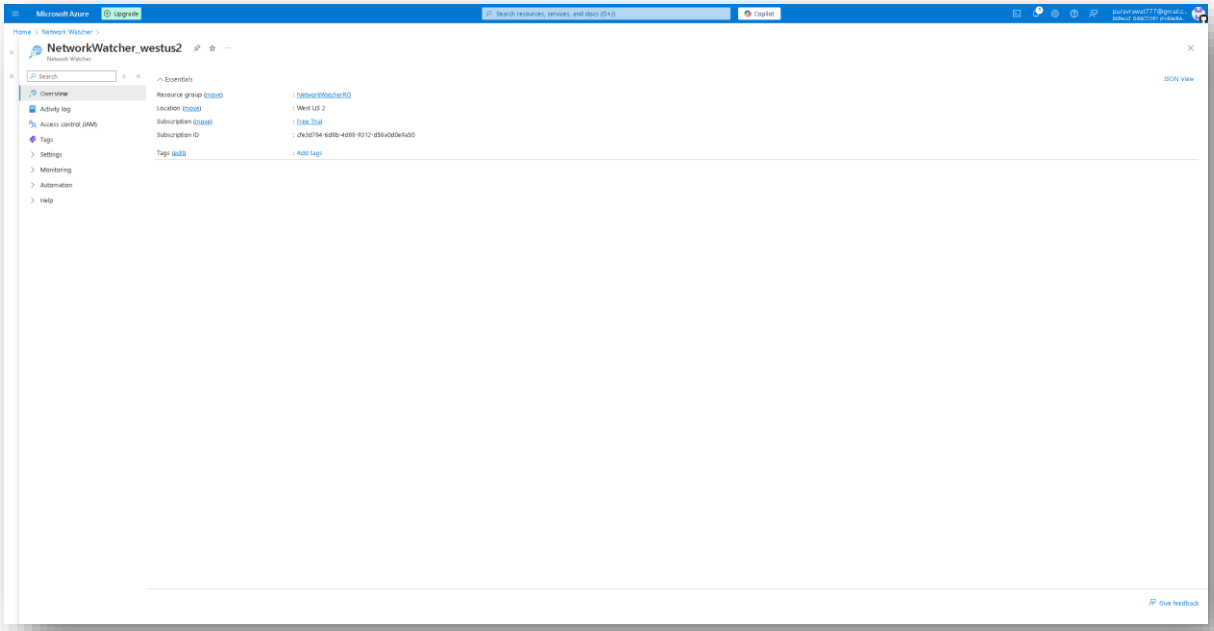
Verification:

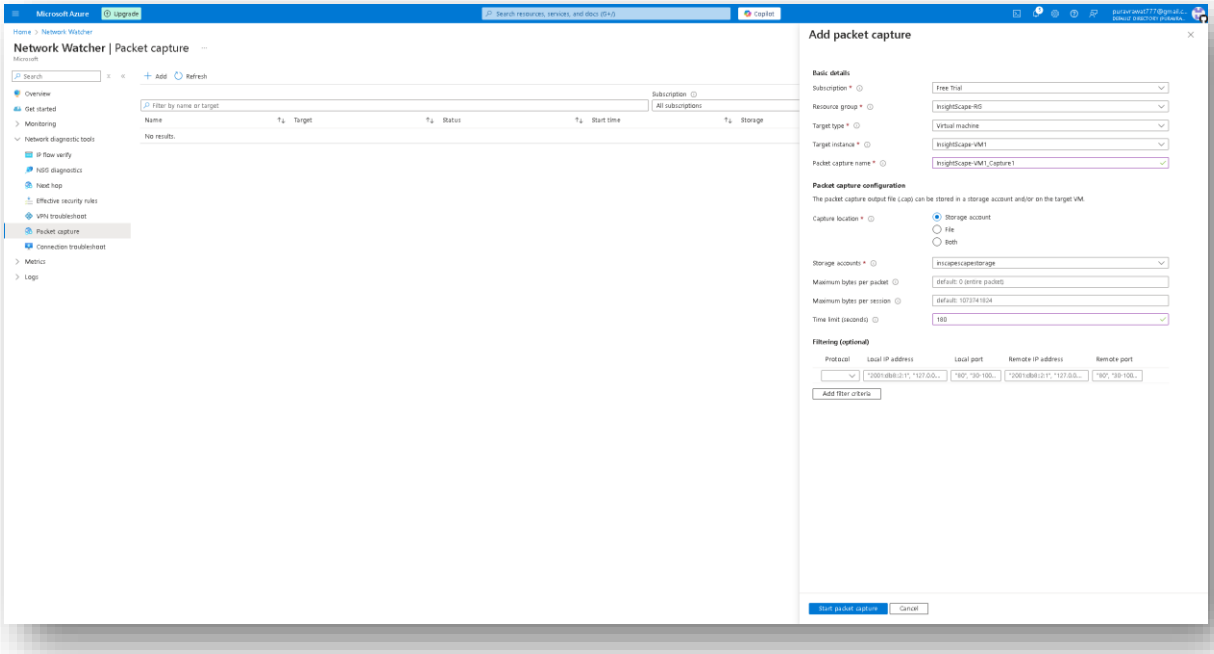
- In the Overview tab of the Connection Monitor, I was able to see "VM1-toVM2-Monitor" with the status showing a Green Tick.
- The Pass section indicated: 1 out of 1 (Green Tick).
- I clicked on the VM1-to-VM2-Monitor to see the aggregated performance metrics, including:
    - Checks failed (%)
    - Round trip time (ms)
    - Top failing tests
    - Test groups
    - Test Configurations
    - Sources and Destinations

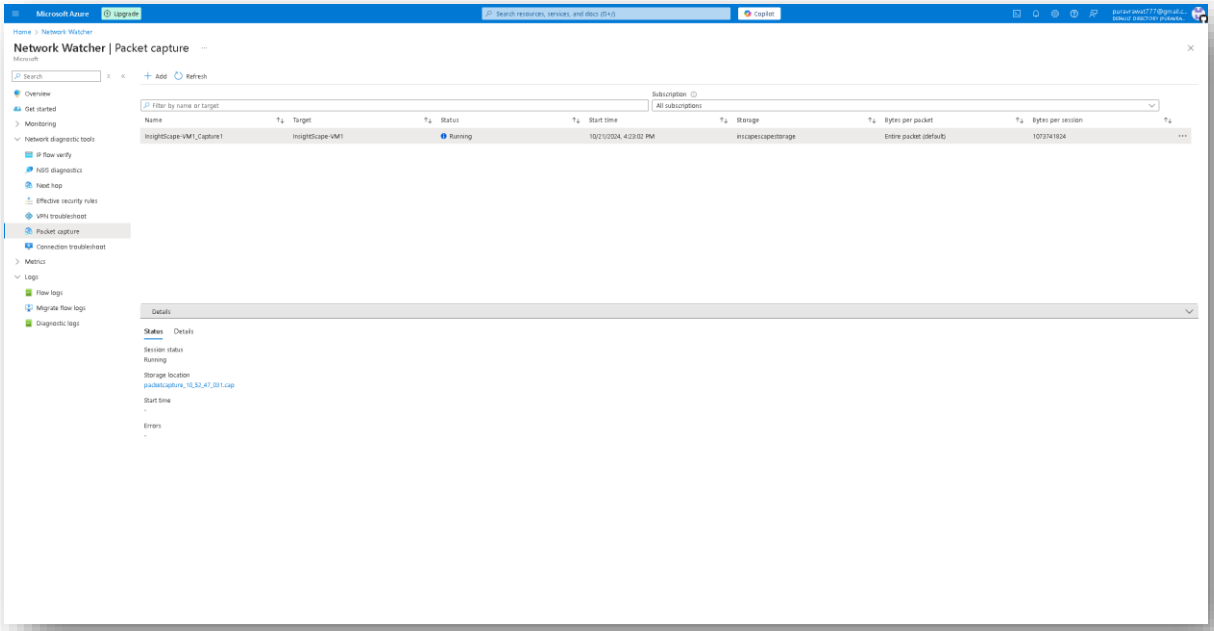
Screenshots –

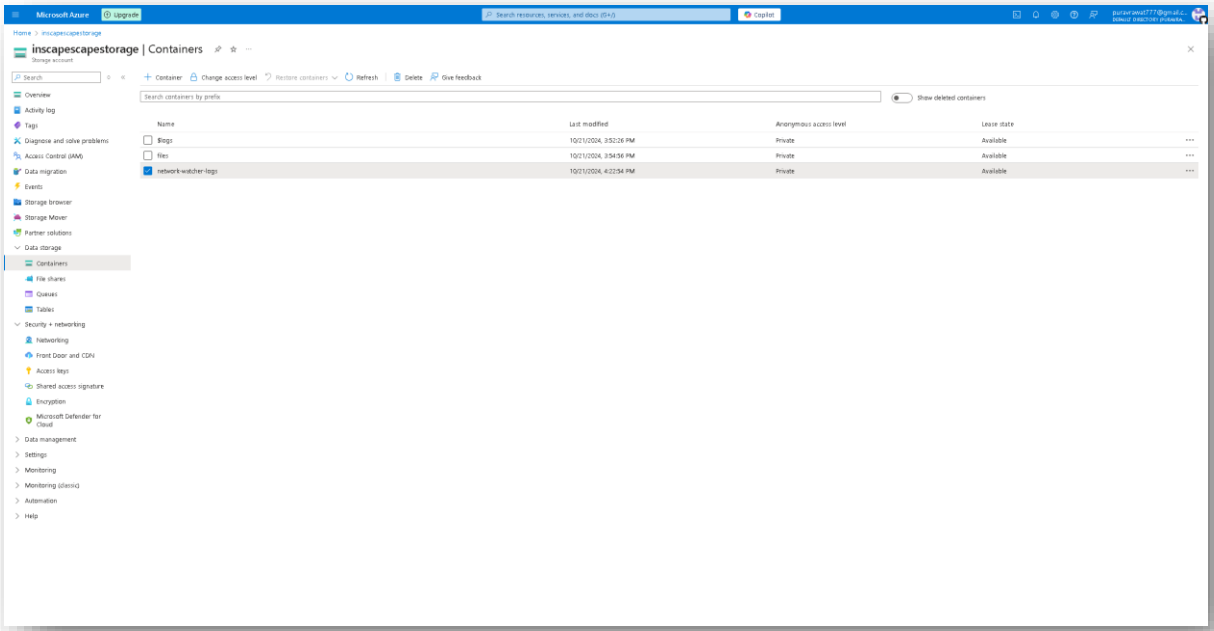


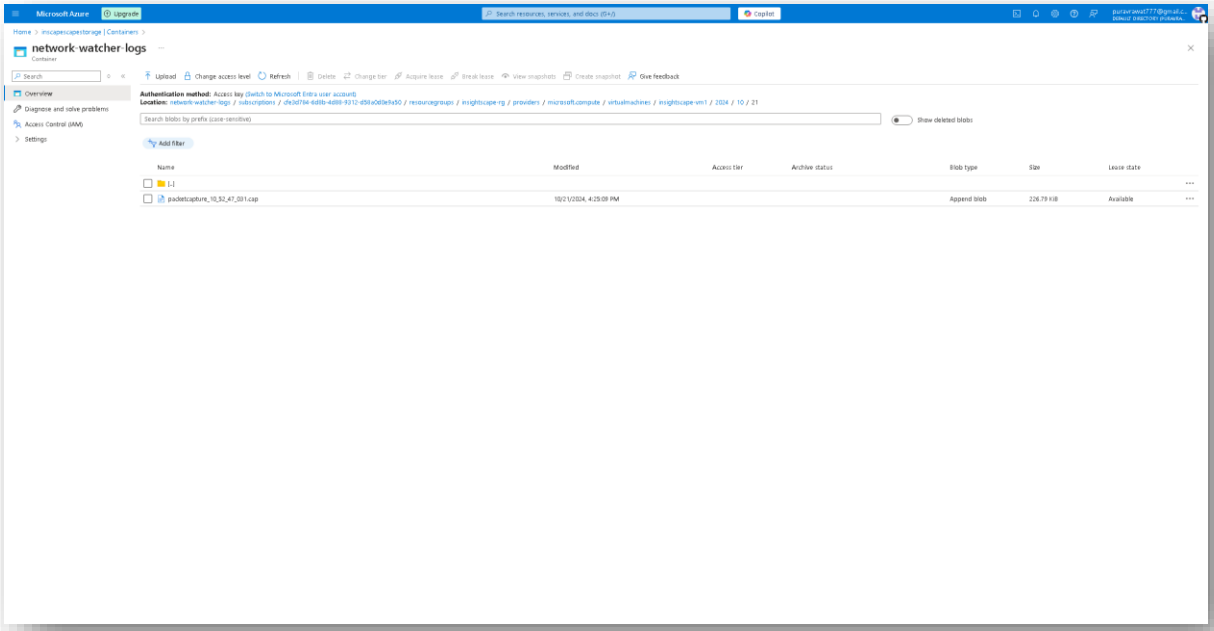


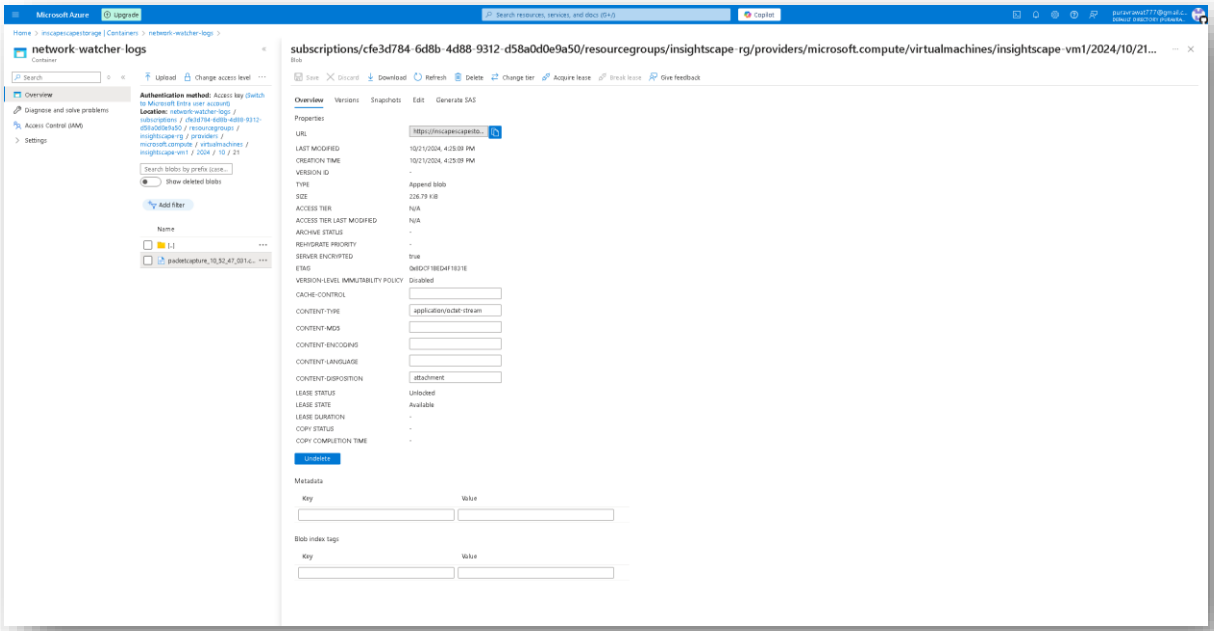

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Network Watcher >
NetworkWatcher_westus2
Network Watcher
Search
Overview
Activity log
Access control (IAM)
Tags
Settings
Monitoring
Automation
Help
Essentials
JSON View
Resource group (move) : NetworkWatcherRG
Location (move) : West US 2
Subscription (move) : Free Trial
Subscription ID : cfe3d784-6d8b-4d88-9312-d58a0d0e9a50
Tags (edit) : Add tags
Give feedback

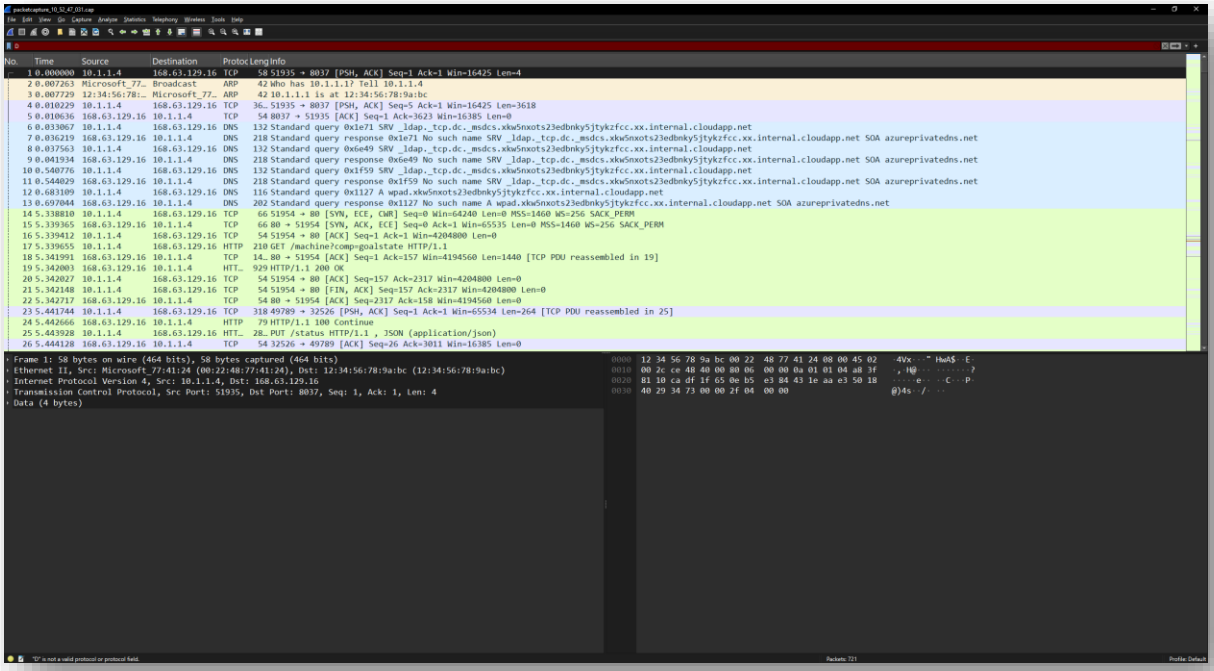

Microsoft Azure
Upgrade
Copilot
Home > Network Watcher
Network Watcher | Packet capture
Microsoft
Search
Overview
Get started
Monitoring
Network diagnostic tools
IP flow verify
NSG diagnostics
Next hop
Effective security rules
VPN troubleshoot
Packet capture
Connection troubleshoot
Metrics
Logs
Add
Refresh
Filter by name or target
Subscription
All subscriptions
Name
Target
Status
Start time
Storage
No results.
Add packet capture
Basic details
Subscription * Free Trial
Resource group * InsightScape-RG
Target type * Virtual machine
Target instance * InsightScape-VM1
Packet capture name * InsightScape-VM1_Capture1
Packet capture configuration
The packet capture output file (.cap) can be stored in a storage account and/or on the target VM.
Capture location * Storage account
File
Both
Storage accounts * insightscapestorage
Maximum bytes per packet default: 0 (entire packet)
Maximum bytes per session default: 1073741824
Time limit (seconds) 180
Filtering (optional)
Protocol
Local IP address
Local port
Remote IP address
Remote port
Add filter criteria
Start packet capture
Cancel

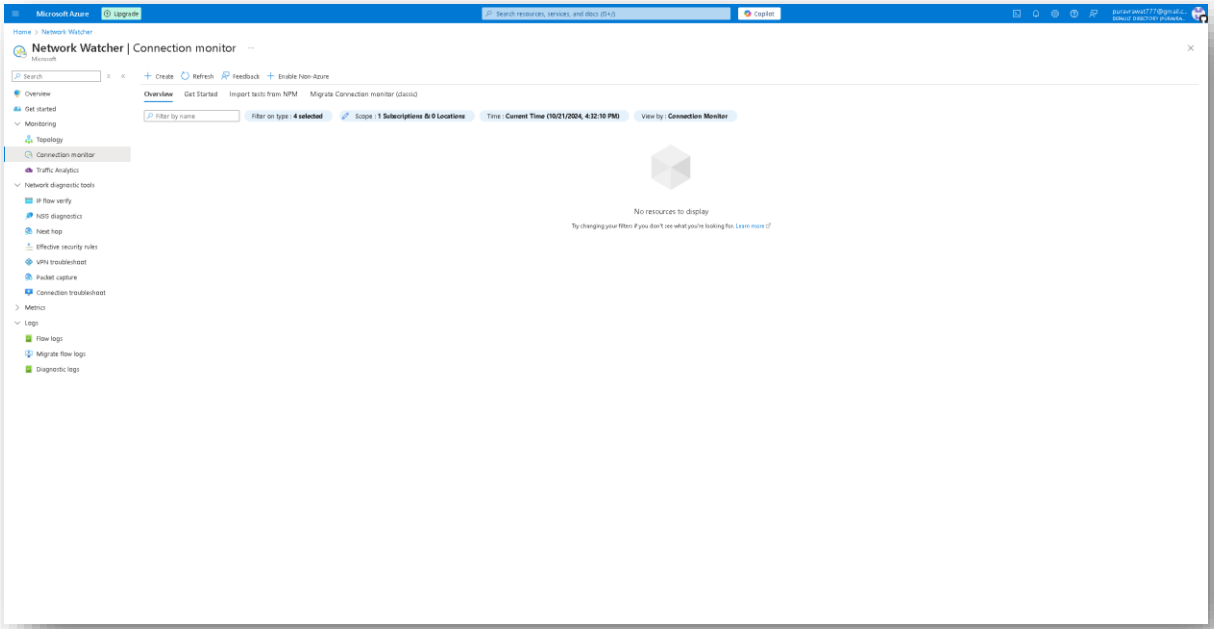

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Network Watcher
Network Watcher | Packet capture
Microsoft
Search
Add
Refresh
Overview
Get started
Monitoring
Network diagnostic tools
IP flow verify
NSG diagnostics
Next hop
Effective security rules
VPN troubleshoot
Packet capture
Connection troubleshoot
Metrics
Logs
Flow logs
Migrate flow logs
Diagnostic logs
Subscription
All subscriptions
Filter by name or target
Name
Target
Status
Start time
Storage
Bytes per packet
Bytes per session
InsightScape-VM1_Capture1
InsightScape-VM1
Running
10/21/2024, 4:23:02 PM
inscapescapestorage
Entire packet (default)
1073741824
Details
Status
Details
Session status
Running
Storage location
packetcapture_10_52_47_031.cap
Start time
-
Errors
-

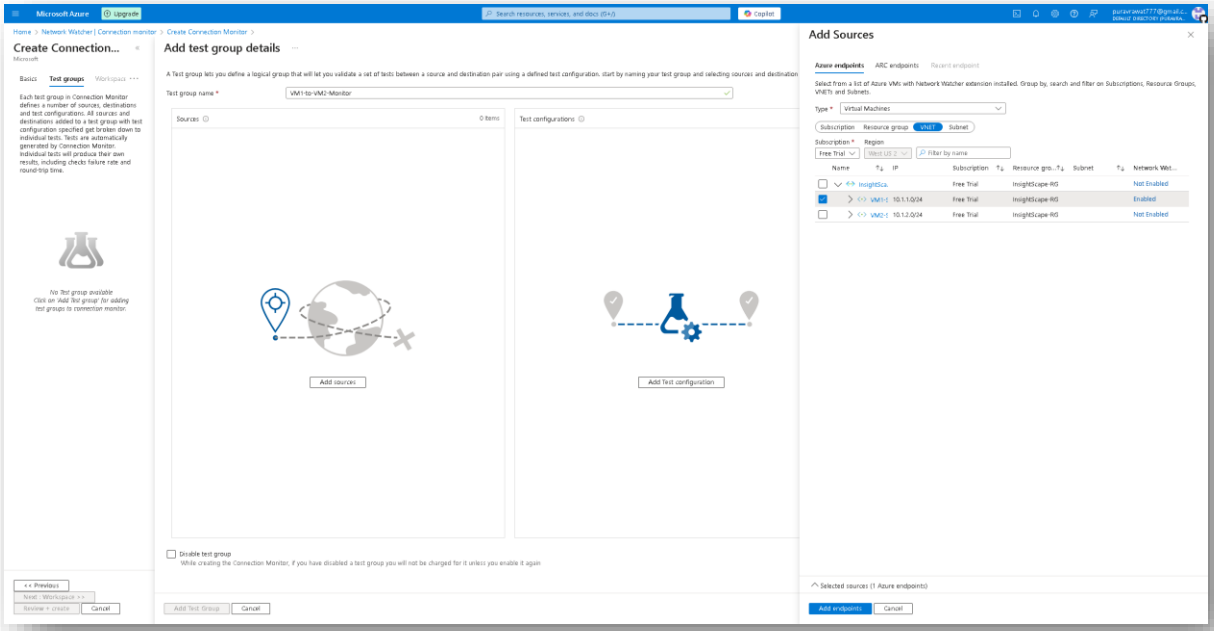

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > inscapescapestorage
inscapescapestorage | Containers
Storage account
Search
Container
Change access level
Restore containers
Refresh
Delete
Give feedback
Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage browser
Storage Mover
Partner solutions
Data storage
Containers
File shares
Queues
Tables
Security + networking
Networking
Front Door and CDN
Access keys
Shared access signature
Encryption
Microsoft Defender for Cloud
Data management
Settings
Monitoring
Monitoring (classic)
Automation
Help
Search containers by prefix
Show deleted containers
Name
Last modified
Anonymous access level
Lease state
Blogs
10/21/2024, 3:52:26 PM
Private
Available
files
10/21/2024, 3:54:56 PM
Private
Available
network-watcher-logs
10/21/2024, 4:22:54 PM
Private
Available

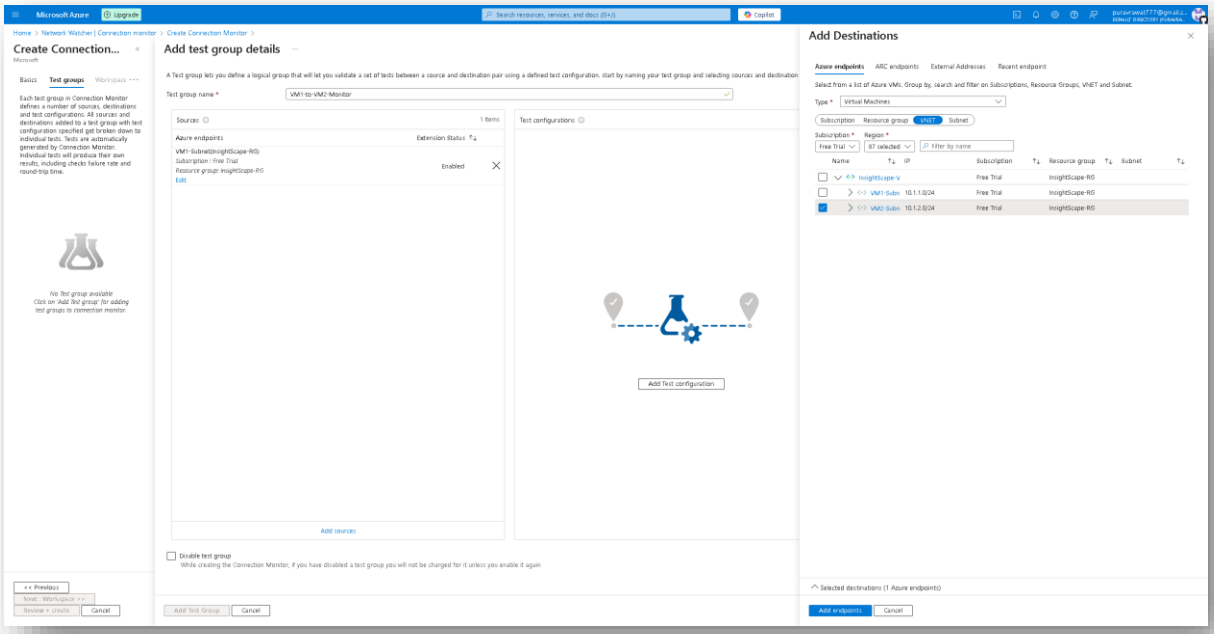

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > inscapecapestorage | Containers >
network-watcher-logs
Container
Search
Overview
Diagnose and solve problems
Access Control (IAM)
Settings
Upload
Change access level
Refresh
Delete
Change tier
Acquire lease
Break lease
View snapshots
Create snapshot
Give feedback
Authentication method: Access key (Switch to Microsoft Entra user account)
Location: network-watcher-logs / subscriptions / cfe3d784-6d8b-4d88-9312-d58a0d0e9a50 / resourcegroups / insightscape-rg / providers / microsoft.compute / virtualmachines / insightscape-vm1 / 2024 / 10 / 21
Search blobs by prefix (case-sensitive)
Show deleted blobs
Add filter
Name
Modified
Access tier
Archive status
Blob type
Size
Lease state
[..]
packetcapture_10_32_47_031.cap
10/21/2024, 4:25:09 PM
Append blob
226.79 KiB
Available

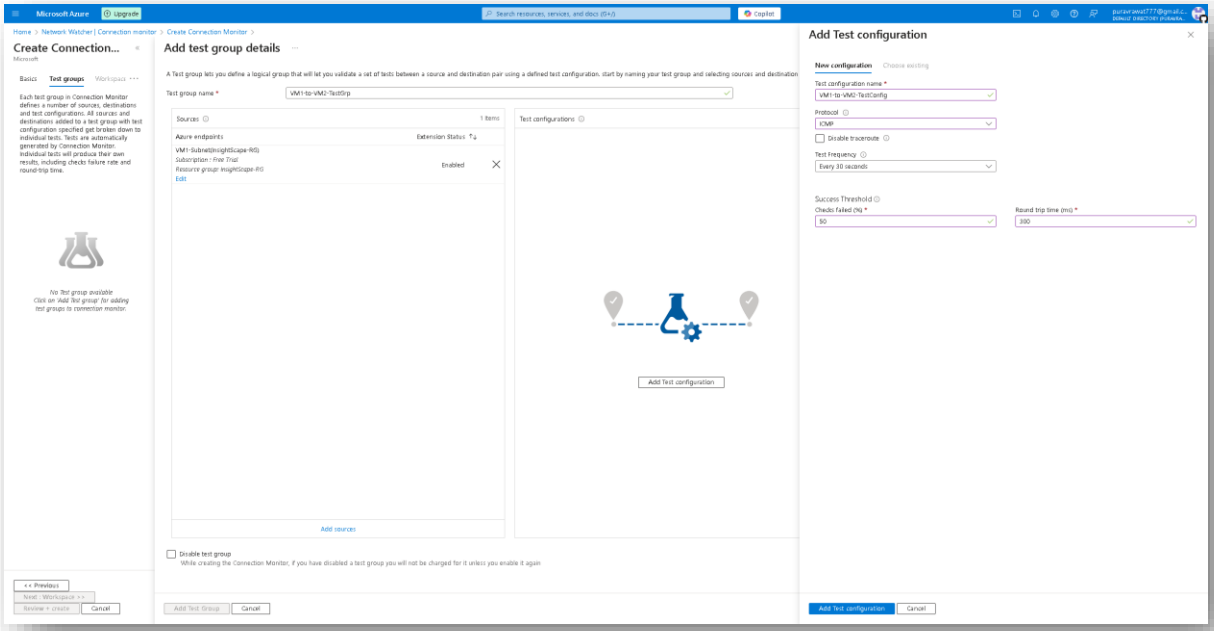

Microsoft Azure
Upgrade
Copilot
Home > inscapecapestorage | Containers > network-watcher-logs >
network-watcher-logs
Container
subscriptions/cfe3d784-6d8b-4d88-9312-d58a0d0e9a50/resourcegroups/insightscape-rg/providers/microsoft.compute/virtualmachines/insightscape-vm1/2024/10/21...
Blob
Save
Discard
Download
Refresh
Delete
Change tier
Acquire lease
Break lease
Give feedback
Overview
Versions
Snapshots
Edit
Generate SAS
Properties
URL
LAST MODIFIED 10/21/2024, 4:25:09 PM
CREATION TIME 10/21/2024, 4:25:09 PM
VERSION ID -
TYPE Append blob
SIZE 226.79 KiB
ACCESS TIER N/A
ACCESS TIER LAST MODIFIED N/A
ARCHIVE STATUS -
REHYDRATE PRIORITY -
SERVER ENCRYPTED true
ETAG 0x8DCF18E04F1831E
VERSION-LEVEL IMMUTABILITY POLICY Disabled
CACHE-CONTROL
CONTENT-TYPE application/octet-stream
CONTENT-MD5
CONTENT-ENCODING
CONTENT-LANGUAGE
CONTENT-DISPOSITION attachment
LEASE STATUS Unlocked
LEASE STATE Available
LEASE DURATION -
COPY STATUS -
COPY COMPLETION TIME -
Undelete
Metadata
Key
Value
Blob index tags
Key
Value

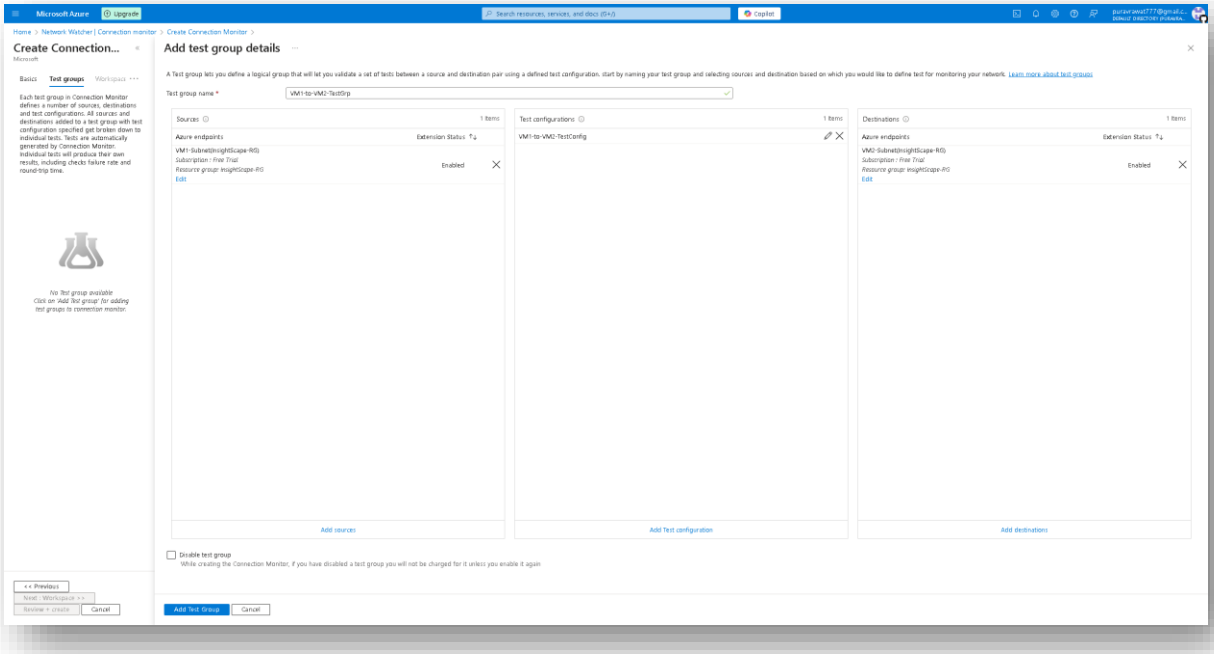

packetcapture_10_52_47_031.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protoc Leng Info
1 0.000000 10.1.1.4 168.63.129.16 TCP 58 51935 → 8037 [PSH, ACK] Seq=1 Ack=1 Win=16425 Len=4
2 0.007263 Microsoft_77… Broadcast ARP 42 Who has 10.1.1.1? Tell 10.1.1.4
3 0.007729 12:34:56:78:… Microsoft_77… ARP 42 10.1.1.1 is at 12:34:56:78:9a:bc
4 0.010229 10.1.1.4 168.63.129.16 TCP 36… 51935 → 8037 [PSH, ACK] Seq=5 Ack=1 Win=16425 Len=3618
5 0.010636 168.63.129.16 10.1.1.4 TCP 54 8037 → 51935 [ACK] Seq=1 Ack=3623 Win=16385 Len=0
6 0.033067 10.1.1.4 168.63.129.16 DNS 132 Standard query 0x1e71 SRV _ldap._tcp.dc._msdcs.xkw5nxots23edbnky5jtykzfcc.xx.internal.cloudapp.net
7 0.036219 168.63.129.16 10.1.1.4 DNS 218 Standard query response 0x1e71 No such name SRV _ldap._tcp.dc._msdcs.xkw5nxots23edbnky5jtykzfcc.xx.internal.cloudapp.net SOA azureprivatedns.net
8 0.037563 10.1.1.4 168.63.129.16 DNS 132 Standard query 0x6e49 SRV _ldap._tcp.dc._msdcs.xkw5nxots23edbnky5jtykzfcc.xx.internal.cloudapp.net
9 0.041934 168.63.129.16 10.1.1.4 DNS 218 Standard query response 0x6e49 No such name SRV _ldap._tcp.dc._msdcs.xkw5nxots23edbnky5jtykzfcc.xx.internal.cloudapp.net SOA azureprivatedns.net
10 0.540776 10.1.1.4 168.63.129.16 DNS 132 Standard query 0x1f59 SRV _ldap._tcp.dc._msdcs.xkw5nxots23edbnky5jtykzfcc.xx.internal.cloudapp.net
11 0.544029 168.63.129.16 10.1.1.4 DNS 218 Standard query response 0x1f59 No such name SRV _ldap._tcp.dc._msdcs.xkw5nxots23edbnky5jtykzfcc.xx.internal.cloudapp.net SOA azureprivatedns.net
12 0.683109 10.1.1.4 168.63.129.16 DNS 116 Standard query 0x1127 A wpad.xkw5nxots23edbnky5jtykzfcc.xx.internal.cloudapp.net
13 0.697044 168.63.129.16 10.1.1.4 DNS 202 Standard query response 0x1127 No such name A wpad.xkw5nxots23edbnky5jtykzfcc.xx.internal.cloudapp.net SOA azureprivatedns.net
14 5.338810 10.1.1.4 168.63.129.16 TCP 66 51954 → 80 [SYN, ECE, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
15 5.339365 168.63.129.16 10.1.1.4 TCP 66 80 → 51954 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
16 5.339412 10.1.1.4 168.63.129.16 TCP 54 51954 → 80 [ACK] Seq=1 Ack=1 Win=4204800 Len=0
17 5.339655 10.1.1.4 168.63.129.16 HTTP 210 GET /machine?comp=goalstate HTTP/1.1
18 5.341991 168.63.129.16 10.1.1.4 TCP 14… 80 → 51954 [ACK] Seq=1 Ack=157 Win=4194560 Len=1440 [TCP PDU reassembled in 19]
19 5.342003 168.63.129.16 10.1.1.4 HTT… 929 HTTP/1.1 200 OK
20 5.342027 10.1.1.4 168.63.129.16 TCP 54 51954 → 80 [ACK] Seq=157 Ack=2317 Win=4204800 Len=0
21 5.342148 10.1.1.4 168.63.129.16 TCP 54 51954 → 80 [FIN, ACK] Seq=157 Ack=2317 Win=4204800 Len=0
22 5.342717 168.63.129.16 10.1.1.4 TCP 54 80 → 51954 [ACK] Seq=2317 Ack=158 Win=4194560 Len=0
23 5.441744 10.1.1.4 168.63.129.16 TCP 318 49789 → 32526 [PSH, ACK] Seq=1 Ack=1 Win=65534 Len=264 [TCP PDU reassembled in 25]
24 5.442666 168.63.129.16 10.1.1.4 HTTP 79 HTTP/1.1 100 Continue
25 5.443928 10.1.1.4 168.63.129.16 HTT… 28… PUT /status HTTP/1.1 , JSON (application/json)
26 5.444128 168.63.129.16 10.1.1.4 TCP 54 32526 → 49789 [ACK] Seq=26 Ack=3011 Win=16385 Len=0
Frame 1: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
Ethernet II, Src: Microsoft_77:41:24 (00:22:48:77:41:24), Dst: 12:34:56:78:9a:bc (12:34:56:78:9a:bc)
Internet Protocol Version 4, Src: 10.1.1.4, Dst: 168.63.129.16
Transmission Control Protocol, Src Port: 51935, Dst Port: 8037, Seq: 1, Ack: 1, Len: 4
Data (4 bytes)
0000 12 34 56 78 9a bc 00 22 48 77 41 24 08 00 45 02
0010 00 2c ce 48 40 00 80 06 00 00 0a 01 01 04 a8 3f
0020 81 10 ca df 1f 65 0e b5 e3 84 43 1e aa e3 50 18
0030 40 29 34 73 00 00 2f 04 00 00
"D" is not a valid protocol or protocol field.
Packets: 721
Profile: Default

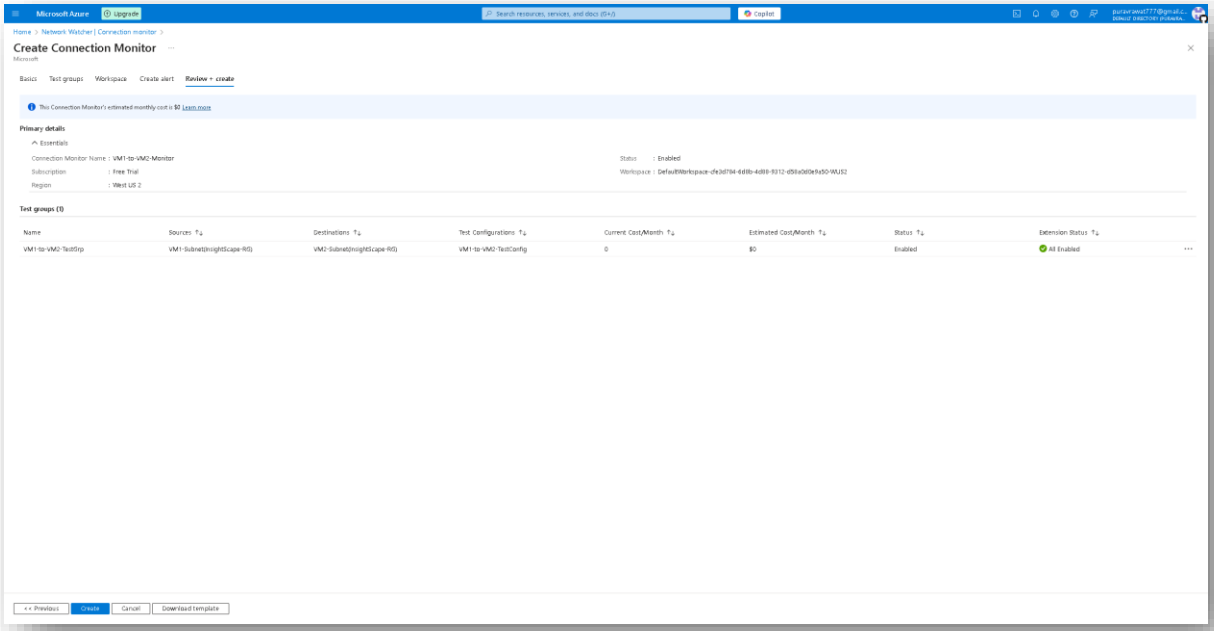

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Network Watcher
Network Watcher | Connection monitor
Microsoft
Search
Create
Refresh
Feedback
Enable Non-Azure
Overview
Get started
Monitoring
Topology
Connection monitor
Traffic Analytics
Network diagnostic tools
IP flow verify
NSG diagnostics
Next hop
Effective security rules
VPN troubleshoot
Packet capture
Connection troubleshoot
Metrics
Logs
Flow logs
Migrate flow logs
Diagnostic logs
Overview
Get Started
Import tests from NPM
Migrate Connection monitor (classic)
Filter by name
Filter on type : 4 selected
Scope : 1 Subscriptions & 0 Locations
Time : Current Time (10/21/2024, 4:32:10 PM)
View by : Connection Monitor
No resources to display
Try changing your filters if you don't see what you're looking for. Learn more

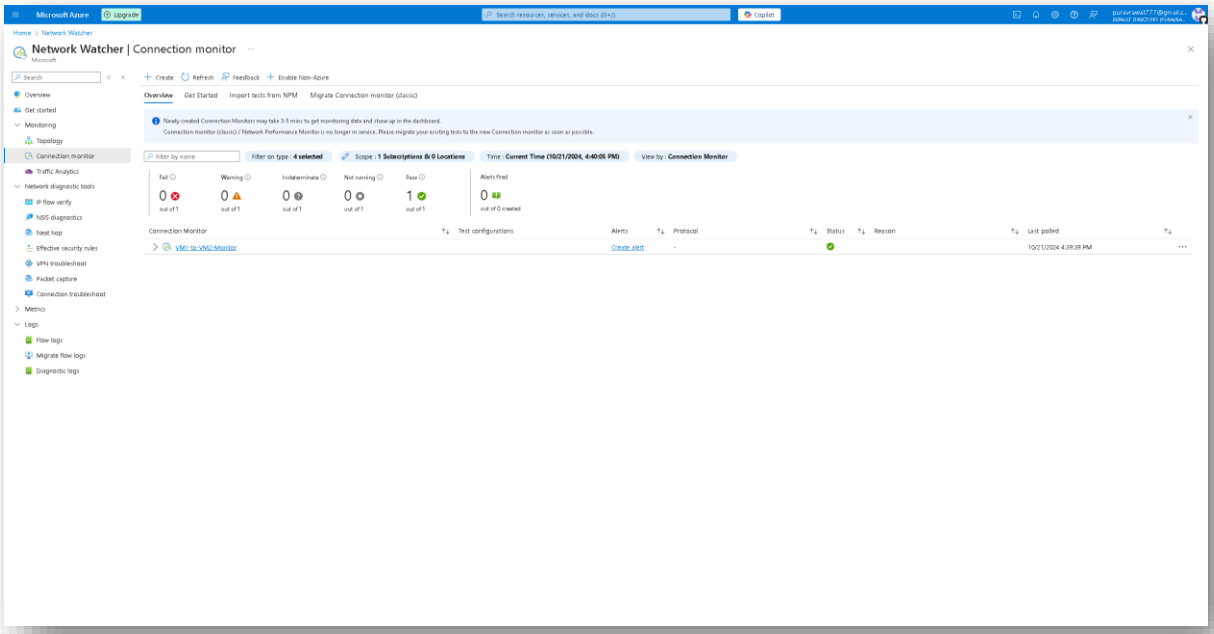

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Network Watcher | Connection monitor > Create Connection Monitor >
Create Connection...
Microsoft
Basics
Test groups
Workspace
Each test group in Connection Monitor defines a number of sources, destinations and test configurations. All sources and destinations added to a test group with test configuration specified get broken down to individual tests. Tests are automatically generated by Connection Monitor. Individual tests will produce their own results, including checks failure rate and round-trip time.
No Test group available
Click on 'Add Test group' for adding test groups to connection monitor.
« Previous
Next : Workspace > >
Review + create
Cancel
Add test group details
A Test group lets you define a logical group that will let you validate a set of tests between a source and destination pair using a defined test configuration. start by naming your test group and selecting sources and destination
Test group name *
VM1-to-VM2-Monitor
Sources
0 Items
Test configurations
Add sources
Add Test configuration
Disable test group
While creating the Connection Monitor, if you have disabled a test group you will not be charged for it unless you enable it again
Add Test Group
Cancel
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 *
Region
Free Trial
West US 2
Filter by name
Name
IP
Subscription
Resource gro...
Subnet
Network Wat...
InsightSca
Free Trial
InsightScape-RG
Not Enabled
VM1-t
10.1.1.0/24
Enabled
VM2-t
10.1.2.0/24
Selected sources (1 Azure endpoints)
Add endpoints
Cancel

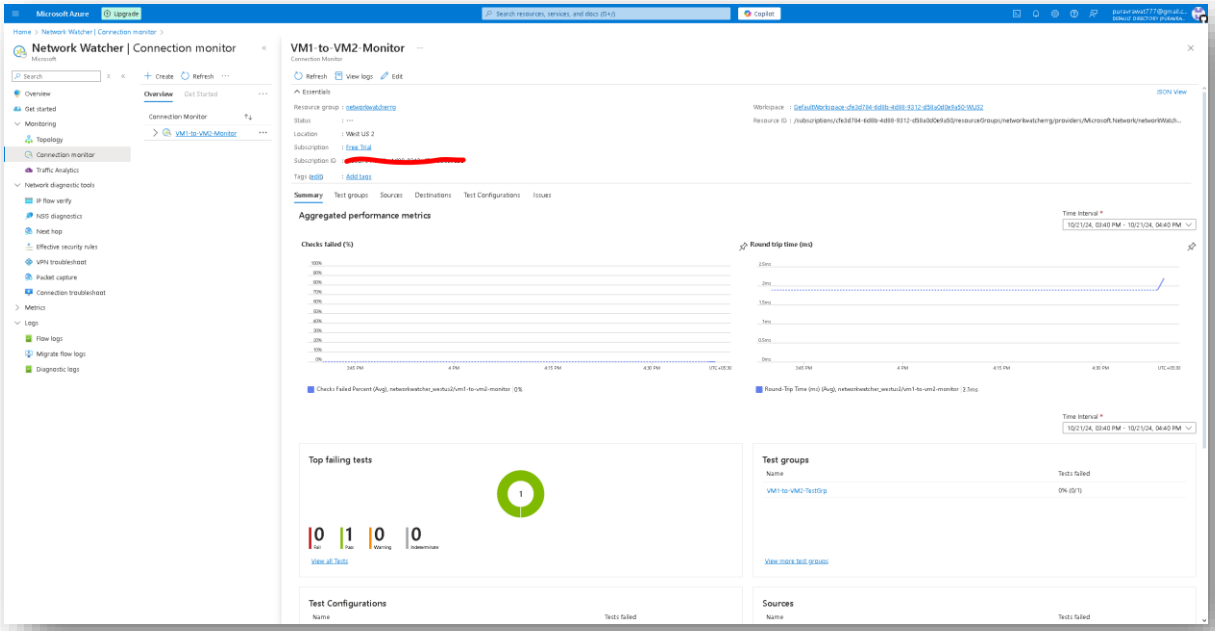

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Network Watcher | Connection monitor > Create Connection Monitor >
Create Connection...
Microsoft
Basics
Test groups
Workspace
Each test group in Connection Monitor defines a number of sources, destinations and test configurations. All sources and destinations added to a test group with test configuration specified get broken down to individual tests. Tests are automatically generated by Connection Monitor. Individual tests will produce their own results, including checks failure rate and round-trip time.
No Test group available
Click on 'Add Test group' for adding test groups to connection monitor.
« Previous
Next : Workspace > >
Review + create
Cancel
Add test group details
A Test group lets you define a logical group that will let you validate a set of tests between a source and destination pair using a defined test configuration. start by naming your test group and selecting sources and destination
Test group name *
VM1-to-VM2-Monitor
Sources
1 Items
Azure endpoints
Extension Status
VM1-Subnet(InsightScape-RG)
Subscription : Free Trial
Resource group: InsightScape-RG
Edit
Enabled
Test configurations
Add Test configuration
Add sources
Disable test group
While creating the Connection Monitor, if you have disabled a test group you will not be charged for it unless you enable it again
Add Test Group
Cancel
Add Destinations
Azure endpoints
ARC endpoints
External Addresses
Recent endpoint
Select from a list of Azure VMs. Group by, search and filter on Subscriptions, Resource Groups, VNET and Subnet.
Type *
Virtual Machines
Subscription
Resource group
VNET
Subnet
Subscription *
Region *
Free Trial
87 selected
Filter by name
Name
IP
Subscription
Resource group
Subnet
InsightScape-V
Free Trial
InsightScape-RG
VM1-Subn
10.1.1.0/24
VM2-Subn
10.1.2.0/24
Selected destinations (1 Azure endpoints)
Add endpoints
Cancel


Microsoft Azure
Upgrade
Copilot
Home > Network Watcher | Connection monitor > Create Connection Monitor
Create Connection...
Basics
Test groups
Workspace
Each test group in Connection Monitor defines a number of sources, destinations and test configurations. All sources and destinations added to a test group with test configuration specified get broken down to individual tests. Tests are automatically generated by Connection Monitor. Individual tests will produce their own results, including checks failure rate and round-trip time.
No Test group available
Click on 'Add Test group' for adding test groups to connection monitor.
Add test group details
A Test group lets you define a logical group that will let you validate a set of tests between a source and destination pair using a defined test configuration. start by naming your test group and selecting sources and destination
Test group name *
VM1-to-VM2-TestGrp
Sources
1 Items
Azure endpoints
Extension Status
VM1-Subnet(InsightScape-RG)
Subscription : Free Trial
Resource group: InsightScape-RG
Edit
Enabled
Add sources
Test configurations
Add Test configuration
Disable test group
While creating the Connection Monitor, if you have disabled a test group you will not be charged for it unless you enable it again
<< Previous
Next : Workspace >>
Review + create
Cancel
Add Test Group
Add Test configuration
New configuration
Choose existing
Test configuration name *
VM1-to-VM2-TestConfig
Protocol
ICMP
Disable traceroute
Test Frequency
Every 30 seconds
Success Threshold
Checks failed (%) *
50
Round trip time (ms) *
300


Microsoft Azure
Upgrade
Copilot
Home > Network Watcher | Connection monitor > Create Connection Monitor
Create Connection...
Basics
Test groups
Workspace
Each test group in Connection Monitor defines a number of sources, destinations and test configurations. All sources and destinations added to a test group with test configuration specified get broken down to individual tests. Tests are automatically generated by Connection Monitor. Individual tests will produce their own results, including checks failure rate and round-trip time.
No Test group available
Click on 'Add Test group' for adding test groups to connection monitor.
Add test group details
A Test group lets you define a logical group that will let you validate a set of tests between a source and destination pair using a defined test configuration. start by naming your test group and selecting sources and destination based on which you would like to define test for monitoring your network. Learn more about test groups
Test group name *
VM1-to-VM2-TestGrp
Sources
1 Items
Azure endpoints
Extension Status
VM1-Subnet(InsightScape-RG)
Subscription : Free Trial
Resource group: InsightScape-RG
Edit
Enabled
Add sources
Test configurations
1 Items
VM1-to-VM2-TestConfig
Add Test configuration
Destinations
1 Items
Azure endpoints
Extension Status
VM2-Subnet(InsightScape-RG)
Subscription : Free Trial
Resource group: InsightScape-RG
Edit
Enabled
Add destinations
Disable test group
While creating the Connection Monitor, if you have disabled a test group you will not be charged for it unless you enable it again
<< Previous
Next : Workspace >>
Review + create
Cancel
Add Test Group
Cancel


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Network Watcher | Connection monitor >
Create Connection Monitor
Microsoft
Basics
Test groups
Workspace
Create alert
Review + create
This Connection Monitor's estimated monthly cost is $0 Learn more
Primary details
Essentials
Connection Monitor Name : VM1-to-VM2-Monitor
Subscription : Free Trial
Region : West US 2
Status : Enabled
Workspace : DefaultWorkspace-cfe3d784-4d8b-4d88-9312-d5fda0d0e9a50-WUS2
Test groups (1)
Name
Sources
Destinations
Test Configurations
Current Cost/Month
Estimated Cost/Month
Status
Extension Status
VM1-to-VM2-TestGrp
VM1-Subnet(InsightScape-RG)
VM2-Subnet(InsightScape-RG)
VM1-to-VM2-TestConfig
0
$0
Enabled
All Enabled
<< Previous
Create
Cancel
Download template


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Network Watcher
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
Metrics
Logs
Flow logs
Migrate flow logs
Diagnostic logs
Create
Refresh
Feedback
Enable Non-Azure
Overview
Get Started
Import tests from NPM
Migrate Connection monitor (classic)
Newly created Connection Monitors may take 3-5 mins to get monitoring data and show up in the dashboard.
Connection monitor (classic) / Network Performance Monitor is no longer in service. Please migrate your existing tests to the new Connection monitor as soon as possible.
Filter by name
Filter on type : 4 selected
Scope : 1 Subscriptions & 0 Locations
Time : Current Time (10/21/2024, 4:40:05 PM)
View by : Connection Monitor
Fail
Warning
Indeterminate
Not running
Pass
Alerts fired
0 out of 1
0 out of 1
0 out of 1
0 out of 1
1 out of 1
0 out of 0 created
Connection Monitor
Test configurations
Alerts
Protocol
Status
Reason
Last polled
VM1-to-VM2-Monitor
Create alert
-
10/21/2024 4:39:38 PM


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
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
Metrics
Logs
Flow logs
Migrate flow logs
Diagnostic logs
Create
Refresh
Overview
Get Started
Connection Monitor
VM1-to-VM2-Monitor
VM1-to-VM2-Monitor
Connection Monitor
Refresh
View logs
Edit
Essentials
JSON View
Resource group : networkwatcherrg
Status : ...
Location : West US 2
Subscription : Free Trial
Subscription ID : [redacted]
Tags (edit) : Add tags
Workspace : DefaultWorkspace-cfe3d784-6d8b-4d88-9312-d58a0d0e9a50-WUS2
Resource ID : /subscriptions/cfe3d784-6d8b-4d88-9312-d58a0d0e9a50/resourceGroups/networkwatcherrg/providers/Microsoft.Network/networkWatch...
Summary
Test groups
Sources
Destinations
Test Configurations
Issues
Aggregated performance metrics
Time Interval *
10/21/24, 03:40 PM - 10/21/24, 04:40 PM
Checks failed (%)
Round trip time (ms)
Checks Failed Percent (Avg), networkwatcher_westus2|vm1-to-vm2-monitor : 0%
Round-Trip Time (ms) (Avg), networkwatcher_westus2|vm1-to-vm2-monitor : 2.5ms
Time Interval *
10/21/24, 03:40 PM - 10/21/24, 04:40 PM
Top failing tests
0
1
0
0
View all Tests
Test groups
Name
Tests failed
VM1-to-VM2-TestGrp
0% (0/1)
View more test groups
Test Configurations
Name
Tests failed
Sources
Name
Tests failed

f) Azure Backup

To set up Azure Backup, I followed these steps:

1. Recovery Services Vault Creation:

- I created a Recovery Services Vault with the following configurations:

Basics Tab:

- Resource Group: InsightScape-RG
- Vault Name: InsightScape-Vault
- Region:West US 2
- Used Default Settings for remaining configurations.
- After configuring these settings, I clicked on "Review + Create" to create the Recovery Services Vault.

