Contents

[Overview 1](#_Toc97233000)

[1. New AKS Cluster 1](#_Toc97233001)

[a) RBAC 1](#_Toc97233002)

[b) vNet 1](#_Toc97233003)

[c) TripsAPI Namespaces 1](#_Toc97233004)

[d) Availability (2 pods on 2 nodes) 1](#_Toc97233005)

[2. vNet 1](#_Toc97233006)

[3. Stuff 1](#_Toc97233007)

[4. Namespaces 1](#_Toc97233008)

[5. RBAC Roles 1](#_Toc97233009)

[a) Implement Azure RBAC for Kubernetes - success 1](#_Toc97233010)

[b) Test Azure RBAC for Kubernetes with Hacker1 - success 1](#_Toc97233011)

[c) Test Azure RBAC for Kubernetes with generic user oh6testc3 - success 1](#_Toc97233012)

[6. Deploy Tripinsights 1](#_Toc97233013)

[a) Verify Hacker6 Access to Kubernetes - success 1](#_Toc97233014)

[b) Attach Container Registry - success 1](#_Toc97233015)

[c) Apply YAML 1](#_Toc97233016)

[d) Web and API Users 1](#_Toc97233017)

# Overview

## New AKS Cluster

### RBAC

### vNet

### TripsAPI Namespaces

### Availability (2 pods on 2 nodes)

## vNet

(2 node (ha) + 1 node (scale) ) x ( 1 ip (node) + 5 Ips (pods) = 18

3 nodes x 31 ips/node (def) = 93 default

Scale this down if possible

vNet = 10.2.0.0/22 = 1024 10.2.0.0 - 10.2.3.255

vm-subnet = 10.2.0.0/24 = 256 - 5 ips = 251 ips 10.2.0.0 - 10.2.0.255

aks subnet 10.2.1.0/24 or use vm-subnet?

service subnet

docker subnet 172.17.0.1/16

## Stuff

az login

az aks get-credentials --resource-group oh6-aks-03 --name oh6aks03-cl01

az aks update -n oh6aks03-cl01 -g oh6-aks-03 --attach-acr registryavr8853

## Namespaces

kubectl apply -f namespaces-c3.yaml

kubectl get pods --namespace web

NAME READY STATUS RESTARTS AGE

tripviewer-deployment-865667bc54-pqk4m 1/1 Running 0 16m

kubectl get pods --namespace api

NAME READY STATUS RESTARTS AGE

poi-deployment-7d74c846cf-jk7vr 1/1 Running 0 12m

trips-5b6c56745-4lmmd 0/1 CreateContainerConfigError 0 28m

userjava-deployment-5f6c98fc95-bwcwg 1/1 Running 0 14m

userprofile-75c74c6fbc-c84kl 1/1 Running 0 11m

## RBAC Roles

See the "Trial and Error" version of this for more info.

Reference this link https://docs.microsoft.com/en-us/azure/aks/concepts-identity#summary

Portal create results in 1st option (Azure AD by member of an admin group)

I wanted 2nd option (Azure AD with Azure RBAC for Kubernetes Authorization).

I determined this with failed attempts to kubctl get pods. User needs to be in aksclusteradmin group.

To update use this https://docs.microsoft.com/en-us/azure/aks/manage-azure-rbac#integrate-azure-rbac-into-an-existing-cluster by CLI

Don't know if it can be done from portal during create?

To create role bindings scoped to namespaces requires CLI

https://docs.microsoft.com/en-us/azure/aks/concepts-identity#summary

These are the options for AAD/Azure RBAC integration which are relevant. https://docs.microsoft.com/en-us/azure/aks/concepts-identity#summary



Text

Description automatically generated

This is the cluster config from the portal.

Note for Role-based access control - Enables Kubernetes role-based access control which provides fine-grained control over cluster resources.

Note for AKS-managed Azure Active Directory - Configure Kubernetes role-based access control (RBAC) using Azure Active Directory group membership. This can be used to control access to specific namespaces inside your Kubernetes cluster based on a user's membership in specified Azure Active Directory groups. Once this feature is enabled, it cannot be disabled

Graphical user interface, text, application, email

Description automatically generated

These are the hacker6 roles, and group membership

Table

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Only the AAD group assigned as aks cluster admin at cluster create in portal has an aks role binding. This must be Azure AD by member of an admin group. And enableAzureRBAC is not set



Text

Description automatically generated

### Implement Azure RBAC for Kubernetes - success

https://docs.microsoft.com/en-us/azure/aks/manage-azure-rbac#integrate-azure-rbac-into-an-existing-cluster

*az aks update -g oh6-aks-03 -n oh6aks03-cl01 --enable-azure-rbac*

Apparently successful

*az aks show -g oh6-aks-03 -n oh6aks03-cl01|grep -i rbac*

A picture containing graphical user interface

Description automatically generated

Although don't see any role bindings yet



### Test Azure RBAC for Kubernetes with Hacker1 - success

**hacker1u5q@msftopenhack6878ops.onmicrosoft.com**

$04PjCujmY

\*not in clusteradmin group (or owner of it for completeness)

\*user has no roles assigned and kubectl get pods fails as expected

Text

Description automatically generated

\*now add just Azure Kubernetes Service Cluster User and Azure Kubernetes Service RBAC Cluster Admin, wait 5 mins, and just like that - it works

