CONTENTS

1. Agenda

The problem of an application failing to run correctly when moved from one environment to another is as old as software development itself. Such problems typically arise due to differences in configuration underlying library requirements and other dependencies.

Containers address this problem by providing a lightweight, immutable infrastructure for application packaging and deployment. An application or service, its dependencies, and its configuration are packaged together as a container image. The containerized application can be tested as a unit and deployed as a container image instance to the host operating system.

There are many options for teams to build and deploy cloud native and containerized applications on Azure. There are many options for teams to build and deploy cloud native and containerized applications on Azure.

In this task, you will get acquainted with the following Azure Container services:

- Azure Container Registry
- Azure Container Instance
- Web App for Containers
- Azure Container Apps
- Azure Kubernetes Service

Every Azure resource has pros and cons. There's no perfect solution for every use case and every team.

In this task we are asking you to build production design and reproduce the typical steps which you will be in touch working some Azure Container resources. In the task you need to automate provisioning for mentioned above azure resources by means of Terraform. You will build and deploy a simple application in these Azure services via Terraform as well.

Please use useful links to do your homework successfully

2. ACCEPTANCE CRITERIA

1. Homework corresponds to task details, requirements and attachment recommendations.
2. Terraform configuration has normal view and meets all requirements and best practices studied on previous modules.
3. Terraform configuration for each Azure resources must be as a module.
4. A tutor should be able to execute your Terraform configuration without modifications. Any hardcode that can affect re-run must be fixed. If your code is related some how to OS (or shell), inform about it your tutor and provide description why you did.
5. Minimal Terraform version is 1.5.0.
6. All resource names should use a common name pattern and be aligned with Azure abbreviation examples. No resource names are hardcoded
7. TF configuration has usable outputs, that are used to access to resources, such as storage account name, vault name, cdn endpoint, etc.

3. Task

1. Create Terraform configuration that provisions the following resources:
   a. Azure Redis Cache
   b. Azure Container Registry
   c. Azure Key Vault
2. Redis password and Redis Url must be saved in Key Vault as a secrets. Add in Terraform configuration block that builds Docker image using the Dockerfile provided below, and upload built image to Azure Container Registry. Any sensitive values (such as ACR admin key should be provided dynamically)
3. Update your Terraform configuration to create Azure Container Instance which will host a container from the image built earlier. All sensitive variables must be provided to ACI as secure_environment_variables (when it is possible).
   Define “CREATOR” variable for container with value “Azure_Container_Instance”

   Keep in mind that the Docker container works in pair with Azure Redis, and required parameters must be provided to container during the initialization (see app.py)

   Application must be accessible via HTTP/HTTPs from the internet.
4. Update your Terraform configuration to create Azure WebApp for Containers Instance which will host a container from the image built earlier. Sensitive variables for this WebApp must be stored in Azure KeyVault and provided to WebAPP during the container initialization (see useful links).
   Define “CREATOR” variable for container with value “Azure_Web_APP”.

   Application must be accessible via HTTP/HTTPs from the internet.
5. Update your Terraform configuration to create Azure Container APP Instance which will host a container from the image built earlier.
   Define “CREATOR” variable for container with value “Azure_Container_App”.

   Application must be accessible via HTTP/HTTPs from the internet.
6. Update your Terraform configuration to create Azure Kubernetes Service integrated with Azure KeyVault created above, and which will host a container from the image built earlier.
   Define “CREATOR” variable for container with value “K8S”.

   Pods in k8s should obtain secrets form KeyVault during the initialization. Use “Access with a user-assigned managed identity” approach. Optionally you can use Azure AD workload identity to get access to KeyVault instead of UMI.
7. Deploy the image built earlier to k8s. You can update your Terraform configuration to deploy Docker image(optionally) or just connect to k8s and deploy using k8s manifests. Sensitive variable must be stored in KeyVault in any case. Application must available from the internet at least via IP address.

4. TASK RESULT

A result of this task is a running applications on different Azure services such as ACI, WebAPP, Container APP and AKS that are available by IP address or URLs.

5. USEFUL LINKS

Dockerfile reference | Docker Docs

Provisioner: local-exec | Terraform | HashiCorp Developer

Quickstart - Create registry in portal - Azure Container Registry | Microsoft Learn

Welcome to Flask — Flask Documentation (2.3.x) (palletsprojects.com)

What is Azure Key Vault? | Microsoft Learn

What is Azure Cache for Redis? | Microsoft Learn

Quickstart: Create an Azure Container Instance with a public IP address using Terraform - Azure Container Instances | Microsoft Learn

Deploy and run a containerized web app with Azure App Service - Training | Microsoft Learn

Azure Container Apps overview | Microsoft Learn

Quickstart: Create an Azure Kubernetes Service (AKS) cluster by using Terraform - Azure Kubernetes Service | Microsoft Learn

null_resource | Resources | hashicorp/null | Terraform | Terraform Registry

azurerm_container_app - Cannot deploy container with ingress enabled · Issue #20435 · hashicorp/terraform-provider-azurerm · GitHub

Use Key Vault references - Azure App Service | Microsoft Learn

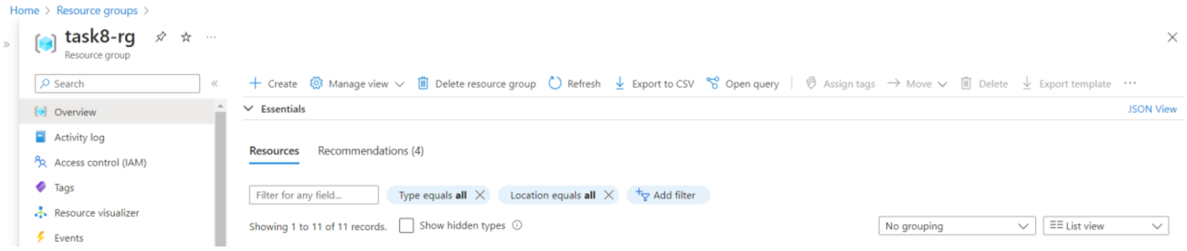
Use the Azure Key Vault Provider for Secrets Store CSI Driver for Azure Kubernetes Service (AKS) secrets - Azure Kubernetes Service | Microsoft Learn

Provide an access identity to the Azure Key Vault Provider for Secrets Store CSI Driver for Azure Kubernetes Service (AKS) secrets - Azure Kubernetes Service | Microsoft Learn

Provide an access identity to the Azure Key Vault Provider for Secrets Store CSI Driver for Azure Kubernetes Service (AKS) secrets - Azure Kubernetes Service | Microsoft Learn

Resource Group:

In Azure Cloud Resource Group is the primary thing we need to create to store all the resources . Create the Resource Group using Terraform modules. Click on GitHub Url to check the Module Source code: https://github.com/gmk1995/azure-terraform-modules



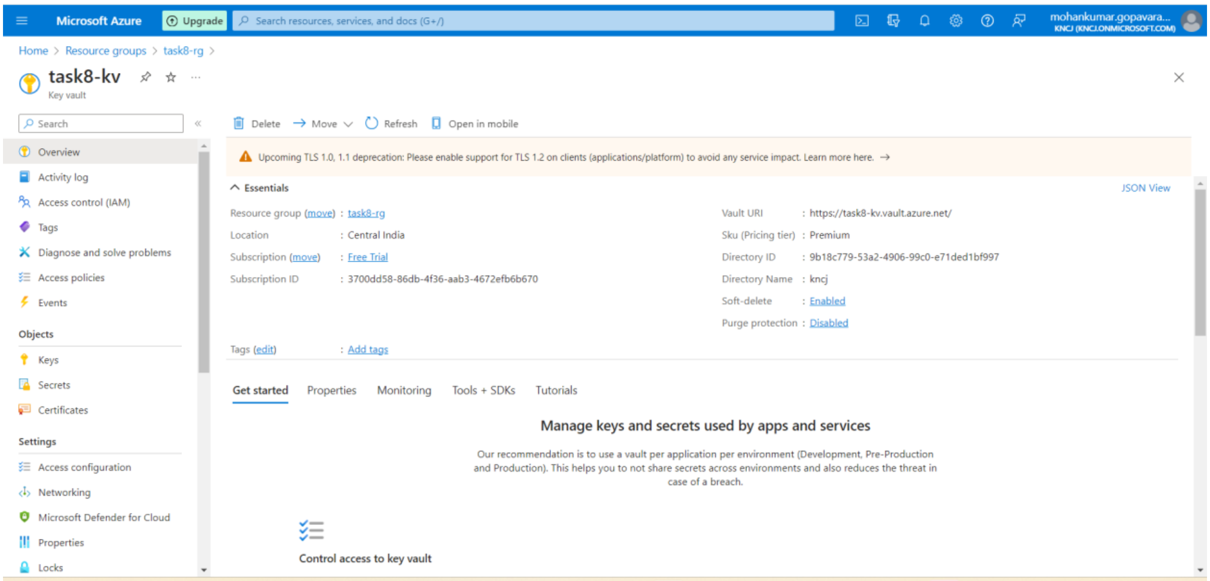
Type equals **all**

Location equals **all**

Showing 1 to 11 of 11 records. □ Show hidden types

Key Vault and Access Policies:

As Per Task we need to create the Key Vault to store Redis Cache Hostname and Access Keys. We need to create Access Policy also to access the key vault secrets. Click on below GitHub Url to access the Terraform Module source code: https://github.com/gmk1995/azure-terraform-modules



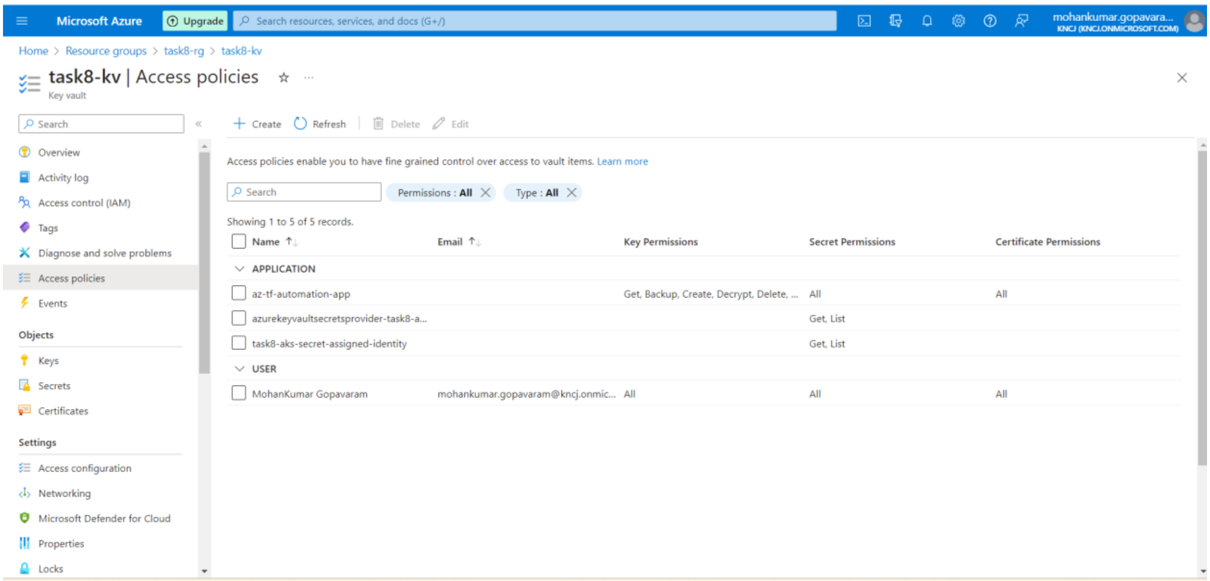
Upcoming TLS 1.0, 1.1 deprecation: Please enable support for TLS 1.2 on clients (applications/platform) to avoid any service impact. Learn more here. →

Essentials

Resource group (move)	task8-rg
Location	Central India
Subscription (move)	Free Trial
Subscription ID	3700dd58-86db-4f36-aab3-4672efb6b670
Vault URI	https://task8-kv.vault.azure.net/
Sku (Pricing tier)	Premium
Directory ID	9b18c779-53a2-4906-99c0-e71ded1bf997
Directory Name	kncj
Soft-delete	Enabled
Purge protection	Disabled
Tags (edit)	Add tags

Manage keys and secrets used by apps and services

Our recommendation is to use a vault per application per environment (Development, Pre-Production and Production). This helps you to not share secrets across environments and also reduces the threat in case of a breach.



Access policies enable you to have fine grained control over access to vault items. Learn more

Showing 1 to 5 of 5 records.