2. Backup Item Configuration:

- After the successful deployment of the vault, I navigated to the Backup Items tab under Protected Items and selected "Azure Virtual Machine".
- I then proceeded to add a Backup Item.

Backup Goal:

- Where is your workload running? Azure
- What do you want to back up?: Virtual Machine
- After setting the backup goal, I clicked on "Backup".

3. Backup Configuration and Enabling Backup:

- To configure and enable the backup, I chose the following settings:

Policy Sub Type: Standard Backup Policy: DefaultPolicy

- I then proceeded to add the Virtual Machine:
- Virtual Machine: InsightScape-VM1
- After selecting the VM, I clicked on "Enable Backup".

4. Verification:

- After the successful deployment, I navigated back to the Backup Items tab, and InsightScape-VM1 was visible in the list of backup items.
- I selected InsightScape-VM1 and clicked on "Backup now" to trigger a manual backup.

5. Backup Jobs Verification:

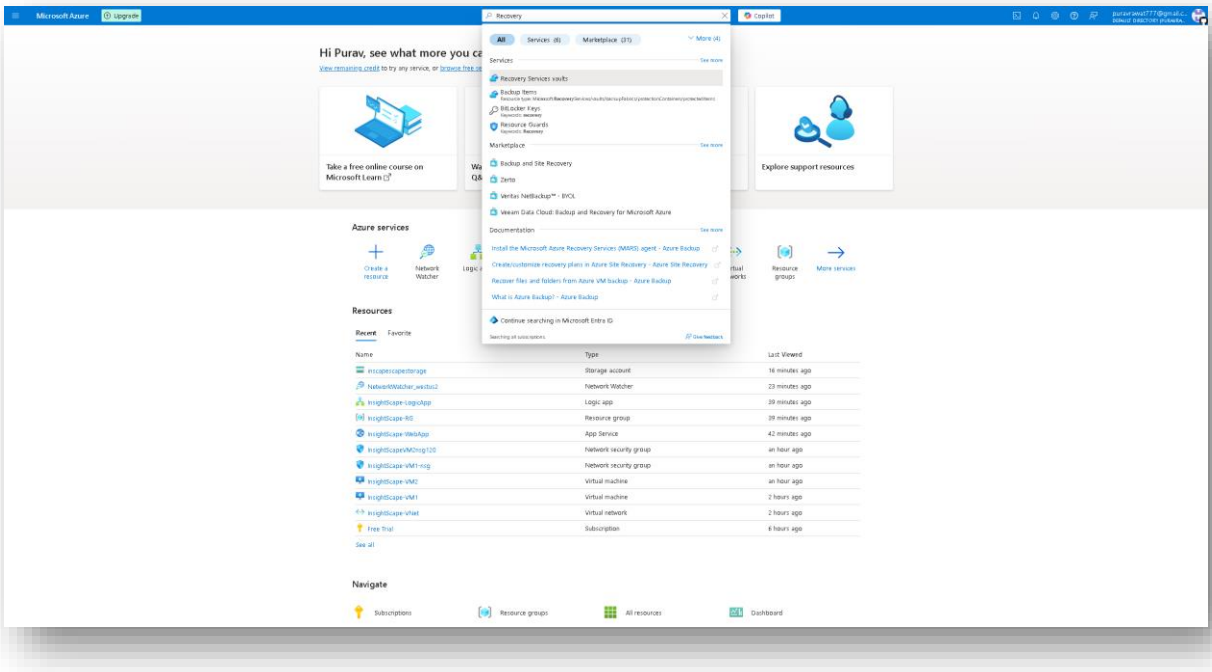
- To verify that the backup was successful, I accessed the Backup Jobs tab, where I could see two workload items for InsightScape-VM1:
    - InsightScape-VM1:
        - Operation: Backup

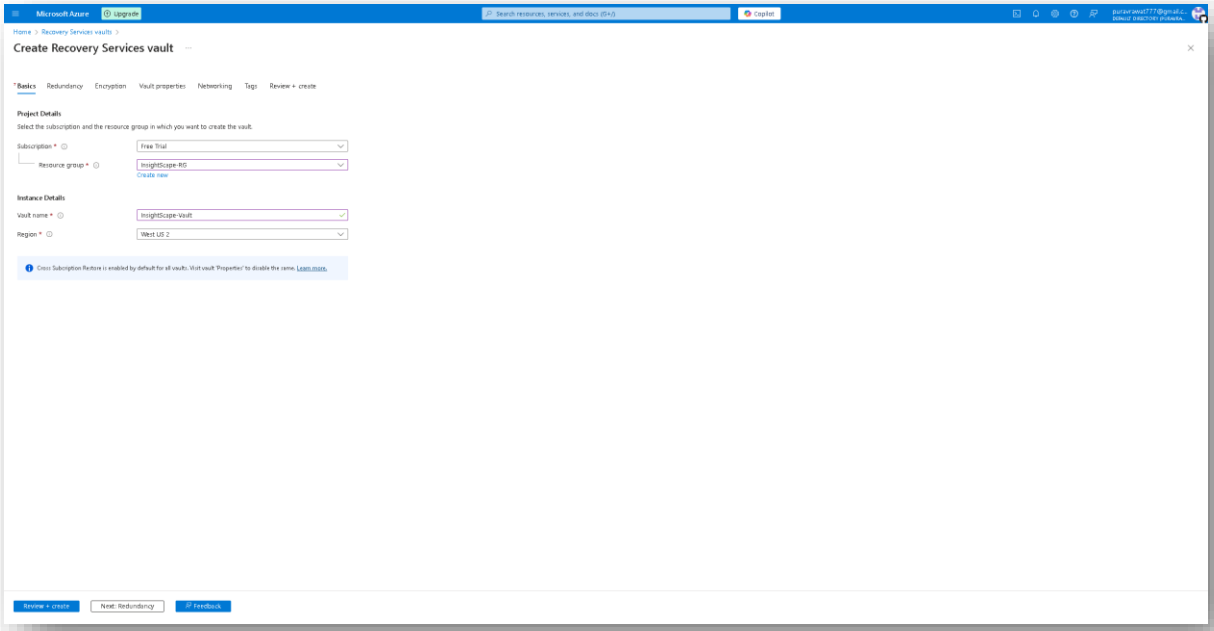
- Status: Completed (Green Tick)
- Type: Azure Virtual Machine
- Total Duration: 00:41:08

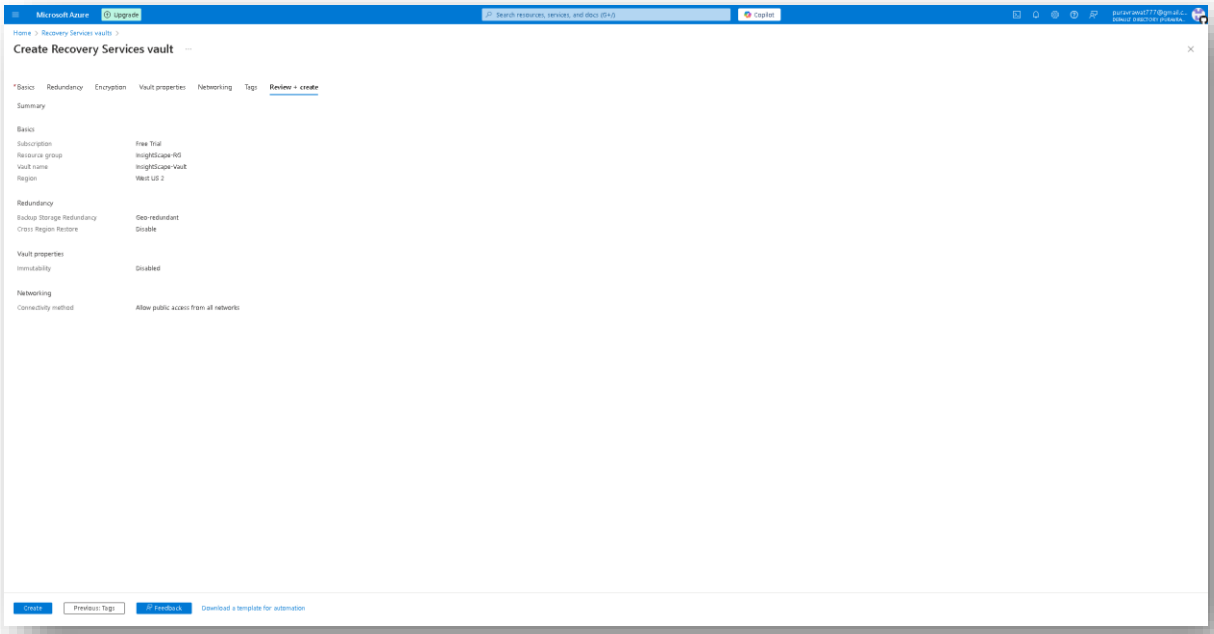
- InsightScape-VM1:
  - Operation: Configure Backup
  - Status: Completed (Green Tick)
  - Type: Azure Virtual Machine
  - Total Duration: 00:00:50

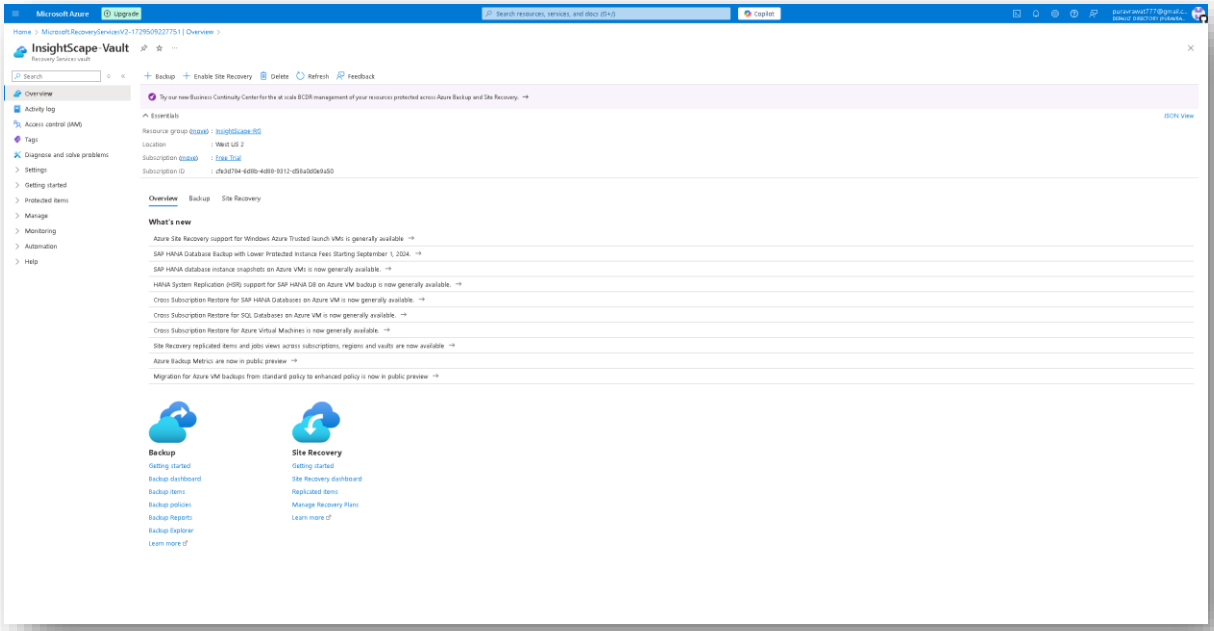
With this setup and verification, the Azure Backup for InsightScape-VM1 was successfully completed.

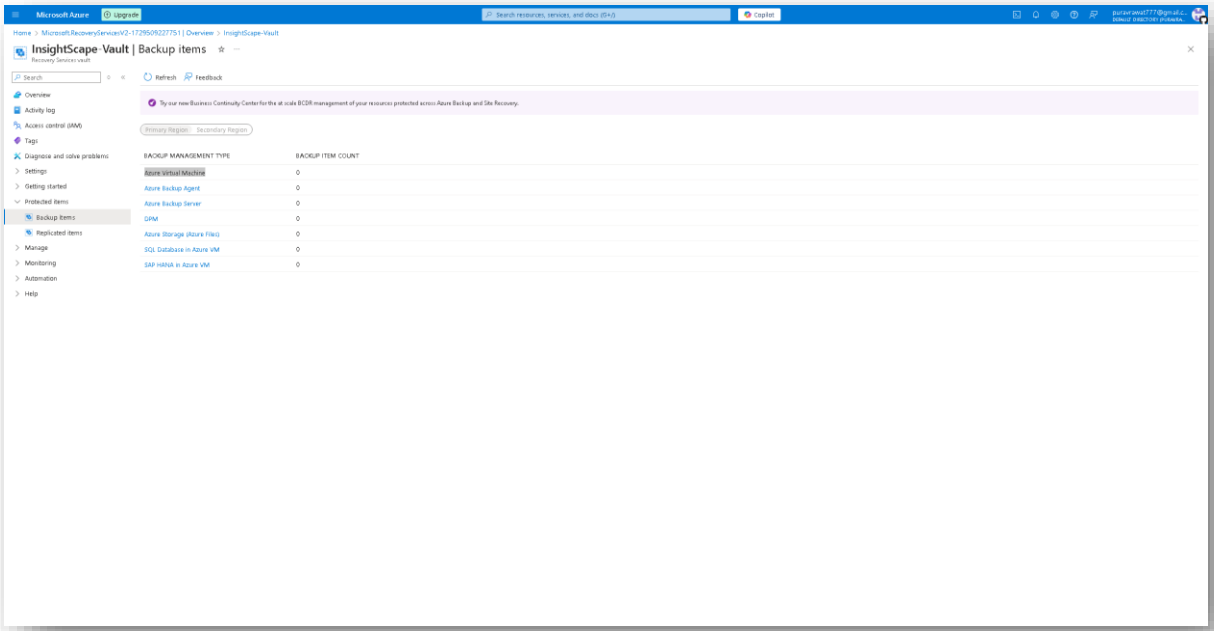
Screenshots -

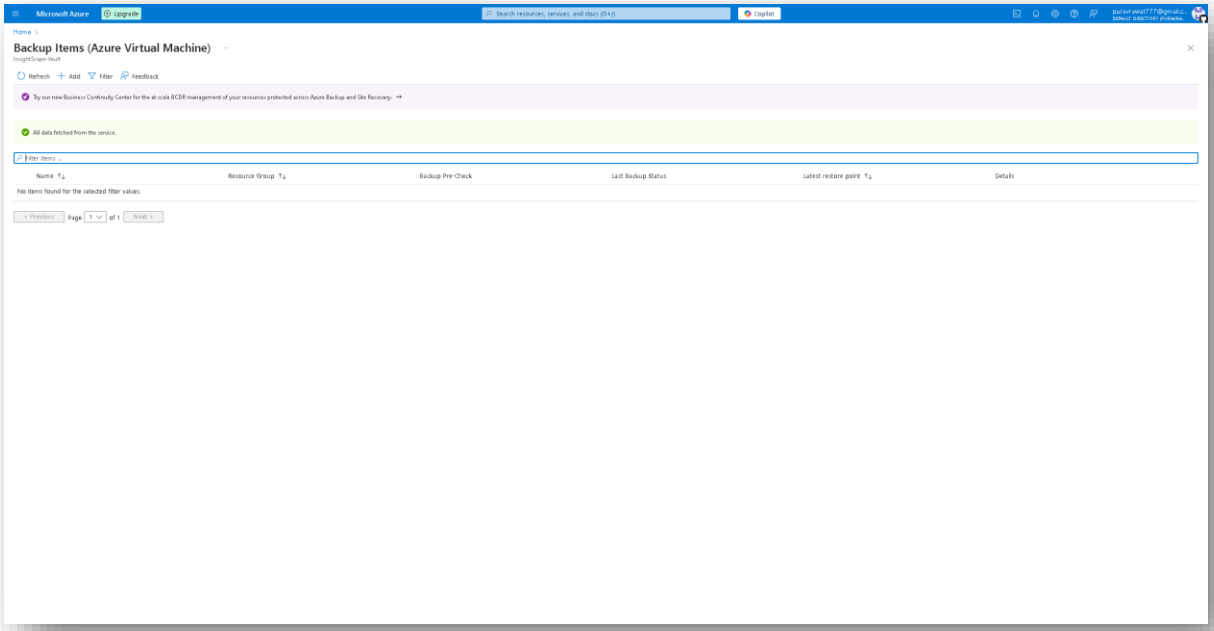


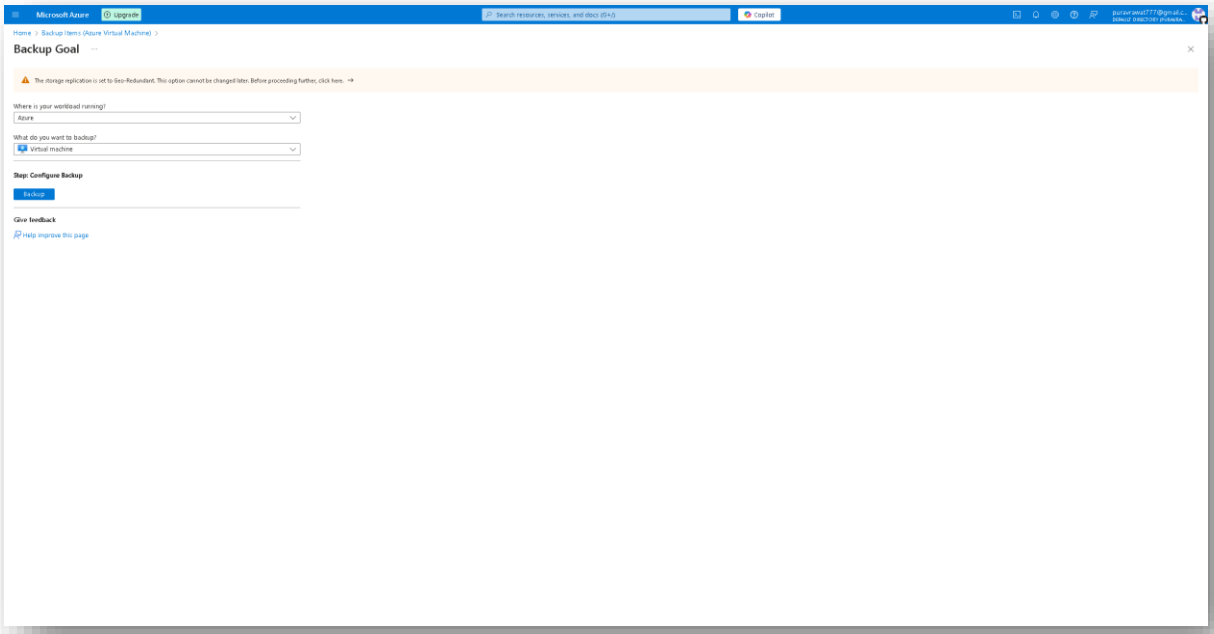

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Recovery Services vaults >
Create Recovery Services vault
*Basics Redundancy Encryption Vault properties Networking Tags Review + create
Project Details
Select the subscription and the resource group in which you want to create the vault.
Subscription *
Free Trial
Resource group *
InsightScape-RG
Create new
Instance Details
Vault name *
InsightScape-Vault
Region *
West US 2
Cross Subscription Restore is enabled by default for all vaults. Visit vault 'Properties' to disable the same. Learn more.
Review + create
Next: Redundancy
Feedback

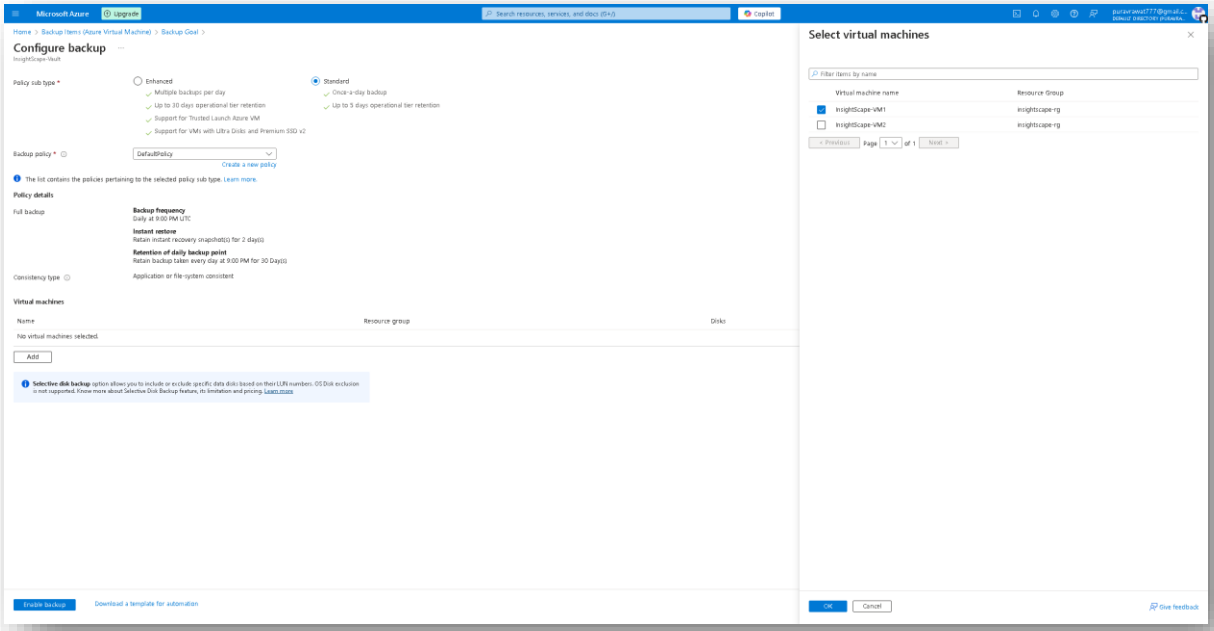

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Recovery Services vaults >
Create Recovery Services vault
*Basics Redundancy Encryption Vault properties Networking Tags Review + create
Summary
Basics
Subscription
Free Trial
Resource group
InsightScape-RG
Vault name
InsightScape-Vault
Region
West US 2
Redundancy
Backup Storage Redundancy
Geo-redundant
Cross Region Restore
Disable
Vault properties
Immutability
Disabled
Networking
Connectivity method
Allow public access from all networks
Create
Previous: Tags
Feedback
Download a template for automation

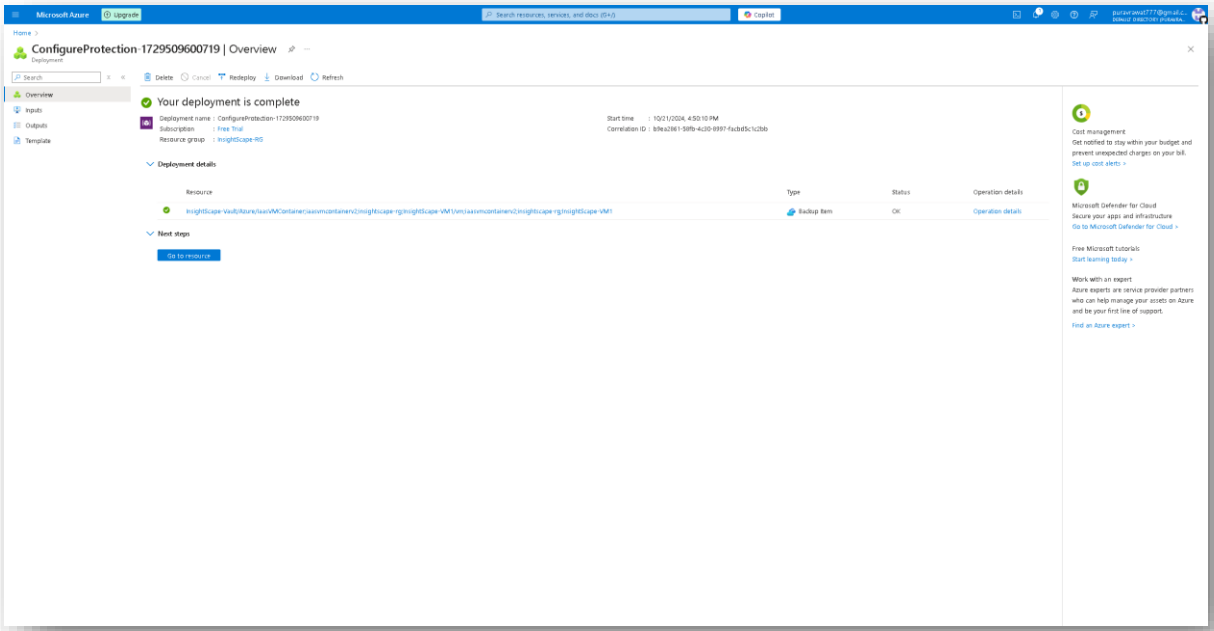

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft.RecoveryServicesV2-1729509227751 | Overview >
InsightScape-Vault
Recovery Services vault
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Getting started
Protected items
Manage
Monitoring
Automation
Help
Backup
Enable Site Recovery
Delete
Refresh
Feedback
Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery.
Essentials
JSON View
Resource group (move) : InsightScape-RG
Location : West US 2
Subscription (move) : Free Trial
Subscription ID : cfe3d784-6d0b-4d80-9312-c55a0d0e9a50
Overview
Backup
Site Recovery
What's new
Azure Site Recovery support for Windows Azure Trusted launch VMs is generally available.
SAP HANA Database Backup with Lower Protected Instance Fees Starting September 1, 2024.
SAP HANA database instance snapshots on Azure VMs is now generally available.
HANA System Replication (HSR) support for SAP HANA DB on Azure VM backup is now generally available.
Cross Subscription Restore for SAP HANA Databases on Azure VM is now generally available.
Cross Subscription Restore for SQL Databases on Azure VM is now generally available.
Cross Subscription Restore for Azure Virtual Machines is now generally available.
Site Recovery replicated items and jobs views across subscriptions, regions and vaults are now available
Azure Backup Metrics are now in public preview
Migration for Azure VM backups from standard policy to enhanced policy is now in public preview
Backup
Getting started
Backup dashboard
Backup items
Backup policies
Backup Reports
Backup Explorer
Learn more
Site Recovery
Getting started
Site Recovery dashboard
Replicated items
Manage Recovery Plans
Learn more

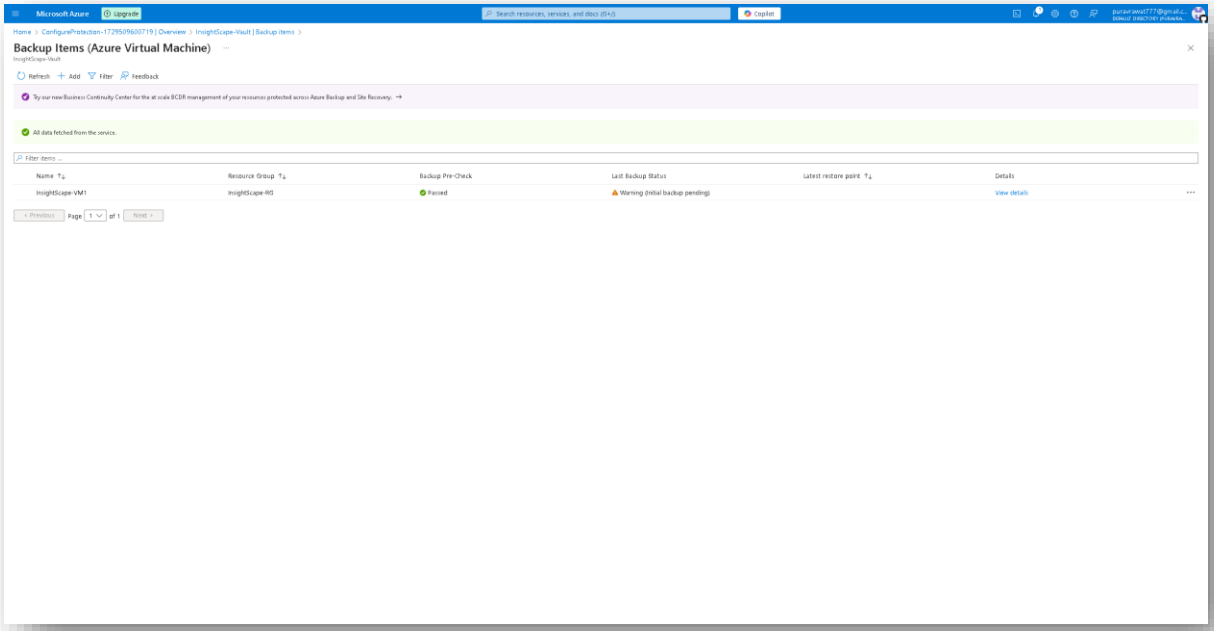

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft.RecoveryServicesV2-1729509227751 | Overview > InsightScape-Vault
InsightScape-Vault | Backup items
Recovery Services vault
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Getting started
Protected items
Backup items
Replicated items
Manage
Monitoring
Automation
Help
Refresh
Feedback
Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery.
Primary Region
Secondary Region
BACKUP MANAGEMENT TYPE
BACKUP ITEM COUNT
Azure Virtual Machine 0
Azure Backup Agent 0
Azure Backup Server 0
DPM 0
Azure Storage (Azure Files) 0
SQL Database in Azure VM 0
SAP HANA in Azure VM 0

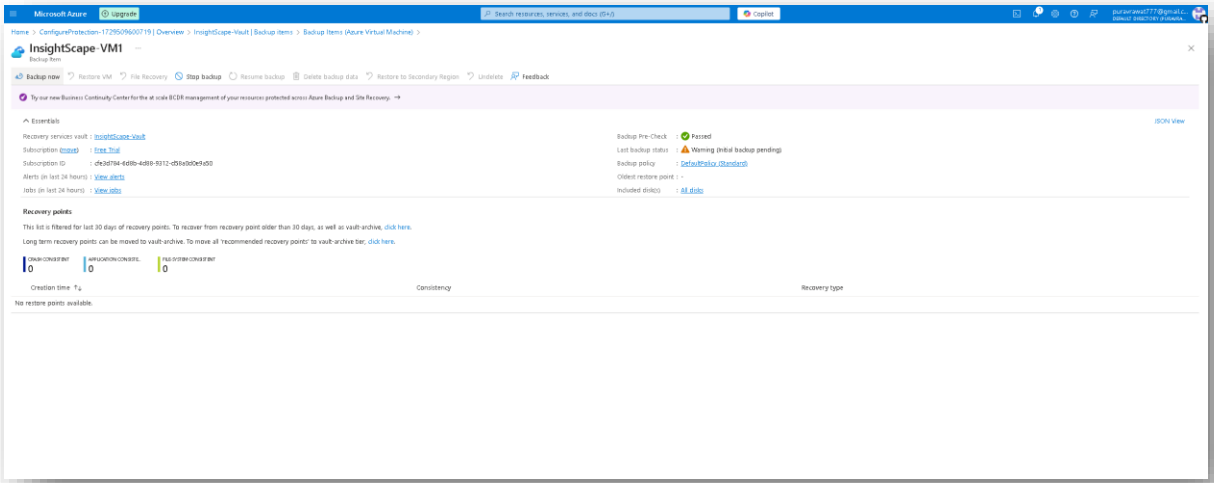

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home >
Backup Items (Azure Virtual Machine)
InsightScope-Vault
Refresh
Add
Filter
Feedback
Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery.
All data fetched from the service.
Filter items ...
Name
Resource Group
Backup Pre-Check
Last Backup Status
Latest restore point
Details
No items found for the selected filter values.
Previous
Page 1 of 1
Next

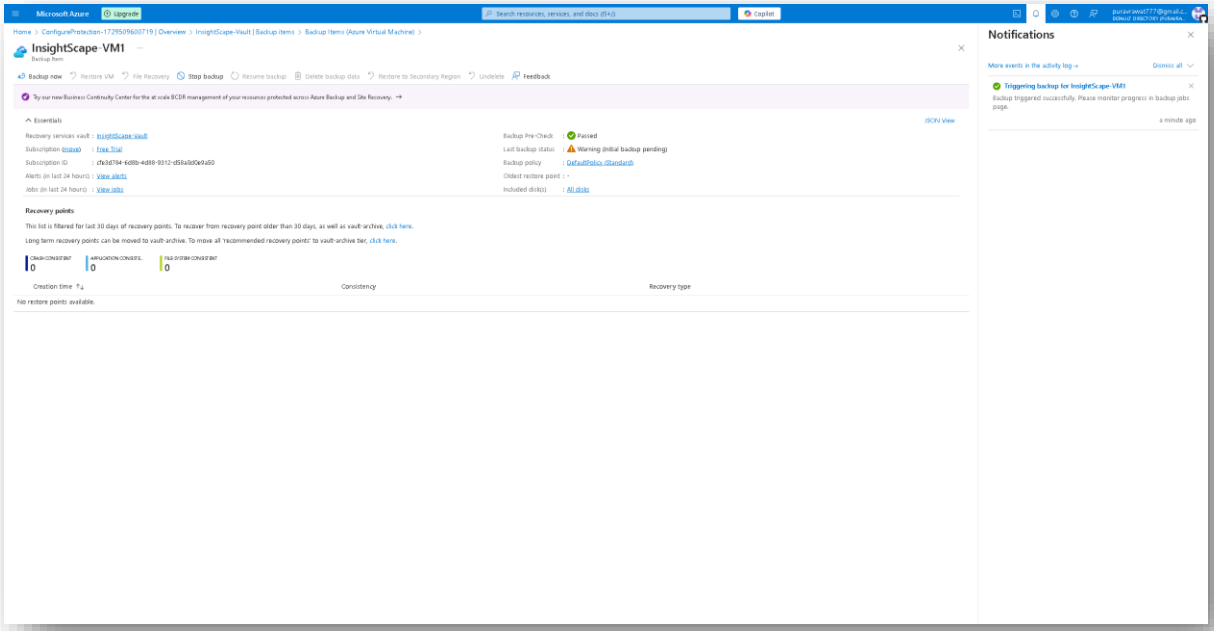

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Backup Items (Azure Virtual Machine) >
Backup Goal
The storage replication is set to Geo-Redundant. This option cannot be changed later. Before proceeding further, click here.
Where is your workload running?
Azure
What do you want to backup?
Virtual machine
Step: Configure Backup
Backup
Give feedback
Help improve this page

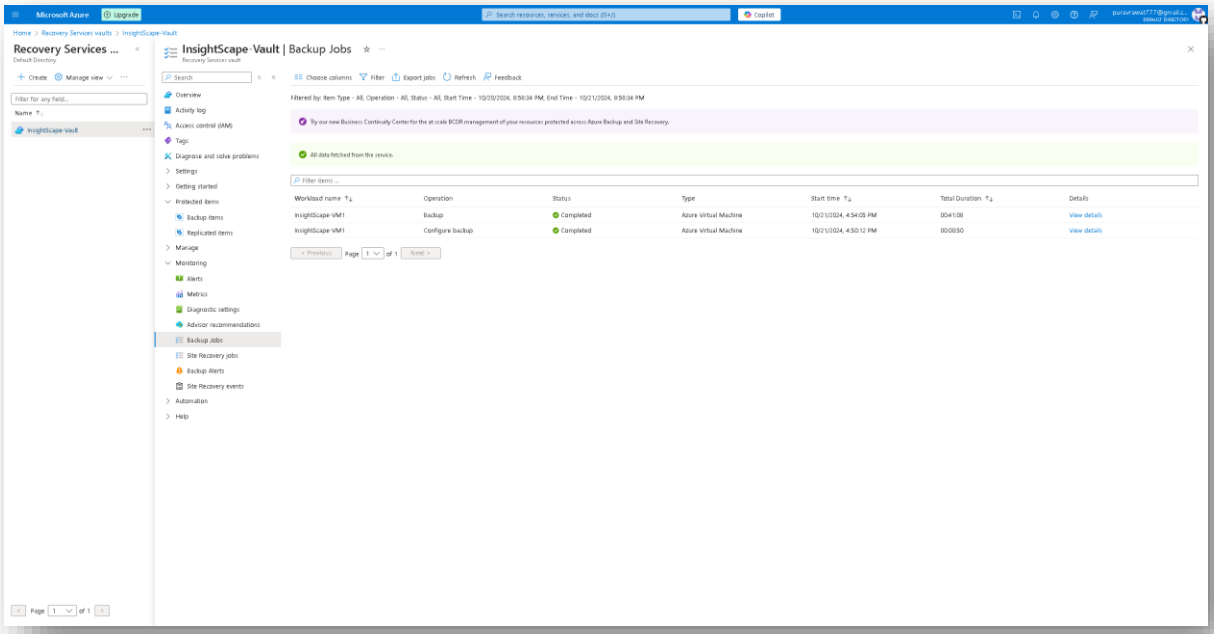

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Backup Items (Azure Virtual Machine) > Backup Goal >
Configure backup
InsightScape-Vault
Policy sub type *
Enhanced
Multiple backups per day
Up to 30 days operational tier retention
Support for Trusted Launch Azure VM
Support for VMs with Ultra Disks and Premium SSD v2
Standard
Once-a-day backup
Up to 5 days operational tier retention
Backup policy *
DefaultPolicy
Create a new policy
The list contains the policies pertaining to the selected policy sub type. Learn more.
Policy details
Full backup
Backup frequency
Daily at 9:00 PM UTC
Instant restore
Retain instant recovery snapshot(s) for 2 day(s)
Retention of daily backup point
Retain backup taken every day at 9:00 PM for 30 Day(s)
Consistency type
Application or file-system consistent
Virtual machines
Name
Resource group
Disks
No virtual machines selected.
Add
Selective disk backup option allows you to include or exclude specific data disks based on their LUN numbers. OS Disk exclusion is not supported. Know more about Selective Disk Backup feature, its limitation and pricing. Learn more
Enable backup
Download a template for automation
Select virtual machines
Filter items by name
Virtual machine name
Resource Group
InsightScape-VM1
insightscape-rg
InsightScape-VM2
insightscape-rg
< Previous
Page 1 of 1
Next >
OK
Cancel
Give feedback


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home >
ConfigureProtection-1729509600719 | Overview
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Your deployment is complete
Deployment name : ConfigureProtection-1729509600719
Subscription : Free Trial
Resource group : InsightScape-RG
Start time : 10/21/2024, 4:50:10 PM
Correlation ID : b9ea2661-98fb-4c30-8997-facbd5c1c2bb
Deployment details
Resource
Type
Status
Operation details
InsightScape-Vault/Azure/IaasVMContainer;iaasvmcontainerv2;insightscape-rg;InsightScape-VM1;vm;iaasvmcontainerv2;insightscape-rg;InsightScape-VM1
Backup Item
OK
Operation details
Next steps
Go to resource
Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > ConfigureProtection-1729509600719 | Overview > InsightScape-Vault | Backup items >
Backup Items (Azure Virtual Machine)
InsightScape-Vault
Refresh
Add
Filter
Feedback
Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery. →
All data fetched from the service.
Filter items ...
Name
Resource Group
Backup Pre-Check
Last Backup Status
Latest restore point
Details
InsightScape-VM1
InsightScape-RG
Passed
Warning (Initial backup pending)
View details
< Previous
Page 1 of 1
Next >


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > ConfigureProtection-1729509600719 | Overview > InsightScape-Vault | Backup items > Backup Items (Azure Virtual Machine) >
InsightScape-VM1
Backup Item
Backup now
Restore VM
File Recovery
Stop backup
Resume backup
Delete backup data
Restore to Secondary Region
Undelete
Feedback
Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery. →
Essentials
JSON View
Recovery services vault : InsightScape-Vault
Subscription (move) : Free Trial
Subscription ID : cfe3d784-6d8b-4d88-9312-d58a0d0e9a50
Alerts (in last 24 hours) : View alerts
Jobs (in last 24 hours) : View jobs
Backup Pre-Check : Passed
Last backup status : Warning (Initial backup pending)
Backup policy : DefaultPolicy (Standard)
Oldest restore point : -
Included disk(s) : All disks
Recovery points
This list is filtered for last 30 days of recovery points. To recover from recovery point older than 30 days, as well as vault-archive, click here.
Long term recovery points can be moved to vault-archive. To move all 'recommended recovery points' to vault-archive tier, click here.
CRASH-CONSISTENT
0
APPLICATION-CONSISTE...
0
FILE-SYSTEM-CONSISTENT
0
Creation time
Consistency
Recovery type
No restore points available.


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > ConfigureProtection-1729509600719 | Overview > InsightScape-Vault | Backup items > Backup Items (Azure Virtual Machine) >
InsightScape-VM1
Backup Item
Backup now
Restore VM
File Recovery
Stop backup
Resume backup
Delete backup data
Restore to Secondary Region
Undelete
Feedback
Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery. →
Essentials
JSON View
Recovery services vault : InsightScape-Vault
Subscription (move) : Free Trial
Subscription ID : cfe3d784-6d8b-4d88-9312-d5f8a9d0e9a50
Alerts (in last 24 hours) : View alerts
Jobs (in last 24 hours) : View jobs
Backup Pre-Check : Passed
Last backup status : Warning (Initial backup pending)
Backup policy : DefaultPolicy (Standard)
Oldest restore point : -
Included disk(s) : All disks
Recovery points
This list is filtered for last 30 days of recovery points. To recover from recovery point older than 30 days, as well as vault-archive, click here.
Long term recovery points can be moved to vault-archive. To move all 'recommended recovery points' to vault-archive tier, click here.
CRASH CONSISTENT
0
APPLICATION CONSISTE...
0
FILE-SYSTEM CONSISTENT
0
Creation time
Consistency
Recovery type
No restore points available.
Notifications
More events in the activity log →
Dismiss all
Triggering backup for InsightScape-VM1
Backup triggered successfully. Please monitor progress in backup jobs page.
a minute ago


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Recovery Services vaults > InsightScape-Vault
Recovery Services ...
Default Directory
Create
Manage view
Filter for any field...
Name
InsightScape-Vault
InsightScape-Vault | Backup Jobs
Recovery Services vault
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Getting started
Protected items
Backup items
Replicated items
Manage
Monitoring
Alerts
Metrics
Diagnostic settings
Advisor recommendations
Backup Jobs
Site Recovery jobs
Backup Alerts
Site Recovery events
Automation
Help
Choose columns
Filter
Export jobs
Refresh
Feedback
Filtered by: Item Type - All, Operation - All, Status - All, Start Time - 10/20/2024, 8:58:34 PM, End Time - 10/21/2024, 8:58:34 PM
Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery.
All data fetched from the service.
Filter items ...
Workload name
Operation
Status
Type
Start time
Total Duration
Details
InsightScape-VM1
Backup
Completed
Azure Virtual Machine
10/21/2024, 4:54:05 PM
00:41:08
View details
InsightScape-VM1
Configure backup
Completed
Azure Virtual Machine
10/21/2024, 4:50:12 PM
00:00:50
View details
< Previous
Page 1 of 1
Next >

Azure Monitor Integration

1) Monitoring Setup for Deployed Resources

For this phase of the project, I started by navigating to Azure Monitor to configure monitoring for my deployed resources.

Virtual Machines Monitoring Setup:

- First, I clicked on the Virtual Machines tab under Insights in Azure Monitor.
- On the Get Started page, I selected the "Configure Insights" option and enabled monitoring configurations for both InsightScape-VM1 and InsightScape-VM2.
- To enable monitoring, I created a new Data Collection Rule and selected the Default Log Analytics Workspace for both VMs.

After the successful deployment of VM Insights for both VMs, I proceeded with the "Analyze data" option on the Get Started page under the Virtual Machines tab in Azure Monitor.

Upon clicking Analyze Data, I was taken to the Performance Page in Virtual Machines under Azure Monitor, where I could see various Top N Charts for metrics like CPU Utilization %, Available Memory, Bytes Sent Rate, Bytes Received Rate, and Logical Disk Space Used % for both VMs.

Setting Up Alerts for VMs:

The last part of integrating Azure Monitor with the VMs was to set up alerts.

- To configure alerts, I went to the Alerts tab in Azure Monitor and clicked on "+ Create Alert Rule".

Alert Configuration for InsightScape-VM1:

- Scope Tab:
  - Selected InsightScape-VM1 as the resource.
- Conditions Tab:
  - Signal Name: Percentage CPU
  - Alert Logic:
    - Threshold: Static
    - Aggregation Type: Average
    - Operator: Greater than
    - Threshold Value: 50
  - When to Evaluate:
    - Check Every: 1 Minute
    - Lookback Period: 1 Minute

- Actions Tab:
    - Used Quick Actions with the following details:
        - Action Group Name: InsightScape-AlertGroup
        - Display Name: CPUUsageAlrt
        - Actions: Email
    - Entered my email address and clicked on Save.
- Details Tab:
    - Resource Group: InsightScape-RG
    - Severity: 2 - Warning
    - Alert Rule Name: High CPU Usage Alert for VM1

After configuring the alert, I clicked on "Review + Create", and the alert was successfully created. Shortly after, I received an email saying, "You're now in the CPUUsageAlrt action group."

Testing the Alert:

For my case, testing the alert was straightforward I purposely selected a Virtual Machine with only 1 GB of RAM. This allowed me to easily simulate high CPU usage by simply opening the Task Manager and the Settings app simultaneously, which quickly pushed the CPU usage above 90%, triggering the alert.

However, another method to test the alert would be:

- RDP into InsightScape-VM1 and opened Windows PowerShell.
- run the following command to put a load on the CPU:

```
while ($true) {
Start-Process taskmgr.exe
Start-Sleep -Milliseconds 100;
Stop-Process -Name taskmgr
}
```

- As expected the CPU Utilization percentage will shot more than 90%
- To check if the alert was triggered, you go to the Alerts tab in Azure Monitor.
- There, you will see the Alert Condition: Fired, and shortly afterward, you will receive an alert email confirming the alert had been fired, along with a summary of the alert metrics.

This verified that the alert was successfully set up. I did not create any more alerts at this stage, as I had already planned a later phase called "Alerts Configuration"

Azure Monitor Integration for Web App:

- After setting up the VM monitoring, I proceeded with Azure Monitor integration for the Web App.

- I navigated to the Application Insights tab under Settings in InsightScape-WebApp and made sure it was enabled.
- Then, I went to Applications under Insights in Azure Monitor, where InsightScapeWebApp was listed.
- In the Overview section, I could see metrics such as Failed Requests, Server Response Time, Server Requests, and Availability for the Web App.
- I did not make any additional configurations in Application Insights at this stage, as I had already planned to cover this in a later phase called "Application Insights".

Azure Monitor Integration for Logic App:

- Moving on, I integrated Azure Monitor with InsightScape-LogicApp.
- I went to Diagnostics Settings under Monitoring in InsightScape-LogicApp and added a Diagnostic Setting with the following configurations:
    - Diagnostic Setting Name: LogicApp-Diagnostics

    Logs:

    - allLogs (Ticked)

    Metrics:

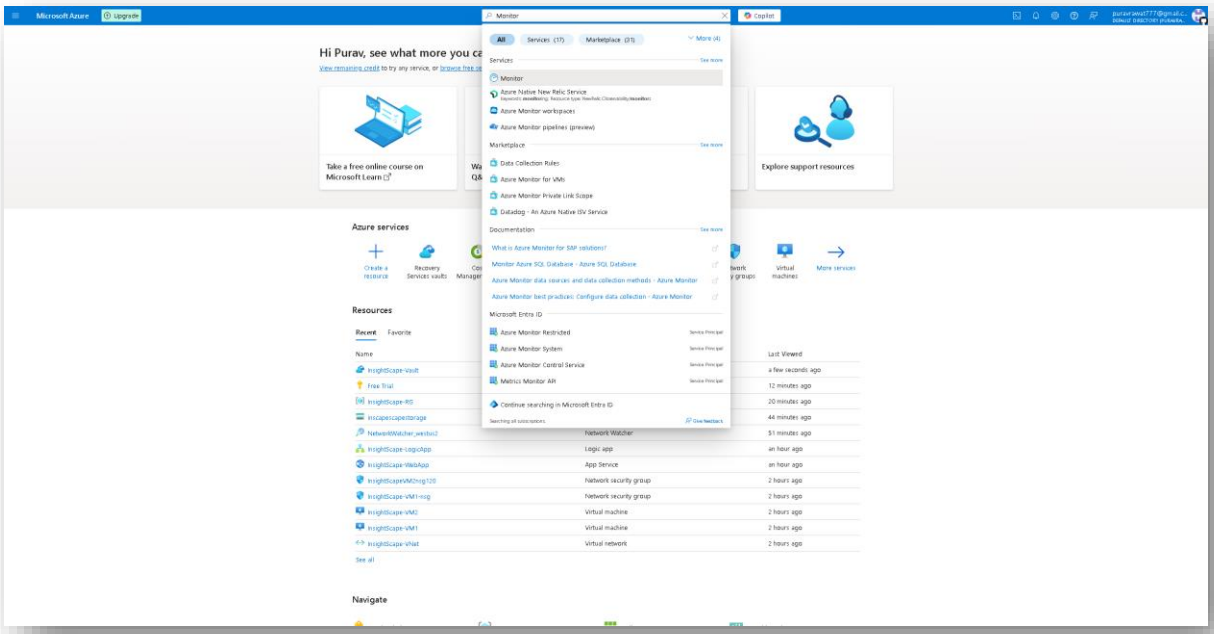
    - AllMetrics (Ticked)

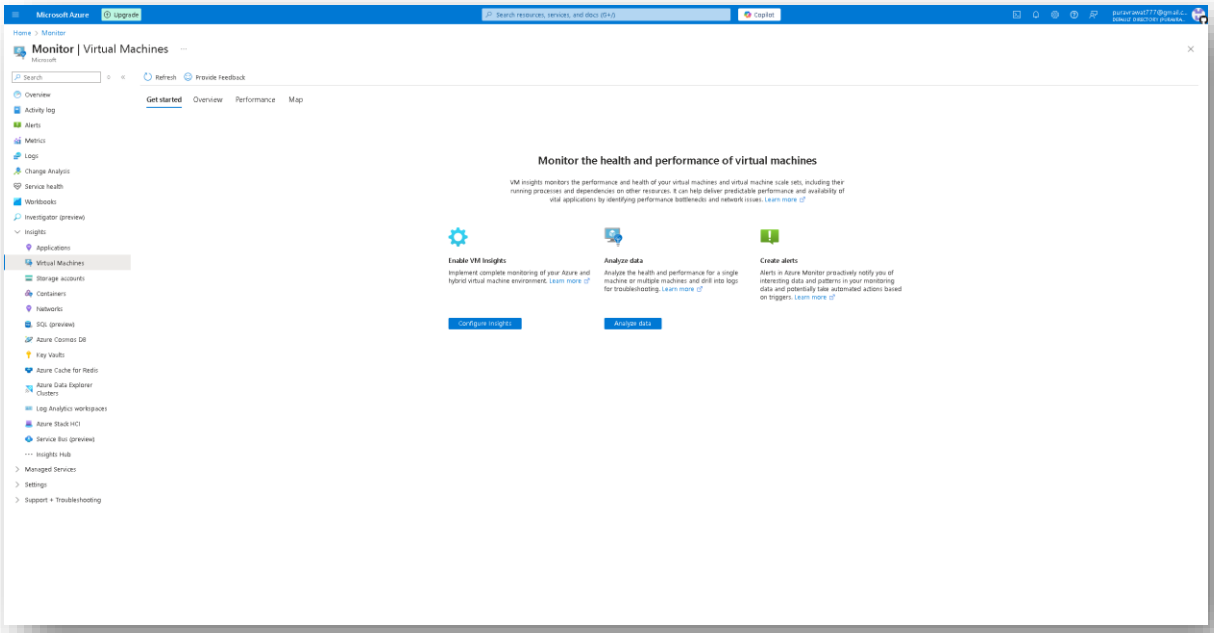
    Destination Details:

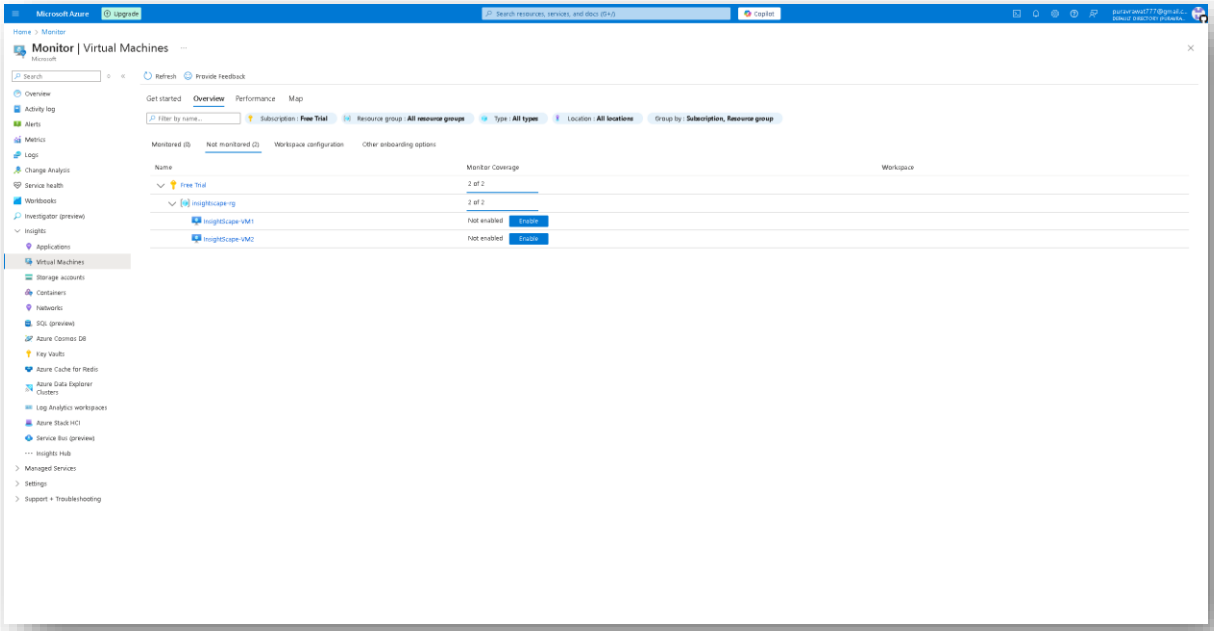
    - Send to Log Analytics Workspace (Ticked)
    - Log Analytics Workspace: Default Workspace.
- After completing the configuration, I saved the Diagnostic Settings.

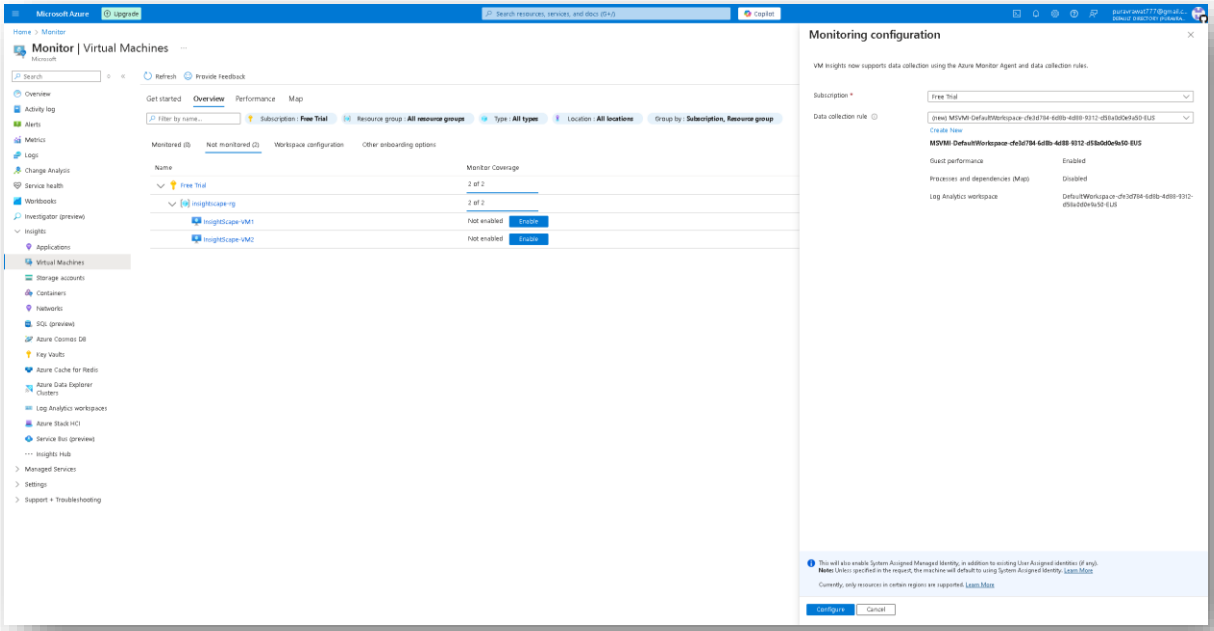
This completed the Monitoring Setup for Deployed Resources phase.

