|  |
| --- |
| GSP342 : Ensure Access & Identity in Google Cloud: Challenge Lab :- |
|  |  |
|  | ---------------------------------------------------------------------------------------------------------------------------------------------- |
|  |  |
|  | Task 1 : Create a custom security role :- |
|  |  |
|  | nano role-definition.yaml |
|  |  |
|  | // Copy the below content to file :- |
|  |  |
|  | title: "orca\_storage\_update" |
|  | description: "Permissions" |
|  | stage: "ALPHA" |
|  | includedPermissions: |
|  | - storage.buckets.get |
|  | - storage.objects.get |
|  | - storage.objects.list |
|  | - storage.objects.update |
|  | - storage.objects.create |
|  |  |
|  | // Save by : ctrl + o -> enter -> ctrl + x |
|  |  |
|  | gcloud iam roles create orca\_storage\_update --project $DEVSHELL\_PROJECT\_ID \ |
|  | --file role-definition.yaml |
|  |  |
|  | ---------------------------------------------------------------------------------------------------------------------------------------------- |
|  |  |
|  | Task 2 & 3 : Create a service account and Bind a custom security role to an account :- |
|  |  |
|  | // Navigate to IAM & Admin -> Service Accounts -> CREATE SERVICE ACCOUNT. |
|  |  |
|  | Service account name : orca-private-cluster-sa , then click create and add roles. |
|  | Roles : orca\_storage\_update |
|  | Monitoring Viewer |
|  | Monitoring Metric Writer |
|  | Logs Writer |
|  |  |
|  | // Click CONTINUE -> DONE |
|  |  |
|  | ---------------------------------------------------------------------------------------------------------------------------------------------- |
|  |  |
|  | Task 4 : Create and configure a new Kubernetes Engine private cluster :- |
|  |  |
|  | // Replace the project id :- |
|  |  |
|  | gcloud container clusters create orca-test-cluster --num-nodes 1 --master-ipv4-cidr=172.16.0.64/28 --network orca-build-vpc --subnetwork orca-build-subnet --enable-master-authorized-networks --master-authorized-networks 192.168.10.2/32 --enable-ip-alias --enable-private-nodes --enable-private-endpoint --service-account orca-private-cluster-sa@<Project ID>.iam.gserviceaccount.com --zone us-east1-b |
|  |  |
|  | ---------------------------------------------------------------------------------------------------------------------------------------------- |
|  |  |
|  | Task 5 : Deploy an application to a private Kubernetes Engine cluster :- |
|  | // SSH to orca-jumphost VM instance |
|  |  |
|  | // Replace the project id :- |
|  |  |
|  | gcloud container clusters get-credentials orca-test-cluster --internal-ip --zone us-east1-b --project <Project ID> |
|  |  |
|  | kubectl create deployment hello-server --image=gcr.io/google-samples/hello-app:1.0 |