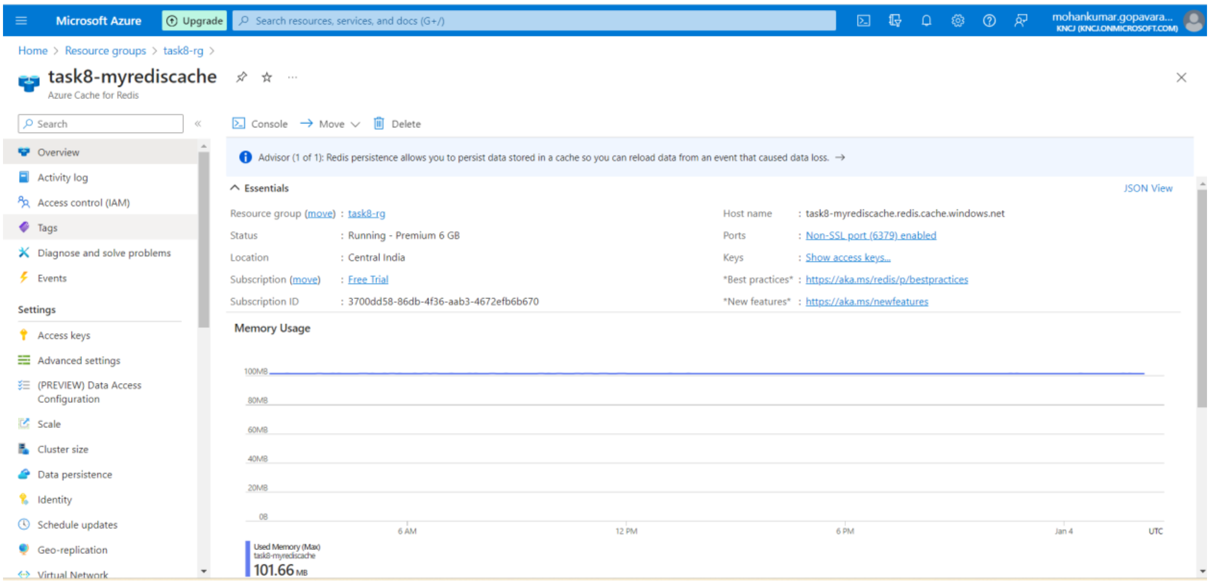
Name	Email	Key Permissions	Secret Permissions	Certificate Permissions
APPLICATION				
az-tf-automation-app		Get, Backup, Create, Decrypt, Delete, ...	All	All
azurekeyvaultsecretsprovider-task8-a...			Get, List	
task8-aks-secret-assigned-identity			Get, List	
USER				
MohanKumar Gopavaram	mohankumar.gopavaram@kncj.onmic...	All	All	All

Azure Redis Cache:

We need to create the Azure redis cache for store the cache memory of number of time we have visited the web app. Click on the below link to get the Terraform source code module.

https://github.com/gmk1995/azure-terraform-modules

Note: We have stored the Redis Hostname and Access Key on the Key vault Secrets using terraform code.

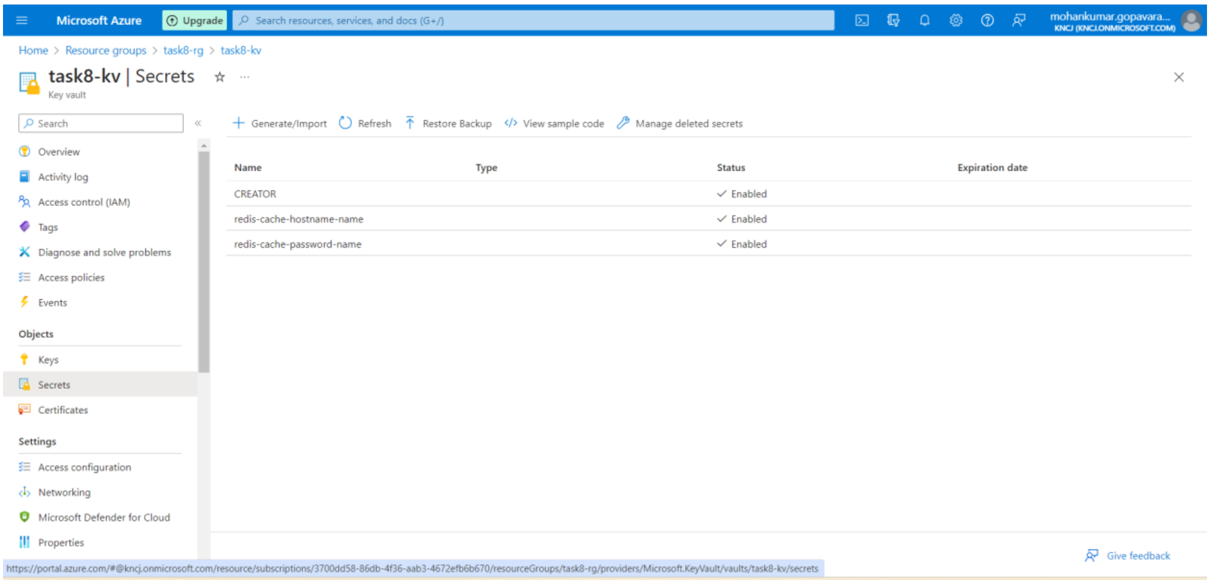


task8-myrediscache
Azure Cache for Redis

Advisor (1 of 1): Redis persistence allows you to persist data stored in a cache so you can reload data from an event that caused data loss. →

Resource group (move) : task8-rg
Status : Running - Premium 6 GB
Location : Central India
Subscription (move) : Free Trial
Subscription ID : 3700dd58-86db-4f36-aab3-4672efb6b670
Host name : task8-myrediscache.redis.cache.windows.net
Ports : Non-SSL port (6379) enabled
Keys : Show access keys...
Best practices : https://aka.ms/redis/p/bestpractices
New features : https://aka.ms/newfeatures

Azure Redis Cache Hostname and Access Key Stored in the Azure Key Vault Secret:



task8-kv | Secrets
Key vault

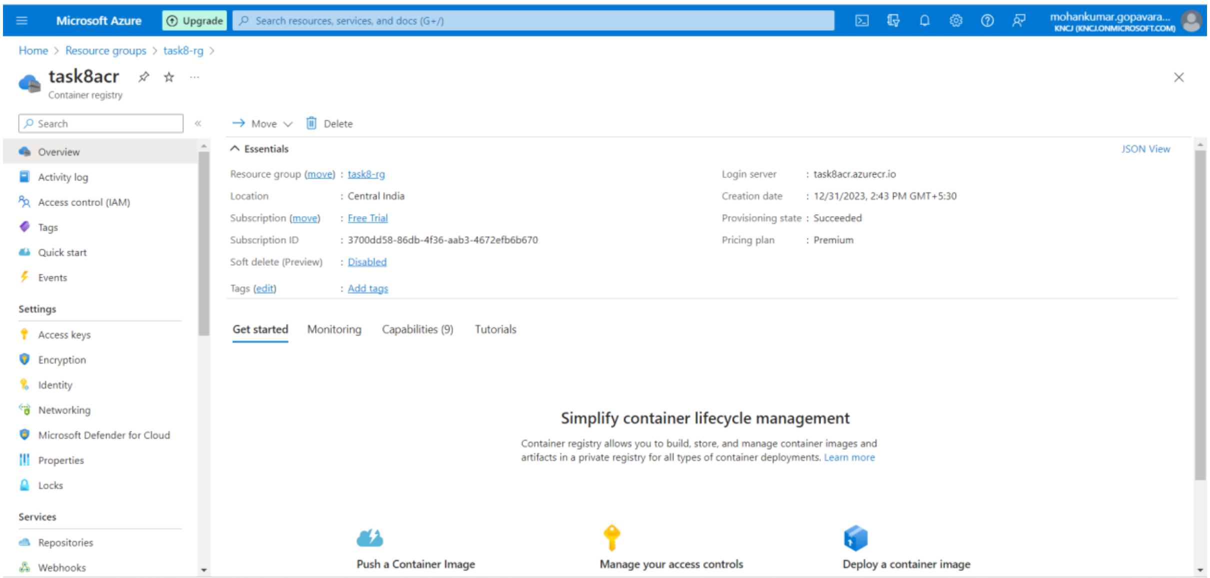
Name	Type	Status	Expiration date
CREATOR		✓ Enabled	
redis-cache-hostname-name		✓ Enabled	
redis-cache-password-name		✓ Enabled	

https://portal.azure.com/#@kncj.onmicrosoft.com/resource/subscriptions/3700dd58-86db-4f36-aab3-4672efb6b670/resourceGroups/task8-rg/providers/Microsoft.KeyVault/vaults/task8-kv/secrets

Azure Container Registry:

To store the images we need to create the Azure container registry using Terraform code. Click on the link to access the Terraform module source code:

https://github.com/gmk1995/azure-terraform-modules



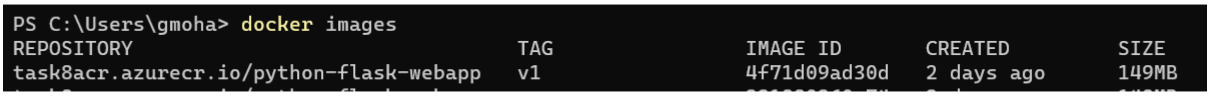
Resource group (move) : task8-rg
Location : Central India
Subscription (move) : Free Trial
Subscription ID : 3700dd58-86db-4f36-aab3-4672efb6b670
Soft delete (Preview) : Disabled
Tags (edit) : Add tags
Login server : task8acr.azurecr.io
Creation date : 12/31/2023, 2:43 PM GMT+5:30
Provisioning state : Succeeded
Pricing plan : Premium

Simplify container lifecycle management

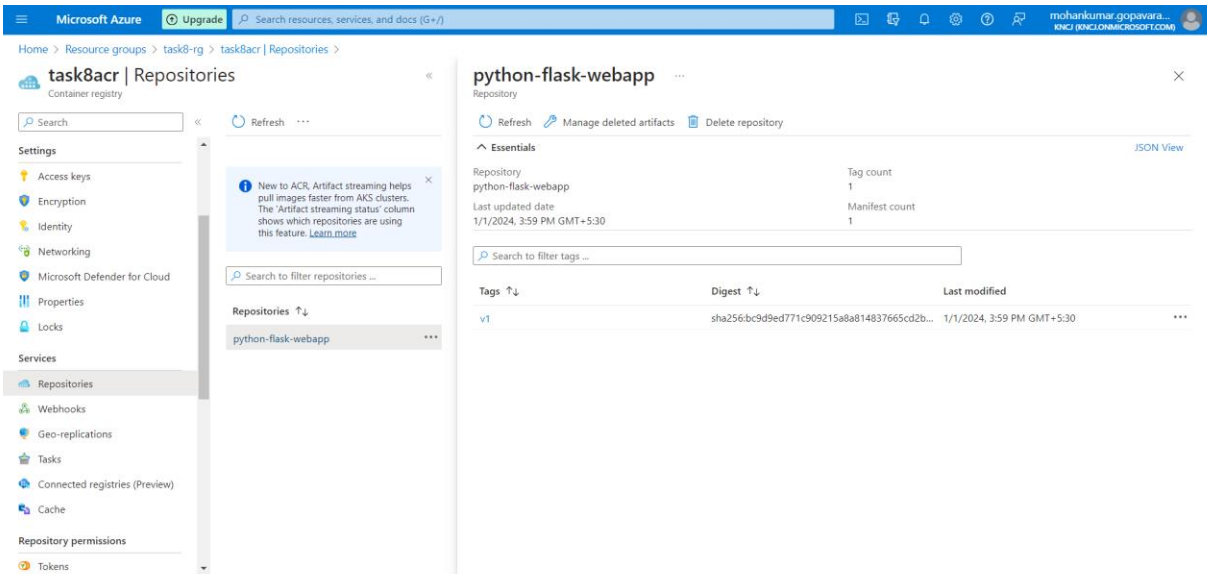
Container registry allows you to build, store, and manage container images and artifacts in a private registry for all types of container deployments. Learn more

Docker builds Image and Pushes it to the Azure container Registry:

We need to build the images from the Dockerfile using terraform code and then we need to push the image to the previously created Azure Container Registry. Click here to access the Terraform Module Source Code https://github.com/gmk1995/azure-terraform-modules



```
PS C:\Users\gmoha> docker images
REPOSITORY                                TAG              IMAGE ID       CREATED        SIZE
task8acr.azurecr.io/python-flask-webapp   v1               4f71d09ad30d   2 days ago     149MB
```



New to ACR, Artifact streaming helps pull images faster from AKS clusters. The 'Artifact streaming status' column shows which repositories are using this feature. Learn more

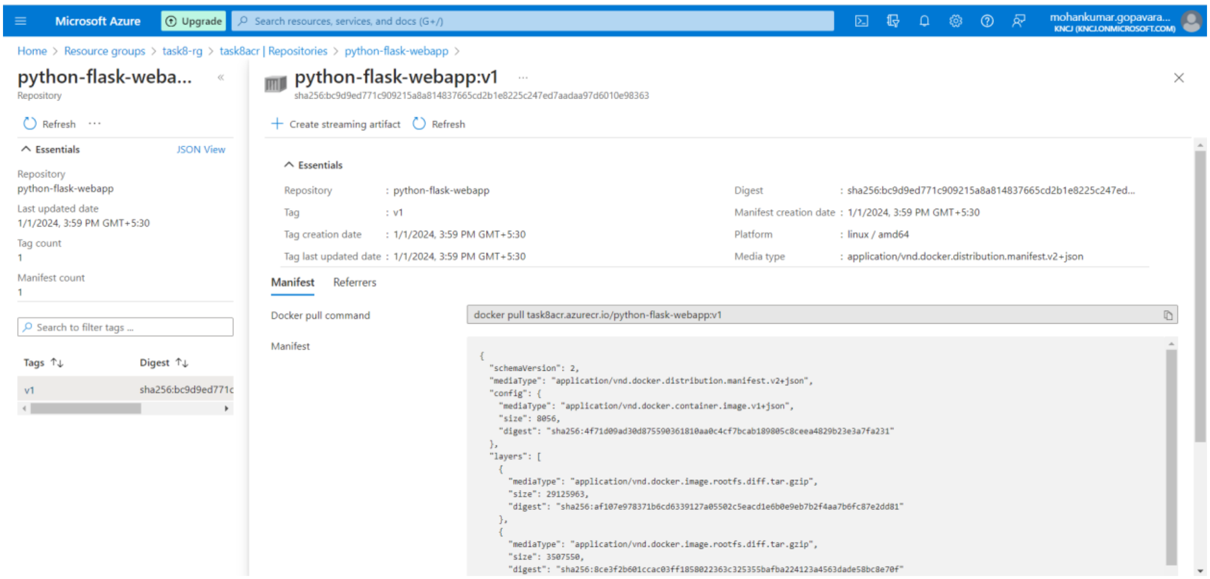
Repository
python-flask-webapp

Last updated date
1/1/2024, 3:59 PM GMT+5:30

Tag count
1

Manifest count
1

Tags	Digest	Last modified
v1	sha256:bc9d9ed771c909215a8a814837665cd2b...	1/1/2024, 3:59 PM GMT+5:30



Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
mohankumar.gopavara...
KNCJ (KNCJ.ONMICROSOFT.COM)
Home > Resource groups > task8-rg > task8acr | Repositories > python-flask-webapp >
Refresh
Create streaming artifact
Refresh
JSON View
Search to filter tags ...

python-flask-weba...
Repository

Essentials

Repository
python-flask-webapp
Last updated date
1/1/2024, 3:59 PM GMT+5:30
Tag count
1
Manifest count
1

Tags	Digest
v1	sha256:bc9d9ed771c

python-flask-webapp:v1
sha256:bc9d9ed771c909215a8a814837665cd2b1e8225c247ed7aadaa97d6010e98363

Essentials

Repository	: python-flask-webapp	Digest	: sha256:bc9d9ed771c909215a8a814837665cd2b1e8225c247ed...
Tag	: v1	Manifest creation date	: 1/1/2024, 3:59 PM GMT+5:30
Tag creation date	: 1/1/2024, 3:59 PM GMT+5:30	Platform	: linux / amd64
Tag last updated date	: 1/1/2024, 3:59 PM GMT+5:30	Media type	: application/vnd.docker.distribution.manifest.v2+json

Manifest   Referrers

Docker pull command

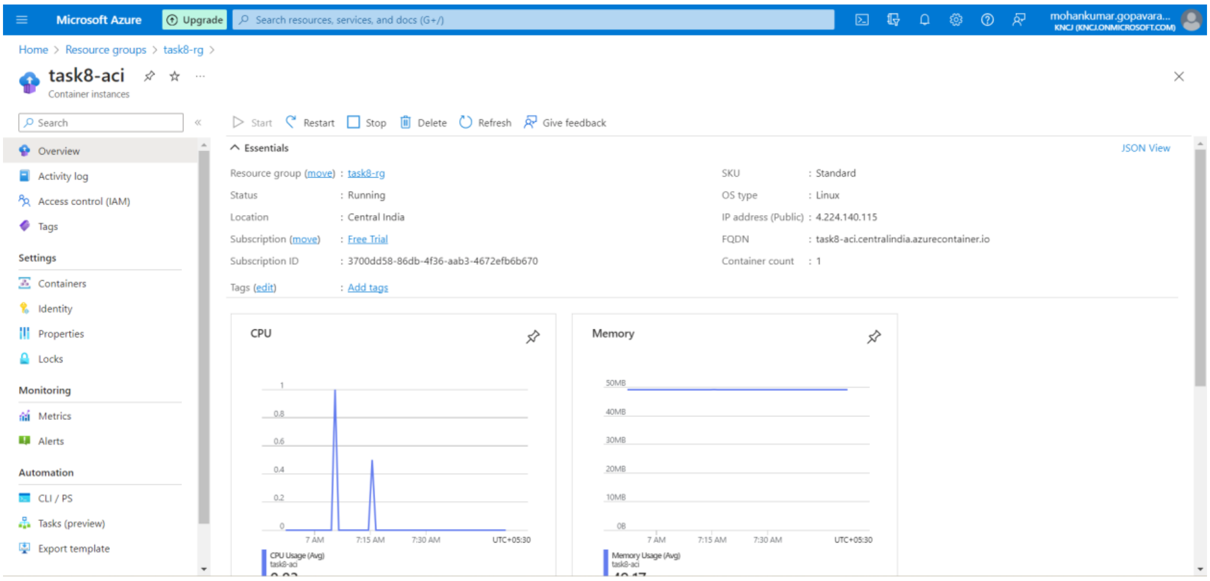
```
docker pull task8acr.azurecr.io/python-flask-webapp:v1
```

Manifest

```
{
  "schemaVersion": 2,
  "mediaType": "application/vnd.docker.distribution.manifest.v2+json",
  "config": {
    "mediaType": "application/vnd.docker.container.image.v1+json",
    "size": 8056,
    "digest": "sha256:4f71d09ad30d875590361810aa0c4cf7bcab189805c8ceea4829b23e3a7fa231"
  },
  "layers": [
    {
      "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
      "size": 29125963,
      "digest": "sha256:af107e978371b6cd6339127a05502c5eacd1e6b0e9eb7b2f4aa7b6fc87e2dd81"
    },
    {
      "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
      "size": 3507550,
      "digest": "sha256:8ce3f2b601ccac03ff1858022363c325355bafba224123a4563dade58bc8e70f"
```

Azure Container Instance:

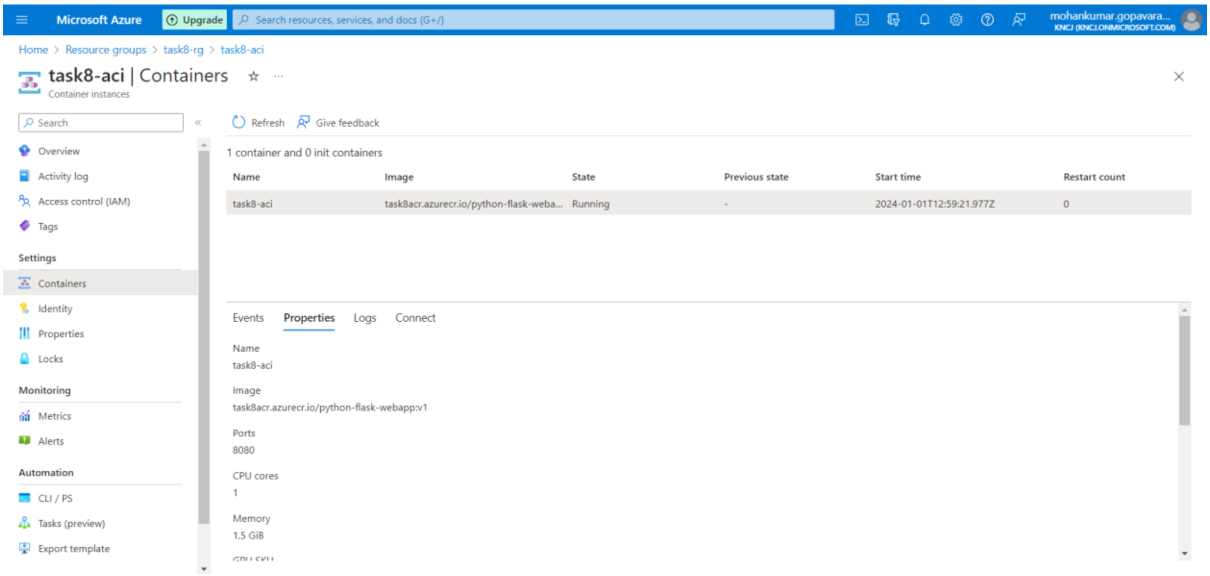
We need to Create the Azure Container Instance to Create the Container from the Previously build and pushed image from the Azure container using Terraform code. Click here to access the Terraform Module Source Code Module: https://github.com/gmk1995/azure-terraform-modules



task8-aci
Container instances

Essentials

Resource group (move)	: task8-rg	SKU	: Standard
Status	: Running	OS type	: Linux
Location	: Central India	IP address (Public)	: 4.224.140.115
Subscription (move)	: Free Trial	FQDN	: task8-aci.centralindia.azurecontainer.io
Subscription ID	: 3700dd58-86db-4f36-aab3-4672efb6b670	Container count	: 1
Tags (edit)	: Add tags		



task8-aci | Containers

1 container and 0 init containers

Name	Image	State	Previous state	Start time	Restart count
task8-aci	task8acr.azurecr.io/python-flask-weba...	Running	-	2024-01-01T12:59:21.977Z	0

Name
task8-aci

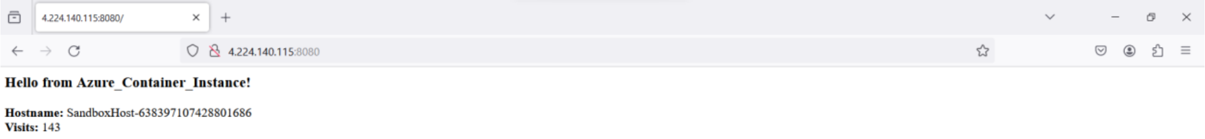
Image
task8acr.azurecr.io/python-flask-webapp:v1

Ports
8080

CPU cores
1

Memory
1.5 GiB

Access the Deployed Container through the web Using the IP address with Port Number of the Container: https://github.com/gmk1995/azure-terraform-modules



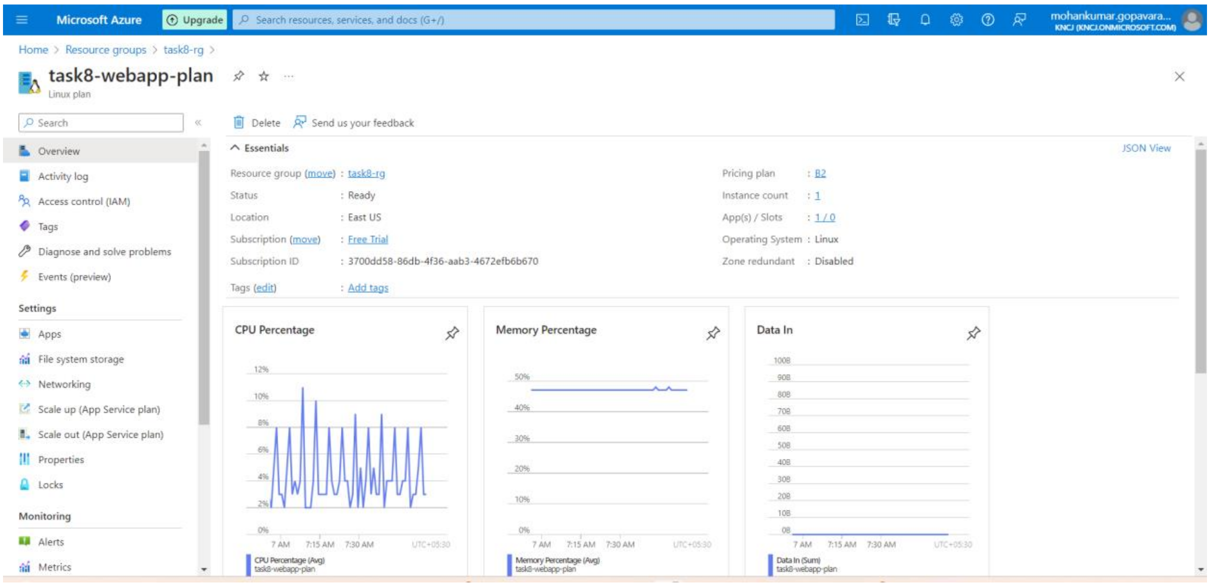
Hello from Azure_Container_Instance!

Hostname: SandboxHost-638397107428801686
Visits: 143

Azure Web Apps:

Previously build and pushed image to the Azure Container Registry used to Create the Azure Web App. Here we need to create the Azure Web App Service Plan First and then Azure Web App. We need to Assign a Role to the Web App to Pull the Images from Azure Container Registry. Click on the below link to access Terraform Module Source Code. https://github.com/gmk1995/azure-terraform-modules

Service Plan:

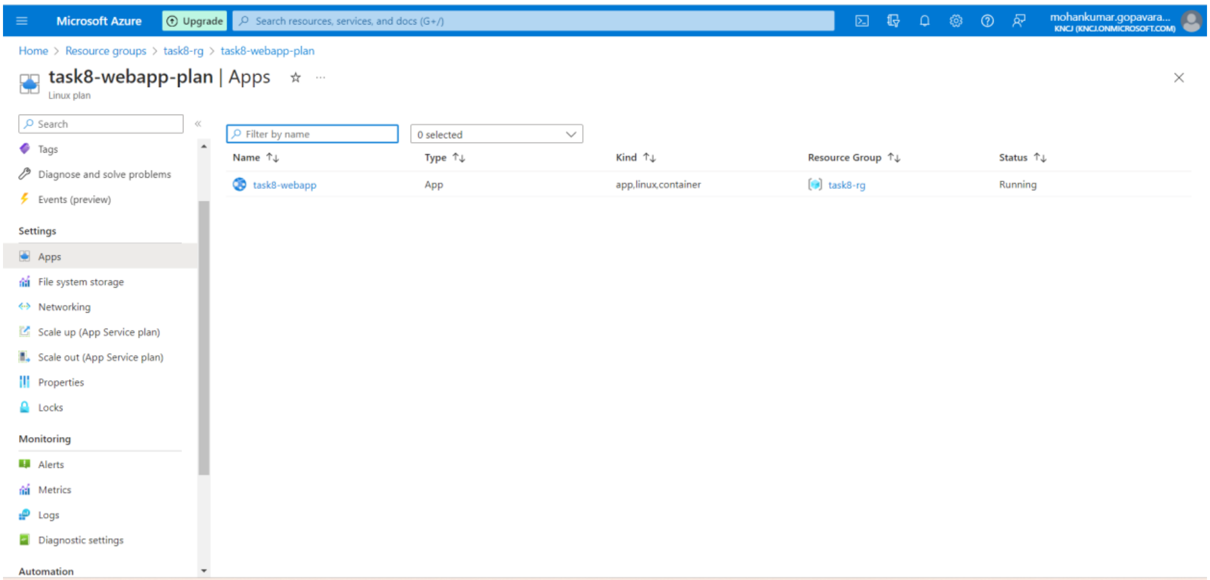


task8-webapp-plan

Resource group (move) : task8-rg
Status : Ready
Location : East US
Subscription (move) : Free Trial
Subscription ID : 3700dd58-86db-4f36-aab3-4672efb6b670
Tags (edit) : Add tags

Pricing plan : B2
Instance count : 1
App(s) / Slots : 1 / 0
Operating System : Linux
Zone redundant : Disabled