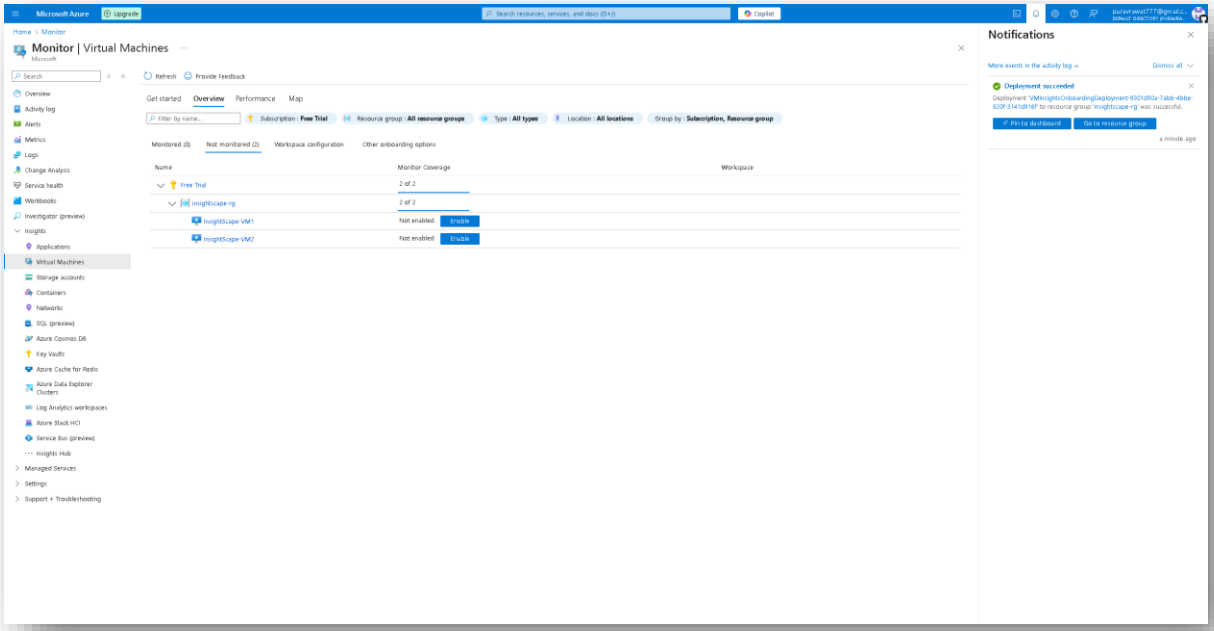
Screenshots-

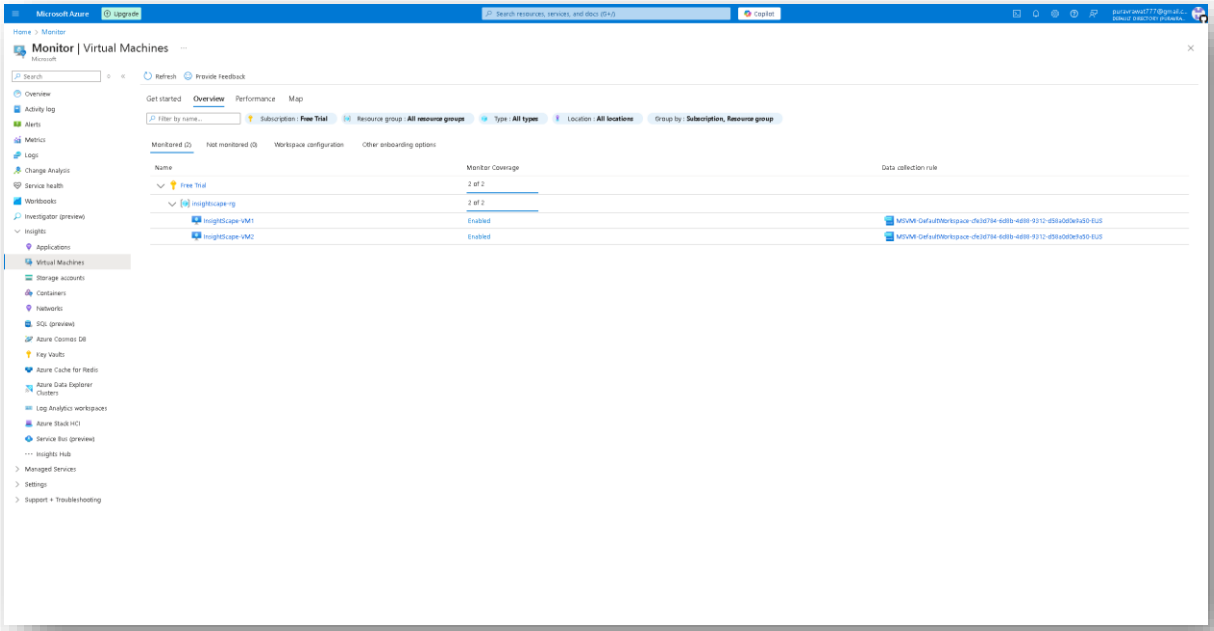


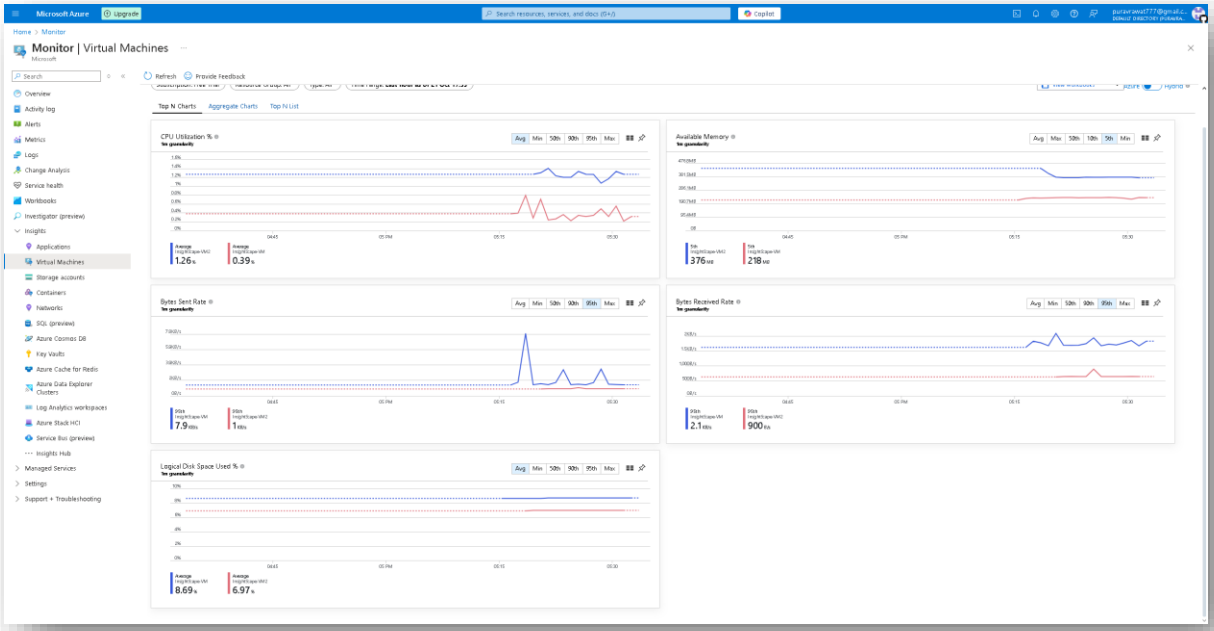


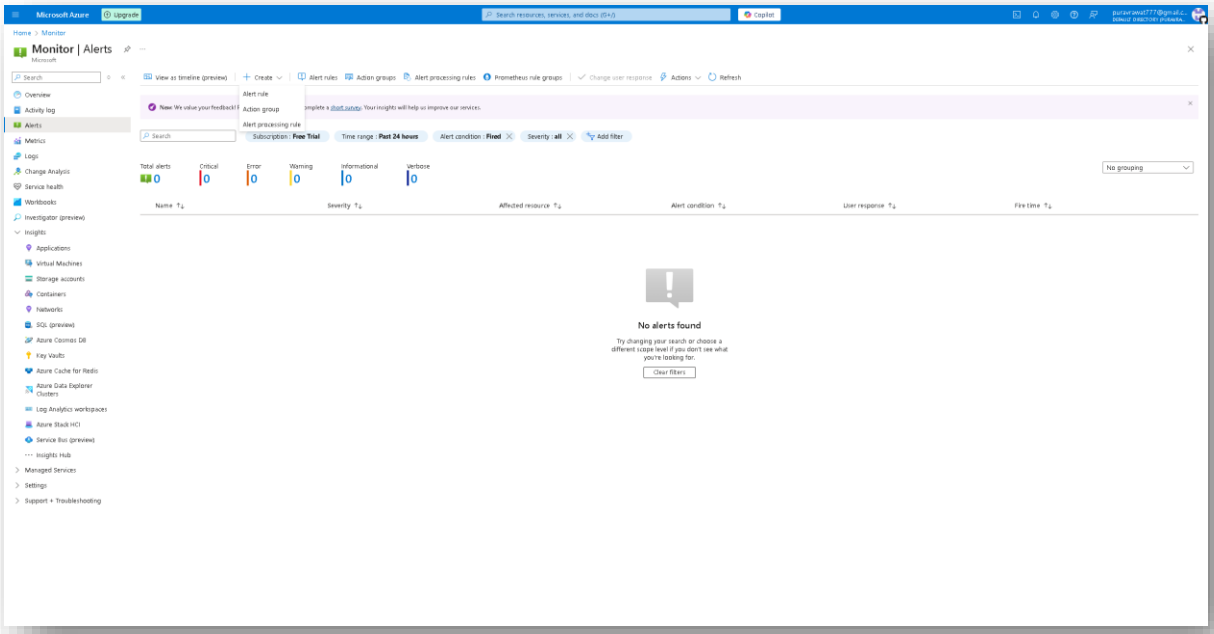

Microsoft Azure
Upgrade
Copilot
Home > Monitor
Monitor | Virtual Machines
Microsoft
Search
Refresh
Provide Feedback
Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Investigator (preview)
Insights
Applications
Virtual Machines
Storage accounts
Containers
Networks
SQL (preview)
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Azure Data Explorer Clusters
Log Analytics workspaces
Azure Stack HCI
Service Bus (preview)
Insights Hub
Managed Services
Settings
Support + Troubleshooting
Get started
Overview
Performance
Map
Filter by name...
Subscription : Free Trial
Resource group : All resource groups
Type : All types
Location : All locations
Group by : Subscription, Resource group
Monitored (0)
Not monitored (2)
Workspace configuration
Other onboarding options
Name
Monitor Coverage
Workspace
Free Trial
2 of 2
insightscape-rg
2 of 2
InsightScape-VM1
Not enabled
Enable
InsightScape-VM2
Not enabled
Enable

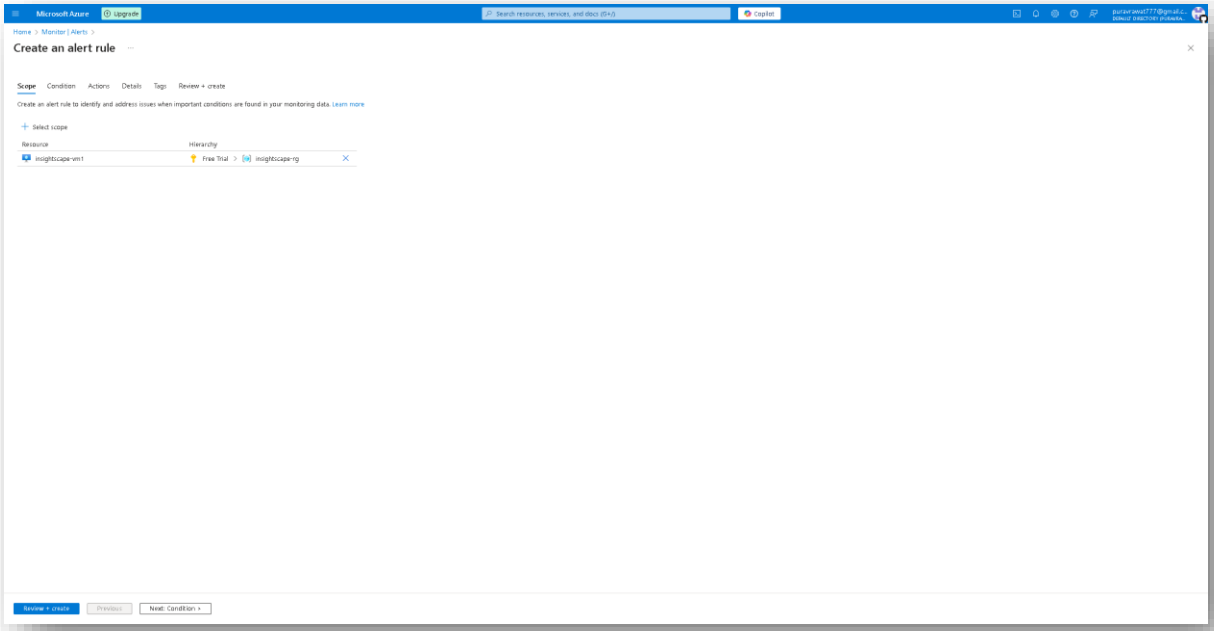

Microsoft Azure
Upgrade
Copilot
Home > Monitor
Monitor | Virtual Machines
Microsoft
Search
Refresh
Provide Feedback
Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Investigator (preview)
Insights
Applications
Virtual Machines
Storage accounts
Containers
Networks
SQL (preview)
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Azure Data Explorer Clusters
Log Analytics workspaces
Azure Stack HCI
Service Bus (preview)
Insights Hub
Managed Services
Settings
Support + Troubleshooting
Get started
Overview
Performance
Map
Filter by name...
Subscription : Free Trial
Resource group : All resource groups
Type : All types
Location : All locations
Group by : Subscription, Resource group
Monitored (0)
Not monitored (2)
Workspace configuration
Other onboarding options
Name
Monitor Coverage
Free Trial
2 of 2
insightscape-rg
2 of 2
InsightScape-VM1
Not enabled
Enable
InsightScape-VM2
Not enabled
Enable
Monitoring configuration
VM insights now supports data collection using the Azure Monitor Agent and data collection rules.
Subscription *
Free Trial
Data collection rule
Create New
Guest performance
Enabled
Processes and dependencies (Map)
Disabled
Log Analytics workspace
Configure
Cancel

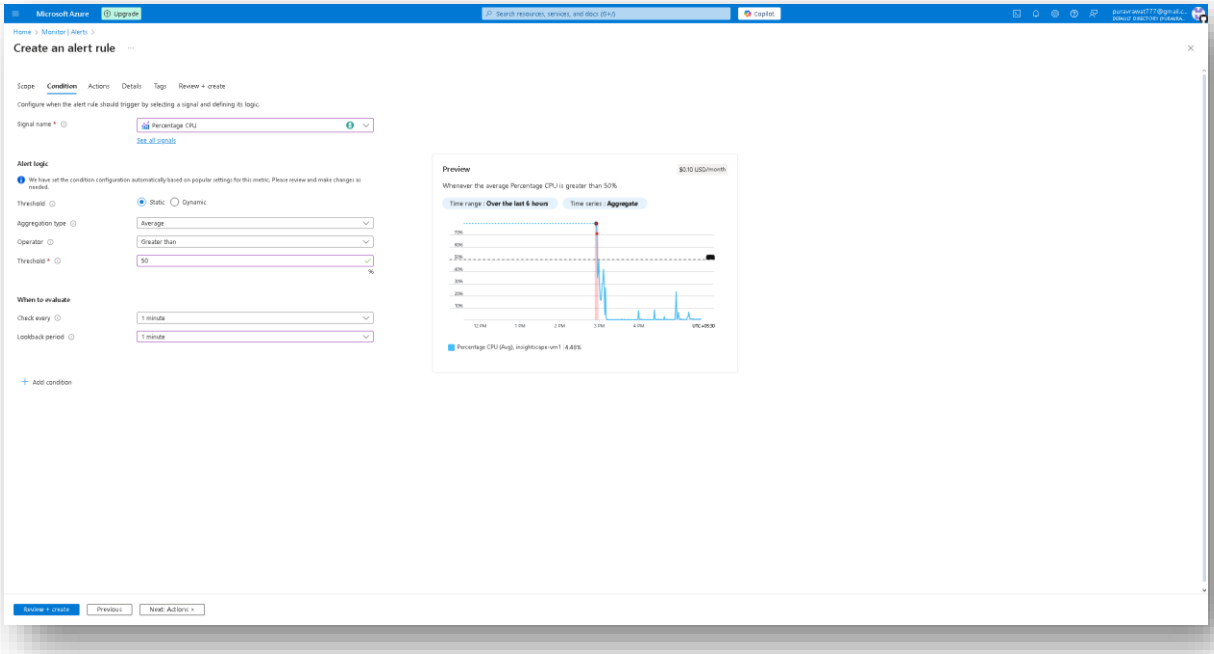

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor
Monitor | Virtual Machines
Microsoft
Search
Refresh
Provide Feedback
Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Investigator (preview)
Insights
Applications
Virtual Machines
Storage accounts
Containers
Networks
SQL (preview)
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Azure Data Explorer Clusters
Log Analytics workspaces
Azure Stack HCI
Service Bus (preview)
Insights Hub
Managed Services
Settings
Support + Troubleshooting
Get started
Overview
Performance
Map
Filter by name...
Subscription : Free Trial
Resource group : All resource groups
Type : All types
Location : All locations
Group by : Subscription, Resource group
Monitored (0)
Not monitored (2)
Workspace configuration
Other onboarding options
Name
Monitor Coverage
Workspace
Free Trial
2 of 2
insightscape-rg
2 of 2
InsightScape-VM1
Not enabled
Enable
InsightScape-VM2
Not enabled
Enable
Notifications
More events in the activity log →
Dismiss all
Deployment succeeded
Deployment 'VMInsightsOnboardingDeployment-9301d90a-7abb-4bbe-820f-3141d916f' to resource group 'insightscape-rg' was successful.
Pin to dashboard
Go to resource group
a minute ago

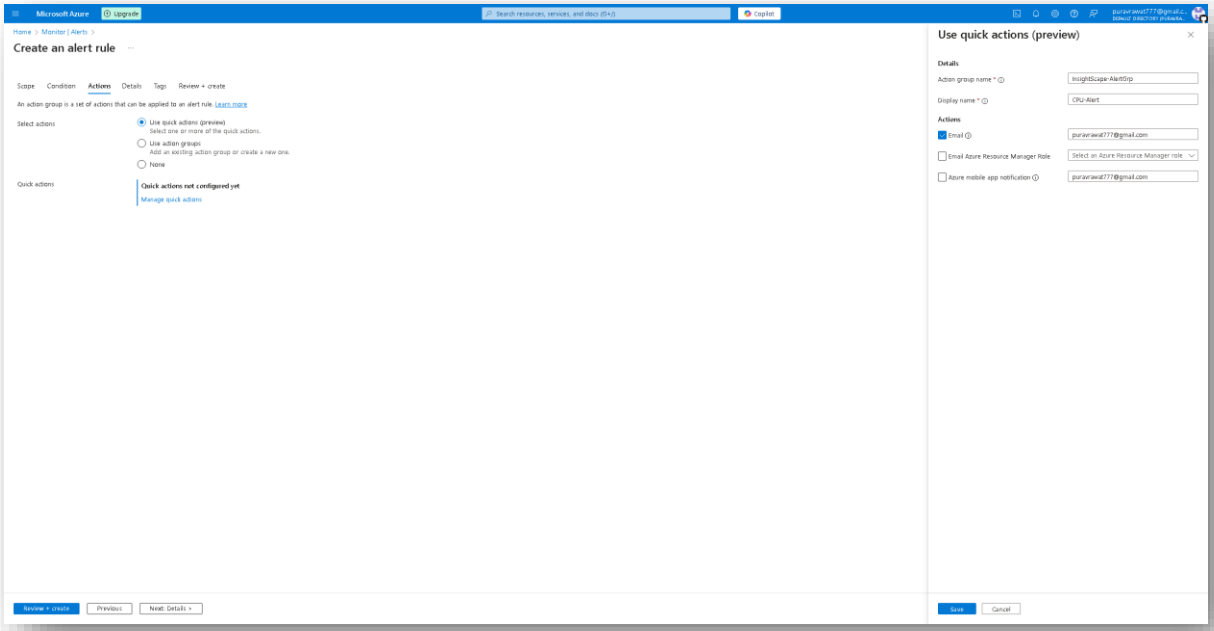

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor
Monitor | Virtual Machines
Microsoft
Search
Refresh
Provide Feedback
Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Investigator (preview)
Insights
Applications
Virtual Machines
Storage accounts
Containers
Networks
SQL (preview)
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Azure Data Explorer Clusters
Log Analytics workspaces
Azure Stack HCI
Service Bus (preview)
Insights Hub
Managed Services
Settings
Support + Troubleshooting
Get started
Overview
Performance
Map
Filter by name...
Subscription : Free Trial
Resource group : All resource groups
Type : All types
Location : All locations
Group by : Subscription, Resource group
Monitored (2)
Not monitored (0)
Workspace configuration
Other onboarding options
Name
Monitor Coverage
Data collection rule
Free Trial
2 of 2
insightscape-rg
2 of 2
InsightScape-VM1
Enabled
MSVMI-DefaultWorkspace-cfe3d794-6d8b-4d88-9312-d58a0d0efa50-EUS
InsightScape-VM2
Enabled
MSVMI-DefaultWorkspace-cfe3d794-6d8b-4d88-9312-d58a0d0efa50-EUS

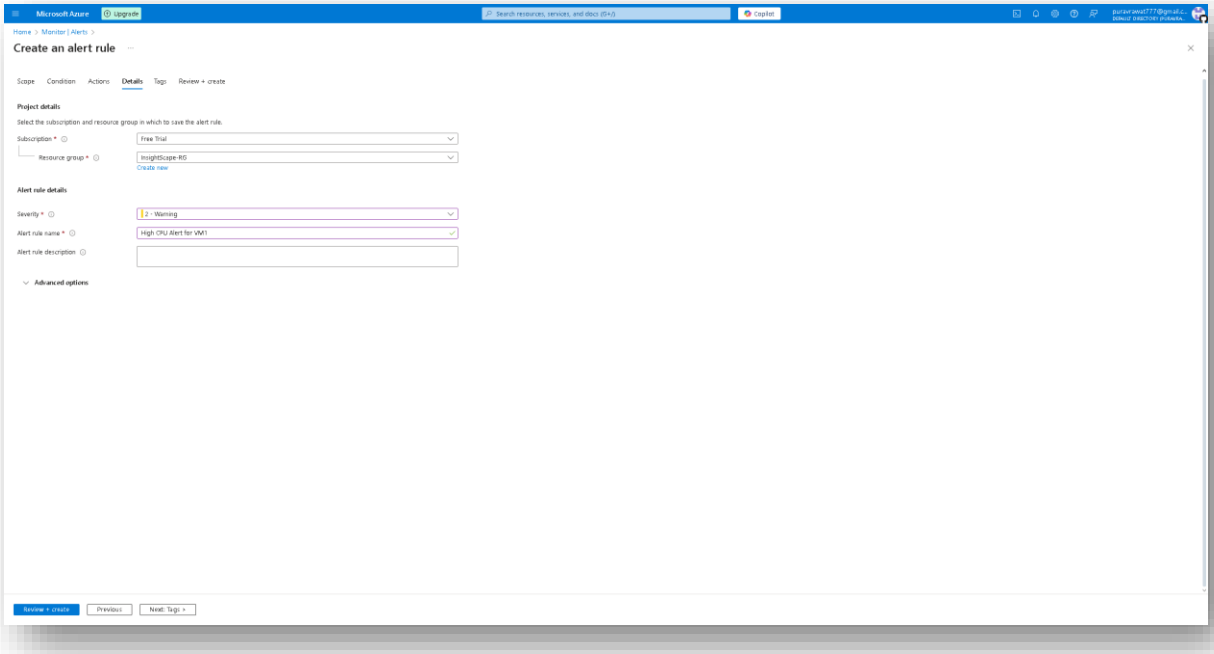

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor
Monitor | Virtual Machines
Microsoft
Search
Refresh
Provide Feedback
Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Investigator (preview)
Insights
Applications
Virtual Machines
Storage accounts
Containers
Networks
SQL (preview)
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Azure Data Explorer Clusters
Log Analytics workspaces
Azure Stack HCI
Service Bus (preview)
Insights Hub
Managed Services
Settings
Support + Troubleshooting
Top N Charts
Aggregate Charts
Top N List
CPU Utilization %
Avg Min 50th 90th 95th Max
1.26
0.39
Available Memory
Avg Max 50th 10th 5th Min
376
218
Bytes Sent Rate
Avg Min 50th 90th 95th Max
7.9
1
Bytes Received Rate
Avg Min 50th 90th 95th Max
2.1
900
Logical Disk Space Used %
Avg Min 50th 90th 95th Max
8.69
6.97

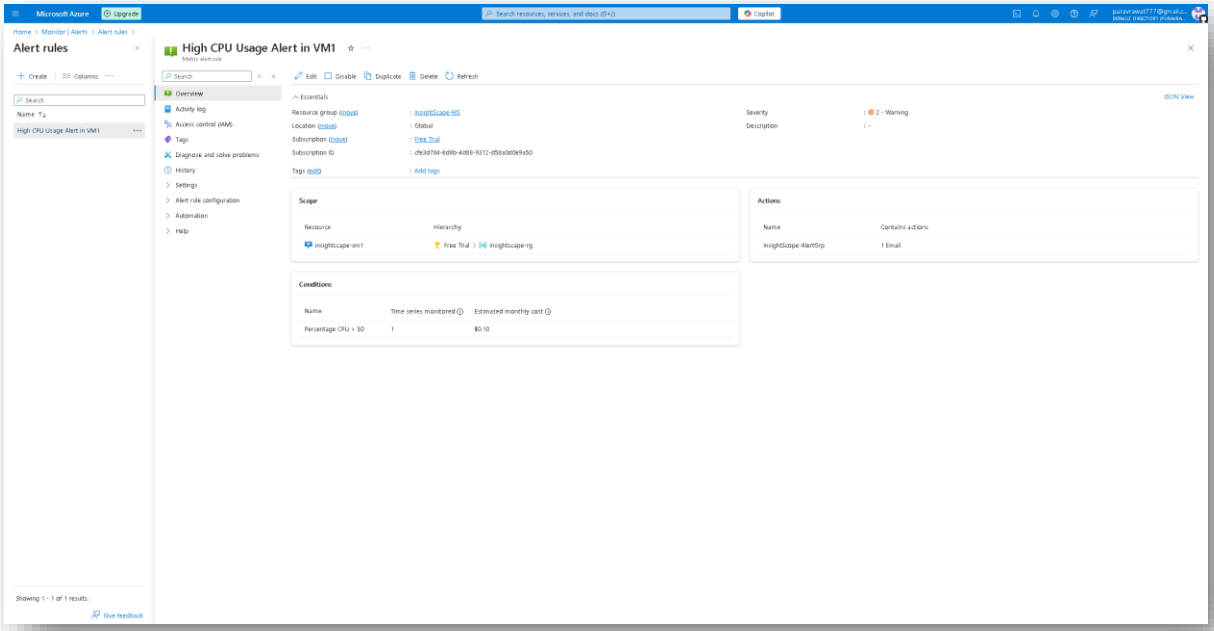

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor
Monitor | Alerts
Microsoft
Search
View as timeline (preview)
Create
Alert rules
Action groups
Alert processing rules
Prometheus rule groups
Change user response
Actions
Refresh
Alert rule
Action group
Alert processing rule
Subscription : Free Trial
Time range : Past 24 hours
Alert condition : Fired
Severity : all
Add filter
Total alerts
Critical
Error
Warning
Informational
Verbose
0
No grouping
Name
Severity
Affected resource
Alert condition
User response
Fire time
No alerts found
Try changing your search or choose a different scope level if you don't see what you're looking for.
Clear filters

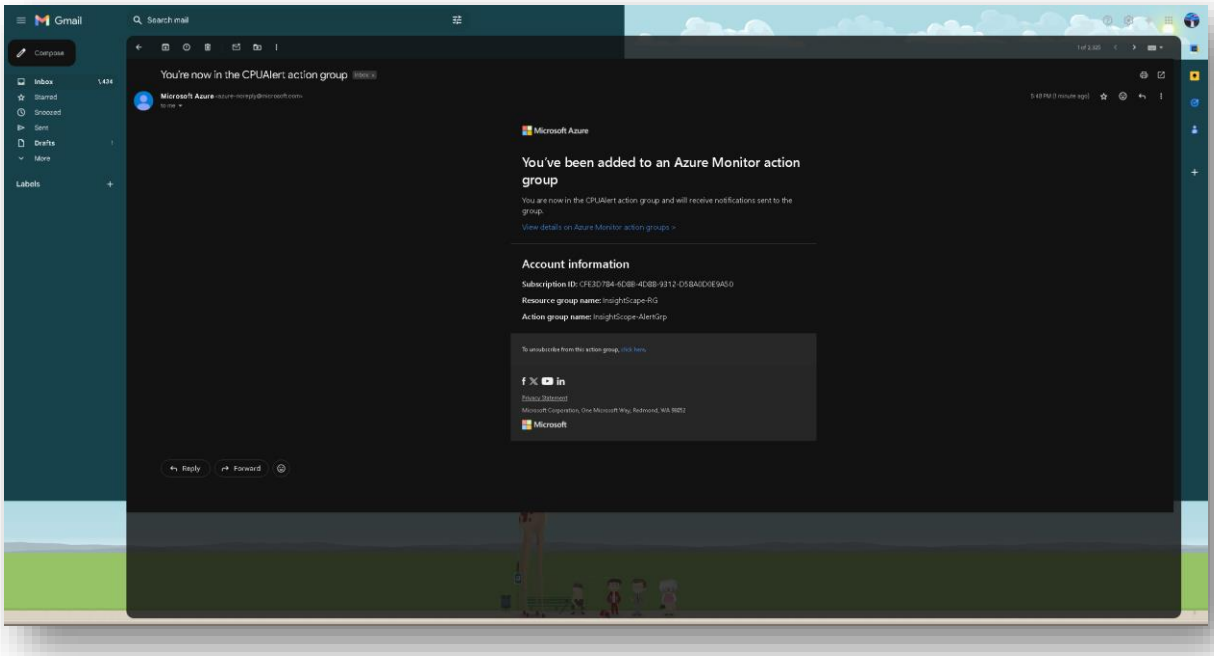

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor | Alerts >
Create an alert rule
Scope
Condition
Actions
Details
Tags
Review + create
Create an alert rule to identify and address issues when important conditions are found in your monitoring data. Learn more
Select scope
Resource
Hierarchy
insightscape-vm1
Free Trial > insightscape-rg
Review + create
Previous
Next: Condition >

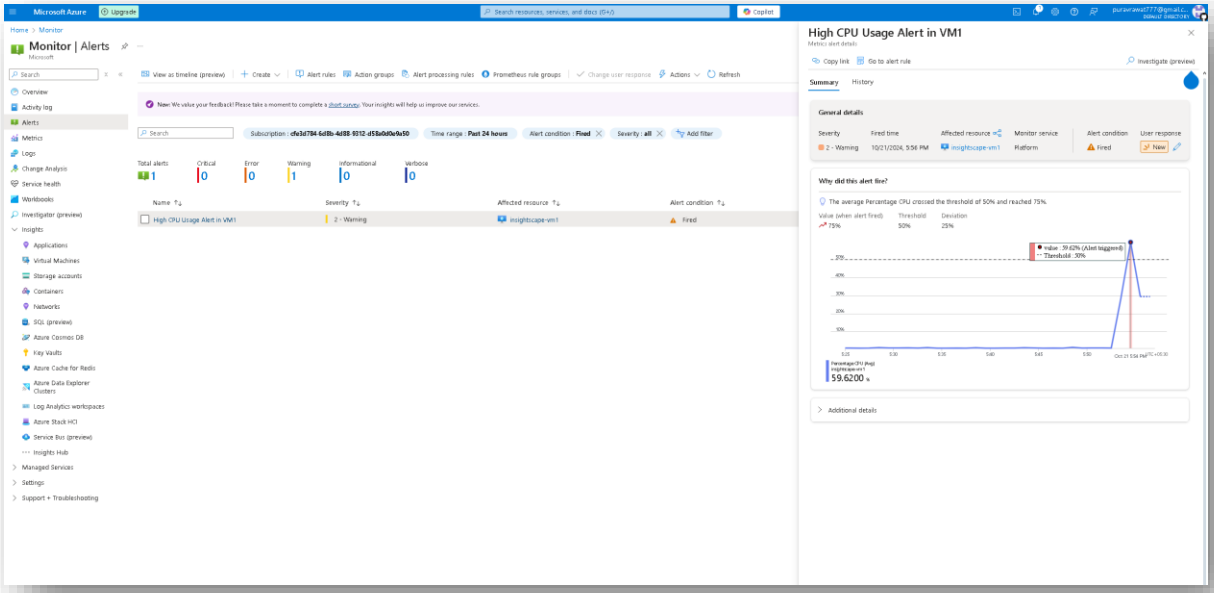

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor | Alerts >
Create an alert rule
Scope
Condition
Actions
Details
Tags
Review + create
Configure when the alert rule should trigger by selecting a signal and defining its logic.
Signal name *
Percentage CPU
See all signals
Alert logic
We have set the condition configuration automatically based on popular settings for this metric. Please review and make changes as needed.
Threshold
Static
Dynamic
Aggregation type
Average
Operator
Greater than
Threshold *
50
%
When to evaluate
Check every
1 minute
Lookback period
1 minute
Add condition
Preview
$0.10 USD/month
Whenever the average Percentage CPU is greater than 50%
Time range : Over the last 6 hours
Time series : Aggregate
Percentage CPU (Avg), insightscape-vm1
Review + create
Previous
Next: Actions >

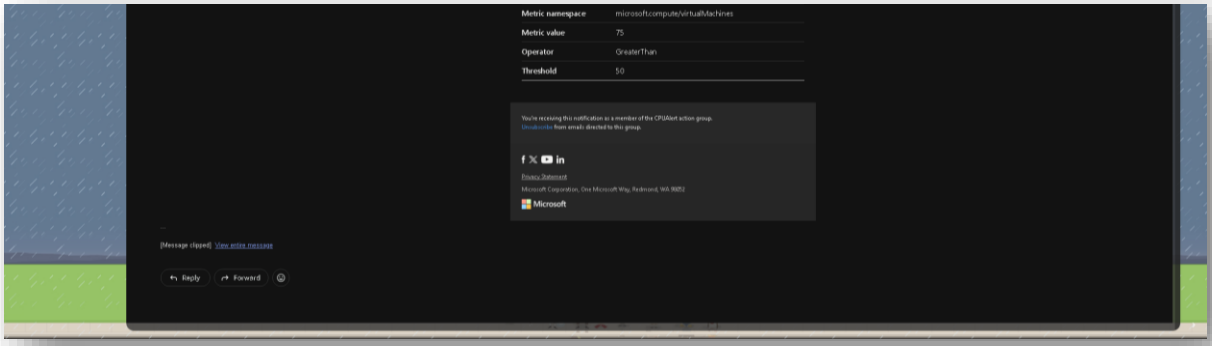

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor | Alerts >
Create an alert rule
Scope
Condition
Actions
Details
Tags
Review + create
An action group is a set of actions that can be applied to an alert rule. Learn more
Select actions
Use quick actions (preview)
Select one or more of the quick actions.
Use action groups
Add an existing action group or create a new one.
None
Quick actions
Quick actions not configured yet
Manage quick actions
Review + create
Previous
Next: Details >
Use quick actions (preview)
Details
Action group name *
InsightScape-AlertGrp
Display name *
CPU-Alert
Actions
Email
Email Azure Resource Manager Role
Select an Azure Resource Manager role
Azure mobile app notification
Save
Cancel

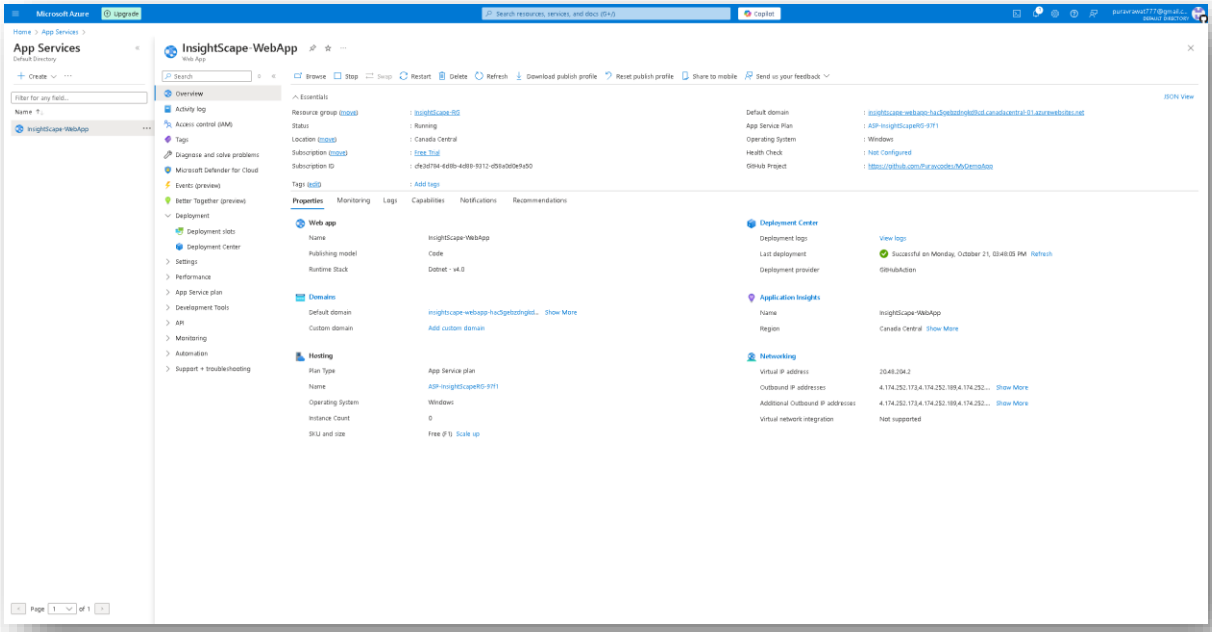

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor | Alerts >
Create an alert rule
Scope
Condition
Actions
Details
Tags
Review + create
Project details
Select the subscription and resource group in which to save the alert rule.
Subscription *
Free Trial
Resource group *
InsightScape-RG
Create new
Alert rule details
Severity *
2 - Warning
Alert rule name *
High CPU Alert for VM1
Alert rule description
Advanced options
Review + create
Previous
Next: Tags >

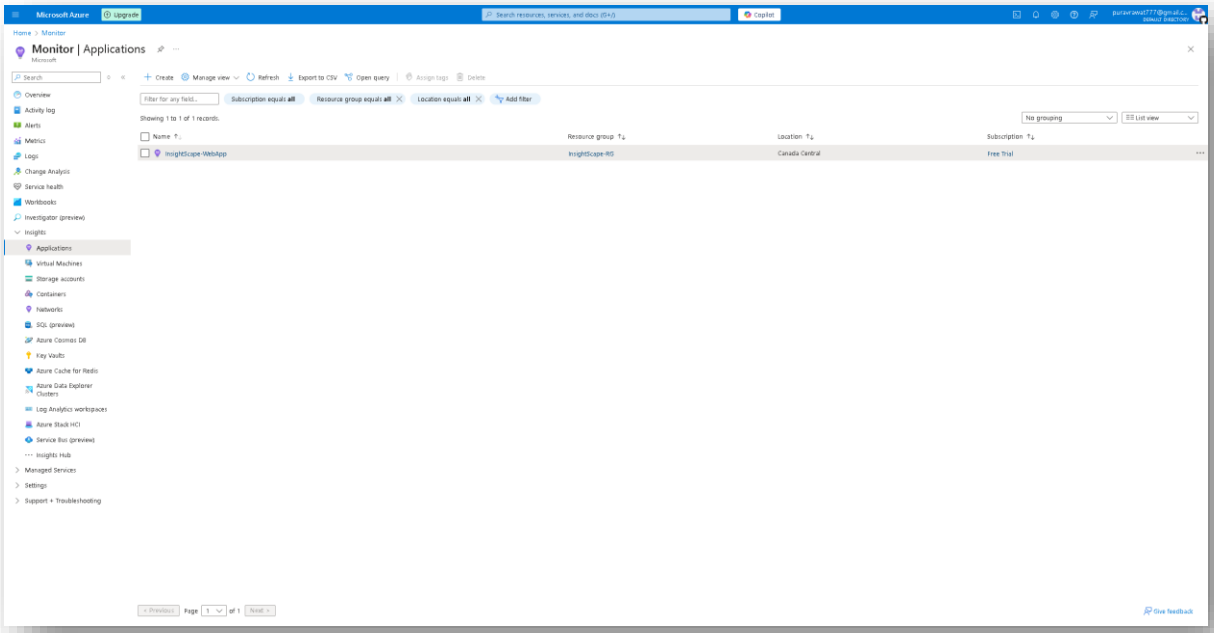

Microsoft Azure
Upgrade
Copilot
Alert rules
Create
Columns
Name
High CPU Usage Alert in VM1
Showing 1 - 1 of 1 results.
Give feedback
High CPU Usage Alert in VM1
Metric alert rule
Edit
Disable
Duplicate
Delete
Refresh
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
History
Settings
Alert rule configuration
Automation
Help
Essentials
JSON View
Resource group (move) : InsightScape-RG
Location (move) : Global
Subscription (move) : Free Trial
Subscription ID : cfe3d7b4-6d8b-4d88-9312-d58a0d0e9a50
Tags (edit) : Add tags
Severity : 2 - Warning
Description : -
Scope
Resource
Hierarchy
insightscape-vm1
Free Trial > insightscape-rg
Actions
Name
Contains actions
InsightScope-AlertGrp
1 Email
Conditions
Name
Time series monitored
Estimated monthly cost
Percentage CPU > 50
1
$0.10

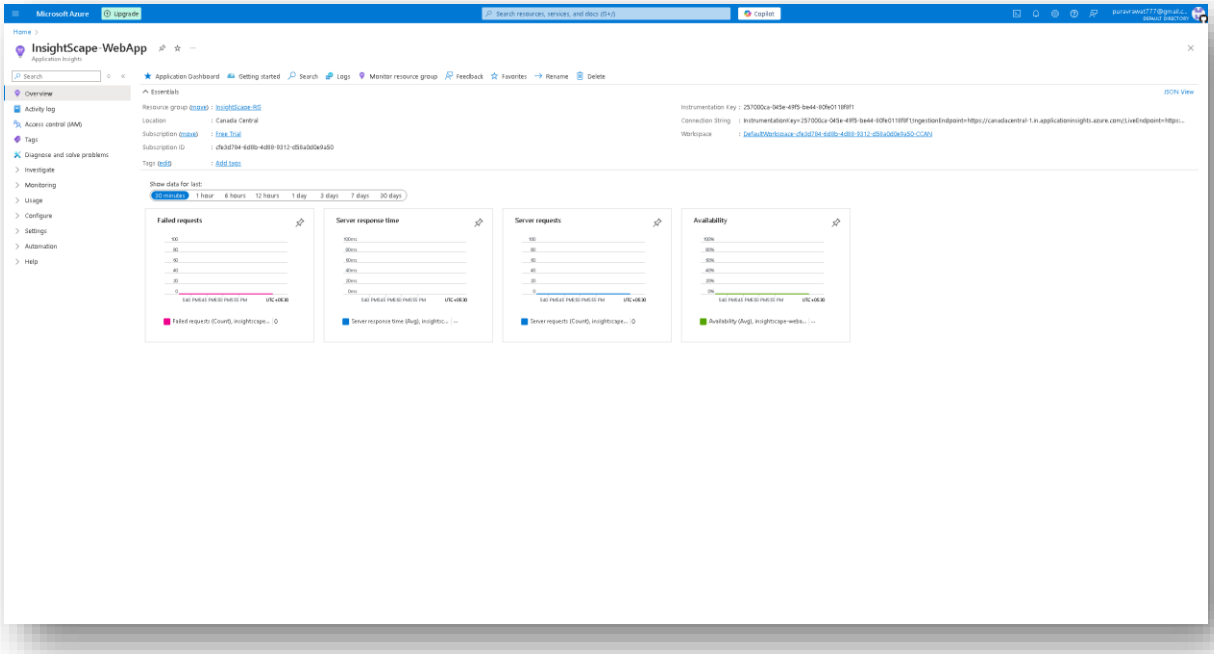

Gmail
Search mail
Compose
Inbox
Starred
Snoozed
Sent
Drafts
More
Labels
You're now in the CPUAlert action group
Microsoft Azure
You've been added to an Azure Monitor action group
You are now in the CPUAlert action group and will receive notifications sent to the group.
View details on Azure Monitor action groups >
Account information
Subscription ID: CFE3D7B4-6D8B-4D88-9312-D58A0D0E9A50
Resource group name: InsightScape-RG
Action group name: InsightScope-AlertGrp
To unsubscribe from this action group, click here.
Privacy Statement
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052
Microsoft
Reply
Forward

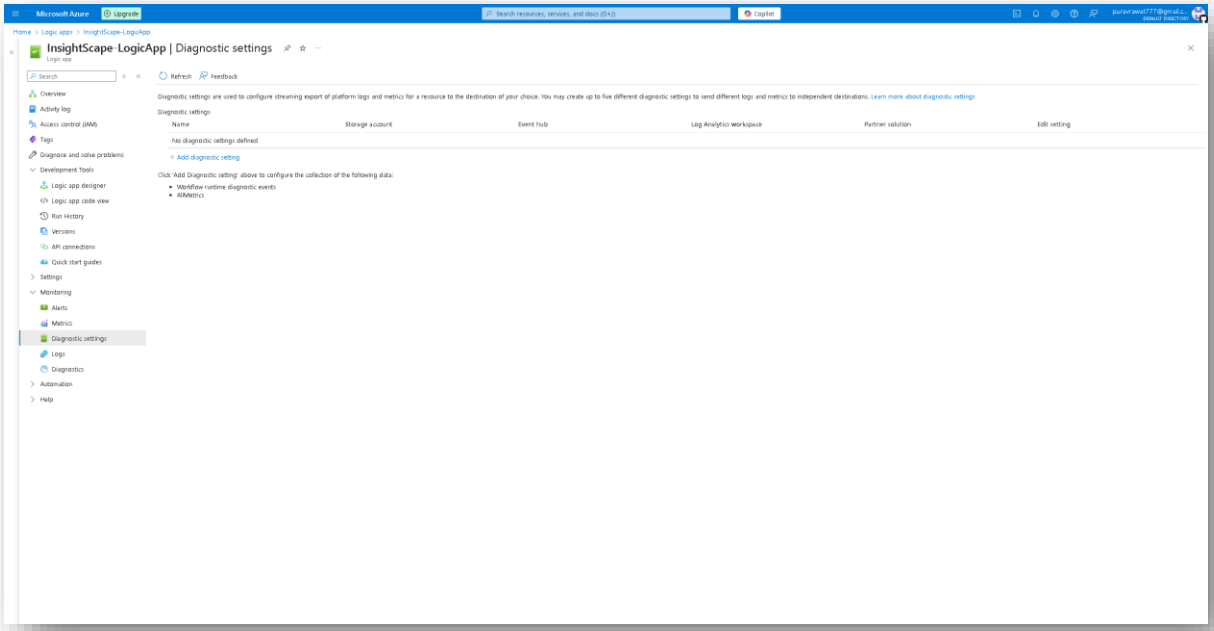

Monitor | Alerts
High CPU Usage Alert in VM1
Fired:Sev2 Azure Monitor Alert High CPU Usage Alert in VM1 on insightscape-vm1 (microsoft.compute/virtualmachines) at 10/21/2024 12:26:43 PM
Microsoft Azure
Fired:Sev2 Azure Monitor Alert High CPU Usage Alert in VM1 on insightscape-vm1 (microsoft.compute/virtualmachines) at 10/21/2024 12:26:43 PM
View the alert in Azure Monitor >
Investigate >
Summary
Alert name
High CPU Usage Alert in VM1
Severity
Sev2
Monitor condition
Fired
Affected resource
insightscape-vm1
Resource type
microsoft.compute/virtualmachines
Resource group
insightscape-rg
Monitoring service
Platform
Signal type
Metric
Fired time
October 21, 2024 12:26 UTC
Alert ID
Alert rule ID
Metric alert condition type
MultipleResourceMultipleMetricCriteria
Time aggregation
Average
Metric name
Percentage CPU

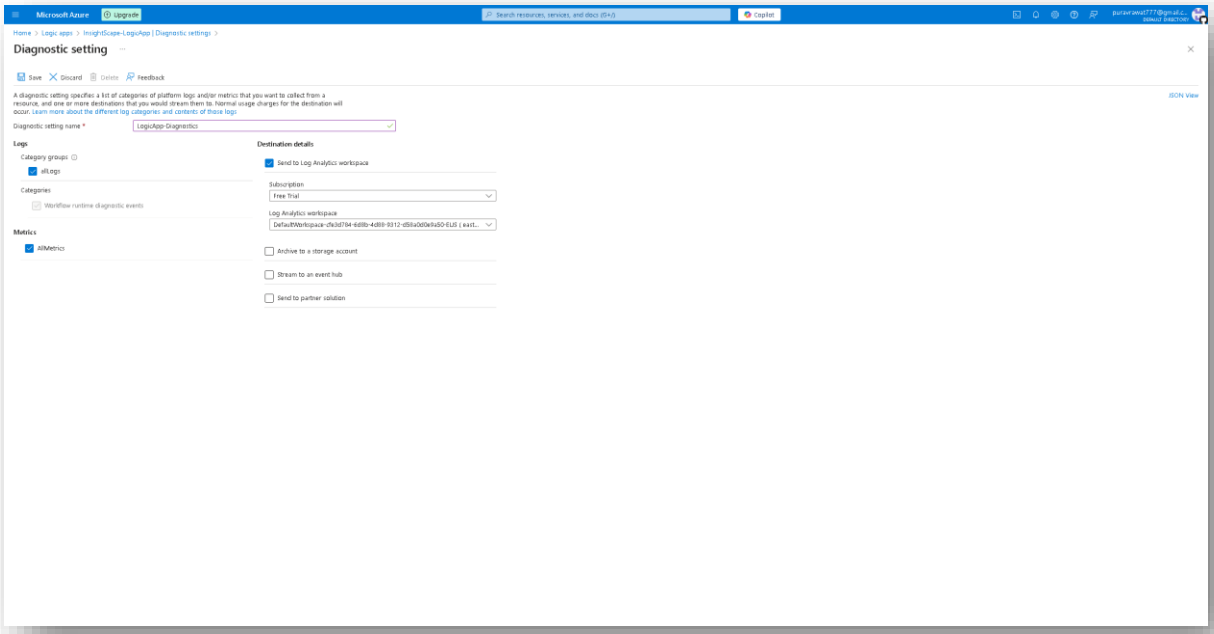

Metric namespace
microsoft.compute/virtualmachines
Metric value
75
Operator
GreaterThan
Threshold
50
Microsoft
Reply
Forward

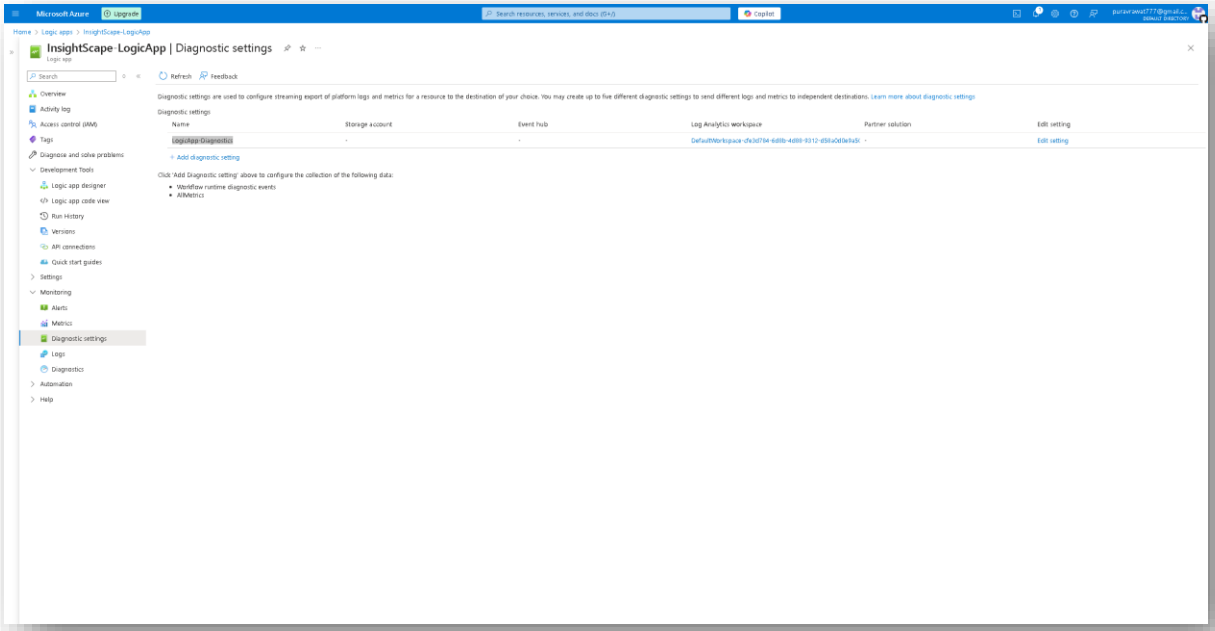

Microsoft Azure
App Services
InsightScape-WebApp
Web App
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events (preview)
Deployment
Settings
Performance
App Service plan
Development Tools
API
Monitoring
Automation
Browse
Stop
Restart
Delete
Refresh
Download publish profile
Reset publish profile
Share to mobile
Send us your feedback
Properties
Monitoring
Logs
Capabilities
Notifications
Recommendations
Web app
Deployment Center
Domains
Application Insights
Hosting
Networking


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor
Monitor | Applications
Microsoft
Search
Create
Manage view
Refresh
Export to CSV
Open query
Assign tags
Delete
Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Investigator (preview)
Insights
Applications
Virtual Machines
Storage accounts
Containers
Networks
SQL (preview)
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Azure Data Explorer Clusters
Log Analytics workspaces
Azure Stack HCI
Service Bus (preview)
Insights Hub
Managed Services
Settings
Support + Troubleshooting
Filter for any field...
Subscription equals all
Resource group equals all
Location equals all
Add filter
Showing 1 to 1 of 1 records.
No grouping
List view
Name
Resource group
Location
Subscription
InsightScape-WebApp
InsightScape-RG
Canada Central
Free Trial
< Previous
Page 1 of 1
Next >
Give feedback


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home >
InsightScape-WebApp
Application Insights
Search
Application Dashboard
Getting started
Search
Logs
Monitor resource group
Feedback
Favorites
Rename
Delete
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Investigate
Monitoring
Usage
Configure
Settings
Automation
Help
Essentials
JSON View
Resource group (move) : InsightScape-RG
Location : Canada Central
Subscription (move) : Free Trial
Subscription ID : cfe3d784-6d8b-4d88-9312-d5fa0d0e9a50
Tags (edit) : Add tags
Instrumentation Key : 257000ca-045e-49f5-be44-80fe0118f8f1
Connection String : InstrumentationKey=257000ca-045e-49f5-be44-80fe0118f8f1;IngestionEndpoint=https://canadacentral-1.in.applicationinsights.azure.com/;LiveEndpoint=https...
Workspace : DefaultWorkspace-cfe3d784-6d8b-4d88-9312-d5fa0d0e9a50-CCAN
Show data for last:
30 minutes
1 hour
6 hours
12 hours
1 day
3 days
7 days
30 days
Failed requests
Server response time
Server requests
Availability


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Logic apps > InsightScape-LogicApp
InsightScape-LogicApp | Diagnostic settings
Logic app
Search
Refresh
Feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Run History
Versions
API connections
Quick start guides
Settings
Monitoring
Alerts
Metrics
Diagnostic settings
Logs
Diagnostics
Automation
Help
Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostic settings
Diagnostic settings
Name
Storage account
Event hub
Log Analytics workspace
Partner solution
Edit setting
No diagnostic settings defined
+ Add diagnostic setting
Click 'Add Diagnostic setting' above to configure the collection of the following data:
Workflow runtime diagnostic events
AllMetrics


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Logic apps > InsightScape-LogicApp | Diagnostic settings >
Diagnostic setting
Save
Discard
Delete
Feedback
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
JSON View
Diagnostic setting name *
LogicApp-Diagnostics
Logs
Category groups
allLogs
Categories
Workflow runtime diagnostic events
Metrics
AllMetrics
Destination details
Send to Log Analytics workspace
Subscription
Free Trial
Log Analytics workspace
Archive to a storage account
Stream to an event hub
Send to partner solution


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Logic apps > InsightScape-LogicApp
InsightScape-LogicApp | Diagnostic settings
Logic app
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Run History
Versions
API connections
Quick start guides
Settings
Monitoring
Alerts
Metrics
Diagnostic settings
Logs
Diagnostics
Automation
Help
Refresh
Feedback
Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostic settings
Diagnostic settings
Name
Storage account
Event hub
Log Analytics workspace
Partner solution
Edit setting
LogicApp-Diagnostics
-
-
DefaultWorkspace-cfe3d784-6d8b-4d88-9312-d98a0d0e9a5f
-
Edit setting
+ Add diagnostic setting
Click 'Add Diagnostic setting' above to configure the collection of the following data:
Workflow runtime diagnostic events
AllMetrics

2) Activity Logs, Metrics, and Diagnostic Settings

For this phase of the project:

Activity Log Setup:

- First, I accessed the Activity Log in Azure Monitor. This log captures every event, which is very beneficial for monitoring purposes and provides detailed information regarding resource changes and activities.

Setting Up Metrics for VMs, WebApp, and Logic App:

VM Metrics:

- I navigated to the Metrics tab in Azure Monitor, where I selected both InsightScapeVM1 and InsightScape-VM2 as the scope.
- I configured the following metrics:
    - Percentage CPU, Aggregation: Avg - This metric helps monitor the percentage of CPU usage for both VMs.
    - OS Disk Latency, Aggregation: Avg - This metric helps understand the disk latency of the OS disks.
    - Available Memory Bytes, Aggregation: Avg - This shows the available memory for each VM.
    - Disk Read Bytes, Aggregation: Sum (You can use Avg over here as well)- This provides insight into the disk read performance of the VMs.
- After successfully setting up these metrics, I pinned each metric chart to my Dashboard for easy and quick access.

WebApp Metrics:

- I proceeded to set up metrics for the WebApp:
    - Scope: InsightScape-WebApp
    - Configured the following metrics:
        - Requests, Aggregation: Sum - To monitor the number of requests received.
        - Response Time, Aggregation: Avg - To track the average response time of the web app.
        - Average Memory Working Set, Aggregation: Avg - To monitor memory usage.
        - CPU Time, Aggregation: Sum - To monitor the total CPU time consumed.
- I pinned each of these metric charts to my Dashboard as well.

Logic App Metrics:

- Finally, I set up metrics for the Logic App:
    - Scope: InsightScape-LogicApp
    - Configured the following metrics:

        - Runs Succeeded, Aggregation: Count - To track successful executions of the Logic App.
        - Triggers Completed, Aggregation: Count - To monitor the total triggers completed.
        - Triggers Failed, Aggregation:Sum (you can use Count here in my case there were 0 trigger failures) - To track any failed triggers.
- I pinned each of these metric charts to my Dashboard.

Diagnostic Settings for VMs, WebApp, and Log Analytics Workspace:

VM Diagnostic Settings:

- InsightScape-VM1:
    - I went to the Extensions + applications tab in InsightScape-VM1.
    - I provisioned the Azure Performance Diagnostics with the following configurations:
        - Storage Account Name: insightscapestorage
        - Storage Account Key: (Entered the Storage Account Key)
        - Performance Scenario: Collect basic configurations
        - With this, the Diagnostics settings extension was successfully installed on InsightScape-VM1.
- InsightScape-VM2:
    - For setting up diagnostic settings in Linux, it's important to note that the **Linux Diagnostic Extension (LAD)** has been discontinued and replaced by the **Azure Monitor Agent (AMA)**. You can install the new agent through two methods: via the Azure portal or by using SSH to access the Linux VM directly.

