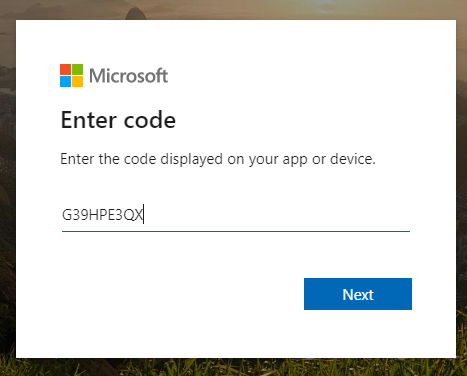
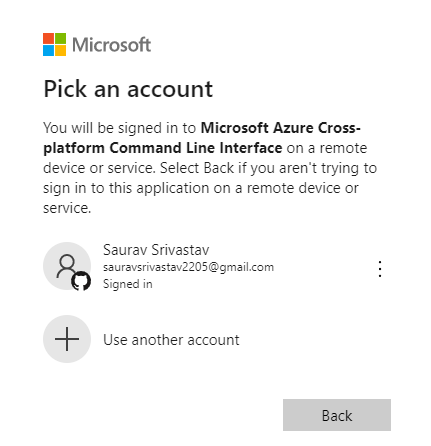
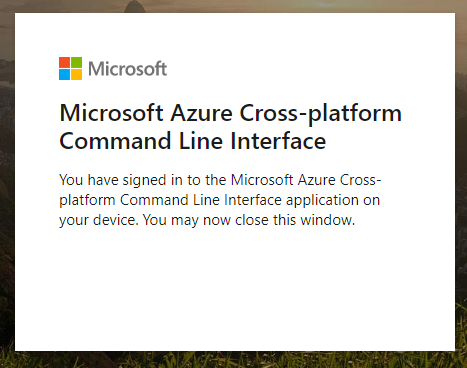
**A) Create a container registry**

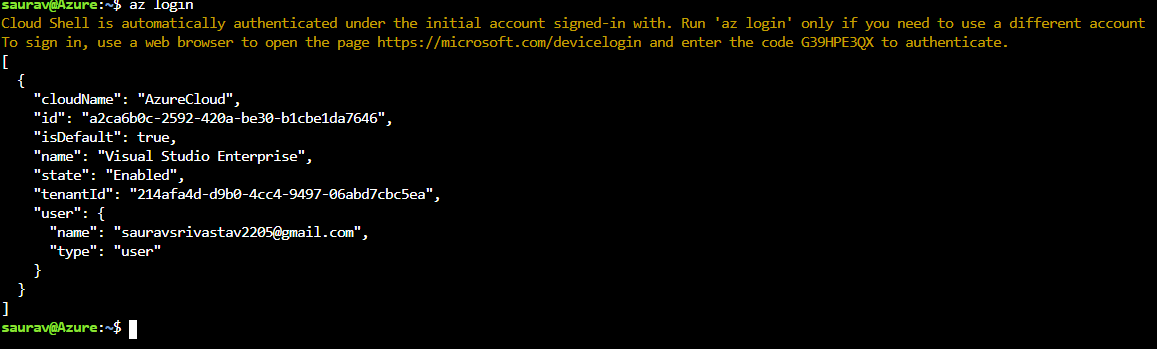
Step1: Login: az login





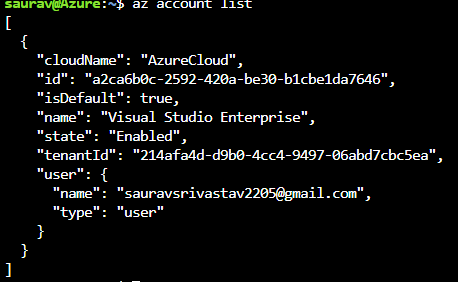






Step2: Review and Select Subscription:

