

InsightScape

(Monitor and Back up Azure resources)

Manual By-
Purav Rawat

Date: 21 October 2024

Contact:

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

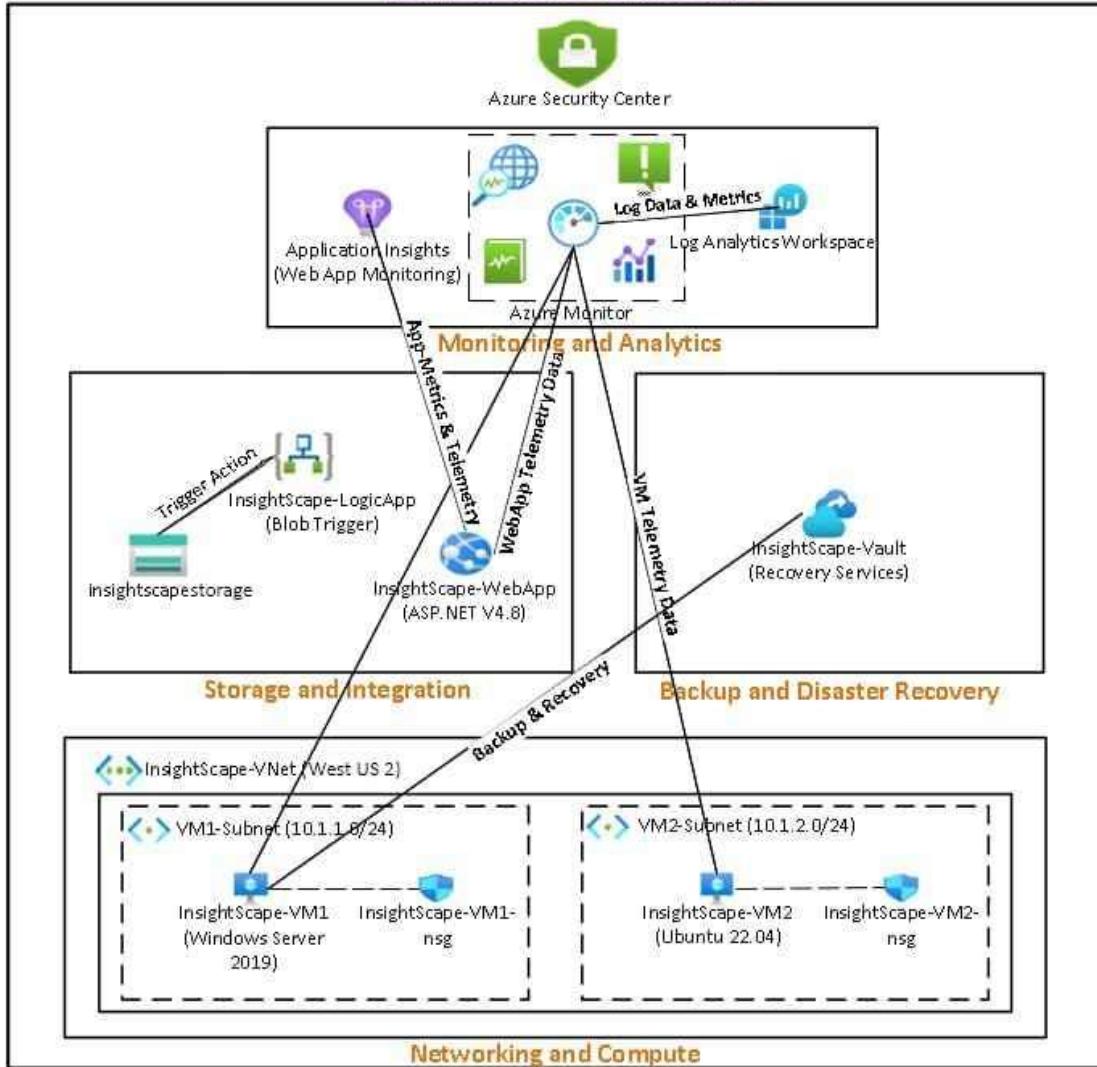
GitHub: soon

Table of Contents

- Project Architecture Diagram
- Introduction
- Azure Monitor Integration
- Application Insights
- Network Monitoring
- Security & Compliance
- Alerts Configuration
- Backup and Disaster Recovery
- Conclusion
- Lessons Learned

Project Architecture Diagram

InsightScape: Azure Monitoring and Maintenance Architecture



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 -

This screenshot shows the Microsoft Azure portal homepage. At the top, there's a search bar and a 'Create' button. Below the search bar, a message says 'Hi Purav, see what more you can do'. There are sections for 'Azure services' (Create a resource, Resource groups, Virtual networks), 'Resources' (Recent, Favorite, Insightscape, Free trial, See all), 'Navigate' (Subscriptions, Resource groups, All resources, Dashboard), 'Tools' (Microsoft Learn, Azure Monitor, Microsoft Defender for Cloud, Cost Management), and 'Useful links' (Technical Documentation, Azure Services, Recent Azure Logins, Azure mobile app). On the right, there's a sidebar with 'Explore support resources' and a 'Feedback' link.

This screenshot shows the Microsoft Azure portal for the 'InsightScape RG' resource group. The left sidebar has options like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Cost Management, Monitoring, Automation, and Help. The main area shows the 'Essentials' section with a 'Subscription' card (Subscription ID: 0aa701, Subscription ID: 0984f749-46fb-48ff-9112-d3b2a0d6d0) and a 'Tags' card (Tags: 0, Add tags). The 'Resources' section shows a table with columns: Name, Type, and Location. A note says 'Showing 0 to 0 of 0 records.' and 'No grouping' is selected. The 'Recommendations' section shows a note 'No resources match your filters' with 'Try changing or clearing your filters.' and buttons for 'Create resource' and 'Clear filters'. At the bottom right, there's a 'Give feedback' link.

Microsoft Azure | Upgrade

Hi Purav, see what more you can do

View remaining usage to try any service, or [choose free services](#)

Take a free online course on Microsoft Learn.

What's new?

Azure services

Create a resource Resource groups Cost Management

Resources

Recent Favorites

Name	Type	Last Viewed
insightscape	Resource group	a few seconds ago
free trial	Subscription	5 minutes ago

Navigate

Subscriptions Resource groups All resources Dashboard

Tools

Microsoft Learn Microsoft 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 Services Find an Azure expert Recent Azure Updates Dashboard center Azure mobile app

Apple Store Google Play

Search resources, services, and docs (S+I)

Puravaw777@gmail.com

Virtual networks | Marketplace | See more

All Services (31) Marketplace (0) More (4)

Virtual networks

- Virtual networks (classic)
- Virtual network gateways
- Virtual Network Manager

Marketplace

- Virtual network
- Virtual network gateway
- Storage and VHD Deployment
- Trend Micro Cloud One™ - Network Security

Documentation

- Quickstart: Use the Azure portal to create a virtual network - Azure Virtual Network
- Configure Virtual Networks for Azure AI services - Azure AI services
- Virtual networks for Azure services
- Virtual network integration of Azure services for network isolation

Continue searching in Microsoft Entra ID

Give feedback

See all

Microsoft Azure | Upgrade

Home > Virtual networks >

Create virtual network

Basics Security IP addresses Tags Review + create

About Azure Virtual Networks (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 all the advantages of Azure's infrastructure such as scale, availability, and resilience.

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:

Instance details

Virtual network name *:

Region *:

Deploy to an Azure Extended Zone

Previous Next Review + create Give feedback

Create virtual network

IP addresses

Configure your virtual network's 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 /16 65536 addresses

Subnets IP address range Size NAT gateway

Add IPv4 address space | ~

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 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, you must 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

Provide 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

Previous Next Review + create

Create virtual network

IP addresses

Configure your virtual network's 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 /16 65536 addresses

Subnets IP address range Size NAT gateway

VM1-Subnet 10.1.1.0 - 10.1.1.255 /24 (256 addresses) -

Add IPv4 address space | ~

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 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, you must 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

Provide 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

Previous Next Review + create

Create virtual network

IP addresses

Configure your virtual network's 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 resources an IP address from the subnet. [Learn more](#)

+ Add a subnet

10.0.0/16

Subnets IP address range Size NAT gateway

VM1-Subnet 10.1.0 - 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](#)

InsightScape VNet-1729502099389

Overview

Essentials

Activity log, Access control (IAM), Tags, Diagnostic and solve problems, Settings, Address space, Connected devices, Subnets, Firewall, DDoS protection, Peering, Service endpoints, Private endpoints, Locks, Monitoring, Automation, Help.

Resource group: [InsightScape RG](#), Location: [US West 2](#), Subscription: [Free Trial](#), Subscription ID: [cfd3d14e-edbf-4d88-9312-d3ba0d4a50](#).

Address space: 10.0.0/16, DNS servers: Azure provided DNS service, Flow timeout: 1 hour, BGP community string: [Configure](#), Virtual network ID: [d0f5adfb-97d3-413a-85aa-c76312b0512](#).

Tags [Add tags](#)

Topology, Properties, Capabilities (0), Recommendations, Tutorials.

Capabilities

- DDoS protection: Not configured
- Azure Firewall: Protect your network with a standard or firewall.
- Peering: Seamlessly connect two or more virtual networks.
- Microsoft Defender for Cloud: Strengthen the security posture of your environment.
- Private endpoints: Privately access Azure services without exposing traffic across internet.

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 –

This screenshot shows the Microsoft Azure portal homepage. At the top, there's a search bar with the word "virtual". Below it, a sidebar lists "Services (0)" and "Marketplace (0)". A main content area displays a welcome message: "Hi Purav, see what more you can do with Azure" and "View remaining credit to try any service, or learn how to use Azure services". It also features a "Take a free online course on Microsoft Learn" button. The "Azure services" section includes a "Create a resource" button and links for "Virtual machines", "Virtual networks", "Virtual Appointments Builder", "Virtual clusters", and "Marketplace". The "Resources" section shows a table with three items: "InsightsScope-vnet" (Virtual network), "InsightsScope-RG" (Resource group), and "Free trial" (Subscription). The "Navigate" section has links for "Subscriptions", "Resource groups", "All resources", and "Dashboard". The "Tools" section includes links for "Microsoft Learn", "Azure Monitor", "Microsoft Defender for Cloud", and "Cost Management". The "Useful links" section contains links for "Azure mobile app" and "Azure DevOps".

This screenshot shows the "Create a virtual machine" wizard in the Microsoft Azure portal. The page title is "Create a virtual machine". There are four tabs at the top: "Basic", "Disk", "Networking", and "Management". The "Basic" tab is selected. The form fields include:

- Subscription:** Free Trial
- Resource group:** InsightsScope-RG
- Virtual machine name:** InsightsScope-VM1
- Region:** US West US 2
- Availability options:** No infrastructure redundancy required
- Security type:** Standard
- Image:** Windows Server 2019 Datacenter - x64 Gen2 (free services eligible)
- VM architecture:** x64 (selected)
- Run with Azure Spot discount:** Unchecked
- Size:** Standard_B1s - 1 vCPU, 1 GB memory (990.25/month) (free services eligible)
- Enable Hibernation:** Unchecked

At the bottom, there are "Next: Disks" and "Review + create" buttons.

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](#)

Networking

Define network connectivity for your virtual machines 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 [Create new](#)

Subnet [Manage subnet configuration](#)

Public IP [Create new](#)

NIC network security group None Basic Advanced

Public inbound ports None Allow selected ports

Select inbound ports

⚠️ 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 access 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](#)

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](#)

⚠️ This step has failed. You have opted to skip validation. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Basics

Subscription	Free Trial
Resource group	InsightScope-RG
Virtual machine name	InsightScope-VM1
Region	West US 2
Availability options	No infrastructure redundancy required
Zone options	Standard
Security type	Standard
Image	Windows Server 2019 Datacenter - Gen2
VM architecture	x64
Size	Standard_B1s (1 vCPU, 1 GB memory)
Enable Hibernation	No
Username	InsightScope-User1
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
Create a disk with VM	Enabled
Spherical OS disk	No

Networking

Virtual network	InsightScope-VNet
Subnet	VM1-Subnet (10.1.1.0/24)
Public IP	(new) InsightScope-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

Home > Overview-MicrosoftWindowsServer-2019-20241021144644 | Overview

InsightScape VM1

Search resources, services, and docs (S+)

Connect Start Stop Hibernate Capture Delete Refresh Open in mobile CU / PS

Overview

Activity log

Tag

Diagnose and solve problems

Connect

Availability + scale

Settings

Security

Backup + disaster recovery

Operations

Monitoring

Automation

Help

Essentials

Resource group [InsightScape-RG](#)

Status: Running

Location: West US 2

Subscription [Free Trial](#)

Subscription ID: [XXXXXXXXXX](#)

Operating system: Windows (Windows Server 2019 Datacenter)

Size: Standard_B1s (1 vcpu, 1 GB memory)

Public IP address: [137.77.137.190](#)

Virtual network/subnet: [InsightScape-VNet/VM1-Subnet](#)

DNS name: [not configured](#)

Health state: -

Time created: 10/21/2024, 9:22 AM UTC

Tags (0) | Add tags

Properties Monitoring Capabilities (B) Recommendations Tutorial

Virtual machine

Computer name: InsightScape-VM

Operating system: Windows (Windows Server 2019 Datacenter)

VM generation: V2

VM architecture: x64

Agent status: Ready

Agent version: 2.74.461.1025

Reservation: Disabled

Host group: -

Host: -

Priority placement group: -

Calculated 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: -

Networking

Public IP address: [137.77.137.190](#) | Network interface [insightScape-vm1-1714](#)

Private IP address (IPv6): -

Private IP address (IPv4): 10.1.1.4

Virtual network/subnet: [InsightScape-VNet/VM1-Subnet](#)

DNs name: [Configure](#)

Size

Size: Standard_B1s

vCPUs: 1

RAM: 1 GB

Source image details

Source image publisher: MicrosoftWindowsServer

Source image offer: WindowsServer

Source image plan: 2019-datacenter-gen-second

Disk

OS disk: [InsightScape-VM1_OsDisk_1_8955d944eb7410082014779d0e062c2](#)

Encryption at host: Disabled

Allow disk encryption: Not enabled

General OS disk: N/A

Data disks: 0

Auto shutdown

Auto shutdown: Not enabled

Scheduled shutdown: -

Health monitoring

Health monitoring: Not enabled

JSON View

Microsoft Azure | Upgrade

Home > Virtual machines

Create a virtual machine

Changing basic options may result in selections you have made. Review all options prior to creating the virtual machine.

Help me create a low cost VM | Help me choose a VM optimized for high availability | Help me choose the right VM size for my workload

Basics 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. You can also upload a file. 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 display 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 - 64-bit \(2 cores\) \(eligible\)](#)

This image is compatible with additional security features. Click here to learn more about the [TrustLaunch security hub](#).

See all images | Configure VM generation

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 GB memory \(651.61/month\) \(free services eligib...\)](#)

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

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](#)

Networking

Define network connectivity for your virtual machines 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 * [InsightScope-VNet](#) [Create new](#)

Subnet * [VM2-Subnet \(10.12.0.0/24\)](#) [Manage subnet configuration](#)

Public IP [\(new\) InsightScope-VM2-ip](#) [Create new](#)

NIC network security group [None](#) [Basic](#) [Advanced](#)

Public inbound ports * [None](#) [Allow selected ports](#)

Select inbound ports * [SSH \(22\)](#)

Warning: 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 fit a more specific known IP address.

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](#) [Create](#) [Give feedback](#)

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	InsightScope-RG
Virtual machine name	InsightScope-VM2
Region	West US
Availability options	No infrastructure redundancy required
Zone options	Self-redundant zone
Security type	Standard
Image	Ubuntu Server 24.04 LTS - Gen2
VM architecture	x64
Size	Standard B1s (1 vcpu, 1 GB memory)
Enable virtualization	No
Authentication type	Password
Username	InsightScope-User2
Public inbound ports	SSH, HTTPS, HTTP
Azure Spot	No

Disk

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	InsightScope-VNet
Subnet	VM2-Subnet (10.12.0.0/24)
Public IP	(new) InsightScope-VM2-ip
Accelerated networking	Off
Place this virtual machine behind an existing load balancer	No
Delete public IP and NIC when VM is deleted	Enabled

Management

Windows Defender for Cloud	Basic (free)
System assigned managed identity	Off
Login with Microsoft Entra ID	Off
Auto shutdown	Off
Backup	Disabled
Enable hepatitis	Off

[« Previous](#) [Next: Create](#) [Download a template for automation](#) [Give feedback](#)

Microsoft Azure | Upgrade

Home > [Create] > Overview > InsightScape-VM2

Overview

Connect Start Stop Hibernate Capture Delete Refresh Open in mobile CU / PS

Search resources, services, and docs (Sx)

Copy

InsightScape-VM2

Resource group: insightScape-RG

Status: Running

Location: West US 2

Subscription: Free Trial

Subscription ID: [REDACTED]

Operating system: Linux (Ubuntu 24.04)

Size: Standard B1s (1 vcpu, 1 GB memory)

Public IP address: 52.148.174.238

Virtual network/subnet: insightScape-VNet/VM2-Subnet

DNS name: [REDACTED].privatelink.com

Health state: -

Time created: 10/21/2024, 9:49 AM UTC

JSON View

Activity log

Tag

Diagnose and solve problems

Connect

Networking

Settings

Availability + scale

Tags (0) Add tags

Properties Monitoring Capabilities (7) Recommendations Tutorial

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

Reservation: Disabled

Host group: -

Host: -

Priority placement group: -

Calculation 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: 52.148.174.238 (Network interface insightScape-vm2t10)

Private IP address: -

Private IP address (IPv6): -

Virtual network/subnet: insightScape-VNet/VM2-Subnet

DNS name: Configure

Size

Size: Standard B1s

vCPUs: 1

RAM: 1 GB

Source image details

Source image publisher: canonical

Source image offer: Ubuntu-24.04-It

Source image plan: server

Disk

OS disk: insightScape-VM2_OsDisk_1_b0f271ff-e0c7-484d-b172fc04fa0

Encryption at host: Disabled

Allow disk encryption: Not enabled

General OS disk: fq4

Data disks: 0

Auto shutdown

Auto shutdown: Not enabled

Scheduled shutdown: -

Microsoft Azure | Upgrade

Home > Network security groups

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

No grouping List view

Showing 1 to 2 of 2 records.

Name	Resource group	Location	Subscription	Flow log	Actions
insightScape-VM1-NSG	insightScape-RG	West US 2	Free Trial	-	...
insightScape-VM2-NSG	insightScape-RG	West US 2	Free Trial	-	...

Page 1 of 1

Give feedback

Microsoft Azure | Upgrade

Home > Network security groups > InsightScape-VM1-nsg

Network security group

Default Directory (pwnaserv177@msft-on-prem.local)

Overview

Inbound security rules

Add inbound security rule

Search resources, services, and docs (S+)

Filter for any field...

Name: InsightScape-VM1-nsg

Activity log

Tags

Diagnose and solve problems

Settings

- Inbound security rules
- Outbound security rules
- Network interface

Subnets

Properties

Monitoring

Automation

Help

Page 1 of 1

Search by name

+ Add

Port: 80

Protocol: TCP

Source: Any

Destination: Any

Action: Allow

Priority: 300

Name: HTTP

Port: 443

Protocol: TCP

Source: Any

Destination: Any

Action: Allow

Priority: 300

Name: AllowAllInbound

Port: Any

Protocol: Any

Source: Any

Destination: Any

Action: Allow

Priority: 300

Name: DenyAllInbound

Port: Any

Protocol: Any

Source: Any

Destination: Any

Action: Deny

Add Cancel Give feedback

Priority: 300

Name: HTTP

Description:

Microsoft Azure | Upgrade

Home > Network security groups > InsightScape-VM1-nsg

Network security group

Default Directory (pwnaserv177@msft-on-prem.local)

Overview

Inbound security rules

Created security rule

Successfully created security rule: HTTP

Search resources, services, and docs (S+)

Filter for any field...

Name: InsightScape-VM1-nsg

Activity log

Tags

Diagnose and solve problems

Settings

- Inbound security rules
- Outbound security rules
- Network interface

Subnets

Properties

Monitoring

Automation

Help

Page 1 of 1

Search by name

+ Add

Port: 80

Protocol: TCP

Source: Any

Destination: Any

Action: Allow

Priority: 300

Name: HTTP

Port: 443

Protocol: TCP

Source: Any

Destination: Any

Action: Allow

Priority: 300

Name: AllowAllInbound

Port: Any

Protocol: Any

Source: Any

Destination: Any

Action: Allow

Priority: 300

Name: DenyAllInbound

Port: Any

Protocol: Any

Source: Any

Destination: Any

Action: Deny

Microsoft Azure Upgrade

Network security groups > Network security groups

Custom security rules: 3 inbound, 0 outbound

InsightScapeVM2nsg120

Search resources, services, and docs (F1)

Custom security rules : 3 inbound, 0 outbound

Associated with : 0 subnets, 1 network interface

Overview Essentials

Name : InsightScapeVM2nsg120

Resource group (Subscription) : InsightScape RG

Location : West US 2

Subscription (Subscription) : free Trial

Subscription ID : dca0f4e4-64b8-9312-d5ba069a9650

Tags

Diagnostic and solve problems

+ Create Manage view

Filter for any field.

Inbound security rules

Outbound security rules

Network interface

Subnets

Properties

Locks

Monitoring

Automation

Help

Priority ↑ Name ↑ Port ↑ Protocol ↑ Source ↑ Destination ↑ Action ↑

Inbound Security Rules

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
300	SSH	22	TCP	Any	Any	Allow
320	HTTP	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
65002	DenyAllInbound	Any	Any	Any	Any	Deny
65000	AllowVnetOutbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutbound	Any	Any	Internet	Any	Allow
65002	DenyAllOutbound	Any	Any	Any	Any	Deny

Outbound Security Rules

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 -

This screenshot shows the Microsoft Azure portal's App Service dashboard. At the top, there's a banner for Microsoft Learn with a link to "Take a free online course on Microsoft Learn". Below the banner, there are sections for "Azure services" (Create a resource, Network security groups, Virtual machine) and "Resources" (Recent: insightscopeVMing10, insightscopeVMing, insightscope-RG, insightscope-VNet, insightscope-Web, Free Trial; Favorites: Microsoft Azure App Service, Application Insights Configuration Service). On the right, there's a sidebar with links for "Explore support resources", "support", "Logic apps", and "More services". The main area shows a table of resources with columns for Name, Type, Service Principal, and Last Viewed. At the bottom, there are "Navigate" buttons for Subscriptions, Resource groups, All resources, and Dashboard, along with "Tools" for Microsoft Learn, Azure Monitor, Microsoft Defender for Cloud, and Cost Management.

This screenshot shows the "Create Web App" wizard in the Microsoft Azure portal. The steps are: Basics, Deployment, Networking, Monitor + secure, Tags, Review + create. The "Basics" step is active. It asks for a Project Details (Subscription: Free Trial, Resource Group: insightscope-RG), Instance Details (Name: insightscope-Webapp, Publish: Code, Runtime stack: ASP.NET V4.8, Operating System: Windows, Region: Canada Central), Pricing plan (Windows Plan: Canada Central, Pricing plan: Free F1 (Shared infrastructure)), and Zone redundancy (Zone redundancy: Enabled). At the bottom, there are "Review + create", "Previous", and "Next: Deployment" buttons.

Create Web App

Basic Deployment Networking Monitor + secure Tags Review + create

The following features are optional and billed separately. Microsoft recommends enabling them to ensure the most robust protection and capabilities to monitor and secure your web application.

Application Insights

Azure Monitor application insights is an Application Performance Management (APM) service for developers and DevOps professionals. It collects and analyzes application logs, metrics, and dependencies from your services, and provides powerful analysis tools to help you diagnose issues and understand what users actually do with your app. Your bill is based on an amount of data used by Application Insights and your data retention settings. [Learn more](#)

App Insights pricing

Enable Application Insights? Yes No

Application Insights * [Check 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 instances, and more—detecting threats and stopping attacks to your resources. [More benefits of Defender for App Service](#) [Learn more](#)

Defender for Cloud pricing? [View](#)

Enable Defender for App Service

[Review + create](#) [Previous](#) [Next: Tags >](#)

InsightScape WebApp

Web App

Search Browse Stop Swap Restart Delete Refresh Download publish profile Reset publish profile Share to mobile Send us your feedback

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

Properties

Essentials	Default domain
Resource group InsightScape-RG	insightscape-webapp-1a89b90d.cana
Status	Running
Location Cloud	Canada Central
Subscription Free Trial	ASP-insightscapeRG-FTR
Tags Add tags	
Default domain: insightscape-webapp-1a89b90d.cana	
Health check: Cannot fetch health check data. Please try again later.	

Web app

Name	InsightScape-WebApp
Publishing model	Code
Runtime Stack	Other - v4.0

Domains

Default domain	insightscape-webapp-1a89b90d... Show More
Custom domain	Add custom domain

Hosting

Plan Type	App Service plan
Name	ASP-InsightScapeRG-FTR
Operating System	Windows
Instance Count	0
SKU and size	Free (F1) Scale up

Deployment Center

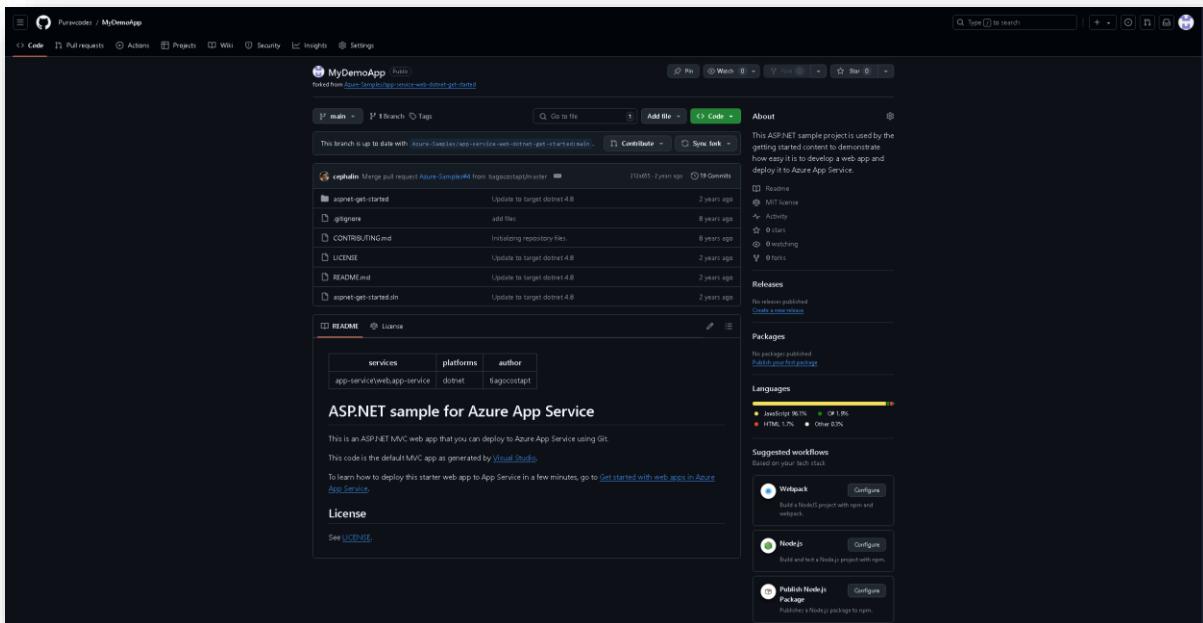
Deployment logs	View logs
Last deployment	No deployments found. Refresh
Deployment provider	None

Application Insights

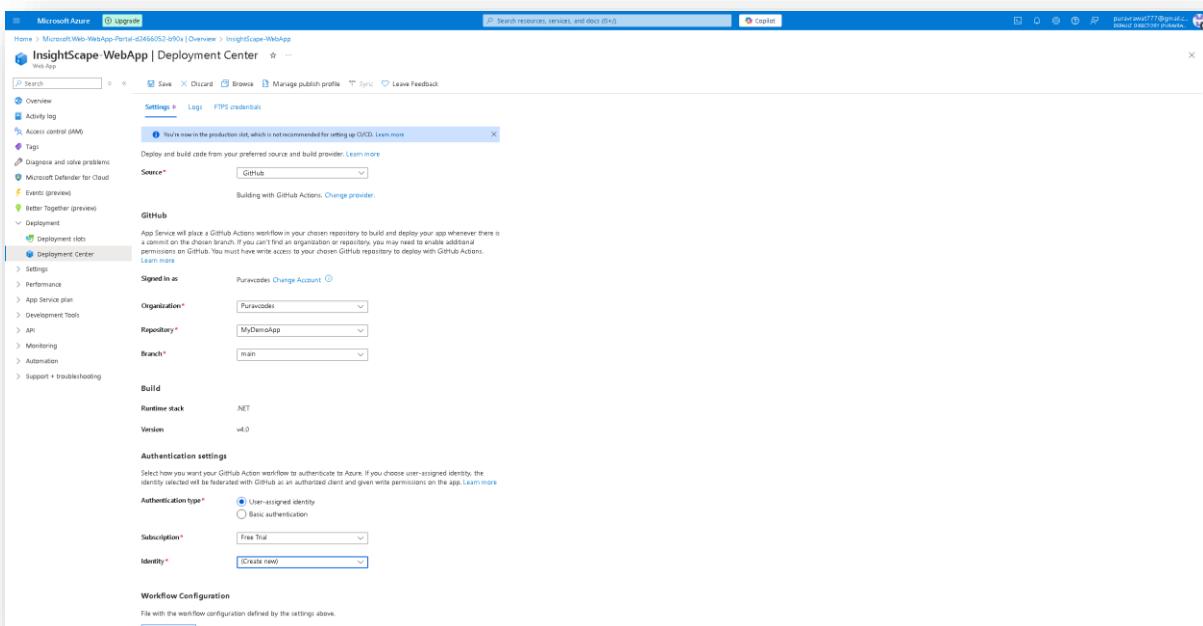
Name	InsightScape-WebApp
Region	Canada Central Show More

Networking

Virtual IP address	10.49.204.3
Outbound IP addresses	4.174.252.173, 4.174.252.189, 4.174.252...
Additional Outbound IP addresses	4.174.252.173, 4.174.252.189, 4.174.252...
Virtual network integration	Not supported



This screenshot shows the GitHub repository page for 'MyDemoApp'. The repository is based on the 'Azure-Samples/app-service-web-dotnet-get-started' template. The main branch is 'main', and there are 11 branches and 1 tag. The repository has 18 commits from 'caphalin' and 1 pull request. The README file is visible, and the repository is described as an ASP.NET sample for Azure App Service. It includes sections for Readme, Activity, Stars, Forks, Releases, Packages, Languages, and Suggested workflows (Webpack, Node.js, Publish Node.js package).