      Method 1: Install via Azure Portal

        1. Navigate to your Linux VM in the Azure portal.
        2. In the left-hand menu, select Extensions + applications.
        3. Click on + Add and search for Azure Monitor Agent.
        4. Select Azure Monitor Agent from the list and click Next.
        5. Follow the installation prompts to complete the setup of the agent.

      Method 2: Install via SSH

```
az vm extension set \
  --resource-group <your-resource-group> \
  --vm-name <your-vm-name> \
  --name AzureMonitorLinuxAgent \
  --publisher Microsoft.Azure.Monitor
```

There is another Method which you can use to download the Linux Diagnostic Agent where you use the Azure CLI and then ran a series of commands to install the Extension:

1. Check the version of the waagent:

   ```
   /usr/sbin/waagent -version
   ```

2. Update and install walinuxagent:

   ```
   sudo apt-get update && sudo apt-get install
   walinuxagent
   ```

3. Install wget:

   ```
   sudo apt-get install -y wget
   ```

4. Install Python 2:

   ```
   sudo apt-get install -y python2
   ```

5. Set Python 2 as the default Python version:

   ```
   sudo update-alternatives --install
   /usr/bin/python python /usr/bin/python2 1
   ```

6. Assign a managed identity to the VM:

   ```
   az vm identity assign --resource-group
   InsightScape-RG -- name InsightScape-VM2
   ```

7. Download the diagnostics settings JSON file:

   ```
   wget
   https://raw.githubusercontent.com/Azure/azure
   -linux-
   extensions/master/Diagnostic/tests/lad_2_3_co
   mpatible_por tal_pub_settings.json -O
   portal_public_settings.json
   ```

8. Set the diagnostic storage account name:

   ```
   my_diagnostic_storage_account="insightscapest
   orage"
   ```

9. Get the resource ID of the VM:

```
my_vm_resource_id=$(az vm show --resource-
group InsightScape-RG --name InsightScape-VM2
--query "id" -o tsv)
```

10. Update the diagnostic storage account in the settings file:

```
sed -i
"s#_DIAGNOSTIC_STORAGE_ACCOUNT_#$my_diagnosti
c_storage_ac count#g"
portal_public_settings.json
```

11. Update the VM resource ID in the settings file:

```
sed -i
"s#_VM_RESOURCE_ID_#$my_vm_resource_id#g"
portal_public_settings.json
```

12. Generate a SAS token for the diagnostic storage account:

```
my_diagnostic_storage_account_sastoken=$(az
storage account generate-sas --account-name
$my_diagnostic_storage_account --expiry 2037-
12- 31T23:59:00Z --permissions wlacu --
resource-types co -- services b --output tsv)
```

13. Create the protected settings for the extension:

```
my_lad_protected_settings="{\"storageAccountN
ame\": \"$my_diagnostic_storage_account\",
\"storageAccountSasToken\":
\"$my_diagnostic_storage_account_sastoken\"}"
```

14. Set the Linux diagnostics extension on the VM:

```
az vm extension set --publisher
Microsoft.Azure.Diagnostics --name
LinuxDiagnostic -- version 4.0 --resource-
group InsightScape-RG --vm-name InsightScape-
```

```
VM2 --protected-settings
"$my_lad_protected_settings" --settings
portal_public_settings.json
```

- With this, the LinuxDiagnostic extension was successfully installed on InsightScapeVM2.

WebApp Diagnostic Settings:

- I went to the Diagnostic Settings tab under Settings in Azure Monitor and clicked on InsightScape-WebApp.
- These were the configurations for InsightScape-WebApp:
    - Diagnostic Setting Name: WebApp-Diagnostics Logs: o HTTP

  Logs (Ticked)

    - App Service Console Logs (Ticked)
    - App Service Application Logs (Ticked)
    - Access Audit Logs (Ticked)
    - IPSecurity Audit Logs (Ticked)
    - App Service Platform Logs (Ticked)
    - App Service Authentication Logs (preview) (Ticked)

  Metrics:

    - AllMetrics (Ticked)

  Destination Details: I selected the Default Log Analytics Workspace.

Verifying Link to Log Analytics Workspace:

- After configuring diagnostic settings, I verified that both VMs were linked to the Default Log Analytics Workspace by accessing the Virtual Machines (deprecated) tab in the Default Log Analytics Workspace.

Log Analytics Workspace Diagnostic Settings:

- At the end of this phase, I added diagnostic settings for the Default Log Analytics Workspace with the following configurations:
    - Diagnostic Setting Name: Workspace-Diagnostics

  Logs:

    - Audit (Ticked)
    - allLogs (Ticked)

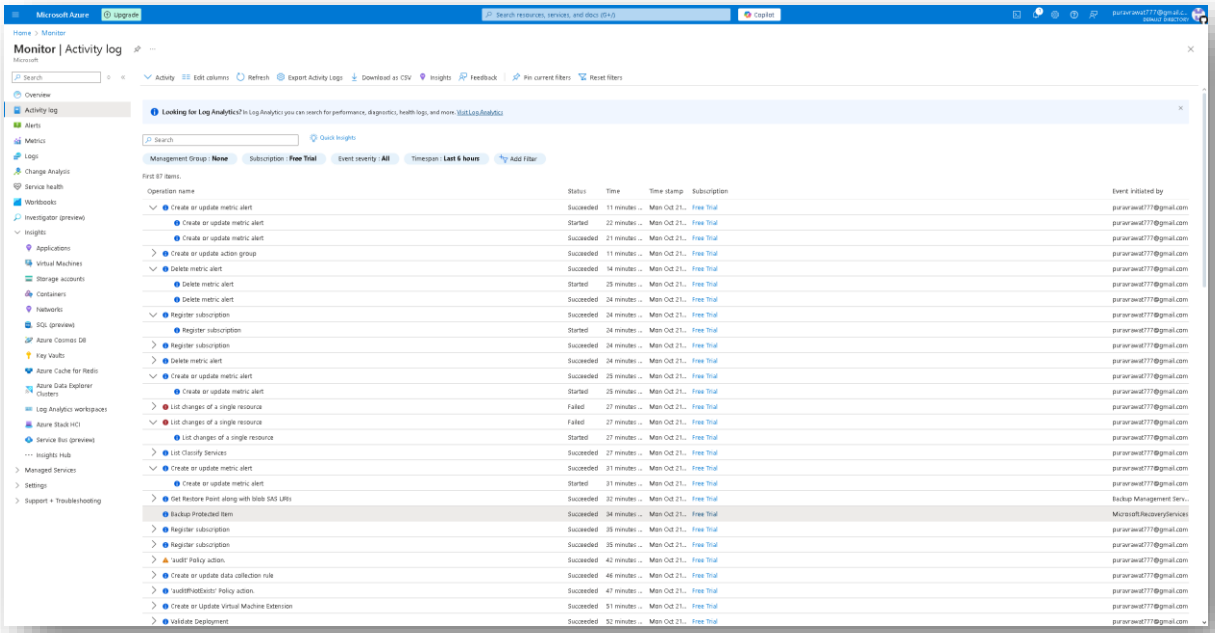
  Metrics:

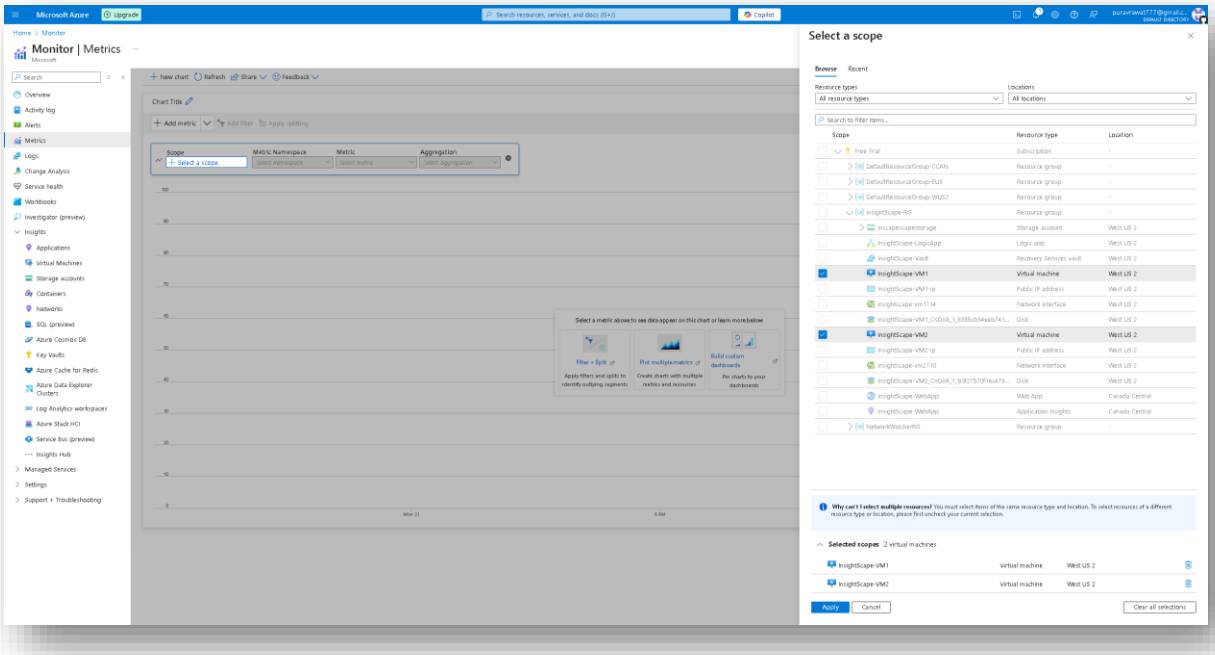
    - AllMetrics (Ticked)

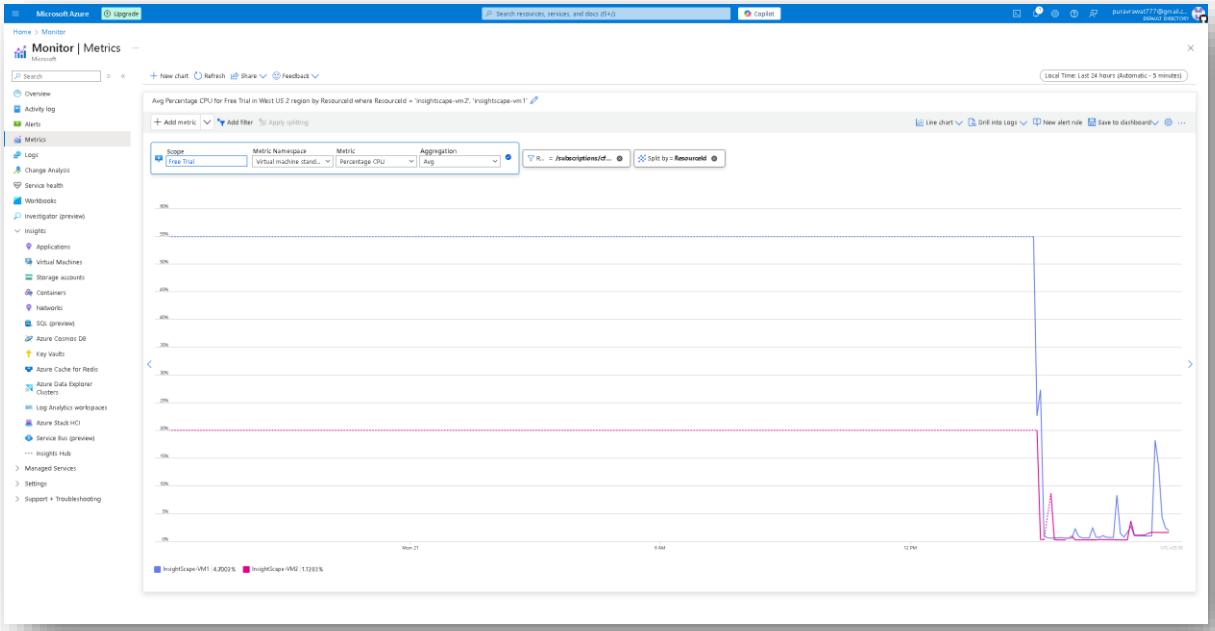
Destination Details: I selected the Default Log Analytics Workspace.

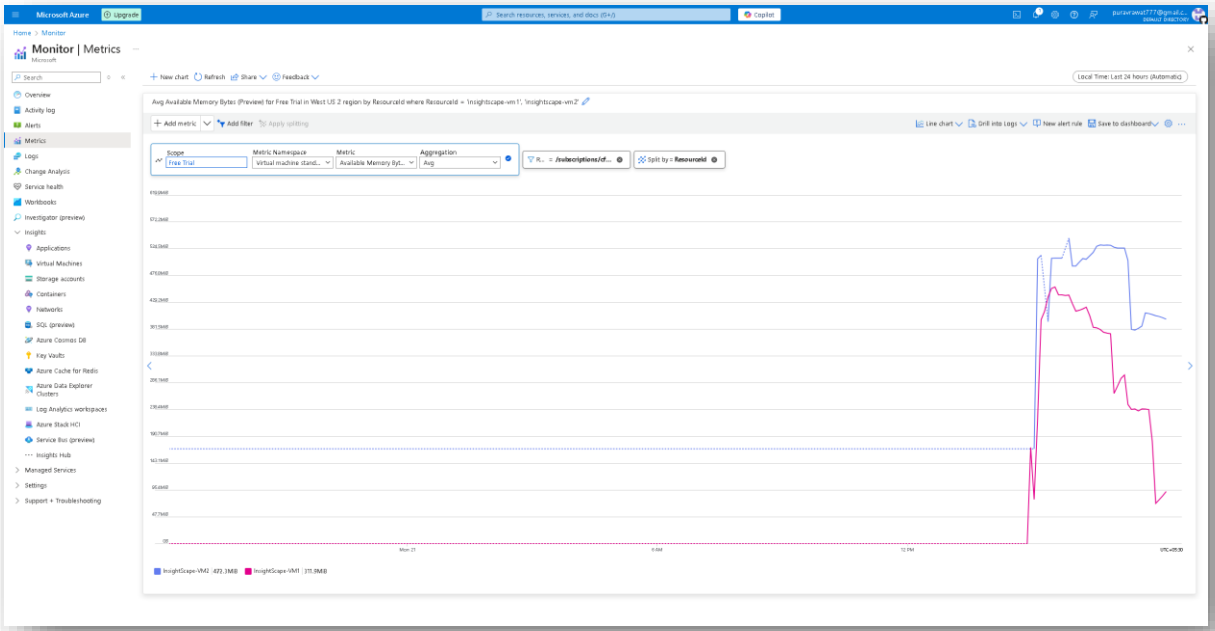
This completed the Activity Logs, Metrics, and Diagnostic Settings phase successfully.

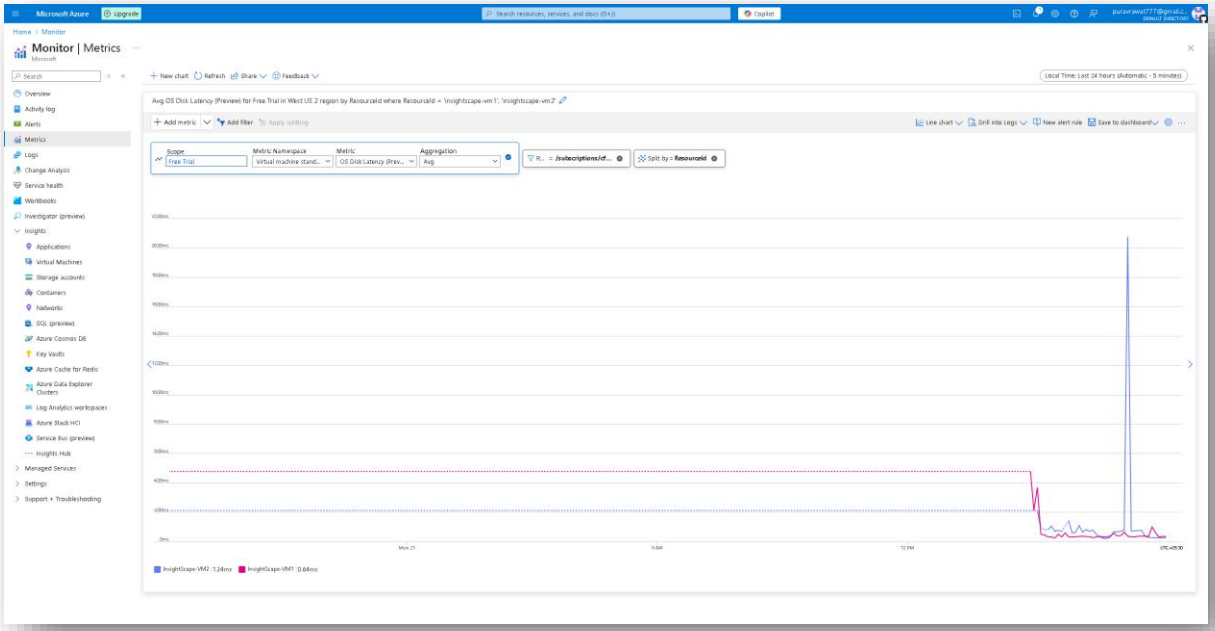
Screenshots -

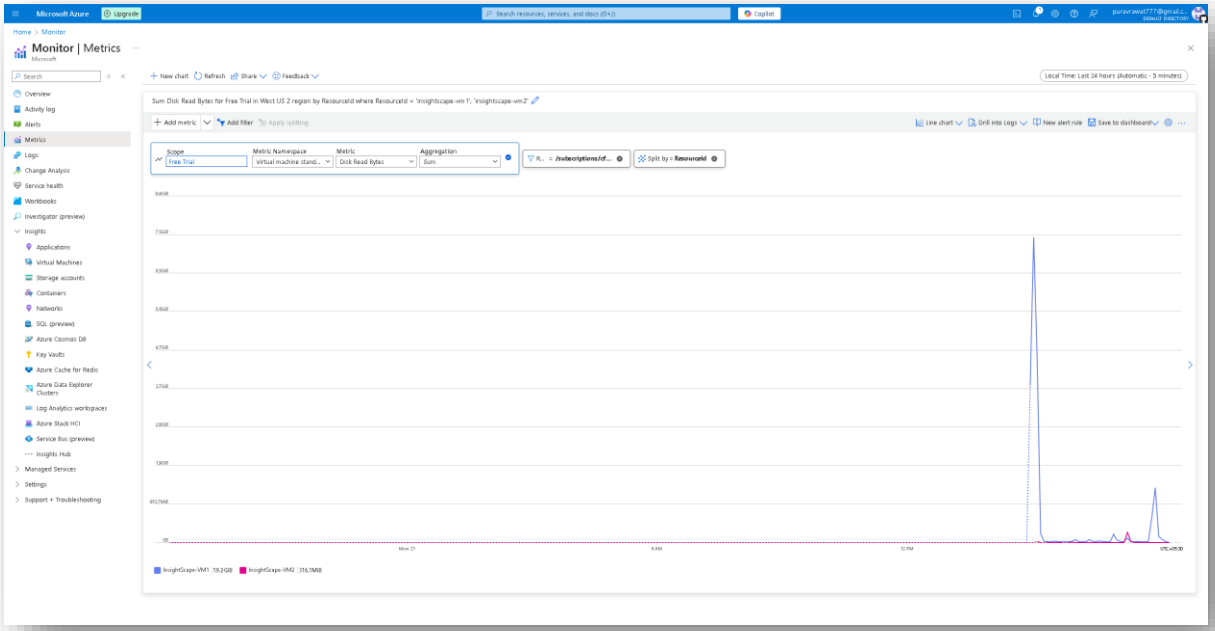


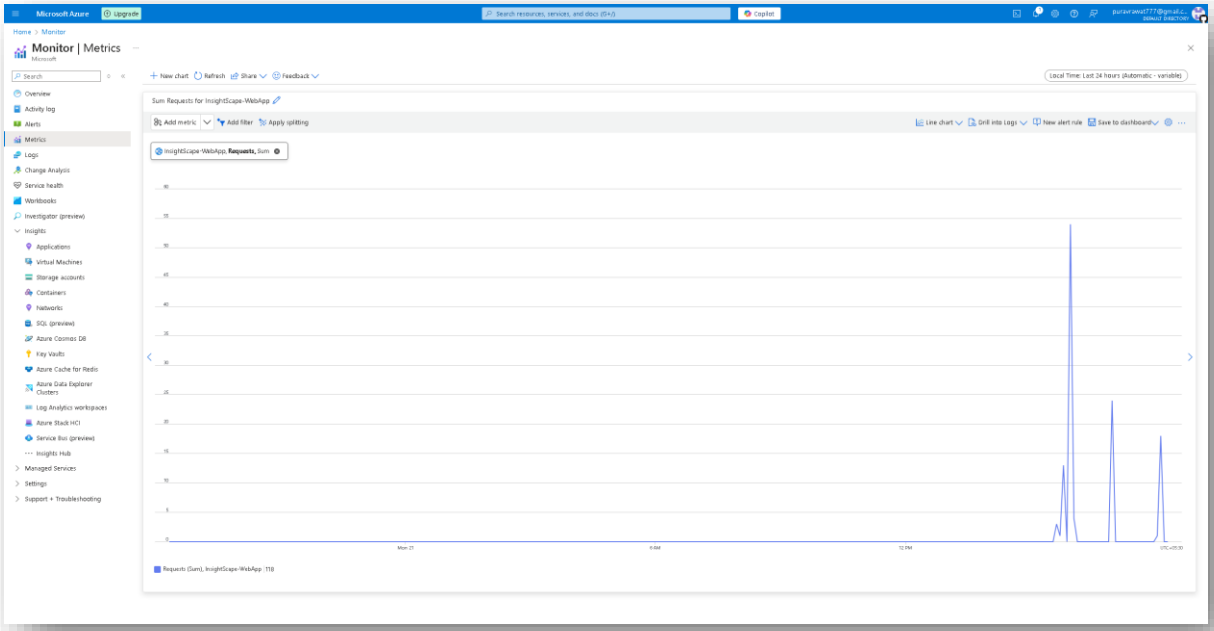


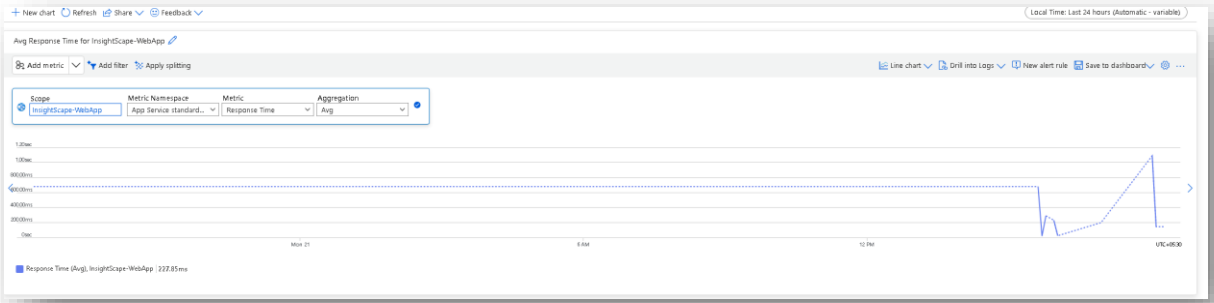

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor
Monitor | Metrics
Microsoft
Search
Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Investigator (preview)
Insights
Applications
Virtual Machines
Storage accounts
Containers
Networks
SQL (preview)
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Azure Data Explorer Clusters
Log Analytics workspaces
Azure Stack HCI
Service Bus (preview)
Insights Hub
Managed Services
Settings
Support + Troubleshooting
New chart
Refresh
Share
Feedback
Local Time: Last 24 hours (Automatic - 5 minutes)
Avg Percentage CPU for Free Trial in West US 2 region by Resourceid where ResourceId = 'insightscape-vm2', 'insightscape-vm1'
Add metric
Add filter
Apply splitting
Line chart
Drill into Logs
New alert rule
Save to dashboard
Scope
Free Trial
Metric Namespace
Virtual machine stand...
Metric
Percentage CPU
Aggregation
Avg
Split by = Resourceid
Mon 21
6 AM
12 PM
InsightScape-VM1 : 4.7002 %
InsightScape-VM2 : 1.1283 %

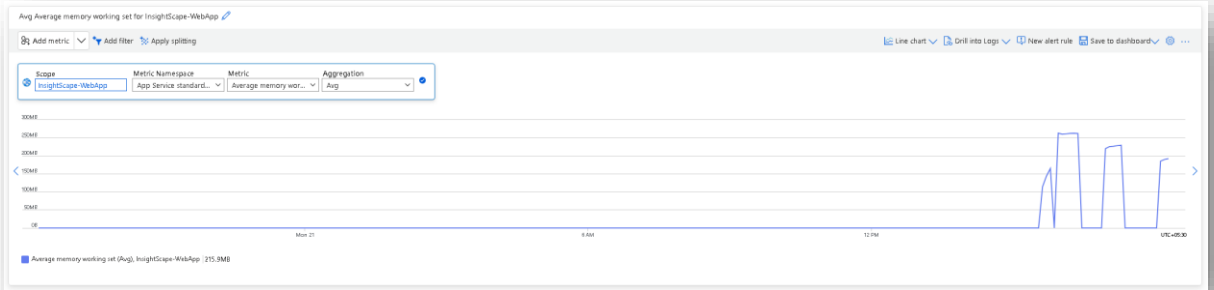

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor
Monitor | Metrics
Microsoft
Search
Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Investigator (preview)
Insights
Applications
Virtual Machines
Storage accounts
Containers
Networks
SQL (preview)
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Azure Data Explorer Clusters
Log Analytics workspaces
Azure Stack HCI
Service Bus (preview)
Insights Hub
Managed Services
Settings
Support + Troubleshooting
New chart
Refresh
Share
Feedback
Local Time: Last 24 hours (Automatic)
Avg Available Memory Bytes (Preview) for Free Trial in West US 2 region by Resourceid where ResourceId = 'insightscape-vm1', 'insightscape-vm2'
Add metric
Add filter
Apply splitting
Line chart
Drill into Logs
New alert rule
Save to dashboard
Scope
Free Trial
Metric Namespace
Virtual machine stand...
Metric
Available Memory Byt...
Aggregation
Avg
Split by = Resourceid
Mon 21
6 AM
12 PM
InsightScape-VM2 : 672.1 MB
InsightScape-VM1 : 371.8 MB

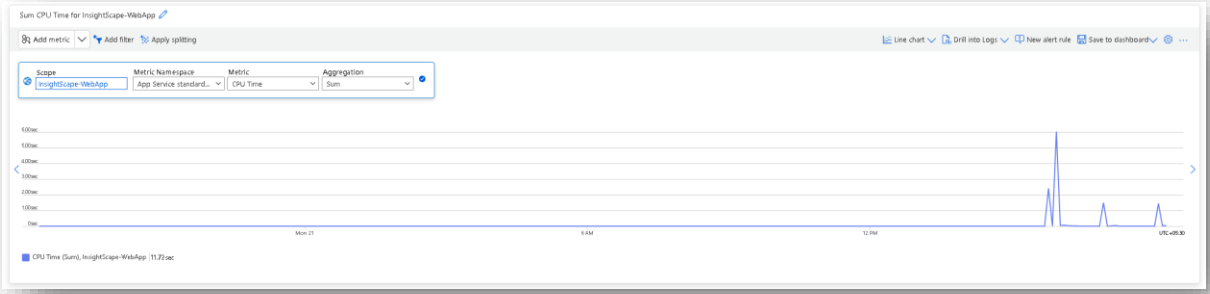

Microsoft Azure
Upgrade
Copilot
Home > Monitor
Monitor | Metrics
Microsoft
New chart
Refresh
Share
Feedback
Local Time: Last 24 hours (Automatic - 5 minutes)
Avg OS Disk Latency (Preview) for Free Trial in West US 2 region by ResourceId where ResourceId = 'insightscape-vm1', 'insightscape-vm2'
Add metric
Add filter
Apply splitting
Line chart
Drill into Logs
New alert rule
Save to dashboard
Scope
Free Trial
Metric Namespace
Virtual machine stand...
Metric
OS Disk Latency (Prev...
Aggregation
Avg
Split by = ResourceId
Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Investigator (preview)
Insights
Applications
Virtual Machines
Storage accounts
Containers
Networks
SQL (preview)
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Azure Data Explorer Clusters
Log Analytics workspaces
Azure Stack HCI
Service Bus (preview)
Insights Hub
Managed Services
Settings
Support + Troubleshooting
Mon 21
8 AM
12 PM
UTC+05:30
InsightScape-VM2 5.24ms
InsightScape-VM1 0.64ms

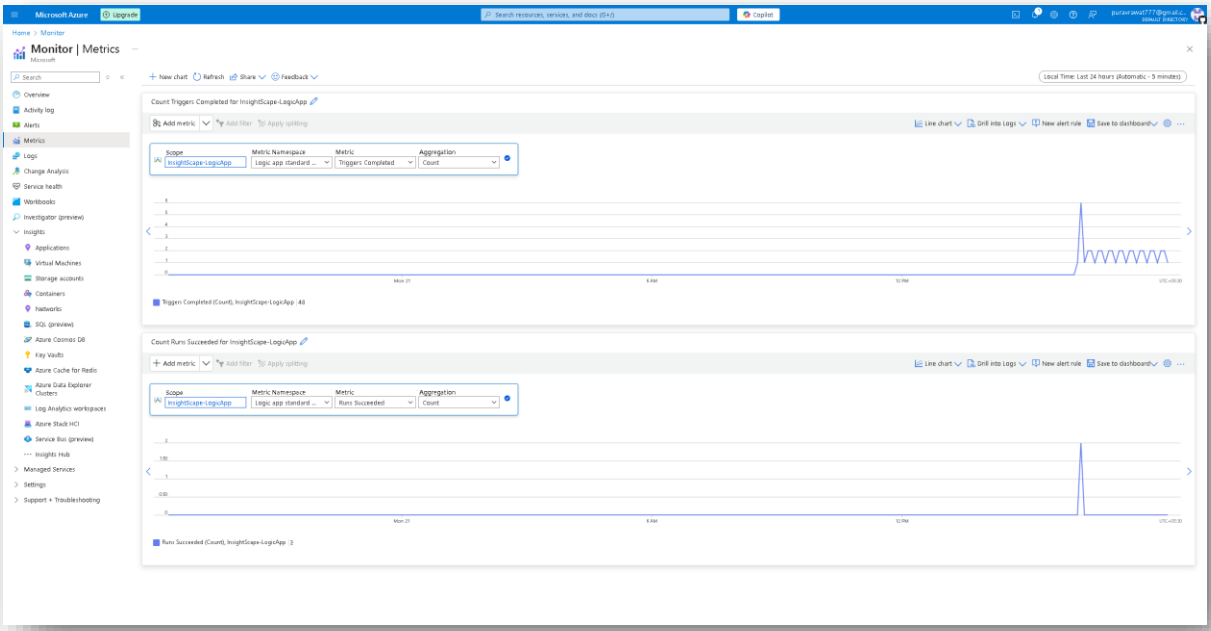

Microsoft Azure
Upgrade
Copilot
Home > Monitor
Monitor | Metrics
Microsoft
New chart
Refresh
Share
Feedback
Local Time: Last 24 hours (Automatic - 5 minutes)
Sum Disk Read Bytes for Free Trial in West US 2 region by ResourceId where ResourceId = 'insightscape-vm1', 'insightscape-vm2'
Add metric
Add filter
Apply splitting
Line chart
Drill into Logs
New alert rule
Save to dashboard
Scope
Free Trial
Metric Namespace
Virtual machine stand...
Metric
Disk Read Bytes
Aggregation
Sum
Split by = ResourceId
Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Investigator (preview)
Insights
Applications
Virtual Machines
Storage accounts
Containers
Networks
SQL (preview)
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Azure Data Explorer Clusters
Log Analytics workspaces
Azure Stack HCI
Service Bus (preview)
Insights Hub
Managed Services
Settings
Support + Troubleshooting
Mon 21
8 AM
12 PM
UTC+05:30
InsightScape-VM1 19.2 GB
InsightScape-VM2 316.7MB

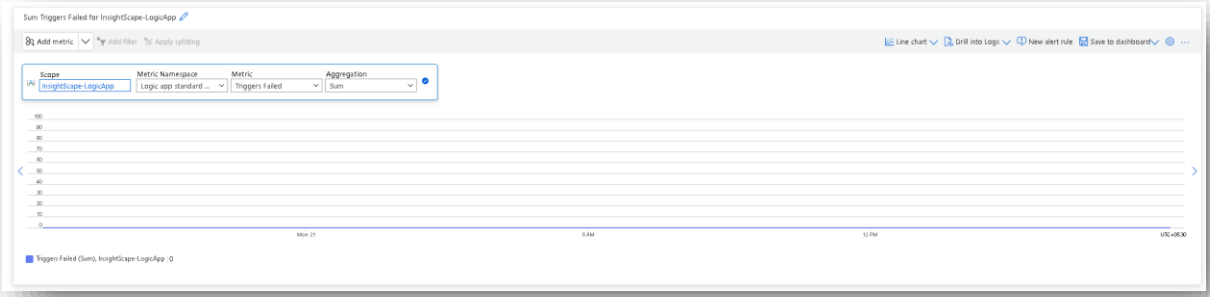

Microsoft Azure
Upgrade
Copilot
Home > Monitor
Monitor | Metrics
Microsoft
New chart
Refresh
Share
Feedback
Local Time: Last 24 hours (Automatic - variable)
Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Investigator (preview)
Insights
Applications
Virtual Machines
Storage accounts
Containers
Networks
SQL (preview)
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Azure Data Explorer Clusters
Log Analytics workspaces
Azure Stack HCI
Service Bus (preview)
Insights Hub
Managed Services
Settings
Support + Troubleshooting
Sum Requests for InsightScape-WebApp
Add metric
Add filter
Apply splitting
Line chart
Drill into Logs
New alert rule
Save to dashboard
InsightScape-WebApp, Requests, Sum
Mon 21
6 AM
12 PM
UTC+05:30
Requests (Sum), InsightScape-WebApp 118

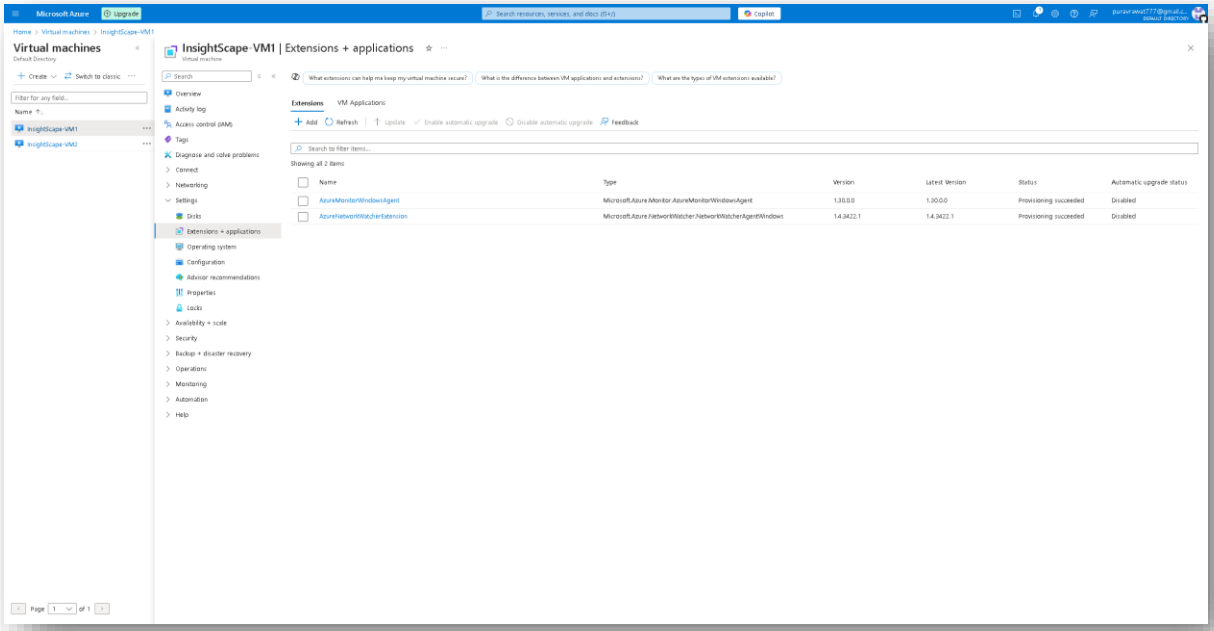

New chart
Refresh
Share
Feedback
Local Time: Last 24 hours (Automatic - variable)
Avg Response Time for InsightScape-WebApp
Add metric
Add filter
Apply splitting
Line chart
Drill into Logs
New alert rule
Save to dashboard
Scope
InsightScape-WebApp
Metric Namespace
App Service standard...
Metric
Response Time
Aggregation
Avg
Mon 21
8 AM
12 PM
UTC+05:30
Response Time (Avg), InsightScape-WebApp 227.85 ms

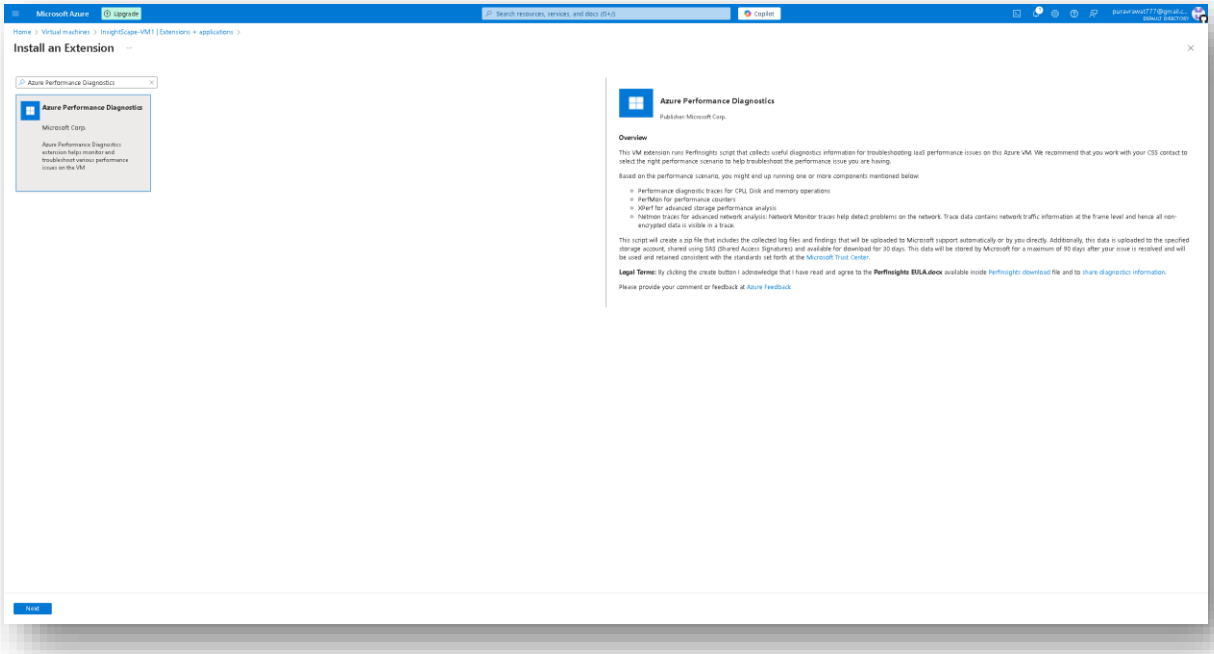

Avg Average memory working set for InsightScape-WebApp
Add metric
Add filter
Apply splitting
Line chart
Drill into Logs
New alert rule
Save to dashboard
Scope
InsightScape-WebApp
Metric Namespace
App Service standard...
Metric
Average memory wor...
Aggregation
Avg
Mon 21
6 AM
12 PM
UTC+05:30
Average memory working set (Avg), InsightScape-WebApp 215.9 MB

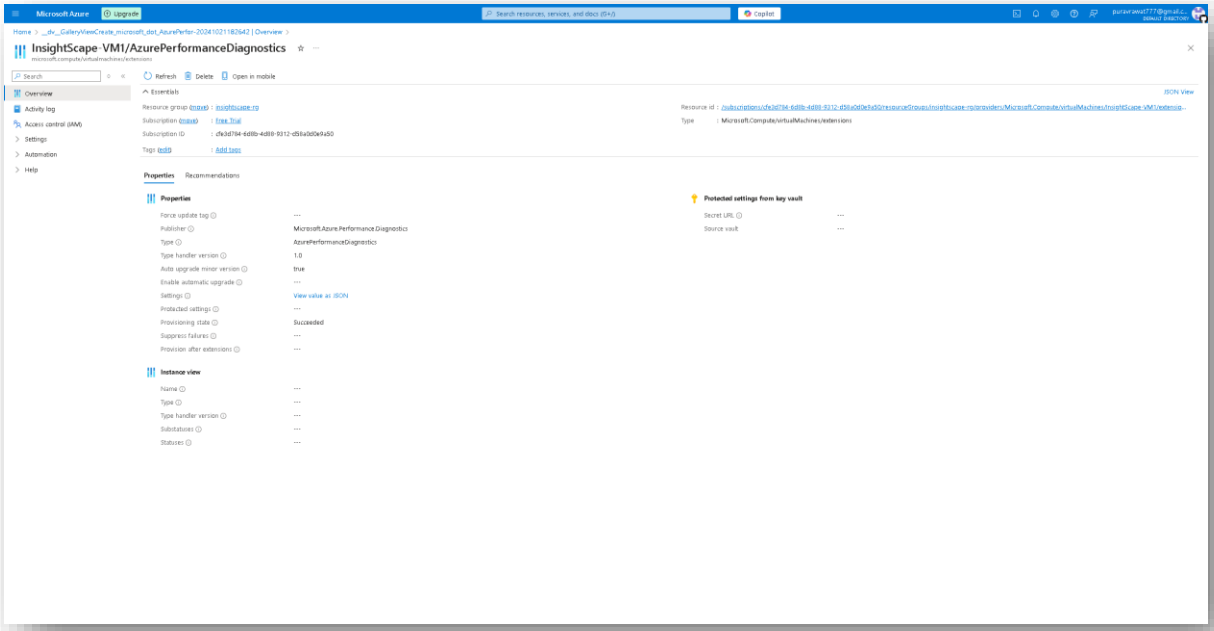

Sum CPU Time for InsightScape-WebApp
Add metric
Add filter
Apply splitting
Line chart
Drill into Logs
New alert rule
Save to dashboard
Scope
InsightScape-WebApp
Metric Namespace
App Service standard...
Metric
CPU Time
Aggregation
Sum
Mon 21
6 AM
12 PM
UTC+05:30
CPU Time (Sum), InsightScape-WebApp 11.72sec

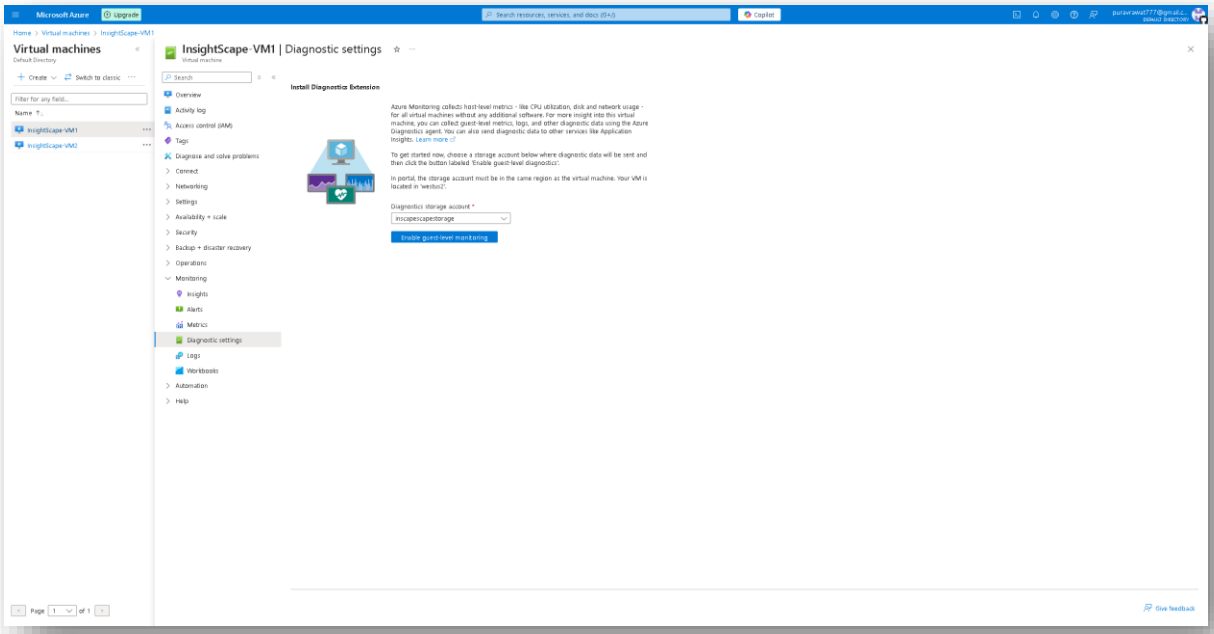

Microsoft Azure
Upgrade
Copilot
Home > Monitor
Monitor | Metrics
Microsoft
New chart
Refresh
Share
Feedback
Local Time: Last 24 hours (Automatic - 5 minutes)
Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Investigator (preview)
Insights
Applications
Virtual Machines
Storage accounts
Containers
Networks
SQL (preview)
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Azure Data Explorer Clusters
Log Analytics workspaces
Azure Stack HCI
Service Bus (preview)
Insights Hub
Managed Services
Settings
Support + Troubleshooting
Count Triggers Completed for InsightScape-LogicApp
Add metric
Add filter
Apply splitting
Line chart
Drill into Logs
New alert rule
Save to dashboard
Scope
InsightScape-LogicApp
Metric Namespace
Logic app standard ...
Metric
Triggers Completed
Aggregation
Count
Mon 21
6 AM
12 PM
UTC+05:30
Triggers Completed (Count), InsightScape-LogicApp 48
Count Runs Succeeded for InsightScape-LogicApp
Add metric
Add filter
Apply splitting
Line chart
Drill into Logs
New alert rule
Save to dashboard
Scope
InsightScape-LogicApp
Metric Namespace
Logic app standard ...
Metric
Runs Succeeded
Aggregation
Count
Mon 21
6 AM
12 PM
UTC+05:30
Runs Succeeded (Count), InsightScape-LogicApp 2

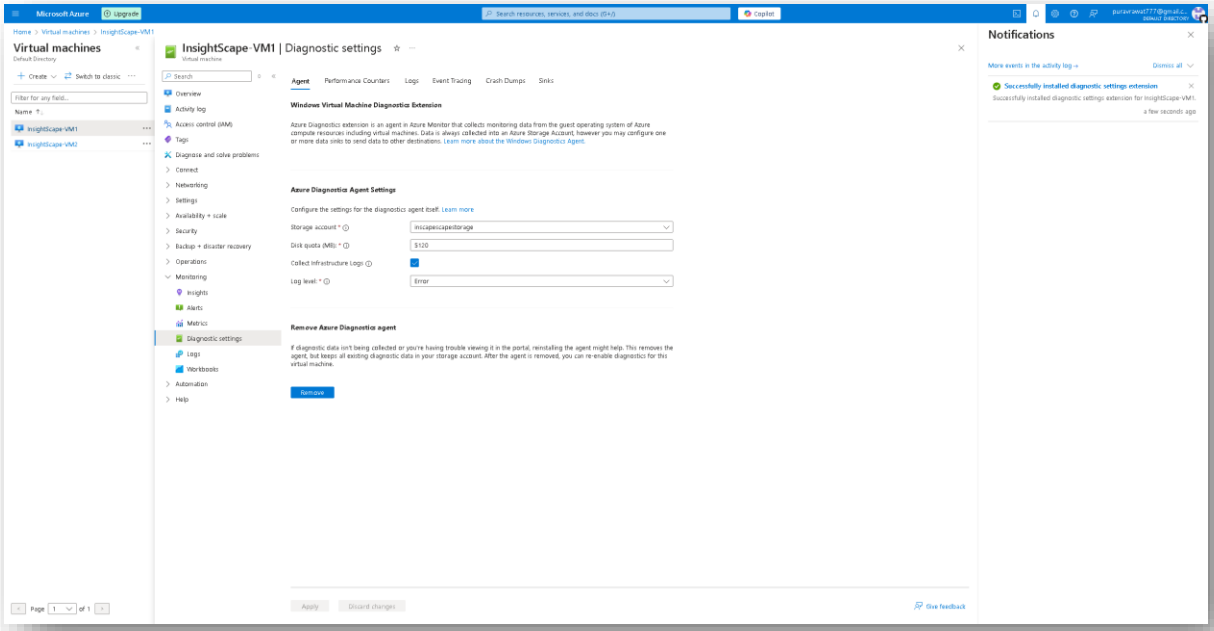

Sum Triggers Failed for InsightScape-LogicApp
Add metric
Add filter
Apply splitting
Line chart
Drill into Logs
New alert rule
Save to dashboard
Scope
InsightScape-LogicApp
Metric Namespace
Logic app standard ...
Metric
Triggers Failed
Aggregation
Sum
Mon 21
6 AM
12 PM
UTC+05:30
Triggers Failed (Sum), InsightScape-LogicApp 0

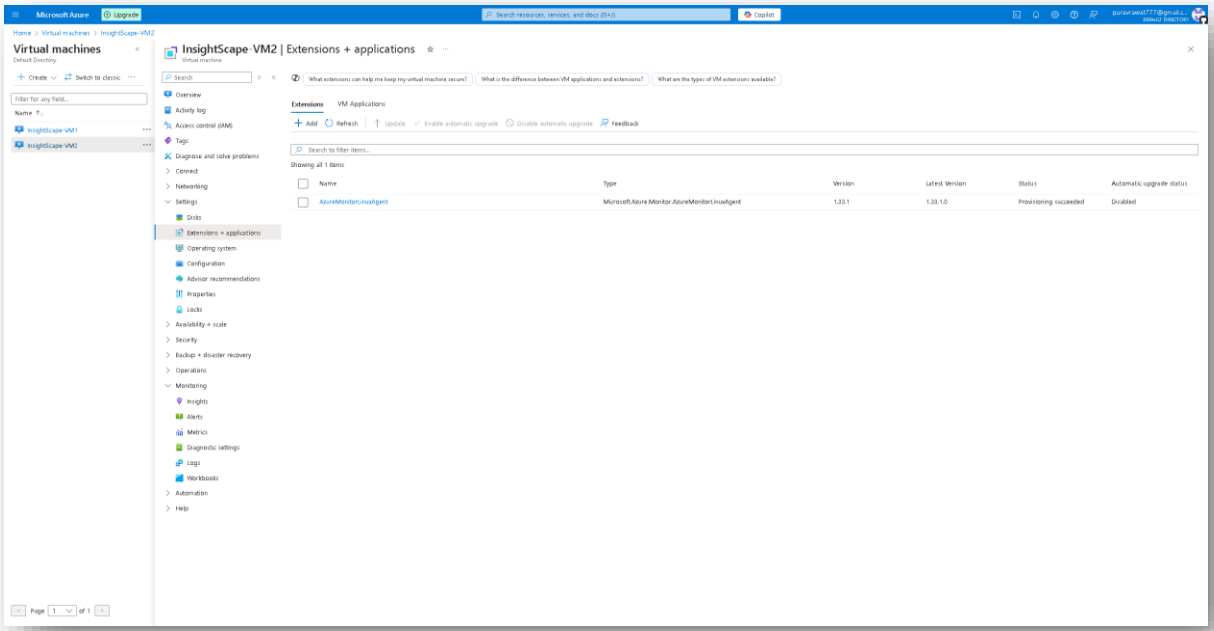

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Virtual machines > InsightScape-VM1
Virtual machines
Default Directory
Create
Switch to classic
Filter for any field...
Name
InsightScape-VM1
InsightScape-VM2
Page 1 of 1
InsightScape-VM1 | Extensions + applications
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Connect
Networking
Settings
Disks
Extensions + applications
Operating system
Configuration
Advisor recommendations
Properties
Locks
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Automation
Help
What extensions can help me keep my virtual machine secure?
What is the difference between VM applications and extensions?
What are the types of VM extensions available?
Extensions
VM Applications
Add
Refresh
Update
Enable automatic upgrade
Disable automatic upgrade
Feedback
Search to filter items...
Showing all 2 items
Name
Type
Version
Latest Version
Status
Automatic upgrade status
AzureMonitorWindowsAgent
Microsoft.Azure.Monitor.AzureMonitorWindowsAgent
1.30.0.0
1.30.0.0
Provisioning succeeded
Disabled
AzureNetworkWatcherExtension
Microsoft.Azure.NetworkWatcher.NetworkWatcherAgentWindows
1.4.3422.1
1.4.3422.1
Provisioning succeeded
Disabled

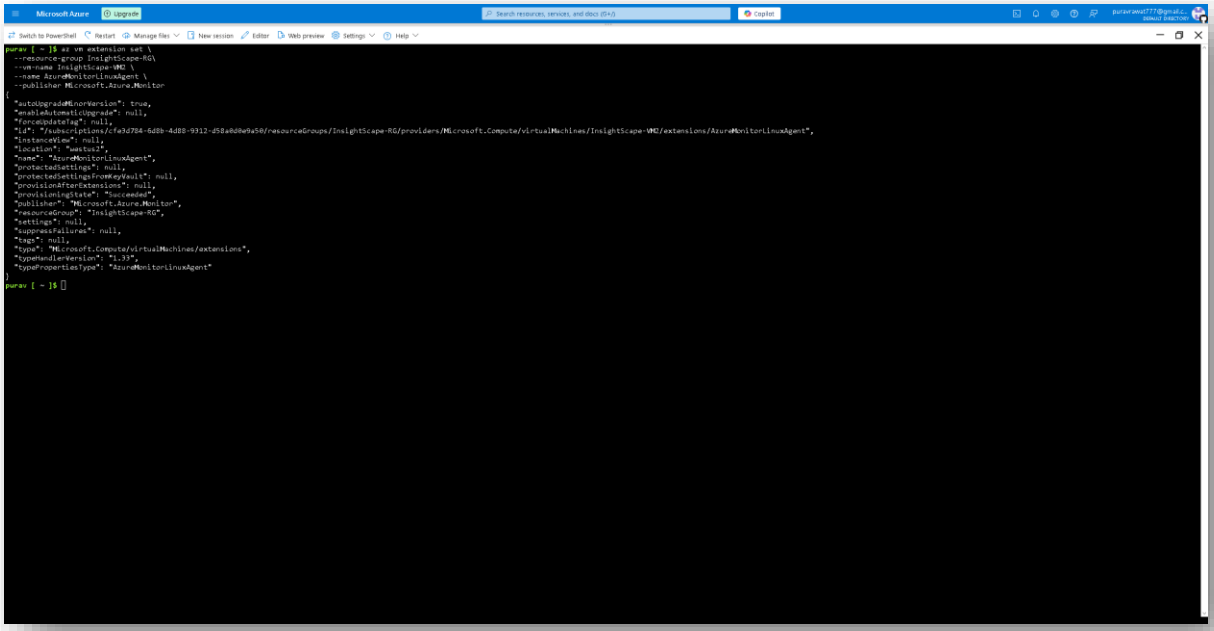

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Virtual machines > InsightScape-VM1 | Extensions + applications >
Install an Extension
Azure Performance Diagnostics
Azure Performance Diagnostics
Microsoft Corp.
Azure Performance Diagnostics extension helps monitor and troubleshoot various performance issues on the VM
Azure Performance Diagnostics
Publisher: Microsoft Corp.
Overview
This VM extension runs PerfInsights script that collects useful diagnostics information for troubleshooting IaaS performance issues on this Azure VM. We recommend that you work with your CSS contact to select the right performance scenario to help troubleshoot the performance issue you are having.
Based on the performance scenario, you might end up running one or more components mentioned below.
Performance diagnostic traces for CPU, Disk and memory operations
PerfMon for performance counters
XPerf for advanced storage performance analysis
Netmon traces for advanced network analysis: Network Monitor traces help detect problems on the network. Trace data contains network traffic information at the frame level and hence all non-encrypted data is visible in a trace.
This script will create a zip file that includes the collected log files and findings that will be uploaded to Microsoft support automatically or by you directly. Additionally, this data is uploaded to the specified storage account, shared using SAS (Shared Access Signatures) and available for download for 30 days. This data will be stored by Microsoft for a maximum of 90 days after your issue is resolved and will be used and retained consistent with the standards set forth at the Microsoft Trust Center.
Legal Terms: By clicking the create button I acknowledge that I have read and agree to the PerfInsights EULA.docx available inside PerfInsights download file and to share diagnostics information.
Please provide your comment or feedback at Azure Feedback
Next

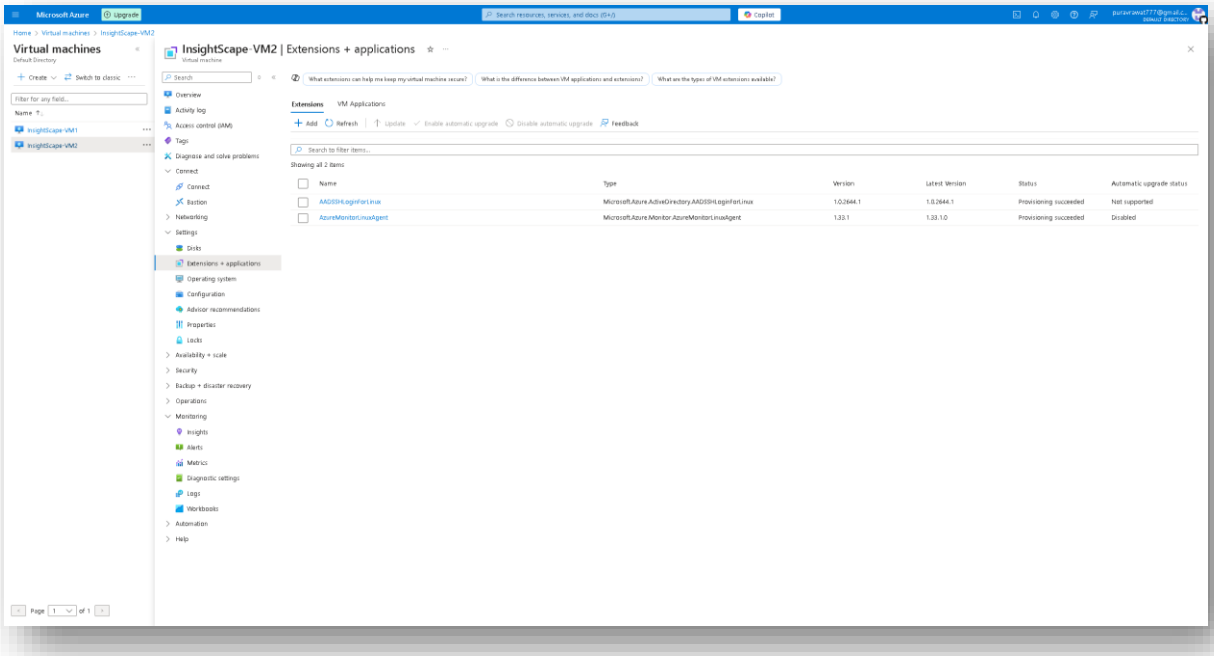

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home
InsightScape-VM1/AzurePerformanceDiagnostics
Overview
Activity log
Access control (IAM)
Settings
Automation
Help
Refresh
Delete
Open in mobile
Essentials
JSON View
Properties
Recommendations
Properties
Protected settings from key vault
Instance view