Text

Description automatically generated

### Test Azure RBAC for Kubernetes with generic user oh6testc3 - success

\*just for completeness validate with oh6testc3 - plain user, no rights, no groups and cannot do anything; user cannot do anything

Text

Description automatically generated

## Deploy Tripinsights

### Verify Hacker6 Access to Kubernetes - success

Text

Description automatically generated

### Attach Container Registry - success

It should be there, I did it during cluster setup but can't find reference in portal or cli

az aks update -n oh6aks01-cl01 -g oh6-aks-01 --attach-acr registryavr8853

A screenshot of a computer

Description automatically generated with medium confidence

### Apply YAML

#### I think the keyvault integration breaks secrets - secret store csi driver

It can be turned off in portal. Could not get secrets to work until it was off. Tried with and without namespaces.

Turned back on, redid deployment, did not break this time.

\*namespaces first

\*need to redo secrets - make yaml

**sqlcmd -S sqlserveravr8853.database.windows.net -d mydrivingDB -U sqladminaVr8853 -P 'Password123!"**

echo -n 'sqladminaVr8853' > ./username.txt

echo -n 'Password123!' > ./password.txt

**default ns**

kubectl create secret generic db-user-pass --from-file=password=./password.txt --from-file=username=./username.txt

secret/db-user-pass created

shpopov$ kubectl get secret

NAME TYPE DATA AGE

db-user-pass Opaque 2 12s

default-token-fthbf kubernetes.io/service-account-token 3 19h

shpopov$ kubectl get deployment

No resources found in default namespace.

shpopov$ kubectl apply -f trips-secret-c3.yaml

deployment.apps/trips created

service/trips-service created

**api ns ! reqired by ns**

shpopov$ kubectl create secret generic db-user-pass --from-file=password=./password.txt --from-file=username=./username.txt **--namespace=api**

kubectl apply -f *file-c3.yaml*

kubectl get pods --namespace=api

kuebctl get pods --namespace=web

kubectl get service --all-namespaces

### Configure RBAC for Web Dev and API Dev Users

**web-dev** user (View access for API resources, Edit access for Web resources).

[**webdev@msftopenhack6878ops.onmicrosoft.com**](mailto:webdev@msftopenhack6878ops.onmicrosoft.com) **/ Javo1832 / Openhack123!**

**needs**

**Azure Kubernetes Service User - for basic access**

**Azure Kubernetes Service RBAC Reader for api**

**Azure Kubernetes Service RBAC Writer for web**

**api-dev** user (View access to Web resources, Edit access to API resources)

[**apidev@msftopenhack6878ops.onmicrosoft.com**](mailto:apidev@msftopenhack6878ops.onmicrosoft.com) **/ Wuru5216 / Openhack123!**

**Azure Kubernetes Service Cluster User - for basic access**

**Azure Kubernetes Service RBAC Reader for web**

**Azure Kubernetes Service RBAC Writer for api**

**Will just do for web-dev**

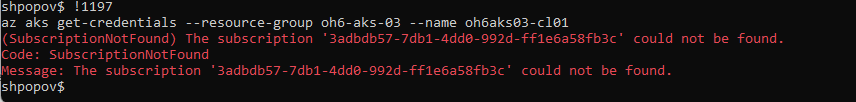
AKS\_ID=$(az aks show -g oh6-aks-03 -n oh6aks03-cl01 --query id -o tsv)

**/subscriptions/9c6ff056-c6b2-4256-9a64-d908474e1191/resourcegroups/oh6-aks-03/providers/Microsoft.ContainerService/managedClusters/oh6aks03-cl01**

**az role assignment create --role "Azure Kubernetes Service RBAC Reader" --assignee** [**webdev@msftopenhack6878ops.onmicrosoft.com**](mailto:webdev@msftopenhack6878ops.onmicrosoft.com) **--scope $AKS\_ID/namespaces/api**

**az role assignment create --role "Azure Kubernetes Service RBAC WRiter" --assignee** [**webdev@msftopenhack6878ops.onmicrosoft.com**](mailto:webdev@msftopenhack6878ops.onmicrosoft.com) **--scope $AKS\_ID/namespaces/web**

With no roles - can't access cluster at all - complains about no subscriptions



With Azure Kubernetes Service Cluster User get access to cluster but can't return anything

A picture containing text

Description automatically generated

### Validate Cluster Namespace Access for webdev User - success

In api namespace can describe but not delete pods

In web namespace and describe and delete pods

## Connectivity

Put cluster in the "wrong" vnet so stood up a vm in cluster vNet.

Confirm ping 10.240.0.36 (vm) from pod

Text

Description automatically generated

# Success Criteria

**Done : Your team** successfully created an RBAC enabled AKS cluster within the address space allocated to you by the network team

**Done:**  **Your team** successfully redeployed the TripInsights application, now segmented into api and web namespaces, into the cluster

DO: **Your team** must demonstrate connectivity to and from your cluster by being able to reach the internal-vm (already deployed)

**Done**: **Your team** must demonstrate that you are prompted on cluster access to authenticate with AAD

**Done**: **Different members** of your team must be able to connect to your cluster using the **api-dev** and **web-dev** AAD users and demonstrate appropriate access levels