This screenshot shows the Microsoft Azure Deployment Center for the 'InsightScape WebApp'. The app service plan is set to 'd3466052-49a0-4' and the deployment center is active. The configuration includes GitHub as the source provider, with the organization set to 'Purwodes' and the repository to 'MyDemoApp' on the 'main' branch. The runtime stack is .NET, version v4.0. Authentication settings use 'User-assigned identity' with a free trial subscription and a new identity named '(Create new)'. Workflow configuration is defined by the settings above.

InsightScape-WebApp | Deployment Center

Web App

Search Save Discard Browse Manage publish profile Sync Leave Feedback

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 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	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 your application's logic.

[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 –

The screenshot shows the Microsoft Azure portal homepage. At the top, there's a search bar and a navigation bar with links for Storage, Services (19), Marketplace (0%), and More (4). A banner at the top left says "Hi Purav, see what more you can do" with a link to Microsoft Learn. Below the banner, there's a section for "Azure services" with a "Create a new resource" button, App Services, and Network security. The "Resources" section lists recent and favorite resources, including "insightspage-RG" and "insightspage-VM-1". On the right, there's a "Storage" section with a "Storage accounts" list showing items like "Storage Resource Provider", "Azure Storage", and "Diagnostic Services Trusted Storage Access". Below this is a "Documentation" section with links to "Storage in Azure Kubernetes Service (AKS) - Azure Kubernetes Service", "Change an Azure storage service - Azure Architecture Center", and "Monitor Azure Storage services with Azure Monitor Storage insights". Further down are sections for "Last viewed" resources and "Navigate" buttons for Subscriptions, Resource groups, All resources, and Dashboard.

This screenshot shows the "Create a storage account" wizard, Step 1: Basics. The title is "Create a storage account". It has tabs for Basics, Advanced, Networking, Data protection, Encryption, Tags, Review + create, and a "Previous" button. The Basics tab is selected. A note about Azure Storage is displayed, mentioning it's a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. It includes Azure Blob objects, Azure Data Lake Storage Gen2, Azure File, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. There's a "Learn more about Azure storage accounts" link. The "Subscription" dropdown is set to "Free Trial" and the "Resource group" dropdown is set to "insightspage-RG" with a "Create new" option. The "Storage account name" field contains "incopenstorage". The "Region" dropdown is set to "US West US 2" with a note about deploying to an Azure Extended Zone. The "Primary冗余" dropdown is set to "Azure Blob Storage or Azure Data Lake Storage Gen2". Under "Performance", the "Standard: Recommended for most scenarios (general-purpose S2 account)" radio button is selected. Under "Redundancy", the "Locally-redundant storage (LRS)" dropdown is selected. At the bottom, there are "Next" and "Review + create" buttons, and a "Give feedback" link.

Create a storage account

Review + create

Basics

Subscription	Free Trial
Resource group	InsightScope-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
Block anonymous access	Enabled
Allow storage account key access	Enabled
Default to Microsoft Entra authentication	Disabled
the Azure portal	
Minimum TLS version	Version 1.2
Permitted scope for copy operations	From any storage account
private	

Networking

Network connectivity	Public endpoint (all networks)
Default routing tier	Microsoft network routing

Data protection

Point-in-time restores	Disabled
blob soft delete	Enabled
blob retention period in days	7
Container soft delete	Enabled
Container retention period in days	7
File share soft delete	Enabled

Tags

Previous Next Create

Give feedback

inscapescapestorage

Storage account

Overview

Upload Open in Explorer Delete Move Refresh Open in mobile CU PS Feedback

Properties

Resource group	: insightScope-RG
Location	: westus2
Subscription	: Free Trial
Subscription ID	: c93d784-6d1b-4e89-9112-e591a0dfe1d0
Disk state	: Available
Tags	: Add tags

Essentials

Performance	: Standard
Replication	: Locally-redundant storage (LRS)
Account kind	: StorageV2 (general purpose v2)
Provisioning state	: Succeeded
Created	: 10/21/2024, 3:52:20 PM

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

Blade service

Hierarchical namespace	: Disabled
Default access tier	: Hot
Block 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 failover assignments	: None

File service

Large file shares	: Enabled
Identity-based access	: Not configured
Default share-level permissions	: Disabled
Soft delete	: Enabled (7 days)

Queue service

CORS support	: Disabled
--------------	------------

Table service

CORS support	: Disabled
--------------	------------

Microsoft Azure Upgrade

Home > inscapescapestorage_1779506035859 | Overview > inscapescapestorage | Containers

inscapescapestorage | Containers Import account

Search Container Change access level Restore containers Refresh Select Give feedback

Overview Tag log Activity log Diagnosis 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

Name Show deleted containers

Last modified Name Anonymous access level Lease

10/21/2024, 3:52:26 PM Private Available

Anonymous access level: Private (no anonymous access)

The access level is set to private because anonymous access is disabled on this storage account.

New container

Name * File

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

Home > inscapescapestorage_1779506035859 | Overview > inscapescapestorage | Containers > file

files Container

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 user account)

Location: file

Search blobs by prefix (case-sensitive)

Show deleted blobs

Add filter

Name	Modified	Access tier	Archive status	Blob type	Size	Last modified
No results						

Microsoft Azure (Upgrade)

Hi Purav, see what more you can do

View remaining credit to try any service, or [Learn more](#)

Take a free online course on Microsoft Learn [Get started](#)

Azure services

Create a resource App Services

Recent

- InsightCape-WEBapp
- InsightCape-RD
- InsightCape-WEB10
- InsightCape-VM-req
- InsightCape-VM2
- InsightCape-VM1
- InsightCape-Web1
- Free Trial

Resources

Microsoft Entra ID

Logic Apps

Services (19) Marketplace (11) More (4)

Logic apps

- Logic App Custom Connector
- App Services
- App Configuration
- Marketplace
- Logic App
- Logic App Custom Connector
- Logic App Management (Preview)
- Azure Logic Apps solution for Sentinel

Documentation

Edit and manage logic apps using Visual Studio - Azure Logic Apps

Create or join parallel branches in workflow - Azure Logic Apps

Import a Logic App as an API with the Azure portal

Create an Azure Logic Apps connector

Microsoft Entra ID

Azure Logic Apps

Service Principal

Continuous searching in Microsoft Entra ID

Search for more services

Last Viewed

a few seconds ago

Storage account

7 minutes ago

Resource group

9 minutes ago

Network security group

22 minutes ago

Network security group

23 minutes ago

Virtual machine

37 minutes ago

Virtual machine

an hour ago

Virtual network

an hour ago

Subscription

5 hours ago

See all

Navigate

Subscriptions Resource groups All resources Dashboard

Tools

Explore support resources

Microsoft Azure (Upgrade)

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 [\(1\)](#)

Consumption		Standard	
Multi-tenant Fully managed and easy to get started.	<input checked="" type="radio"/> Workflow Service Plan Single tenant runtime with in-app connectors and scaling features.	<input type="radio"/> App Service Environment V3 Single tenant runtime with full isolation and scale out feature across App Service plan.	<input type="radio"/> Hybrid PREVIEW Local processing and multi-cloud support with Kubernetes Event-Driven AutoScaling
Compute	Shared	Dedicated	Dedicated
Networking	Public cloud	VNET Integration	VNET Integration
Pricing	Pay-per-operation	Per workflow service plan instance	Per App Service for App Service Environment instance

Next

Create Logic App (Multi-tenant)

Basics Top 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 workflow 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 * Resource Group * Create new

Instance Details

Logic App name * Region *

Enable log analytics * Yes No

Looking for the classic consumption create experience? [Click here](#)

Review + create < Previous Next > Tags

InsightScape LogicApp

Overview

Search Run Refresh Edit Delete Disable Open in mobile Export Provide feedback

Essentials

Resource group <input type="text" value="InsightScape-RG"/>	Location <input type="text" value="West US 2"/>	Definition <input type="text" value="0 triggers, 0 actions"/>
Subscription <input type="text" value="free trial"/>	Status <input type="text" value="Enabled"/>	Runs last 24 hours <input type="text" value="0 successful, 0 failed"/>
Workflow URL <input type="text" value="https://azurelogicapp-00000000000000000000000000000000.logic.azure.com:443/InsightScape-LogicApp?%7B%7D"/>	Integration Account <input type="text" value=""/>	
Tags <input type="text" value=""/>	Add tags	

Get started Run history Trigger history Metrics

Recent Specify the run identifier to open monitor view directly

Identifier	Status	Start time (Local Time)	Duration	Static results
Showing 0 runs				

Microsoft Azure Upgrade

Home > Microsoft Web App Consumption Plan-55c05f51-a0ef | Overview > InsightScape-LogicApp

InsightScape LogicApp | Logic app designer

Log app

Search Save Discard Parameters Code view Errors Info File a bug Enable Legacy Designer

Add a trigger

App

Runtime Select a runtime Action type Trigger

Group by Connector

Load more results...

When a blob is added or modified (properties only) (V2)

When a post is created

Create Webhook subscription

See more

Add a trigger

The screenshot shows the Logic App designer interface. On the left, there's a navigation sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Logic app designer (which is selected), Logic app code view, Run history, Versions, API connections, Quick start guides, Settings, Monitoring, Automation, and Help. The main area is titled 'Add a trigger' and lists several triggers from different connectors: 'When a blob is added or modified (properties only) (V2)', 'When a post is created', and 'Create Webhook subscription'. There are also sections for 'See more' and 'Loading more results...'. At the bottom left, there are icons for '+' (New), '...', and 'O'.

Microsoft Azure Upgrade

Home > inscapescapestorage

inscapescapestorage | Access keys

Storage account

Search 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

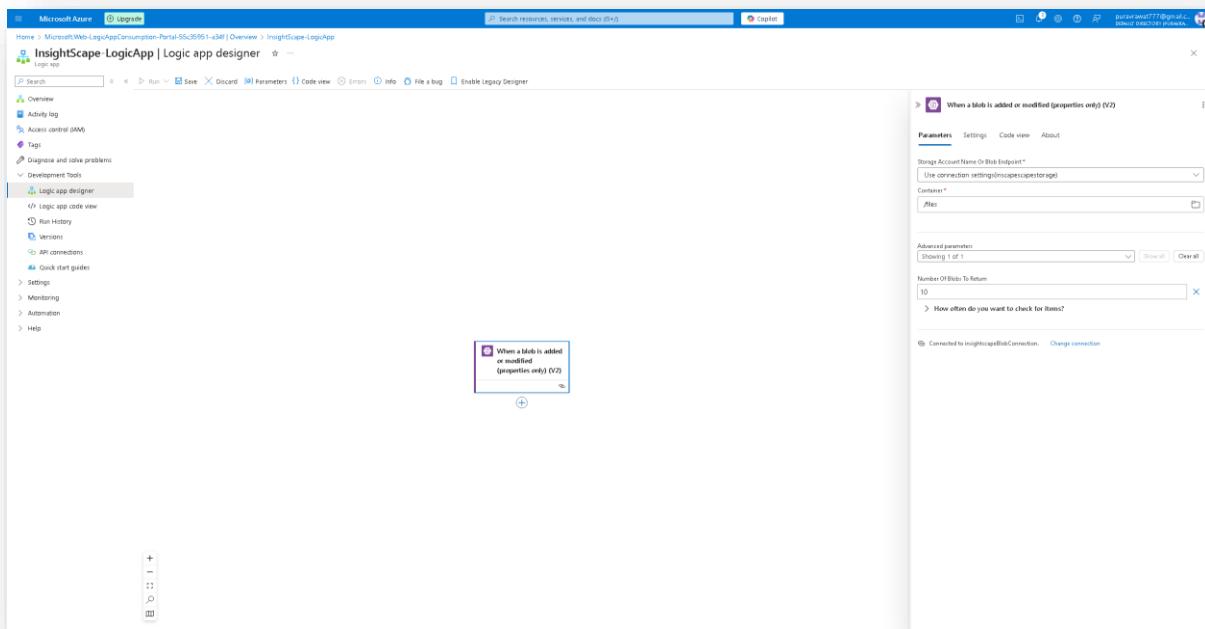
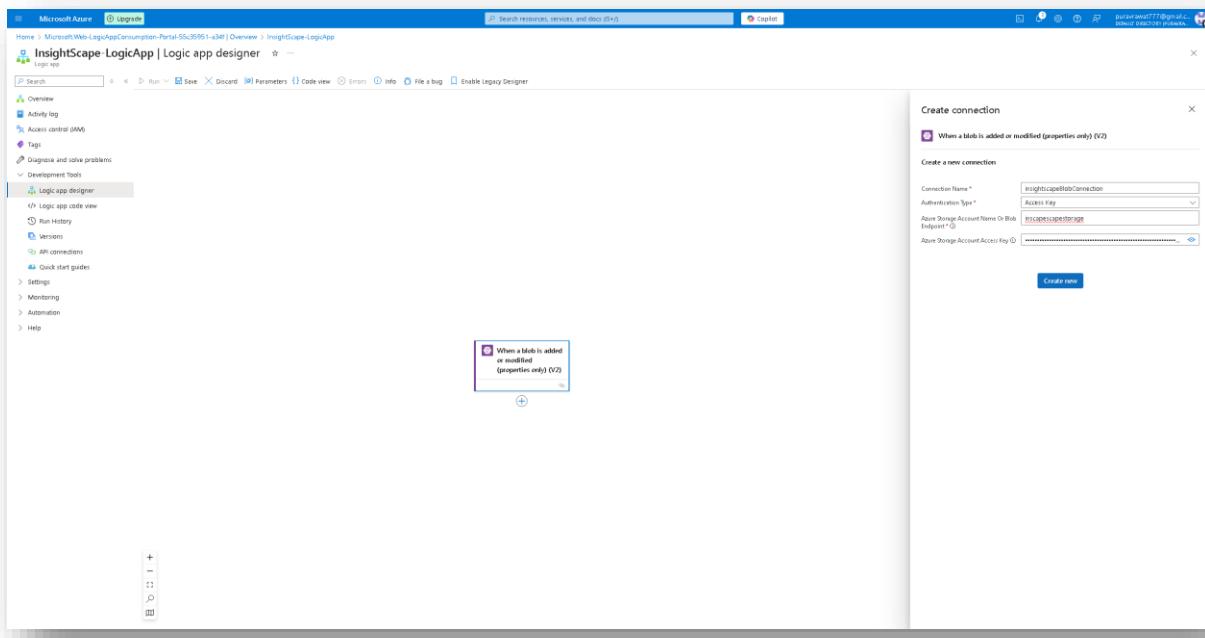
Storage account name: inscapescapestorage

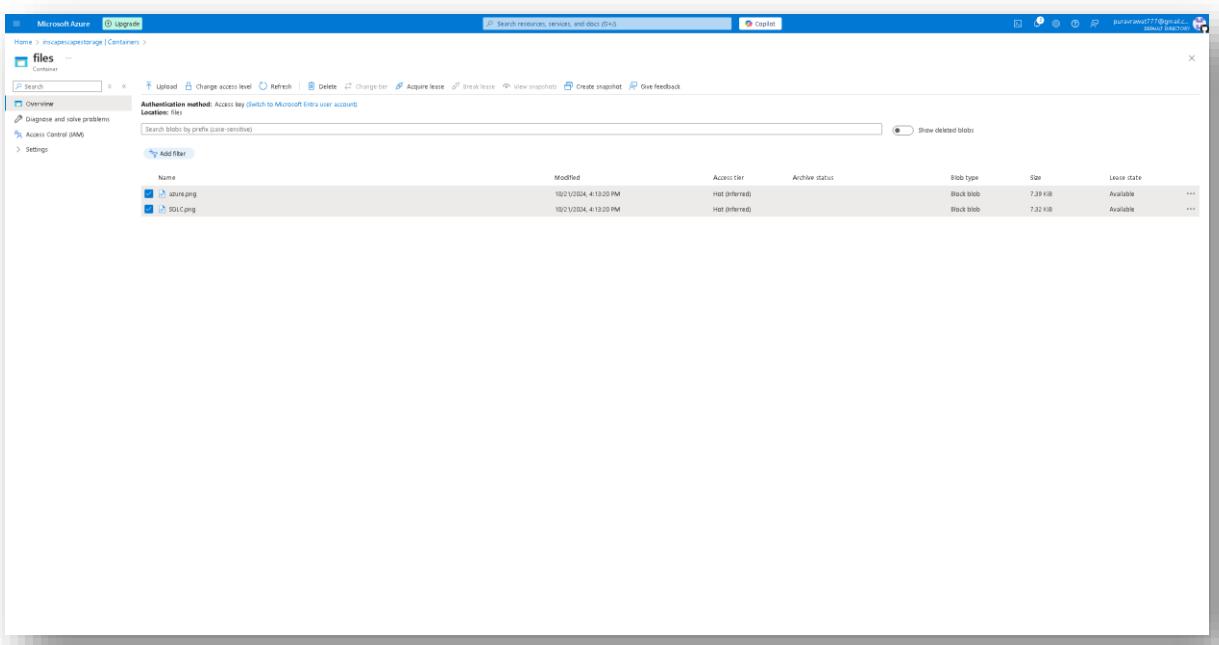
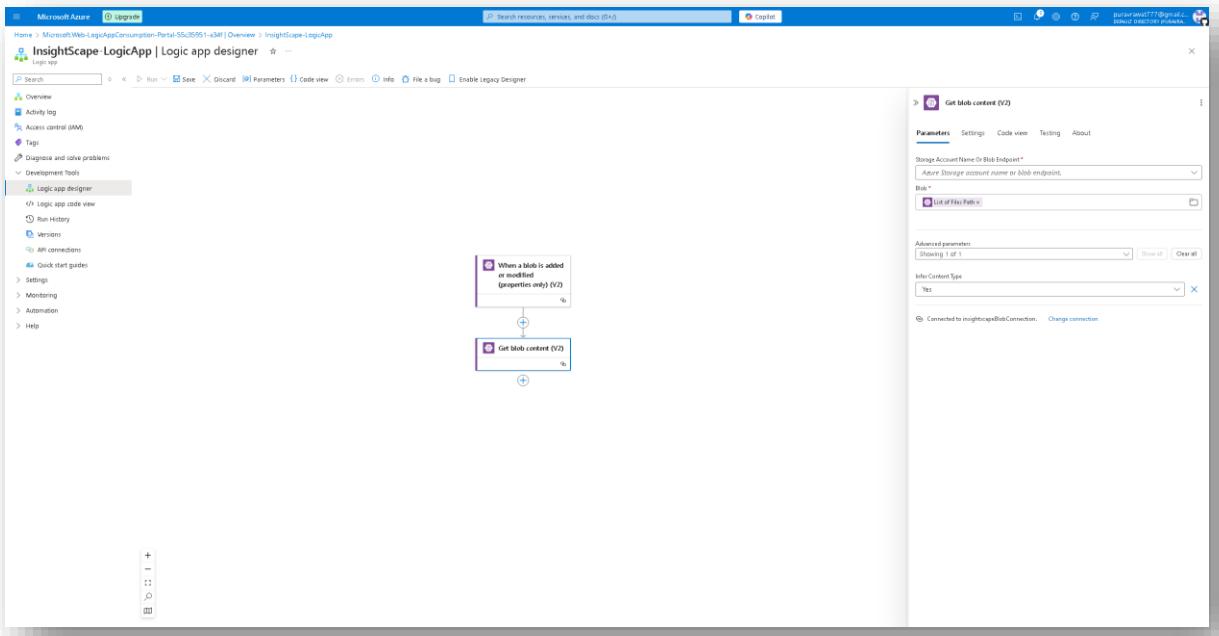
key1 Rotate key
Last rotated: 10/21/2024 (0 days ago)
Key: [REDACTED] Show
Connection string: [REDACTED] Show

key2 Rotate key
Last rotated: 10/21/2024 (0 days ago)
Key: [REDACTED] Show
Connection string: [REDACTED] Show

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

The screenshot shows the 'Access keys' page for the 'inscapescapestorage' storage account. It displays two sets of access keys: 'key1' and 'key2'. Both keys were last rotated on 10/21/2024. Each key has a 'Show' button next to its value. Below each key, there is a 'Connection string' field with a 'Show' button. The left sidebar contains links for 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 (which is selected), Shared access signature, Encryption, Microsoft Defender for Cloud, Data management, Settings, Monitoring, Monitoring (classic), Automation, and Help.





Microsoft Azure | LogicApp

Home > Microsoft Web LogicAppConsumption-Portal-5535951-a34f | Overview > InsightScape-LogicApp

InsightScape-LogicApp | Run History

Log 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	Durian	Static Results
Succeeded	10/21/2024, 4:14 PM	065472099385796752004719419C04	274 Milliseconds	
Succeeded	10/21/2024, 4:14 PM	0654720993857967521048719419C09	209 Milliseconds	

Microsoft Azure | LogicApp

Home > Microsoft Web LogicAppConsumption-Portal-5535951-a34f | Overview > InsightScape-LogicApp | Run History

InsightScape-LogicApp | Run History

Log app

Search | Refresh

Run Details | Resubmit | Cancel Run | Refresh | 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

Start time Duration

10/21/2024, 4:14 PM 274 Milliseconds

10/21/2024, 4:14 PM 209 Milliseconds

Get blob content (V2) | Submit from this action

Parameters | Settings | Code view | About

Use connection settings(Inspectsappteststorage)

blob

/Hiles/feature.png

Show more

OUTPUTS

statusCode: 200

headers:

```

    "X-Content-Type-Options": "nosniff",
    "X-Frame-Options": "SAMEORIGIN",
    "X-Request-Id": "00000000-0000-0000-0000-000000000000",
    "X-Ms-ApiHub-Cached-Response": "true",
    "X-Ms-ApiHub-Obso": "false",
    "Date": "Tue, 21 Oct 2024 10:14:59 GMT",
    "Content-Length": "7906",
    "Content-Type": "image/png",
    "Expires": "-1"
  
```

body:

```

  {
    "response-type": "image/png",
    "content": "data:image/png;base64, iVBORw0KGgoAAAQABAAQDQABgAIAACXQWABTUVVWDX//Bsc73/... "
  }
  
```

PROPERTIES

Start time: 10/21/2024, 4:14:59 PM (Local time)

End time: 10/21/2024, 4:14:59 PM (Local time)

Status: Succeeded

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-to-VM2-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 –

This screenshot shows the Microsoft Azure portal homepage. At the top, there's a banner with a welcome message: "Hi Purav, see what more you can do" followed by links to "View running code" and "Learn how to code". Below the banner, there's a "Take a free online course on Microsoft Learn" button. The main navigation bar includes "All Services (60)", "Documentation (99+)", and a "More (4)" dropdown. The "Azure services" section lists "Create a resource", "Logic apps", and "App Service". The "Resources" section shows a table of recent resources, including "insightscope-azapp", "insightscope-400", "insightscope-500", "insightscope-storage", "insightscope-vm10", "insightscope-VM100", "insightscope-VM2", "insightscope-VM3", "insightscope-VM4", and "Free trial". The "Explore support resources" section features a "Continue searching in Microsoft Extras ID" button. The bottom of the page has a "Navigate" section with links to "Subscriptions", "Resource groups", "All resources", and "Dashboard".

This screenshot shows the "Network Watcher" blade in the Microsoft Azure portal. The top navigation bar includes "Create", "Manage view", "Refresh", "Export to CSV", "Open query", "Assign tags", and "Disable". There are filters for "Subscription equals all", "Resource group equals all", and "Location equals all". The main area displays a table with one record: "Name": "NetworkWatcher-website2", "Subscription": "74", "Location": "West US 2", and "Free trial". The bottom of the page includes a "Page 1 of 1" navigation indicator and a "Give feedback" link.

Microsoft Azure (0) Upgrade

Home > Network Watcher

NetworkWatcher_westus2

Resource Overview

Essentials

- Resource group: NetworkWatcherRG
- Location (map): West US 2
- Subscription: free trial
- Subscription ID: dfe3d784-6d1b-4d88-9310-d38a0ebe450
- Tags: Add tags

Activity log

Access control (IAM)

Tags

Settings

Monitoring

Automation

Help

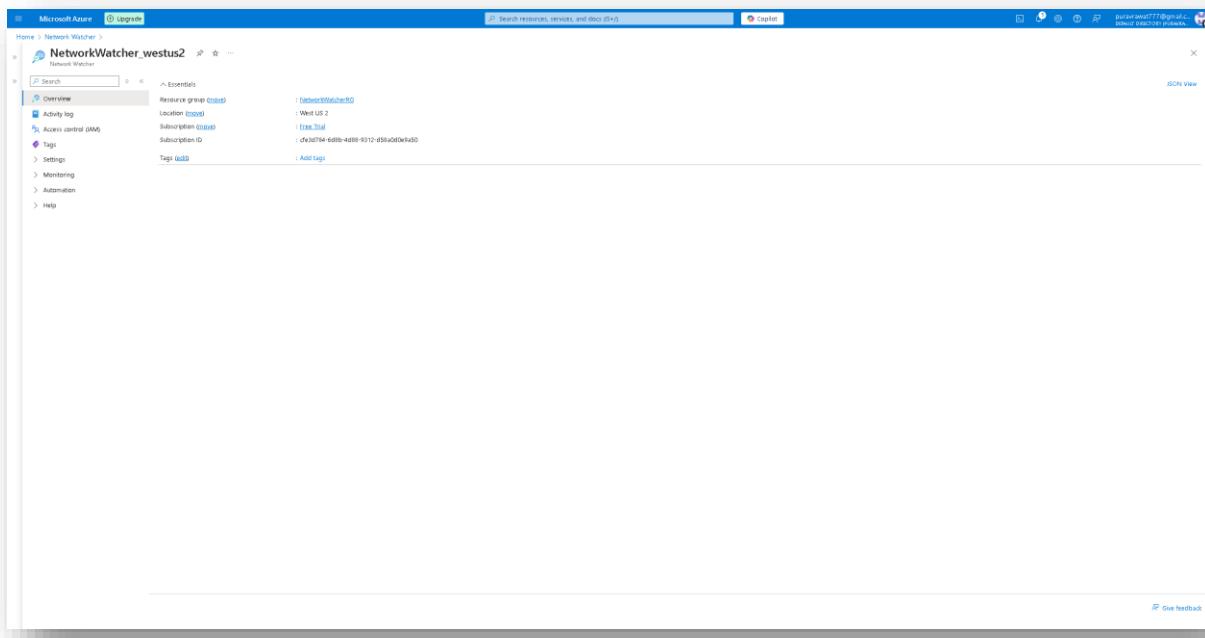
Search

Search resources, services, and docs (S+Q)

Copy

JSON View

Give feedback



Microsoft Azure (0) Upgrade

Home > Network Watcher

Network Watcher | Packet capture

Microsoft

Overview

Add Refresh

Get started

Monitoring

Network diagnostic tools

- IP flow verify
- NDIS diagnostics
- Net hop
 - Effective security rules
- VPN troubleshooting
- Packet capture
- Connection troubleshooting

Metric

Logs

Filter by name or target

Name	Target	Status	Start time	Storage
No results.				