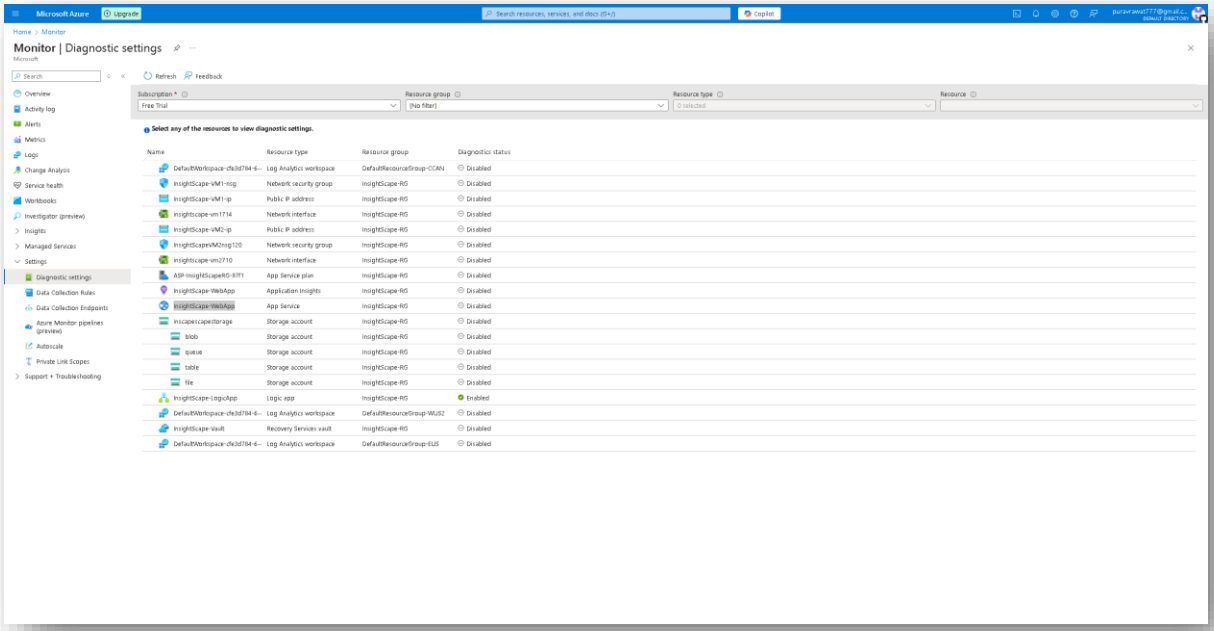

Microsoft Azure
Upgrade
Copilot
Home
Virtual machines
InsightScape-VM1
InsightScape-VM2
InsightScape-VM1 | Diagnostic settings
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Networking
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Insights
Alerts
Metrics
Diagnostic settings
Logs
Workbooks
Automation
Help
Install Diagnostics Extension
Azure Monitoring collects host-level metrics - like CPU utilization, disk and network usage - for all virtual machines without any additional software. For more insight into this virtual machine, you can collect guest-level metrics, logs, and other diagnostic data using the Azure Diagnostics agent. You can also send diagnostic data to other services like Application Insights. Learn more
To get started now, choose a storage account below where diagnostic data will be sent and then click the button labeled 'Enable guest-level diagnostics'.
In portal, the storage account must be in the same region as the virtual machine. Your VM is located in 'westus2'.
Diagnostics storage account *
inscapescapeitorage
Enable guest-level monitoring
Give feedback

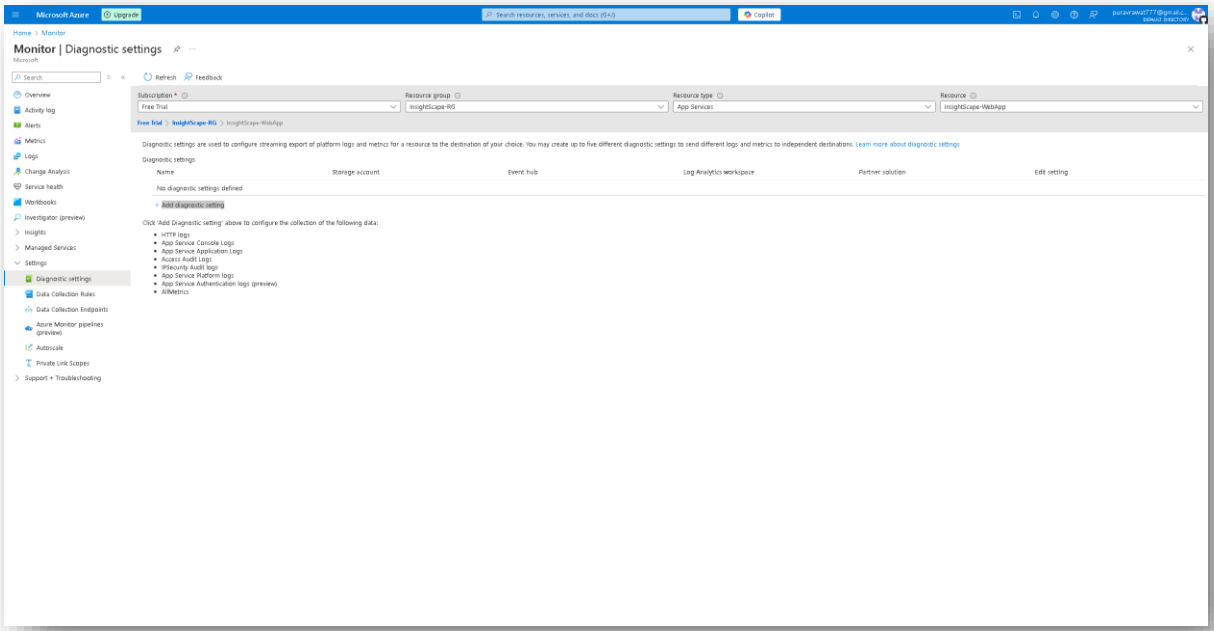

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Virtual machines > InsightScape-VM1
Virtual machines
Default Directory
Create
Switch to classic
Filter for any field...
Name
InsightScape-VM1
InsightScape-VM2
Page 1 of 1
InsightScape-VM1 | Diagnostic settings
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Connect
Networking
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Insights
Alerts
Metrics
Diagnostic settings
Logs
Workbooks
Automation
Help
Agent
Performance Counters
Logs
Event Tracing
Crash Dumps
Sinks
Windows Virtual Machine Diagnostics Extension
Azure Diagnostics extension is an agent in Azure Monitor that collects monitoring data from the guest operating system of Azure compute resources including virtual machines. Data is always collected into an Azure Storage Account, however you may configure one or more data sinks to send data to other destinations. Learn more about the Windows Diagnostics Agent.
Azure Diagnostics Agent Settings
Configure the settings for the diagnostics agent itself. Learn more
Storage account *
insightscapestorage
Disk quota (MB) *
5120
Collect Infrastructure Logs
Log level *
Error
Remove Azure Diagnostics agent
If diagnostic data isn't being collected or you're having trouble viewing it in the portal, reinstalling the agent might help. This removes the agent, but keeps all existing diagnostic data in your storage account. After the agent is removed, you can re-enable diagnostics for this virtual machine.
Remove
Apply
Discard changes
Give feedback
Notifications
More events in the activity log →
Dismiss all
Successfully installed diagnostic settings extension
Successfully installed diagnostic settings extension for InsightScape-VM1.
a few seconds ago

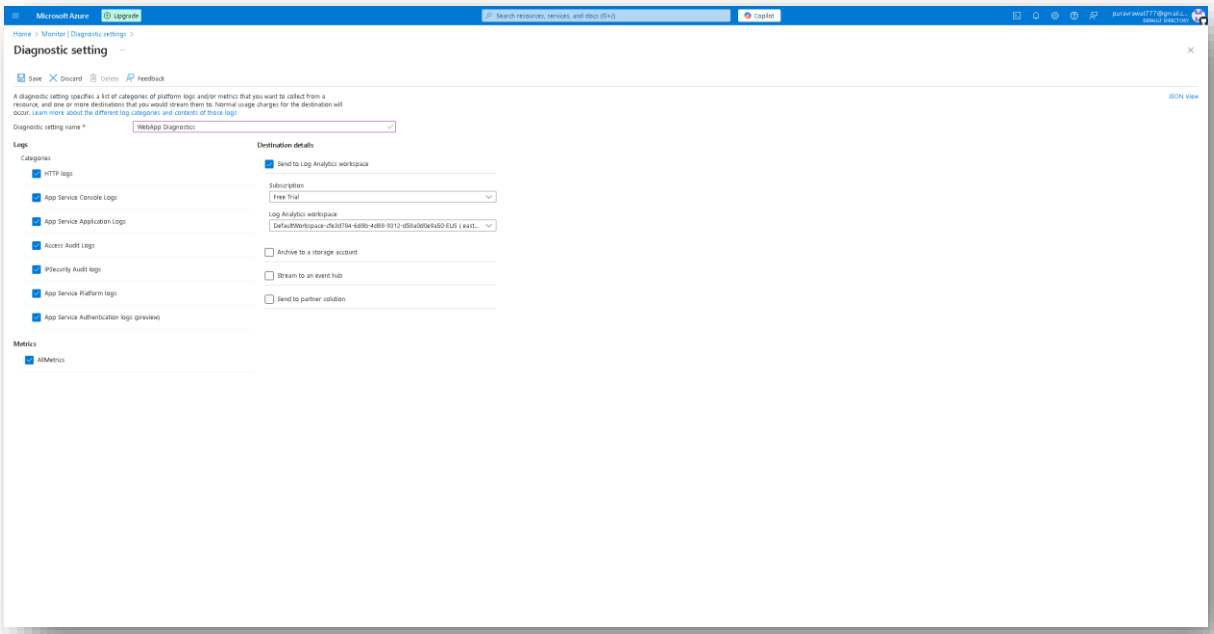

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Virtual machines > InsightScape-VM2
Virtual machines
Default Directory
Create
Switch to classic
Filter for any field...
Name
InsightScape-VM1
InsightScape-VM2
Page 1 of 1
InsightScape-VM2 | Extensions + applications
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Connect
Networking
Settings
Disks
Extensions + applications
Operating system
Configuration
Advisor recommendations
Properties
Locks
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Insights
Alerts
Metrics
Diagnostic settings
Logs
Workbooks
Automation
Help
What extensions can help me keep my virtual machine secure?
What is the difference between VM applications and extensions?
What are the types of VM extensions available?
Extensions
VM Applications
Add
Refresh
Update
Enable automatic upgrade
Disable automatic upgrade
Feedback
Search to filter items...
Showing all 1 items
Name
Type
Version
Latest Version
Status
Automatic upgrade status
AzureMonitorLinuxAgent
Microsoft.Azure.Monitor.AzureMonitorLinuxAgent
1.33.1
1.33.1.0
Provisioning succeeded
Disabled

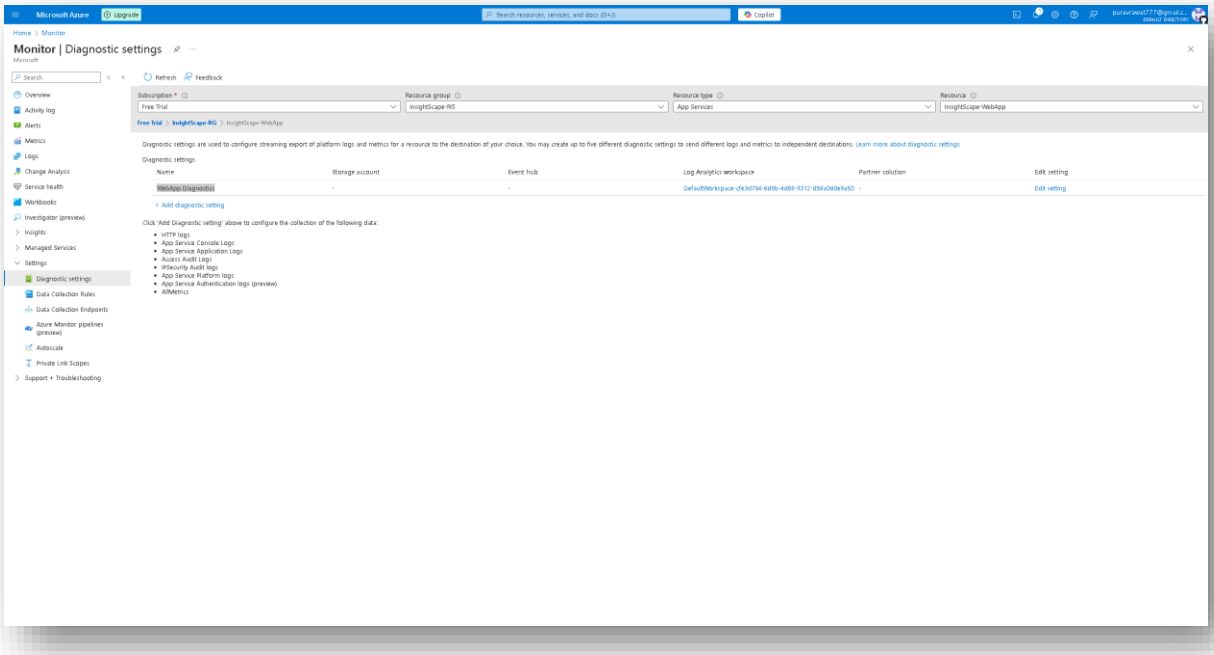

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Switch to PowerShell
Restart
Manage files
New session
Editor
Web preview
Settings
Help
purav [~]$ az vm extension set \
--resource-group InsightScape-RG\
--vm-name InsightScape-VM2 \
--name AzureMonitorLinuxAgent \
--publisher Microsoft.Azure.Monitor
{
"autoUpgradeMinorVersion": true,
"enableAutomaticUpgrade": null,
"forceUpdateTag": null,
"id": "/subscriptions/cfe3d784-6d8b-4d88-9312-d58a808e9a50/resourceGroups/InsightScape-RG/providers/Microsoft.Compute/virtualMachines/InsightScape-VM2/extensions/AzureMonitorLinuxAgent",
"instanceView": null,
"location": "westus2",
"name": "AzureMonitorLinuxAgent",
"protectedSettings": null,
"protectedSettingsFromKeyVault": null,
"provisionAfterExtensions": null,
"provisioningState": "Succeeded",
"publisher": "Microsoft.Azure.Monitor",
"resourceGroup": "InsightScape-RG",
"settings": null,
"suppressFailures": null,
"tags": null,
"type": "Microsoft.Compute/virtualMachines/extensions",
"typeHandlerVersion": "1.33",
"typePropertiesType": "AzureMonitorLinuxAgent"
}
purav [~]$

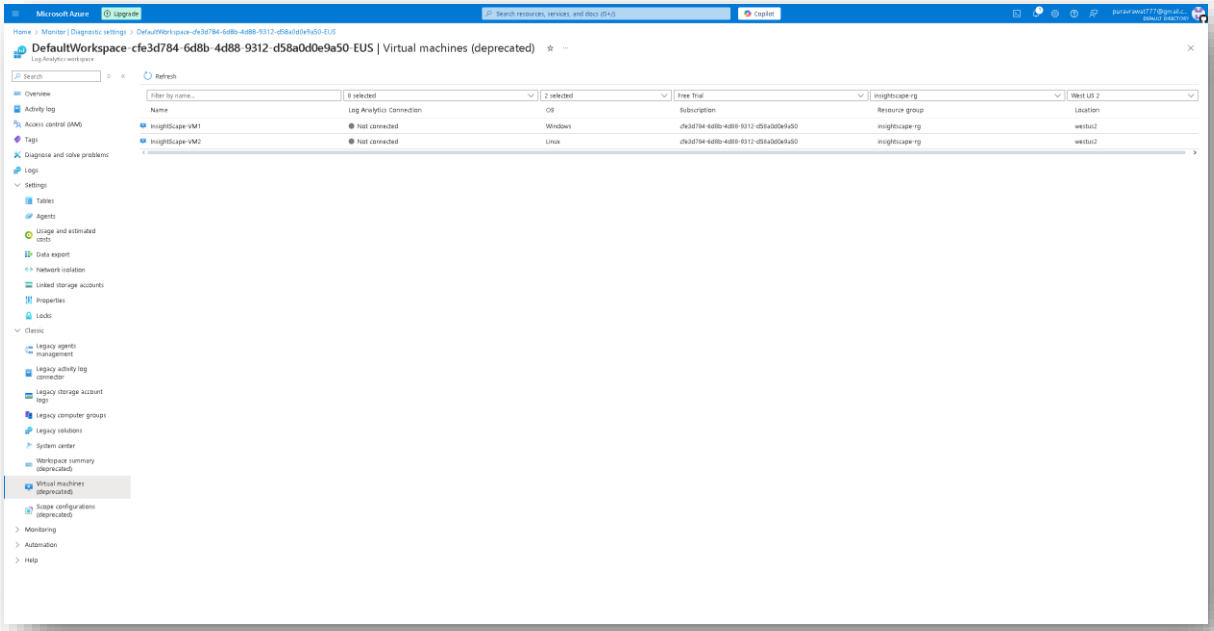

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Virtual machines > InsightScape-VM2
Virtual machines
Default Directory
Create
Switch to classic
Filter for any field...
Name
InsightScape-VM1
InsightScape-VM2
InsightScape-VM2 | Extensions + applications
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Connect
Connect
Bastion
Networking
Settings
Disks
Extensions + applications
Operating system
Configuration
Advisor recommendations
Properties
Locks
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Insights
Alerts
Metrics
Diagnostic settings
Logs
Workbooks
Automation
Help
What extensions can help me keep my virtual machine secure?
What is the difference between VM applications and extensions?
What are the types of VM extensions available?
Extensions
VM Applications
Add
Refresh
Update
Enable automatic upgrade
Disable automatic upgrade
Feedback
Search to filter items...
Showing all 2 items
Name
Type
Version
Latest Version
Status
Automatic upgrade status
AADSSHLoginForLinux
Microsoft.Azure.ActiveDirectory.AADSSHLoginForLinux
1.0.2644.1
1.0.2644.1
Provisioning succeeded
Not supported
AzureMonitorLinuxAgent
Microsoft.Azure.Monitor.AzureMonitorLinuxAgent
1.33.1
1.33.1.0
Provisioning succeeded
Disabled
Page 1 of 1


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor
Monitor | Diagnostic settings
Microsoft
Search
Refresh
Feedback
Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Investigator (preview)
Insights
Managed Services
Settings
Diagnostic settings
Data Collection Rules
Data Collection Endpoints
Azure Monitor pipelines (preview)
Autoscale
Private Link Scopes
Support + Troubleshooting
Subscription *
Free Trial
Resource group
[No filter]
Resource type
0 selected
Resource
Select any of the resources to view diagnostic settings.
Name
Resource type
Resource group
Diagnostics status
DefaultWorkspace-cfe3d784-6... Log Analytics workspace DefaultResourceGroup-CCAN Disabled
InsightScape-VM1-nsg Network security group InsightScape-RG Disabled
InsightScape-VM1-ip Public IP address InsightScape-RG Disabled
insightscape-vm1714 Network interface InsightScape-RG Disabled
InsightScape-VM2-ip Public IP address InsightScape-RG Disabled
InsightScapeVM2nsg120 Network security group InsightScape-RG Disabled
insightscape-vm2710 Network interface InsightScape-RG Disabled
ASP-InsightScapeRG-97f1 App Service plan InsightScape-RG Disabled
InsightScape-WebApp Application Insights InsightScape-RG Disabled
InsightScape-WebApp App Service InsightScape-RG Disabled
inscapescapestorage Storage account InsightScape-RG Disabled
blob Storage account InsightScape-RG Disabled
queue Storage account InsightScape-RG Disabled
table Storage account InsightScape-RG Disabled
file Storage account InsightScape-RG Disabled
InsightScape-LogicApp Logic app InsightScape-RG Enabled
DefaultWorkspace-cfe3d784-6... Log Analytics workspace DefaultResourceGroup-WUS2 Disabled
InsightScape-Vault Recovery Services vault InsightScape-RG Disabled
DefaultWorkspace-cfe3d784-6... Log Analytics workspace DefaultResourceGroup-ELIS Disabled

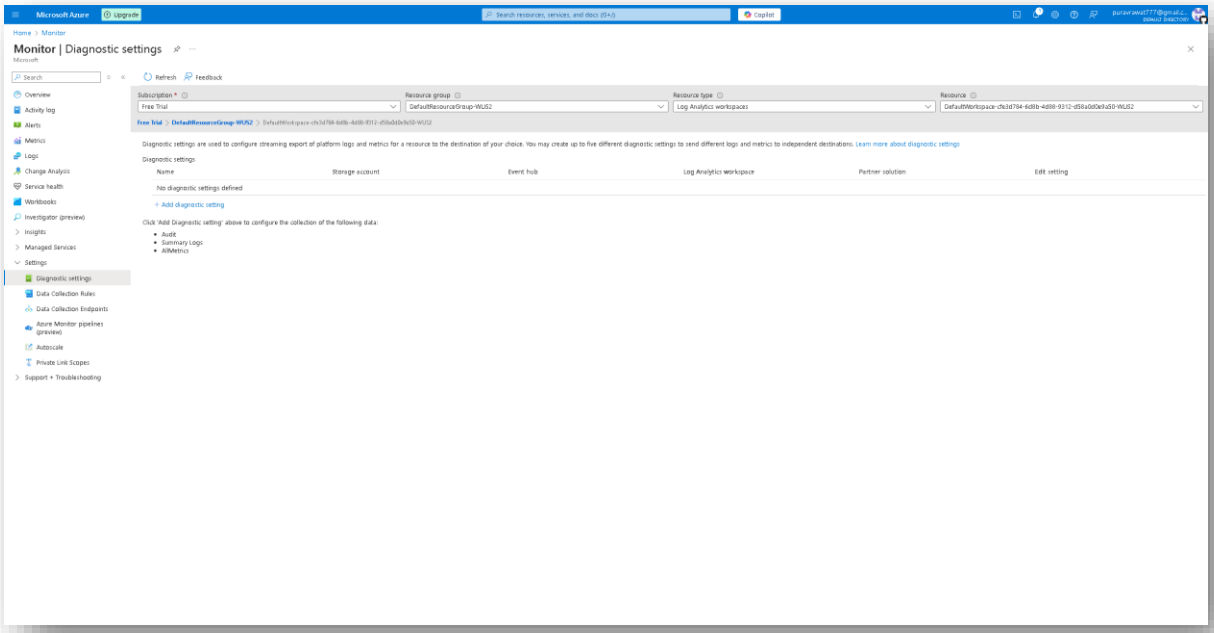

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor
Monitor | Diagnostic settings
Microsoft
Search
Refresh
Feedback
Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Investigator (preview)
Insights
Managed Services
Settings
Diagnostic settings
Data Collection Rules
Data Collection Endpoints
Azure Monitor pipelines (preview)
Autoscale
Private Link Scopes
Support + Troubleshooting
Subscription *
Free Trial
Resource group
InsightScape-RG
Resource type
App Services
Resource
InsightScape-WebApp
Free Trial > InsightScape-RG > InsightScape-WebApp
Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostic settings
Diagnostic settings
Name
Storage account
Event hub
Log Analytics workspace
Partner solution
Edit setting
No diagnostic settings defined
+ Add diagnostic setting
Click 'Add Diagnostic setting' above to configure the collection of the following data:
HTTP logs
App Service Console Logs
App Service Application Logs
Access Audit Logs
IPSecurity Audit logs
App Service Platform logs
App Service Authentication logs (preview)
AllMetrics

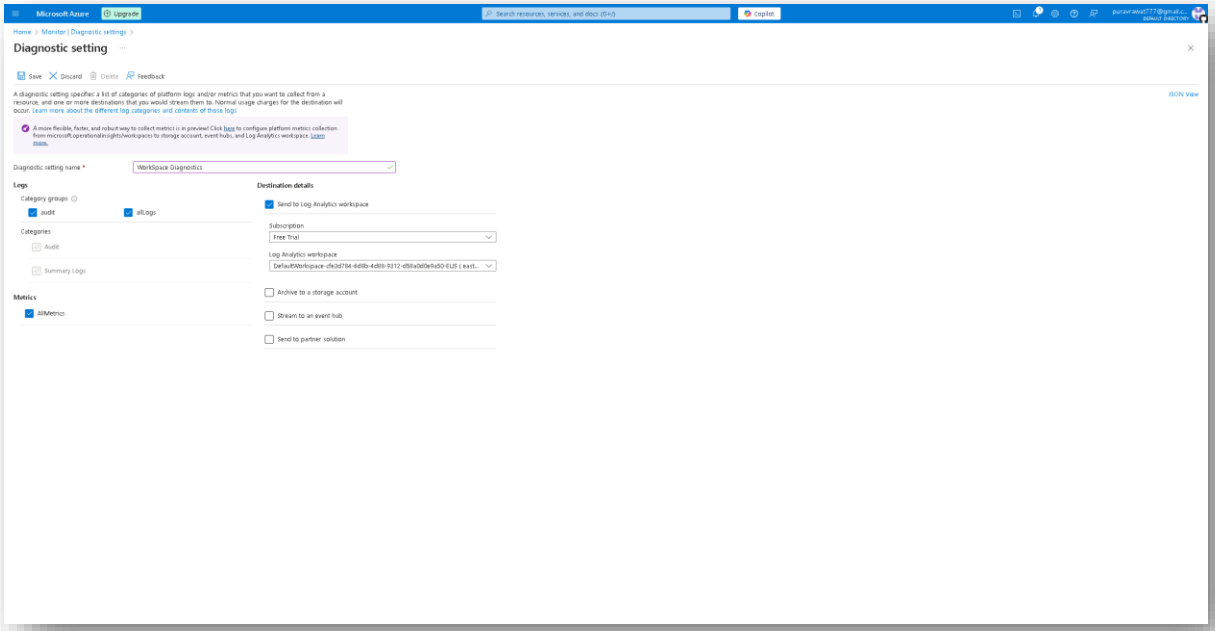

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor | Diagnostic settings >
Diagnostic setting
Save
Discard
Delete
Feedback
A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more 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
JSON View
Diagnostic setting name *
WebApp Diagnostics
Logs
Categories
HTTP logs
App Service Console Logs
App Service Application Logs
Access Audit Logs
IPSecurity Audit logs
App Service Platform logs
App Service Authentication logs (preview)
Destination details
Send to Log Analytics workspace
Subscription
Free Trial
Log Analytics workspace
Archive to a storage account
Stream to an event hub
Send to partner solution
Metrics
AllMetrics


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor
Monitor | Diagnostic settings
Microsoft
Search
Refresh
Feedback
Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Investigator (preview)
Insights
Managed Services
Settings
Diagnostic settings
Data Collection Rules
Data Collection Endpoints
Azure Monitor pipelines (preview)
Autoscale
Private Link Scopes
Support + Troubleshooting
Subscription *
Free Trial
Resource group
InsightScape-RG
Resource type
App Services
Resource
InsightScape-WebApp
Free Trial > InsightScape-RG > InsightScape-WebApp
Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostic settings
Diagnostic settings
Name
Storage account
Event hub
Log Analytics workspace
Partner solution
Edit setting
WebApp Diagnostics
Edit setting
+ Add diagnostic setting
Click 'Add Diagnostic setting' above to configure the collection of the following data:
HTTP logs
App Service Console Logs
App Service Application Logs
Access Audit Logs
IPSecurity Audit logs
App Service Platform logs
App Service Authentication logs (preview)
AllMetrics



(The "Not Connected" status in the Virtual Machines (deprecated) section indicates that the old diagnostics agents (Linux Diagnostics Agent) are no longer in use. However, since you have already installed the Azure Monitor Agent on your virtual machines, you are on the right track.)




Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor | Diagnostic settings >
Diagnostic setting
Save
Discard
Delete
Feedback
JSON View
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
A more flexible, faster, and robust way to collect metrics is in preview! Click here to configure platform metrics collection from microsoft.operationalinsights/workspaces to storage account, event hubs, and Log Analytics workspace. Learn more.
Diagnostic setting name *
Workspace Diagnostics
Logs
Category groups
audit
allLogs
Categories
Audit
Summary Logs
Metrics
AllMetrics
Destination details
Send to Log Analytics workspace
Subscription
Free Trial
Log Analytics workspace
DefaultWorkspace-cfe3d794-6d8b-4d88-9312-d581a0d0e9a0-EUS (east...
Archive to a storage account
Stream to an event hub
Send to partner solution

3) Monitor Resource Health

In this phase, my purpose and plan were to monitor the Resource Health of each of the main resources I had deployed: Virtual Machines, WebApp, and Logic App.

Virtual Machines Health Monitoring:

- I went to Resource Health under Service Health in Azure Monitor.
- I selected Virtual Machine as the resource type. After doing this, both InsightScapeVM1 and InsightScape-VM2 were listed.
- For the sake of this project, I clicked on InsightScape-VM1 to monitor the health of the VM.

WebApp Health Monitoring:

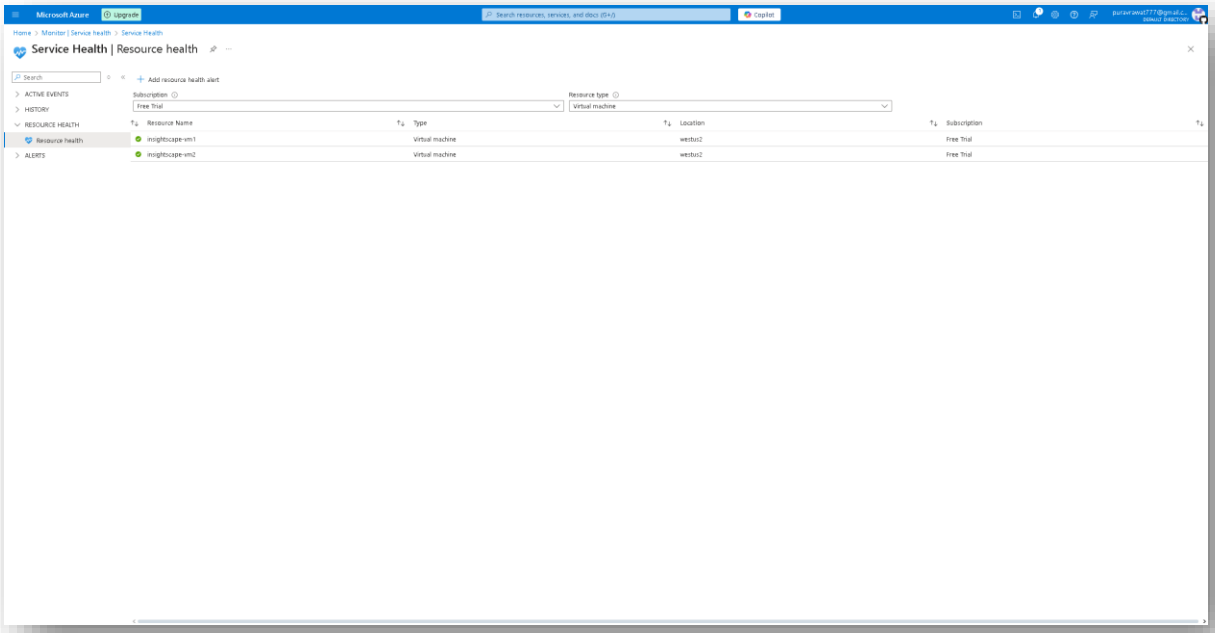
- Next, I monitored the WebApp by selecting Website as the resource type in the Resource Health tab.
- InsightScape-WebApp was listed, and I clicked on it. Upon inspecting the health, I noticed a Critical Risk alert for Health Check Failure.
- To fix this, I configured and enabled the health check, which resolved the alert. This process demonstrated that I was capable of using the Resource Health Service for the WebApp, even though I did not address all alerts as I needed to proceed with the project.

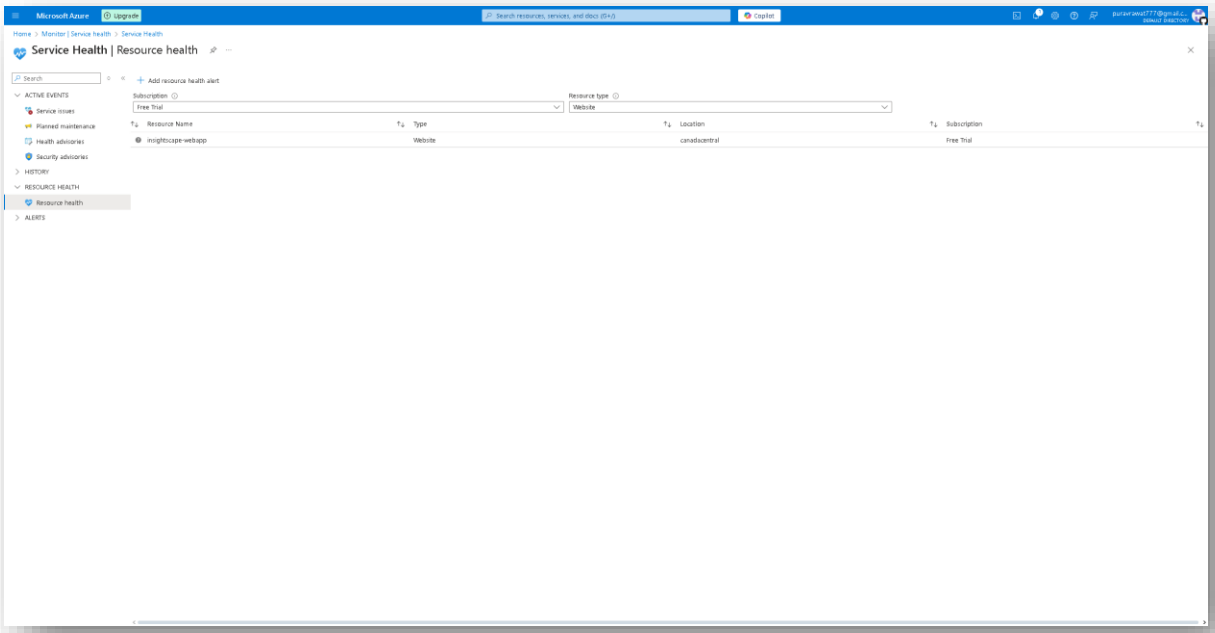
Logic App Health Monitoring:

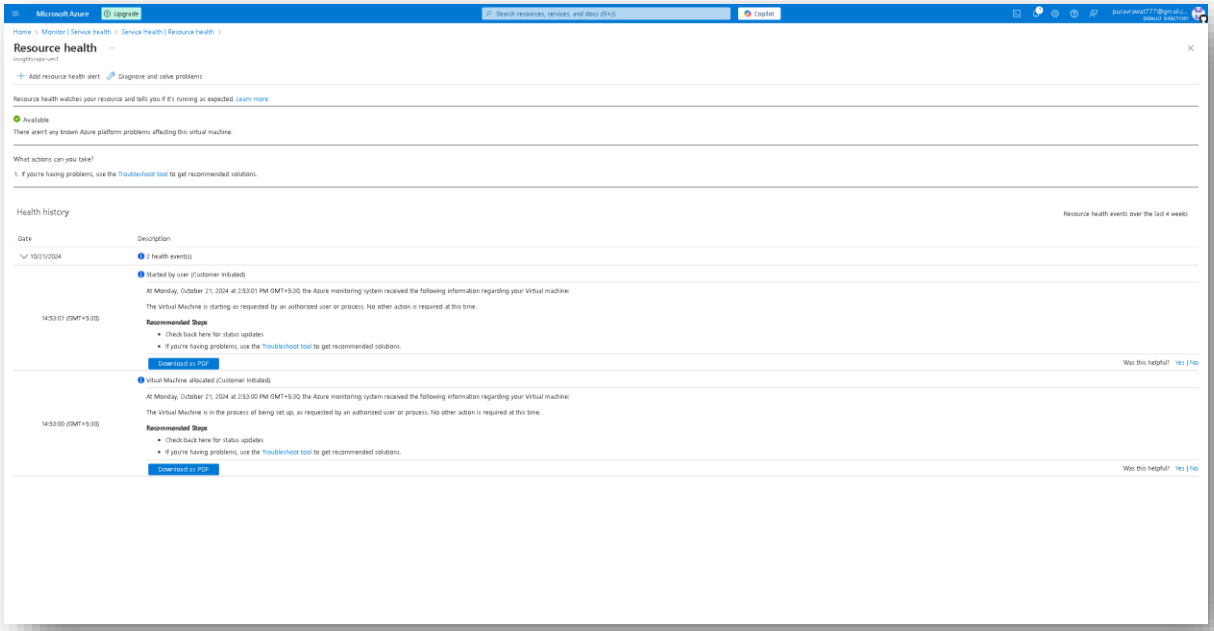
- For InsightScape-LogicApp, I used two methods to monitor health:
    - Run History Tab: I navigated to the Run History tab under Development Tools in InsightScape-LogicApp. As I had already verified in the initial phases of the project, there were two successful runs.
    - Metrics Tab: Then, I went to the Metrics tab under the Monitoring section of InsightScape-LogicApp. I selected Actions Failed as the metric and Count as the aggregation. The graph showed 0 in the metrics chart, indicating that no actions had failed.

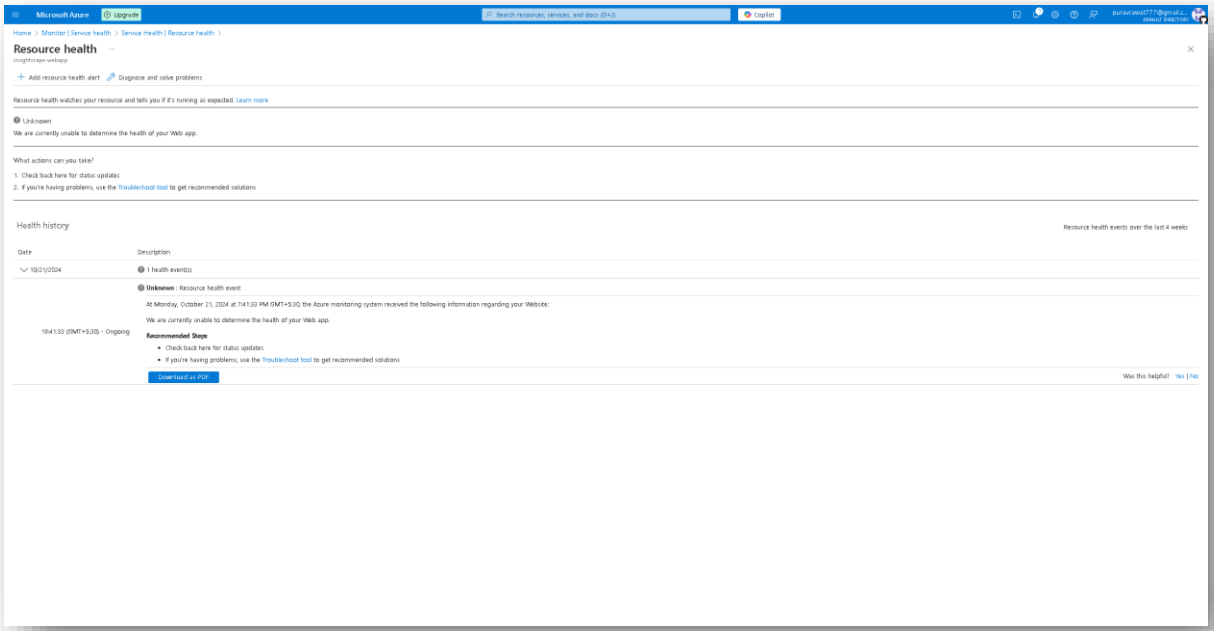
With this, the entire Step 2: Azure Monitor Integration phase was successfully and thoroughly completed.

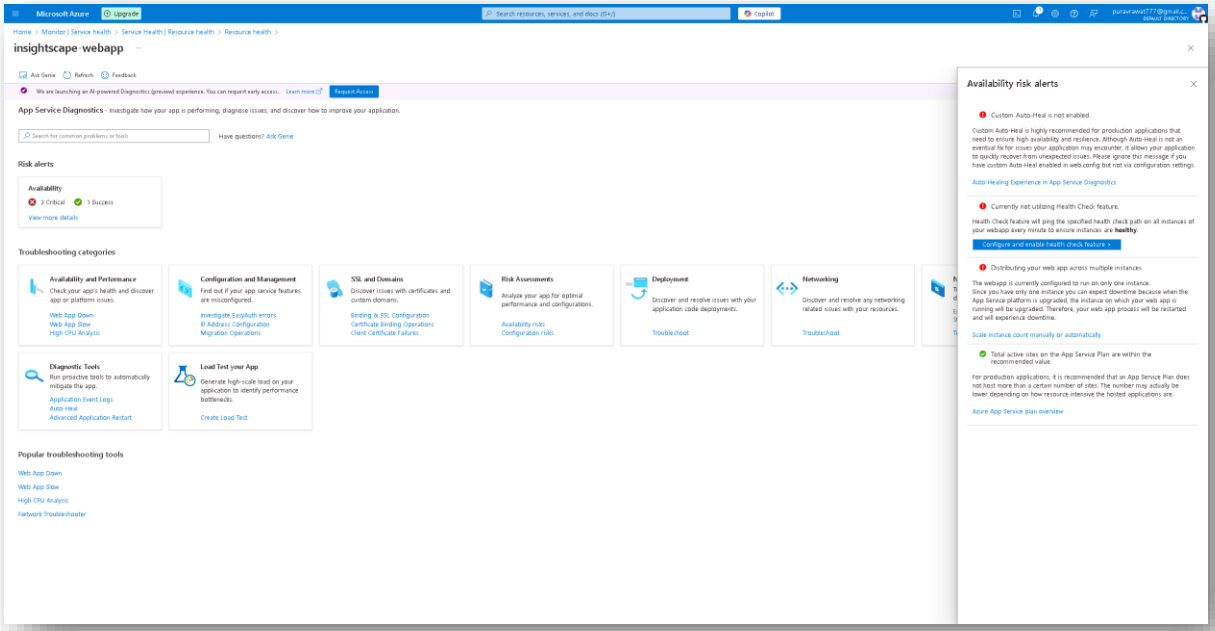
Screenshots-

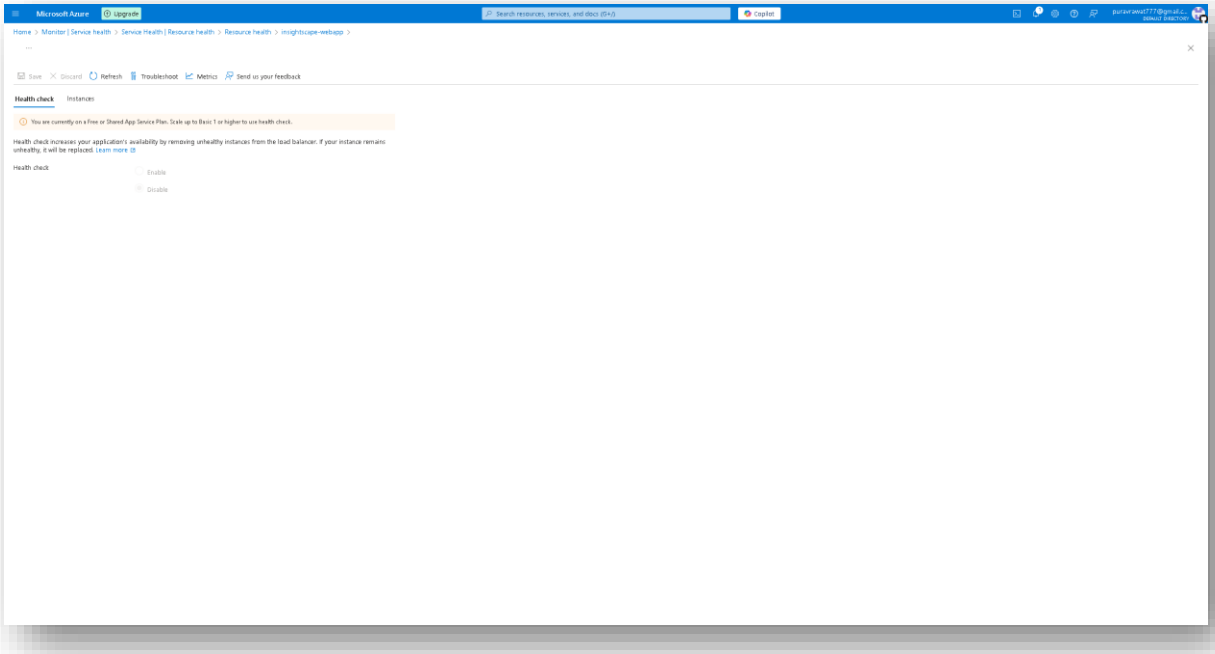


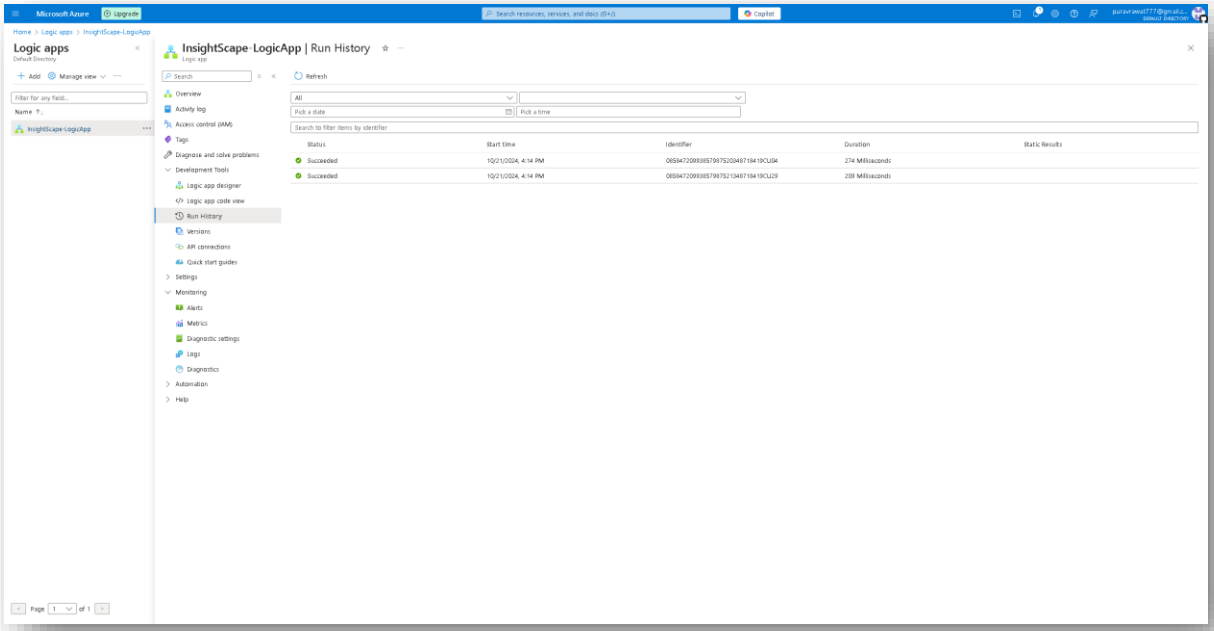


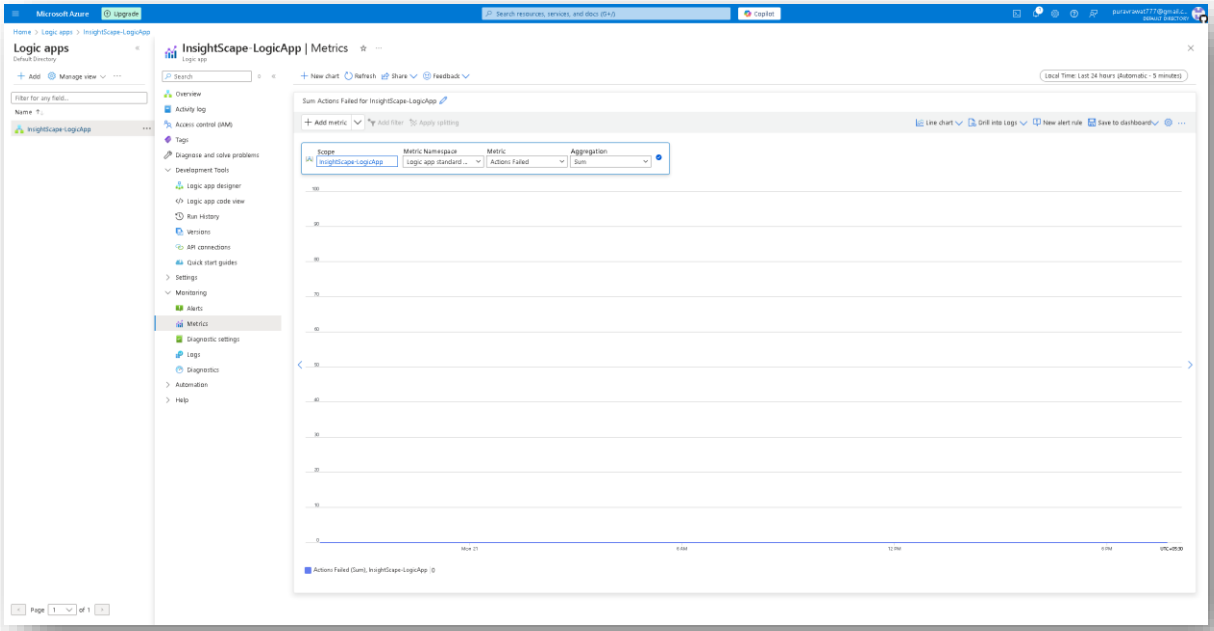

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor | Service health > Service Health | Resource health >
Resource health
insightscape-vm1
Add resource health alert
Diagnose and solve problems
Resource health watches your resource and tells you if it's running as expected. Learn more
Available
There aren't any known Azure platform problems affecting this virtual machine.
What actions can you take?
1. If you're having problems, use the Troubleshoot tool to get recommended solutions.
Health history
Resource health events over the last 4 weeks
Date
Description
10/21/2024
2 health event(s)
Started by user (Customer Initiated)
At Monday, October 21, 2024 at 2:53:01 PM GMT+5:30, the Azure monitoring system received the following information regarding your Virtual machine:
The Virtual Machine is starting as requested by an authorized user or process. No other action is required at this time.
Recommended Steps
Check back here for status updates
If you're having problems, use the Troubleshoot tool to get recommended solutions.
14:53:01 (GMT+5:30)
Download as PDF
Was this helpful? Yes | No
Virtual Machine allocated (Customer Initiated)
At Monday, October 21, 2024 at 2:53:00 PM GMT+5:30, the Azure monitoring system received the following information regarding your Virtual machine:
The Virtual Machine is in the process of being set up, as requested by an authorized user or process. No other action is required at this time.
Recommended Steps
Check back here for status updates
If you're having problems, use the Troubleshoot tool to get recommended solutions.
14:53:00 (GMT+5:30)
Download as PDF
Was this helpful? Yes | No


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor | Service health > Service Health | Resource health >
Resource health
insightscape-webapp
Add resource health alert
Diagnose and solve problems
Resource health watches your resource and tells you if it's running as expected. Learn more
Unknown
We are currently unable to determine the health of your Web app.
What actions can you take?
1. Check back here for status updates
2. If you're having problems, use the Troubleshoot tool to get recommended solutions
Health history
Resource health events over the last 4 weeks
Date
Description
10/21/2024
1 health event(s)
Unknown : Resource health event
At Monday, October 21, 2024 at 7:41:33 PM GMT+5:30, the Azure monitoring system received the following information regarding your Website:
We are currently unable to determine the health of your Web app.
Recommended Steps
Check back here for status updates
If you're having problems, use the Troubleshoot tool to get recommended solutions
19:41:33 (GMT+5:30) - Ongoing
Download as PDF
Was this helpful? Yes | No


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor | Service health > Service Health | Resource health > Resource health >
insightscape-webapp
Ask Genie
Refresh
Feedback
We are launching an AI-powered Diagnostics (preview) experience. You can request early access.
Learn more
Request Access
App Service Diagnostics - Investigate how your app is performing, diagnose issues, and discover how to improve your application.
Search for common problems or tools
Have questions? Ask Genie
Risk alerts
Availability
3 Critical
1 Success
View more details
Troubleshooting categories
Availability and Performance
Check your app's health and discover app or platform issues.
Web App Down
Web App Slow
High CPU Analysis
Configuration and Management
Find out if your app service features are misconfigured.
Investigate EasyAuth errors
IP Address Configuration
Migration Operations
SSL and Domains
Discover issues with certificates and custom domains.
Binding & SSL Configuration
Certificate Binding Operations
Client Certificate Failures
Risk Assessments
Analyze your app for optimal performance and configurations.
Availability risks
Configuration risks
Deployment
Discover and resolve issues with your application code deployments.
Troubleshoot
Networking
Discover and resolve any networking related issues with your resources.
Troubleshoot
Diagnostic Tools
Run proactive tools to automatically mitigate the app.
Application Event Logs
Auto-Heal
Advanced Application Restart
Load Test your App
Generate high-scale load on your application to identify performance bottlenecks.
Create Load Test
Popular troubleshooting tools
Web App Down
Web App Slow
High CPU Analysis
Network Troubleshooter
Availability risk alerts
Custom Auto-Heal is not enabled.
Custom Auto-Heal is highly recommended for production applications that need to ensure high availability and resilience. Although Auto-Heal is not an eventual fix for issues your application may encounter, it allows your application to quickly recover from unexpected issues. Please ignore this message if you have custom Auto-Heal enabled in web.config but not via configuration settings.
Auto-Healing Experience in App Service Diagnostics
Currently not utilizing Health Check feature.
Health Check feature will ping the specified health check path on all instances of your webapp every minute to ensure instances are healthy.
Configure and enable health check feature >
Distributing your web app across multiple instances
The webapp is currently configured to run on only one instance. Since you have only one instance you can expect downtime because when the App Service platform is upgraded, the instance on which your web app is running will be upgraded. Therefore, your web app process will be restarted and will experience downtime.
Scale instance count manually or automatically
Total active sites on the App Service Plan are within the recommended value
For production applications, it is recommended that an App Service Plan does not host more than a certain number of sites. The number may actually be lower depending on how resource intensive the hosted applications are.
Azure App Service plan overview


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor | Service health > Service Health | Resource health > Resource health > insightscape-webapp >
Save
Discard
Refresh
Troubleshoot
Metrics
Send us your feedback
Health check
Instances
You are currently on a Free or Shared App Service Plan. Scale up to Basic 1 or higher to use health check.
Health check increases your application's availability by removing unhealthy instances from the load balancer. If your instance remains unhealthy, it will be replaced. Learn more
Health check
Enable
Disable


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Logic apps > InsightScape-LogicApp
Logic apps
Default Directory
Add
Manage view
Filter for any field...
Name
InsightScape-LogicApp
InsightScape-LogicApp | Run History
Logic app
Search
Refresh
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Run History
Versions
API connections
Quick start guides
Settings
Monitoring
Alerts
Metrics
Diagnostic settings
Logs
Diagnostics
Automation
Help
All
Pick a date
Pick a time
Search to filter items by identifier
Status
Start time
Identifier
Duration
Static Results
Succeeded
10/21/2024, 4:14 PM
274 Milliseconds
Succeeded
10/21/2024, 4:14 PM
209 Milliseconds
Page 1 of 1


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Logic apps > InsightScape-LogicApp
Logic apps
Default Directory
Add
Manage view
Filter for any field...
Name
InsightScape-LogicApp
InsightScape-LogicApp | Metrics
Logic app
Search
New chart
Refresh
Share
Feedback
Local Time: Last 24 hours (Automatic - 5 minutes)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Run History
Versions
API connections
Quick start guides
Settings
Monitoring
Alerts
Metrics
Diagnostic settings
Logs
Diagnostics
Automation
Help
Sum Actions Failed for InsightScape-LogicApp
Add metric
Add filter
Apply splitting
Line chart
Drill into Logs
New alert rule
Save to dashboard
Scope
InsightScape-LogicApp
Metric Namespace
Logic app standard ...
Metric
Actions Failed
Aggregation
Sum
100
90
80
70
60
50
40
30
20
10
0
Mon 21
6 AM
12 PM
6 PM
UTC+05:30
Actions Failed (Sum), InsightScape-LogicApp
Page 1 of 1

Application Insights

In this phase of the project, my plan was to work with and monitor the **WebApp** through **Application Insights.**

a) Overview Page Monitoring

First, I went to Application Insights in the Azure Portal.

- In the Overview Page of the InsightScape-WebApp's Application Insights, I monitored the charts showing:
    - Failed Requests: Number of failed requests.
    - Server Response Time: Average response time of the server.
    - Server Requests: Count of server requests.
    - Availability: Uptime metrics of the web app.

b) Performance Analysis

Next, to monitor performance in more detail, I navigated to the Performance Tab under Investigate in Application Insights.

- Operations Page:
    - I analyzed in-depth how different operations within the application were executed, including evaluating their response times, success rates, and performance metrics across various endpoints.
    - This provided a holistic view of the application's efficiency and areas requiring optimization over time.
- Roles Page:
    - Within the same Performance tab, I accessed the Roles Page.
    - I analyzed performance metrics for different roles within the application, focusing on indicators such as:
        - CPU Usage
        - Memory Availability
        - Request Rates
        - Average Request Duration
    - The goal was to identify any deviations or bottlenecks specific to each role, ensuring that individual components are effectively optimized and balanced for overall application efficiency.

c) Failure Analysis

Then, I moved to the Failures Tab under Investigate in Application Insights.

