gcloud Incident Investigation Quick Reference Cheat Sheet

by casimkhan via cheatography.com/184196/cs/38390/

GCP Logging

Default Logs

Following are the logs generally available for GCP

Activity Logs: Record of all activity within a user's GCP project, including operations performed by users, systems, and services.

System Logs: Record of system-level events and messages related to the health and performance of GCP services.

Audit Logs: Record of administrative and security-related activity, including authentication and authorization events, resource management operations, and data access events.

IAM commands

gcloud iam - manage IAM service accounts and keys

#To list account name
gcloud auth list
gcloud auth activate-service-account [ACCOUNT]
gcloud auth print-identity-token --impersonate-service-account=-SA@PROJECT_ID.iam.gserviceaccount.com
#Check token info
curl "https://oauth2.googleapis.com/tokeninfo?id_token=ID_TOKEN"
#Revoke token
gcloud auth revoke
#Find iam roles for organisation
gcloud iam roles list --organization=my-org-id
#Find Specific role
gcloud iam roles list --organization=my-org-id | grep [role-name]

IAM commands (continue)

#Search iam policies to specific user on project
gcloud projects get-iam-policy [project-id] --flatten="bindings-[].members" --filter="example-users@example.com"
#Search iam policies to specific user across organization
gcloud asset search-all-iam-policies --scope=organizations/[organization_id] --query='policy:example-user@example.com'
#Search specific role on specific project
gcloud asset search-all-iam-policies --scope=projects/[project-name] --query='policy:roles/owner'

GCP Folders commands

gcloud alpha resource-manager folders - manage Cloud Folders

#List folder for a specific organization
gcloud alpha resource-manager folders list --organization=my--org-id
#List folder within folder
gcloud alpha resource-manager folders list --folder=my-folder-id

gcloud SDK

Google Cloud CLI installation

https://cloud.google.com/sdk/docs/install

gcloud commands reference

https://cloud.google.com/sdk/gcloud/reference

GCP Projects commands

gcloud projects - create and manage project access policies

#List projects within organization
gcloud projects list --filter 'parent.id=my-org-id AND parent.type=organization'
#List project label information
gcloud projects describe my-project
#View iam policies which user is member of what
gcloud projects get-iam-policy my-project

GCP Organization commands

gcloud organizations - create and manage GCP Organizations

#List available organizations for tenant
gcloud organizations list
#Detail description
gcloud organizations describe my-org_id
#Show what policies are enable
gcloud resource-manager org-policies list --organization=my--org-id --show-unset
#Show all projects within an Organization (e.g Org_name) by looking at labels
gcloud projects list --format=json | jq '.[].labels | select(.organisation =="my_org_name")' | grep projectname | sort -u | wc -l

IAM commands (continue)

#Find specific reviewer role permissions
gcloud iam roles describe [role--name] --organization=my-org-id
#Search for a specific permission for a given organization
gcloud asset search-all-iam-policies --scope=organizations/[organization-id] --query='policy.role.permissions:resourcemanager.projects.setIamPolicy'
#Finding keys creation and expiration date/time of a specific iam service account
gcloud iam service-accounts keys list --iam-account=[example@iam.gserviceaccount.com]

GCP Bucket commands

gcloud storage - create and manage Cloud Storage buckets and objects

#To list buckets for specific project
gsutil ls -p my-project
#Prints the object size, creation time stamp, and name of each matching object
gsutil ls -l gs://bucket/*.html* *gs://bucket/*.txt
#Print additional details
gsutil ls -L gs://my-project/
#List objects within bucket (--recursive)
gcloud storage objects list gs://my-project/ --limit=1
gcloud storage ls --recursive gs://my-project/

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com

gcloud Incident Investigation Quick Reference Cheat Sheet

by casimkhan via cheatography.com/184196/cs/38390/

Basic Initialization commands

Initial setup tasks

```
gcloud init
#To verify existing config
gcloud config list OR gcloud info
#To set Project
gcloud config set project [proje-
ct-name]
#To remove project
gcloud config unset project
[project-name]
```

Compute commands

gcloud compute - create and manipulate Compute Engine resources

```
#To list compute images for
particular project
gcloud compute images list --
project=[project-id]
#To list compute instances for
particular project
gcloud compute instances list --
project=[project-id]
#Detail description about the
instance
gcloud compute instances
describe my-instance --project-
=my-project
#View in different formatting
gcloud compute instances
describe my-instance --project-
=my-project --format=flattened
```

Disk and Snapshots commands

Read and manipulate Compute Engine disks/snapshots

```
#List disks for a specific project
gcloud compute disks list --proj-
ect=my-project
#Read metadata info for a
specific disk
gcloud compute disks describe
my-disk-name --zone=country--
southeast1-a --project=my-pr-
oject
#List snapshots for a project
gcloud compute snapshots list --
project=my-project
#Count of snapshots within
specific projects
gcloud compute snapshots list --
project=my-project --format='va-
lue(NAME)' | wc -l
```

Disk and Snapshots commands (continue)

```
#Create a snapshot of a
persistent disk in zone us-cen-
tral1-a
gcloud compute disks snapshot
test --zone=us-central1-a --
snapshot-names=snapshot-test
--description="Example snapsh-
ot"
#Create an image from a
snapshot
gcloud compute images create
my-image --source-snapshot=-
source-snapshot
#Export a VMDK file my-image
from a project to a Storage
bucket
gcloud compute images export -
-image=my-image --destination-
uri=gs://my-bucket/my-ima-
ge.vmdk --export-format=vmdk -
-project=my-project
```

Incident Investigation commands

List of useful commands for incident investigation

```
#List logs available for project
gcloud logging logs list --project-
=my-project
#Logs with matching insertId
gcloud logging read insertId="-
my-InsertId" --project=my-pr-
oject
# Json format with jq filter on
source ip
gcloud logging read insertId="-
my-InsertId" --project=my-pr-
oject --format=json | jq '.[] .proto-
Payload.requestMetadata.cal-
lerIp'
```

Incident Investigation commands (continue)

```
#By default search return result
for past 1 day
#Use freshness to go beyond 1
day
--freshness=7d
# Finding logs by Principal Email
address
gcloud logging read "protoPayl-
oad.authenticationInfo.princip-
alEmail:'youremail@domain'" --
project=my-project --form-
at=json --limit=1
#Finding logs for specific time
gcloud logging read 'timestam-
p>="2023-01-30T18:50:59Z"
AND timestamp<="2023-01-31-
T00:00:00Z"' --project=my-pr-
oject --format=json
```

Incident Investigation commands (continue)

```
#Timestamp Z shows that its in
UTC format
#To read logs from specific log
source and filter activity
matching on time
gcloud logging read 'logName=-
projects/[my-project]/logs/clo-
udaudit.googleapis.com%2Fac-
tivity' --project=my-project --
format=json | jq '.[] | select(.t-
imestamp >= "2023-02-03T00:2-
0:18.984704107Z")' | grep
callerIp
```

Incident Investigation commands (continue)

```
#Timestamp Z shows that its in
UTC format
#To read logs from specific log
source and filter activity
matching on time
gcloud logging read 'logName=-
projects/[my-project]/logs/clo-
udaudit.googleapis.com%2Fac-
tivity' --project=my-project --
format=json | jq '.[] | select(.t-
imestamp >= "2023-02-03T00:2-
0:18.984704107Z")' | grep
callerIp
```


Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com