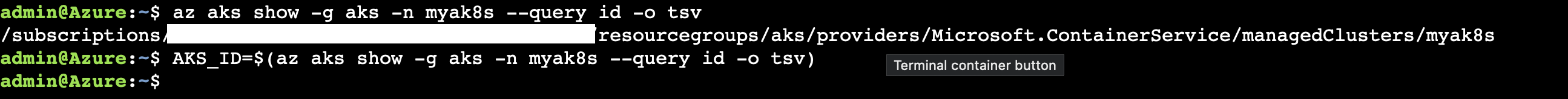
1. Aks role base access configure

During the creation process, make sure to enable “AKS-Managed AAD”

Graphical user interface, text

Description automatically generated

Assign Aks id value to a variable



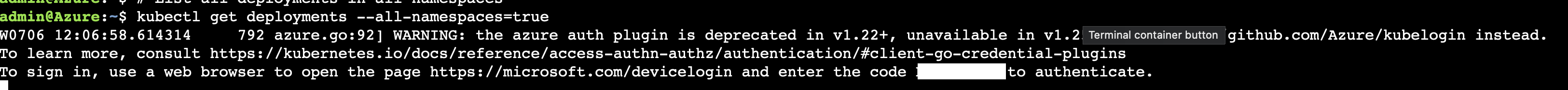
Previously we already selected admin user account. If not -> create admin role

az role assignment create --role "Azure Kubernetes Service RBAC Admin" --assignee <userAccount> --scope $AKS\_ID

get credential: az aks get-credentials --resource-group aks --name myak8s

list all the namespace:

kubectl get deployments --all-namespaces=true



Graphical user interface, text

Description automatically generated

A picture containing diagram

Description automatically generated

Assign reader role for an AAD user devops1 user

Text

Description automatically generated

Or create custom role assign to specific user

{

"Name": "AKS Deployment Reader",

"Description": "Lets you view all deployments in cluster/namespace.",

"Actions": [],

"NotActions": [],

"DataActions": [

"Microsoft.ContainerService/managedClusters/apps/deployments/read"

],

"NotDataActions": [],

"assignableScopes": [

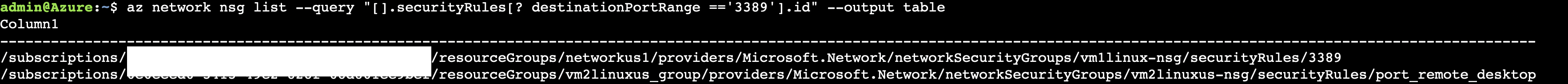
"/subscriptions/<YOUR SUBSCRIPTION ID>"

]

}

1. Ensure that no network security groups allow unrestricted inbound access on TCP port 3389 (Remote Desktop Protocol – RDP).
   1. List all the 3389 rules

az network nsg list --query "[].securityRules[? destinationPortRange =='3389'].id" --output table



* 1. Delete those rule

az network nsg rule delete --ids <id1> <id2> <idn>

note: space-delimited

Text

Description automatically generated

1. Ensure there is a sufficient daily backup retention period configured for Azure virtual machines

Go to Azure Portal -> Select VM -> Backup -> Enable Backup if it is not enabled:

Select proper policy

Graphical user interface, text

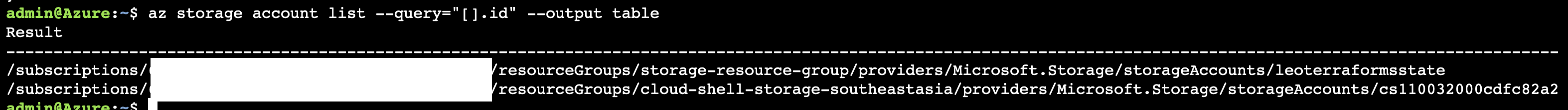
Description automatically generated

Text

Description automatically generated

1. Ensure that Azure Blob Storage service has a lifecycle management policy configured.
   1. List all the Azure blob storage account

az storage account list --query="[].id" --output table



* 1. List all the policy if it has in above storage accounts

az storage account management-policy show --account-name <storage account> --resource-group <rg-name>

Text

Description automatically generated

* 1. Add your life cycle policy by go to Azure portal (or use az cli) Storage account -> life Cycle management -> add rule to match the requirements

Graphical user interface, application

Description automatically generated

1. Enable HTTP to HTTPS redirects for your Microsoft Azure App Service web applications.

Go to web application -> configuration -> enable Https Only -> save

Graphical user interface, text, application, Teams

Description automatically generated