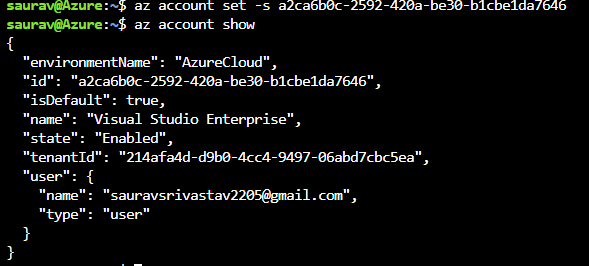
> List - az account list



> Choice - az account set -s <subscription id>

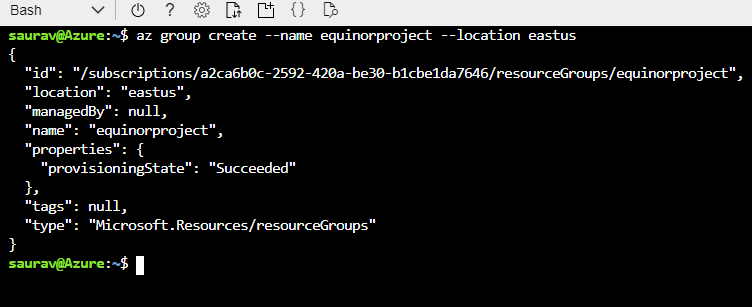
az account set -s a2ca6b0c-2592-420a-be30-b1cbe1da7646

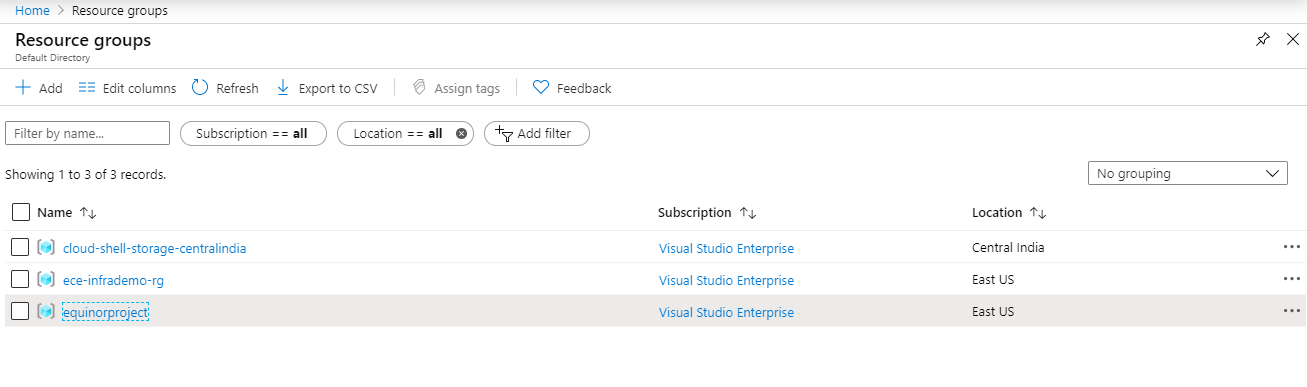
> Verification - az account show



Step3: Creating a resource group:

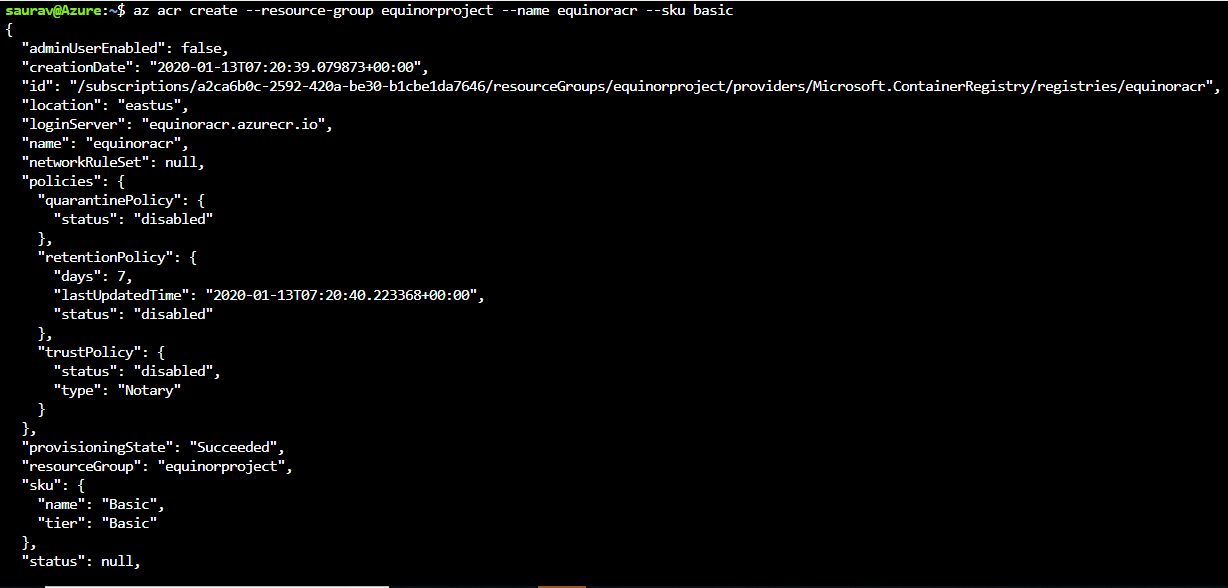
az group create --name equinorproject --location eastus