Subscription: All subscriptions

Add packet capture

Add packet capture

Basic details

Subscription: free trial

Resource group: InsightScope-RG

Target type: Virtual machine

Target instance: InsightScope-VM

Packet capture name: InsightScope-VM_Capture

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

Storage accounts: insightscopestorage

Maximum bytes per packet: default: 0 (entire packet)

Maximum bytes per session: default: 10241624

Time limit (seconds): 100

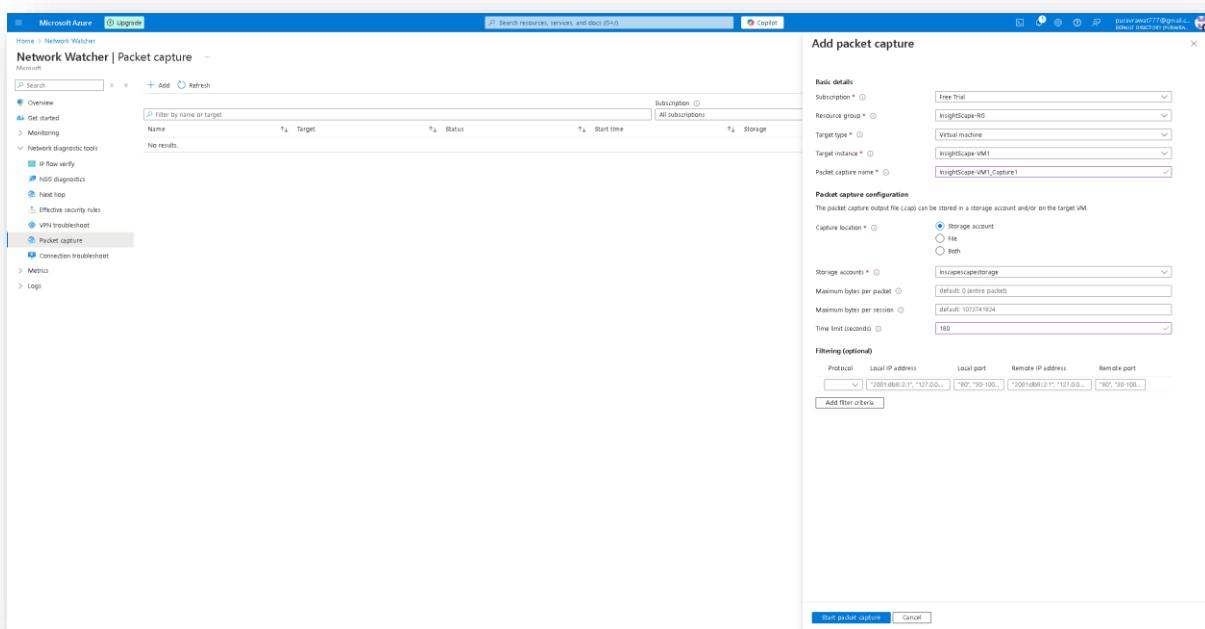
Filtrering (optional)

Protocol: Local IP address: *10.0.0.1*, Remote IP address: *10.0.0.1*

Local port: *1024-65535*, Remote port: *1024-65535*

Add filter criteria

Start packet capture Cancel



Microsoft Azure (Upgrade)

Home > Network Watcher

Network Watcher | Packet capture

Overview

Get started

Monitoring

- Network diagnostic tools
 - IP flow verify
 - NDS diagnostics
 - Next hop
 - Effective security rules
 - VPN troubleshooting
 - Packet capture
- Metric
- Logs
 - Flow logs
 - Migrate flow logs
 - Diagnostic logs
- Connection troubleshooting

Search + Add Refresh

Filter by name or target:

Name	Target	Status	Start time	Storage	Bytes per packet	Bytes per session	...
InsightScope-VM1_Capture1	InsightScope-VM1	Running	10/21/2024, 4:23:02 PM	inscapescapestorage	Entire packet (default)	1073741824	...

Subscription: All subscriptions

Details

Status: Details

Session status: Running

Storage location: packetcapture_10_32_e7_0111.cap

Start time: -

Errors: -

Microsoft Azure (Upgrade)

Home > inscapescapestorage

inscapescapestorage | Containers

Storage account

Overview

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
 - Frost 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:

Name	Last modified	Anonymous access level	Lease state	...
Logs	10/21/2024, 3:52:26 PM	Private	Available	...
File	10/21/2024, 3:54:56 PM	Private	Available	...
network-watcher-logs	10/21/2024, 4:22:54 PM	Private	Available	...

Show deleted containers

Microsoft Azure | Log In

Home > insightscapestorage | Containers > network-watcher-logs

Container

Search Upload Change access level Refresh Delete Change tier Acquire lease Break lease View snapshots Create snapshot Give feedback

Overview

Authentication method: Access key (Switch to Microsoft Entra user account)

Location: network-watcher-logs / insightscape-rg / 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	Last modified	...
<input type="checkbox"/>  packetcapture_10_32_47_001.cap	10/21/2024, 4:29:09 PM			Append blob	226.79 kB	Available	...

Microsoft Azure | Log In

Home > insightscapestorage | Containers > network-watcher-logs

Container

Search Upload Change access level Refresh Delete Change tier Acquire lease Break lease Give feedback

Overview

Authentication method: Access key (Switch to Microsoft Entra user account)

Location: network-watcher-logs / insightscape-rg / 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	Last modified	...
<input type="checkbox"/>  packetcapture_10_32_47_001.cap	10/21/2024, 4:29:09 PM			Append blob	226.79 kB	Available	...

Blob

Overview Versions Snapshots Edit Generate SAS

Properties

URL: <https://insightscapeprod...>

LAST MODIFIED: 10/21/2024, 4:29:09 PM

CREATION TIME: 10/21/2024, 4:25:09 PM

VERSION ID:

TYPE: Append Blob

SIZE: 226.79 kB

ACCESS TIER: N/A

ACCESS TIER LAST MODIFIED: N/A

ARCHIVE STATUS: N/A

REGRAGATE PRIORITY: -

SERVER ENCRYPTED: true

ETAG: d8d0f18d411821e

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: -

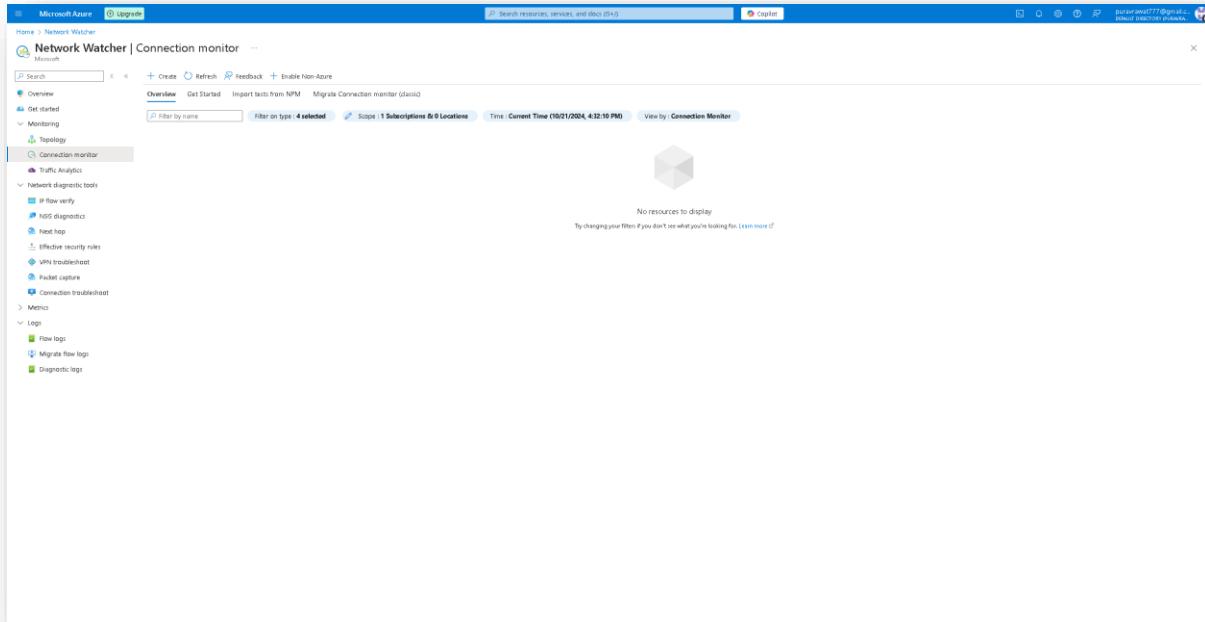
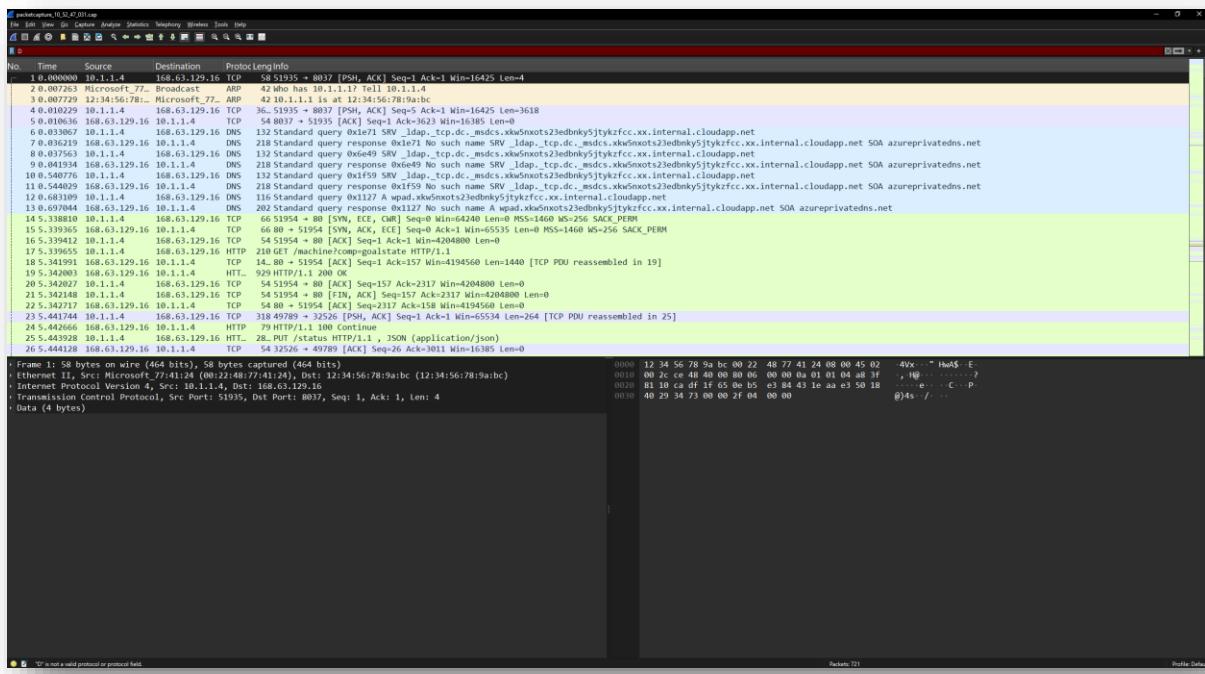
COPY COMPLETION TIME: -

Metadata

Key	Value

Blob index tags

Key	Value



Create 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-Monitor

Sources: 0 items

Test configurations: 0 items

No test group available. Click on Add test group for adding test groups to connection monitor.

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 **Subscription:** InsightScope RG **Resource group:** InsightScope-RG **Region:** West US 2 **Type:** Virtual Machines **Filter by name:**

Selected sources (1 Azure endpoint)

Add endpoints | **Cancel**

Create 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-Monitor

Sources: 1 item

Test configurations: 0 items

No test group available. Click on Add test group for adding test groups to connection monitor.

Add resources

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 Destinations

Azure endpoints **Subscription:** InsightScope RG **Resource group:** InsightScope-RG **Region:** West US 2 **Type:** Virtual Machines **Filter by name:**

Selected destinations (1 Azure endpoint)

Add endpoints | **Cancel**

Create Connection... > 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.

Sources: VM1-Subnet1(NgScape-RG)
Subscription: Free Trial
Resource group: NgScape-RG
Edit

Test configurations: VM1-to-VM2-TestConfig

Test group name: VM1-to-VM2-TestGrp

Extension status: Enabled

Test Frequency: Every 30 seconds

Success threshold: Checks failed (avg): 30
Round trip time (ms): 300

Add Test configuration:

Add sources:

Add destinations:

Add Test configuration:

Add Test Group: Add Test Group | Cancel

Add Test configuration: Add Test configuration | Cancel

Create Connection... > 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.

Sources: VM1-Subnet1(NgScape-RG)
Subscription: Free Trial
Resource group: NgScape-RG
Edit

Test configurations: VM1-to-VM2-TestConfig

Destinations: VM2-Subnet1(NgScape-RG)
Subscription: Free Trial
Resource group: NgScape-RG
Edit

Extension status: Enabled

Add sources:

Add destinations:

Add Test configuration:

Add Test Group: Add Test Group | Cancel

Add Test configuration: Add Test configuration | Cancel

Create Connection Monitor

This Connection Monitor's estimated monthly cost is \$0 [Learn more](#)

Primary details

Connection Monitor Name : VM1-to-VM2-Monitor
Subscription : Free Trial
Region : West US 2

Status : Enabled
Workspace : DefaultWorkspace-ef3d794-6dbb-4db9-9112-d9f8a0e4d0-9452

Test groups (0)

Name	Sources	Destinations	Test Configurations	Current Cost/Month	Estimated Cost/Month	Status	Extension Status
VM1-to-VM2-TestGroup	VM1-Subnet(mgmtCape-RG)	VM2-Subnet(mgmtCape RG)	VM1-to-VM2-TestConfig	\$0	\$0	Enabled	All Enabled

[Create](#) [Cancel](#) [Download template](#)

Network Watcher | Connection monitor

Ready-made Connection Monitors may take 5-10 minutes to get monitoring data and show up in the dashboard. Connection monitor (classic) / Network Performance Monitor (NPM) is no longer in service. Please migrate your existing tests to the new Connection monitor as soon as possible.

Overview [Get Started](#) [Import tests from NPM](#) [Migrate Connection monitor \(classic\)](#)

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

Protocol	Alerts	Status	Reason	Last polled	...
VM1-to-VM2-Monitor	0	Green	-	10/21/2024 4:39:29 PM	...

Microsoft Azure Upgrade

Home Network Watcher | Connection monitor

Network Watcher | Connection monitor

VM1-to-VM2-Monitor

Overview Get Started Overview Connection Monitor VM1-to-VM2-Monitor

Search

Overview Refresh ...

Essentials

Resource group: networkwatcher

Status: Normal

Location: West US 2

Subscription: Free Trial

Subscription ID: 00000000-0000-0000-0000-000000000000

Tags: None

Summary Test groups Sources Destinations Test Configurations Issues

Aggregated performance metrics

Checks failed (%)

Round trip time (ms)

Time Interval: 10/21/24, 09:40 PM - 10/21/24, 06:40 PM

Metrics

Logs

Flow logs

Migrate flow logs

Diagnostic logs

Top failing tests

Test Configurations

Sources

Test groups

Time Interval: 10/21/24, 09:40 PM - 10/21/24, 06:40 PM

JSON View

Workshop: [DefaultWorkshop](#) (Created by: [Network Watcher](#))

Resource ID: /subscriptions/cf0d6f14-40ff-9312-0301-000000000000/resourceGroups/networkWatchers/providers/Microsoft.Network/networkWatchers

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.

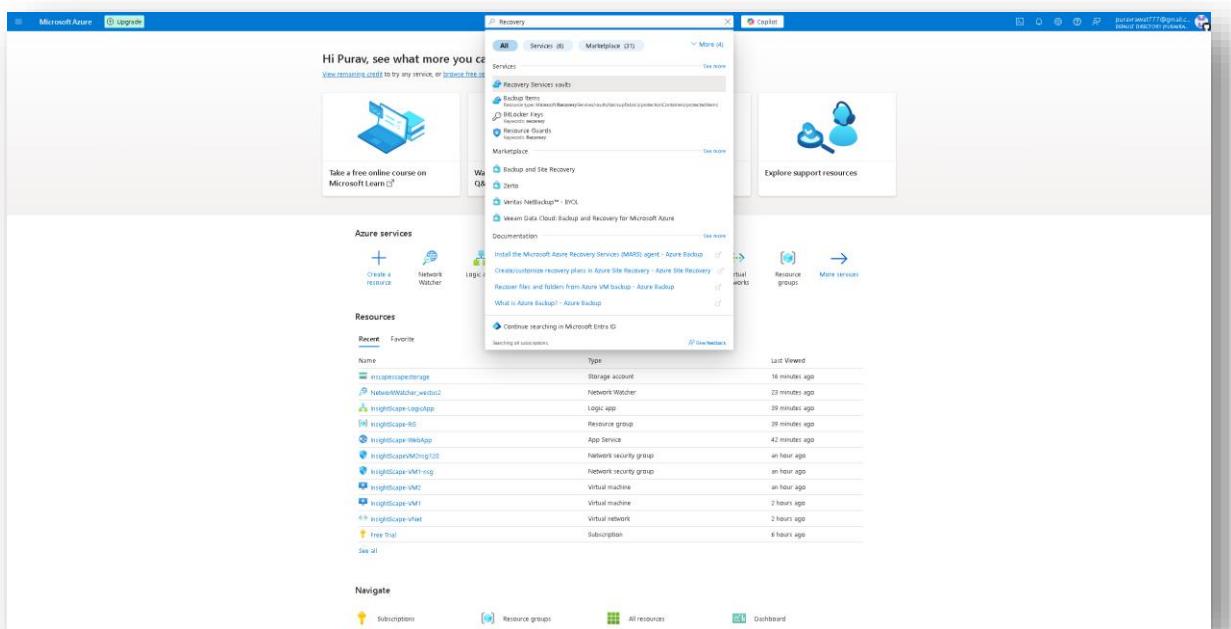
5. Backup Jobs Verification:

- 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

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 * InsightScope-RG Create new

Instance Details
Vault name * InsightScope-Vault

Region * West US 2

Cross Subscription Restore is enabled by default for all vaults. Visit vault 'Properties' to disable the name. [Learn more](#).

Review + create Next: Redundancy API Feedback

Microsoft Azure Upgrade

Home > Recovery Services vaults > Create Recovery Services vault

Basics Redundancy Encryption Vault properties Networking Tags Review + create

Summary

Basics

Subscription	Free Trial
Resource group	InsightScope-RG
Vault name	InsightScope-Vault
Region	West US 2

Redundancy

Blob Storage Redundancy	Geo-redundant
Cross Region Restore	Enabled

Vault properties

Immutability	Disabled
--------------	----------

Networking

Connectivity method	Allow public access from all networks
---------------------	---------------------------------------

Create Previous: Tags API Feedback Download a template for automation

Microsoft Azure | Upgrade

Home > Microsoft.RecoveryServiceV2-172950922751 | Overview > InsightScape Vault

Search resources, services, and docs (S+)

Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery.

Resource group: **InsightScape-RS**

Location: West US 2

Subscription: **East Trial**

Subscription ID: cfd2d14e-60fb-4d89-9112-d51ab0bca0

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 VM 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

Home > Microsoft.RecoveryServiceV2-172950922751 | Overview > InsightScape-Vault

Search resources, services, and docs (S+)

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 File)	0
SQL Database in Azure VM	0
SAP HANA in Azure VM	0

Microsoft Azure (Upgrade)

Home > Backup Items (Azure Virtual Machine) >

Search resources, services, and docs (S+)

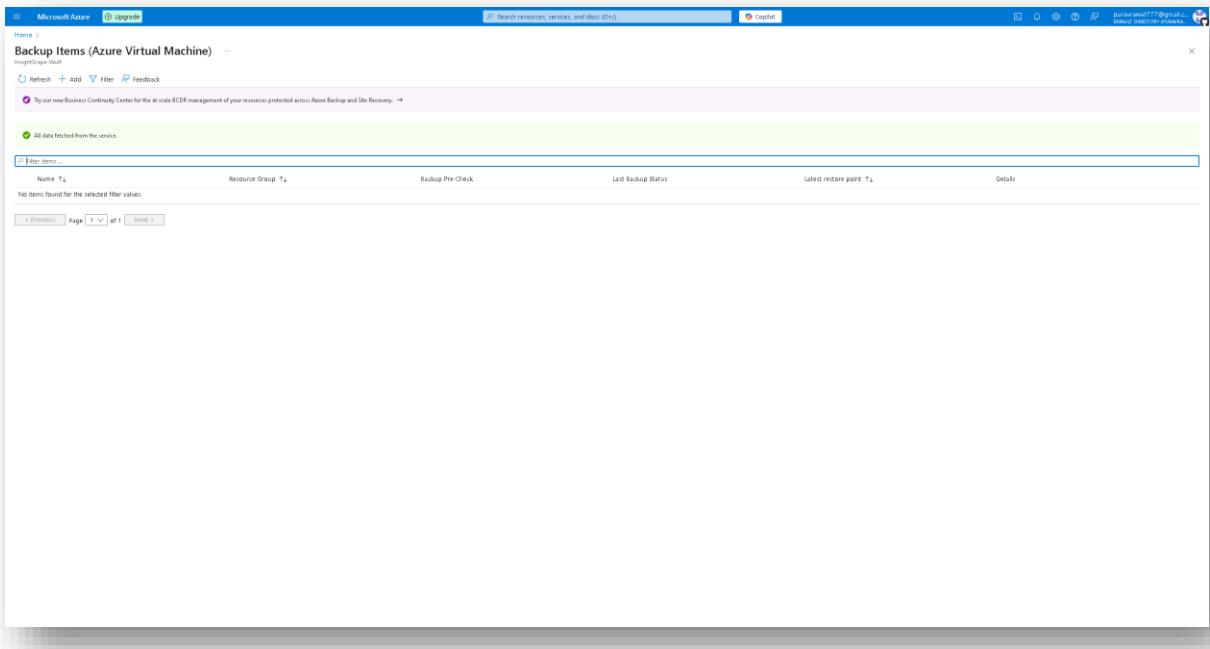
Try our new Business Continuity Center for the at-scale BCR management of your resources protected across Azure Backup and Site Recovery. →

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.					

Page 1 of 1 Next >



Microsoft Azure (Upgrade)

Home > Backup Items (Azure Virtual Machine) > Backup Goal

Search resources, services, and docs (S+)

The storage replication is set to Geo-Redundant. This option cannot be changed later. Before proceeding further, click here. →

Where is your workload running?

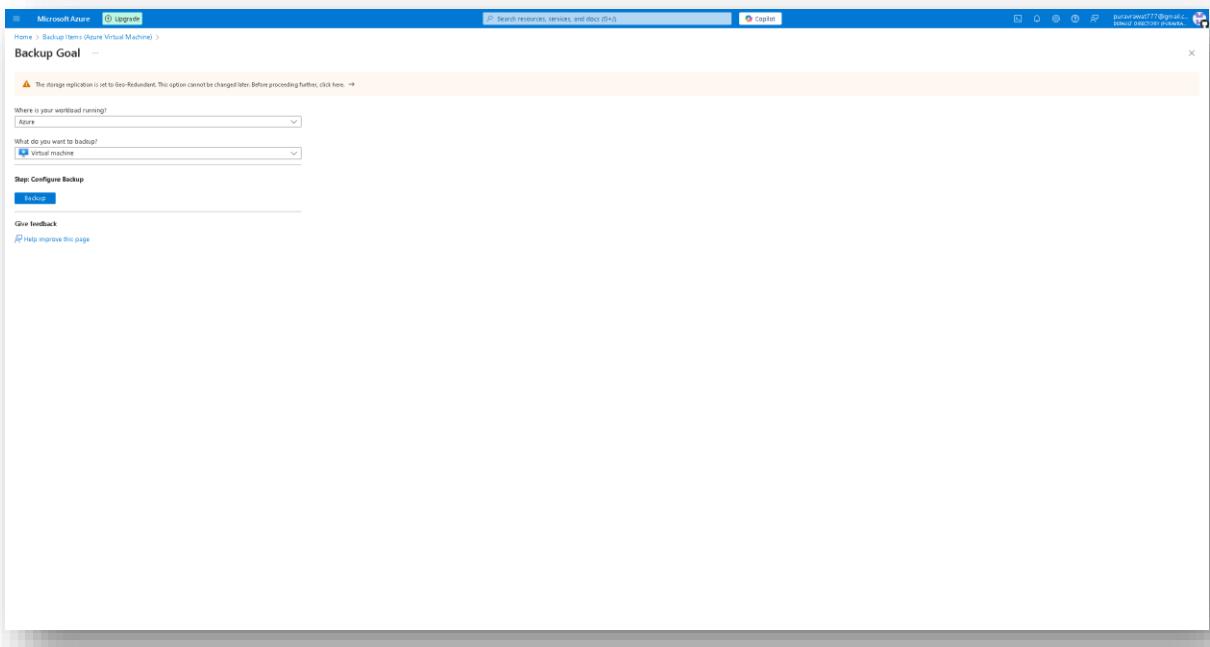
What do you want to backup? virtual machine

Step: Configure Backup

Backup

Give feedback

Help improve this page



Configure backup

Configure backup ...

InsightScope VM1

Policy sub-type *

- Enhanced
 - Multiple backups per day
 - Up to 30 days operational tier retention
 - Support for Monitor, Log Analytics and Metrics
 - 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 Recovery: Instant recovery (snapshots) for 2 days(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	Disk
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

OK Cancel Give feedback

ConfigureProtection 1729509600719 | Overview

Deployment

Search

Your deployment is complete

Deployment name: ConfigureProtection-1729509600719
Subscription: Free Trial
Resource group: InsightScope RG

Start time: 10/21/2024, 4:50:10 PM
Correlation ID: b3ea28e1-59fb-4c30-6997-fabdf51c3b6

Deployment details

Resource	Type	Status	Operation details
InsightScope Vault\Azure\kv\VMContainer\avm\vm\env\insightscope\rg\insightScope-VM\VM\vm\avm\containers\2\insightscope_rg\insightScope VM1	Backup item	OK	Operation details

Next steps

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 Log out

Home > ConfigureProtection-1729509600719 | Overview > InsightScope-Vault | Backup items > Backup Items (Azure Virtual Machine)

Backup Items (Azure Virtual Machine) ...| Insights| Log Analytics

Refresh + Add Filter Feedback

By 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
InsightScope-VM1	InsightScope-RG	Passed	Warning (Initial backup pending)		View details

< Previous Page 1 of 1 Next >

Microsoft Azure Upgrade Log out

Home > ConfigureProtection-1729509600719 | Overview > InsightScope-Vault | Backup items > Backup Items (Azure Virtual Machine) > InsightScope-VM1

Backup Items (Azure Virtual Machine) ...| Insights| Log Analytics

Backup now Restore VM File Recovery Stop backup Resume backup Delete backup data Restore to Secondary Region Undelete Feedback

By our new Business Continuity Center for the at-scale BCDR management of your resources protected across Azure Backup and Site Recovery. →

Essentials

Recovery service vault : [InsightScope-Vault](#)
Subscription ID : [\[REDACTED\]](#)
Description ID : [\[REDACTED\]](#)
Alerts in last 24 hours : [\[REDACTED\]](#)
Jobs in last 24 hours : [\[REDACTED\]](#)

Backup Pre-Check Passed
Last backup status : Warning (Initial backup pending)
Backup policy : [GetDefaultBackupPolicy](#)
Latest restore point : [\[REDACTED\]](#)
Included disks : [All disks](#)

JSON View

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 bar, click here.

Creation time ↑	Consistency	Recovery type
0	0	0

No restore points available.

Microsoft Azure Upgrade

Home > ConfigureProtection-1779079602719 | Overview > InsightScape-Vault | Backup items > Backup items (Azure Virtual Machine)

InsightScape VM1

Restore 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

Recovery service vault : [InsightScape-Vault](#)
Subscription [Subscription](#) [Free Trial](#)
Subscription ID : [c9d1f194-6db8-4d88-9312-d3fa3d0e9460](#)
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 disks : [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-archives, click here.
Long term recovery point can be moved to vault-archives. To move all recommended recovery points to vault-archives set, click here.