- In the Roles Page within the Failures Tab, I analyzed the failure metrics for different roles in the application, focusing on key aspects such as:

    - Dependency Failures: Failures in external dependencies.
    - Failed Requests: Failed HTTP requests.
    - Total Exceptions: Number of exceptions thrown by the application.
- This helped identify problem areas that could impact the application's reliability and stability, allowing for targeted improvements and better fault tolerance.

d) User Analysis

Next, I went to the Users Tab under Usage in Application Insights.

- I analyzed user interactions with the application, including metrics such as:
    - Number of Sessions: How many sessions were initiated by users.
    - Events Triggered: User-generated events in the application.
    - User Demographics: Details like user location and browser types.
- This data helped me understand how users engaged with the web application, identify any performance concerns, and evaluate the overall user experience and satisfaction.

e) Live Metrics

Then, I went to the Live Metrics tab to monitor real-time telemetry for the InsightScapeWebApp.

- I set up real-time telemetry to monitor the performance of the WebApp, demonstrating my skills in Azure resource monitoring and maintenance.
- At the time of observation, data was temporarily unavailable, which can happen due to temporary backend issues or configuration updates.
- I resolved the issue by verifying the Instrumentation Key and restarting the application to refresh the connection. After this, I was able to proceed successfully.

f) Diagnostics Settings

After completing performance, failure, and user analysis, I added Diagnostic Settings for the Application Insights:

- Diagnostic Setting Name: AppInsights-Diagnostics
- Logs:
    - allLogs (Ticked)
- Destination Details:
    - Send to Log Analytics Workspace: Selected the Default Log Analytics workspace.

g) Dashboard Analysis

In the end, I accessed the InsightScape-WebApp Dashboard to analyze the consolidated telemetry data across various aspects of the application, including:

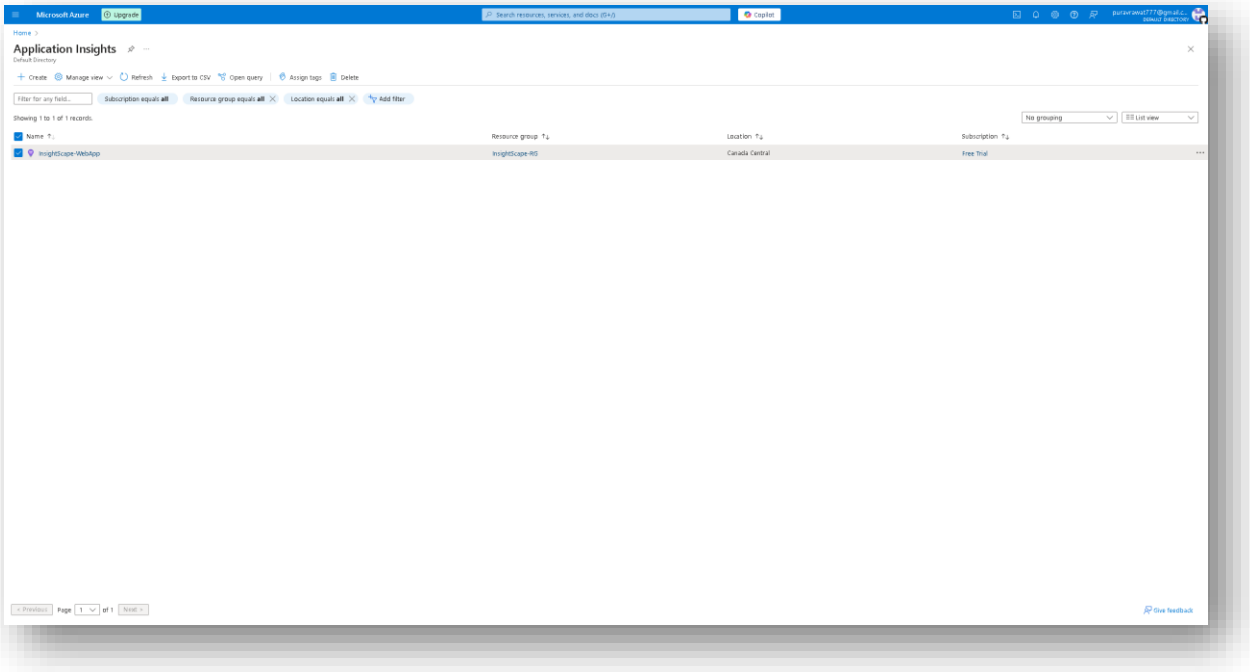
- Usage: Number of sessions and unique users.
- Reliability: Failed requests and server errors.

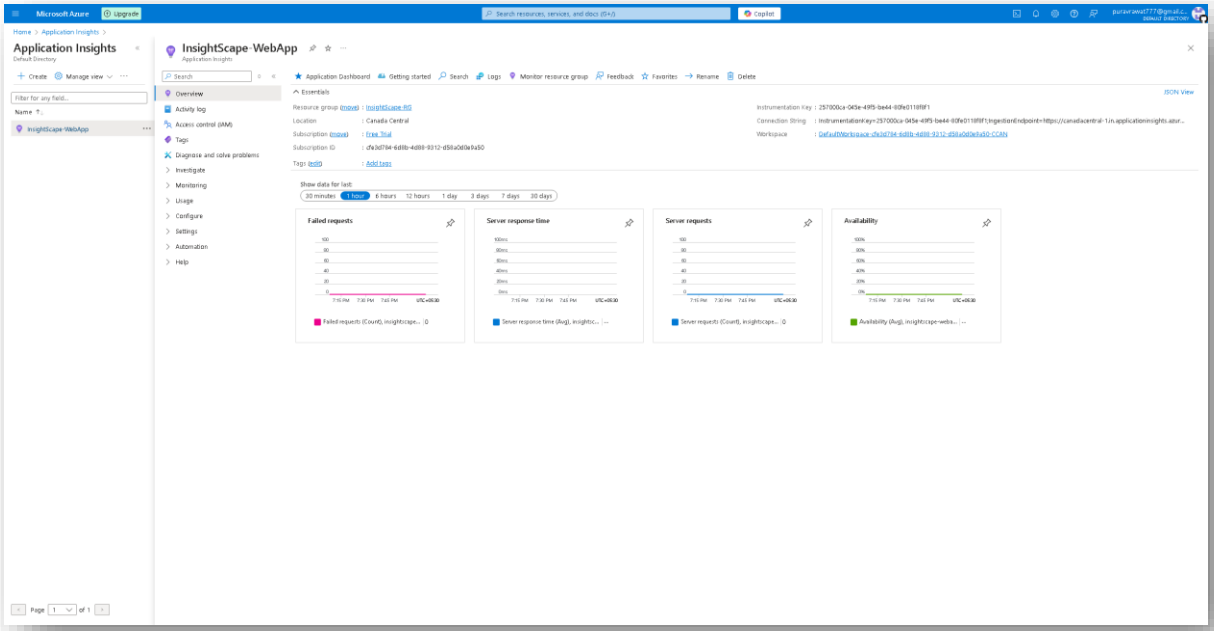
- Responsiveness: Average server response times.
- Resource Utilization: CPU and memory usage for the web app.

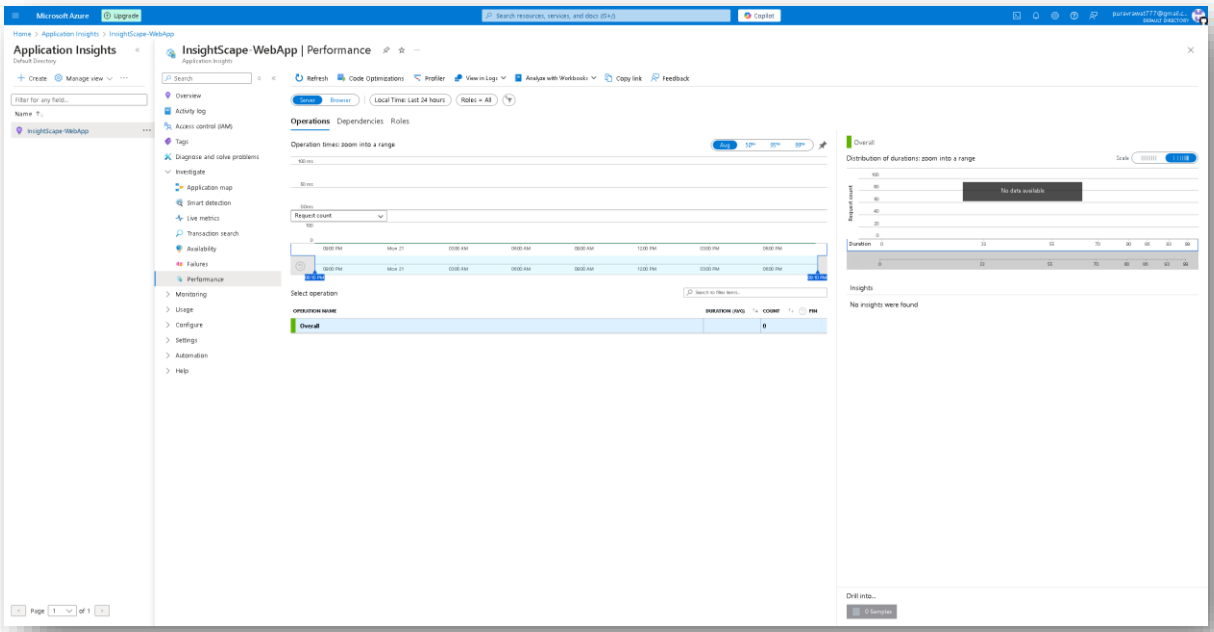
I focused on metrics such as unique sessions, server response times, and failed requests to gain insights into the overall health and performance of the application, ensuring all key components were functioning optimally.

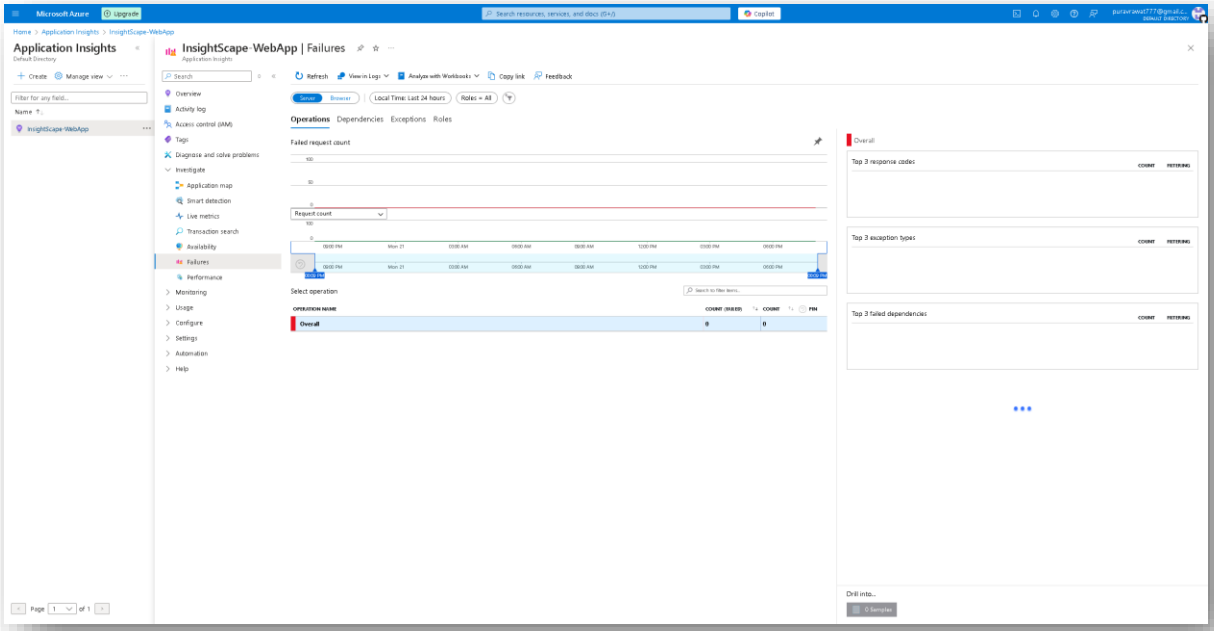
With this, the entire Step 3: Application Insights phase of the project was successfully completed.

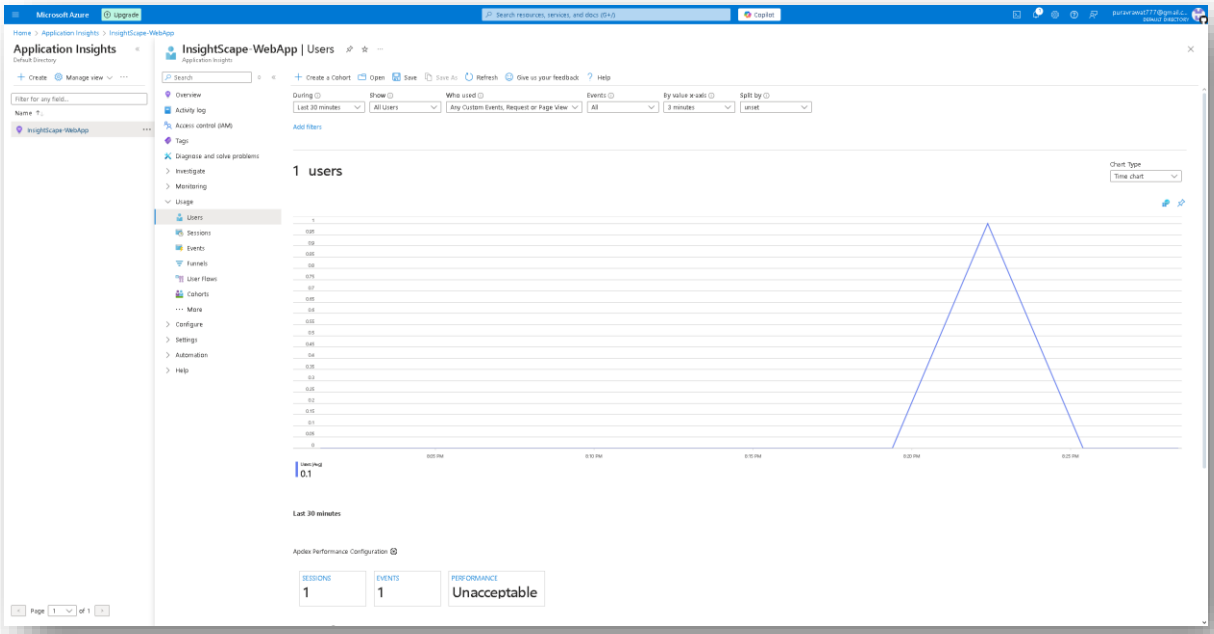
Screenshots-

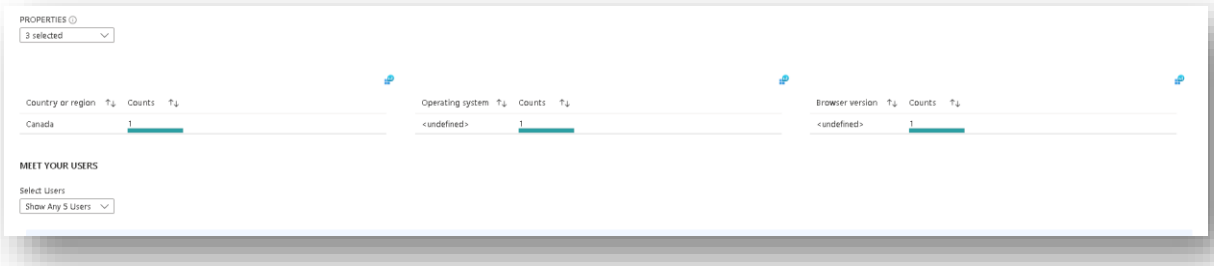


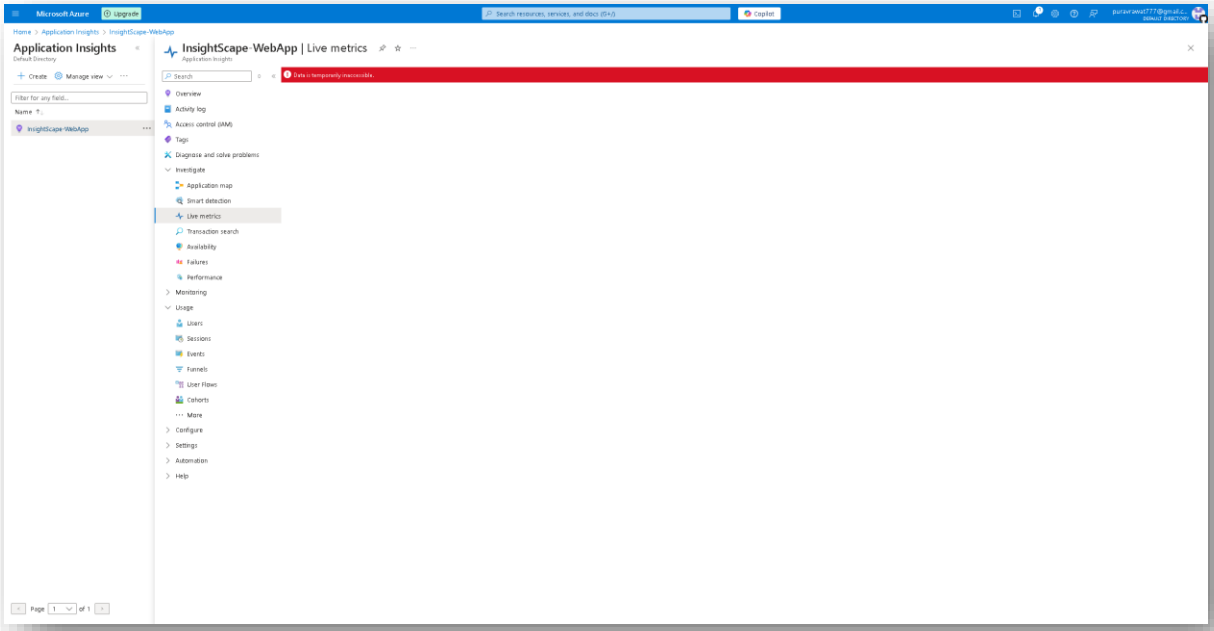

Microsoft Azure
Upgrade
Copilot
Application Insights
InsightScape-WebApp
Application Insights
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Investigate
Monitoring
Usage
Configure
Settings
Automation
Help
Application Dashboard
Getting started
Search
Logs
Monitor resource group
Feedback
Favorites
Rename
Delete
Essentials
JSON View
Failed requests
Server response time
Server requests
Availability

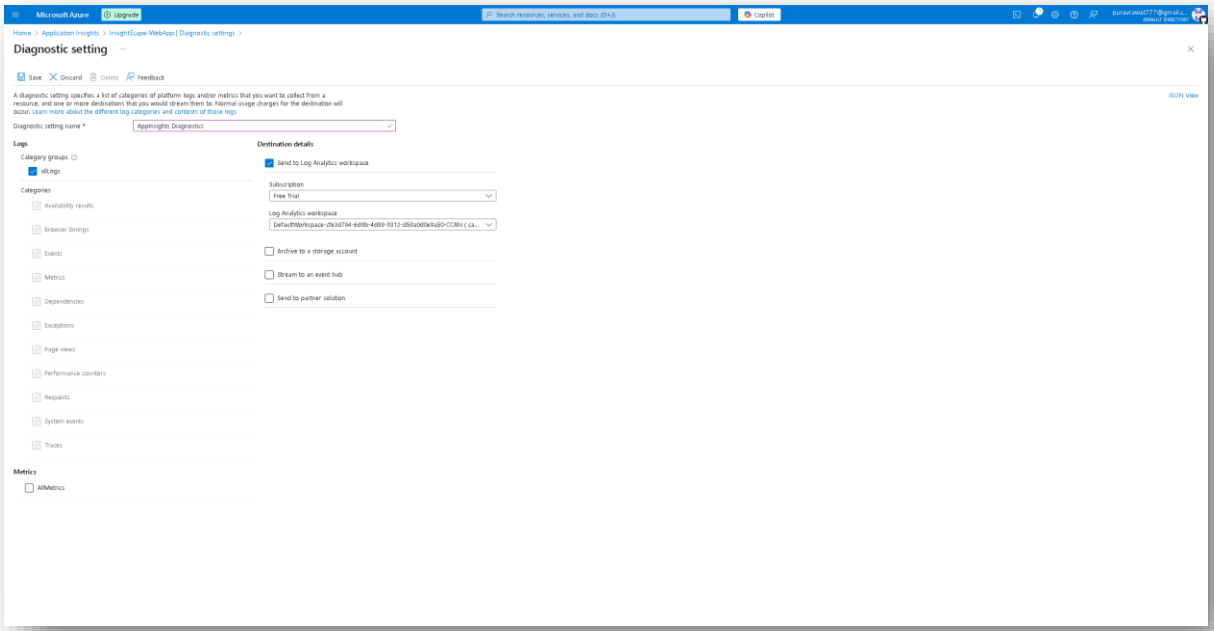

Microsoft Azure
Upgrade
Copilot
Application Insights
InsightScape-WebApp | Performance
Application Insights
Refresh
Code Optimizations
Profiler
View in Logs
Analyze with Workbooks
Copy link
Feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Investigate
Application map
Smart detection
Live metrics
Transaction search
Availability
Failures
Performance
Monitoring
Usage
Configure
Settings
Automation
Help
Operations
Dependencies
Roles
Operation times: zoom into a range
Distribution of durations: zoom into a range
No data available
Select operation
Insights
No insights were found
Drill into...

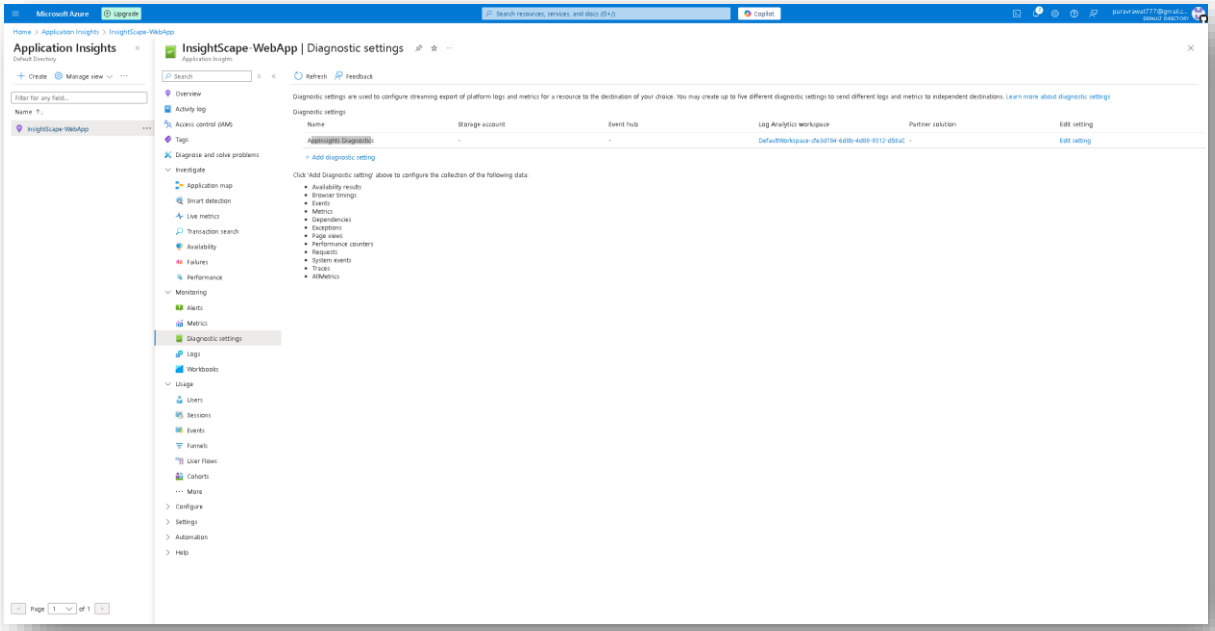

Microsoft Azure
Application Insights
InsightScope-WebApp | Failures
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Investigate
Application map
Smart detection
Live metrics
Transaction search
Availability
Failures
Performance
Monitoring
Usage
Configure
Settings
Automation
Help
Refresh
View in Logs
Analyze with Workbooks
Copy link
Feedback
Local Time: Last 24 hours
Operations
Dependencies
Exceptions
Roles
Failed request count
Request count
Select operation
Overall
Top 3 response codes
Top 3 exception types
Top 3 failed dependencies
Drill into...


Microsoft Azure
Application Insights
InsightScope-WebApp | Users
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Investigate
Monitoring
Usage
Users
Sessions
Events
Funnels
User Flows
Cohorts
More
Configure
Settings
Automation
Help
Create a Cohort
Open
Save
Refresh
Give us your feedback
Help
Add filters
1 users
Chart Type
Time chart
0.1
Last 30 minutes
Apdex Performance Configuration
SESSIONS
1
EVENTS
1
PERFORMANCE
Unacceptable


PROPERTIES
3 selected
Country or region
Counts
Canada
1
Operating system
Counts
<undefined>
1
Browser version
Counts
<undefined>
1
MEET YOUR USERS
Select Users
Show Any 5 Users


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Application Insights > InsightScope-WebApp
Application Insights
Default Directory
Create
Manage view
Filter for any field...
Name
InsightScope-WebApp
InsightScope-WebApp | Live metrics
Application Insights
Search
Data is temporarily inaccessible.
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Investigate
Application map
Smart detection
Live metrics
Transaction search
Availability
Failures
Performance
Monitoring
Usage
Users
Sessions
Events
Funnels
User Flows
Cohorts
More
Configure
Settings
Automation
Help
Page 1 of 1


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Application Insights > InsightScope-WebApp | Diagnostic settings >
Diagnostic setting
Save
Discard
Delete
Feedback
JSON View
Diagnostic setting name *
AppInsights Diagnostics
Logs
Category groups
allLogs
Categories
Availability results
Browser timings
Events
Metrics
Dependencies
Exceptions
Page views
Performance counters
Requests
System events
Traces
Metrics
AllMetrics
Destination details
Send to Log Analytics workspace
Subscription
Free Trial
Log Analytics workspace
Archive to a storage account
Stream to an event hub
Send to partner solution


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Application Insights > InsightScape-WebApp
Application Insights
Default Directory
Create
Manage view
Filter for any field...
Name
InsightScape-WebApp
InsightScape-WebApp | Diagnostic settings
Application Insights
Search
Refresh
Feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Investigate
Application map
Smart detection
Live metrics
Transaction search
Availability
Failures
Performance
Monitoring
Alerts
Metrics
Diagnostic settings
Logs
Workbooks
Usage
Users
Sessions
Events
Funnels
User Flows
Cohorts
More
Configure
Settings
Automation
Help
Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostic settings
Diagnostic settings
Name
Storage account
Event hub
Log Analytics workspace
Partner solution
Edit setting
Add diagnostic setting
Click 'Add Diagnostic setting' above to configure the collection of the following data:
Availability results
Browser timings
Events
Metrics
Dependencies
Exceptions
Page views
Performance counters
Requests
System events
Traces
AllMetrics
Page 1 of 1

Network Monitoring

In this phase of the project, my goal was to work with Network Watcher to monitor and analyze network resources effectively.

a) Network Topology Analysis

First of all, I went to Network Watcher for my region, which was "**NetworkWatcher_westus2**".

- I navigated to the Topology feature under Monitoring in Network Watcher.
- I selected the following scope:
    - Resource Group: InsightScape-RG
    - Location:West US 2
- Using the Network Watcher Topology feature, I visualized and analyzed the network infrastructure of my Azure environment. This tool provided:
    - A geographic overview and detailed topology of resources like:
        - Virtual Networks
        - Subnets
        - Network Security Groups (NSGs)
        - Virtual Machines (VMs)
    - By exploring the different tabs, such as Geo Map and Virtual Network, I could:
        - Pinpoint the deployment location of resources.
        - Examine network configuration details.
        - Assess how different components interact.
    - This comprehensive view helped me identify network bottlenecks, connectivity issues, and ensured optimal resource allocation across Azure regions.

b) NSG Diagnostics

Next, I proceeded to work with NSG diagnostics, which is available under Network Diagnostic Tools in Network Watcher.

- First, I accessed both VMs' NSGs (InsightScape-VM1-nsg and InsightScape-VM2-nsg) to analyze their inbound and outbound rules.
    - I noticed that Port 80 Inbound Access was allowed from any network in the InsightScape-VM1-nsg.
    - This made it an ideal scenario for testing with NSG diagnostics.

NSG Diagnostics Test 1: Allow Traffic

I went to the NSG diagnostics tool and configured the following settings:

- Target Resource:

    - Target Resource Type: Virtual Machine
    - Virtual Machine: InsightScape-VM1
- Traffic Details:
    - Protocol: TCP
    - Direction: Inbound
    - Source Type: IPv4 Address/CIDR
    - IPv4 Address/CIDR: 192.168.0.1 (Random IP)
    - Destination IP Address: 52.170.47.103 (Public IP of InsightScape-VM1)
    - Destination Port: 80

After entering these configurations, I clicked on "Run NSG diagnostic".

- Results:
    - Traffic Status:

Allowed NSG Diagnostics Test 2: Deny Traffic.

Next, I wanted to test a different scenario. I specifically added a new Inbound Security Rule in InsightScape-VM1-nsg:

- Priority: 100 (Lower priority than the other rules)
- Name: DenyCidrBlockHTTPInbound-Simulation
- Port: 80
- Protocol: TCP
- Source: 192.168.0.1 (Random IP)
- Destination: 52.170.47.103 (Public IP of InsightScape-VM1)
- Action: Deny

After adding this rule, I ran the NSG diagnostic again with the following settings:

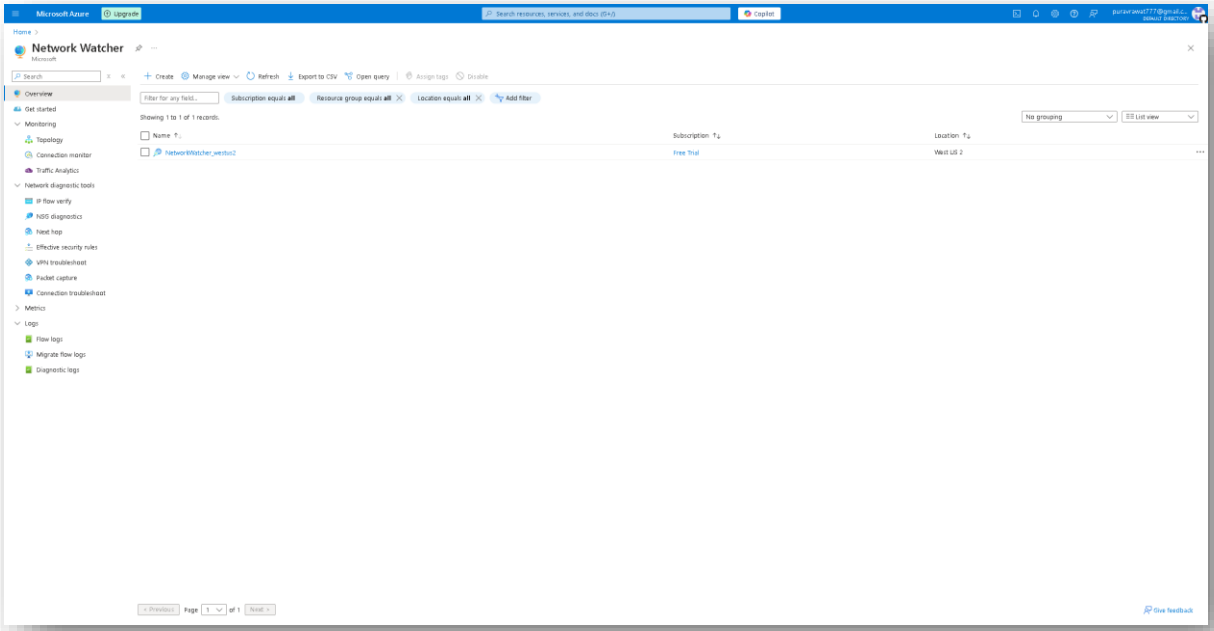
- Target Resource:
    - Target Resource Type: Virtual Machine
    - Virtual Machine: InsightScape-VM1
- Traffic Details:
    - Protocol: TCP
    - Direction: Inbound o Source Type: IPv4 Address/CIDR
    - IPv4 Address/CIDR: 10.1.1.0 (Random IP)
    - Destination IP Address: 52.170.47.103 (Public IP of InsightScape-VM1) o
    - Destination Port: 80
- Results:
    - Traffic Status: Denied

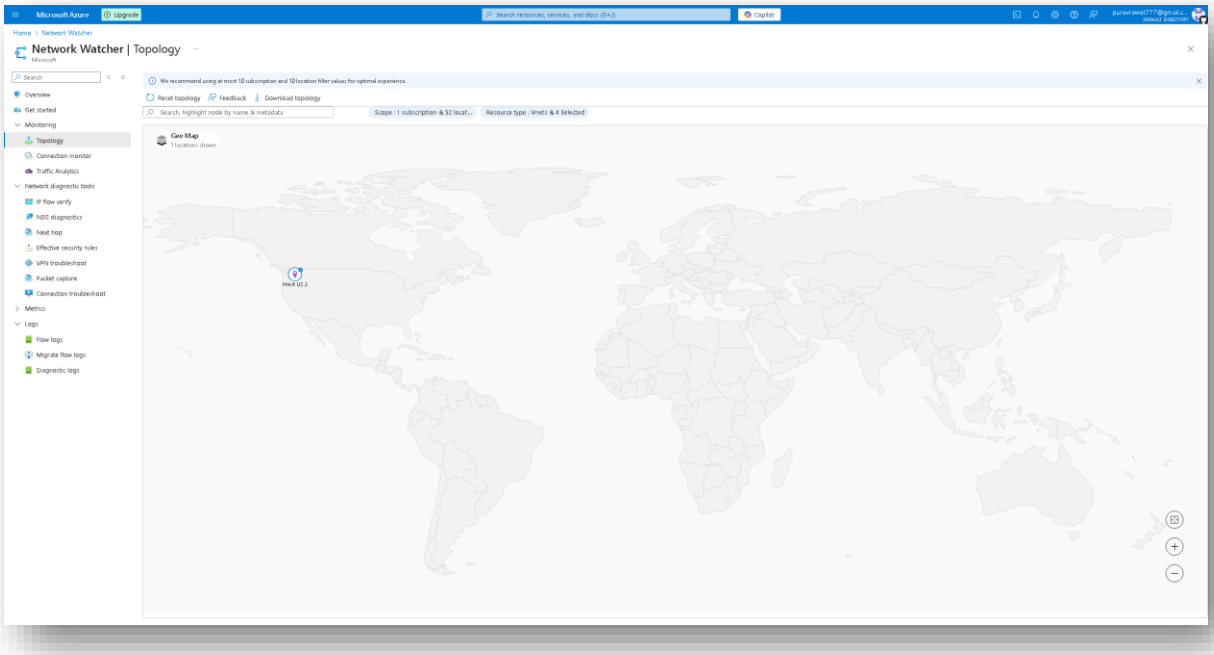
c) Conclusion

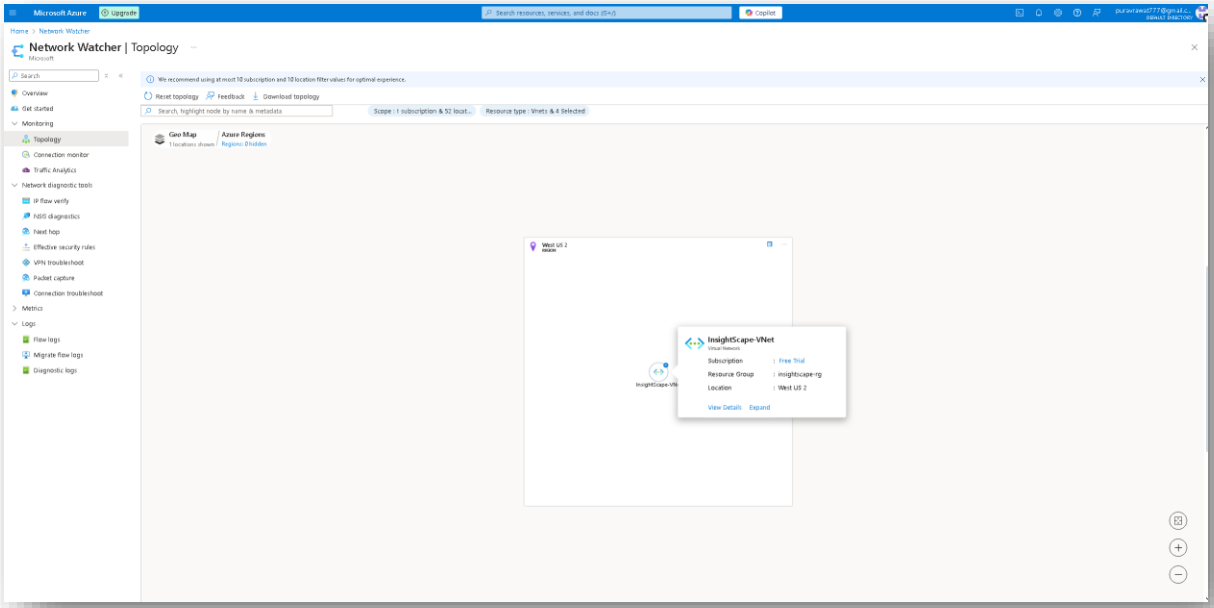
With these tests, I successfully demonstrated the use of NSG diagnostics to validate inbound traffic configurations and to verify how security rules impacted traffic flow to the virtual machines.

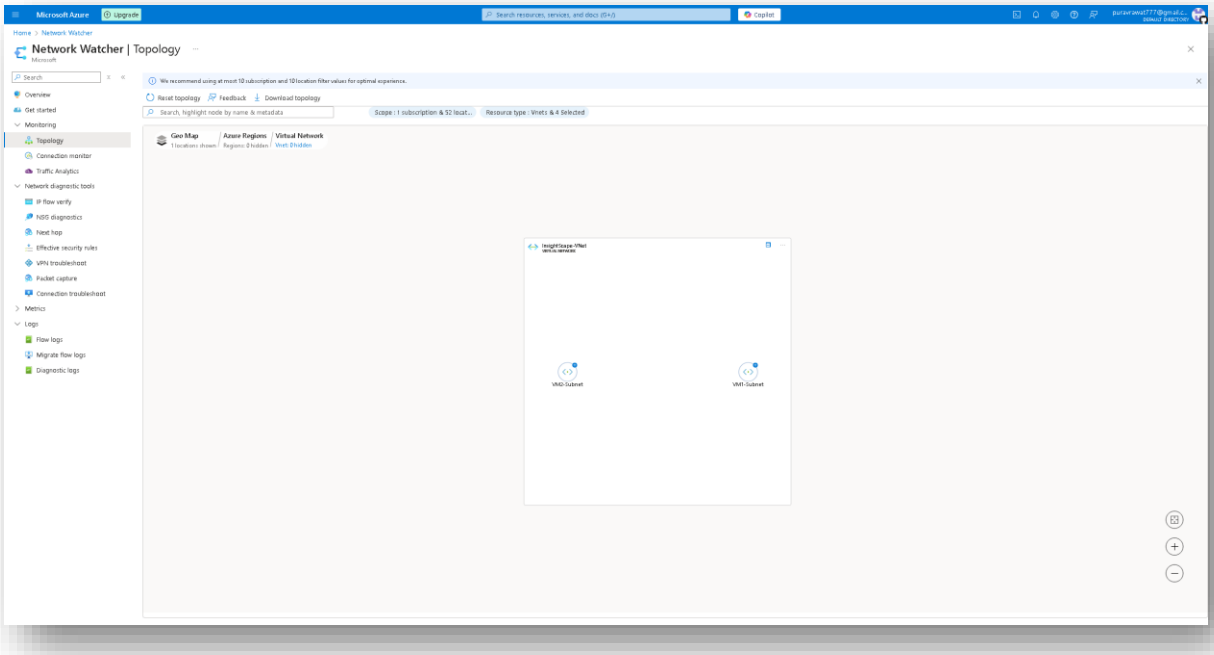
This concluded the Step 4: Network Monitoring phase of the project, and it was successfully completed.

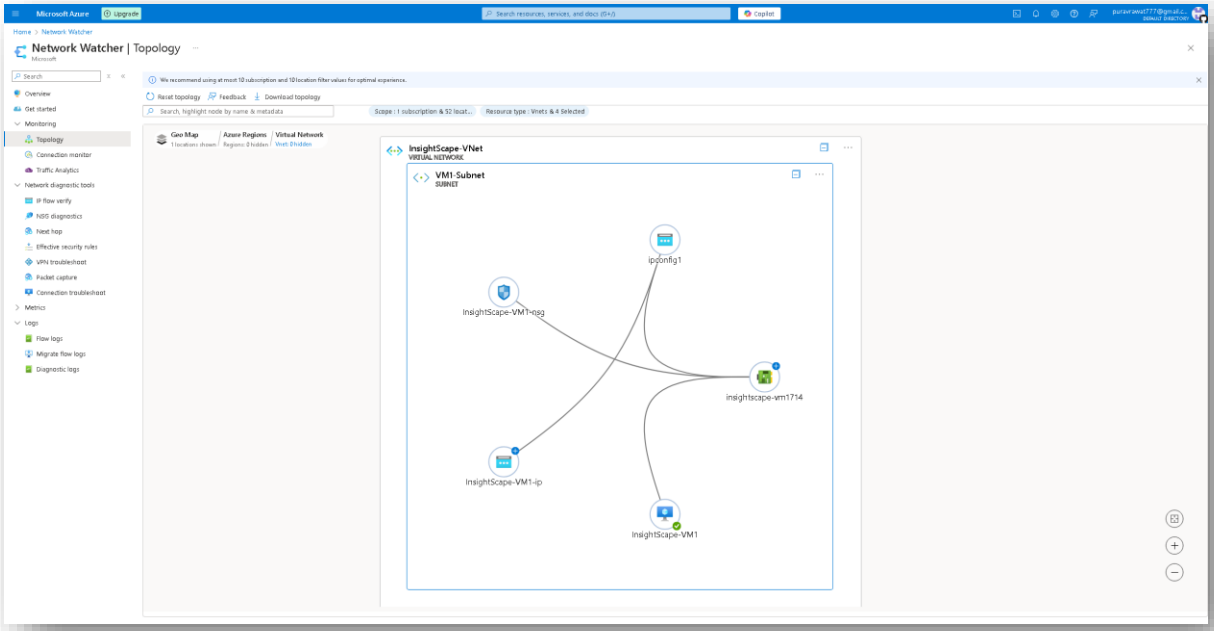
Screenshots-

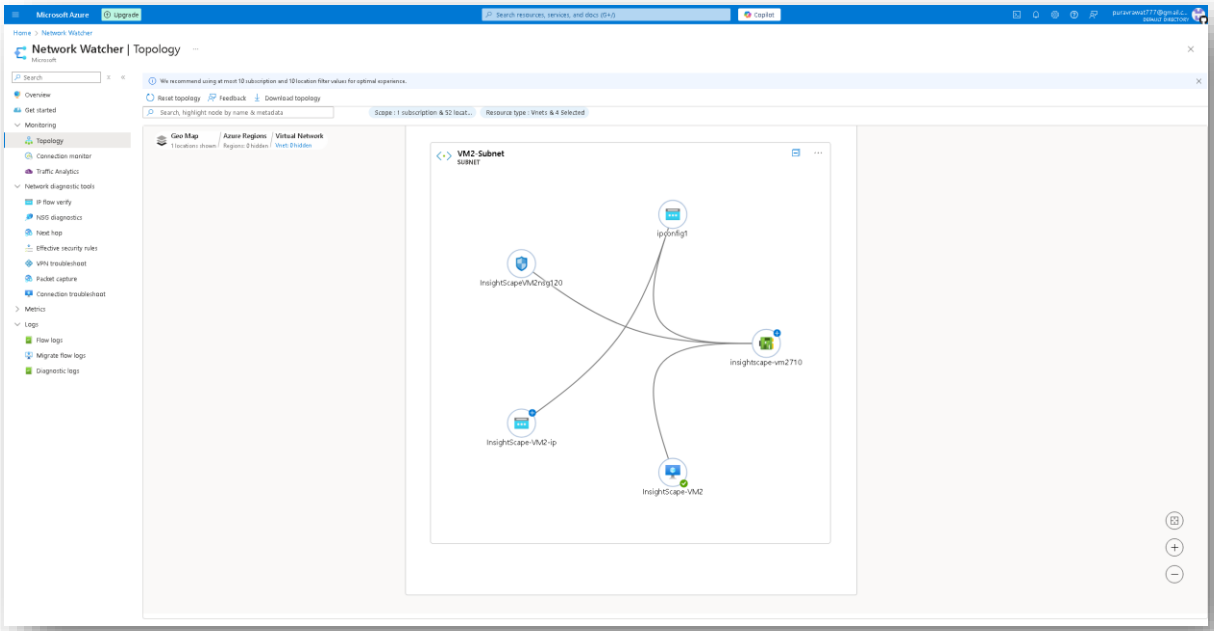


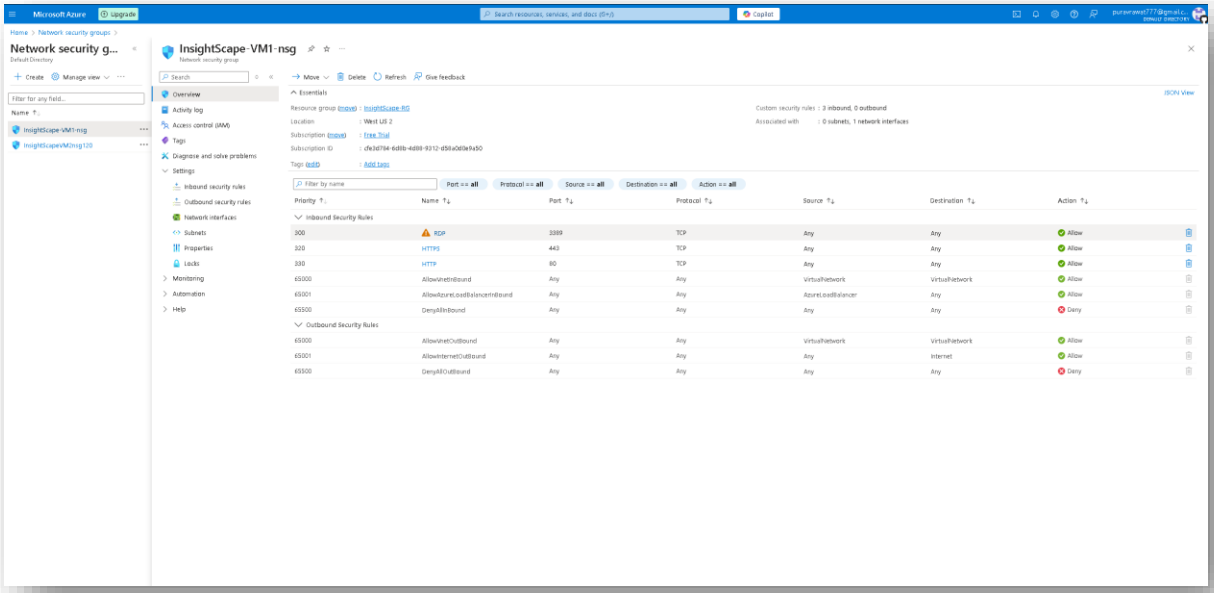


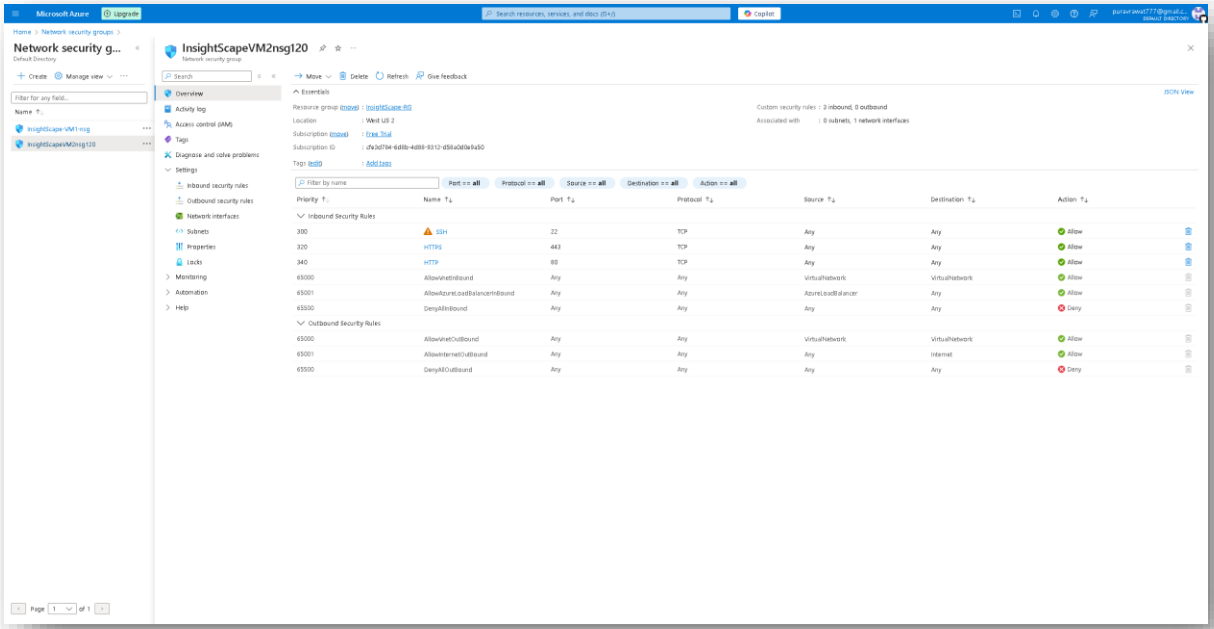

Microsoft Azure
Upgrade
Copilot
Home > Network Watcher
Network Watcher | Topology
Microsoft
Search
Overview
Get started
Monitoring
Topology
Connection monitor
Traffic Analytics
Network diagnostic tools
IP flow verify
NSG diagnostics
Next hop
Effective security rules
VPN troubleshoot
Packet capture
Connection troubleshoot
Metrics
Logs
Flow logs
Migrate flow logs
Diagnostic logs
We recommend using at most 10 subscription and 10 location filter values for optimal experience.
Reset topology
Feedback
Download topology
Search, highlight node by name & metadata
Scope : 1 subscription & 52 locat...
Resource type : Vnets & 4 Selected
Geo Map
1 locations shown
Azure Regions
Regions: 0 hidden
West US 2
InsightScape-VNet
Virtual Network
Subscription : Free Trial
Resource Group : insightscape-rg
Location : West US 2
View Details
Expand

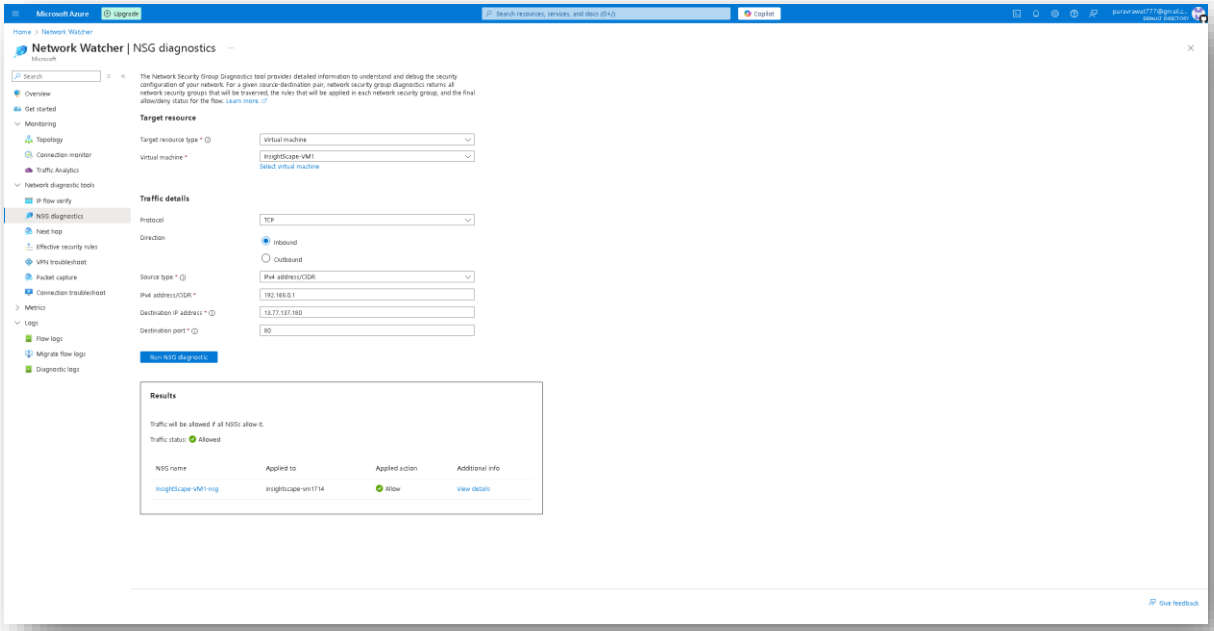

Microsoft Azure
Upgrade
Copilot
Home > Network Watcher
Network Watcher | Topology
Microsoft
Search
Overview
Get started
Monitoring
Topology
Connection monitor
Traffic Analytics
Network diagnostic tools
IP flow verify
NSG diagnostics
Next hop
Effective security rules
VPN troubleshoot
Packet capture
Connection troubleshoot
Metrics
Logs
Flow logs
Migrate flow logs
Diagnostic logs
We recommend using at most 10 subscription and 10 location filter values for optimal experience.
Reset topology
Feedback
Download topology
Search, highlight node by name & metadata
Scope : 1 subscription & 52 locat...
Resource type : Vnets & 4 Selected
Geo Map
1 locations shown
Azure Regions
Regions: 0 hidden
Virtual Network
Vnet: 0 hidden
InsightScape-VNet
VM0-Subnet
VM1-Subnet

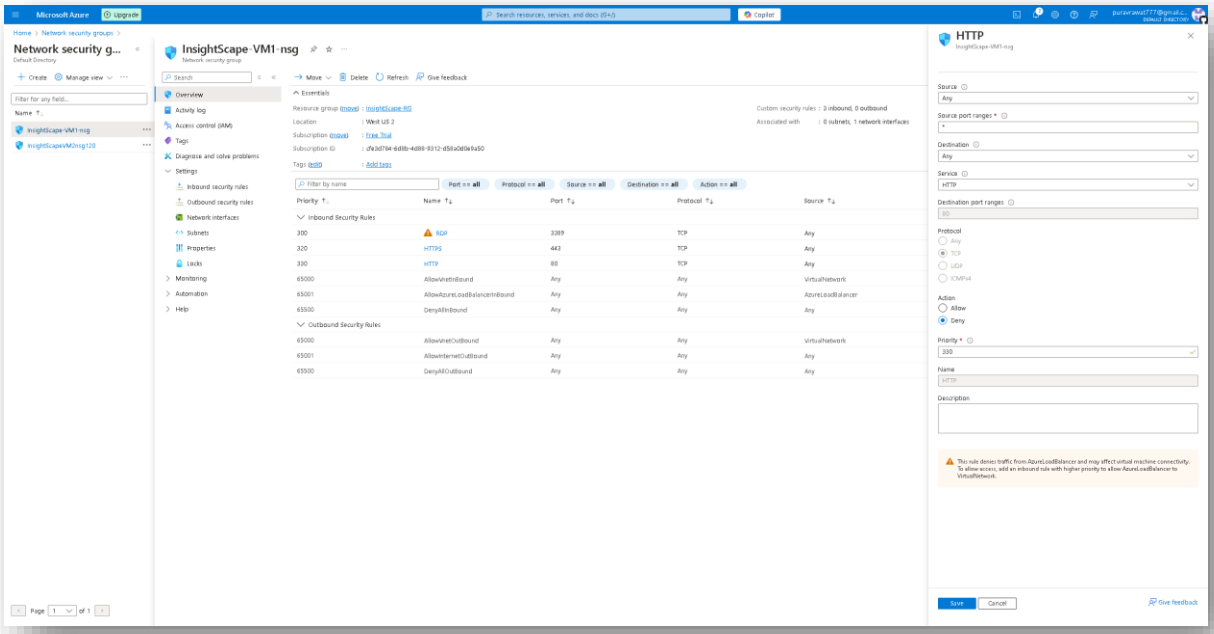

Microsoft Azure
Upgrade
Copilot
Home > Network Watcher
Network Watcher | Topology
Microsoft
Overview
Get started
Monitoring
Topology
Connection monitor
Traffic Analytics
Network diagnostic tools
IP flow verify
NSG diagnostics
Next hop
Effective security rules
VPN troubleshoot
Packet capture
Connection troubleshoot
Metrics
Logs
Flow logs
Migrate flow logs
Diagnostic logs
Reset topology
Feedback
Download topology
Geo Map
Azure Regions
Virtual Network
InsightScape-VNet
VIRTUAL NETWORK
VM1-Subnet
SUBNET
ipconfig1
InsightScape-VM1-nsg
insightscape-vm1714
InsightScape-VM1-ip
InsightScape-VM1