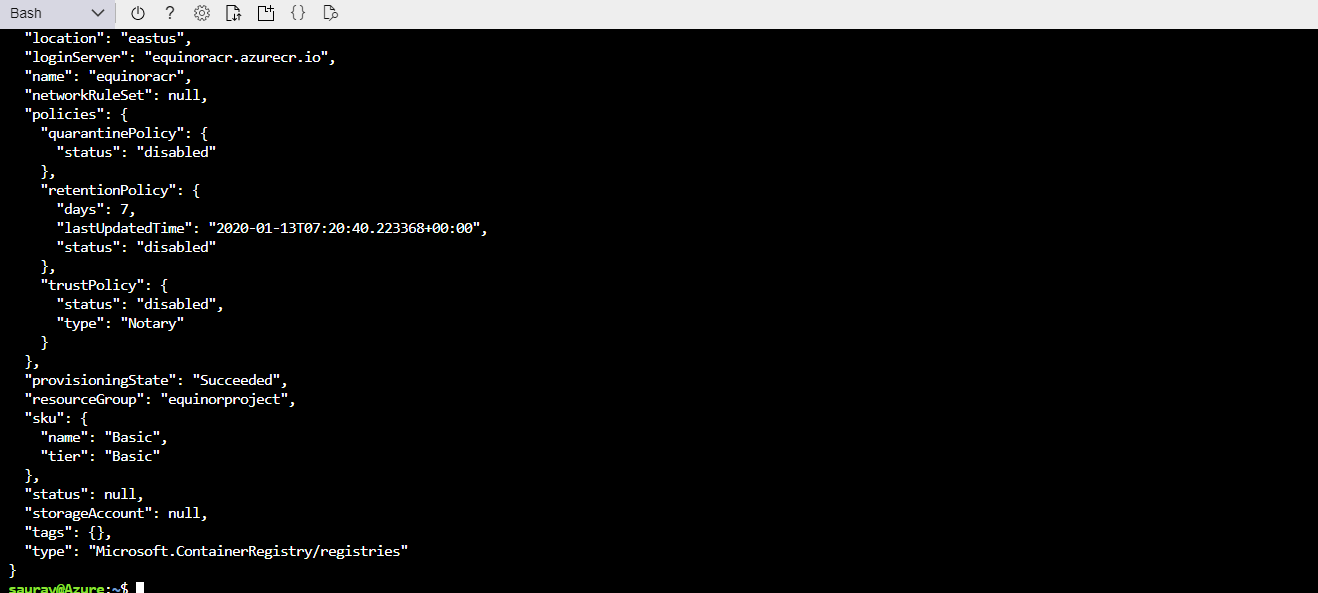


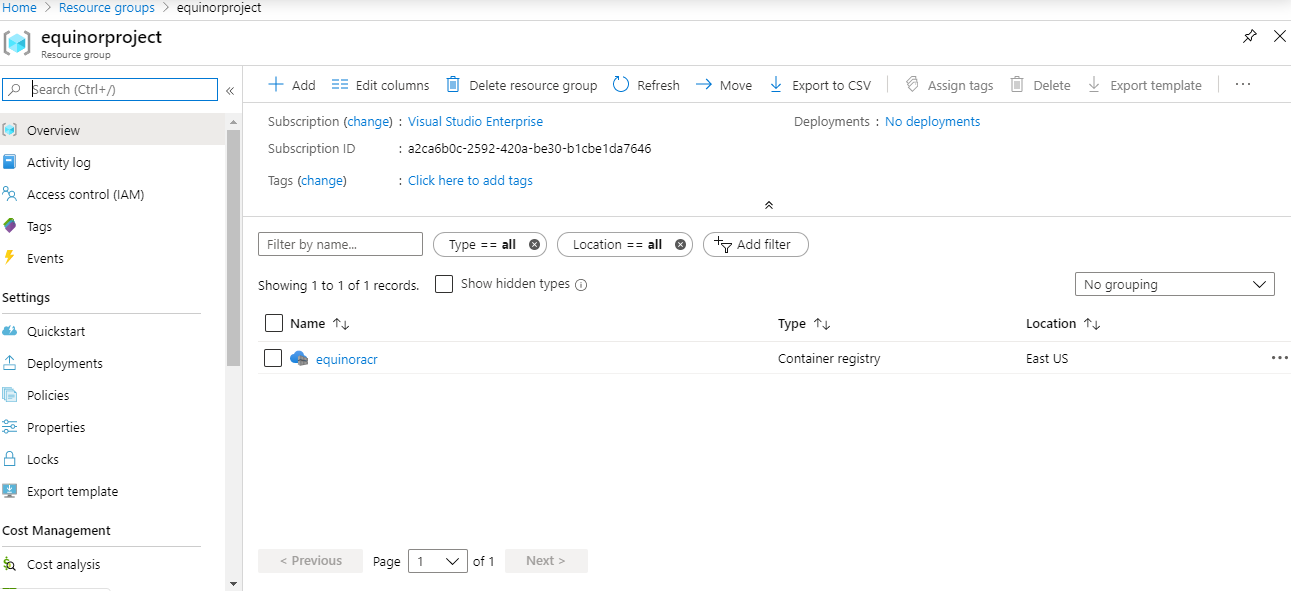


Step4: Creating a container registry (ACR):

az acr create --resource-group equinorproject --name equinoracr --sku basic







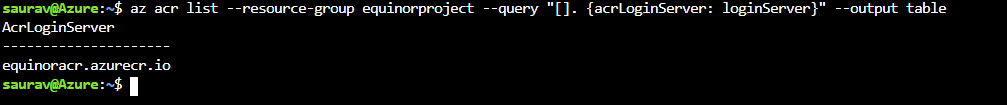
Step5: Login to Container Registry (ACR):

az acr login -n equinoracr



Step6: Get the login server name of the container registry (ACR):

az acr list --resource-group equinorproject --query "[]. {acrLoginServer: loginServer}" --output table



Step7: Check the image pushed to the container registry (ACR):

az acr repository list --name equinoracr --output table

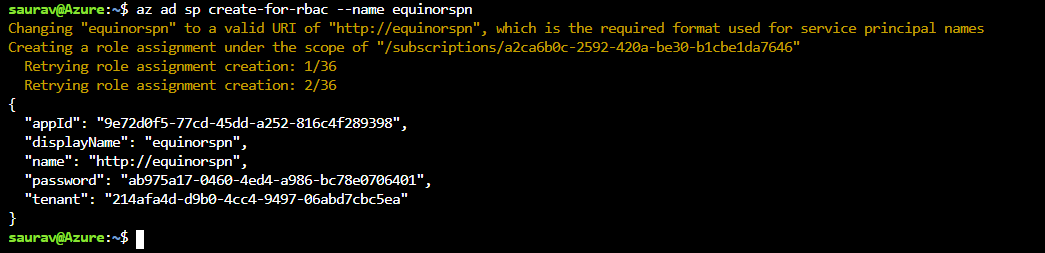
B) Creation Of Azure Kubernetes Cluster

Step1: Creating a service principal

In the Azure version of SPN , even if thesubscription is changed, can you maintain the authority to operate from azure-cli.

> az ad sp create-for-rbac --skip-assignment

> az ad sp create-for-rbac --name equinorspn



The above values ​​can be confirmed from the following command.(Search the output file based on "azure-cli-" of displayName)

> az ad sp list> sp\_list.txt

Once created, it can be reused because it remains, even if ResourceGroup is deleted.

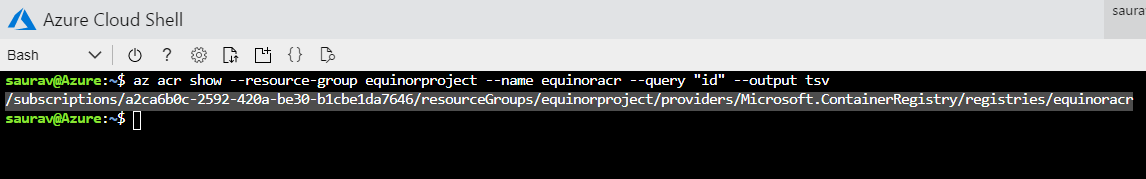
However, if you do not write down the password, you cannot reuse it.