Creation time	Consistency	Recovery type
0	0	0

Creation time ↑ Consistency Recovery type

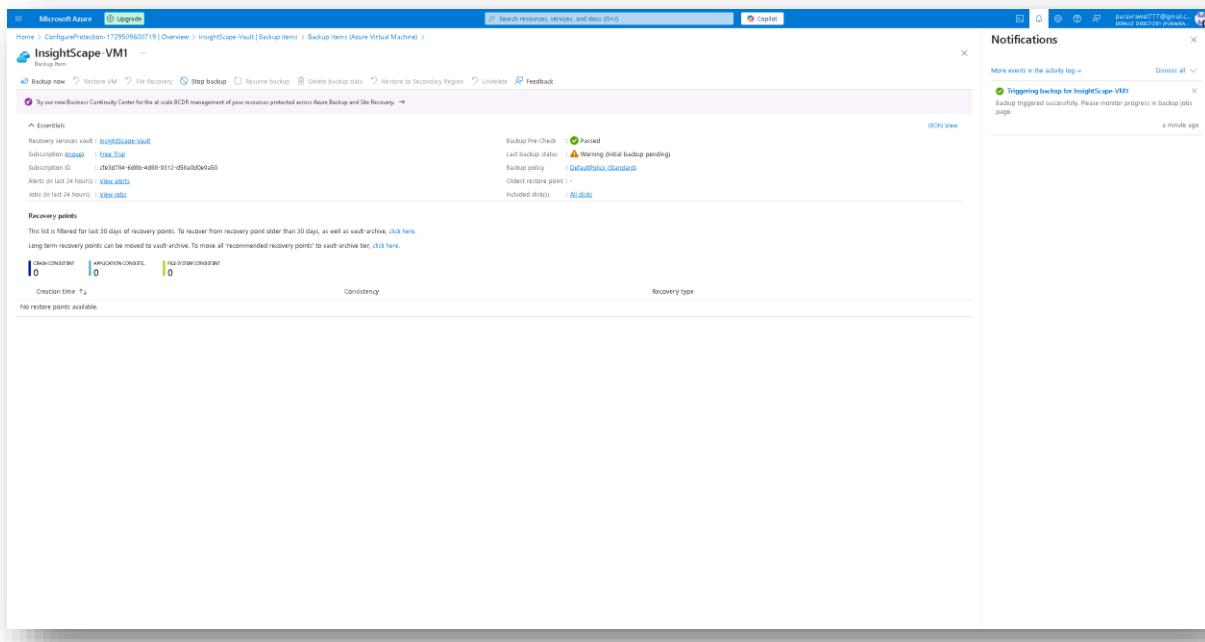
No restore points available.

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

Home > Recovery Services vaults > InsightScape-Vault

InsightScape Vault | Backup Jobs ...

Create Manage view ...

Search Choose columns Filter Export jobs Refresh Feedback

Filtered by: Item Type - All, Operation - All, Status - All, Start Time - 10/21/2024, 0:00:00 PM, End Time - 10/21/2024, 6:58:04 PM

Try our new Business Continuity Center for the at-scale BCDR management of your resources protected across Azure Backup and Site Recovery.

Protected 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	00:41:01	View details
InsightScape-VM1	Configure backup	Completed	Azure Virtual Machine	10/21/2024, 4:50:12 PM	00:00:00	View details

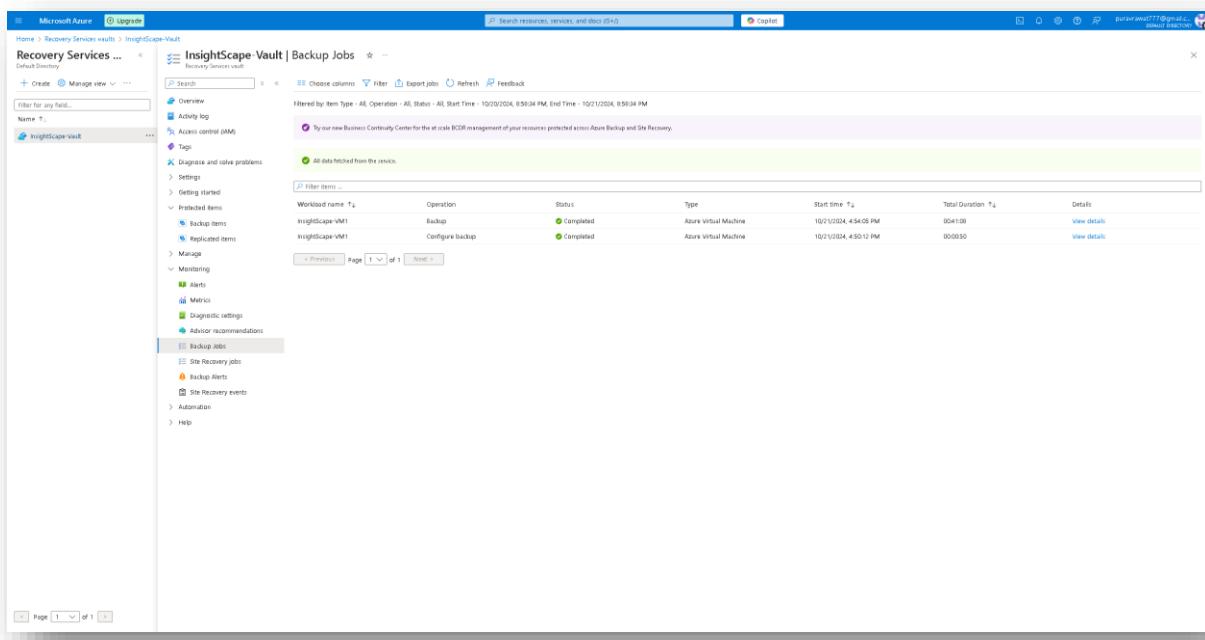
Manage

- Monitoring
 - Alerts
 - Metrics
 - Diagnostic settings
 - Advisor recommendations
- Backup jobs
- Site Recovery jobs
- Backup Alerts
- Site Recovery events

Automation

Help

Page 1 of 1



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: CPUUsageAlert
 - 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 CPUUsageAlert 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-

The screenshot shows the Microsoft Azure Monitor homepage. At the top, there's a search bar and a 'Monitor' button. Below the search bar, a message says 'Hi Purav, see what more you can do with Azure Monitor'. It includes a link to 'www.microsoft.com' and a 'Learn more' button. To the right, there are sections for 'Services (17)', 'Marketplace (0)', and a 'More (4)' dropdown. A 'Services' sidebar lists 'Azure Native New Relic Service', 'Azure Monitor Workspaces', 'Azure Monitor pipelines (preview)', and 'DataCollection Rules'. A 'Documentation' sidebar provides links to 'What is Azure Monitor for SAP solutions?', 'Monitor Azure SQL Database - Azure SQL Database', 'Azure Monitor data resources and data collection methods - Azure Monitor', and 'Azure Monitor best practices: Configure data collection - Azure Monitor'. On the left, there's a 'Resources' sidebar with a 'Recent' tab showing 'InsightsLog-vault', 'InsightsLog-RS', 'InsightsLogStorage', and 'NetworkWatcher-vnet2'. Other tabs include 'Favorite', 'Name', 'Type', and 'Status'. Below the sidebar is a 'Create a resource' button and a 'Recovery Services vaults' section. The main content area features a 'Work & Q&A' section with a question about 'What is Azure Monitor for SAP solutions?' and a 'Explore support resources' section with icons for 'work groups', 'virtual machines', and 'More (4)'. At the bottom, there's a 'Navigate' section with a 'Last viewed' list.

This screenshot shows the 'Monitor | Virtual Machines' page under the 'Monitor' category. The left sidebar has a 'Get started' button and links for 'Overview', 'Activity log', 'Alerts', 'Metrics', 'Logs', 'Change Analysis', 'Service Health', 'Workbooks', and 'Investigator (preview)'. Under 'Insights', there's a 'Virtual Machines' section with a 'Configure Insights' button. The main content area is titled 'Monitor the health and performance of virtual machines'. It explains that VM Insights monitors the performance and health of virtual machines and virtual machine scale sets. It includes three cards: 'Enable VM Insights' (which implements complete monitoring of your Azure and hybrid virtual machine environment), 'Analyze data' (which monitors the health and performance for a single machine or multiple machines and drills into logs for troubleshooting), and 'Create alerts' (which allows Azure Monitor proactively notify you of interesting data and patterns in your monitoring data and potentially take automated actions based on triggers). There's also a 'Learn more' link for each card.

Microsoft Azure | Upgrade

Home > Monitor

Monitor | Virtual Machines

Overview Get started Overview Performance Map

Search 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 (0) Workspace configuration Other onboarding options

Name Monitor Coverage

Free Trial 2 of 2

insights-rg 2 of 2

insightscope-VM1 Not enabled Enable

insightscope-VM2 Not enabled Enable

Workspace

Get started Overview Performance Map

Search 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 (0) Workspace configuration Other onboarding options

Name Monitor Coverage

Free Trial 2 of 2

insights-rg 2 of 2

insightscope-VM1 Not enabled Enable

insightscope-VM2 Not enabled Enable

Workspace

Get started Overview Performance Map

Search 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 (0) Workspace configuration Other onboarding options

Name Monitor Coverage

Free Trial 2 of 2

insights-rg 2 of 2

insightscope-VM1 Not enabled Enable

insightscope-VM2 Not enabled Enable

Workspace

Microsoft Azure | Upgrade

Home > Monitor

Monitor | Virtual Machines

Overview Get started Overview Performance Map

Search 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 (0) Workspace configuration Other onboarding options

Name Monitor Coverage

Free Trial 2 of 2

insights-rg 2 of 2

insightscope-VM1 Not enabled Enable

insightscope-VM2 Not enabled Enable

Workspace

Get started Overview Performance Map

Search 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 (0) Workspace configuration Other onboarding options

Name Monitor Coverage

Free Trial 2 of 2

insights-rg 2 of 2

insightscope-VM1 Not enabled Enable

insightscope-VM2 Not enabled Enable

Workspace

Get started Overview Performance Map

Search 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 (0) Workspace configuration Other onboarding options

Name Monitor Coverage

Free Trial 2 of 2

insights-rg 2 of 2

insightscope-VM1 Not enabled Enable

insightscope-VM2 Not enabled Enable

Workspace

Monitoring configuration

VM Insights now supports data collection using the Azure Monitor Agent and data collection rules.

Subscription: Free Trial Data collection rule: (new) M365VM DefaultWorkspace-0x7d704-6dbb-4d88-9112-d5ba0e0e0d01 EUS

Create New

M365VM DefaultWorkspace-0x7d704-6dbb-4d88-9112-d5ba0e0e0d01 EUS

Cloud performance	Enabled
Proximity and dependencies (Map)	Disabled
Log Analytics workspace	DefaultWorkspace-0x7d704-6dbb-4d88-9112-d5ba0e0e0d01 EUS

This will also enable System Assigned Managed Identity. In addition to existing User Assigned identity. If any Note: Unless specified in the request, the machine will default to using System Assigned identity. Learn More

Configure Cancel

Microsoft Azure | Upgrade

Home > Monitor

Monitor | Virtual Machines

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 HC Service Bus (preview) Insights Hub Managed Services Settings Support + Troubleshooting

Get started Overview Performance Map

Search Filter by name... Subscription: Free Trial Resource group: All resource groups Type: All types Location: All locations Group by: Subscription, Resource group

Monitored ID: Not monitored (0) Workspace configuration Other onboarding options

Name	Monitor Coverage
Free Trial	2 of 2
insightscope-rg	2 of 2
insightscope-VM1	Not enabled <button>Enable</button>
insightscope-VM2	Not enabled <button>Enable</button>

Workspace

More events in the activity log ▾

Deployment succeeded Deployment VMInsightOnboardingDeployment-9301d90a-7abb-402f-9341bd1f to resource group 'insightscope-rg' was successful.

View details Go to resource group a minute ago

This screenshot shows the Microsoft Azure Monitor Virtual Machines overview page. The left sidebar includes links for Overview, Activity log, Alerts, Metrics, Logs, Change Analysis, Service health, Workbooks, Investigator (preview), Insights, Applications, and Virtual Machines. Under Virtual Machines, there are sub-links for Storage accounts, Containers, Networks, SQL (preview), Azure Cosmos DB, Key Vaults, Azure Cache for Redis, Azure Data Explorer Clusters, Log Analytics workspaces, Azure Stack HC, Service Bus (preview), Insights Hub, Managed Services, Settings, and Support + Troubleshooting. The main content area displays a table of monitored resources. It shows two monitored IDs: 'Free Trial' and 'insightscope-rg'. Under 'insightscope-rg', there are two virtual machines: 'insightscope-VM1' and 'insightscope-VM2'. Both VMs have 'Monitor Coverage' listed as '2 of 2'. Below the table, there is a 'Workspace' section. A notification bar at the top right indicates a deployment success message: 'Deployment VMInsightOnboardingDeployment-9301d90a-7abb-402f-9341bd1f to resource group 'insightscope-rg' was successful.' with a timestamp of 'a minute ago'.

Microsoft Azure | Upgrade

Home > Monitor

Monitor | Virtual Machines

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 HC Service Bus (preview) Insights Hub Managed Services Settings Support + Troubleshooting

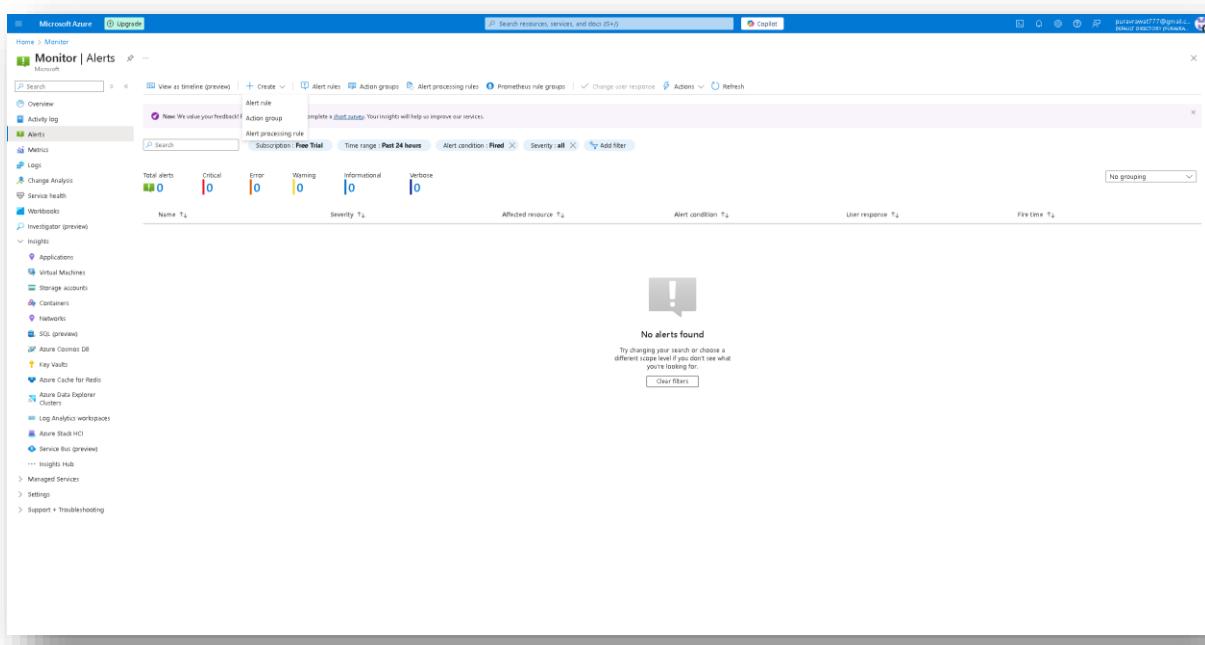
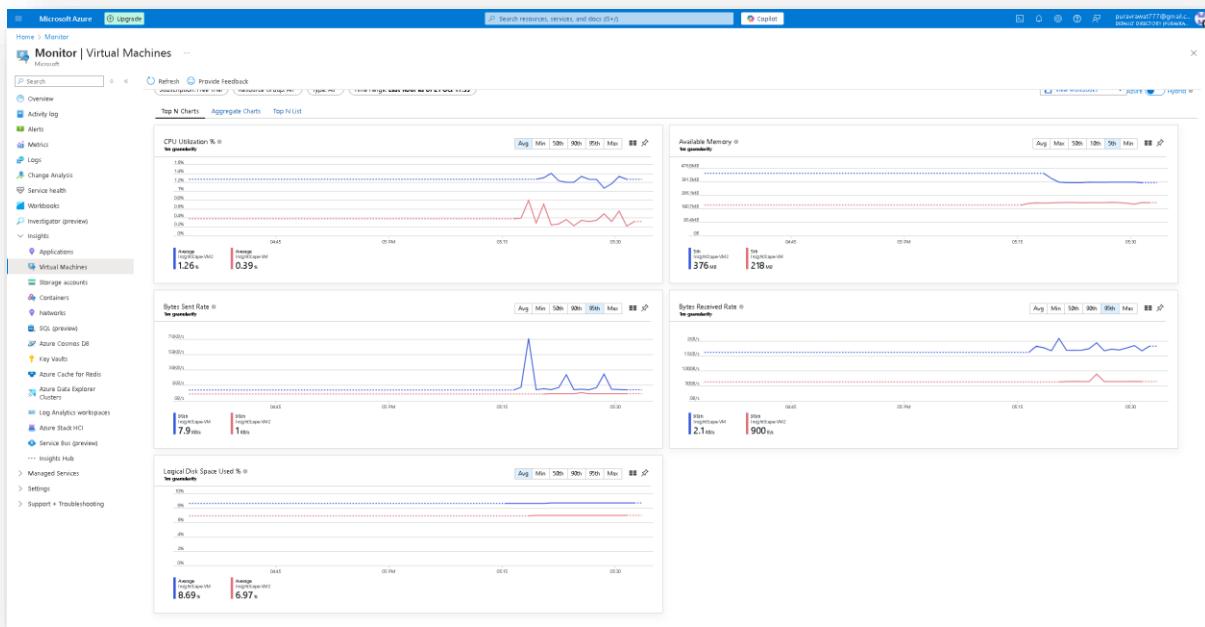
Get started Overview Performance Map

Search Filter by name... Subscription: Free Trial Resource group: All resource groups Type: All types Location: All locations Group by: Subscription, Resource group

Monitored ID: Not monitored (0) Workspace configuration Other onboarding options

Name	Monitor Coverage	Data collection rule
Free Trial	2 of 2	MSVM-DefaultWorkspace-ef367f4-e6db-4688-9312-d91a00da455-EU
insightscope-rg	2 of 2	MSVM-DefaultWorkspace-ef367f4-e6db-4688-9312-d91a00da455-EU
insightscope-VM1	Enabled	MSVM-DefaultWorkspace-ef367f4-e6db-4688-9312-d91a00da455-EU
insightscope-VM2	Enabled	MSVM-DefaultWorkspace-ef367f4-e6db-4688-9312-d91a00da455-EU

This screenshot shows the Microsoft Azure Monitor Virtual Machines overview page. The left sidebar is identical to the first screenshot. The main content area displays a table of monitored resources. It shows two monitored IDs: 'Free Trial' and 'insightscope-rg'. Under 'insightscope-rg', there are two virtual machines: 'insightscope-VM1' and 'insightscope-VM2'. Both VMs have 'Monitor Coverage' listed as '2 of 2'. Below the table, there is a 'Data collection rule' column which lists 'MSVM-DefaultWorkspace-ef367f4-e6db-4688-9312-d91a00da455-EU' for each row. This indicates that data collection rules have been successfully applied to all monitored resources.



Microsoft Azure (0) Upgrade

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

insightscapenv1 Free Trial > insightscaping X

Review + create Previous Next: Condition >

Microsoft Azure (0) Upgrade

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 inputs

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 Sum

Operator Greater than Less than

Threshold * 50 %

When to evaluate

Check every 1 minute

Lookback period 1 minute

Add condition

Review + create Previous Next: Actions >

Preview
Whenever the average Percentage CPU is greater than 50%
Time range: Over the last 6 hours Time series: Aggregate

Percentage CPU (avg), insightscapenv1: A.46%

Microsoft Azure (Upgrade)

Home > Monitor | Alerts > Create an alert rule

Scope Conditions 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 from a list of common 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](#)

Use quick actions (preview) x

Details

Action group name *

Display name *

Actions

Email

Email Azure Resource Manager Role

Azure mobile app notification

[Review + create](#) [Previous](#) [Next: Details >](#) [Save](#) [Cancel](#)

Microsoft Azure (Upgrade)

Home > Monitor | Alerts > Create an alert rule

Scope Conditions Actions Details Tags Review + create

Project details

Select the subscription and resource group in which to save the alert rule.

Subscription *

Resource group *

Alert rule details

Severity *

Alert rule name *

Alert rule description

[Advanced options](#)

[Review + create](#) [Previous](#) [Next: Tags >](#)

Microsoft Azure Logout

Home > Monitor | Alerts > Alert rules >

Alert rules

High CPU Usage Alert in VM1

Overview

Name: High CPU Usage Alert in VM1

Resource group: insightScopeRG

Location: Global

Subscription: Free Trial

Subscription ID: cfe3f784-4d8b-4d8b-9312-d95a030e9d50

Severity: 2 - Warning

Description: 1 -

Scope

Resource: insightScope-vm1

Hierarchy: insightScope-rg

Action: insightScope-WarnGrp

Actions

Name: Contains actions

1 Email

Conditions

Name: Percentage CPU > 50

Time series monitored: 1

Estimated monthly cost: \$0.10

Showing 1 - 1 of 1 results.

Give feedback

Gmail Search mail

You're now in the CPUAlert action group

Microsoft Azure <azure-receive-mail@msftncdm.com> to me 5:49 PM (3 minutes ago)

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: CFE3D784-4D8B-4D8B-9312-D95A030E9D50

Resource group name: insightScope-RG

Action group name: insightScope-WarnGrp

To unsubscribe from this action group, [click here](#).

[Privacy statement](#)
Microsoft Corporation, One Microsoft Way, Redmond, WA 9802

Reply Forward

Screenshot of the Microsoft Azure Monitor Alerts interface showing a High CPU Usage Alert in VM1.

Alert Details:

- Name:** High CPU Usage Alert in VM1
- Severity:** Warning
- Affected resource:** insightscape-vm1
- Alert condition:** Fired

Why did this alert fire?

The average Percentage CPU crossed the threshold of 50% and reached 75%. Value (after alert fired): 75%, Threshold: 50%, Deviation: 25%

Graph:

Additional details:

Screenshot of an email from Microsoft Azure sent to the user, detailing the fired alert.

Subject: 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

From: Microsoft Azure <azure-receive-mail@microsoft.com>

Body:

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 >](#)

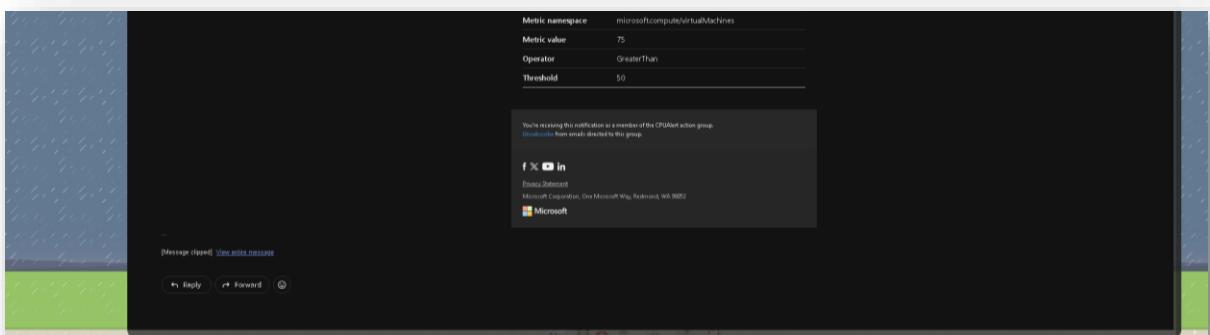
Summary

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
Fire time	October 21, 2024 12:26 UTC
Alert ID	52b9e34b-799c-4217-b076-220006fb0000
Alert rule ID	https://portal.azure.com/#Resource/subscriptions/cfe3d794-6d9b-4e88-9512-d5bafabfa500/resourceGroups/insightscape-rg/providers/microsoft.insights/metricAlerts/highCPUUsageAlertInVM1

Metric alert condition type: MultipleResourceMultipleMetricCriteria

Time aggregation: Average

Metric name: Percentage CPU



The screenshot shows the Microsoft Azure App Services blade for the "InsightScape-WebApp". The left sidebar lists various service categories like Deployment, Settings, Performance, etc. The main content area displays the following details for the Web app:

- Essentials**: Resource group (insightScape-01), Status (Running), Location (Central), Subscription (free Trial), Subscription ID (c9b3f7d4-4dbb-4bb9-9312-d51a0e9a00).
- Tags**: None.
- Properties**: Name (InsightScape-WebApp), Publishing model (Code), Runtime Stack (DotNet - v4.0).
- Domains**: Default domain (insightscape-webapp-hc5pebgzg1d1), Custom domain (Add custom domain).
- Hosting**: Plan type (App Service plan), Name (ASP-InsightScape01-911), Operating System (Windows), Instance Count (0), SKU and size (Free f1 (1) Scale Up).
- Deployment Center**: Deployment logs (View logs), Last deployment (Successful on Monday, October 21, 04:40:05 PM (Refresh)), Deployment provider (GitHub).
- Application Insights**: Name (InsightScape-WebApp), Region (Canada Central).
- Networking**: Virtual IP address (204.120.204.2), Outbound IP addresses (4.174.252.173.174.174.174.174.252...), Additional Outbound IP addresses (4.174.252.173.174.174.174.174.252...), Virtual network integration (Not supported).

Microsoft Azure (Upgrade)

Home > Monitor

Monitor | Applications

Search + Create Manage view Refresh Export to CSV Open query Assign tags Delete

Overview Activity log Alerts Metrics Logs Change Analysis Service health Webhooks 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 HC Service Bus (preview) ... Insights Hub Managed Services Settings Support + Troubleshooting

Name: InsightScape-WebApp

Resource group: InsightScape-RG Location: Canada Central Subscription: Free Trial

No grouping List view

Show 1 of 1 records.

Page 1 of 1 Next

Provide feedback

This screenshot shows the Microsoft Azure Monitor Applications interface. It displays a single application named 'InsightScape-WebApp'. The application is associated with a resource group 'InsightScape-RG', located in 'Canada Central', and is part of a 'Free Trial' subscription. The interface includes a sidebar with various monitoring options like Activity log, Metrics, Logs, and Change Analysis. A search bar at the top allows filtering by name, subscription, resource group, and location. The main content area shows basic details about the application and its deployment environment.

Microsoft Azure (Upgrade)

Home > Application Insights

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 Monitor Usage Configure Settings Help

Instrumentation key: 257000-e94e-495-be44-809e01189f1 Connection String: InstrumentationKey=257000-e94e-495-be44-809e01189f1; ingestionEndpoint=https://canadacentral1.applicationinsights.azure.com/collect/ingest; https://

Subscription: Free Trial Subscription ID: dfa5d14e-6d8b-4d8b-9112-d9aabb0e4a50 Tags:

Show data for last: 1 minute 1 hour 6 hours 12 hours 1 day 3 days 7 days 20 days

Failed requests Server response time Server requests Availability

Last Period: 2023-08-01T00:00:00 UTC+00:00

Failed requests (Count), insightscope-webapp

Server response time (Avg), insightscope-webapp

Server requests (Count), insightscope-webapp

Availability (Avg), insightscope-webapp

JSON View

This screenshot shows the Microsoft Azure Application Insights dashboard for the 'InsightScape WebApp'. The dashboard provides real-time monitoring data across four main metrics: Failed requests, Server response time, Server requests, and Availability. Each metric is represented by a line chart showing data over the last 20 days. The 'Failed requests' chart shows a count of 0. The 'Server response time' chart shows an average of 40ms. The 'Server requests' chart shows a count of 0. The 'Availability' chart shows an availability percentage of 100%. The interface also displays the instrumentation key, connection string, and subscription information for the application.

Microsoft Azure | LogicApp

Home > Logic apps > InsightScape-LogicApp | Diagnostic settings

Search resources, services, and docs (S+)

InsightScape LogicApp | Diagnostic settings

Log App

Overview

Activity log

Access control (IAM)

Tags

Detect and solve problems

Development tools

Logic app designer

Logic app code view

Run history

Versions

AH connections

Quick start guides

Settings

Monitoring

Alerts

Metric

Diagnostic settings

Logs

Metrics

Automator

Help

Diagnostic settings

Name: Log Analytics workspace

Storage account: Event hub

Log Analytics workspace: Partner solution

Edit setting

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.

Add diagnostic setting

Click Add Diagnostic setting above to configure the collection of the following data:

- Workflow runtime diagnostic events
- AllMetric

Microsoft Azure | LogicApp

Home > Logic apps > InsightScape-LogicApp | Diagnostic settings

Search resources, services, and docs (S+)

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.

Diagnostic setting name: LogApp-Diagnostics

Logs

Category groups: All logs

Categories: Workflow runtime diagnostic events

Metrics: allMetric

Destination details

Send to Log Analytics workspace

Subscription: Free Trial

Log Analytics workspace: DefaultLogAnalyticsworkspace-0f5d7b4-d8bb-9312-d8ba00e6a50-EU (last...)