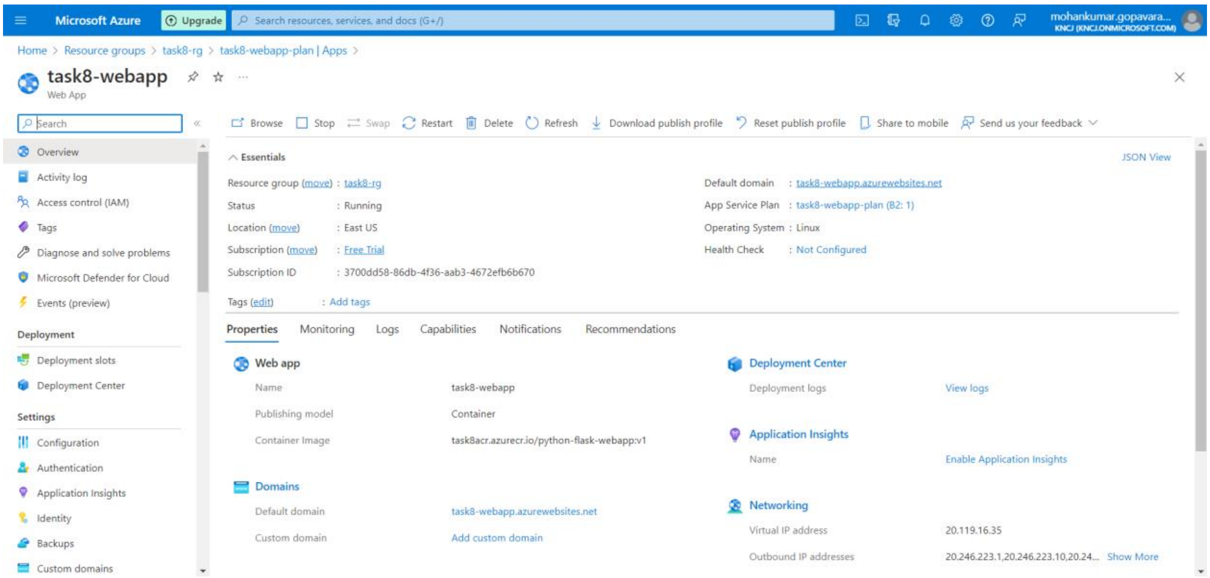
Web App:



task8-webapp-plan | Apps

Linux plan

Name ↑↓	Type ↑↓	Kind ↑↓	Resource Group ↑↓	Status ↑↓
task8-webapp	App	app,linux,container	task8-rg	Running



task8-webapp

Web App

Essentials

Resource group (move) : task8-rg
Status : Running
Location (move) : East US
Subscription (move) : Free Trial
Subscription ID : 3700dd58-86db-4f36-aab3-4672efb6b670
Tags (edit) : Add tags

Default domain : task8-webapp.azurewebsites.net
App Service Plan : task8-webapp-plan (B2: 1)
Operating System : Linux
Health Check : Not Configured

Web app

Name	task8-webapp
Publishing model	Container
Container Image	task8acr.azurecr.io/python-flask-webapp:v1

Domains

Default domain	task8-webapp.azurewebsites.net
Custom domain	Add custom domain

Deployment Center

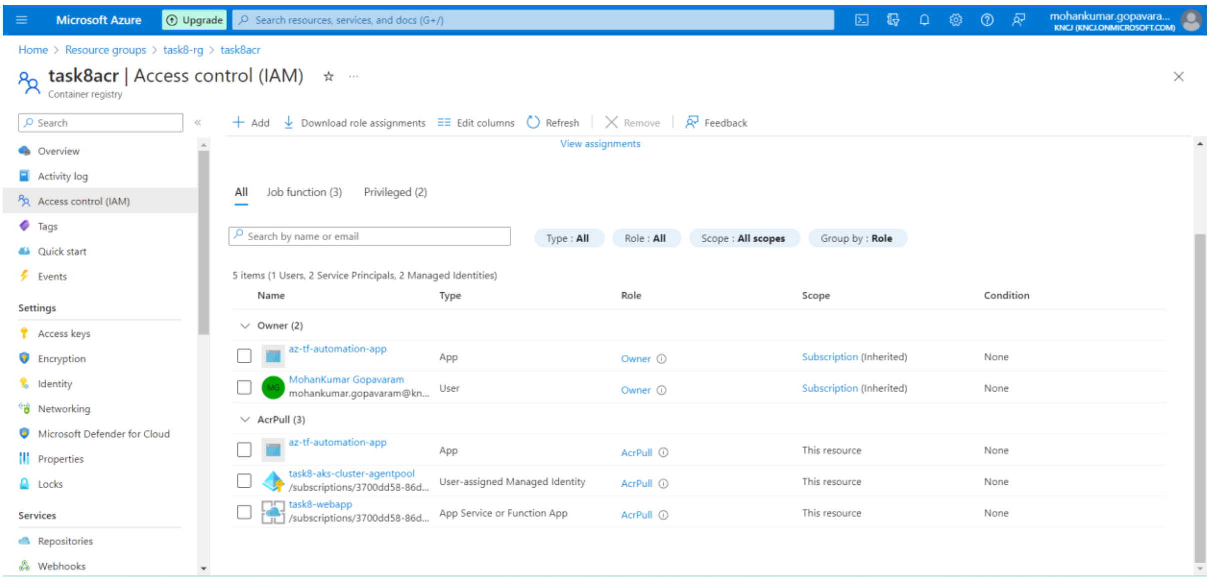
Deployment logs	View logs

Application Insights

Name	Enable Application Insights

Networking

Virtual IP address	20.119.16.35
Outbound IP addresses	20.246.223.1,20.246.223.10,20.24... Show More



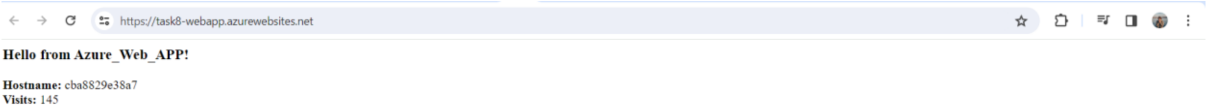
task8acr | Access control (IAM)

Container registry

5 items (1 Users, 2 Service Principals, 2 Managed Identities)

Name	Type	Role	Scope	Condition
Owner (2)				
az-tf-automation-app	App	Owner	Subscription (Inherited)	None
MohanKumar Gopavaram mohankumar.gopavaram@kn...	User	Owner	Subscription (Inherited)	None
AcrPull (3)				
az-tf-automation-app	App	AcrPull	This resource	None
task8-aks-cluster-agentpool /subscriptions/3700dd58-86d...	User-assigned Managed Identity	AcrPull	This resource	None
task8-webapp /subscriptions/3700dd58-86d...	App Service or Function App	AcrPull	This resource	None

Access the Web App from the web browser using the Default Domain Name:



https://task8-webapp.azurewebsites.net

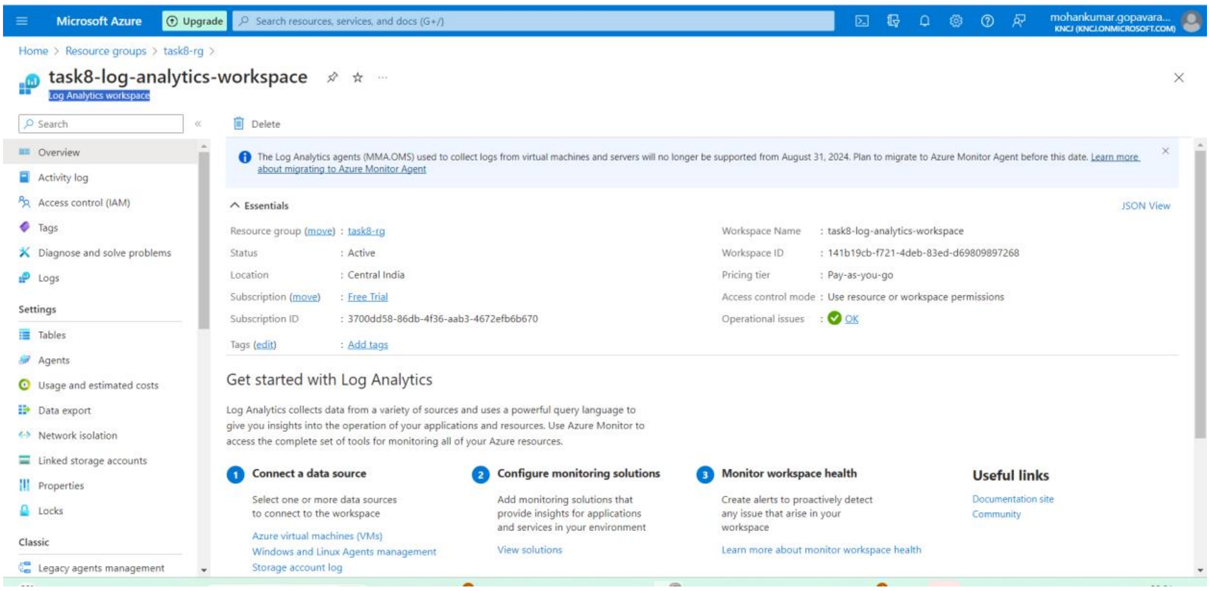
Hello from Azure_Web_APP!

Hostname: cba8829e38a7
Visits: 145

Azure Container App:

First, we need to create a Log Analytic Workspace and Azure Container App Environment and then Azure Container App. Previously build and pushed docker image from Azure Container Registry need to take to create a Azure Container App using terraform Code. Click here to access the Terraform Module Source Code: https://github.com/gmk1995/azure-terraform-modules

Log Analytics workspace:



task8-log-analytics-workspace

Log Analytics workspace

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

Essentials

Resource group (move)	: task8-rg	Workspace Name	: task8-log-analytics-workspace
Status	: Active	Workspace ID	: 141b19cb-f721-4deb-83ed-d69809897268
Location	: Central India	Pricing tier	: Pay-as-you-go
Subscription (move)	: Free Trial	Access control mode	: Use resource or workspace permissions
Subscription ID	: 3700dd58-86db-4f36-aab3-4672efb6b670	Operational issues	: ✓ OK
Tags (edit)	: Add tags		

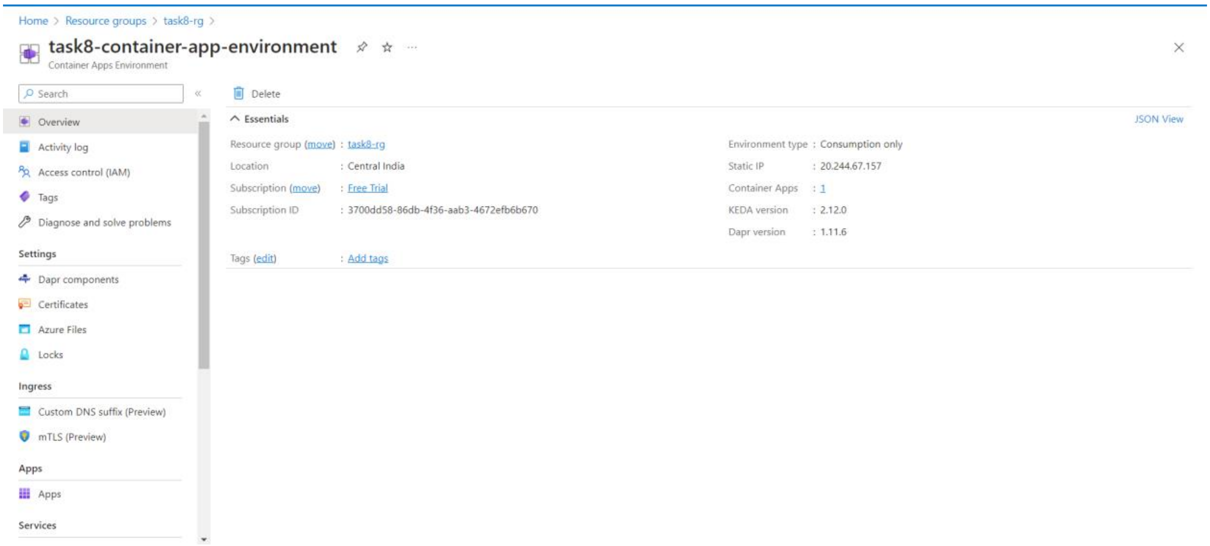
Get started with Log Analytics

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

1. Connect a data source
   Select one or more data sources to connect to the workspace
   Azure virtual machines (VMs)
   Windows and Linux Agents management
   Storage account log
2. Configure monitoring solutions
   Add monitoring solutions that provide insights for applications and services in your environment
   View solutions
3. Monitor workspace health
   Create alerts to proactively detect any issue that arise in your workspace
   Learn more about monitor workspace health

