**AKS Installation**

As a result of architectural design, three Azure Kubernetes Services (AKS) clusters, which are separated by environmental situation, are decided installed using Azure CLI.

As known, Resource Group is one of the important object of Azure in order to create and gather all related object in it. Thus, three Resource Group are created which are called CommercialNonProdRG, CommercialPreProdRG, CommercialProdRG and all these groups are at the West Europe Datacenter of Microsoft Azure. Accomplished by the following commands:

* ***az group create -l westeurope -n CommercialNonProdRG***
* ***az group create -l westeurope -n CommercialPreProdRG***
* ***az group create -l westeurope -n CommercialProdRG***

Before these installation operation and according to environmental separation, the network segmentation of these clusters have high priority. Because of this, the network of these are separated also with names as shown below table 1.1 and this operation accomplish with Azure CLI. This CLI command is included virtual network address and subnet information. (Network addresses are internal and these segmentation and operations responsibility belongs to Network team.)

|  |  |  |  |
| --- | --- | --- | --- |
| **Cluster Name** | **VNET Name** | **VNET Address** | **Subnet Address** |
| CommercialProd | CommercialProdVNet | 10.242.32.0/20 | 10.242.32.0/24 |
| CommercialPreProd | CommercialPreProdVNet | 10.242.16.0/20 | 10.242.16.0/24 |
| CommercialNonProd | CommercialNonProdVNet | 10.242.0.0/20 | 10.242.0.0/24 |

Table 1.1

Accomplished by the following commands:

* **az network vnet create --resource-group CommercialProdRG --name CommercialProdVNet --address-prefixes 10.242.32.0/20 --subnet-name CommercialProdSubnet --subnet-prefix 10.242.32.0/24**
* **az network vnet create --resource-group CommercialPreProdRG --name CommercialPreProdVNet --address-prefixes 10.242.16.0/20 --subnet-name CommercialPreProdSubnet --subnet-prefix 10.242.16.0/24**
* **az network vnet create --resource-group CommercialNonProdRG --name CommercialNonProdVNet --address-prefixes 10.242.0.0/20 --subnet-name CommercialNonProdSubnet --subnet-prefix 10.242.0.0/2**

After the creation of vnet as desired for the clusters, Service Principles for three clusters are created by following command using Azure CLI:

* **az ad sp create-for-rbac --output json**

*Note: Instead of having applications sign in as a fully privileged user, Azure offers service principals. An Azure service principal is an identity created for use with applications, hosted services, and automated tools to access Azure resources.*

The result of the command should be noted in order to use following steps.

After that, two variables, which are called VNET\_ID and SUBNET\_ID, are exported with the help of Azure CLI and these are stored to create AKS cluster. Additionally, you can use these values as clear text, but this possibility is very open to make a mistake. Accomplished by the following commands:

NonProduction:

* **$VNET\_ID=(az network vnet show --resource-group CommercialNonProdRG --name CommercialNonProdVNet --query id -o tsv)**
* **$SUBNET\_ID=(az network vnet subnet show --resource-group CommercialNonProdRG --vnet-name CommercialNonProdVNet --name CommercialNonProdSubnet --query id -o tsv)**

PreProduction:

* **$VNET\_ID=(az network vnet show --resource-group CommercialPreProdRG --name CommercialPreProdVNet --query id -o tsv)**
* **$SUBNET\_ID=(az network vnet subnet show --resource-group CommercialPreProdRG --vnet-name CommercialPreProdVNet --name CommercialPreProdSubnet --query id -o tsv)**

Production:

* **$VNET\_ID=(az network vnet show --resource-group CommercialProdRG --name CommercialProdVNet --query id -o tsv)**
* **$SUBNET\_ID=(az network vnet subnet show --resource-group CommercialProdRG --vnet-name CommercialProdVNet --name CommercialProdSubnet --query id -o tsv)**

Using Service Principle outputs (Especially App ID) and VNET\_ID and SUBNET\_ID variable assignment, the role for the installation of cluster are created. By this way, the company use minimal role and authorization.

* **az role assignment create --assignee "<APP\_ID>" --scope $VNET\_ID --role Contributor**

After all above steps, the following command is ran to install Azure Kubernetes Services Clusters using Azure CLI:

Production:

* **az aks create --resource-group CommercialProdRG --name CommercialProd --node-count 2 --generate-ssh-keys --network-plugin kubenet --service-cidr 10.240.0.0/20 --dns-service-ip 10.240.0.10 --pod-cidr 10.241.0.0/16 --docker-bridge-address 172.17.0.1/16 --vnet-subnet-id $SUBNET\_ID --service-principal "<APP\_ID\_FROM\_SP>" --client-secret "<PASSWORD\_FROM\_SP>" --network-policy calico**

PreProduction:

* **az aks create --resource-group CommercialPreProdRG --name CommercialPreProd --node-count 2 --generate-ssh-keys --network-plugin kubenet --service-cidr 10.240.0.0/20 --dns-service-ip 10.240.0.10 --pod-cidr 10.241.0.0/16 --docker-bridge-address 172.17.0.1/16 --vnet-subnet-id $SUBNET\_ID --service-principal "<APP\_ID\_FROM\_SP>" --client-secret "<PASSWORD\_FROM\_SP>" --network-policy calico**

NonProduction:

* **az aks create --resource-group CommercialNonProdRG --name CommercialNonProd --node-count 2 --generate-ssh-keys --network-plugin kubenet --service-cidr 10.240.0.0/20 --dns-service-ip 10.240.0.10 --pod-cidr 10.241.0.0/16 --docker-bridge-address 172.17.0.1/16 --vnet-subnet-id $SUBNET\_ID --service-principal "<APP\_ID\_FROM\_SP>" --client-secret "<PASSWORD\_FROM\_SP>" --network-policy calico**

To make installation verification and connect to clusters, use the following commands:

Production:

* **az aks get-credentials -g CommercialProdRG --name CommercialProd**
* **kubectl get nodes**

PreProduction:

* **az aks get-credentials -g CommercialPreProdRG --name CommercialPreProd**
* **kubectl get nodes**

NonProduction:

* **az aks get-credentials -g CommercialNonProdRG --name CommercialNonProd**
* **kubectl get nodes**

The explanation of parameters are shown as table 1.2:

|  |  |
| --- | --- |
| **Parameter** | **Explanation** |
| --name -n | Name of the managed cluster. |
| --resource-group -g | Name of resource group. You can configure the default group using az configure --defaults group=<name>. |
| --node-count -c | Number of nodes in the Kubernetes node pool. After creating a cluster, you can change the size of its node pool with az aks scale. |
| --generate-ssh-keys | Generate SSH public and private key files if missing. The keys will be stored in the ~/.ssh directory. |
| --network-plugin | The Kubernetes network plugin to use. |
| --service-cidr | A CIDR notation IP range from which to assign service cluster IPs. |
| --dns-service-ip | An IP address assigned to the Kubernetes DNS service. |
| --pod-cidr | A CIDR notation IP range from which to assign pod IPs when kubenet is used. |
| --docker-bridge-address | A specific IP address and netmask for the Docker bridge, using standard CIDR notation. |
| --vnet-subnet-id | The ID of a subnet in an existing VNet into which to deploy the cluster. |
| --service-principal | Service principal used for authentication to Azure APIs. This argument is required if --reset-service-principal is specified. |
| --client-secret | Secret associated with the service principal. This argument is required if --service-principal is specified. |
| --network-policy | The Kubernetes network policy to use. |