Archive to a storage account

Stream to an event hub

Send to partner solution

JSON View

Microsoft Azure LogicApp

Home > Logic apps > InsightScape LogicApp | Diagnostic settings

Log-tee

Search 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
log-tee-Diagnostic	-	-	DefaultWorkspace-0f3074-4610-4089-9312-d8fa0d0e1e5c	-	Edit setting

Add diagnostic setting

Click "Add diagnostic setting" above to configure the collection of the following data:

- Write live runtime diagnostic events
- AllMetrics

Log Analytics workspace

Partner solution

DefaultWorkspace-0f3074-4610-4089-9312-d8fa0d0e1e5c

Log-tee

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

Metric

Diagnostic settings

Logs

Metrics

Automations

Help

Search resources, services, and docs (F1)

Copy

Parkeraw777@gmail.com

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_port_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_diagnostic_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="{"storageAccountName": "$my_diagnostic_storage_account",  
"storageAccountSasToken":  
"$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:
 - 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 -

Operation name	Status	Time	Time stamp	Subscription	Event Initiated by
Create or update metric alert	Succeeded	11 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
Create or update metric alert	Started	22 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
Create or update metric alert	Succeeded	21 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
Create or update action group	Succeeded	11 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
Delete metric alert	Started	29 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
Delete metric alert	Succeeded	24 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
Register subscription	Succeeded	24 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
Register subscription	Started	24 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
Register subscription	Succeeded	24 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
Delete metric alert	Succeeded	24 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
Create or update metric alert	Succeeded	25 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
Get RetentionPolicy along with blob SAS URL	Started	25 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
Backup Protected Item	Succeeded	32 minutes...	Mon Oct 21...	Free Trial	Microsoft.Featureroller
Register subscription	Succeeded	34 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
Register subscription	Succeeded	35 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
Validate Policy action	Succeeded	35 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
Create or update data collection role	Succeeded	43 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
auditPlaceholder Policy action	Succeeded	47 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
Create or Update Virtual Machine Extension	Succeeded	51 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com
Validate Deployment	Succeeded	52 minutes...	Mon Oct 21...	Free Trial	parawat77@gmail.com

Select a scope

Browse Recent

Resource types: All resource types Location: All locations

Search to filter items...

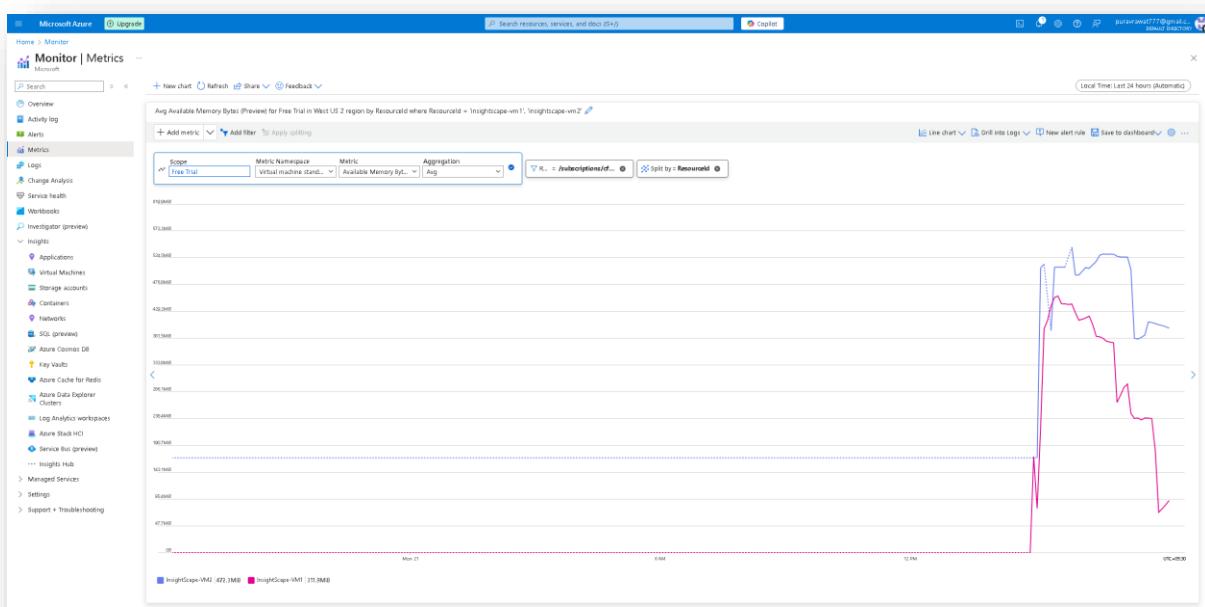
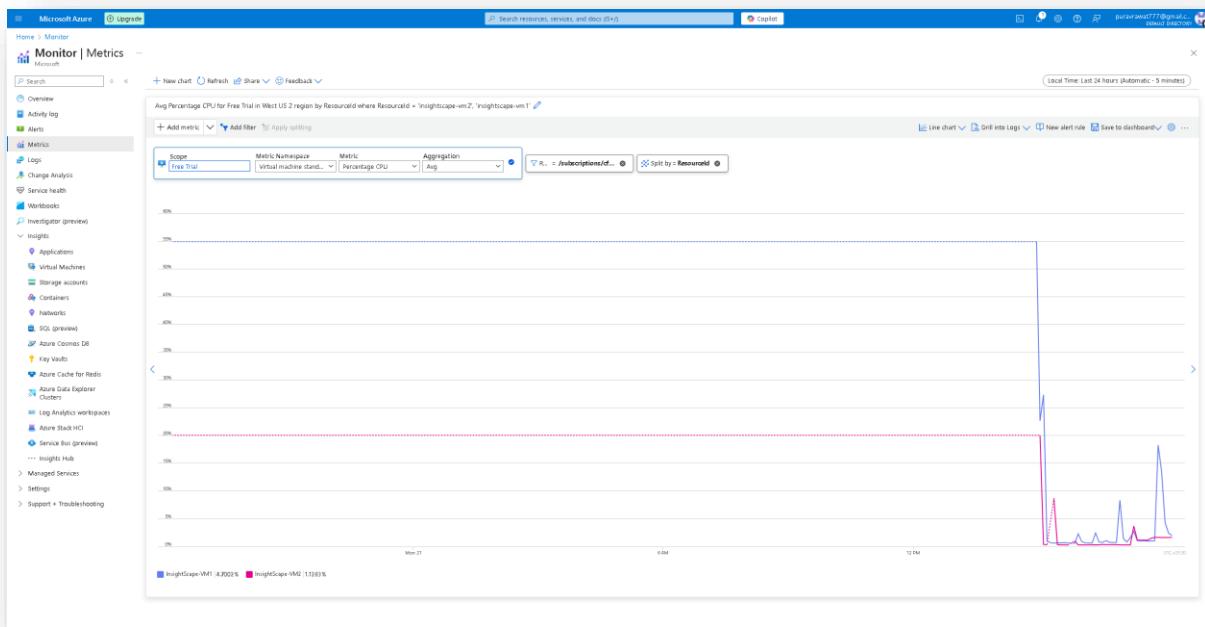
Scope	Resource type	Location
Free Trial	Subscription	-
DefaultResourceGroup-CAN	Resource group	-
DefaultResourceGroup-EU	Resource group	-
DefaultResourceGroup-MU2	Resource group	-
Insightscape-VM1	Virtual machine	West US 2
Insightscape-LogApp	Logic app	West US 2
Insightscape-VmR	Recovery Services vault	West US 2
Insightscape-VM2	Virtual machine	West US 2
Insightscape-VM1-ip	Public IP address	West US 2
Insightscape-en1714	Network interface	West US 2
Insightscape-VM1_COG01_1325d044e07a1	Disk	West US 2
Insightscape-VM2	Virtual machine	West US 2
Insightscape-VM2-ip	Public IP address	West US 2
Insightscape-en2710	Network interface	West US 2
Insightscape-W4C_Condite_34023f9f4e1c	Disk	West US 2
Insightscape-W4bapp	Web App	Canada Central
Insightscape-W4bapp	Application Insights	Canada Central
NetworkWatcherRG	Resource group	-

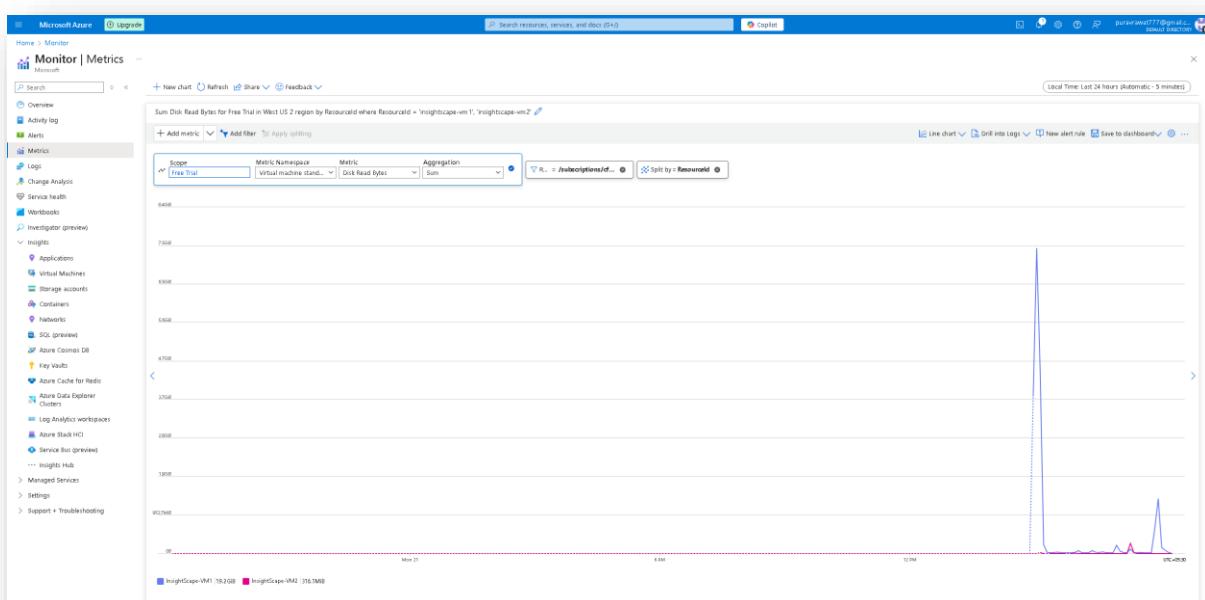
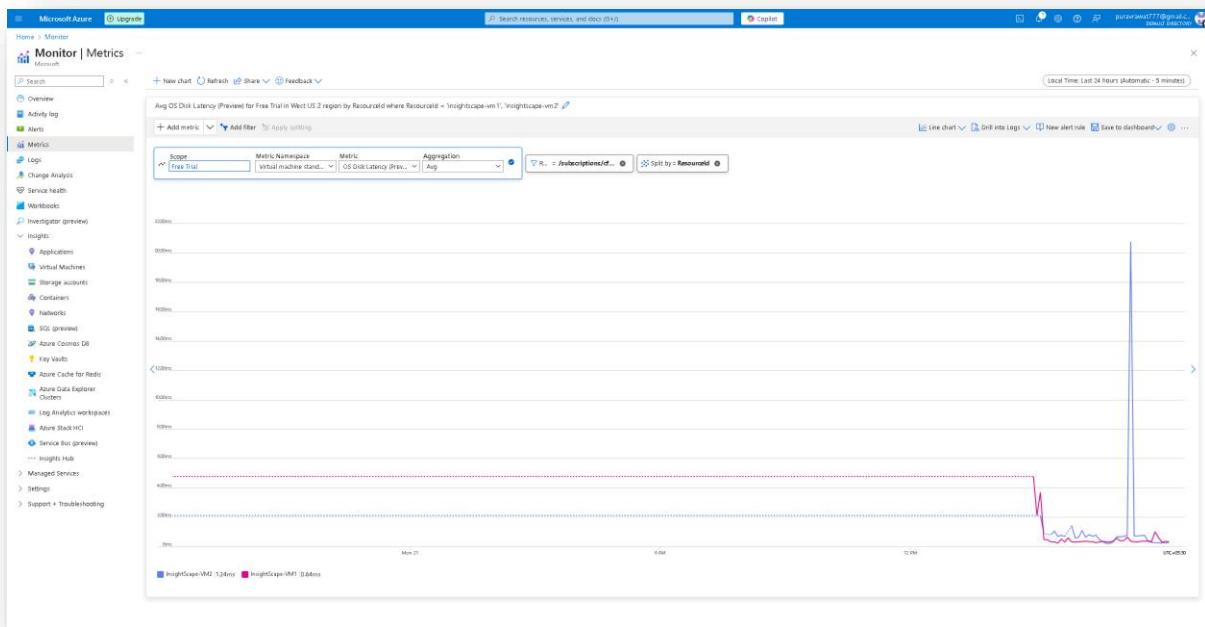
Why can't I select multiple resources? You must select items of the same resource type and location. To select resources of a different resource type or location, please first unselect your current selection.

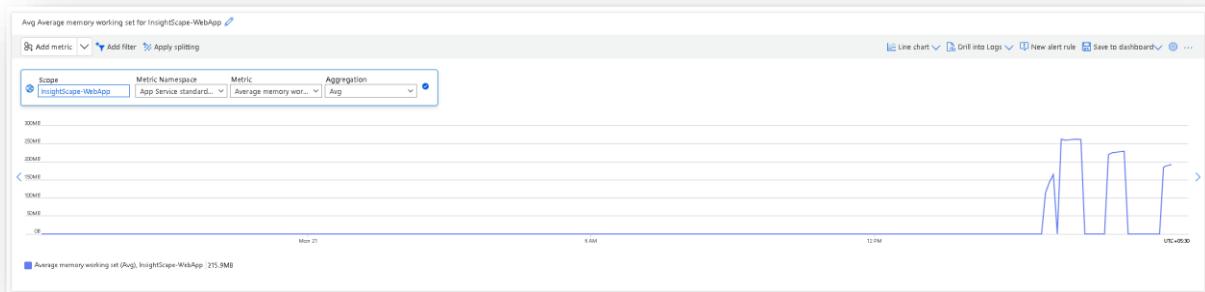
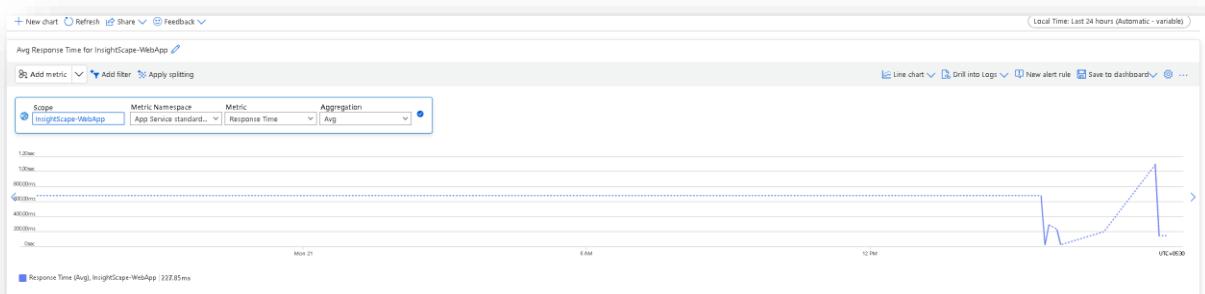
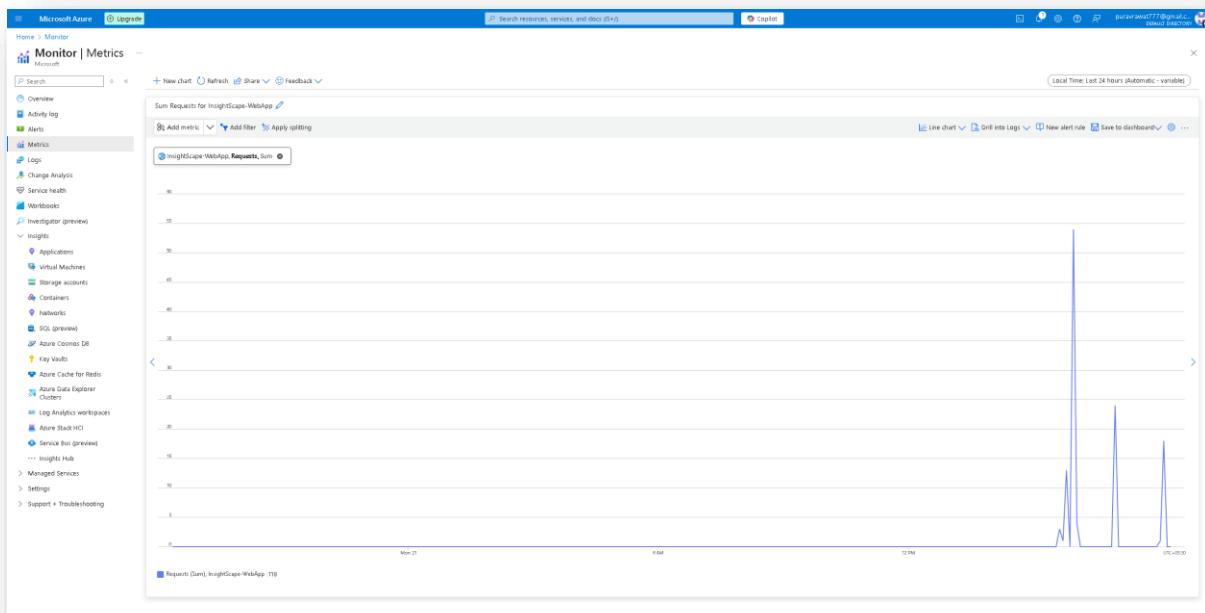
Selected scopes: 2 virtual machines

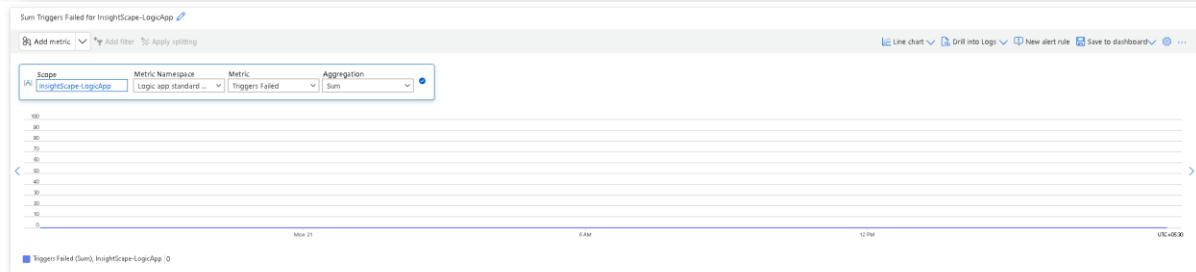
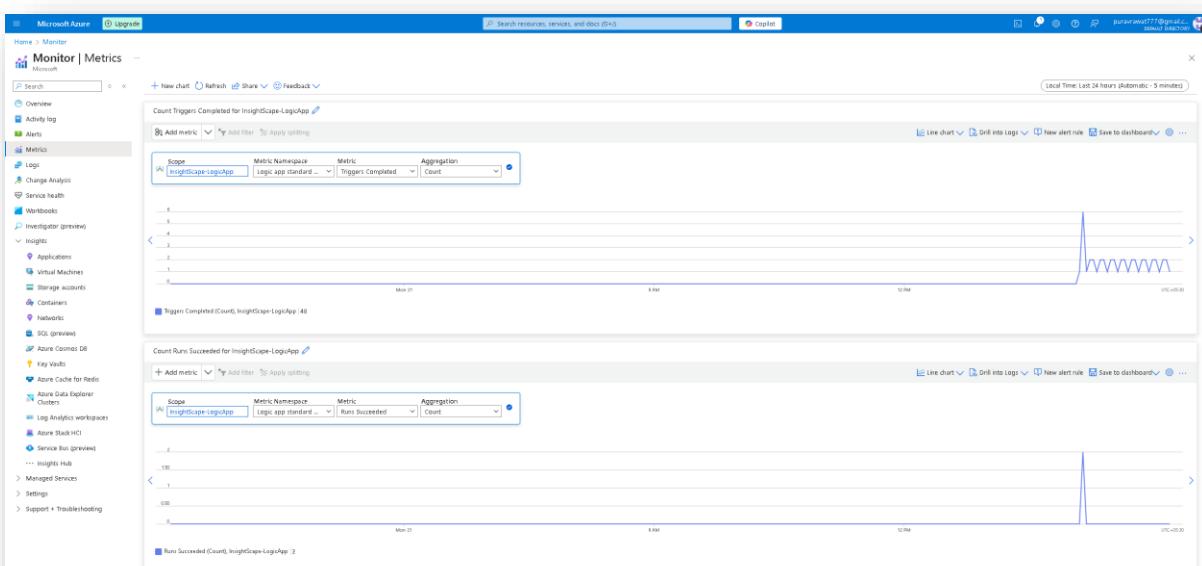
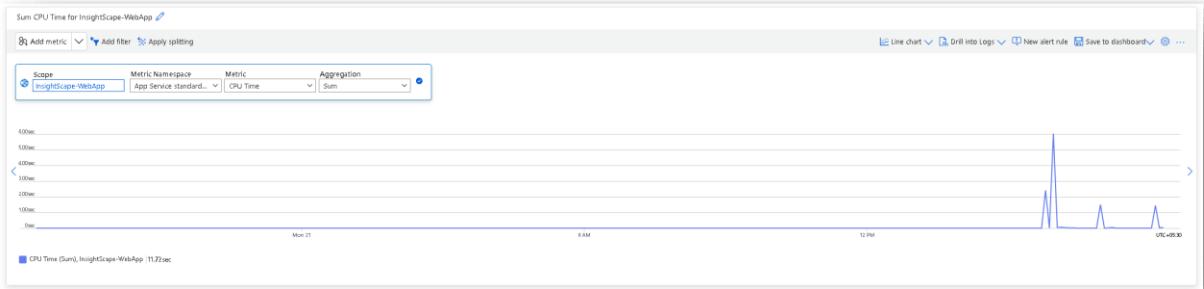
Insightscape-VM1 Insightscape-VM2

Apply Cancel Clear all selections









Microsoft Azure [Upgrade] Search resources, services, and docs (Sx)

Home > Virtual machines > InsightScape-VM1

Virtual machines

InsightScape-VM1 | Extensions + applications

Extensions

VM Applications

+ Add Refresh Update Enable automatic upgrade Feedback

Showing 2 items

Name	Type	Version	Latest Version	Status	Automatic upgrade status
Microsoft.Azure.Monitor.AzureMonitorWindowsAgent	Microsoft Azure Monitor Agent for Windows	1.30.0.0	1.30.0.0	Provisioning succeeded	Disabled
Microsoft.Azure.NetworkWatcherExtension	Microsoft Azure Network Watcher Extension	1.4.9422.1	1.4.9422.1	Provisioning succeeded	Enabled

Page 1 of 1

Microsoft Azure [Upgrade] Search resources, services, and docs (Sx)

Home > Virtual machines > InsightScape-VM1 | Extensions + applications > Install an Extension

Azure Performance Diagnostics

Microsoft Corp.

Azure Performance Diagnostics extension helps you quickly troubleshoot various performance issues on the VM.

Azure Performance Diagnostics

Publisher Microsoft Corp.

Overview

This VM extension runs Perfmon2.ps1 script that collects useful diagnostics information for troubleshooting test performance issues on this Azure VM. We recommend that you work with your CS support contact to select the right performance counter 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 performance analysis
- = Network 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 contains 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 and can be shared via a shared access signature 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 [Perfmon2 EULA.docx](#) available inside [Perfmon2 download](#) file and to [share diagnostics information](#).

Please provide your comment or feedback at [Azure Feedback](#)

Next

Microsoft Azure | Log out

Home > _de_GalleryItemDetails.microsoft_dsc.AzureDiagnostics [Overview] >

InsightScape VM1/AzurePerformanceDiagnostics

Resource ID: /subscriptions/cf63f1e4-e4ff-4312-9b1a-0edc0d0csourceGroups/microsoft-resourceproviders/Microsoft.Compute/virtualMachines/insightscape-vm1/extensions/

Type: Microsoft.Compute/virtualMachines/extensions

View

Search Refresh Delete Open in mobile

Overview

Activity log

Access control (IAM)

Settings

Automation

Help

Properties Recommendations

Properties

Force update tag: ...

Initiator: Microsoft Azure Performance Diagnostic

Time: 2024-02-21T10:48:20Z

Type handler version: AzurePerformanceDiagnostic

Auto upgrade minor version: true

Enable automatic upgrade: ...

Settings: View value as JSON

Protected settings from key vault: ...

Source vault: ...

Provisioning state: Succeeded

Suppress failures: ...

Provision after extension: ...

Instance view

Name: ...

Type: ...

Type handler version: ...

Subscriptions: ...

Statuses: ...

Microsoft Azure | Log out

Home > Virtual machines > InsightScape-VM1

InsightScape VM1 | Diagnostic settings

Install Diagnostic Extension

Default Directory

Create < Switch to classic

Filter for any field...

Name: InsightScape-VM1

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Networking

Settings

Availability + scale

Security

Backup + disaster recovery

Operations

Monitoring

- Logs
- Metrics
- Diagnostic settings:
- Logs
- Metrics

Automation

Help

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 Diagnostic agent. We'll help you set up guest-level monitoring.

To get started now, choose a storage account below where diagnostic data will be sent and then click the blue "Enable guest-level monitoring" button.

Diagnostic storage account: insightspectorgmt

Enable guest-level monitoring

Page 1 of 1

Give feedback

The screenshot shows the Azure portal interface for managing a virtual machine named 'InsightScape-VM1'. The left sidebar lists several monitoring categories: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Networking, Settings, Availability + scale, Security, Backup + disaster recovery, Operations, Monitoring (with Insights, Alerts, Metrics), and Diagnostic settings. The 'Diagnostic settings' section is currently selected. The main content area is titled 'InsightScape-VM1 | Diagnostic settings'. It contains a sub-section for 'Windows Virtual Machine Diagnostic Extension' which provides a brief description of the extension's function. Below this is the 'Azure Diagnostic Agent Settings' section, which includes fields for 'Storage account' (set to 'insightscapelstorage'), 'Disk quota (MB)' (set to '\$100'), and 'Collect infrastructure Log' (set to 'True'). The 'Log level' dropdown is set to 'Error'. At the bottom of this section is a 'Remove' button. To the right of the main content, a 'Notifications' bar is visible, showing a message about successfully installed diagnostic settings for the VM.

Microsoft Azure | Upgrade

Home > Virtual machines > InsightScape-VM2

Virtual machines

Default directory

InsightScape-VM2 | Extensions + applications

Search resources, services, and objects (20,432)

Filter for any field...

Name: Insightscape-VM1

Filter for any field...

Name: Insightscape-VM2

Overview Activity log Access control (IAM) Tags

Diagnose and solve problems

- Connect
- Networking
- Settings
 - Disk
- 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 Enable automatic upgrade Disable automatic upgrade

Search to filter items...

	Type	Version	Latest Version	Status	Automatic upgrade status
<input type="checkbox"/>	MicrosoftAzure Monitor AzureMonitorLogAgent	1.33.1	1.33.1.0	Provisioning succeeded	Disabled

Page 1 of 1

```
Microsoft Azure [ Upgrade ] Search resources, services, and docs (D+D) Capabilities Help
Switch to PowerShell ⌘ ⌘ ⌘ Manage files New revision Editor Web preview Settings ⌘ ⌘ ⌘
parav [ - ] $ az vm extension set \
--resource-group InsightScape-RG \
--vm-name testVM \
--name AzureMonitorLinuxAgent \
--publisher Microsoft.Azure.Monitor
{
  "autoUpgradeMinorVersion": true,
  "enableAutomaticUpgrade": null,
  "forceUpdateTag": null,
  "id": "/subscriptions/fad78a-f6d8-4d88-9312-d58ab0e9a50/resourceGroups/InsightScape-RG/providers/Microsoft.Compute/virtualMachines/testVM/extensions/AzureMonitorLinuxAgent",
  "improvementType": "Major",
  "location": "westus2",
  "name": "AzureMonitorLinuxAgent",
  "protectedSettingsFromKeyVault": null,
  "provisionAfterExtensions": null,
  "publisher": "Microsoft.Azure.Monitor",
  "resourceGroup": "InsightScape-RG",
  "tags": null,
  "suppressFailure": null,
  "type": "Microsoft.Compute/virtualMachines/extensions",
  "typeHandlerVersion": "1.33",
  "typeProperties": "AzureMonitorLinuxAgent"
}
parav [ - ] $
```

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure' and 'Upgrade' buttons, followed by a search bar with placeholder text 'Search resources, services, and documentation' and a 'Create' button. Below the search bar, the URL 'https://www.azure.com/#blade/Microsoft_Azure门户/ResourceGroupsBlade/resourceGroup=InsightScape-VM2/resourceType=VirtualMachines/resourceName=InsightScape-VM2/refresh=true' is visible.