Useful links
Documentation site
Community

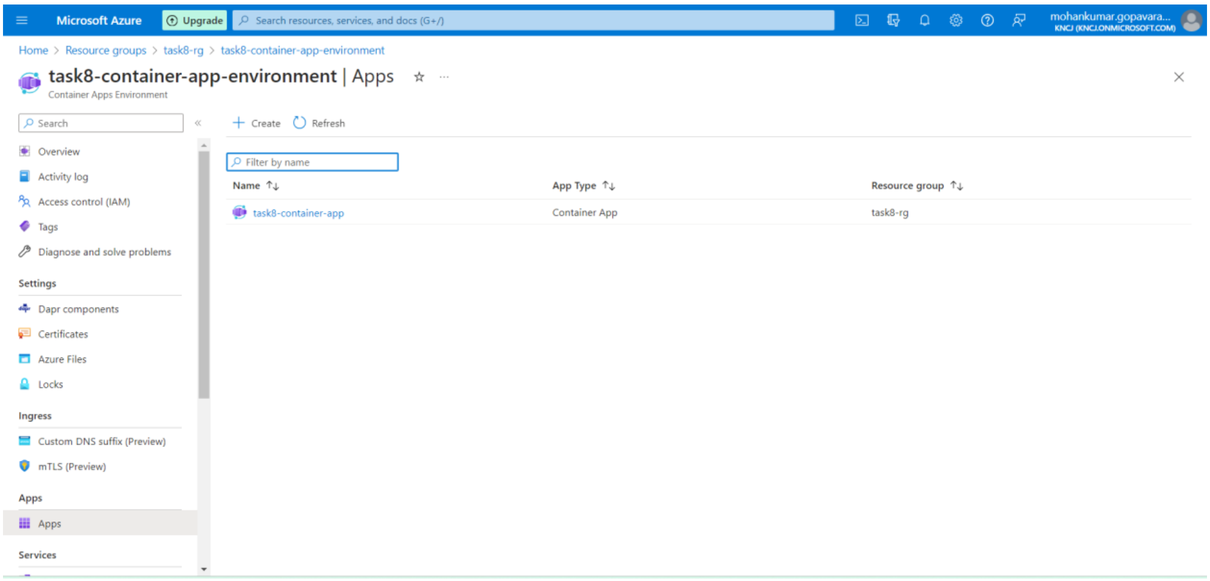
Container Apps Environment:



task8-container-app-environment
Container Apps Environment

Essentials

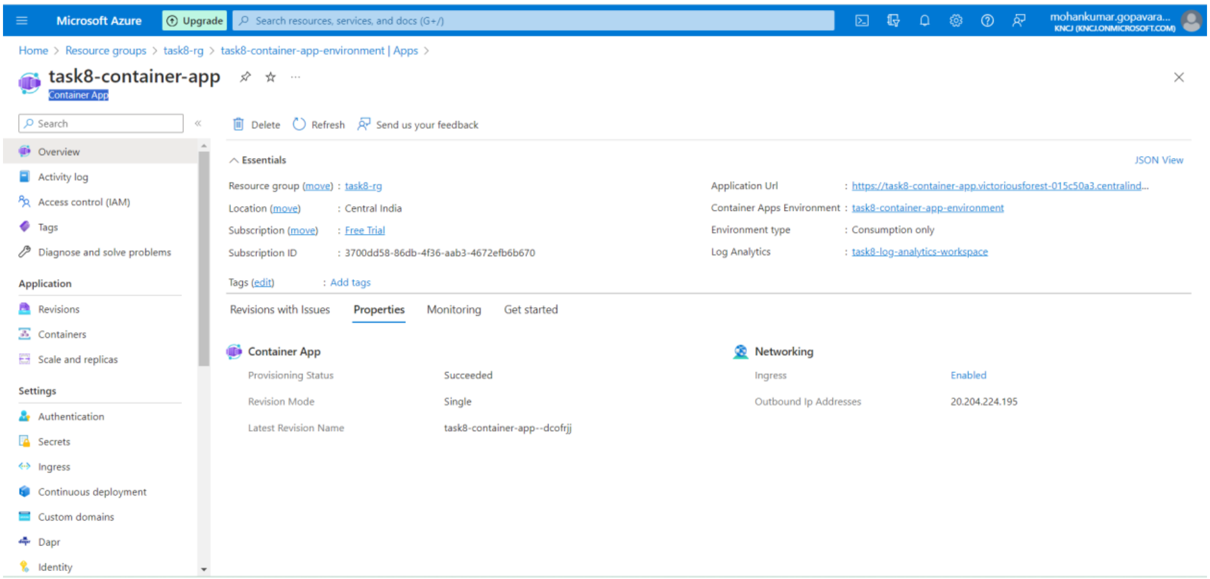
Resource group (move)	: task8-rg	Environment type	: Consumption only
Location	: Central India	Static IP	: 20.244.67.157
Subscription (move)	: Free Trial	Container Apps	: 1
Subscription ID	: 3700dd58-86db-4f36-aab3-4672efb6b670	KEDA version	: 2.12.0
		Dapr version	: 1.11.6
Tags (edit)	: Add tags		



task8-container-app-environment | Apps
Container Apps Environment

Name ↑↓	App Type ↑↓	Resource group ↑↓
task8-container-app	Container App	task8-rg

Container App:



task8-container-app
Container App

Essentials

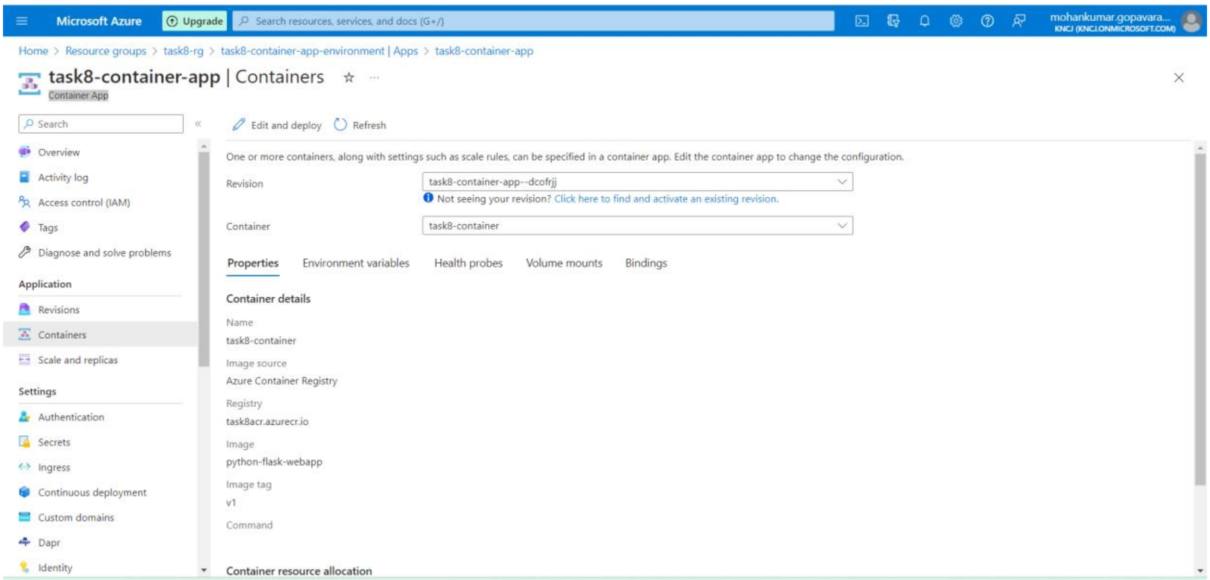
Resource group (move)	: task8-rg	Application Url	: https://task8-container-app.victoriousforest-015c50a3.centralind...
Location (move)	: Central India	Container Apps Environment	: task8-container-app-environment
Subscription (move)	: Free Trial	Environment type	: Consumption only
Subscription ID	: 3700dd58-86db-4f36-aab3-4672efb6b670	Log Analytics	: task8-log-analytics-workspace
Tags (edit)	: Add tags		

Container App

Provisioning Status	Succeeded
Revision Mode	Single
Latest Revision Name	task8-container-app--dcofrjj

Networking

Ingress	Enabled
Outbound Ip Addresses	20.204.224.195



task8-container-app | Containers

One or more containers, along with settings such as scale rules, can be specified in a container app. Edit the container app to change the configuration.

Revision: task8-container-app--dcofrjj

Not seeing your revision? Click here to find and activate an existing revision.

Container: task8-container

Container details

Name
task8-container

Image source
Azure Container Registry

Registry
task8acr.azurecr.io

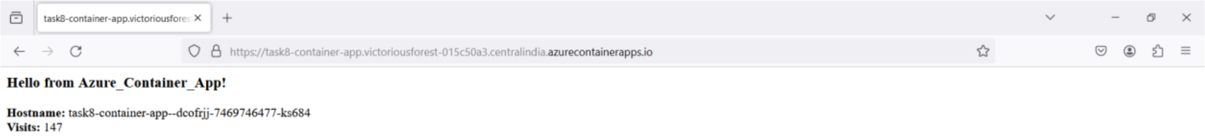
Image
python-flask-webapp

Image tag
v1

Command

Container resource allocation

Access the container build in the container apps using application url


task8-container-app.victoriousfore
https://task8-container-app.victoriousforest-015c50a3.centralindia.azurecontainerapps.io

Hello from Azure_Container_App!

Hostname: task8-container-app--dcofrjj-7469746477-ks684
Visits: 147

Azure Kubernetes Services:

To create Azure Kubernetes Service integrated with Azure KeyVault created above, and which will host a container from the image built earlier.

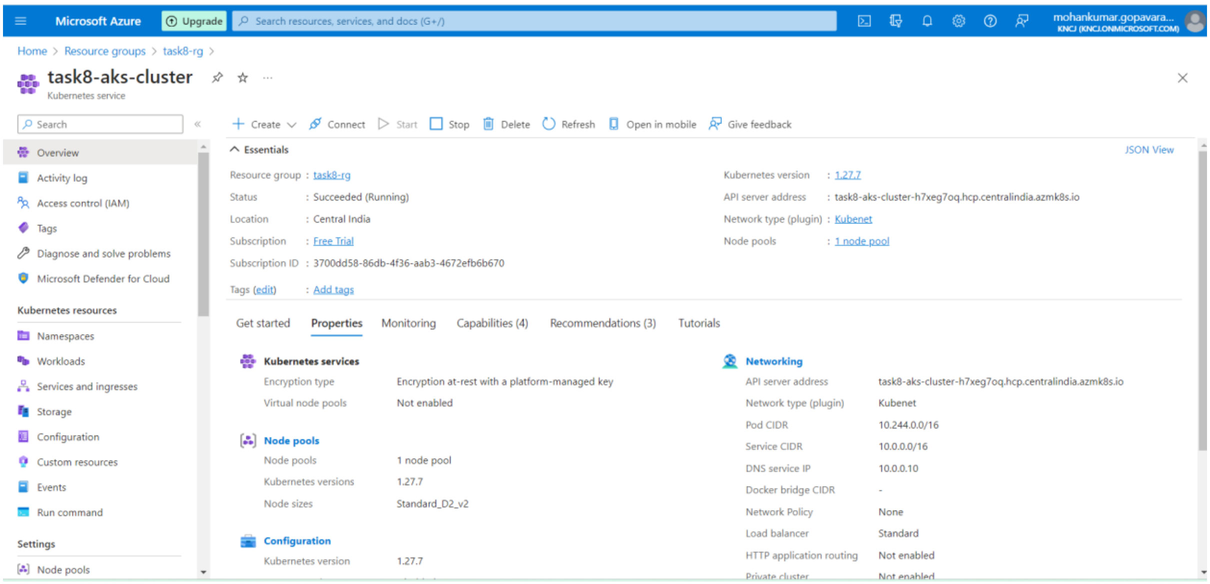
Define “CREATOR” variable for container with value “K8S”.

Pods in k8s should obtain secrets form KeyVault during the initialization. Use “Access with a user-assigned managed identity” approach.

Key Vault Administrator and AcrPull Role Assignments needs to be added to the user-assigned managed identity to pull the images from Azure Container Registry and Access the Key Vault Secrets.

Key Access Policy Also need to add to the user-assigned managed identity to access the secrets.

Click here to access the Terraform Module Source Code. https://github.com/gmk1995/azure-terraform-modules



task8-aks-cluster

Kubernetes service

Essentials

Resource group : task8-rg

Status : Succeeded (Running)

Location : Central India

Subscription : Free Trial

Subscription ID : 3700dd58-86db-4f36-aab3-4672efb6b670

Tags (edit) : Add tags

Kubernetes version : 1.27.7

API server address : task8-aks-cluster-h7xeg7oq.hcp.centralindia.azmk8s.io

Network type (plugin) : Kubenet

Node pools : 1 node pool

Kubernetes services

Encryption type	Encryption at-rest with a platform-managed key
Virtual node pools	Not enabled

Node pools

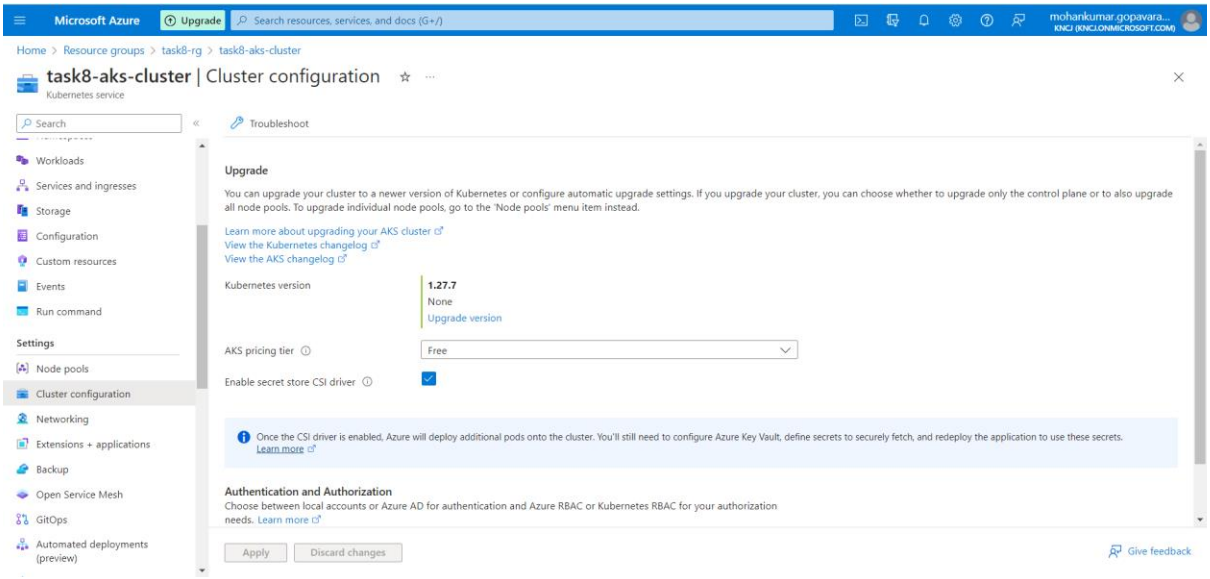
Node pools	1 node pool
Kubernetes versions	1.27.7
Node sizes	Standard_D2_v2

Configuration

Kubernetes version	1.27.7

Networking

API server address	task8-aks-cluster-h7xeg7oq.hcp.centralindia.azmk8s.io
Network type (plugin)	Kubenet
Pod CIDR	10.244.0.0/16
Service CIDR	10.0.0.0/16
DNS service IP	10.0.0.10
Docker bridge CIDR	-
Network Policy	None
Load balancer	Standard
HTTP application routing	Not enabled
Private cluster	Not enabled



task8-aks-cluster | Cluster configuration

Kubernetes service

Upgrade

You can upgrade your cluster to a newer version of Kubernetes or configure automatic upgrade settings. If you upgrade your cluster, you can choose whether to upgrade only the control plane or to also upgrade all node pools. To upgrade individual node pools, go to the 'Node pools' menu item instead.