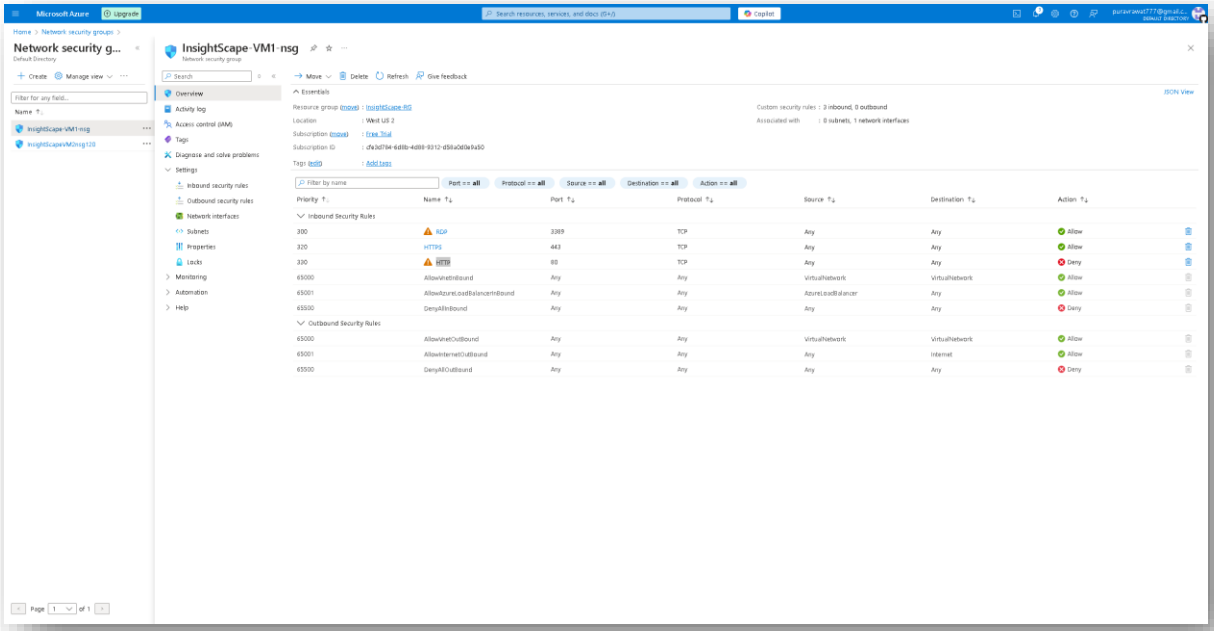

Microsoft Azure
Upgrade
Copilot
Home > Network Watcher
Network Watcher | Topology
Microsoft
Overview
Get started
Monitoring
Topology
Connection monitor
Traffic Analytics
Network diagnostic tools
IP flow verify
NSG diagnostics
Next hop
Effective security rules
VPN troubleshoot
Packet capture
Connection troubleshoot
Metrics
Logs
Flow logs
Migrate flow logs
Diagnostic logs
Reset topology
Feedback
Download topology
Geo Map
Azure Regions
Virtual Network
VM2-Subnet
SUBNET
ipconfig1
InsightScapeVM2nsg120
insightscape-vm2710
InsightScape-VM2-ip
InsightScape-VM2

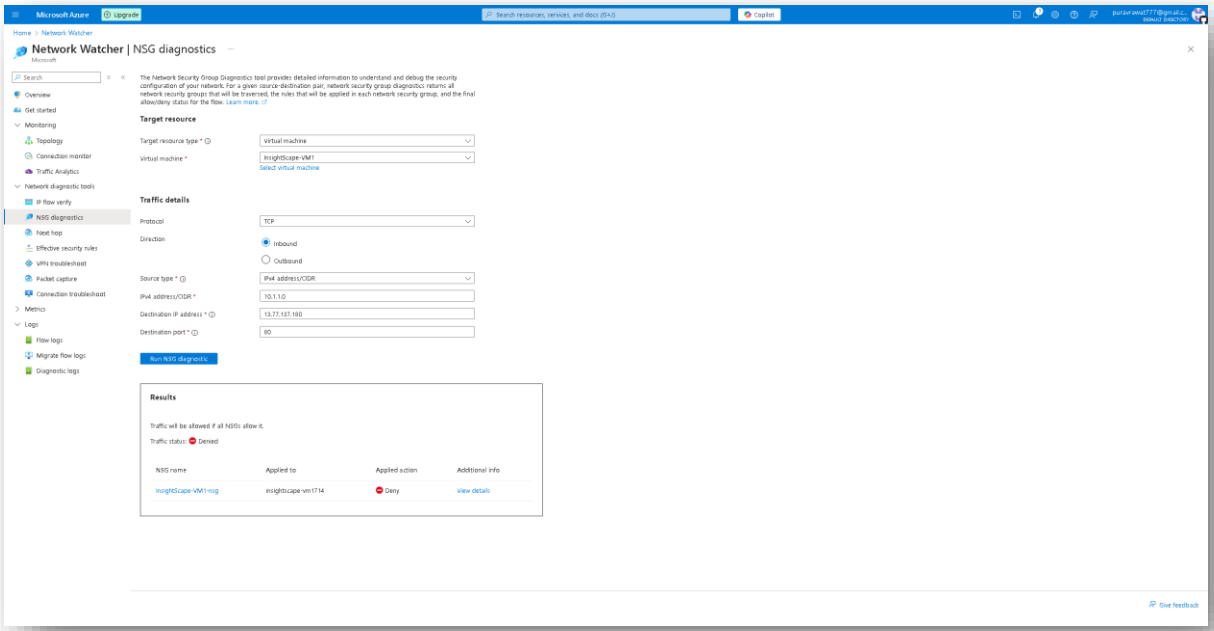

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Network security groups >
Network security g...
Default Directory
Create
Manage view
Filter for any field...
Name
InsightScape-VM1-nsg
InsightScapeVM2nsg120
InsightScape-VM1-nsg
Network security group
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Monitoring
Automation
Help
Move
Delete
Refresh
Give feedback
Essentials
JSON View
Resource group (move) : InsightScape-RG
Location : West US 2
Subscription (move) : Free Trial
Subscription ID : cfe3d794-6d8b-4d88-9312-d58a0d0e9a50
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
300 RDP 3389 TCP Any Any Allow
320 HTTPS 443 TCP Any Any Allow
330 HTTP 80 TCP Any 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
65000 AllowVnetOutBound Any Any VirtualNetwork VirtualNetwork Allow
65001 AllowInternetOutBound Any Any Any Internet Allow
65500 DenyAllOutBound Any Any Any Any Deny


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Network security groups >
Network security g...
Default Directory
Create
Manage view
Filter for any field...
Name
InsightScape-VM1-nsg
InsightScapeVM2nsg120
InsightScapeVM2nsg120
Network security group
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Monitoring
Automation
Help
Move
Delete
Refresh
Give feedback
Essentials
JSON View
Resource group (move) : InsightScape-RG
Location : West US 2
Subscription (move) : Free Trial
Subscription ID : cfe3d794-6d8b-4d88-9312-d58a0d0e9a50
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
300 SSH 22 TCP Any Any Allow
320 HTTPS 443 TCP Any Any Allow
340 HTTP 80 TCP Any 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
65000 AllowVnetOutBound Any Any VirtualNetwork VirtualNetwork Allow
65001 AllowInternetOutBound Any Any Any Internet Allow
65500 DenyAllOutBound Any Any Any Any Deny
Page 1 of 1


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Network Watcher
Network Watcher | NSG diagnostics
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
Metrics
Logs
Flow logs
Migrate flow logs
Diagnostic logs
The Network Security Group Diagnostics tool provides detailed information to understand and debug the security configuration of your network. For a given source-destination pair, network security group diagnostics returns all network security groups that will be traversed, the rules that will be applied in each network security group, and the final allow/deny status for the flow. Learn more.
Target resource
Target resource type *
Virtual machine
Virtual machine *
InsightScape-VM1
Select virtual machine
Traffic details
Protocol
TCP
Direction
Inbound
Outbound
Source type *
IPv4 address/CIDR
IPv4 address/CIDR *
192.168.0.1
Destination IP address *
13.77.137.160
Destination port *
80
Run NSG diagnostic
Results
Traffic will be allowed if all NSGs allow it.
Traffic status: Allowed
NSG name
Applied to
Applied action
Additional info
InsightScape-VM1-nsg
insightscape-vm1714
Allow
View details
Give feedback


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Network security groups >
Network security g...
Default Directory
Create
Manage view
Filter for any field...
Name
InsightScape-VM1-nsg
InsightScapeVM2nsg120
InsightScape-VM1-nsg
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
Automation
Help
Essentials
Resource group (move) : InsightScape-RG
Location : West US 2
Subscription (move) : Free Trial
Subscription ID : d7e3d784-6d8b-4d88-9312-d58a0d0a9a50
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
Inbound Security Rules
300 RDP 3389 TCP Any
320 HTTPS 443 TCP Any
330 HTTP 80 TCP Any
65000 AllowVnetInBound Any Any VirtualNetwork
65001 AllowAzureLoadBalancerInBound Any Any AzureLoadBalancer
65500 DenyAllInBound Any Any Any
Outbound Security Rules
65000 AllowVnetOutBound Any Any VirtualNetwork
65001 AllowInternetOutBound Any Any Any
65500 DenyAllOutBound Any Any Any
Page 1 of 1
HTTP
InsightScape-VM1-nsg
Source
Any
Source port ranges *
*
Destination
Any
Service
HTTP
Destination port ranges
80
Protocol
Any
TCP
UDP
ICMPv4
Action
Allow
Deny
Priority *
330
Name
HTTP
Description
This rule denies traffic from AzureLoadBalancer and may affect virtual machine connectivity. To allow access, add an inbound rule with higher priority to allow AzureLoadBalancer to VirtualNetwork.
Save
Cancel
Give feedback


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Network security groups >
Network security g...
Default Directory
Create
Manage view
Filter for any field...
Name
InsightScape-VM1-nsg
InsightScapeVM2nsg120
Page 1 of 1
InsightScape-VM1-nsg
Network security group
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Monitoring
Automation
Help
Move
Delete
Refresh
Give feedback
Essentials
JSON View
Resource group (move) : InsightScape-RG
Location : West US 2
Subscription (move) : Free Trial
Subscription ID : d1e3d784-6d8b-4d88-9312-d58a0d0a9a50
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
300 RDP 3389 TCP Any Any Allow
320 HTTPS 443 TCP Any Any Allow
330 HTTP 80 TCP Any Any Deny
65000 AllowVnetInBound Any Any VirtualNetwork VirtualNetwork Allow
65001 AllowAzureLoadBalancerInBound Any Any AzureLoadBalancer Any Allow
65500 DenyAllInBound Any Any Any Any Deny
Outbound Security Rules
65000 AllowVnetOutBound Any Any VirtualNetwork VirtualNetwork Allow
65001 AllowInternetOutBound Any Any Any Internet Allow
65500 DenyAllOutBound Any Any Any Any Deny


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Network Watcher
Network Watcher | NSG diagnostics
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
Metrics
Logs
Flow logs
Migrate flow logs
Diagnostic logs
The Network Security Group Diagnostics tool provides detailed information to understand and debug the security configuration of your network. For a given source-destination pair, network security group diagnostics returns all network security groups that will be traversed, the rules that will be applied in each network security group, and the final allow/deny status for the flow. Learn more.
Target resource
Target resource type * : Virtual machine
Virtual machine * : InsightScape-VM1
Select virtual machine
Traffic details
Protocol : TCP
Direction : Inbound / Outbound
Source type * : IPv4 address/CIDR
IPv4 address/CIDR * : 10.1.1.0
Destination IP address * : 13.77.137.160
Destination port * : 80
Run NSG diagnostic
Results
Traffic will be allowed if all NSGs allow it.
Traffic status: Denied
NSG name
Applied to
Applied action
Additional info
InsightScape-VM1-nsg
insightscape-vm1714
Deny
View details
Give feedback

Security & Compliance

In this phase of the project, my goal was to work with Azure Security Center and Microsoft Defender for Cloud to ensure that all resources were secure and compliant with best practices.

a) Accessing Security Center

First, I searched for Security in the Azure Portal's search box and accessed Security Center under the Protect section.

- I reviewed the Security Recommendations in Azure Security Center, categorized by severity, to identify and address potential vulnerabilities.
- These recommendations helped me enhance the security posture of my environment by prioritizing which vulnerabilities to address first based on their impact.

b) Microsoft Defender for Cloud Overview

- After reviewing the security recommendations, I proceeded to Microsoft Defender for Cloud: I clicked on Microsoft Defender for Cloud from the same page, which took me to the Overview page.
- Here, I evaluated the overall security posture of the Azure environment.
    - I analyzed critical factors such as vulnerabilities, assessed resources, and security recommendations across multiple cloud platforms.
    - This helped me ensure that all security measures were effectively implemented, minimizing risks.

c) Inventory Assessment

Next, I went to the Inventory section under General in Microsoft Defender for Cloud:

- I assessed the resource inventory, identifying unhealthy resources across different environments.
- I analyzed specific recommendations provided for each resource to mitigate vulnerabilities and ensure compliance with best practices.

d) Reviewing Security Recommendations

I accessed the Recommendations tab under General in Microsoft Defender for Cloud:

- I reviewed the risk-based security recommendations, categorized by severity. These recommendations helped me prioritize actions to strengthen the security posture of Azure resources.
- I focused on best practices for managing ports, securing virtual machines, and addressing potential vulnerabilities.

e) Implementing Security Recommendations

To work on some specific recommendations, I began with VM Updates and Patches:

1. VM Updates and Patches:
    - Since I had chosen not to enable updates on this virtual machine, there were no updates available, and therefore, I was unable to perform any updates.
2. Disk Encryption:
    - I moved on to another recommendation regarding Disk Encryption.
    - I accessed the Encryption tab under Settings for InsightScape-VM1 OsDisk _1_8355cb84eeb7418082014773dOe862c2.
    - For Key management, I selected "Platform-managed key" and saved the changes.
    - After a few seconds, the disk was updated successfully.
3. Storage Accounts Should Restrict Network Access:
    - I addressed the recommendation to restrict network access for storage accounts using virtual network rules.
    - I accessed the Networking tab under the Security + networking section in the insightscapeblob storage account.
    - In the Firewalls and virtual networks page:
        - Selected "Enabled from selected virtual networks and IP addresses".
        - In the Add networks settings:
            - Virtual Networks: InsightScape-VNet
            - Subnets: VM1-Subnet and VM2-Subnet (2 selected)
        - Enabled these settings and clicked on Save.

f) Secure Score Analysis

- I analyzed the secure score recommendations to identify key areas for improving the security posture of Azure resources.
    - This included enabling Multi-Factor Authentication (MFA), securing management ports, remediating vulnerabilities, and applying system updates.
    - These actions helped enhance the overall security and mitigate potential risks.

g) Security Alerts Verification

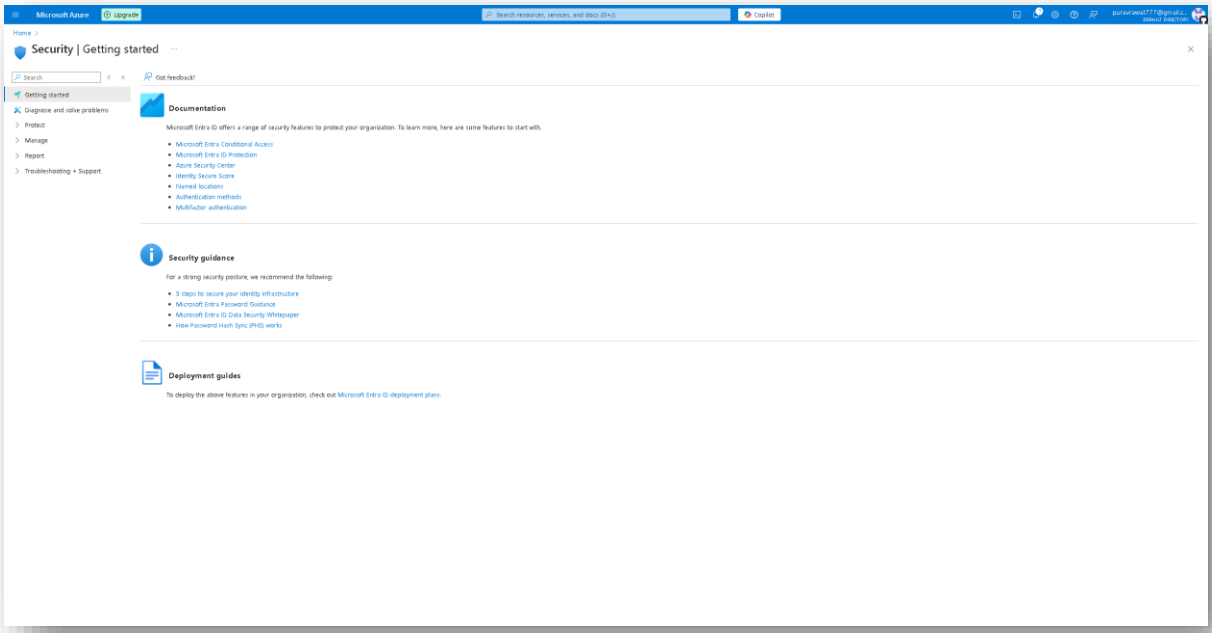
Lastly, I accessed the Security Alerts tab in Microsoft Defender for Cloud:

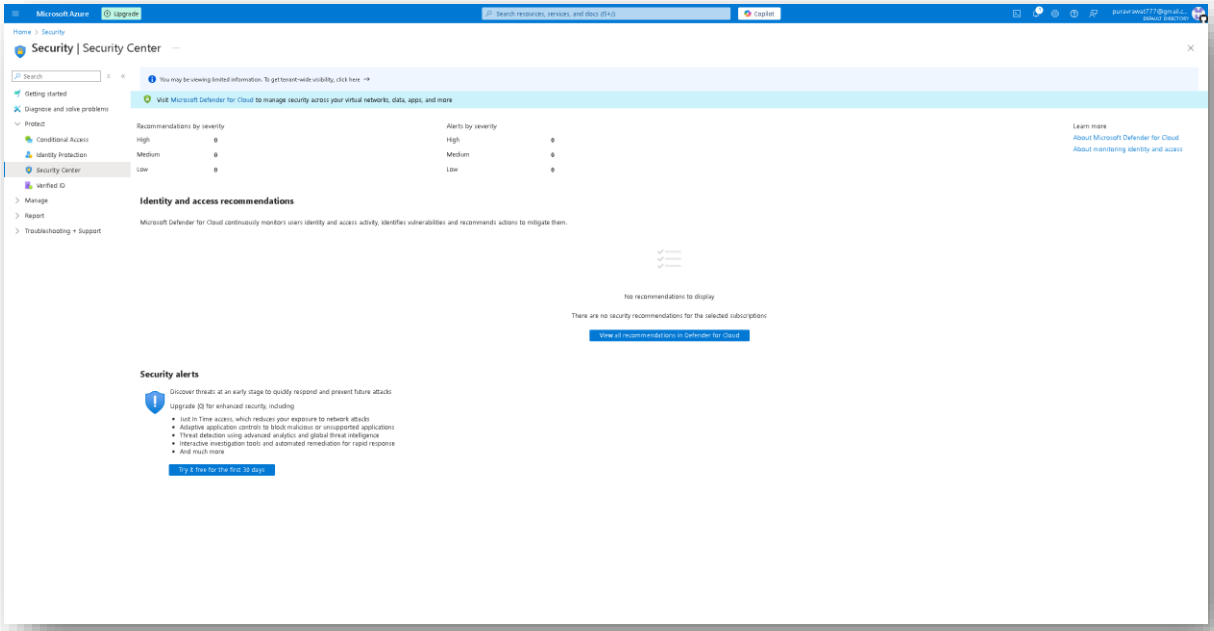
- At the time of observation, there were no alerts detected, indicating a secure state for the resources.

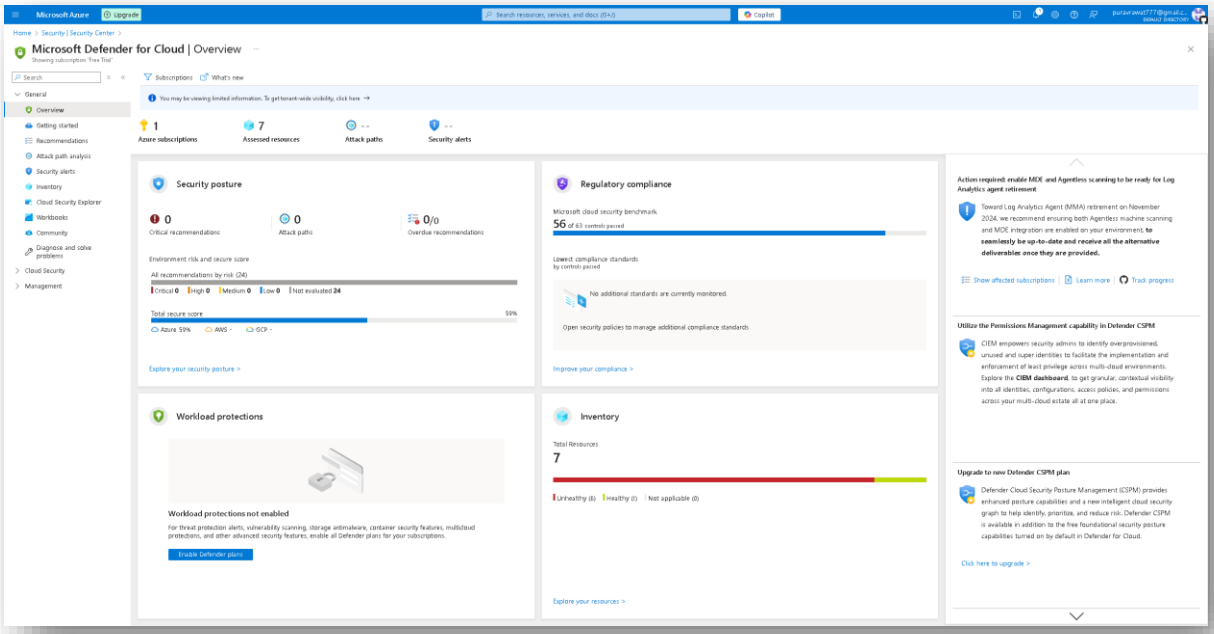
- I continued with the assessment, ensuring that the cloud environment remained secure and aligned with best practices.

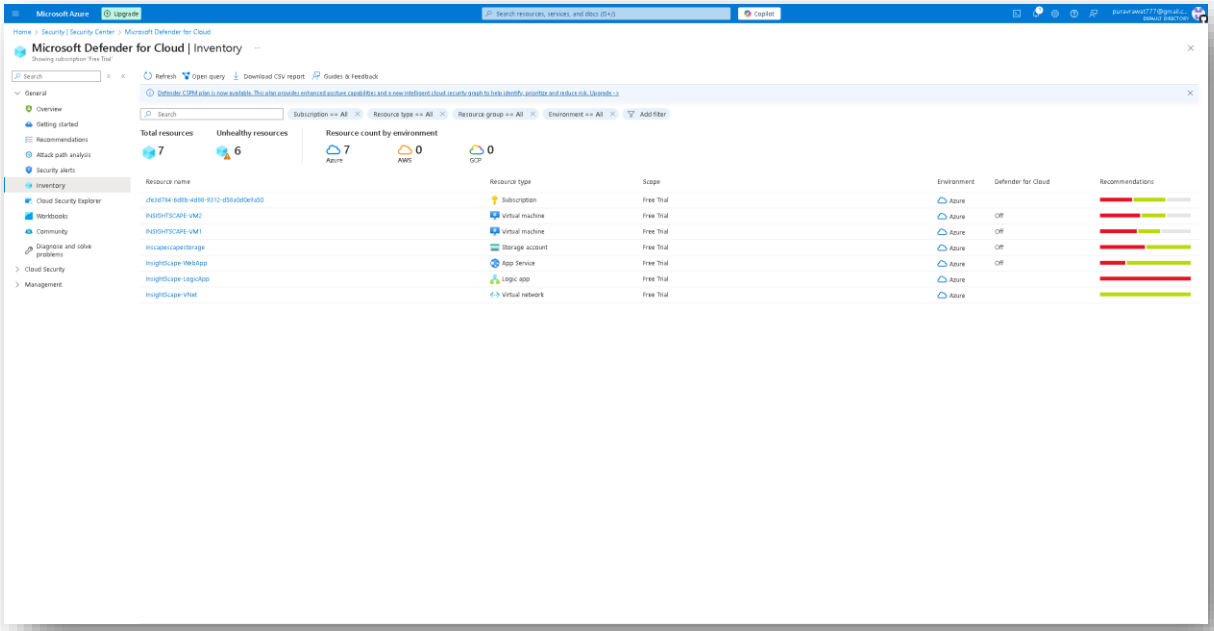
This concluded the Step 5: Security & Compliance phase of the project, which was successfully completed.

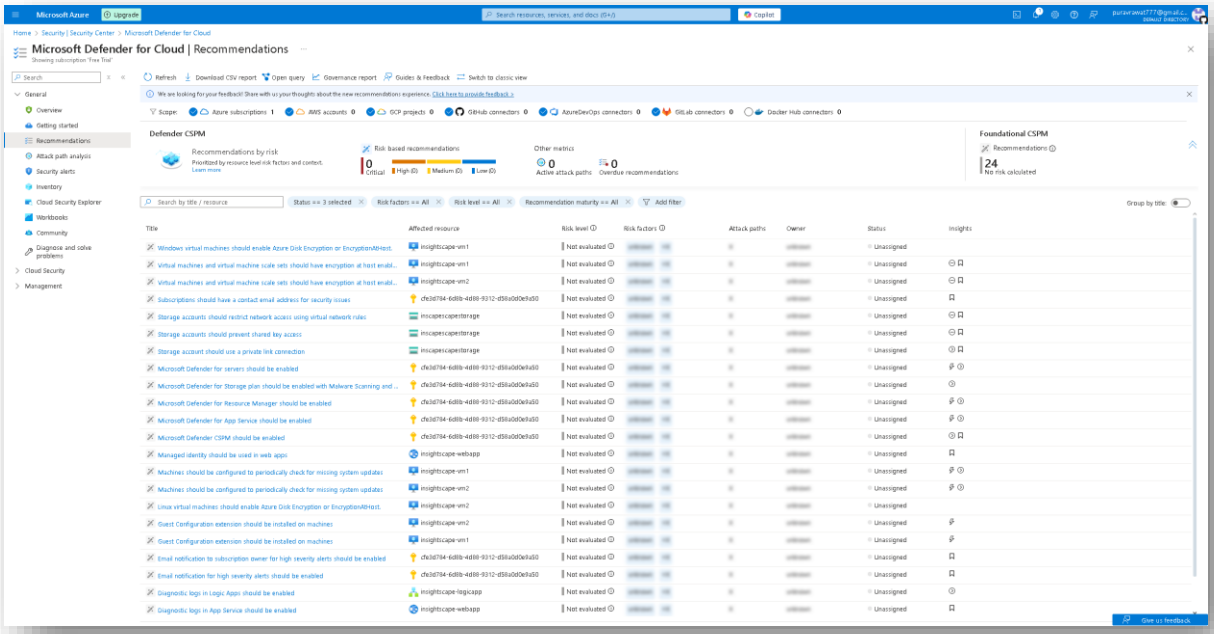
Screenshots-

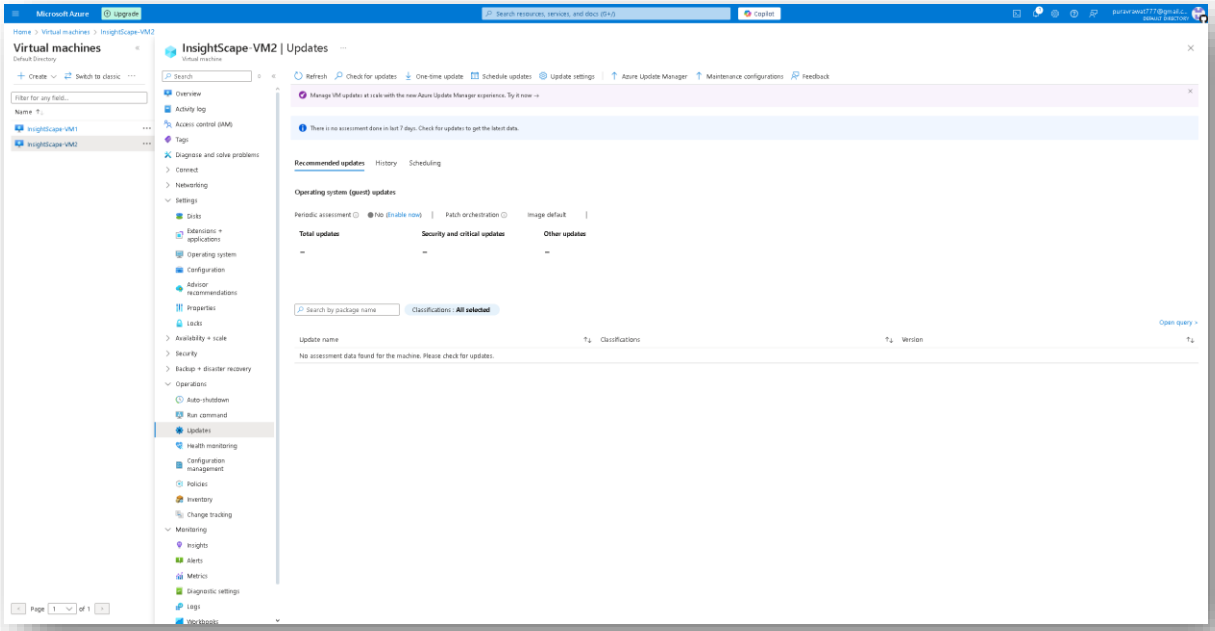


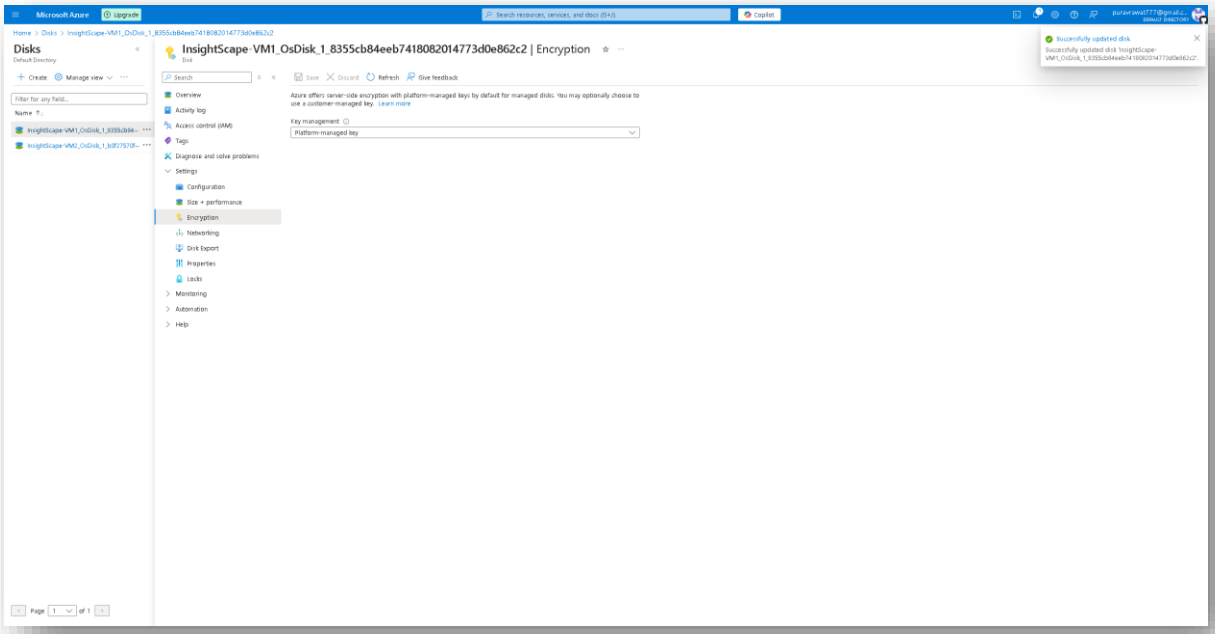

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Security
Security | Security Center
Search
Getting started
Diagnose and solve problems
Protect
Conditional Access
Identity Protection
Security Center
Verified ID
Manage
Report
Troubleshooting + Support
You may be viewing limited information. To get tenant-wide visibility, click here
Visit Microsoft Defender for Cloud to manage security across your virtual networks, data, apps, and more
Recommendations by severity
High 0
Medium 0
Low 0
Alerts by severity
High 0
Medium 0
Low 0
Learn more
About Microsoft Defender for Cloud
About monitoring identity and access
Identity and access recommendations
Microsoft Defender for Cloud continuously monitors users identity and access activity, identifies vulnerabilities and recommends actions to mitigate them.
No recommendations to display
There are no security recommendations for the selected subscriptions
View all recommendations in Defender for Cloud
Security alerts
Discover threats at an early stage to quickly respond and prevent future attacks
Upgrade (1) for enhanced security, including
Just In Time access, which reduces your exposure to network attacks
Adaptive application controls to block malicious or unsupported applications
Threat detection using advanced analytics and global threat intelligence
Interactive investigation tools and automated remediation for rapid response
And much more
Try it free for the first 30 days

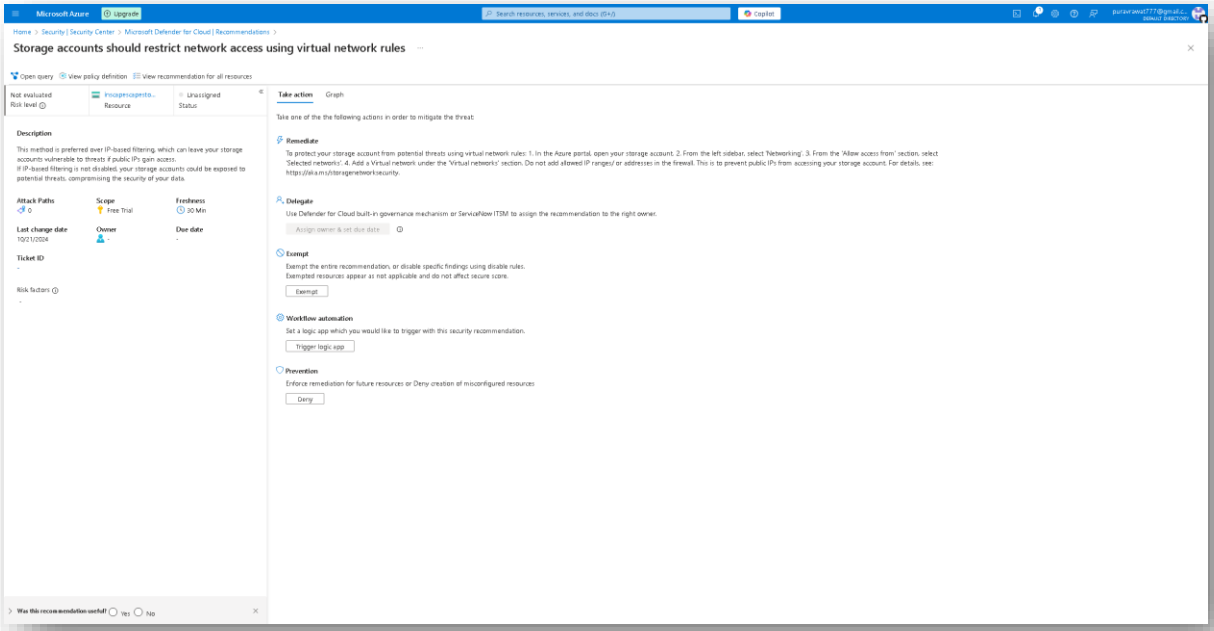

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Security | Security Center >
Microsoft Defender for Cloud | Overview
Showing subscription Free Trial
Search
General
Overview
Getting started
Recommendations
Attack path analysis
Security alerts
Inventory
Cloud Security Explorer
Workbooks
Community
Diagnose and solve problems
Cloud Security
Management
Subscriptions
What's new
You may be viewing limited information. To get tenant-wide visibility, click here
1 Azure subscriptions
7 Assessed resources
-- Attack paths
-- Security alerts
Security posture
0 Critical recommendations
0 Attack paths
0/0 Overdue recommendations
Environment risk and secure score
All recommendations by risk (24)
Critical 0 High 0 Medium 0 Low 0 Not evaluated 24
Total secure score 59%
Azure 59% AWS - GCP -
Explore your security posture >
Regulatory compliance
Microsoft cloud security benchmark
56 of 63 controls passed
Lowest compliance standards by controls passed
No additional standards are currently monitored.
Open security policies to manage additional compliance standards
Improve your compliance >
Workload protections
Workload protections not enabled
For threat protection alerts, vulnerability scanning, storage antimalware, container security features, multicloud protections, and other advanced security features, enable all Defender plans for your subscriptions.
Enable Defender plans
Inventory
Total Resources
7
Unhealthy (6) Healthy (1) Not applicable (0)
Explore your resources >
Action required: enable MDE and Agentless scanning to be ready for Log Analytics agent retirement
Toward Log Analytics Agent (MMA) retirement on November 2024, we recommend ensuring both Agentless machine scanning and MDE integration are enabled on your environment, to seamlessly be up-to-date and receive all the alternative deliverables once they are provided.
Show affected subscriptions | Learn more | Track progress
Utilize the Permissions Management capability in Defender CSPM
CIEM empowers security admins to identify overprovisioned, unused and super identities to facilitate the implementation and enforcement of least privilege across multi-cloud environments. Explore the CIEM dashboard, to get granular, contextual visibility into all identities, configurations, access policies, and permissions across your multi-cloud estate all at one place.
Upgrade to new Defender CSPM plan
Defender Cloud Security Posture Management (CSPM) provides enhanced posture capabilities and a new intelligent cloud security graph to help identify, prioritize, and reduce risk. Defender CSPM is available in addition to the free foundational security posture capabilities turned on by default in Defender for Cloud.
Click here to upgrade >

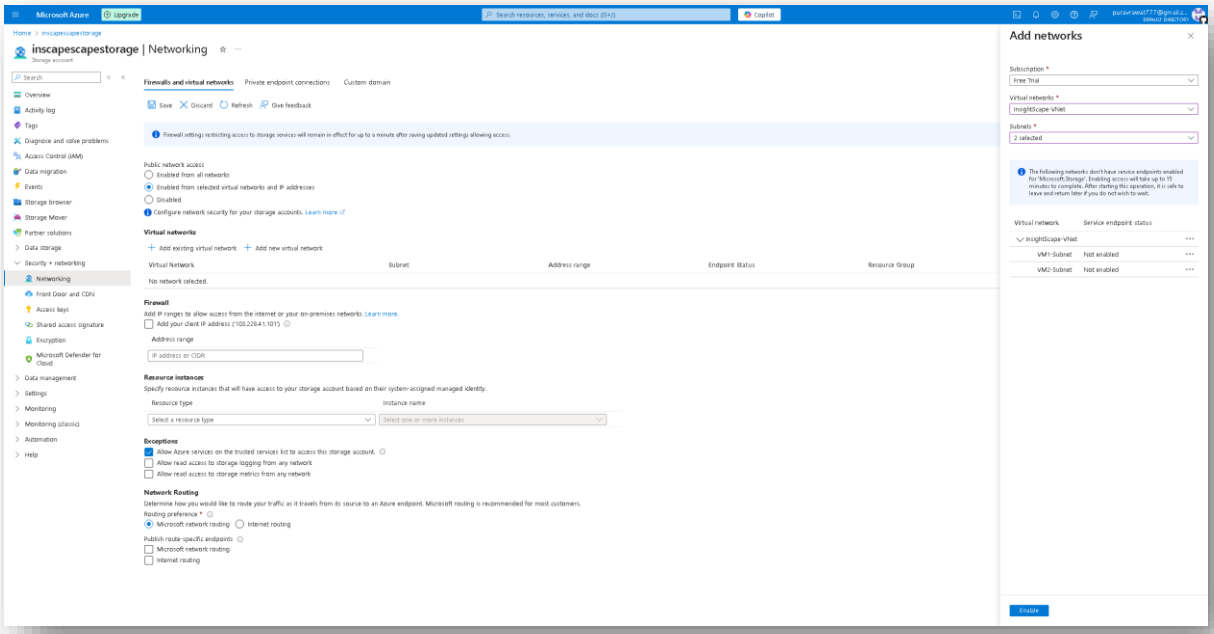

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Security | Security Center > Microsoft Defender for Cloud
Microsoft Defender for Cloud | Inventory
Showing subscription Free Trial
Search
General
Overview
Getting started
Recommendations
Attack path analysis
Security alerts
Inventory
Cloud Security Explorer
Workbooks
Community
Diagnose and solve problems
Cloud Security
Management
Refresh
Open query
Download CSV report
Guides & Feedback
Defender CSPM plan is now available. This plan provides enhanced posture capabilities and a new intelligent cloud security graph to help identify, prioritize and reduce risk. Upgrade >
Search
Subscription == All
Resource type == All
Resource group == All
Environment == All
Add filter
Total resources
7
Unhealthy resources
6
Resource count by environment
Azure 7
AWS 0
GCP 0
Resource name
Resource type
Scope
Environment
Defender for Cloud
Recommendations
cfe3d784-6d8b-4d88-9312-d58a0d0e9a50
Subscription
Free Trial
Azure
INSIGHTSCAPE-VM2
Virtual machine
Free Trial
Azure
Off
INSIGHTSCAPE-VM1
Virtual machine
Free Trial
Azure
Off
insightscapestorage
Storage account
Free Trial
Azure
Off
InsightScape-WebApp
App Service
Free Trial
Azure
Off
InsightScape-LogicApp
Logic app
Free Trial
Azure
InsightScape-vNet
Virtual network
Free Trial
Azure

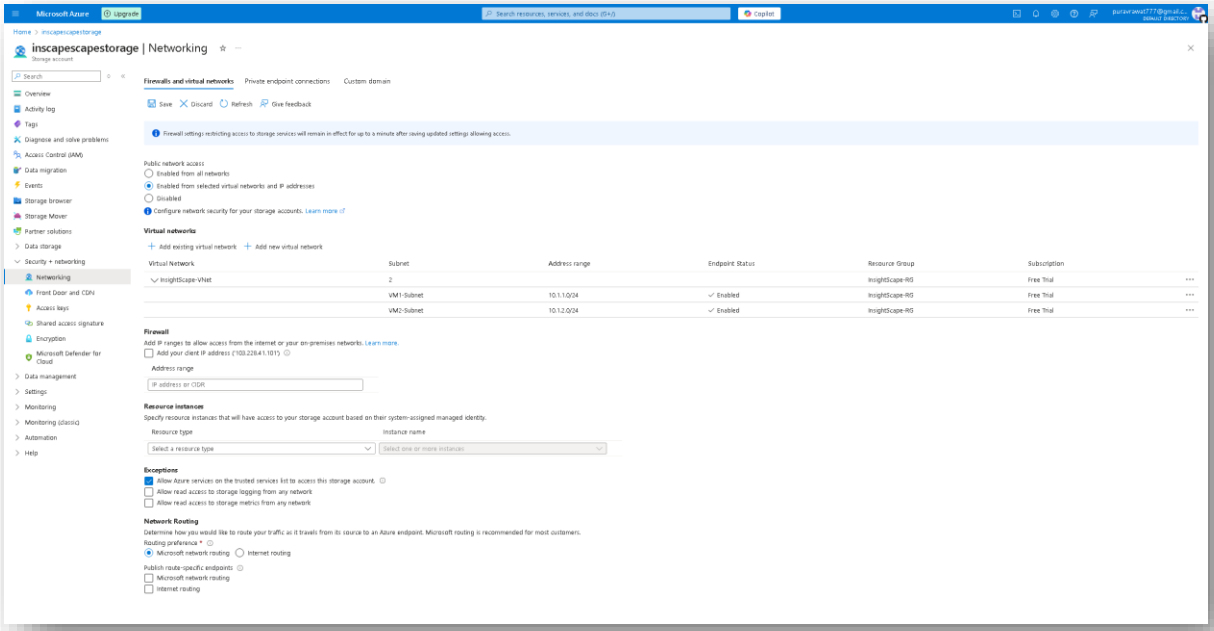

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Security | Security Center > Microsoft Defender for Cloud
Microsoft Defender for Cloud | Recommendations
Showing subscription Free Trial
Search
General
Overview
Getting started
Recommendations
Attack path analysis
Security alerts
Inventory
Cloud Security Explorer
Workbooks
Community
Diagnose and solve problems
Cloud Security
Management
Refresh
Download CSV report
Open query
Governance report
Guides & Feedback
Switch to classic view
We are looking for your feedback! Share with us your thoughts about the new recommendations experience. Click here to provide feedback >
Scope:
Azure subscriptions 1
AWS accounts 0
GCP projects 0
GitHub connectors 0
AzureDevOps connectors 0
GitLab connectors 0
Docker Hub connectors 0
Defender CSPM
Recommendations by risk
Prioritized by resource level risk factors and context.
Learn more
Risk based recommendations
0
Critical
High (0)
Medium (0)
Low (0)
Other metrics
0
Active attack paths
0
Overdue recommendations
Foundational CSPM
Recommendations
24
No risk calculated
Search by title / resource
Status == 3 selected
Risk factors == All
Risk level == All
Recommendation maturity == All
Add filter
Group by title
Title
Affected resource
Risk level
Risk factors
Attack paths
Owner
Status
Insights
Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.
insightscape-vm1
Not evaluated
Unassigned
Virtual machines and virtual machine scale sets should have encryption at host enabl...
insightscape-vm1
Not evaluated
Unassigned
Virtual machines and virtual machine scale sets should have encryption at host enabl...
insightscape-vm2
Not evaluated
Unassigned
Subscriptions should have a contact email address for security issues
cfe3d784-6d8b-4d88-9312-d58a0d0e9a50
Not evaluated
Unassigned
Storage accounts should restrict network access using virtual network rules
insightscapestorage
Not evaluated
Unassigned
Storage accounts should prevent shared key access
insightscapestorage
Not evaluated
Unassigned
Storage account should use a private link connection
insightscapestorage
Not evaluated
Unassigned
Microsoft Defender for servers should be enabled
cfe3d784-6d8b-4d88-9312-d58a0d0e9a50
Not evaluated
Unassigned
Microsoft Defender for Storage plan should be enabled with Malware Scanning and ...
cfe3d784-6d8b-4d88-9312-d58a0d0e9a50
Not evaluated
Unassigned
Microsoft Defender for Resource Manager should be enabled
cfe3d784-6d8b-4d88-9312-d58a0d0e9a50
Not evaluated
Unassigned
Microsoft Defender for App Service should be enabled
cfe3d784-6d8b-4d88-9312-d58a0d0e9a50
Not evaluated
Unassigned
Microsoft Defender CSPM should be enabled
cfe3d784-6d8b-4d88-9312-d58a0d0e9a50
Not evaluated
Unassigned
Managed identity should be used in web apps
insightscape-webapp
Not evaluated
Unassigned
Machines should be configured to periodically check for missing system updates
insightscape-vm1
Not evaluated
Unassigned
Machines should be configured to periodically check for missing system updates
insightscape-vm2
Not evaluated
Unassigned
Linux virtual machines should enable Azure Disk Encryption or EncryptionAtHost.
insightscape-vm2
Not evaluated
Unassigned
Guest Configuration extension should be installed on machines
insightscape-vm2
Not evaluated
Unassigned
Guest Configuration extension should be installed on machines
insightscape-vm1
Not evaluated
Unassigned
Email notification to subscription owner for high severity alerts should be enabled
cfe3d784-6d8b-4d88-9312-d58a0d0e9a50
Not evaluated
Unassigned
Email notification for high severity alerts should be enabled
cfe3d784-6d8b-4d88-9312-d58a0d0e9a50
Not evaluated
Unassigned
Diagnostic logs in Logic Apps should be enabled
insightscape-logicapp
Not evaluated
Unassigned
Diagnostic logs in App Service should be enabled
insightscape-webapp
Not evaluated
Unassigned
Give us feedback

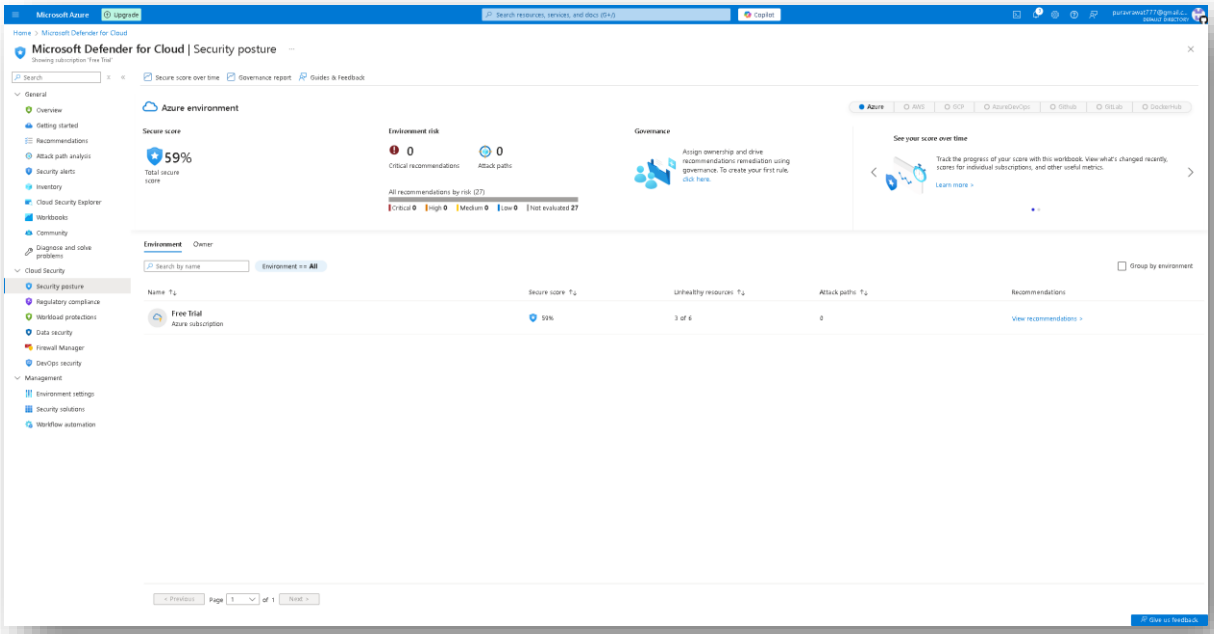

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Virtual machines > InsightScape-VM2
Virtual machines
Default Directory
Create
Switch to classic
Filter for any field...
Name
InsightScape-VM1
InsightScape-VM2
Page 1 of 1
InsightScape-VM2 | Updates
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Connect
Networking
Settings
Disks
Extensions + applications
Operating system
Configuration
Advisor recommendations
Properties
Locks
Availability + scale
Security
Backup + disaster recovery
Operations
Auto-shutdown
Run command
Updates
Health monitoring
Configuration management
Policies
Inventory
Change tracking
Monitoring
Insights
Alerts
Metrics
Diagnostic settings
Logs
Workbooks
Refresh
Check for updates
One-time update
Schedule updates
Update settings
Azure Update Manager
Maintenance configurations
Feedback
Manage VM updates at scale with the new Azure Update Manager experience. Try it now →
There is no assessment done in last 7 days. Check for updates to get the latest data.
Recommended updates
History
Scheduling
Operating system (guest) updates
Periodic assessment
No (Enable now)
Patch orchestration
Image default
Total updates
Security and critical updates
Other updates
Search by package name
Classifications : All selected
Open query >
Update name
Classifications
Version
No assessment data found for the machine. Please check for updates.

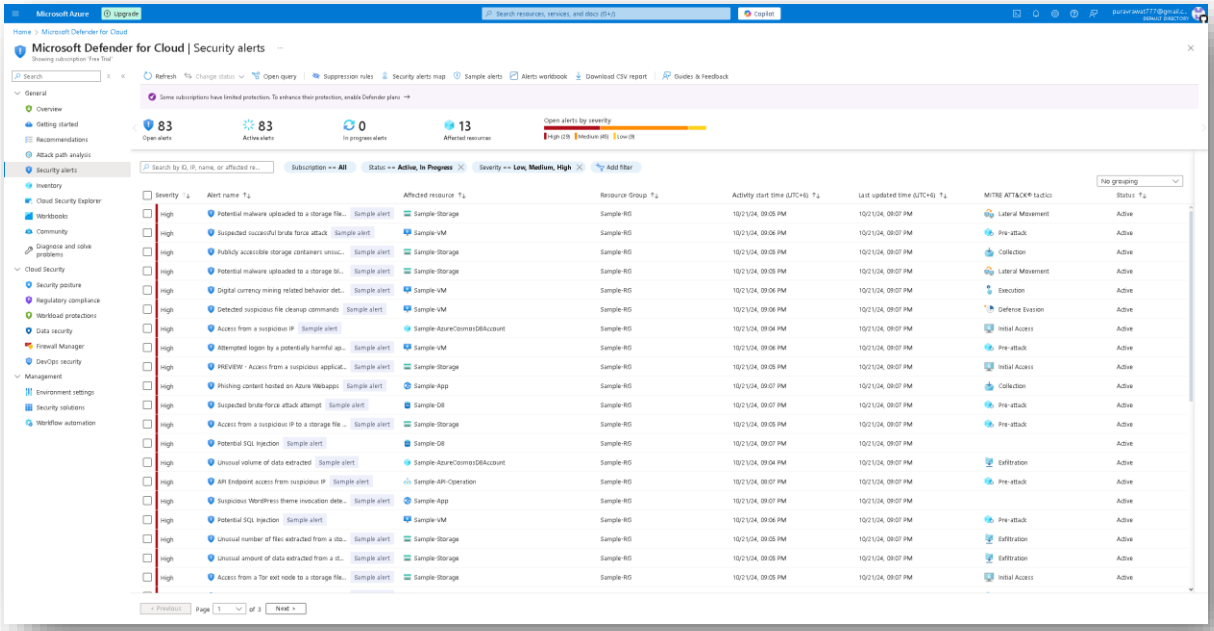

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Disks > InsightScape-VM1_OsDisk_1_8355cb84eeb7418082014773d0e862c2
Disks
Default Directory
Create
Manage view
Filter for any field...
Name
InsightScape-VM1_OsDisk_1_8355cb84...
InsightScape-VM2_OsDisk_1_b0f27570f...
Page 1 of 1
InsightScape-VM1_OsDisk_1_8355cb84eeb7418082014773d0e862c2 | Encryption
Disk
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Size + performance
Encryption
Networking
Disk Export
Properties
Locks
Monitoring
Automation
Help
Save
Discard
Refresh
Give feedback
Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. Learn more
Key management
Platform-managed key
Successfully updated disk
Successfully updated disk 'InsightScape-VM1_OsDisk_1_8355cb84eeb7418082014773d0e862c2'.


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Security | Security Center > Microsoft Defender for Cloud | Recommendations >
Storage accounts should restrict network access using virtual network rules
Open query
View policy definition
View recommendation for all resources
Not evaluated
Risk level
Unassigned
Status
Description
This method is preferred over IP-based filtering, which can leave your storage accounts vulnerable to threats if public IPs gain access.
If IP-based filtering is not disabled, your storage accounts could be exposed to potential threats, compromising the security of your data.
Attack Paths
Scope
Free Trial
Freshness
30 Min
Last change date
10/21/2024
Owner
Due date
Ticket ID
Risk factors
Was this recommendation useful?
Yes
No
Take action
Graph
Take one of the the following actions in order to mitigate the threat:
Remediate
To protect your storage account from potential threats using virtual network rules: 1. In the Azure portal, open your storage account. 2. From the left sidebar, select 'Networking'. 3. From the 'Allow access from' section, select 'Selected networks'. 4. Add a Virtual network under the 'Virtual networks' section. Do not add allowed IP ranges/ or addresses in the firewall. This is to prevent public IPs from accessing your storage account. For details, see: https://aka.ms/storagenetworksecurity.
Delegate
Use Defender for Cloud built-in governance mechanism or ServiceNow ITSM to assign the recommendation to the right owner.
Assign owner & set due date
Exempt
Exempt the entire recommendation, or disable specific findings using disable rules.
Exempted resources appear as not applicable and do not affect secure score.
Exempt
Workflow automation
Set a logic app which you would like to trigger with this security recommendation.
Trigger logic app
Prevention
Enforce remediation for future resources or Deny creation of misconfigured resources
Deny


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > inscapecapestorage
inscapecapestorage | Networking
Storage account
Search
Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage browser
Storage Mover
Partner solutions
Data storage
Security + networking
Networking
Front Door and CDN
Access keys
Shared access signature
Encryption
Microsoft Defender for Cloud
Data management
Settings
Monitoring
Monitoring (classic)
Automation
Help
Firewalls and virtual networks
Private endpoint connections
Custom domain
Save
Discard
Refresh
Give feedback
Firewall settings restricting access to storage services will remain in effect for up to a minute after saving updated settings allowing access.
Public network access
Enabled from all networks
Enabled from selected virtual networks and IP addresses
Disabled
Configure network security for your storage accounts. Learn more
Virtual networks
Add existing virtual network
Add new virtual network
Virtual Network
Subnet
Address range
Endpoint Status
Resource Group
No network selected.
Firewall
Add IP ranges to allow access from the internet or your on-premises networks. Learn more.
Add your client IP address ('103.226.41.101')
Address range
IP address or CIDR
Resource instances
Specify resource instances that will have access to your storage account based on their system-assigned managed identity.
Resource type
Instance name
Select a resource type
Select one or more instances
Exceptions
Allow Azure services on the trusted services list to access this storage account.
Allow read access to storage logging from any network
Allow read access to storage metrics from any network
Network Routing
Determine how you would like to route your traffic as it travels from its source to an Azure endpoint. Microsoft routing is recommended for most customers.
Routing preference
Microsoft network routing
Internet routing
Publish route-specific endpoints
Microsoft network routing
Internet routing
Add networks
Subscription
Free Trial
Virtual networks
InsightScape-VNet
Subnets
2 selected
The following networks don't have service endpoints enabled for 'Microsoft.Storage'. Enabling access will take up to 15 minutes to complete. After starting this operation, it is safe to leave and return later if you do not wish to wait.
Virtual network
Service endpoint status
InsightScape-VNet
VM1-Subnet
Not enabled
VM2-Subnet
Not enabled
Enable


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > inscapecapestorage
inscapecapestorage | Networking
Storage account
Search
Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage browser
Storage Mover
Partner solutions
Data storage
Security + networking
Networking
Front Door and CDN
Access keys
Shared access signature
Encryption
Microsoft Defender for Cloud
Data management
Settings
Monitoring
Monitoring (classic)
Automation
Help
Firewalls and virtual networks
Private endpoint connections
Custom domain
Save
Discard
Refresh
Give feedback
Firewall settings restricting access to storage services will remain in effect for up to a minute after saving updated settings allowing access.
Public network access
Enabled from all networks
Enabled from selected virtual networks and IP addresses
Disabled
Configure network security for your storage accounts. Learn more
Virtual networks
Add existing virtual network
Add new virtual network
Virtual Network
Subnet
Address range
Endpoint Status
Resource Group
Subscription
InsightScape-VNet
2
InsightScape-RG
Free Trial
VM1-Subnet
10.1.1.0/24
Enabled
VM2-Subnet
10.1.2.0/24
Firewall
Add IP ranges to allow access from the internet or your on-premises networks. Learn more.
Add your client IP address ('103.226.41.101')
Address range
IP address or CIDR
Resource instances
Specify resource instances that will have access to your storage account based on their system-assigned managed identity.
Resource type
Instance name
Select a resource type
Select one or more instances
Exceptions
Allow Azure services on the trusted services list to access this storage account.
Allow read access to storage logging from any network
Allow read access to storage metrics from any network
Network Routing
Determine how you would like to route your traffic as it travels from its source to an Azure endpoint. Microsoft routing is recommended for most customers.
Routing preference *
Microsoft network routing
Internet routing
Publish route-specific endpoints
Microsoft network routing
Internet routing


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Defender for Cloud
Microsoft Defender for Cloud | Security posture
Showing subscription 'Free Trial'
Search
General
Overview
Getting started
Recommendations
Attack path analysis
Security alerts
Inventory
Cloud Security Explorer
Workbooks
Community
Diagnose and solve problems
Cloud Security
Security posture
Regulatory compliance
Workload protections
Data security
Firewall Manager
DevOps security
Management
Environment settings
Security solutions
Workflow automation
Secure score over time
Governance report
Guides & Feedback
Azure environment
Azure
AWS
GCP
AzureDevOps
Github
GitLab
DockerHub
Secure score
59%
Total secure score
Environment risk
0
Critical recommendations
0
Attack paths
All recommendations by risk (27)
Critical 0
High 0
Medium 0
Low 0
Not evaluated 27
Governance
Assign ownership and drive recommendations remediation using governance. To create your first rule, click here.
See your score over time
Track the progress of your score with this workbook. View what's changed recently, scores for individual subscriptions, and other useful metrics.
Learn more >
Environment
Owner
Search by name
Environment == All
Group by environment
Name
Secure score
Unhealthy resources
Attack paths
Recommendations
Free Trial
Azure subscription
59%
3 of 6
0
View recommendations >
< Previous
Page 1 of 1
Next >
Give us feedback



This is a Sample Alert.