The main content area is titled 'Insightscape VM2 | Extensions + applications'. On the left, there's a sidebar with a tree view of the VM settings, including sections like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems' (with 'Connect', 'Cloud', 'Button', and 'Networking' options), 'Settings' (with 'Orbs', 'Extensions + applications' which is selected and highlighted in blue, 'Operating system', 'Configuration', 'Advisor recommendations', 'Properties', 'Locks', 'Availability + scale', 'Security', 'Backup + disaster recovery', 'Operational', 'Monitoring' (with 'Logs', 'Metrics', 'Diagnostic settings', 'Logs', 'Metrics', 'Logs', 'Metrics'), 'Automate', and 'Help'), and 'Help'.

The main pane displays the 'Extensions' section under 'VM Applications'. It shows two extensions listed:

Name	Type	Version	Latest Version	Status	Automatic upgrade status
ADLSGen2FileForLinux	MicrosoftAzure.ActiveDirectory.ADSHLogonForLinux	1.0.2644.1	1.0.2644.1	Provisioning succeeded	Not supported
AzureMonitorLinuxAgent	Microsoft.Azure.Monitor.AzureMonitorIngestAgent	1.33.1	1.28.1.0	Provisioning succeeded	Disabled

Microsoft Azure (Upgrade)

Home > Monitor

Monitor | Diagnostic settings

Overview Alerts Metrics Log Change Analysis Service Health Workbooks Investigator (preview) Insights Managed Services Settings Diagnostic settings Data Collection Rules Data Collector Endpoints Azure Monitor pipelines (preview) Autoscale Private Link Scopes Support + Troubleshooting

Select any of the resources to view diagnostic settings.

Name	Resource type	Resource group	Diagnostic status
DefaultWorkspace- guid -Log	Log Analytics workspace	DefaultResourceGroup-CAN	Disabled
InsightScope-VM-NSG	Network security group	InsightScope-RG	Disabled
InsightScope-VM1-ip	Public IP address	InsightScope-RG	Disabled
InsightScope-en1714	Network interface	InsightScope-RG	Disabled
InsightScope-e4c4-ip	Public IP address	InsightScope-RG	Disabled
InsightScope-Monitoring10	Network security group	InsightScope-RG	Disabled
InsightScope-mn2710	Network interface	InsightScope-RG	Disabled
ASP-insightScope-8711	App service plan	InsightScope-RG	Disabled
InsightScope-mabApp	Application Insights	InsightScope-RG	Disabled
InsightScope-mabApp	App Service	InsightScope-RG	Disabled
InsightScope-nsa	Storage account	InsightScope-RG	Disabled
blob	Storage account	InsightScope-RG	Disabled
queue	Storage account	InsightScope-RG	Disabled
table	Storage account	InsightScope-RG	Disabled
file	Storage account	InsightScope-RG	Disabled
InsightScope-lagcApp	Logic app	InsightScope-RG	Enabled
DefaultWorkspace- guid -Log	Log Analytics workspace	DefaultResourceGroup-WUS2	Disabled
InsightScope-vault	Recovery services vault	InsightScope-RG	Disabled
DefaultWorkspace- guid -Log	Log Analytics workspace	DefaultResourceGroup-EU	Disabled

Microsoft Azure (Upgrade)

Home > Monitor

Monitor | Diagnostic settings

Overview Alerts Metrics Log Change Analysis Service Health Workbooks Investigator (preview) Insights Managed Services Settings Diagnostic settings Data Collection Rules Data Collector Endpoints Azure Monitor pipelines (preview) Autoscale Private Link Scopes Support + Troubleshooting

Free Trial / InsightScope-RG > InsightScope-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](#)

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:

- event logs
- App Service Console Logs
- App Service Application Logs
- App Service Metrics
- IPSecurity Audit Logs
- App Service Platform logs
- App Service Authentication logs (preview)
- AllMetrics

Microsoft Azure | Log Analytics

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 where destination they should be sent to. Normal usage charges for the destination will occur, and more about the different log properties and contexts of these logs.

Diagnostic setting name * **WebApp-Diagnostics**

Logs

Categories

- HTTP logs
- App Service Console Logs
- App Service Application Logs
- Access Audit Logs
- IP Security Audit logs
- App Service Platform logs
- App Service Authentication logs (preview)

Destination details

Subscription **Free Trial**

Log Analytics workspace **DefaultLogAnalyticsworkspace-02d07f84-6d0b-4d89-9312-d59a00e0d50-EU (existing)**

Archive to a storage account

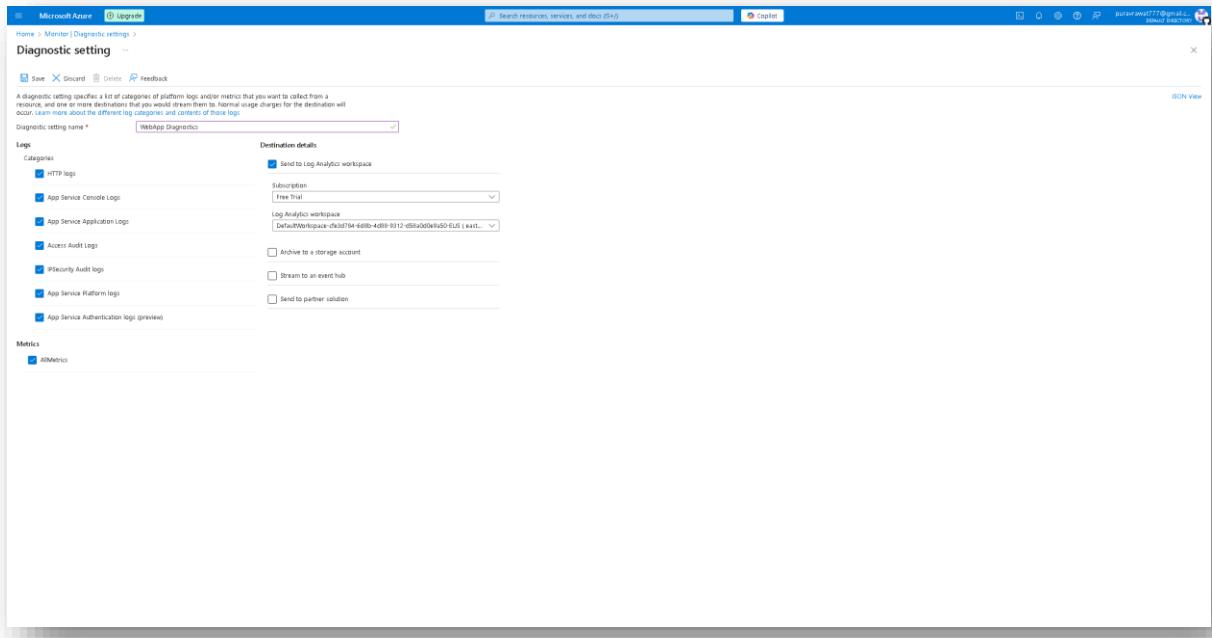
Stream to an event hub

Send to partner solution

Metrics

AllMetrics

JSON View



Microsoft Azure | Log Analytics

Home > Monitor

Monitor | Diagnostic settings -

Search Refresh Feedback

Subscription **Free Trial** Resource group **InsightScope-RG** Resource type **App Services** Resource **InsightScope-WebApp**

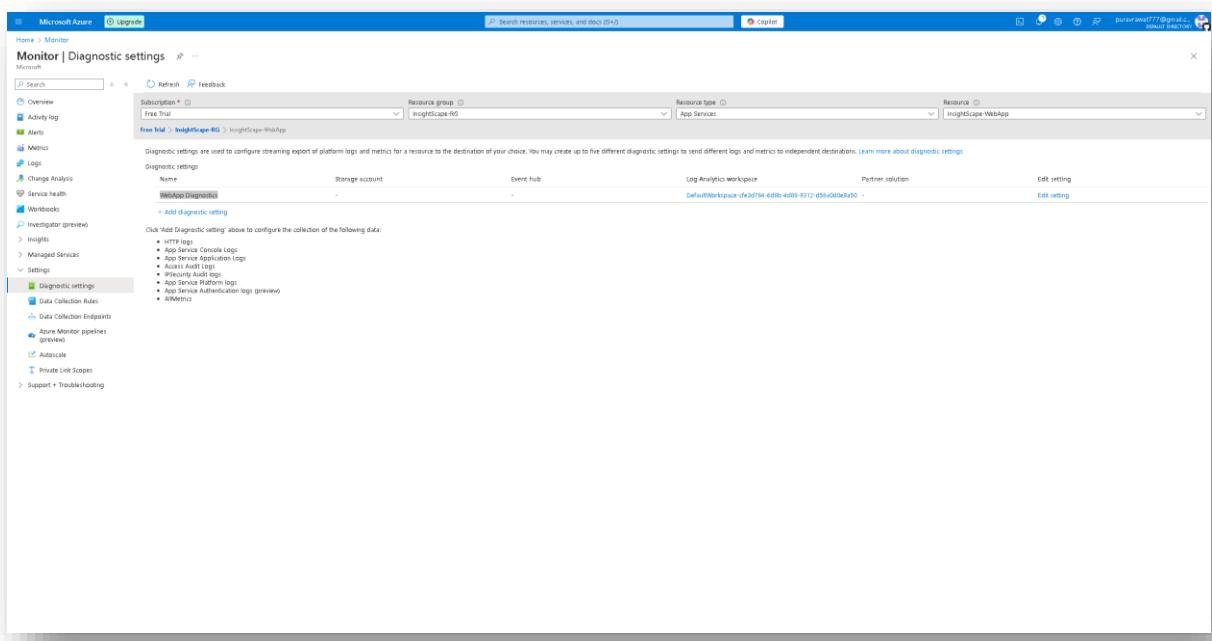
Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. [Learn more about diagnostic settings](#).

Diagnostic setting	Name	Storage account	Event hub	Log Analytics workspace	Partner solution	Edit setting
WebApp-Diagnostics	-	-	-	DefaultLogAnalyticsworkspace-02d07f84-6d0b-4d89-9312-d59a00e0d50-EU	-	Edit 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
- IP Security Audit logs
- App Service Platform logs
- App Service Authentication logs (preview)
- AllMetrics

Overview Activity log Alerts Metrics Log Change Analysis Service health Notebooks Investigator (preview) Insights Managed Services Settings Diagnostic settings Data Collection Rules Data Collection Endpoints Azure Monitor pipelines (preview) Autoscale Private Link Scopes Support + Troubleshooting



Microsoft Azure | Log Analytics

Home > Monitor | Diagnostic settings > DefaultWorkspace-cfe3d784-6db8-4d88-9312-d58a0d0e9a50 EUS | Virtual machines (deprecated)

DefaultWorkspace-cfe3d784-6db8-4d88-9312-d58a0d0e9a50 EUS | Virtual machines (deprecated)

Log Analytics workspace

Search: Refresh Filter by name... 0 selected 2 selected Free trial insightScape-rg West US 2

Name	Log Analytics Connection	OS	Subscription	Resource group	Location
InsightScape-VM1	Not connected	Windows	df3d784-6db8-4d88-9312-d58a0d0e9a50	insightscape-rg	westus2
InsightScape-VM2	Not connected	Linux	df3d784-6db8-4d88-9312-d58a0d0e9a50	insightscape-rg	westus2

Overview Activity log Access control (ARM) Tag Diagnosis and solve problems Log Settings Tables Agents Usage and estimated costs Data export Network isolation Linked storage accounts Properties Logs Classic Legacy agents Legacy activity log connector Legacy storage account logs Legacy computer groups Legacy solutions System center Workspace summary (deprecated) Virtual machines (deprecated) Scope configurations (deprecated) Monitoring Automation Help

(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 | Log Analytics

Home > Monitor

Monitor | Diagnostic settings

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](#)

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:

- Audit
- Summary Logs
- Metrics

Subscription: Free Trial Resource group: DefaultResourceGroup-WUS2 Resource type: Log Analytics workspaces Resource: DefaultWorkspace-cfe3d784-6db8-4d88-9312-d58a0d0e9a50-WUS2

Overview Metrics Log Analytics Workbooks Investigator (preview) Insights Managed Services Settings Diagnostic settings Data Collection Rules Data Collection Endpoints Azure Monitor pipelines (private) Autoscale Private Link Scopes Support + Troubleshooting

Microsoft Azure  Diagnostic settings

Home > Monitor | Diagnostic settings > ...

Diagnostic setting

See Discard Green Feedback

A diagnostic setting specifies a list of categories of platform log, metric, metrics that you want to collect from a resource and one or more destinations the platform streams 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 [Logs](#) to configure platform metric collection from [microsoft/operationalinsights/workspaces](#) to storage account, event hubs, and Log Analytics workspace. [Learn more](#)

Diagnostic setting name *

Logs

Category groups **v1.log**

Categories Audit **allMetrics**

Summary Logs

Destination details

Send to Log Analytics workspace

Subscription

Log Analytics workspace

Archive to a storage account

Stream to an event hub

Send to partner solution

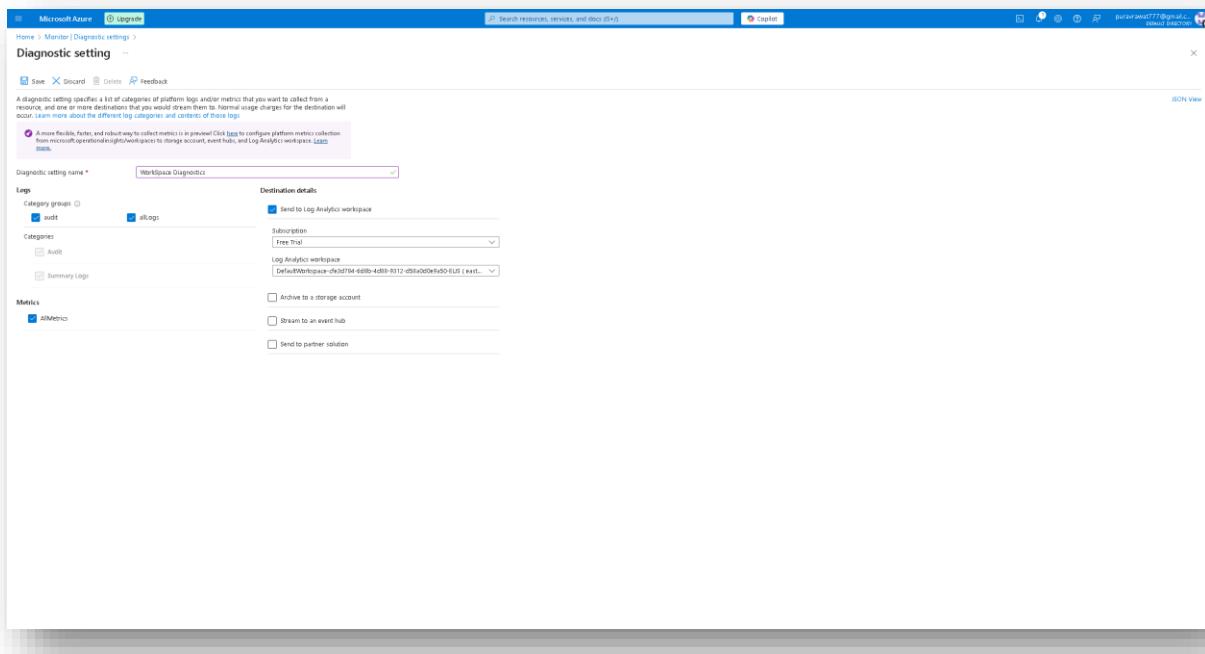
[Edit](#) [Save](#) [Cancel](#)

Search resources, services, and docs (Sx)

Copy

Parterawat777@gmail.com  

JSON View



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-

This screenshot shows the Microsoft Azure Service Health | Resource health page. The left sidebar includes links for ACTIVE EVENTS, HISTORY, RESOURCE HEALTH (selected), and ALERTS. The main area displays two resources: 'insightscope-vm1' and 'insightscope-vm2'. Both are listed under the 'Virtual machine' type, located in 'westus2', and are associated with a 'Free Trial' subscription.

This screenshot shows the Microsoft Azure Service Health | Resource health page. The left sidebar includes links for ACTIVE EVENTS (with Service issues, Planned maintenance, Health advisories, and Security advisories), HISTORY, RESOURCE HEALTH (selected), and ALERTS. The main area displays one resource: 'insightscope-webapp', which is listed under the 'Website' type, located in 'canadacentral', and is associated with a 'Free Trial' subscription.

[Microsoft Azure](#) [Upgrade](#)

Home > Monitor > Service health > Service Health > Resource health

Resource health

nightwatcher

+ 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

Date Description

10/21/2024

2 health events

Started by user (Customer Initiated)

At Monday, October 21, 2024 at 14:53:01 (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.

14:53:01 (GMT+5:30)

Recommended Step

- Check back here for status updates
- If you're having problems, use the [Troubleshoot tool](#) to get recommended solutions.

[Download as PDF](#)

Was this helpful? [Yes](#) | [No](#)

Virtual Machine allocated (Customer Initiated)

At Monday, October 21, 2024 at 14:53:01 (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.

14:53:01 (GMT+5:30)

Recommended Step

- Check back here for status updates
- If you're having problems, use the [Troubleshoot tool](#) to get recommended solutions.

[Download as PDF](#)

Was this helpful? [Yes](#) | [No](#)

[Microsoft Azure](#) [Upgrade](#)

Home > Monitor > Service health > Service Health > Resource health

Resource health

nightwatcher

+ 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

Date Description

10/21/2024

1 health event

Unknown - Resource health event

At Monday, October 21, 2024 at 14:13:33 (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.

194.133 (GMT+5:30) - Ongoing

Recommended Step

- Check back here for status updates
- If you're having problems, use the [Troubleshoot tool](#) to get recommended solutions.

[Download as PDF](#)

Was this helpful? [Yes](#) | [No](#)

Microsoft Azure [Log out]

Home > Monitor | Service health > Service Health | Resource health > Resource health > insightscape-webapp

Search resources, services, and docs (Sx)

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 2 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 enabled. Integrate & Log4j errors IP Address Configuration Migration Operations
- SSL and Domains Discover issues with certificates and bindings. 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

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 essential fix for issues your application may encounter, it allows your application to self-heal and recover from errors automatically. 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

Overutilizing 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 single instance goes down, no instance on which your web app is running will be upgraded. Therefore, your web app process will be restarted and will experience downtime.

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 resources measure the hosted applications are.

Azure App Service plan overview

Microsoft Azure [Log out]

Home > Monitor | Service health > Service Health | Resource health > Resource health > insightscape-webapp

Search resources, services, and docs (Sx)

Save Discard Refresh Troubleshoot Metrics Send 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 Logic apps

Home > Logic apps > InsightScape-LogicApp

Logic apps

Default Directory

+ Add Manage view

Filter for any field... Name: InsightScape-LogicApp

... Insightscape-LogicApp

Run History

Overview Activity log Access control (IAM) Tags 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

Search: All Pick a date Pick a time

Search to filter items by identifier

Status	Start time	Identifier	Durations	Statistic results
Succeeded	10/21/2024, 4:14 PM	0694720993957997520549718419CQ04	274 Milliseconds	
Succeeded	10/21/2024, 4:14 PM	0694720993957997521549718419CQ29	289 Milliseconds	

Page 1 of 1

InsightScape-LogicApp | Run History

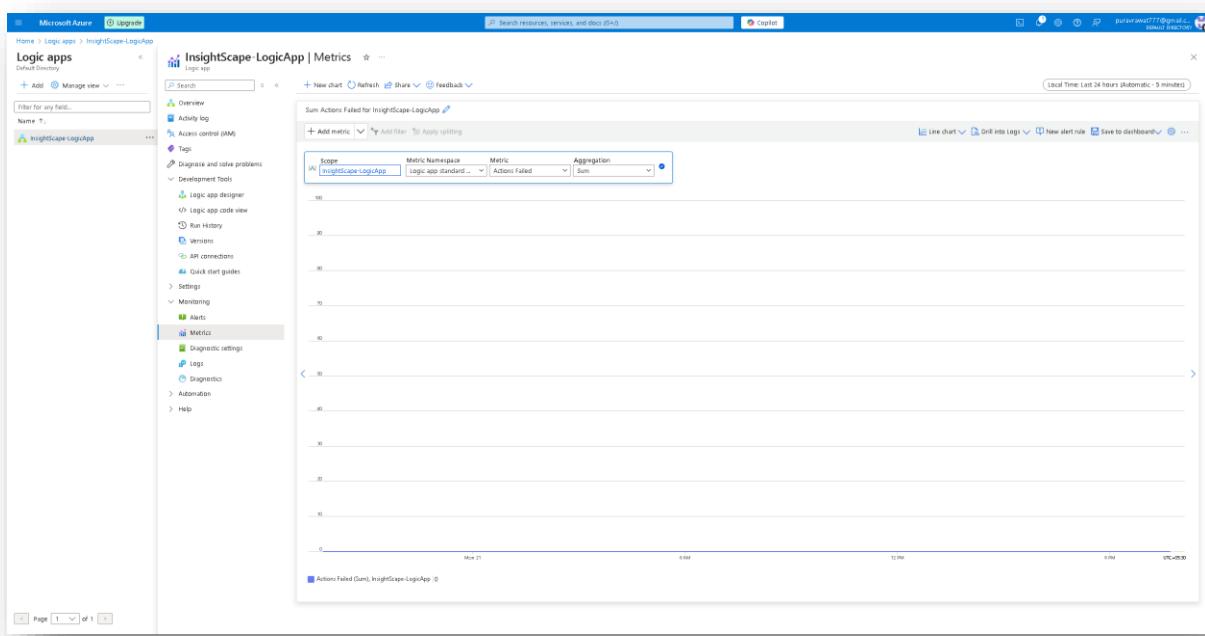
Logic app

Overview Activity log Access control (IAM) Tags 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

Search: All Pick a date Pick a time

Search to filter items by identifier

Status	Start time	Identifier	Durations	Statistic results
Succeeded	10/21/2024, 4:14 PM	0694720993957997520549718419CQ04	274 Milliseconds	
Succeeded	10/21/2024, 4:14 PM	0694720993957997521549718419CQ29	289 Milliseconds	



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-

The screenshot shows the Microsoft Azure Application Insights blade. At the top, there's a navigation bar with 'Microsoft Azure' and a 'Create' button. Below it, the 'Application Insights' section has a 'Default directory' dropdown. The main area displays a table with one row of data:

Name	Resource group	Location	Subscription
InsightScope-WebApp	InsightScope-rg	Canada Central	Free Trial

At the bottom of the table, there are filter buttons: 'Filter for any field...', 'Subscription equals all', 'Resource group equals all', 'Location equals all', and 'Add filter'. Below the table, there are pagination controls: '< Previous', 'Page 1 of 1', and 'Next >'.

Microsoft Azure | Upgrade

Home > Application Insights > InsightScape-WebApp

Application Insights

Default Directory

Name: InsightScape-WebApp

Filter for any field...

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Investigate

Monitoring

Usage

Configure

Settings

Automation

Help

Search

Application Dashboard

Getting started

Search

Logs

Monitor resource group

Feedback

Rename

Delete

Instrumentation key: 237000ca-045e-4f95-be44-09c0118f9f1

Connection String: InstrumentationKey=237000ca-045e-4f95-be44-09c0118f9f1;IngestionEndpoint=https://canadacentral1.in.applicationinsights.azure.com/

Workspace: DefaultWorkspace-237000ca-045e-4f95-be44-09c0118f9f1

RSN View

Show data for last:

20 minutes (selected), 1 hour, 4 hours, 12 hours, 1 day, 3 days, 7 days, 20 days

Failed requests

Server response time

Server requests

Availability

Page 1 of 1

Microsoft Azure | Upgrade

Home > Application Insights > InsightScape-WebApp

Application Insights

Default Directory

Name: InsightScape-WebApp

Filter for any field...

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

Code Optimizations

Profiler

View in Logs

Analyze with Workbooks

Copy link

Feedback

Browse

Last Time: Last 24 hours

Roles = All

Operations Dependencies Roles

Operation timer: zoom into a range

Report count

Overall

Request count

Duration (ms)

Overall

Overall

Distribution of durations: zoom into a range

No data available

Request count

Duration (ms)

Overall

Overall

Insights

No insights were found

Drill into...

0 samples

Page 1 of 1

Microsoft Azure Upgrade

Home > Application Insights > InsightScape-WebApp

Application Insights

Default Directory

+ Create Manage view ...

Filter for any field... Name : InsightScape-WebApp

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Investigate Application map Smart detection Live metrics Transaction search Availability Performance Monitoring Usage Configure Settings Automation Help

InsightScape-WebApp | Failures

Search Refresh View in Logs Analyze with Workbooks Copy link Feedback

Search: Refresh: View in Logs: Analyze with Workbooks: Copy link: Feedback:

Local Time: Last 24 hours Roles: All

Operations Dependencies Exceptions Notes

Failed request count: 0

Request count: 0

Report count: 0

Overall

Top 3 response codes: View details Remove

Top 3 exception types: View details Remove

Top 3 failed dependencies: View details Remove

Drill into... Services

Page 1 of 1

Microsoft Azure Upgrade

Home > Application Insights > InsightScape-WebApp

Application Insights

Default Directory

+ Create Manage view ...

Filter for any field... Name : InsightScape-WebApp

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Investigate Monitoring Usage Configure Settings Automation Help

InsightScape WebApp | Users

Search: + Create a Cohort Open Save Refresh Give us your feedback Help

During: Show: Who used: Events: By value axis: Split by: Add filters:

1 users

Chart Type: Time chart

Last 30 minutes

Apdex Performance Configuration: Edit

SESSIONS	EVENTS	PERFORMANCE
1	1	Unacceptable

Page 1 of 1

PROPERTIES Edit

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

The screenshot shows the Microsoft Azure Application Insights interface. The top navigation bar includes 'Microsoft Azure' and 'Upgrade' buttons, followed by a search bar 'Search resources, services, and docs (0+)' and a 'Capitol' button. The main title is 'InsightScape-WebApp | Live metrics'. On the left, a sidebar menu lists various monitoring categories: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems (with sub-options Investigate, Application map, Smart detection), User metrics (selected and expanded, showing Transaction search, Availability, Failures, Performance, Monitoring, Usage, Sessions, Events, Funnel, User flow, Cohorts, More), Configure, Settings, Automation, and Help. At the bottom left, there's a page navigation bar with 'Page 1 of 1'.

Microsoft Azure [Upgrade](#)

Home > Application Insights > ImageGauge-WebApp | Diagnostic settings >

Diagnostic setting

[Save](#) [Discard](#) [Delete](#) [Feedback](#)

A diagnostic setting specifies a list of categories of platform log, metric metrics that you want to collect from a resource. You can also define which log and metric items to forward to another storage for the destination will occur. Learn more about the different log categories and contents of these logs.

Diagnostic setting name *

Logs

Category group All logs

Availability results
 Browsing timings
 Events
 Metrics
 Dependencies
 Exceptions
 Page views
 Performance counters
 Requests
 System events
 Traces

Destination details

Send to Log Analytics workspace

Subscription

Log Analytics workspace

Archive to a storage account
 Stream to an event hub
 Send to partner solution

Metrics

AllMetrics

Microsoft Azure Log out

Home > Application Insights > InsightScape-WebApp

Application Insights

+ Create Manage view

Name: InsightScape-WebApp

Filter for any field...