Learn more about upgrading your AKS cluster
View the Kubernetes changelog
View the AKS changelog

Kubernetes version: **1.27.7**
None
Upgrade version

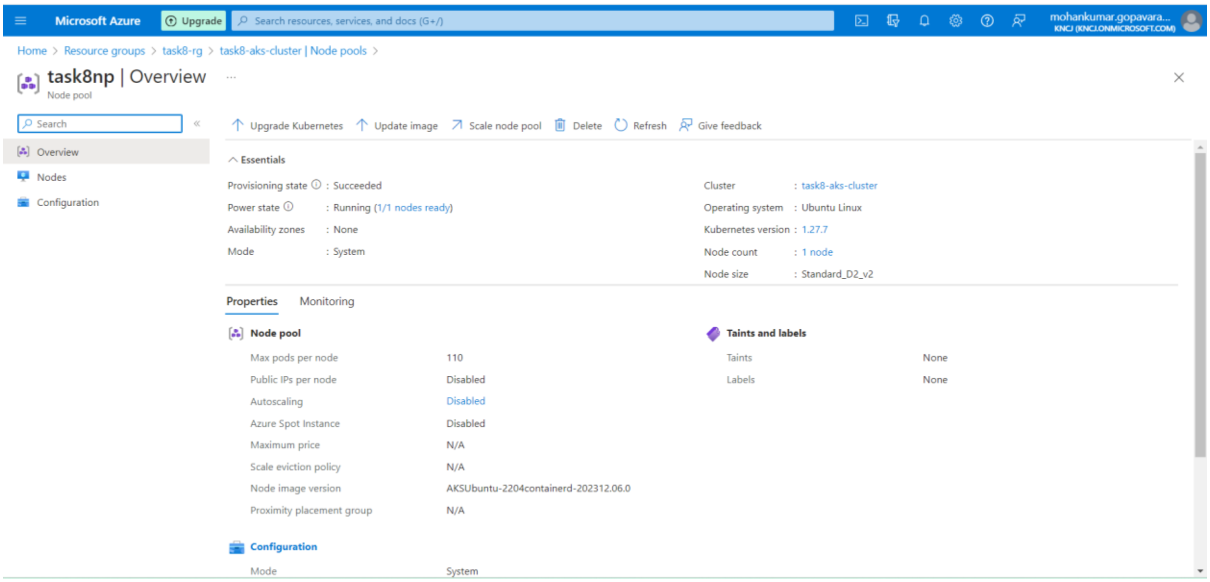
AKS pricing tier: Free

Enable secret store CSI driver: ☑

Once the CSI driver is enabled, Azure will deploy additional pods onto the cluster. You'll still need to configure Azure Key Vault, define secrets to securely fetch, and redeploy the application to use these secrets. Learn more

Authentication and Authorization

Choose between local accounts or Azure AD for authentication and Azure RBAC or Kubernetes RBAC for your authorization needs. Learn more



task8np | Overview

Node pool

Essentials

Provisioning state : Succeeded

Power state : Running (1/1 nodes ready)

Availability zones : None

Mode : System

Cluster : task8-aks-cluster

Operating system : Ubuntu Linux

Kubernetes version : 1.27.7

Node count : 1 node

Node size : Standard_D2_v2

Properties | Monitoring

Node pool

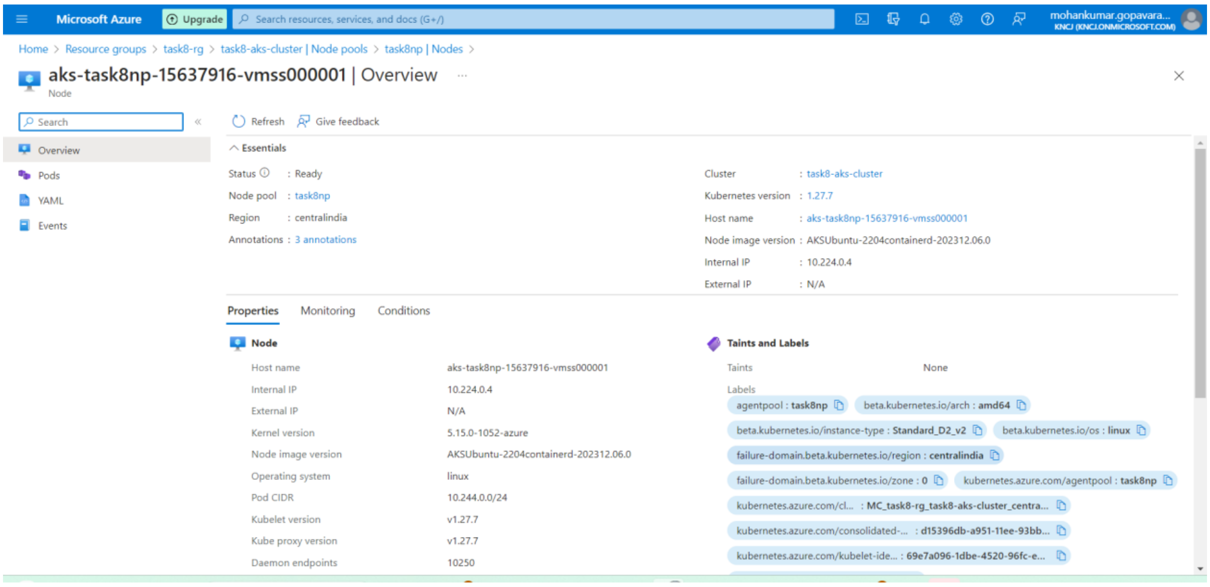
Max pods per node	110
Public IPs per node	Disabled
Autoscaling	Disabled
Azure Spot Instance	Disabled
Maximum price	N/A
Scale eviction policy	N/A
Node image version	AKSUbuntu-2204containerd-202312.06.0
Proximity placement group	N/A

Taints and labels

Taints	None
Labels	None

Configuration

Mode	System


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
mohankumar.gopavara...
KNCJ (KNCJ.ONMICROSOFT.COM)
Home > Resource groups > task8-rg > task8-aks-cluster | Node pools > task8np | Nodes >
Search
Overview
Pods
YAML
Events
Refresh
Give feedback

aks-task8np-15637916-vmss000001 | Overview

Node

Essentials

Status : Ready

Node pool : task8np

Region : centralindia

Annotations : 3 annotations

Cluster : task8-aks-cluster

Kubernetes version : 1.27.7

Host name : aks-task8np-15637916-vmss000001

Node image version : AKSUbuntu-2204containerd-202312.06.0

Internal IP : 10.224.0.4

External IP : N/A

Properties | Monitoring | Conditions

Node

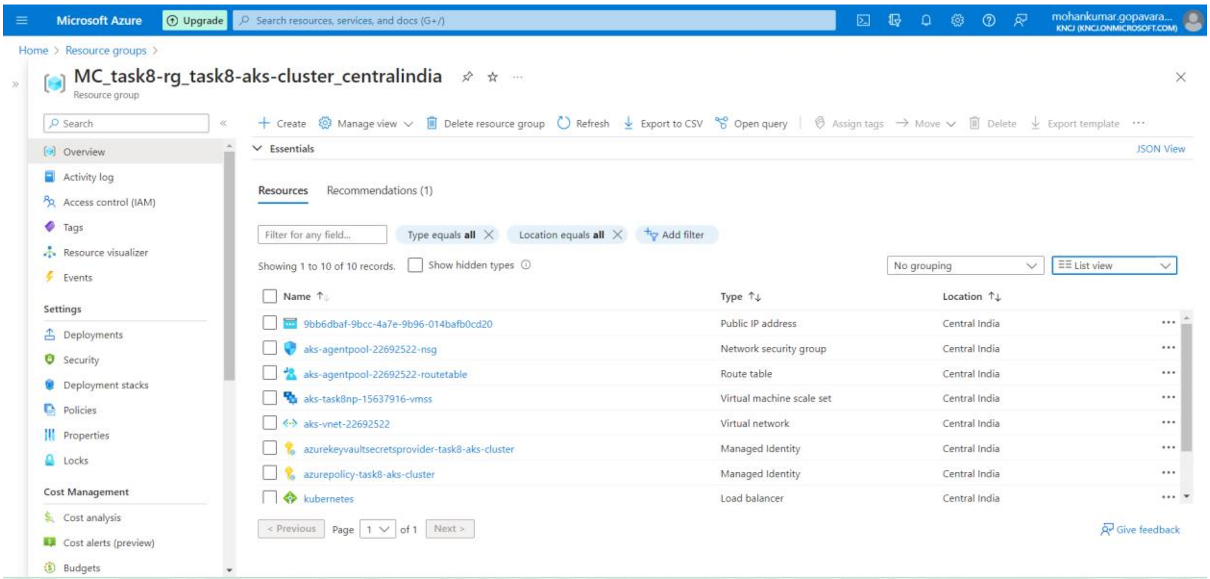
Host name	aks-task8np-15637916-vmss000001
Internal IP	10.224.0.4
External IP	N/A
Kernel version	5.15.0-1052-azure
Node image version	AKSUbuntu-2204containerd-202312.06.0
Operating system	linux
Pod CIDR	10.244.0.0/24
Kubelet version	v1.27.7
Kube proxy version	v1.27.7
Daemon endpoints	10250

Taints and Labels

Taints None

Labels

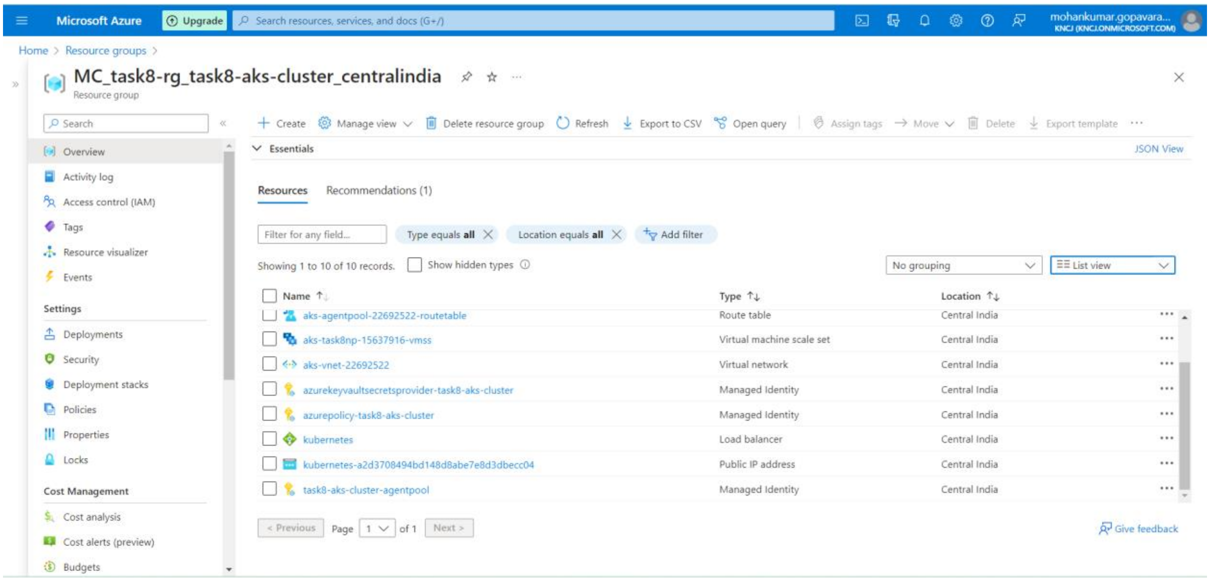
- agentpool : **task8np**
- beta.kubernetes.io/arch : **amd64**
- beta.kubernetes.io/instance-type : **Standard_D2_v2**
- beta.kubernetes.io/os : **linux**
- failure-domain.beta.kubernetes.io/region : **centralindia**
- failure-domain.beta.kubernetes.io/zone : **0**
- kubernetes.azure.com/agentpool : **task8np**
- kubernetes.azure.com/cl... : **MC_task8-rg_task8-aks-cluster_centra...**
- kubernetes.azure.com/consolidated-... : **d15396db-a951-11ee-93bb...**
- kubernetes.azure.com/kubelet-ide... : **69e7a096-1dbe-4520-96fc-e...**



MC_task8-rg_task8-aks-cluster_centralindia

Showing 1 to 10 of 10 records.