In that case, delete and re-create using the following command.

> az ad sp delete --id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

Step2: Grant authority to ACR.

> az acr show --resource-group equinorproject --name equinoracr --query "id" --output tsv



Step3: Grant ACR acrpull privileges to the service principal.

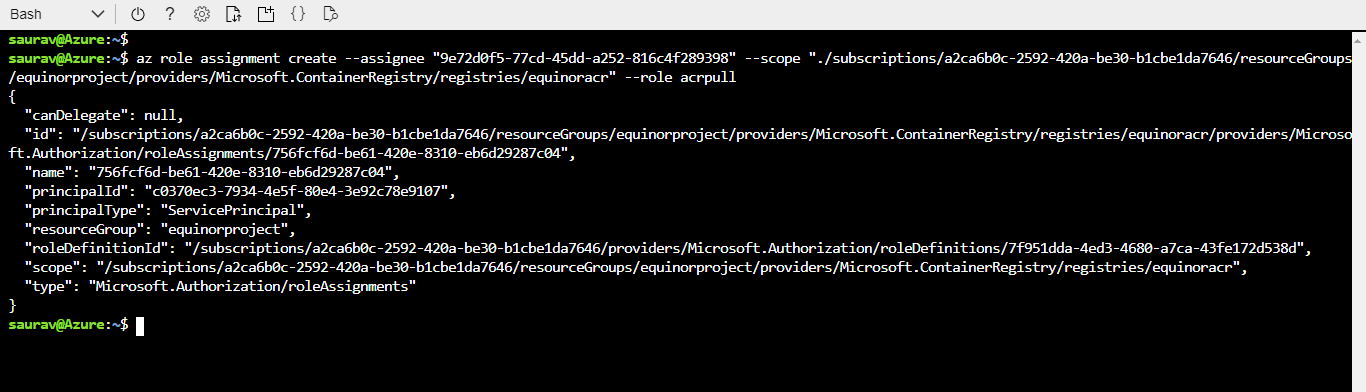
appId: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

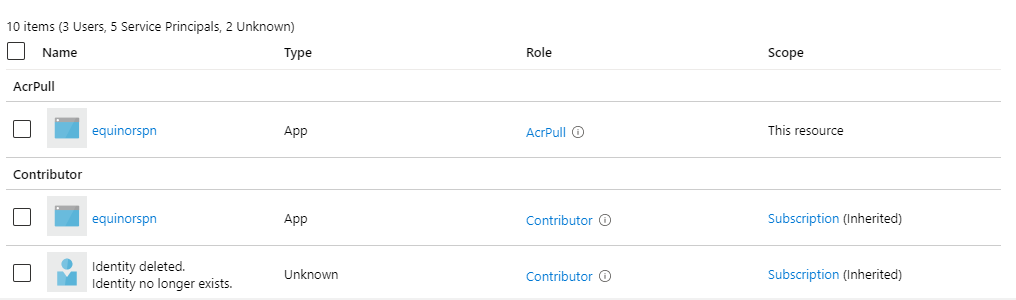
AcrId:./Subscriptions/xxxxxxxxxxxx-Xxxxxxxx-xxxxxxxxxxxx/ResourceGroups/Daisukenishino/Providers/Microsoft ContainerRegistry ?/Registries/equinoracr

./subscriptions/a2ca6b0c-2592-420a-be30-b1cbe1da7646/resourceGroups/equinorproject/providers/Microsoft.ContainerRegistry/registries/equinoracr

> az role assignment create --assignee "<appId>" --scope "<acrId>" --role acrpull

> az role assignment create --assignee "9e72d0f5-77cd-45dd-a252-816c4f289398" --scope "./subscriptions/a2ca6b0c-2592-420a-be30-b1cbe1da7646/resourceGroups/equinorproject/providers/Microsoft.ContainerRegistry/registries/equinoracr" --role acrpull





Step 4: Creating a cluster During creation, an SSH key is created in the user directory under .ssh.

appId: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

password: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

> az aks create --resource-group equinorproject --name equinoroaks --node-count 2 --service-principal <appId> --client-secret ab975a17-0460-4ed4-a986-bc78e0706401 --generate-ssh-keys

>az aks create --resource-group equinorproject --name equinoroaks --node-count 2 --service-principal 9e72d0f5-77cd-45dd-a252-816c4f289398 --client-secret ab975a17-0460-4ed4-a986-bc78e0706401 --generate-ssh-keys