Overview

Activity log

Tags

Diagnose and solve problems

Ingestion

- 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
- Calorts
- More

Configure

Settings

Automation

Help

Page 1 of 1

InsightScape-WebApp | Diagnostic settings

Search 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
DefaultWorkspace-0x307944d8b-4099-9112-d59c	-	-	-	-	Edit setting

Add diagnostic setting

Click 'Add diagnostic setting' above to configure the collection of the following data:

- Availability results
- Browser timing
- Events
- Metric
- Dependencies
- Error
- Page view
- Performance counters
- System events
- Trace
- AllMetric

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
 - 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)
 - Destination Port: 80
- Results:
 - Traffic Status: Denied

c) Conclusion

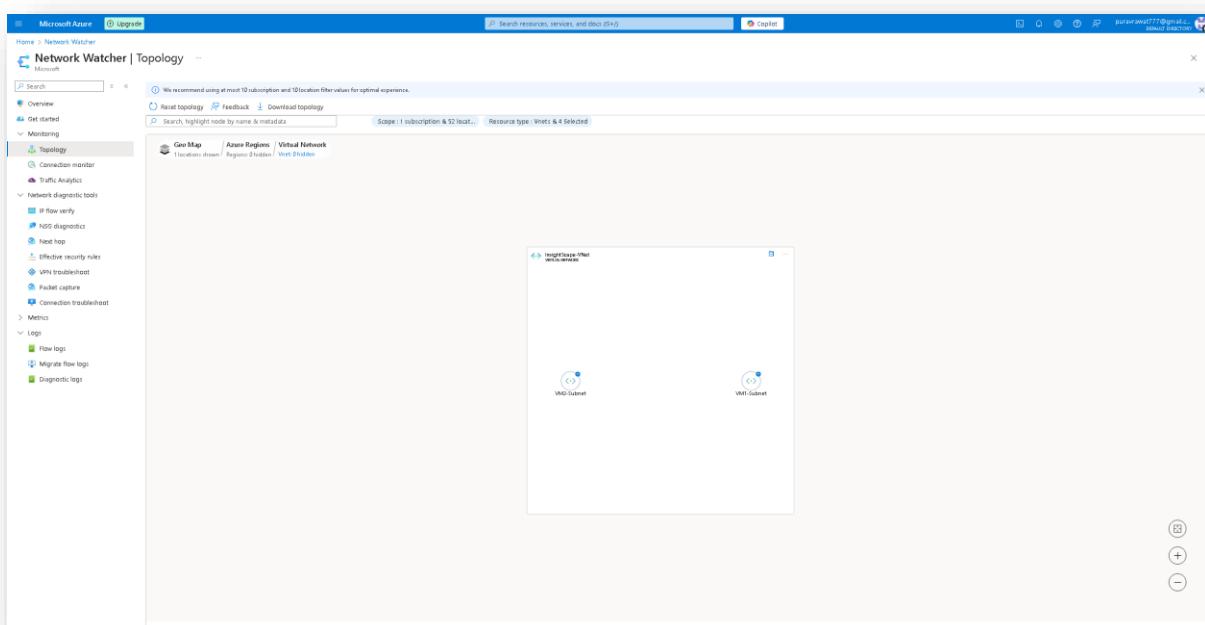
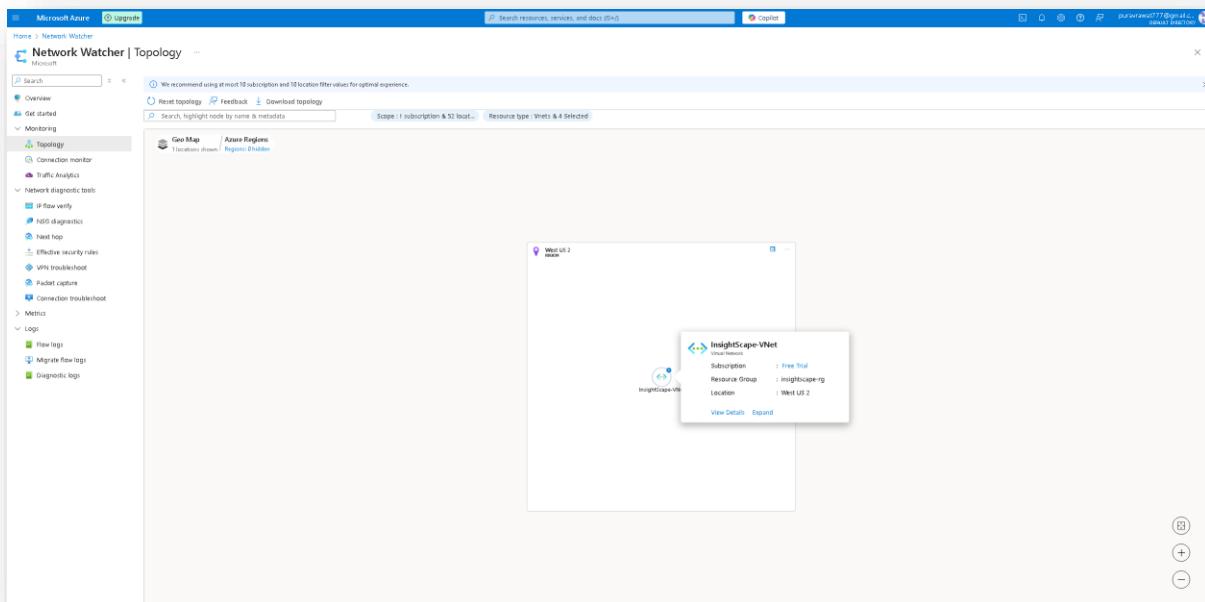
With these tests, I successfully demonstrated the use of NSG diagnostics to validate inbound traffic configurations and to verify how security rules impacted traffic flow to the virtual machines.

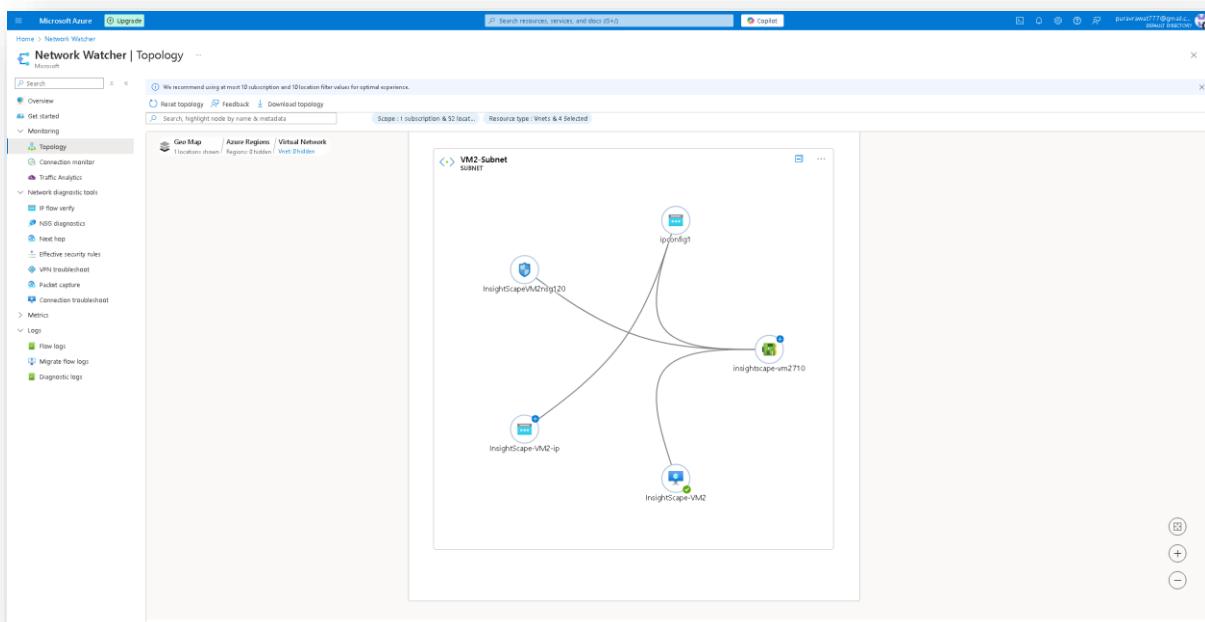
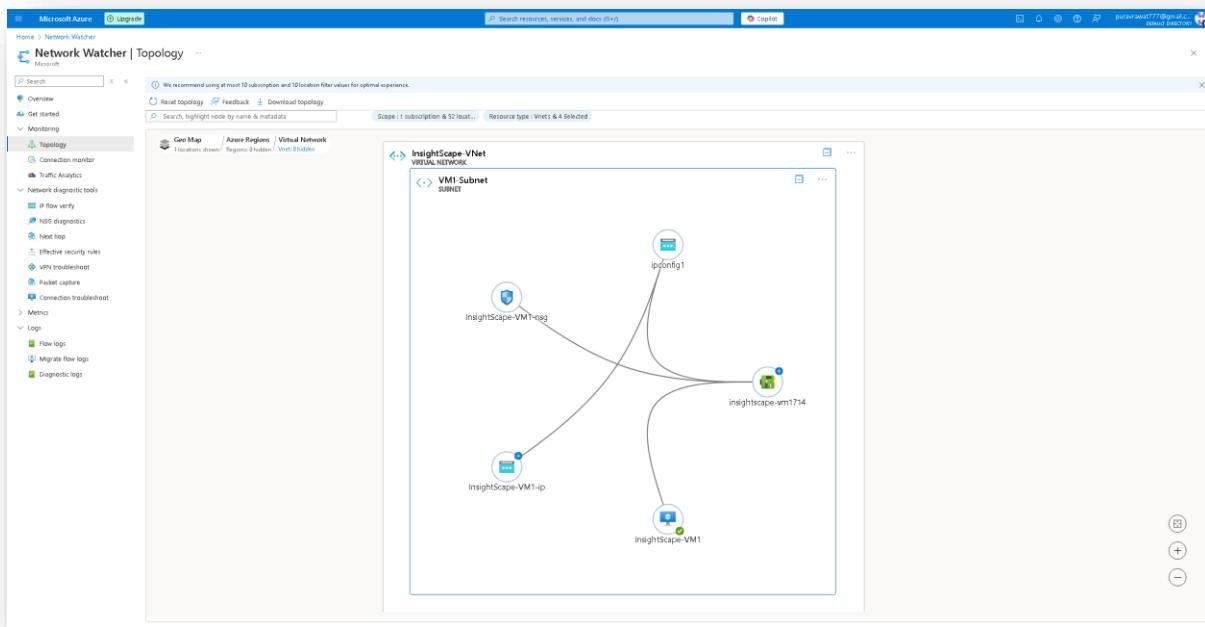
This concluded the Step 4: Network Monitoring phase of the project, and it was successfully completed.

Screenshots-

This screenshot shows the Microsoft Azure Network Watcher Overview page. The left sidebar contains a navigation menu with options like Overview, Get started, Monitoring (Topology, Connection monitor, Traffic Analytics, Network diagnostic tools, IP flow verify, NSG diagnostics, Next hop, Effective security rules, VPN troubleshooting, Packet capture, Connection troubleshooting), Metrics, Logs (Flow logs, Migrate flow logs, Diagnostic logs), and Help. The main content area displays a search bar and filter options (Subscription equals all, Resource group equals all, Location equals all). A single record is listed: "Name: networkWatcher_rg2", "Subscription: Free Trial", and "Location: West US 2". At the bottom, there are navigation links for Previous, Page 1 of 1, and Next, along with a "Give feedback" link.

This screenshot shows the Microsoft Azure Network Watcher Topology page. The left sidebar is identical to the Overview page. The main content area features a world map titled "Geo Map" with the subtitle "Locations shown". A single location is marked with a blue pin: "West US 2". On the right side of the map, there are three circular icons with symbols: a square with a circle, a plus sign, and a minus sign. Below the map, there are buttons for "Reset topology", "Feedback", and "Download topology", along with search and scope filters.





Microsoft Azure Upgrade

Home > Network security groups > Default Directory

InsightScape-VM1-nsg Network security group

+ Create Manage view ...

Filter for any field... Search resources, services, and docs (F1)

Overview Custom security rules : 3 inbound, 0 outbound

Resource group **insightScapeRG** Associated with : 0 subnets, 1 network interface

Location : West US 2 Subscription **free Trial**

Subscription ID : c9e1c794-6d1b-40ff-9312-d5ba0d8e9400

Tags Add tags

Essentials

Inbound security rules Outbound security rules

Subnets Properties

Locks Monitoring

Help Automation

Settings

Inbound security rules Outbound security rules

Network interfaces Inbound Security Rules

Subnets Outbound Security Rules

Properties Inbound Security Rules

Locks Outbound Security Rules

Monitoring Inbound Security Rules

Automation Outbound Security Rules

Help Inbound Security Rules

Table View

Priority Name Port Protocol Source Destination Action

Inbound Security Rules

Priority	Name	Port	Protocol	Source	Destination	Action
300	RD	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
65002	DenyAllInbound	Any	Any	Any	Any	Deny

Outbound Security Rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutbound	Any	Any	Any	Internet	Allow
65002	DenyAllOutbound	Any	Any	Any	Any	Deny

Microsoft Azure Upgrade

Home > Network security groups > Default Directory

InsightScapeVM2nsg120 Network security group

+ Create Manage view ...

Filter for any field... Search resources, services, and docs (F1)

Overview Custom security rules : 3 inbound, 0 outbound

Resource group **insightScapeRG** Associated with : 0 subnets, 1 network interface

Location : West US 2 Subscription **free Trial**

Subscription ID : c9e1c794-6d1b-40ff-9312-d5ba0d8e9400

Tags Add tags

Essentials

Inbound security rules Outbound security rules

Subnets Properties

Locks Monitoring

Help Automation

Settings

Inbound security rules Outbound security rules

Network interfaces Inbound Security Rules

Subnets Outbound Security Rules

Properties Inbound Security Rules

Locks Outbound Security Rules

Monitoring Inbound Security Rules

Automation Outbound Security Rules

Help Inbound Security Rules

Table View

Priority Name Port Protocol Source Destination Action

Inbound Security Rules

Priority	Name	Port	Protocol	Source	Destination	Action
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
65002	DenyAllInbound	Any	Any	Any	Any	Deny

Outbound Security Rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutbound	Any	Any	Any	Internet	Allow
65002	DenyAllOutbound	Any	Any	Any	Any	Deny

Page 1 of 1

Microsoft Azure | Upgrade

Network Watcher | NSG diagnostics

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 allowing status for the flow. Learn more... [\[?\]](#)

Target resource

Target resource type * Virtual machine * Selected virtual machine

Traffic details

Protocol Inbound Outbound

Source type * IP address/UDR Destination IP address * Destination port *

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-vm1174	Allow	View details

[Non-NSG diagnostic](#)

[Give feedback](#)

Microsoft Azure | Upgrade

Network security groups

InsightScape-VM1-nsg

Resource group: Location: West US 2 Subscription: Subscription ID: 1-2430764-6d1b-4e9b-9313-d3b9a03e4b00

Cotton security rules : 3 inbound, 0 outbound
Associated with: 0 virtual networks, 1 network interface

Overview

Essentials

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

- Inbound security rules
- Outbound security rules
- Network interfaces
- Subnets
- Properties
- Logs
- Monitoring
- Automation
- Help

Inbound Security Rules

Priority *	Name <input type="text" value=""/>	Port <input type="text" value="all"/>	Protocol <input type="button" value="TCP"/>	Source <input type="text" value="Any"/>	Destination <input type="text" value="Any"/>	Action <input type="button" value="Allow"/>	Protocol <input type="button" value="Any"/>	Source <input type="text" value="Any"/>
300	AllowRDP	3389	TCP	Any	Any	Allow	Any	Any
200	AllowHTTP	443	TCP	Any	Any	Allow	Any	Any
300	HTTP	80	TCP	Any	VirtualNetwork	Allow	Any	Any

Outbound Security Rules

Priority *	Name <input type="text" value=""/>	Port <input type="text" value="all"/>	Protocol <input type="button" value="TCP"/>	Source <input type="text" value="Any"/>	Destination <input type="text" value="Any"/>	Action <input type="button" value="Allow"/>	Protocol <input type="button" value="Any"/>	Source <input type="text" value="Any"/>
65000	AllowVNetOutbound	Any	TCP	Any	VirtualNetwork	Allow	Any	Any
65001	AllowAzureLoadBalancerOutbound	Any	TCP	Any	AzureLoadBalancer	Allow	Any	Any
65000	DenyAllOutbound	Any	TCP	Any	Any	Deny	Any	Any

HTTP

Source Source port range * Destination Destination port range * Service Protocol Any TCP UDP CMPP4 Action Allow Deny Priority * Name Description To rule device traffic from AzureLoadBalancer and may affect critical instance connectivity. To allow access, add an inbound rule with higher priority to a low-AzureLoadBalancer in VirtualNetworks.

[Save](#) [Cancel](#) [Give feedback](#)

Microsoft Azure | Upgrade

Home > Network security groups

Network security group

Overview

Resource group: insightScape RG | Location: West US 2 | Subscription: true | Subscriptions ID: chuloh4-edbb-4018-9312-d5ba0e9a50

Custom security rules: 3 inbound, 0 outbound
Associated with: 0 subnets, 1 network interface

Filter for any field... Name: ...

Creates Manage view

Access control (IAM) Tags

Diagnostic and solve problems

Settings

- Inbound security rules
- Outbound security rules
- Network interfaces
- Properties
- Locks
- Monitoring
- Automation
- Help

Add tags

Filter by name	Port	Protocol	Source	Destination	Action
Priority: 300	443	TCP	Any	Any	Allow
320	80	TCP	Any	Any	Allow
330	443	HTTP	Any	Any	Deny
65000	AllowInbound	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowOutbound	Any	AzureLoadBalancer	Any	Allow
65002	DenyAllInbound	Any	Any	Any	Deny
65003	AllowInbound	Any	VirtualNetwork	VirtualNetwork	Allow
65004	AllowOutbound	Any	Any	Internet	Allow
65005	DenyAllOutbound	Any	Any	Any	Deny

Page 1 of 1

Microsoft Azure | Upgrade

Home > Network Watcher

Network Watcher | NSG diagnostics

Overview

Get started

Monitoring

- Topology
- Connection monitor
- Traffic Analytics

Network diagnostic tools

- IP flow verify
- NSG diagnostics
- Host hap
- Effective security rules
- VPN troubleshooting
- Packet capture
- Connection troubleshooting
- Metric
- Logs
- Flow logs
- Migrate flow logs
- Diagnostic logs

NSG diagnostics

The Network Security Group Diagnostic tool provides detailed information to understand and debug the security configuration of your network. For a given source-destination pair, network security group diagnostic returns all relevant configurations that will be traversed, the rules that will be applied in each network security group, and the final allowance status for the flow (allow/deny).

Target resource

Target resource type: Virtual machine
Virtual machine: insightScape-VM1
Select virtual machine

Traffic details

Protocol: TCP
Direction: Inbound
Source type: IPv4 address/CDR
IPv4 address/CDR: 10.1.1.0
Destination IP address: 13.27.137.180
Destination port: 80

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-vm114	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

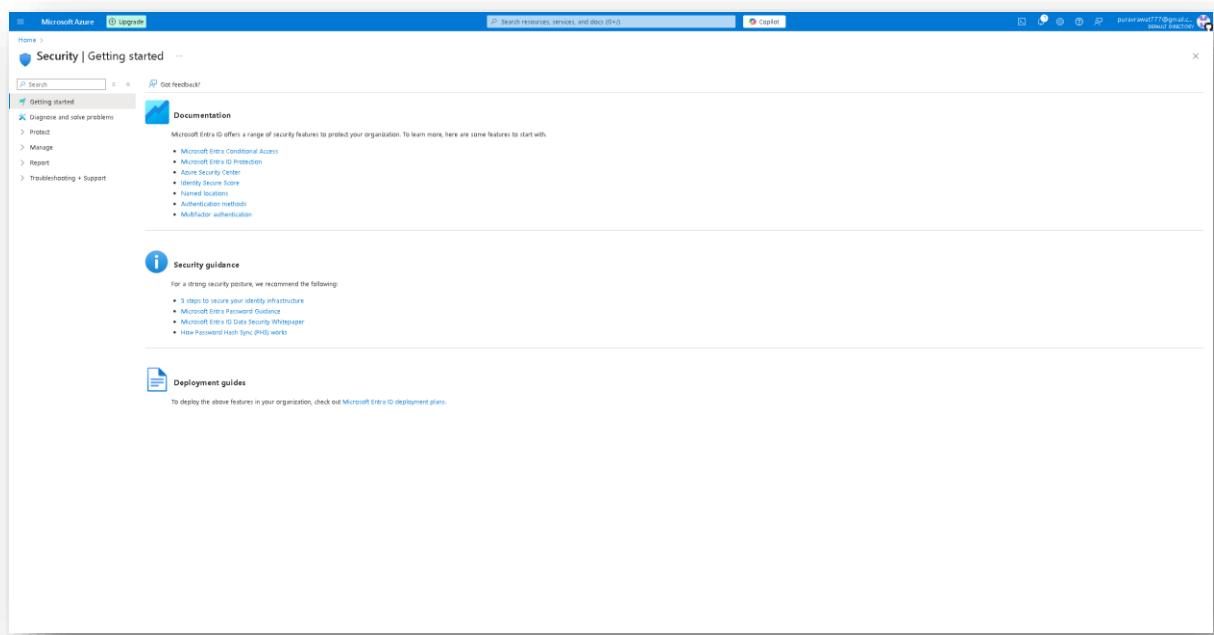
Lastly, I accessed the Security Alerts tab in Microsoft Defender for Cloud:

- 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

Home > Security

Security | Security Center

Getting started

Diagnose and solve problems

Protect

- Conditional Access
- Identity Protection
- Security Center**
- Verified ID
- Manage
- Report
- Troubleshooting + Support

Visit Microsoft Defender for Cloud to manage security across your virtual networks, data, apps, and more.

Recommendations by severity

High	Medium	Low
0	0	0

Alerts by severity

High	Medium	Low
0	0	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 to enhanced security, including

- Just-in-Time access, which reduces your exposure to network attacks
- Identity protection, which monitors user activity across all your applications
- Threat detection using advanced analysis and global threat intelligence
- Interactive mitigation tools and automated remediation for rapid response
- All in one place

[Try it free for the next 30 days](#)

Microsoft Azure | Upgrade

Home > Security | Security Center >

Microsoft Defender for Cloud | Overview

Showing subscription: Free Trial

Search

Subscriptions What's new

You may be viewing limited information. To get tenant-wide visibility, click here →

General

- Overview
- Getting started
- Recommendations
- Attack path analysis
- Security alerts
- Inventory
- Cloud Security Explorer
- Workbooks
- Community
- Diagnose and solve problems
- Cloud Security
- Management

Azure subscriptions

Assessed resources

Attack paths

Security alerts

Security posture

Critical recommendations: 0

Attack paths: 0

Override recommendations: 0/0

Environment risk and score score: 55%

Total secure score: 55%

Explore your security posture >

Regulatory compliance

Microsoft cloud security benchmark: 50 of 63 compliant

Latest compliance standards by control period: 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 anti-malware, container security features, multi-factor protection, and other advanced security features, enable all Defender plans for your subscriptions.

[Enable Defender plans](#)

Inventory

Total Resources: 7

Unhealthy (1) Healthy (0) Not applicable (0)

Explore your resources >

Action required: enable XDK and Agentless scanning to be ready for Log Analytics agent retirement

Toward end-of-Agentless Agent (EAA) retirement on November 2023, we recommend ensuring both Agentless machine scanning and MSE 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 CSM

CIDR empowers security admins to identify overprivileged, unused and super identities to facilitate the implementation and enforcement of least privilege across multi-cloud environments. Explore the CIDR 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 CSM plan

Defender Cloud Identity Protection Management (CIDR) provides enhanced privilege management and a new intelligent threat hunting graph to help identify, prioritize, and reduce risk. Defender CSM is available in addition to the free foundational security posture capabilities turned on by default in Defender for Cloud.

[Click here to upgrade >](#)

Microsoft Defender for Cloud | Inventory

Showing information: Free Trial

Search: Refresh Open query Download CSV report Guides & Feedback

Defender CSPM plan is now available. This plan provides enhanced feature capabilities and a new intelligent cloud security graph to help identify, prioritize and reduce risk. Upgrade to Defender CSPM.

Overview Getting started Recommendations Attack path analysis Security alerts Inventory Cloud Security Explorer Workbooks Community Diagnose and solve problems Cloud Security Management

Total resources Unhealthy resources Resource count by environment

Resource name	Resource type	Scope	Environment	Defender for Cloud	Recommendations
0132f74e-60bb-4f88-9312-d38a0d0e100	Subscription	Free Trial	Azure	Off	Medium
INSIGHTSCAPE-VM2	Virtual machine	Free Trial	Azure	Off	Medium
INSIGHTSCAPE-VM1	Virtual machine	Free Trial	Azure	Off	Medium
Insightescapestorage	Storage account	Free Trial	Azure	Off	Medium
Insightescape-Webapp	App Service	Free Trial	Azure	Off	Medium
Insightescape-LogicApp	Logic App	Free Trial	Azure	Off	Medium
Insightescape-Vnet	Virtual network	Free Trial	Azure	Off	Medium

Microsoft Defender for Cloud | Recommendations

Showing information: Free Trial

Search: Refresh Download CSV report Open query Governance report Guides & Feedback Switch to classic view

We are listening 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 Azure DevOps connectors 0 GitLab connectors 0 Docker Hub connectors 0

Defender CSPM Risk-based recommendations Other metrics Active attack paths Overall recommendations

Risk level: 0 Critical 0 High 0 Medium 0 Low

Foundational CSPM Recommendations 24 No risk isolated

Group by title

Title	Affected resource	Risk level	Risk factors	Attack paths	Owner	Status	Insights
Windows virtual machines should enable Azure Disk Encryption or EncryptBLOBs.	insightescape-vm1	Not evaluated	0	0	0	Unassigned	0
Virtual machines and virtual machine scale sets should have encryption at host level.	insightescape-vm2	Not evaluated	0	0	0	Unassigned	0
Virtual machines and virtual machine scale sets should have encryption at host level.	insightescapestorage	Not evaluated	0	0	0	Unassigned	0
Subscriptions should have a central email address for security issues.	0132f74e-60bb-4f88-9312-d38a0d0e100	Not evaluated	0	0	0	Unassigned	0
Storage accounts should restrict network access using virtual network rules.	insightescapestorage	Not evaluated	0	0	0	Unassigned	0
Storage accounts should present shared key access.	insightescapestorage	Not evaluated	0	0	0	Unassigned	0
Storage account should use a private link connection.	insightescapestorage	Not evaluated	0	0	0	Unassigned	0
Microsoft Defender for Servers should be enabled.	0132f74e-60bb-4f88-9312-d38a0d0e100	Not evaluated	0	0	0	Unassigned	0
Microsoft Defender for Storage plan should be enabled with Malware Scanning and ...	0132f74e-60bb-4f88-9312-d38a0d0e100	Not evaluated	0	0	0	Unassigned	0
Microsoft Defender for Resource Manager should be enabled.	0132f74e-60bb-4f88-9312-d38a0d0e100	Not evaluated	0	0	0	Unassigned	0
Microsoft Defender for App Service should be enabled.	0132f74e-60bb-4f88-9312-d38a0d0e100	Not evaluated	0	0	0	Unassigned	0
Microsoft Defender CSPM should be enabled.	0132f74e-60bb-4f88-9312-d38a0d0e100	Not evaluated	0	0	0	Unassigned	0
Managed identity should be used in web apps.	insightescape-webapp	Not evaluated	0	0	0	Unassigned	0
Machines should be configured to periodically check for missing system updates.	insightescape-vm1	Not evaluated	0	0	0	Unassigned	0
Machines should be configured to periodically check for missing system updates.	insightescape-vm2	Not evaluated	0	0	0	Unassigned	0
Linux virtual machines should enable Azure Disk Encryption or EncryptBLOBs.	insightescape-vm2	Not evaluated	0	0	0	Unassigned	0
Guest Configuration extension should be installed on machines.	insightescape-vm2	Not evaluated	0	0	0	Unassigned	0
Guest Configuration extension should be installed on machines.	insightescape-vm1	Not evaluated	0	0	0	Unassigned	0
Email notification to subscription owner for high severity alerts should be enabled.	0132f74e-60bb-4f88-9312-d38a0d0e100	Not evaluated	0	0	0	Unassigned	0
Email notification for high severity alerts should be enabled.	0132f74e-60bb-4f88-9312-d38a0d0e100	Not evaluated	0	0	0	Unassigned	0
Diagnostic logs in Logic Apps should be enabled.	insightescape-logicapp	Not evaluated	0	0	0	Unassigned	0
Diagnostic logs in App Service should be enabled.	insightescape-webapp	Not evaluated	0	0	0	Unassigned	0

Microsoft Azure | **Upgrade**

Home > Virtual machines > InsightScape-VM2

Virtual machines

+ Create | Switch to classic | ...

Filter for any field... Name: ...

... Insights Scope

InsightScape-VM1

InsightScape-VM2

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

> Connect

> Networking

Settings

- Disk
- Application
- Operating system
- Configuration
- Advisor recommendations
- Properties
- Locks

> Availability + scale

> Security

> Backup + disaster recovery

Operations

- Auto-shutdown

Run command

Updates

- Health monitoring
- Configuration management
- Polices
- Inventory
- Change tracking

Monitoring

- Insights
- Alerts
- Metrics
- Diagnostic settings
- Logs
- Workbooks

Page 1 of 1

InsightScape-VM2 | Updates

Search resources, services, and docs (S+I) | Copy

Manage VM Update at scale with the new Azure Update Manager experience. Try it now →

There is no assessment data 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 Classification: All selected

Update name Classifications Version

No assessment data found for the machine. Please check for updates.

Open query >

Microsoft Azure | **Upgrade**

Home > Disks > InsightScape-VM1_OsDisk_1_b355cb84eeb7418082014773d0e862c2

Disks

+ Create | Manage view | ...

Filter for any field... Name: ...

... Insights Scope

InsightScape-VM1_OsDisk_1_b355cb84eeb7418082014773d0e862c2

InsightScape-VM2_OsDisk_1_b32757...

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

> Configuration

> Size + performance

Encryption

> Networking

> Disk export

> Properties

> Locks

> Monitoring

> Automation

> Help

Page 1 of 1

InsightScape-VM1_OsDisk_1_b355cb84eeb7418082014773d0e862c2 | Encryption

Search resources, services, and docs (S+I) | Copy

Successfully updated disk InsightScape-VM1_OsDisk_1_b355cb84eeb7418082014773d0e862c2.