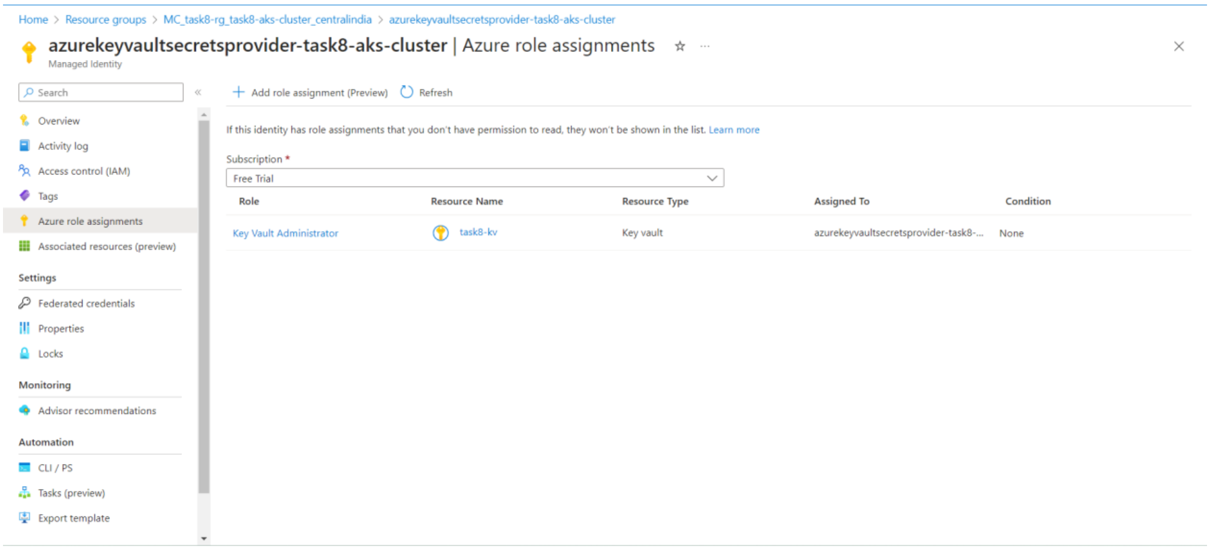
Name	Type	Location
9bb6dbaf-9bcc-4a7e-9b96-014bafb0cd20	Public IP address	Central India
aks-agentpool-22692522-nsg	Network security group	Central India
aks-agentpool-22692522-routetable	Route table	Central India
aks-task8np-15637916-vmss	Virtual machine scale set	Central India
aks-vnet-22692522	Virtual network	Central India
azurekeyvaultsecretsprovider-task8-aks-cluster	Managed Identity	Central India
azurepolicy-task8-aks-cluster	Managed Identity	Central India
kubernetes	Load balancer	Central India



MC_task8-rg_task8-aks-cluster_centralindia

Showing 1 to 10 of 10 records.

Name	Type	Location
aks-agentpool-22692522-routetable	Route table	Central India
aks-task8np-15637916-vmss	Virtual machine scale set	Central India
aks-vnet-22692522	Virtual network	Central India
azurekeyvaultsecretsprovider-task8-aks-cluster	Managed Identity	Central India
azurepolicy-task8-aks-cluster	Managed Identity	Central India
kubernetes	Load balancer	Central India
kubernetes-a2d3708494bd148d8abe7e8d3dbecc04	Public IP address	Central India
task8-aks-cluster-agentpool	Managed Identity	Central India

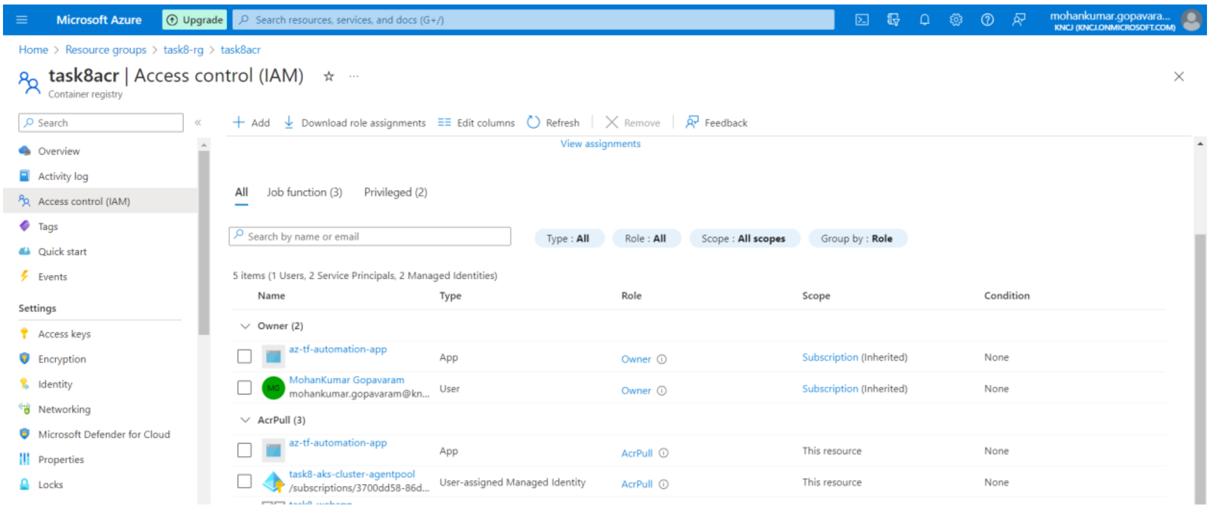


azurekeyvaultsecretsprovider-task8-aks-cluster | Azure role assignments

If this identity has role assignments that you don't have permission to read, they won't be shown in the list. Learn more

Subscription *
Free Trial

Role	Resource Name	Resource Type	Assigned To	Condition
Key Vault Administrator	task8-kv	Key vault	azurekeyvaultsecretsprovider-task8-...	None



5 items (1 Users, 2 Service Principals, 2 Managed Identities)

Name	Type	Role	Scope	Condition
Owner (2)				
az-tf-automation-app	App	Owner	Subscription (Inherited)	None
MohanKumar Gopavaram mohankumar.gopavaram@kn...	User	Owner	Subscription (Inherited)	None
AcrPull (3)				
az-tf-automation-app	App	AcrPull	This resource	None
task8-aks-cluster-agentpool /subscriptions/3700dd58-86d...	User-assigned Managed Identity	AcrPull	This resource	None

Once Azure Kubernetes Cluster is Created Open any Terminal and run the below command to get kubeconfig file to access the AKS Cluster:

az aks get-credentials --resource-group task8-rg --name task8-aks-cluster

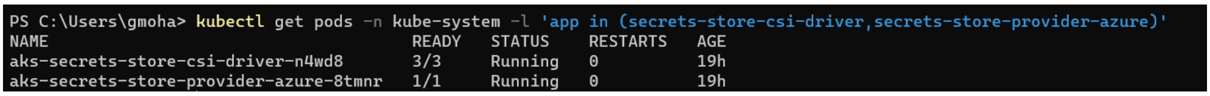
Above Command Response: WARNING: Merged "task8-aks-cluster" as current context in C:\Users\xxxx\.kube\config

Note: resource-group name and aks cluster name required.

Once the kubeconfig file is downloaded, and stored in locally we can access the aks cluster.

Verify the Azure Key Vault provider for Secrets Store CSI Driver installation:

kubectl get pods -n kube-system -l 'app in (secrets-store-csi-driver,secrets-store-provider-azure)'



```
PS C:\Users\gmoha> kubectl get pods -n kube-system -l 'app in (secrets-store-csi-driver,secrets-store-provider-azure)'
NAME                                     READY   STATUS    RESTARTS   AGE
aks-secrets-store-csi-driver-n4wd8       3/3     Running   0          19h
aks-secrets-store-provider-azure-8tmnr   1/1     Running   0          19h
```

Create secretprovider class using below yaml file and command kubectl apply -f secretproviderclass.yaml :

Note: All the Required File are in the GitHub Url: https://github.com/gmk1995/azure-terraform-modules

Update the userAssignedIdentityID: # Set the clientID of the user-assigned managed identity to use. Go the Azure Portal and Get the Client ID of user-assigned managed identity

Update the Azure Key Name keyvaultName: # Set to the name of your key vault

In the Object Name update the objectName: CREATOR   # secret name which you have created and stored in key vault secret

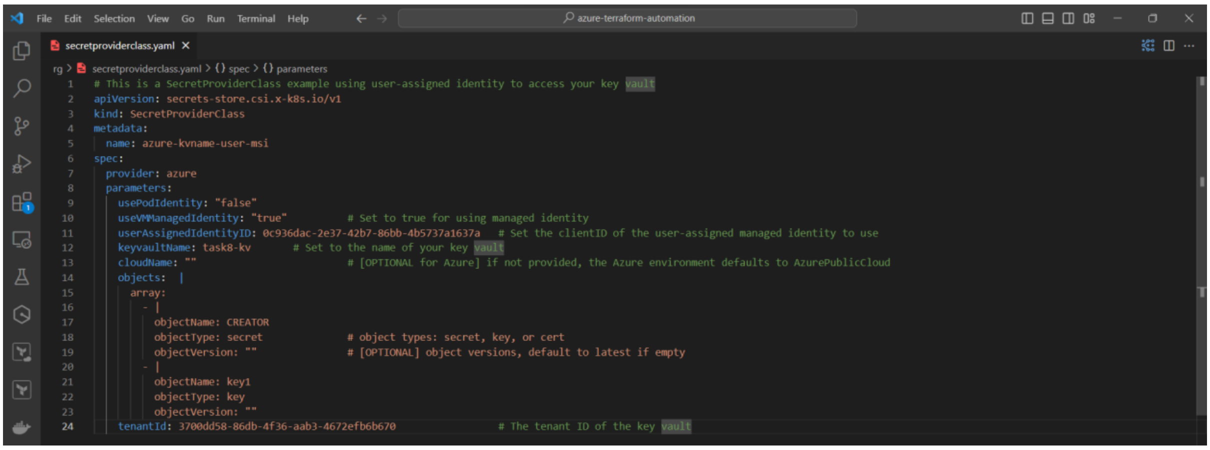
Update the tenantId run the below command to get tenantId of the key vault.

az keyvault show --name task8-kv --query id -o tsv

Response of the above command:

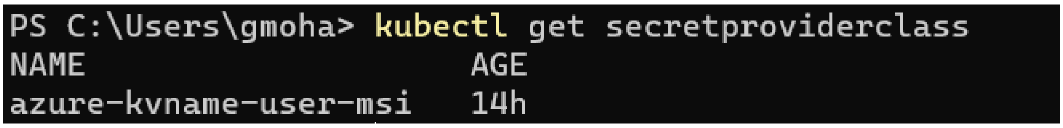
/subscriptions/3700dd58-86db-4f36-aab3-4672efb6b670/resourceGroups/task8-rg/providers/Microsoft.KeyVault/vaults/task8-kv

Update the resource group name and aks-cluster-name


File
Edit
Selection
View
Go
Run
Terminal
Help
azure-terraform-automation
secretproviderclass.yaml
rg > secretproviderclass.yaml > {} spec > {} parameters

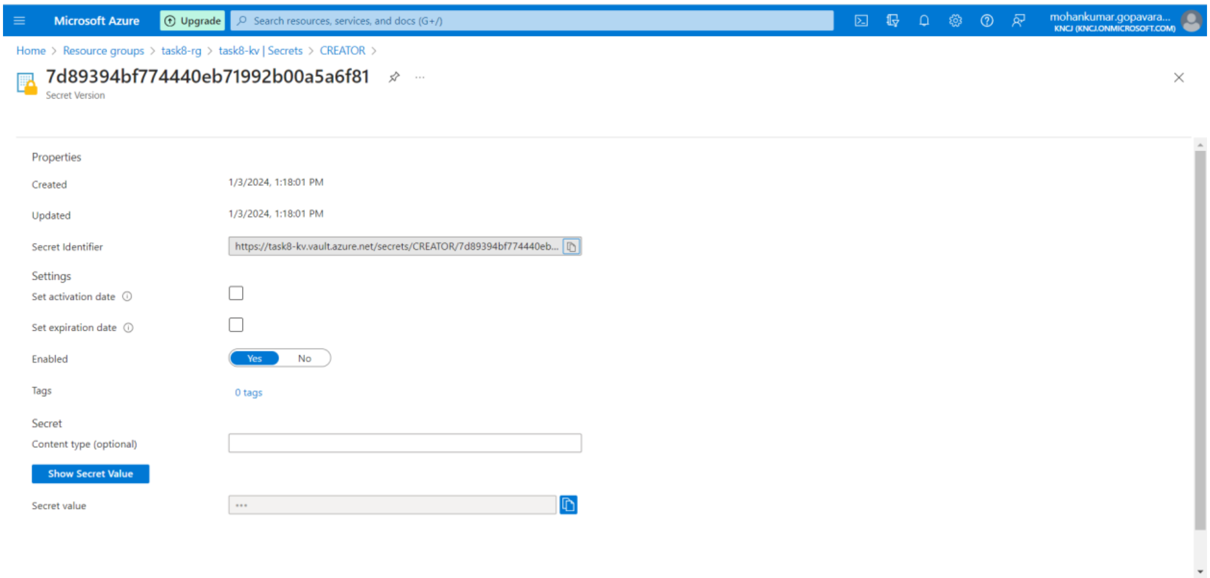
```yaml
# This is a SecretProviderClass example using user-assigned identity to access your key vault
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
  name: azure-kvname-user-msi
spec:
  provider: azure
  parameters:
    usePodIdentity: "false"
    useVMManagedIdentity: "true"          # Set to true for using managed identity
    userAssignedIdentityID: 0c936dac-2e37-42b7-86bb-4b5737a1637a   # Set the clientID of the user-assigned managed identity to use
    keyvaultName: task8-kv       # Set to the name of your key vault
    cloudName: ""                         # [OPTIONAL for Azure] if not provided, the Azure environment defaults to AzurePublicCloud
    objects:  |
      array:
        - |
          objectName: CREATOR
          objectType: secret              # object types: secret, key, or cert
          objectVersion: ""               # [OPTIONAL] object versions, default to latest if empty
        - |
          objectName: key1
          objectType: key
          objectVersion: ""
    tenantId: 3700dd58-86db-4f36-aab3-4672efb6b670                # The tenant ID of the key vault
```

Verify Secret Provider Class using below command:



```
PS C:\Users\gmoha> kubectl get secretproviderclass
NAME                          AGE
azure-kvname-user-msi         14h
```

We have Created a secret to get the Secret from Key Vault:



Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
mohankumar.gopavara...
KNCJ (KNCJ.ONMICROSOFT.COM)

Home > Resource groups > task8-rg > task8-kv | Secrets > CREATOR >

7d89394bf774440eb71992b00a5a6f81

Secret Version

Properties

Created 1/3/2024, 1:18:01 PM

Updated 1/3/2024, 1:18:01 PM

Secret Identifier https://task8-kv.vault.azure.net/secrets/CREATOR/7d89394bf774440eb...