Alerts Configuration

In this phase of the project, my goal was to work with Azure Monitor Alerts to set up custom alerts for the resources I had deployed.

a) Creating Custom Alerts

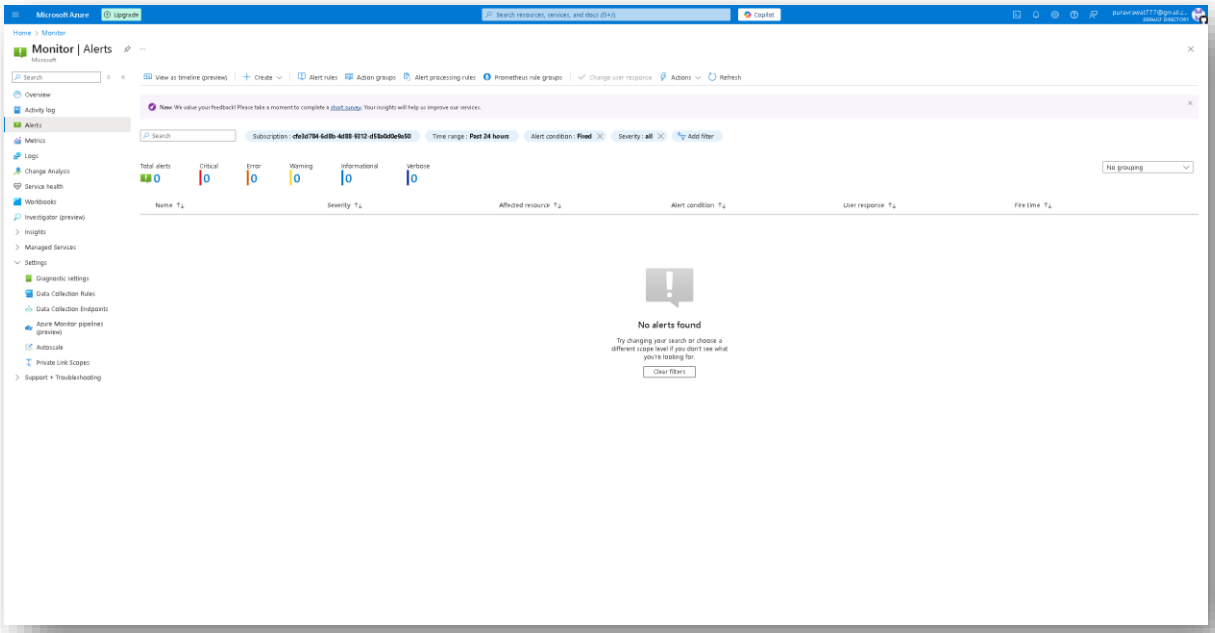
To begin with, I went to the Alerts tab in Azure Monitor and clicked on "+ Create Alert Rule".

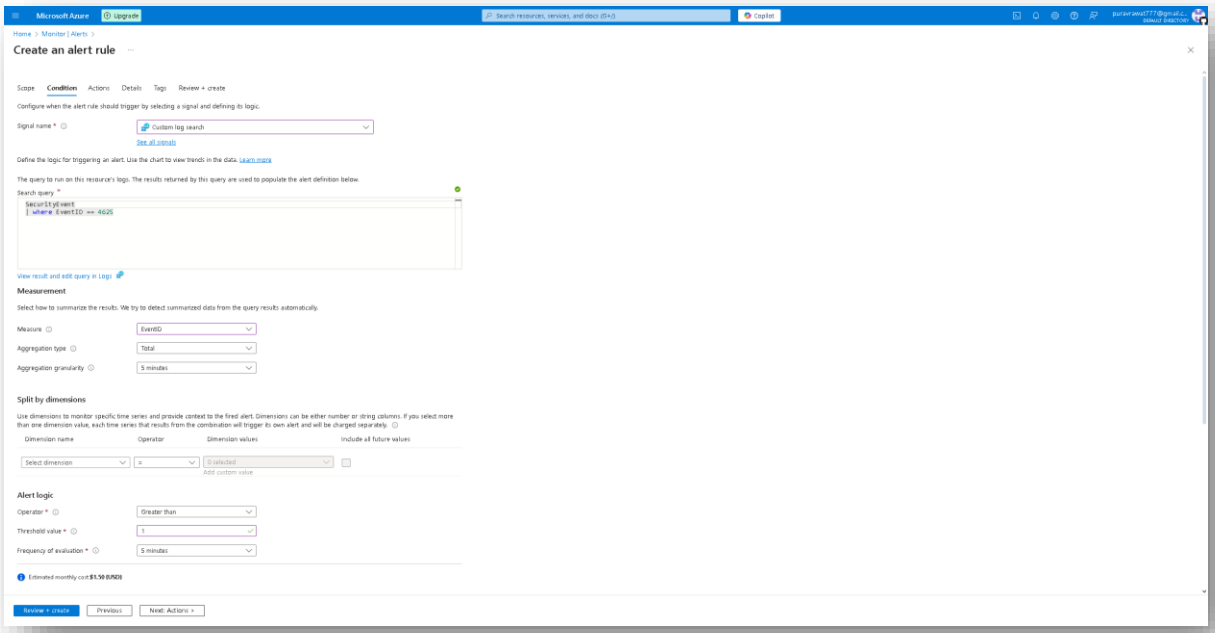
Alert Rule for InsightScape-VM1

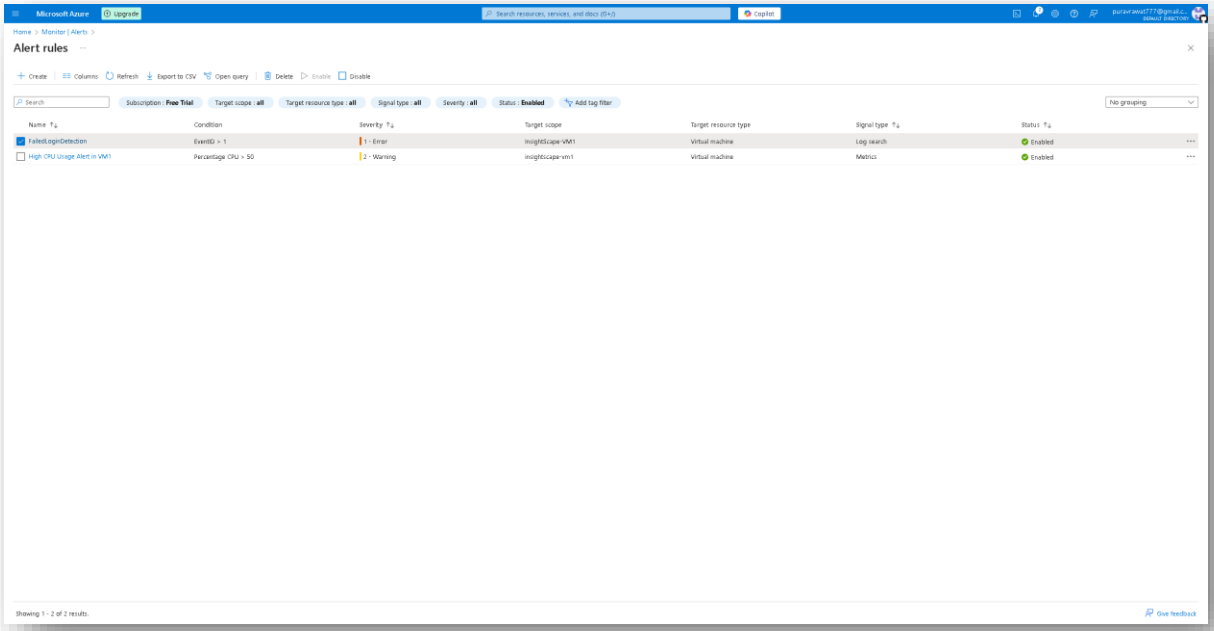
- Scope: Selected InsightScape-VM1.
- Condition:
  - Signal Name: Custom log search.
  - KQL Query: SecurityEvent | where EventID == 4625
  - Measure: EventID
  - Aggregation Type: Total
  - Aggregation Granularity: 5 minutes
  - Alert Logic:
    - Operator: Greater than
    - Threshold Value: 1
    - Frequency of Evaluation: 5 minutes
- Actions:
  - Action Group Name: FailedLoginAlertGroup
  - Display Name: RDPLoginFail
  - Email: Entered my email address and saved.
- Details:
  - Resource Group: InsightScape-RG
  - Severity: 1 - Error
  - Alert Rule Name: FailedLoginDetection
  - Alert Rule Description: This alert monitors failed RDP login attempts on InsightScape-VM1 and triggers when EventID 4625 is logged.
  - Region:West US 2

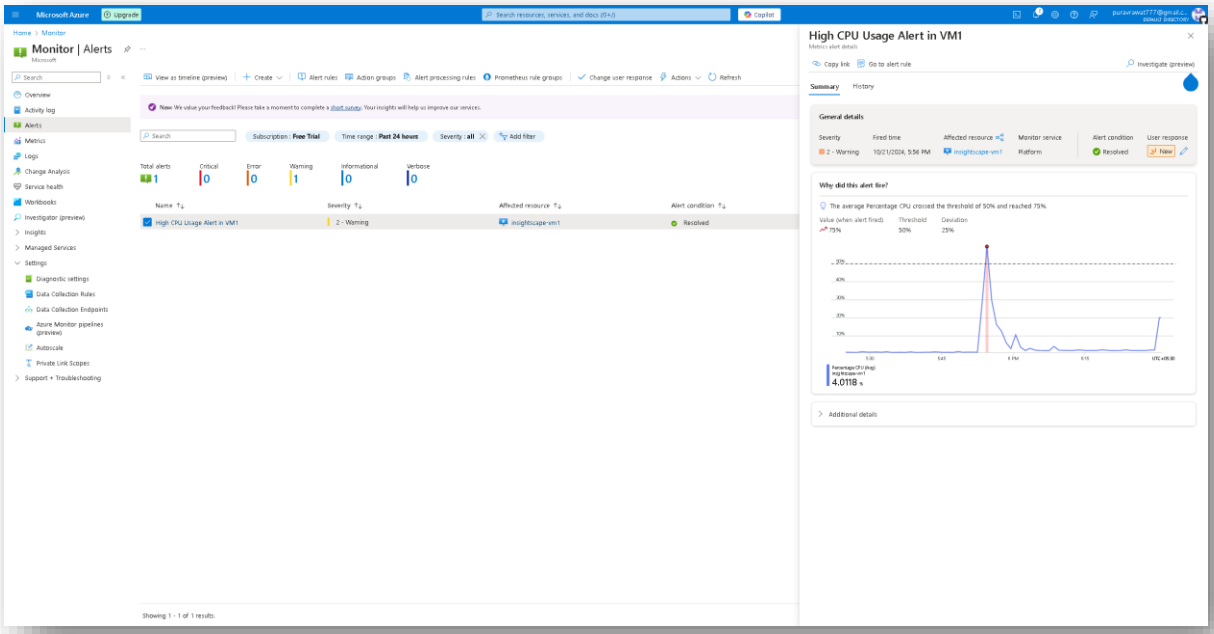
After configuring these settings, I clicked on "Review + Create", and the alert rule got successfully created.

Screenshots-






Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor | Alerts >
Alert rules
Create
Columns
Refresh
Export to CSV
Open query
Delete
Enable
Disable
Search
Subscription : Free Trial
Target scope : all
Target resource type : all
Signal type : all
Severity : all
Status : Enabled
Add tag filter
No grouping
Name
Condition
Severity
Target scope
Target resource type
Signal type
Status
FailedLoginDetection
EventID > 1
1 - Error
InsightScape-VM1
Virtual machine
Log search
Enabled
High CPU Usage Alert in VM1
Percentage CPU > 50
2 - Warning
insightscape-vm1
Virtual machine
Metrics
Enabled
Showing 1 - 2 of 2 results.
Give feedback


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Monitor
Monitor | Alerts
Microsoft
Search
Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Investigator (preview)
Insights
Managed Services
Settings
Diagnostic settings
Data Collection Rules
Data Collection Endpoints
Azure Monitor pipelines (preview)
Autoscale
Private Link Scopes
Support + Troubleshooting
View as timeline (preview)
Create
Alert rules
Action groups
Alert processing rules
Prometheus rule groups
Change user response
Actions
Refresh
New We value your feedback! Please take a moment to complete a short survey. Your insights will help us improve our services.
Search
Subscription : Free Trial
Time range : Past 24 hours
Severity : all
Add filter
Total alerts
Critical
Error
Warning
Informational
Verbose
1
0
0
1
0
0
Name
Severity
Affected resource
Alert condition
High CPU Usage Alert in VM1
2 - Warning
insightscape-vm1
Resolved
Showing 1 - 1 of 1 results.
High CPU Usage Alert in VM1
Metrics alert details
Copy link
Go to alert rule
Investigate (preview)
Summary
History
General details
Severity
Fired time
Affected resource
Monitor service
Alert condition
User response
2 - Warning
10/21/2024, 5:56 PM
insightscape-vm1
Platform
Resolved
New
Why did this alert fire?
The average Percentage CPU crossed the threshold of 50% and reached 75%.
Value (when alert fired)
Threshold
Deviation
75%
50%
25%
4.0118 %
Additional details

Backup and Disaster Recovery

In this phase of the project, my goal was to work on Backup and Disaster Recovery.

a) Confirming Backup Configuration

To begin, I accessed the Backup Items tab in the InsightScape-Vault (Recovery Services Vault) to ensure that InsightScape-VM1 was present in the backup items, as I had configured its backup in the initial phases of the project.

b) Deleting InsightScape-VM1 for Disaster Recovery Validation

Next, to work on Disaster Recovery, I went to InsightScape-VM1 and noted down the details of the VM such as:

- Size: Standard B1s
- Region: West US 2
- Virtual Network/Subnet: InsightScape-VNet/VM1-Subnet

With these details recorded, I deleted InsightScape-VM1 (but retained the associated resources like Disk, NIC, and Public IP).

c) Restoring the Virtual Machine

After the successful deletion of InsightScape-VM1, it was time to restore the VM to validate the disaster recovery capability within this project.

I went to the Backup Items tab in InsightScape-Vault (Recovery Services Vault). I clicked on the three dots beside the listed InsightScape-VM1 and selected "Restore VM". I chose the latest restore point with the following details:

- Time: 10/21/2024 , 4:45:08 am
- Consistency: Application Consistent
- Recovery Type: Snapshot and Vault Standard

For the Restore Configuration, I chose:

- Restore Type: Create new virtual machine
- Virtual Machine Name: InsightScape-VM1-Restored
- Resource Group: InsightScape-RG
- Virtual Network: InsightScape-VNet (InsightScape-RG)
- Subnet: VM1-Subnet
- Staging Location: insightscapestorage (StandardLRS) I then clicked on "Restore".

d) Verification of Successful Restore

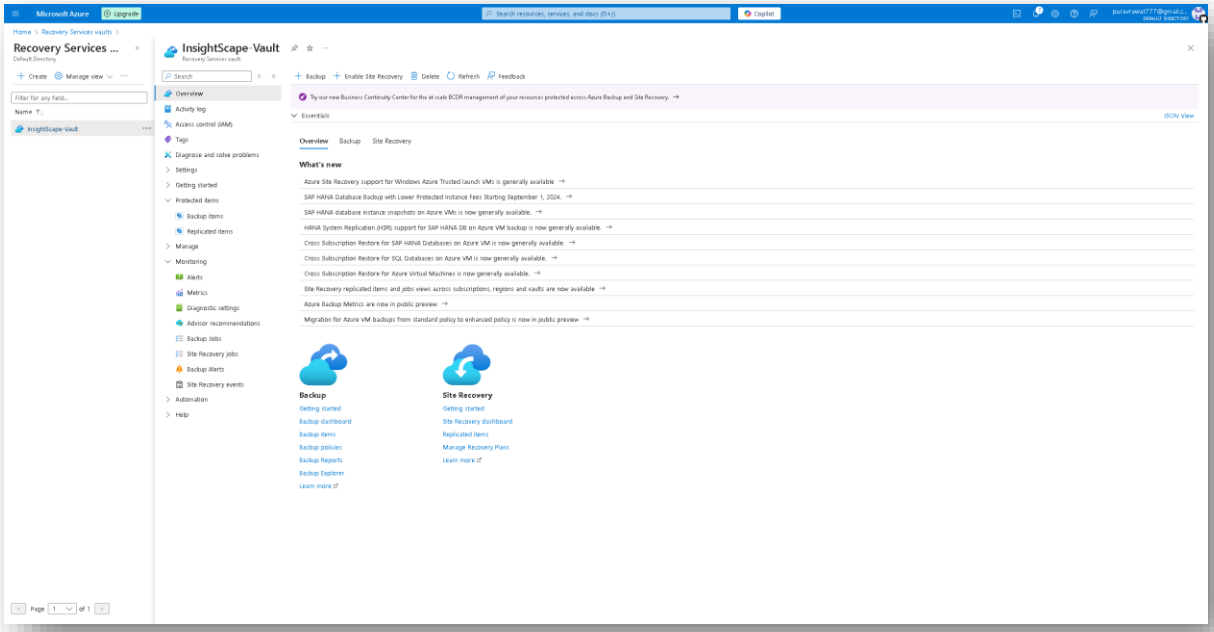
After the successful restore trigger for InsightScape-VM1, I confirmed the restoration using two methods:

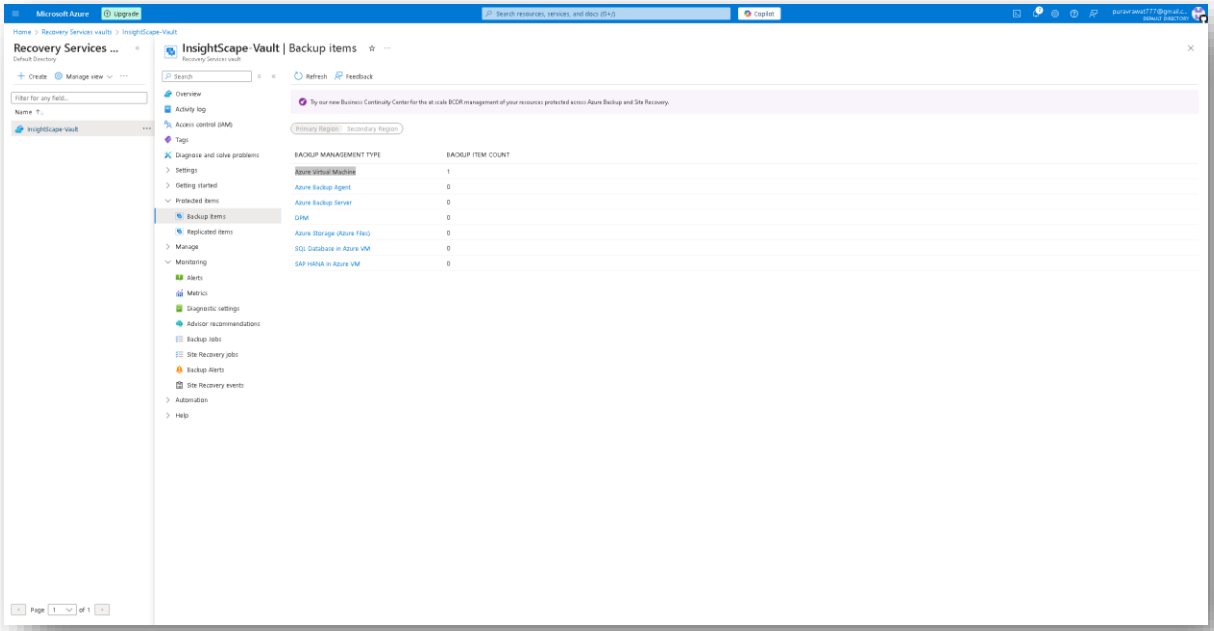
1. Backup Jobs Tab Verification:
    - I accessed the Backup Jobs tab in InsightScape-Vault, where I found the following workload listed:
        - Workload Name: InsightScape-VM1
        - Operation: Restore
        - Status: Completed
        - Type: Azure Virtual Machine
        - Total Duration: 00:02:11
2. Verification of Restored VM Details:
    - I navigated to InsightScape-VM1-Restored and compared its details with those of the original InsightScape-VM1 to ensure they matched. The verified details included:
        - Size: Standard B1s
        - Region: West US 2
        - Virtual Network/Subnet: InsightScape-VNet/VM1-Subnet
    - The details were identical, confirming that the VM was successfully restored.

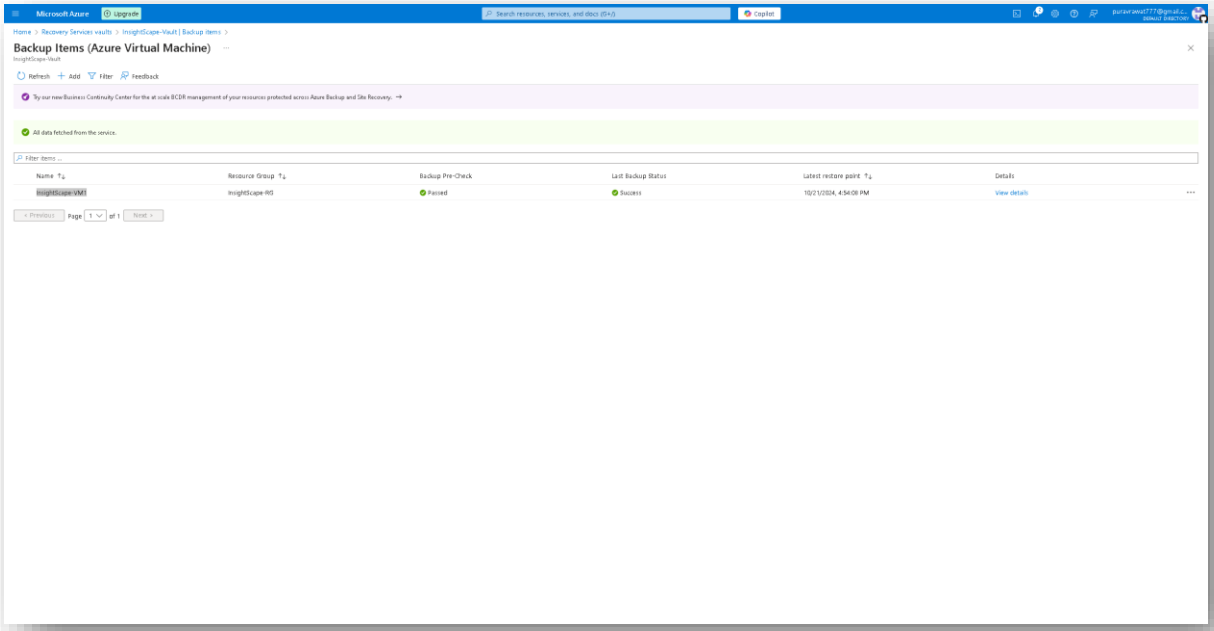
With the successful completion of the Backup and Disaster Recovery phase, I verified that the backup setup and recovery process worked as intended, providing resilience against data loss or failures.

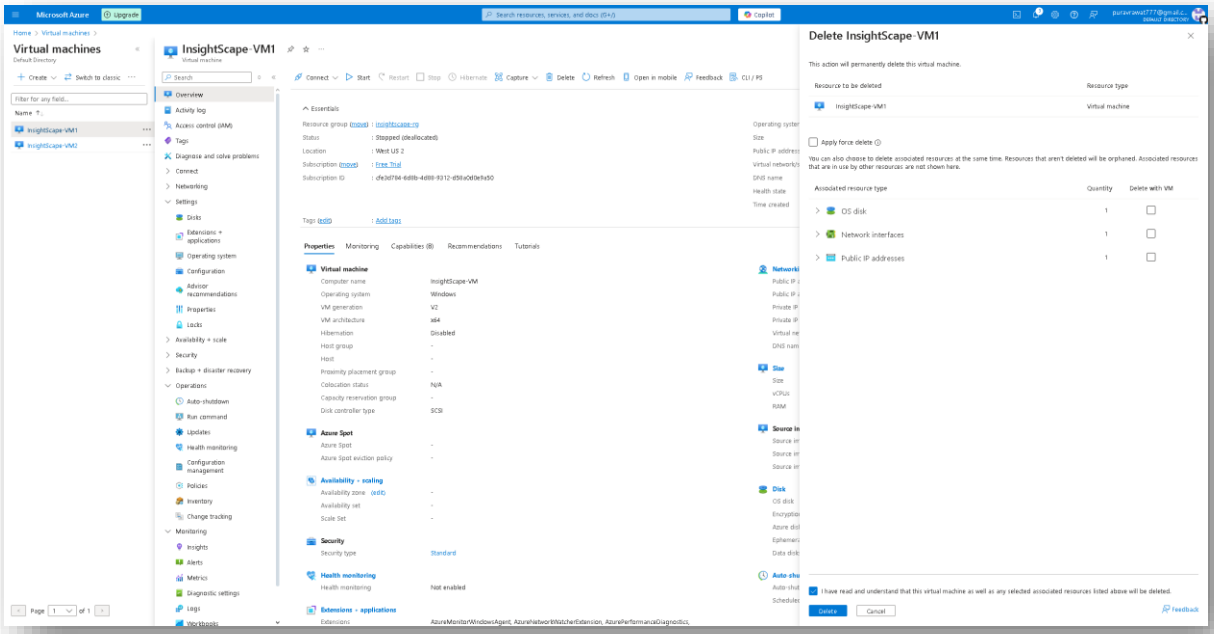
And with this, the entire project was successfully completed!

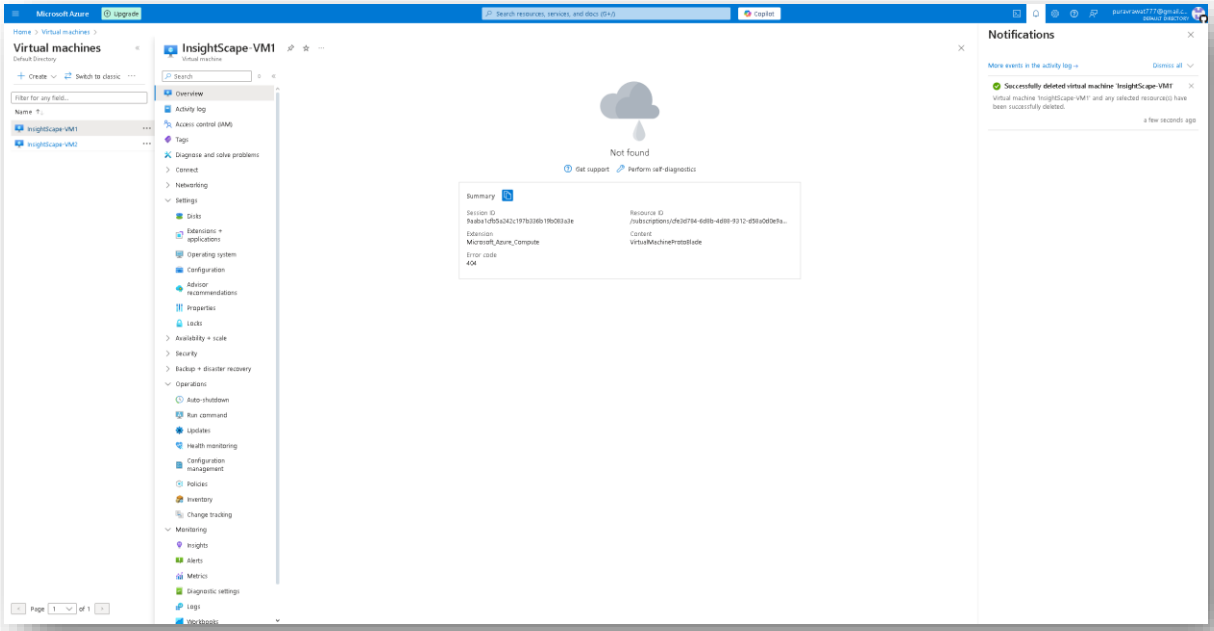
Screenshots-

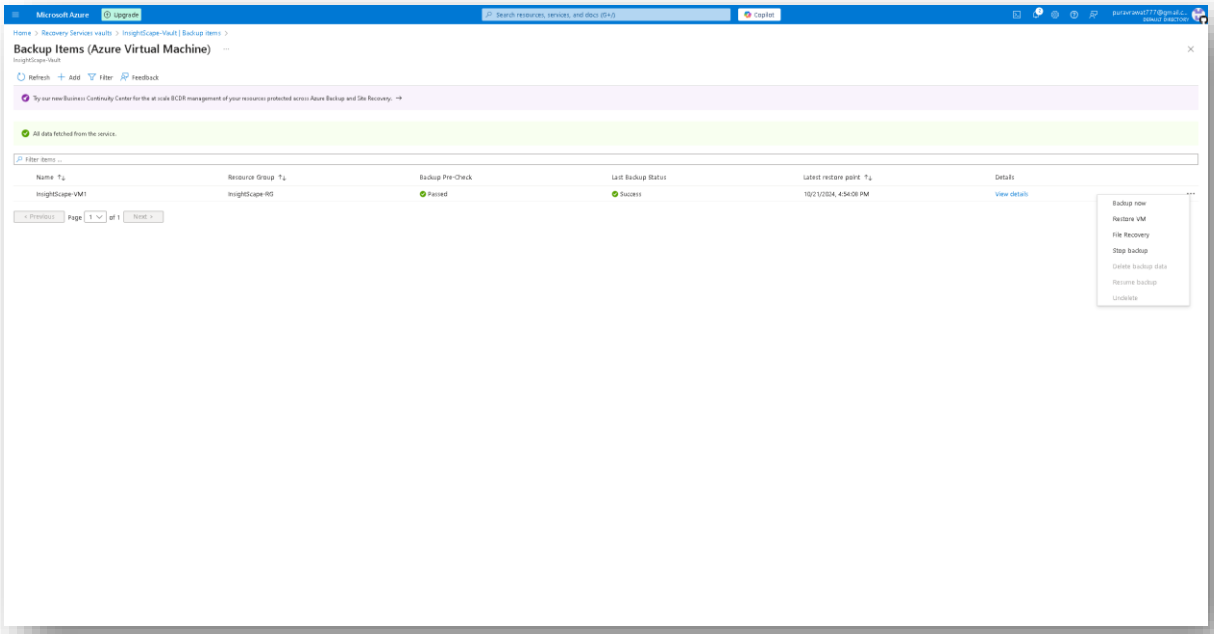


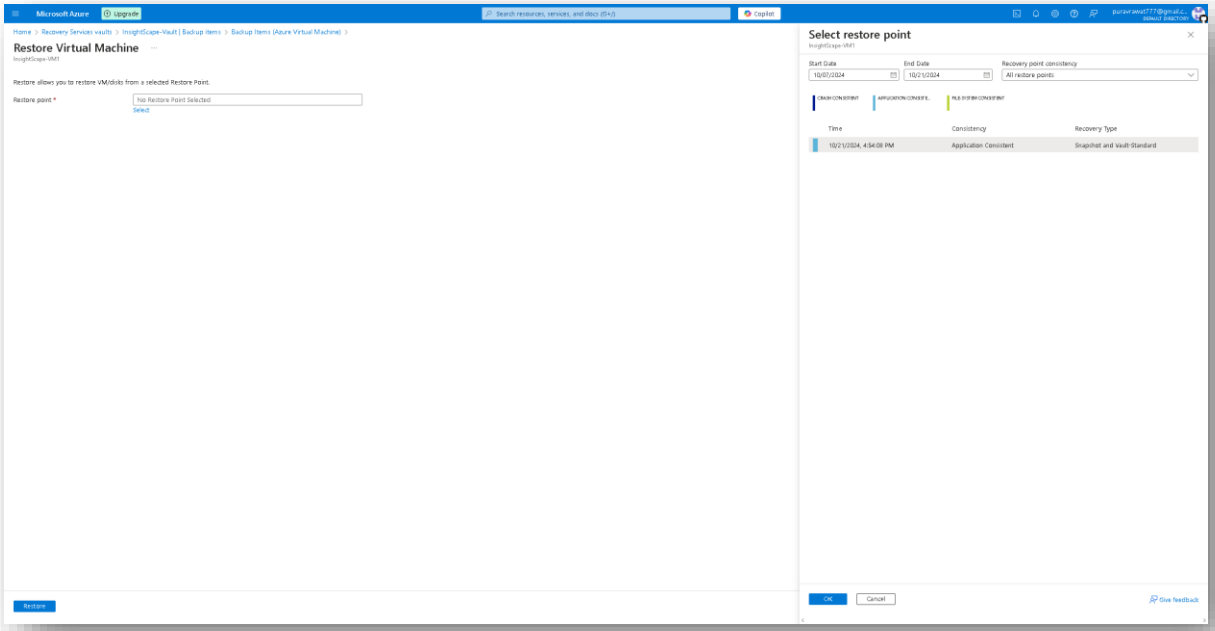


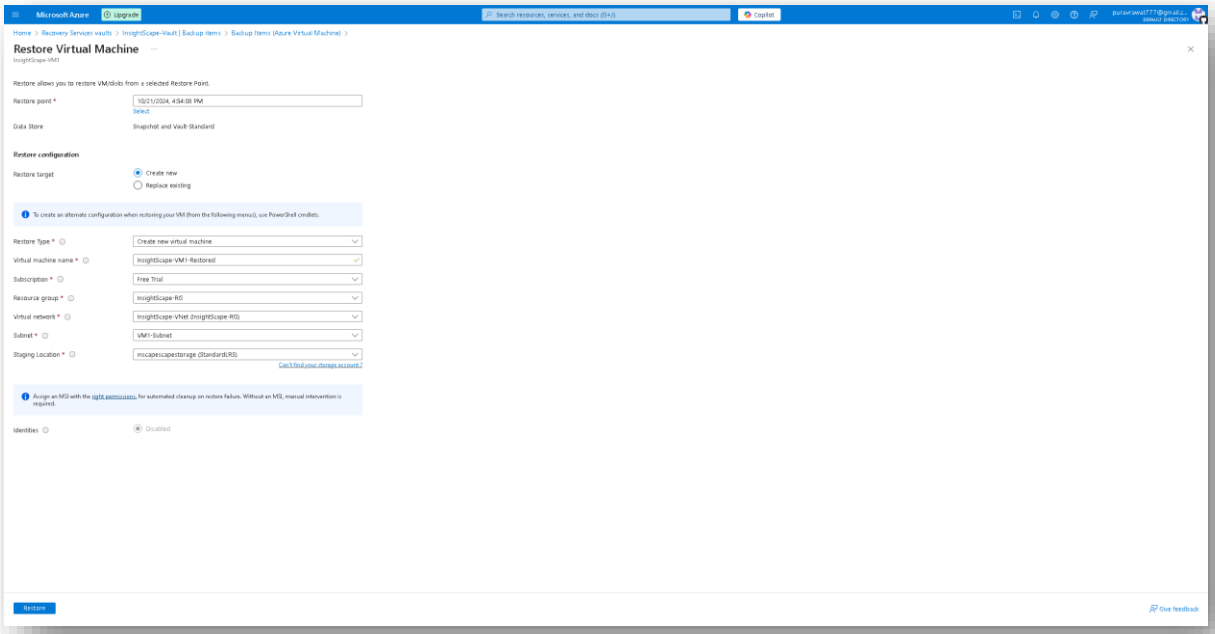

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Recovery Services vaults > InsightScape-Vault | Backup items >
Backup Items (Azure Virtual Machine)
InsightScape-Vault
Refresh
Add
Filter
Feedback
Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery. →
All data fetched from the service.
Filter items ...
Name
Resource Group
Backup Pre-Check
Last Backup Status
Latest restore point
Details
InsightScape-VM1
InsightScape-RG
Passed
Success
10/21/2024, 4:54:08 PM
View details
Previous
Page 1 of 1
Next

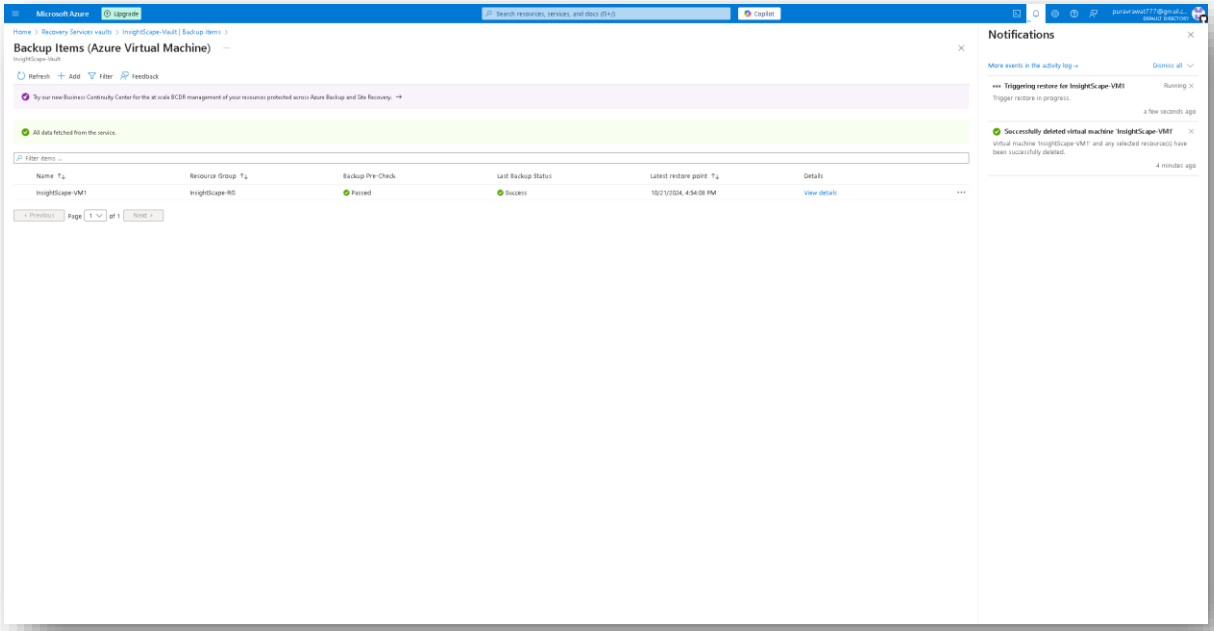

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Virtual machines >
Virtual machines
Default Directory
Create
Switch to classic
Filter for any field...
Name
InsightScape-VM1
InsightScape-VM2
Page 1 of 1
InsightScape-VM1
Virtual machine
Connect
Start
Restart
Stop
Hibernate
Capture
Delete
Refresh
Open in mobile
Feedback
CLI / PS
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Connect
Networking
Settings
Disks
Extensions + applications
Operating system
Configuration
Advisor recommendations
Properties
Locks
Availability + scale
Security
Backup + disaster recovery
Operations
Auto-shutdown
Run command
Updates
Health monitoring
Configuration management
Policies
Inventory
Change tracking
Monitoring
Insights
Alerts
Metrics
Diagnostic settings
Logs
Workbooks
Essentials
Resource group (move) : insightscape-rg
Status : Stopped (deallocated)
Location : West US 2
Subscription (move) : Free Trial
Subscription ID : cfe3d704-6d8b-4d88-9312-d58a0d3e9a50
Tags (edit) : Add tags
Properties
Monitoring
Capabilities (8)
Recommendations
Tutorials
Virtual machine
Computer name InsightScape-VM
Operating system Windows
VM generation V2
VM architecture x64
Hibernation Disabled
Host group -
Host -
Proximity placement group -
Colocation status N/A
Capacity reservation group -
Disk controller type SCSI
Azure Spot
Azure Spot -
Azure Spot eviction policy -
Availability + scaling
Availability zone (edit) -
Availability set -
Scale Set -
Security
Security type Standard
Health monitoring
Health monitoring Not enabled
Extensions + applications
Extensions AzureMonitorWindowsAgent, AzureNetworkWatcherExtension, AzurePerformanceDiagnostics,
Delete InsightScape-VM1
This action will permanently delete this virtual machine.
Resource to be deleted
Resource type
InsightScape-VM1
Virtual machine
Apply force delete
You can also choose to delete associated resources at the same time. Resources that aren't deleted will be orphaned. Associated resources that are in use by other resources are not shown here.
Associated resource type
Quantity
Delete with VM
OS disk 1
Network interfaces 1
Public IP addresses 1
I have read and understand that this virtual machine as well as any selected associated resources listed above will be deleted.
Delete
Cancel
Feedback

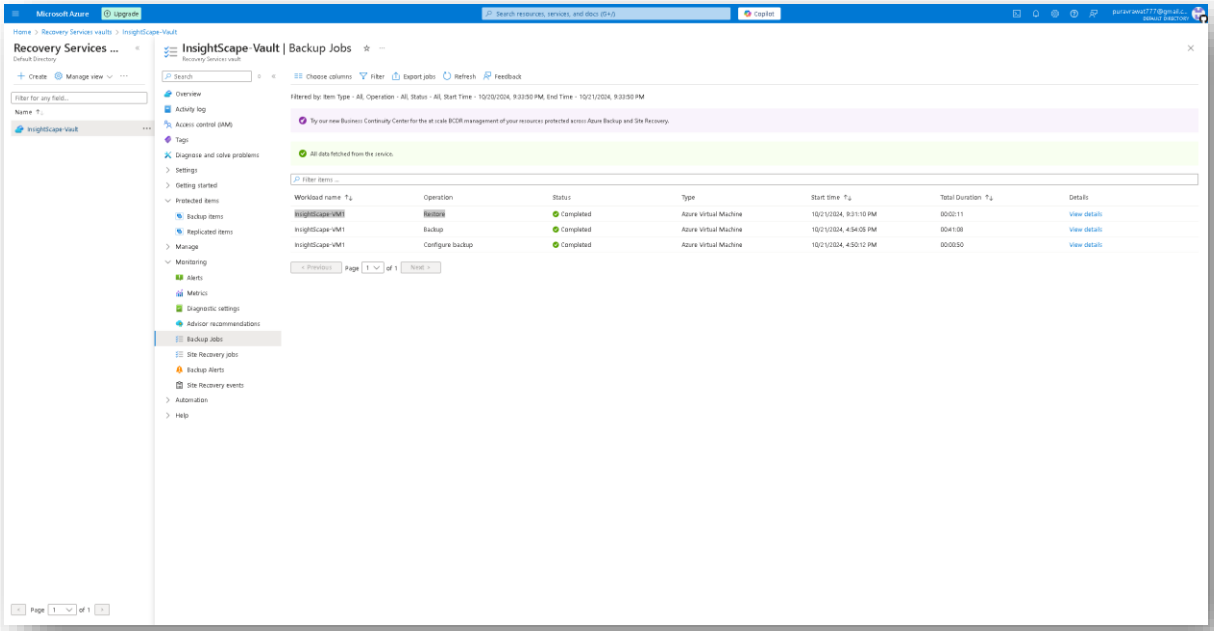

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Virtual machines
Virtual machines
Default Directory
Create
Switch to classic
Filter for any field...
Name
InsightScape-VM1
InsightScape-VM2
Page 1 of 1
InsightScape-VM1
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Connect
Networking
Settings
Disks
Extensions + applications
Operating system
Configuration
Advisor recommendations
Properties
Locks
Availability + scale
Security
Backup + disaster recovery
Operations
Auto-shutdown
Run command
Updates
Health monitoring
Configuration management
Policies
Inventory
Change tracking
Monitoring
Insights
Alerts
Metrics
Diagnostic settings
Logs
Workbooks
Not found
Get support
Perform self-diagnostics
Summary
Session ID
Resource ID
Extension
Microsoft_Azure_Compute
Content
VirtualMachinePrototBlade
Error code
404
Notifications
More events in the activity log →
Dismiss all
Successfully deleted virtual machine 'InsightScape-VM1'
Virtual machine 'InsightScape-VM1' and any selected resource(s) have been successfully deleted.
a few seconds ago

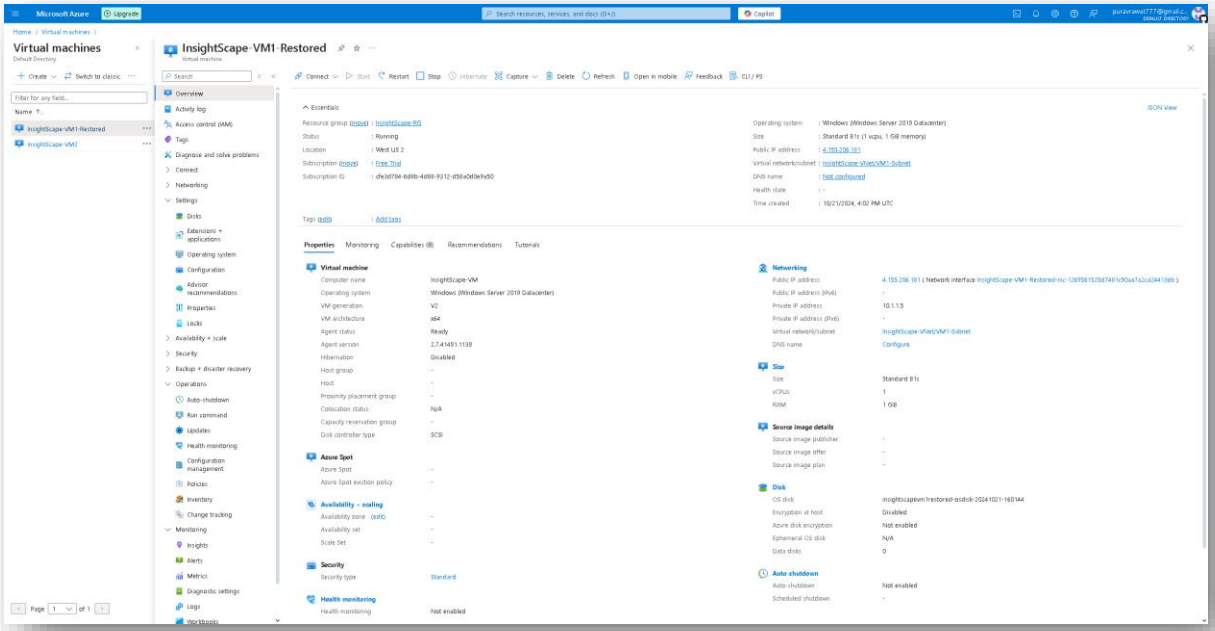

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Recovery Services vaults > InsightScape-Vault | Backup items
Backup Items (Azure Virtual Machine)
InsightScape-Vault
Refresh
Add
Filter
Feedback
Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery. →
All data fetched from the service.
Filter items ...
Name
Resource Group
Backup Pre-Check
Last Backup Status
Latest restore point
Details
InsightScape-VM1
InsightScape-RG
Passed
Success
10/21/2024, 4:54:08 PM
View details
Previous
Page 1 of 1
Next
Backup now
Restore VM
File Recovery
Stop backup
Delete backup data
Resume backup
Undelete


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Recovery Services vaults > InsightScape-Vault | Backup items > Backup Items (Azure Virtual Machine) >
Restore Virtual Machine
InsightScape-VM1
Restore allows you to restore VM/disks from a selected Restore Point.
Restore point *
No Restore Point Selected
Select
Restore
Select restore point
InsightScape-VM1
Start Date
10/07/2024
End Date
10/21/2024
Recovery point consistency
All restore points
Time
Consistency
Recovery Type
10/21/2024, 4:54:08 PM
Application Consistent
Snapshot and Vault-Standard
OK
Cancel
Give feedback


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Recovery Services vaults > InsightScape-Vault | Backup items > Backup Items (Azure Virtual Machine) >
Restore Virtual Machine
InsightScape-VM1
Restore allows you to restore VM/disks from a selected Restore Point.
Restore point *
10/21/2024, 4:54:08 PM
Select
Data Store
Snapshot and Vault-Standard
Restore configuration
Restore target
Create new
Replace existing
To create an alternate configuration when restoring your VM (from the following menus), use PowerShell cmdlets.
Restore Type *
Create new virtual machine
Virtual machine name *
InsightScape-VM1-Restored
Subscription *
Free Trial
Resource group *
InsightScape-RG
Virtual network *
InsightScape-VNet (InsightScape-RG)
Subnet *
VM1-Subnet
Staging Location *
inscapescapestorage (Standard_LRS)
Can't find your storage account?
Assign an MSI with the right permissions for automated cleanup on restore failure. Without an MSI, manual intervention is required.
Identities
Disabled
Restore
Give feedback


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Recovery Services vaults > InsightScape-Vault | Backup items >
Backup Items (Azure Virtual Machine)
InsightScape-Vault
Refresh
Add
Filter
Feedback
Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery.
All data fetched from the service.
Filter items ...
Name
Resource Group
Backup Pre-Check
Last Backup Status
Latest restore point
Details
InsightScape-VM1
InsightScape-RG
Passed
Success
10/21/2024, 4:54:08 PM
View details
Previous
Page 1 of 1
Next
Notifications
More events in the activity log →
Dismiss all
Triggering restore for InsightScape-VM1
Running
Trigger restore in progress.
a few seconds ago
Successfully deleted virtual machine 'InsightScape-VM1'
Virtual machine InsightScape-VM1 and any selected resource(s) have been successfully deleted.
4 minutes ago


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Recovery Services vaults > InsightScape-Vault
Recovery Services ...
Default Directory
Create
Manage view
Filter for any field...
Name
InsightScape-Vault
InsightScape-Vault | Backup Jobs
Recovery Services vault
Search
Choose columns
Filter
Export jobs
Refresh
Feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Getting started
Protected items
Backup items
Replicated items
Manage
Monitoring
Alerts
Metrics
Diagnostic settings
Advisor recommendations
Backup Jobs
Site Recovery jobs
Backup Alerts
Site Recovery events
Automation
Help
Filtered by: Item Type - All, Operation - All, Status - All, Start Time - 10/20/2024, 9:33:50 PM, End Time - 10/21/2024, 9:33:50 PM
Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery.
All data fetched from the service.
Filter items ...
Workload name
Operation
Status
Type
Start Time
Total Duration
Details
InsightScape-VM1
Restore
Completed
Azure Virtual Machine
10/21/2024, 9:31:10 PM
00:02:11
View details
InsightScape-VM1
Backup
Completed
Azure Virtual Machine
10/21/2024, 4:54:05 PM
00:41:08
View details
InsightScape-VM1
Configure backup
Completed
Azure Virtual Machine
10/21/2024, 4:50:12 PM
00:00:50
View details
Previous
Page 1 of 1
Next
Page 1 of 1


Microsoft Azure
Upgrade
Copilot
Virtual machines
InsightScape-VM1-Restored
InsightScape-VM2
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Networking
Settings
Disks
Operating system
Configuration
Properties
Locks
Availability + scale
Security
Backup + disaster recovery
Operations
Auto-shutdown
Run command
Updates
Monitoring
Insights
Alerts
Metrics
Logs
Connect
Restart
Stop
Capture
Delete
Refresh
Open in mobile
Feedback
CLI / PS
Essentials
JSON View
Resource group (move) : InsightScape-RG
Status : Running
Location : West US 2
Subscription (move) : Free Trial
Subscription ID : cfe3d704-6d8b-4d88-9312-d58a0d0e9a50
Operating system : Windows (Windows Server 2019 Datacenter)
Size : Standard B1s (1 vcpu, 1 GiB memory)
Public IP address : 4.155.206.181
Virtual network/subnet : InsightScape-VNet/VM1-Subnet
DNS name : Not configured
Health state : -
Time created : 10/21/2024, 4:02 PM UTC
Tags (edit) : Add tags
Properties
Monitoring
Capabilities (8)
Recommendations
Tutorials
Virtual machine
Computer name InsightScape-VM
Operating system Windows (Windows Server 2019 Datacenter)
VM generation V2
VM architecture x64
Agent status Ready
Agent version 2.7.41491.1139
Hibernation Disabled
Azure Spot
Availability + scaling
Security
Security type Standard
Health monitoring
Health monitoring Not enabled
Networking
Public IP address 4.155.206.181 (Network interface InsightScape-VM1-Restored-nic-126956152fd7481c90aa7a2ca2441deb)
Private IP address 10.1.1.5
Virtual network/subnet InsightScape-VNet/VM1-Subnet
DNS name Configure
Size
Size Standard B1s
vCPUs 1
RAM 1 GiB
Source image details
Disk
OS disk insightscapevm1restored-osdisk-20241021-160144
Encryption at host Disabled
Azure disk encryption Not enabled
Ephemeral OS disk N/A
Data disks 0
Auto-shutdown
Auto-shutdown Not enabled

Conclusion

Summary of Steps

- **Resource Group and Virtual Network Setup**: Established a Resource Group named *InsightScape-RG* and deployed a Virtual Network (*InsightScape-VNet*) in the East US region. Configured *VM1-Subnet* and *VM2-Subnet* to meet specific project requirements.

- **Virtual Machines and Network Security Groups (NSGs)**: Deployed two virtual machines, *InsightScape-VM1* (Windows) and *InsightScape-VM2* (Linux), each allocated to their respective subnets. Configured NSG rules to efficiently manage inbound and outbound traffic, ensuring robust security for both virtual machines.

- **Web App Deployment**: Deployed an Azure Web App named *InsightScape-WebApp* with the ASP.NET V4.8 runtime, integrated with Application Insights for real-time monitoring. Successfully hosted a sample application via GitHub, showcasing the web app's deployment capabilities.

- **Blob Storage and Logic App Automation**: Set up an Azure Blob Storage Account and configured a Logic App to automate the retrieval of blob contents. Verified the functionality of the Logic App by successfully triggering the workflow upon uploading documents to the Blob Storage container.

- **Networking Resources**: Activated Network Watcher to monitor the health of the network. Configured Packet Capture on *InsightScape-VM1* and utilized Connection Monitor to verify connectivity between the virtual machines.

- **Azure Backup Configuration**: Created a Recovery Services Vault and configured automated backups for *InsightScape-VM1*. Successfully initiated and verified backup operations through the Backup Jobs tab.

- **Azure Monitor Integration**: Enabled VM Insights for both *InsightScape-VM1* and *VM2*, actively monitoring key performance metrics such as CPU utilization and memory usage. Configured alerts to notify of high CPU usage scenarios.

- **Application Insights Integration**: Integrated Application Insights with *InsightScape-WebApp* to track application performance. Analyzed key metrics including failed requests, server response times, and user interactions to ensure the web app's optimal performance.

- **Network Monitoring**: Utilized Network Watcher's topology to visualize the network infrastructure. Conducted NSG Diagnostics to analyze traffic flow between resources and adjusted NSG rules to evaluate their impact on traffic.

- **Security and Compliance**: Leveraged Azure Security Center and Microsoft Defender for Cloud to assess the security posture and mitigate potential vulnerabilities. Implemented recommendations such as VM updates, disk encryption, and network security enhancements to improve overall security compliance.

- **Alerts Configuration**: Set up Azure Monitor Alerts for *InsightScape-VM1* to provide proactive monitoring and alerting on critical performance thresholds.

- **Backup and Disaster Recovery Validation**: Validated the backup and disaster recovery process by simulating the deletion of *InsightScape-VM1* and restoring it from the most recent backup. Successfully verified the integrity and functionality of the restored VM.

Skills Demonstrated Through the InsightScape Project

1. **Network Infrastructure Setup**:
    - Designed and deployed Azure Virtual Networks with subnet configurations.
    - Implemented Network Security Groups (NSGs) to manage network traffic, ensuring secure inbound and outbound connections.
2. **Cloud Resource Deployment and Management**:
    - Deployed and configured various Azure resources, including virtual machines, web apps, and blob storage accounts.
    - Demonstrated expertise in managing virtual machine access using public IPs and applying resource-specific security measures.
3. **Automation and Workflow Implementation**:
    - Developed and automated workflows using Azure Logic Apps, streamlining operational processes.
    - Configured triggers to automate actions, showcasing advanced automation skills within the Azure environment.
4. **Security Enhancements and Compliance**:
    - Utilized Azure Security Center and Microsoft Defender for Cloud to assess and improve the security posture of deployed resources.
    - Implemented key security recommendations such as disk encryption, VM patch management, and network security adjustments to ensure compliance with best practices.
5. **Monitoring and Alert Configuration**:
    - Configured Azure Monitor, Application Insights, and Log Analytics to provide real-time insights into resource health and performance.
    - Set up custom alerts for scenarios such as failed login attempts and application errors, ensuring timely responses to critical issues.
6. **Backup and Disaster Recovery**:
    - Implemented Azure Backup for disaster recovery purposes and successfully validated the recovery of a deleted virtual machine.
    - Ensured that essential data and applications could be restored in the event of an emergency.

7. **Performance and Availability Monitoring**:
    - Monitored the performance of virtual machines and web applications, analyzing metrics such as CPU usage, memory consumption, and server response times.
    - Identified and addressed performance bottlenecks, maintaining high availability and optimizing resource performance.
8. **Network Analysis and Troubleshooting**:
    - Employed Azure Network Watcher for visualizing and troubleshooting network infrastructure.
    - Configured Packet Capture and analyzed network traffic to detect and resolve communication issues between resources.
9. **Cost Management and Resource Optimization**:
    - Demonstrated awareness of cost management by cleaning up unused resources post-validation and testing.
    - Managed the lifecycle of Azure resources to ensure efficient and cost-effective use of services.

Hands-On Expertise

Demonstrated strong hands-on capabilities in monitoring and maintaining Azure resources, aligned with the core competencies required for the *Microsoft Certified: Azure Administrator Associate (AZ-104)* certification.