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

Storage accounts should restrict network access using virtual network rules

This insight 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	Firewall
Free Trial	30 Min

Last change date

Owner

Ticket ID

Risk factors

Description

The insight 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.

Take action

Take one of 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 network. 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.

Exempt

Exempt the entire recommendation, or disable specific findings using disable rules. Exempted resources appear as not applicable and do not affect secure score.

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

Was this recommendation useful? Yes No

inscapescapestorage | Networking

Firewalls and virtual networks

Firewall settings: Reducing access to storage services will remain in effect for up to 4 hours 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 range to allow access from the internet or your on-premises networks. Learn more.

Add your client IP address ("10.228.4.103")

Address range

IP address or CIDR

Reverse instances

Specify resource instances that will have access to your storage account based on their system-assigned managed identity.

Resource type

Select a resource type

Instance name

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 method: Microsoft routing

- 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

Virtual network **Service endpoint status**

Virtual network	Service endpoint	status
VM1-Subnet	Not enabled	...
VM2-Subnet	Not enabled	...

Save

Microsoft Azure | Upgrade

inscapescapestorage | Networking

Storage accounts

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

Favorites and quick links

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 5 minutes after saving updated settings allowing access.

Public network access

- Disabled 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	
InsightScope-VNet	2	VM1/Subnet	10.11.0.0/24	✓ Enabled	InsightScope-RG	Free Trial
		VM2/Subnet	10.12.0.0/24	✓ Enabled	InsightScope-RG	Free Trial
					InsightScope-RG	Free Trial

Firewall

Allow traffic to allow access from the Internet or your on-premises networks. Learn more ↗

Add your client IP address (192.236.4.193) ↗

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

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

Routing via specific endpoints ↗

Microsoft network routing Internet routing

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

Routing via specific endpoints ↗

Microsoft network routing Internet routing

Microsoft Azure | Upgrade

Home > Microsoft Defender for Cloud

Showing subscription: Free Trial

Microsoft Defender for Cloud | Security posture

Secure score over time Governance report Guides & feedback

Search

General

- Overview
- Getting started
- Recommendations
- Attack path analysis
- Security alerts
- Inventory
- Cloud Security Explorer
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Cloud Security posture
- Regulatory compliance
- Workload protection
- Data security
- Firewall Manager
- DevOps security
- Management
- Environment settings
- Security solutions
- Workflow automation

Azure environment

Secure score: 59% Total secure score

Environment risk: 0 Critical recommendations, 0 Attack paths

Governance

Assign ownership and other roles to your organization 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 Enrichment == All

Name	Secure score	Unhealthy resources	Attack paths	Recommendations
Free Trial - Azure subscription	59%	3 of 6	0	View recommendations ↗

Page 1 of 1 Next >

Give us feedback

Microsoft Azure Microsoft Defender for Cloud

Microsoft Defender for Cloud | Security alerts

Showing 1000 results for "Security alerts"

83 Open alerts 83 Active alerts 0 In progress alerts 13 Affected resources

Open alerts by severity: High (38), Medium (65), Low (9)

Search by ID, IP, name, or affected resource

Subscription == All Status == Active, In Progress Severity == Low, Medium, High Add filter

Severity	Alert name	Affected resource	Resource Group	Activity start time (UTC+0)	Last updated time (UTC+0)	MITRE ATT&CK® tactics	Status
High	Potential malware uploaded to a storage file...	Sample alert	Sample Storage	10/21/24, 09:05 PM	10/21/24, 09:07 PM	Lateral Movement	Active
High	Suspicious successful brute force attack...	Sample alert	Sample VM	10/21/24, 09:06 PM	10/21/24, 09:07 PM	Pre-attack	Active
High	Publicly accessible storage container unsec...	Sample alert	Sample Storage	10/21/24, 09:05 PM	10/21/24, 09:07 PM	Lateral Movement	Active
High	Potential malware uploaded to a storage fi...	Sample alert	Sample Storage	10/21/24, 09:05 PM	10/21/24, 09:07 PM	Execution	Active
High	Digital currency mining related behavior de...	Sample alert	Sample VM	10/21/24, 09:06 PM	10/21/24, 09:07 PM	Defense Evasion	Active
High	Detected suspicious file cleanup command...	Sample alert	Sample VM	10/21/24, 09:06 PM	10/21/24, 09:07 PM	Initial Access	Active
High	Access from a suspicious IP...	Sample alert	Sample-AzureCompute@GlobalAccount	10/21/24, 09:04 PM	10/21/24, 09:07 PM	Pre-attack	Active
High	Attempted login by a potentially harmful IP...	Sample alert	Sample VM	10/21/24, 09:06 PM	10/21/24, 09:07 PM	Initial Access	Active
High	HEVEIN - Access from a suspicious applicat...	Sample alert	Sample Storage	10/21/24, 09:05 PM	10/21/24, 09:07 PM	Collection	Active
High	Whaling content hosted on Abuse Webhooks...	Sample alert	Sample App	10/21/24, 09:07 PM	10/21/24, 09:07 PM	Pre-attack	Active
High	Suspected brute-force attack attempt...	Sample alert	Sample GDI	10/21/24, 09:07 PM	10/21/24, 09:07 PM	Pre-attack	Active
High	Access from a suspicious IP to a storage fil...	Sample alert	Sample Storage	10/21/24, 09:05 PM	10/21/24, 09:07 PM	Pre-attack	Active
High	Potential SQL injection...	Sample alert	Sample GDI	10/21/24, 09:07 PM	10/21/24, 09:07 PM	Exfiltration	Active
High	Unusual volume of data extracted...	Sample alert	Sample-AzureCompute@GlobalAccount	10/21/24, 09:04 PM	10/21/24, 09:07 PM	Pre-attack	Active
High	API Endpoint access from suspicious IP...	Sample alert	Sample API-Operation	10/21/24, 09:07 PM	10/21/24, 09:07 PM	Initial Access	Active
High	Suspicious WordPress theme invocation dete...	Sample alert	Sample App	10/21/24, 09:07 PM	10/21/24, 09:07 PM	Pre-attack	Active
High	Potential SQL injection...	Sample alert	Sample VM	10/21/24, 09:06 PM	10/21/24, 09:07 PM	Pre-attack	Active
High	Unusual number of files extracted from a da...	Sample alert	Sample Storage	10/21/24, 09:05 PM	10/21/24, 09:07 PM	Exfiltration	Active
High	Unusual amount of data extracted from a da...	Sample alert	Sample Storage	10/21/24, 09:08 PM	10/21/24, 09:07 PM	Exfiltration	Active
High	Access from a Tor exit node to a storage fil...	Sample alert	Sample Storage	10/21/24, 09:05 PM	10/21/24, 09:07 PM	Initial Access	Active

< Previous Page 1 of 3 Next >

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-

This screenshot shows the Microsoft Azure Monitor Alerts dashboard. The left sidebar includes links for Overview, Activity log, Alerts, Metrics, Logs, Change Analysis, Service Health, Workbooks, and Support + Troubleshooting. The main area displays alert statistics: Total alerts (0), Critical (0), Error (0), Warning (0), Informational (0), and Verbose (0). Below this, there are filters for Subscription (selected), Time range (Past 24 hours), Alert condition (Fixed), Severity (all), and Grouping (No grouping). A central message states "No alerts found" with a note to "Try changing your search or choose a different scope level if you don't see what you're looking for." A "Clear filters" button is also present.

This screenshot shows the "Create an alert rule" wizard in Microsoft Azure. The top navigation bar includes Home, Monitor, Alerts, Create, Alert rules, Alert groups, Alert processing rules, Prometheus rule groups, Change user response, Actions, Refresh, and Copy. The main steps are Scope, Condition, Actions, Details, Tags, Review + create. The "Condition" step is active, showing a signal name dropdown set to "Custom log search". Below it, a search query editor contains the query: `SecurityEvent | where EventID == 4625`. The "Measurement" section allows summarizing results by selecting a measure (EventID), aggregation type (Total), and granularity (5 minutes). The "Alert logic" section defines the trigger conditions: Operator (Greater than), Threshold value (1), and Frequency of evaluation (5 minutes). A note indicates an estimated monthly cost of \$1.59 USD. Navigation buttons at the bottom include "Review + create", "Previous", and "Next: Actions >".

Microsoft Azure (Upgrade)

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](#)

Name	Condition	Severity	Target scope	Target resource type	Signal type	Status
<input checked="" type="checkbox"/> FailedLoginDetection	EventID > 1	! - Error	insightscape-VM1	Virtual machine	Log search	Enabled
<input type="checkbox"/> High CPU Usage Alert in VM1	Percentage CPU > 50	! - Warning	insightscape-vm1	Virtual machine	Metrics	Enabled

Showing 1 - 2 of 2 results.

[Give feedback](#)

Microsoft Azure (Upgrade)

Home > Monitor | Alerts > Alert rules

[+ Create](#) [View as timeline \(grouped\)](#) [Subscription: Free Trial](#) [Time range: Past 24 hours](#) [Severity: all](#) [Add filter](#)

Total alerts: Critical: 0 Error: 0 Warning: 1 Informational: 0 Verbose: 0

Name	Severity	Affected resource	Alert condition
<input checked="" type="checkbox"/> High CPU Usage Alert in VM1	! - Warning	insightscape-vm1	Resolved

High CPU Usage Alert in VM1

[Copy link](#) [Go to alert rule](#) [Investigate \(preview\)](#)

Summary **History**

General details

Severity	Fire time	Affected resource	Monitor service	Alert condition	User response
2 - Warning	10/21/2024, 10:56 PM	insightscape-vm1	Platform	Resolved	New

Why did this alert fire?

The average Percentage CPU exceeded the threshold of 50% and reached 75%.

Value when alert fired: Threshold: Duration: 75%

Average CPU Avg: 4.0118 s

> Additional details

(Showing 1 - 1 of 1 results.)

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-

This screenshot shows the Microsoft Azure Recovery Services vault overview page for the 'InsightScape-Vault' resource. The left sidebar contains navigation links for Overview, Backup, Site Recovery, Settings, Getting started, Protected items, Manage, Monitoring, Alerts, Metrics, Diagnostic settings, Advisor recommendations, Backup jobs, Site Recovery jobs, Backup alerts, Site Recovery events, Automation, and Help. The main content area displays a 'What's new' section with several bullet points about Azure Site Recovery support, SAP HANA Database backup, and Cross Subscription Restore. Below this is a 'Backup' section with links to Getting started, Backup dashboard, Backup items, Backup policies, Backup reports, and Backup Explorer. A 'Site Recovery' section follows, with links to Getting started, Site Recovery dashboard, Replicated items, Manage Recovery Plans, and Learn more. At the bottom, there is a 'Page 1 of 1' navigation bar.

This screenshot shows the Microsoft Azure Recovery Services vault backup items page for the 'InsightScape-Vault' resource. The left sidebar is identical to the previous screenshot. The main content area displays a table titled 'BACKUP MANAGEMENT TYPE' and 'BACKUP ITEM COUNT'. The table lists the following items:

BACKUP MANAGEMENT TYPE	BACKUP ITEM COUNT
More Virtual Machine	1
More Backup Agent	0
Azure Backup Server	0
DRM	0
Azure Storage (Azure File)	0
SQL Database in Azure VM	0
SAP HANA in Azure VM	0

At the bottom, there is a 'Page 1 of 1' navigation bar.

Backup Items (Azure Virtual Machine)

All data fetched from the service.

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

Filter items ...

Page 1 of 1

Virtual machines

InsightScape VM1

This action will permanently delete this virtual machine.

Resource to be deleted

Resource type	Quantity
Virtual machine	1

Associated resource type

Quantity	Delete with VM
1	<input type="checkbox"/>
1	<input type="checkbox"/>
1	<input type="checkbox"/>

Properties

Computer name: InsightScape-VM
Operating system: Windows
VM generation: V2
VM architecture: x64
Maintenance: Enabled
Host group: -
Host: -
Priority placement group: -
Placement status: NgA
Capacity reservation group: -
Disk controller type: SCSI

Network

Public IP: -
Private IP: -
Virtual IP: -
DNS name: -

Size

Size: vCoreS1
vCPUs: 1
RAM: 2 GiB

Source VM

Source VM: -
Source ID: -

Data

OS disk: -
Data disk: -
Encryption: -
Azure disk: -
Ephemeral: -
Data disk: -

Auto shutdown

Schedule: -

I have read and understood that this virtual machine as well as any selected associated resources listed above will be deleted.

[Delete](#) [Cancel](#)

Microsoft Azure (Upgrade)

Home > Virtual machines

Virtual machines

InsightScape-VM1

Overview

Not found

Summary

Session ID: f8abef0d5a242c197b30b19b031a7e

Resource ID: /subscriptions/cde3f744-6dbb-46ff-9312-d39a0d6fa...

Description: Microsoft_Azure_Compute

Error code: 404

Get support | Perform self-diagnostics

Activity log | Access control (IAM) | Tags | Diagnose and solve problems | Connect | Networking | Settings | Drives | 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

Page 1 of 1

Notifications

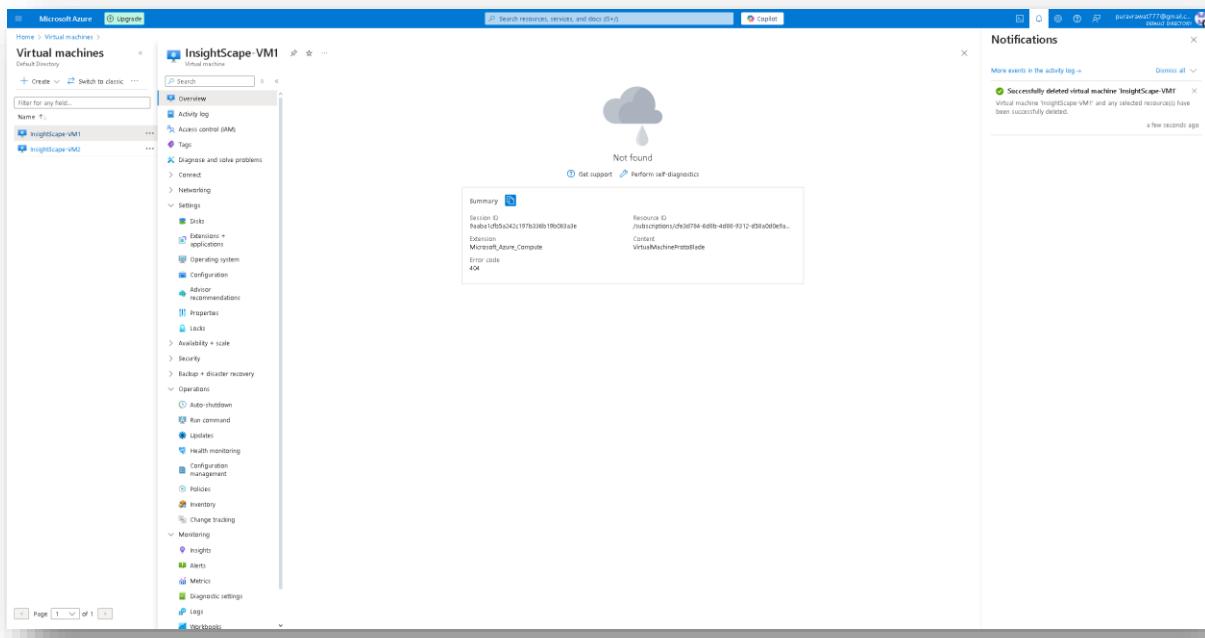
More events in the activity log →

Dismiss all

Successfully deleted virtual machine 'InsightScape-VM1'.

Virtual machine 'InsightScape-VM1' and any selected resources have been successfully deleted.

a few seconds ago



Microsoft Azure (Upgrade)

Home > Recovery Services vaults > InsightScape-Vault > Backup items

Backup Items (Azure Virtual Machine)

InsightScape-Vault

All data fetched from the service.

Filter items ...

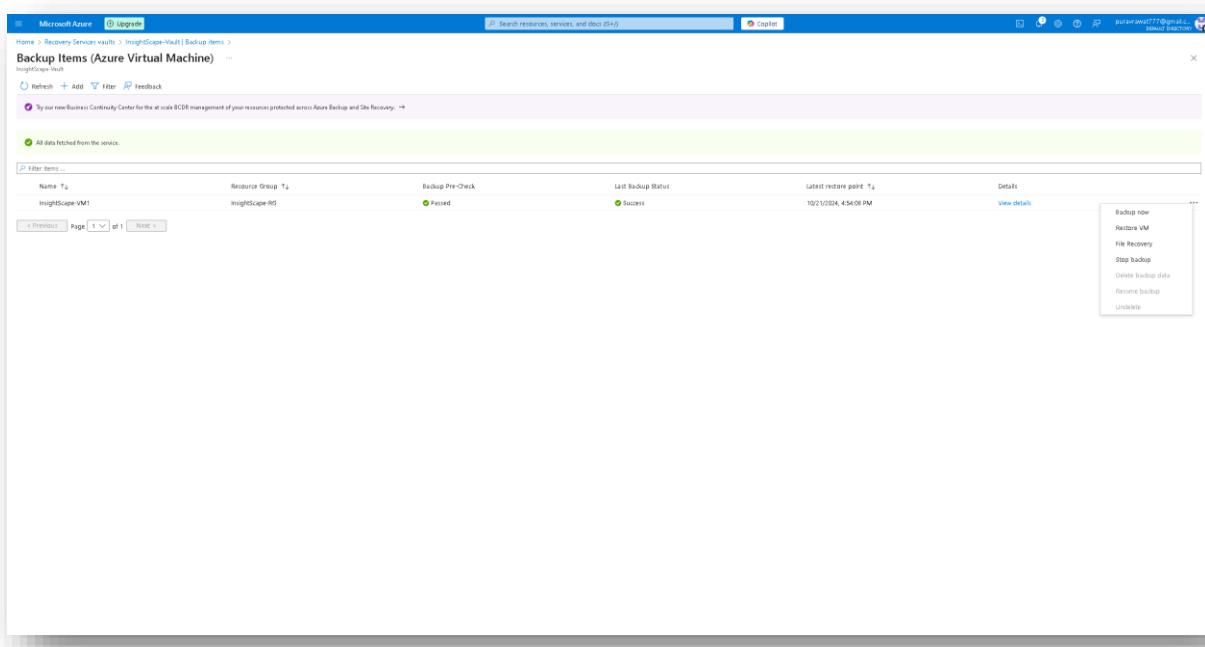
Name	Resource Group	Backup Pre-Check	Last Backup Status	Latest restore point	Details
InsightScape VM1	InsightScape-RG	Passed	Success	10/21/2024, 4:54:09 PM	View details

< Previous Page 1 of 1 Next >

By our new Business Continuity Center for the at-scale BCDR management of your resources protected across Azure Backup and Site Recovery. →

View details

Backup now | Restore VM | File Recovery | Stop backup | Delete backup data | Resume backup | Undelete



Microsoft Azure Upgrade

Home > Recovery Services vaults > InsightScope-Vault | Backup items > Backup Items (Azure Virtual Machine) > Restore Virtual Machine

Restore allows you to restore VM disks from a selected Restore Point.

Restore point *

Data store

Restore configuration

Restore target Create new Replace existing

To create an alternate configuration when restoring your VM (from the following menu), use PowerShell cmdlets.

Restore Type * Create new virtual machine InsightScope VM - Restored

Virtual machine name *

Subscription * Free Trial InsightScope RG

Resource group * InsightScope RG InsightScope-VNet (InsightScope RG)

Virtual network * VM1-Subnet VM2-Subnet

Subnet * VM1-Subnet VM2-Subnet

Staging Location * insightscopepetrorage (StandardRS) Can't find your storage account?

Assign an MSI with the [opt-in permission](#), for automated cleanup on restore failure. Without an MSI, manual intervention is required.

Identities Disabled

Give feedback

Microsoft Azure Upgrade

Home > Recovery Services vaults > InsightScope-Vault | Backup items > Backup Items (Azure Virtual Machine) > Restore Virtual Machine

Restore allows you to restore VM disks from a selected Restore Point.

Restore point *

Data store

Restore configuration

Restore target Create new Replace existing

To create an alternate configuration when restoring your VM (from the following menu), use PowerShell cmdlets.

Restore Type * Create new virtual machine InsightScope VM - Restored

Virtual machine name *

Subscription * Free Trial InsightScope RG

Resource group * InsightScope RG InsightScope-VNet (InsightScope RG)

Virtual network * VM1-Subnet VM2-Subnet

Subnet * VM1-Subnet VM2-Subnet

Staging Location * insightscopepetrorage (StandardRS) Can't find your storage account?

Assign an MSI with the [opt-in permission](#), for automated cleanup on restore failure. Without an MSI, manual intervention is required.

Identities Disabled

Give feedback

Microsoft Azure | Log In

Home > Recovery Services vaults > InsightScape-Vault Backup items > **Backup Items (Azure Virtual Machine)**

By 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

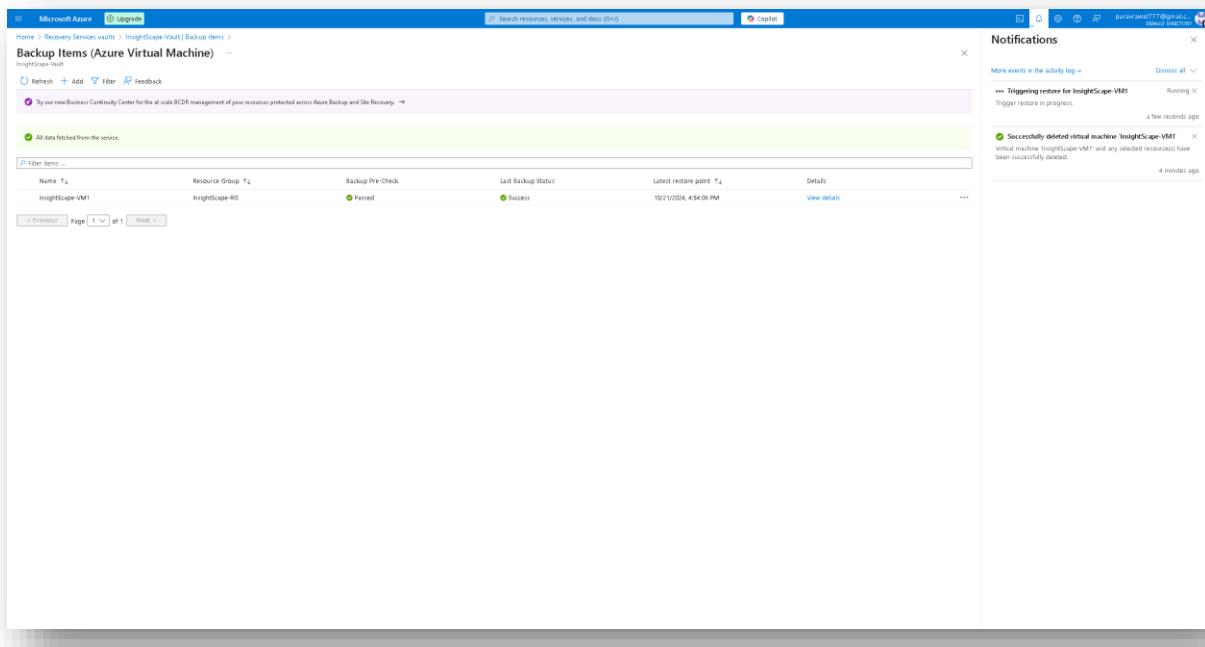
< Previous Page 1 of 1 Next >

Notifications

More events in the activity log →

... Triggering restore for InsightScape-VM1 Running X
Trigger restore in progress.
A few seconds ago

Successfully deleted virtual machine InsightScape-VM1 X
Virtual machine InsightScape-VM1 and any selected resources have been successfully deleted.
4 minutes ago



Microsoft Azure | Log In

Home > Recovery Services vaults > **InsightScape-Vault**

Recovery Services ...

+ Create Manage view ...

Search

InsightScape-Vault

InsightScape-Vault

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings

Getting started

Predicted items

Backup items Replicated items

Manage

Monitoring

- Alerts Metrics Diagnostic settings Advisor recommendations

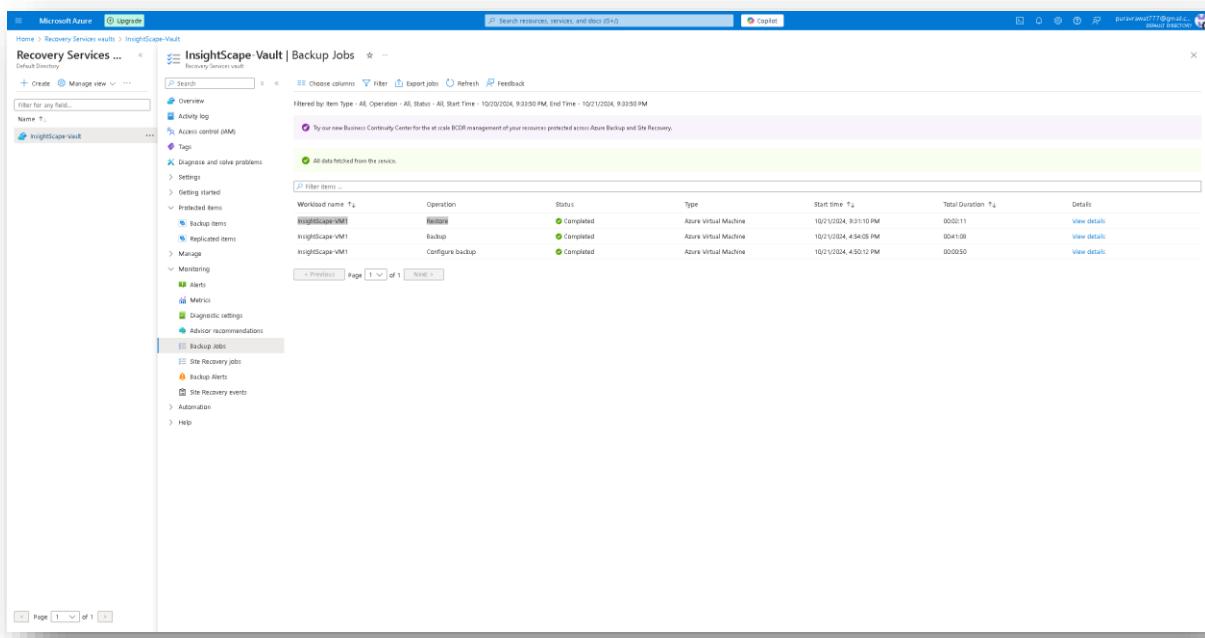
Backup jobs

Site Recovery jobs Backup Alerts Site Recovery events Automation Help

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	00:00:30	View details

Page 1 of 1



Microsoft Azure Upgrade

Virtual machines Overview

InsightScape-VM1-Restored

Name: InsightScape-VM1-Restored

Resource group: insightScape-RG

Status: Running

Location: West US 2

Subscription: free Trial

Subscription ID: 0de3f794-68b4-48ff-9312-d9fa06fe6e50

Operating system: Windows (Windows Server 2019 Datacenter)

Size: Standard B1s (1 vcpu, 1.68 memory)

Public IP address: 4.193.206.161

Virtual network/subnet: insightScape-VNet/VM1-Subnet

SND name: VM1-Subnet

Health state: 1

Time created: 10/21/2024, 4:02 PM UTC

JSON View

Tags: None

Add tags

Properties Monitoring Capabilities 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: 2.7.4493.1139

Host: -

Host group: -

Priority placement group: -

Calculation status: NgR

Capacity reservation group: -

Disk controller type: SCSI

Azure Spot

Azure Spot: -

Azure Spot eviction policy: -

Availability - scaling

Availability zone (v2B): -

Availability set: -

Scale Set: -

Security

Security type: Standard

Health monitoring

Health monitoring: Not enabled

Networking

Public IP address: 4.193.206.161 (Network interface InsightScape-VM1-Restored-HC-128954525d74fc00a7a2c2a411eb)

Public IP address (IPv6): -

Private IP address: 10.1.1.5

Private IP address (IPv6): -

Virtual network/subnet: insightScape-VNet/VM1-Subnet

DNS name: Configure

Size

Size: Standard B1s

vCPUs: 1

RAM: 1.68

Source image details

Source image publisher: -

Source image offer: -

Source image plan: -

Disk

OS disk: insightscaperestored-ardisk-20241021-16044

Encryption at host: Enabled

Azure disk encryption: Not enabled

Encryption on OS disk: N/A

Data disks: 0

Auto shutdown

Auto shutdown: Not enabled

Scheduled shutdown: -

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.

Skills measured

- Manage Azure identities and governance
- Implement and manage storage
- Deploy and manage Azure compute resources
- Implement and manage virtual networking
- Monitor and maintain Azure resources