Settings

Set activation date ☐

Set expiration date ☐

Enabled [✓ Yes] No

Tags 0 tags

Secret

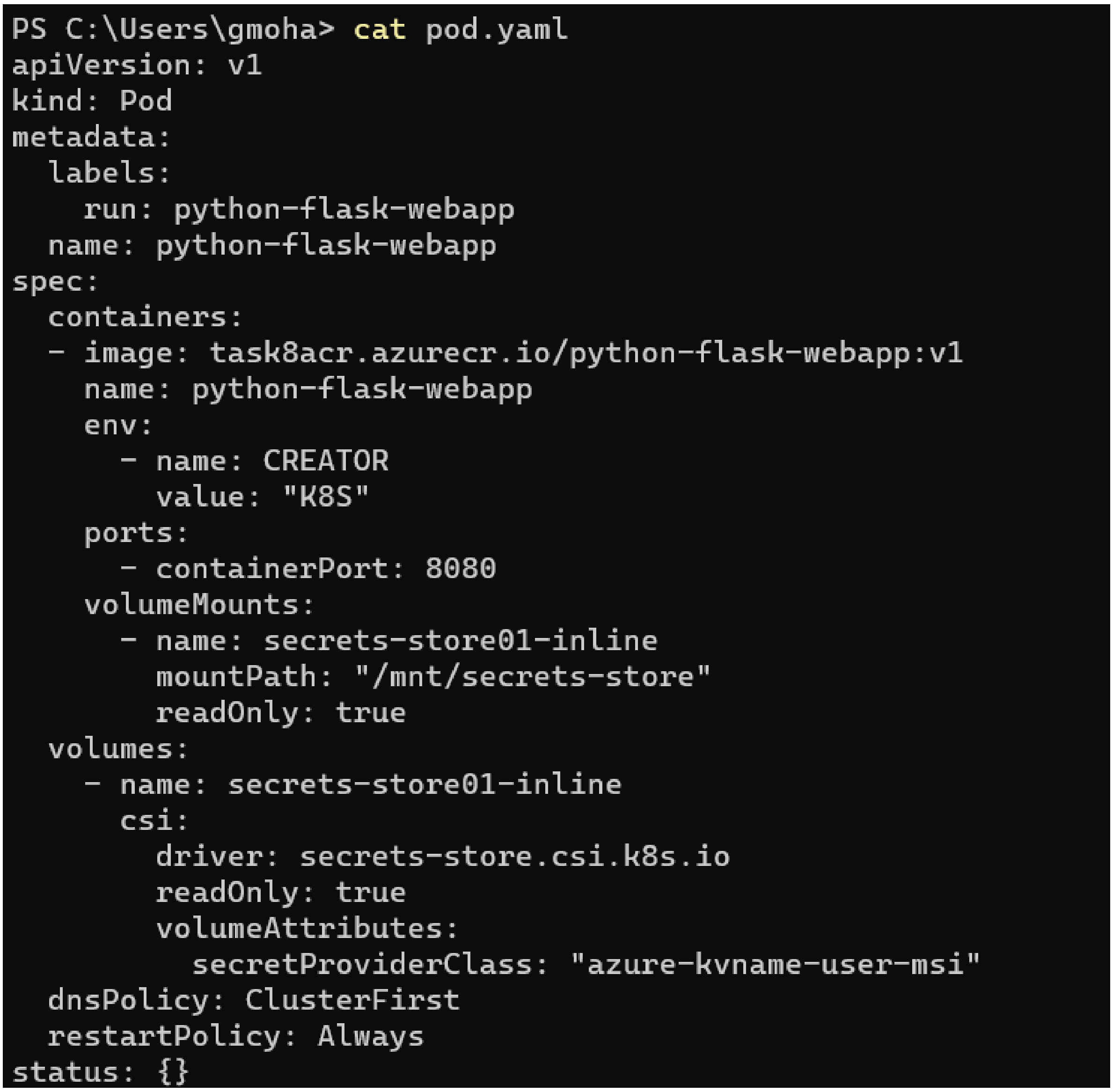
Content type (optional)

Show Secret Value

Secret value •••

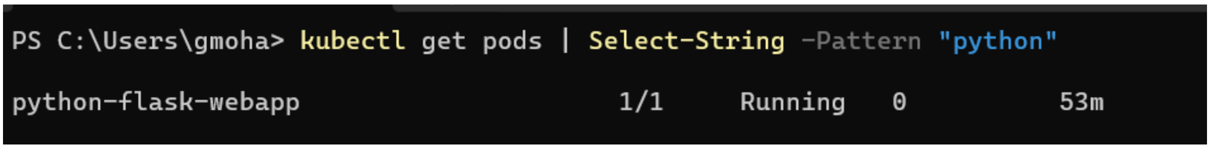
Create a Pod to Mount the Secret as secret volume in the pod using csi driver secetproviderclass and add a environment variable **CREATOR : K8S**

kubectl apply -f pod.yaml



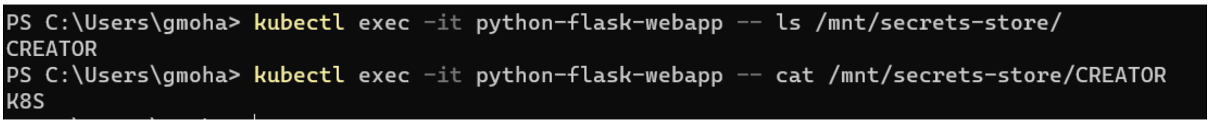
```
PS C:\Users\gmoha> cat pod.yaml
apiVersion: v1
kind: Pod
metadata:
  labels:
    run: python-flask-webapp
  name: python-flask-webapp
spec:
  containers:
  - image: task8acr.azurecr.io/python-flask-webapp:v1
    name: python-flask-webapp
    env:
      - name: CREATOR
        value: "K8S"
    ports:
      - containerPort: 8080
    volumeMounts:
      - name: secrets-store01-inline
        mountPath: "/mnt/secrets-store"
        readOnly: true
  volumes:
    - name: secrets-store01-inline
      csi:
        driver: secrets-store.csi.k8s.io
        readOnly: true
        volumeAttributes:
          secretProviderClass: "azure-kvname-user-msi"
  dnsPolicy: ClusterFirst
  restartPolicy: Always
status: {}
```

Verify the Pod is running status and check whether the secret is mounted as secret volume or not.



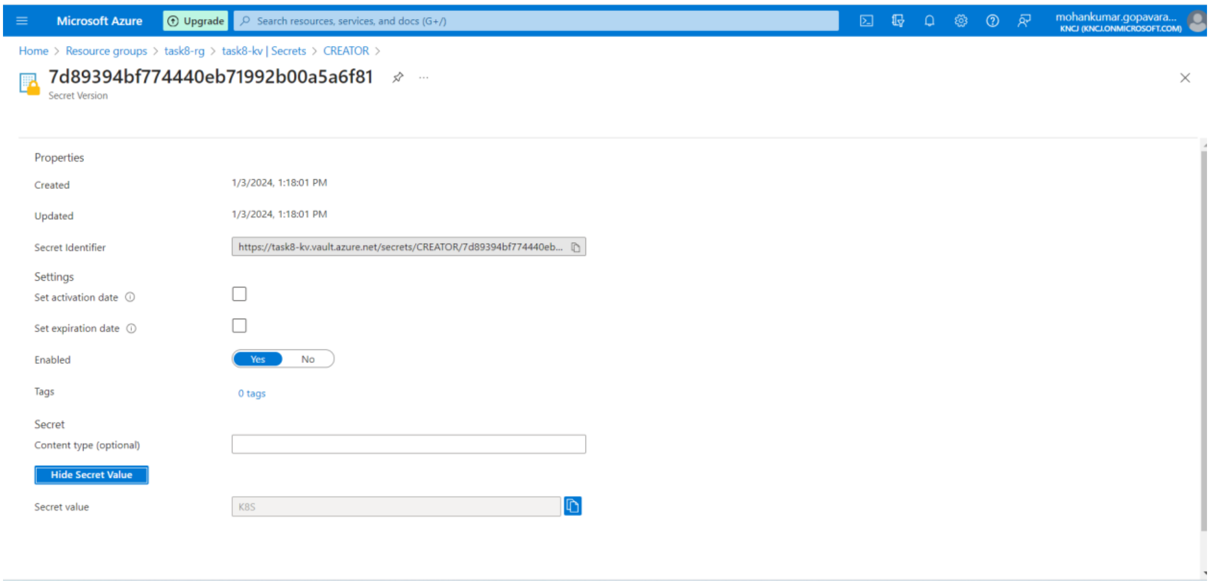
```
PS C:\Users\gmoha> kubectl get pods | Select-String -Pattern "python"

python-flask-webapp                          1/1     Running   0          53m
```



```
PS C:\Users\gmoha> kubectl exec -it python-flask-webapp -- ls /mnt/secrets-store/
CREATOR
PS C:\Users\gmoha> kubectl exec -it python-flask-webapp -- cat /mnt/secrets-store/CREATOR
K8S
```

Check whether the Key Vault secret value and secret volume mounted in pod is same or not



Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
mohankumar.gopavara...
KNCJ (KNCJ.ONMICROSOFT.COM)
Home > Resource groups > task8-rg > task8-kv | Secrets > CREATOR >

7d89394bf774440eb71992b00a5a6f81

Secret Version

Properties

Created 1/3/2024, 1:18:01 PM

Updated 1/3/2024, 1:18:01 PM

Secret Identifier https://task8-kv.vault.azure.net/secrets/CREATOR/7d89394bf774440eb...

Settings

Set activation date □

Set expiration date □

Enabled [✓ Yes] No

Tags 0 tags

Secret

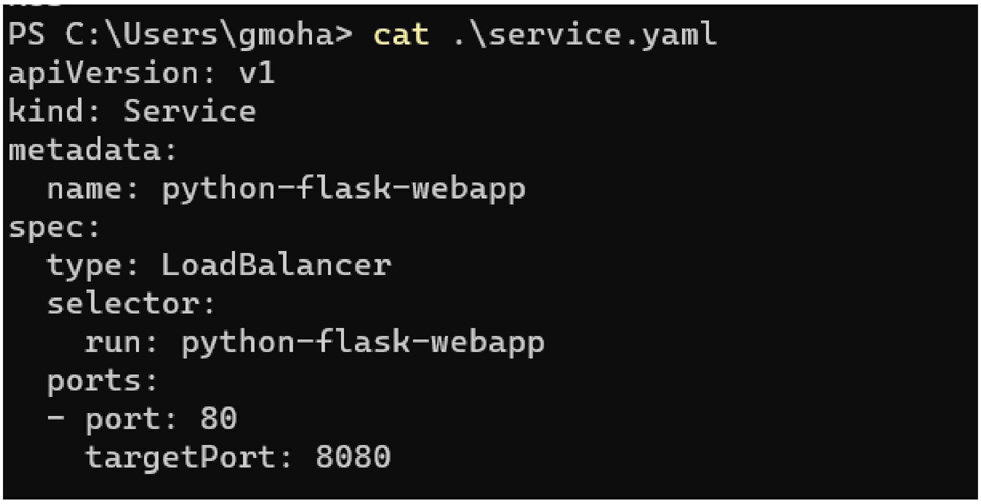
Content type (optional)

Hide Secret Value

Secret value K8S

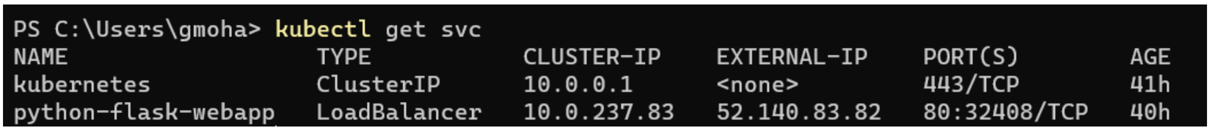
Create a Load Balancer Service to Access the Pod from web browser:

kubectl apply -f service.yaml



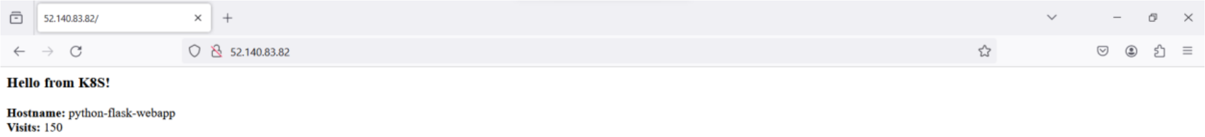
```
PS C:\Users\gmoha> cat .\service.yaml
apiVersion: v1
kind: Service
metadata:
  name: python-flask-webapp
spec:
  type: LoadBalancer
  selector:
    run: python-flask-webapp
  ports:
  - port: 80
    targetPort: 8080
```

Verify whether the service



```
PS C:\Users\gmoha> kubectl get svc
NAME                  TYPE           CLUSTER-IP     EXTERNAL-IP    PORT(S)        AGE
kubernetes            ClusterIP      10.0.0.1       <none>         443/TCP        41h
python-flask-webapp   LoadBalancer   10.0.237.83    52.140.83.82   80:32408/TCP   40h
```

Access the pod with load balancer IP address with port number 80



Hello from K8S!

Hostname: python-flask-webapp
Visits: 150