Monitoring Container Operations in Oracle Cloud Container Engine for Kubernetes

LOGGING AND ANALYZING LOGS FROM AUDIT



Craig Golightly
SENIOR SOFTWARE CONSULTANT

@seethatgo www.seethatgo.com



Oracle Cloud Container Engine for Kubernetes





Managed Kubernetes Service
Oracle Cloud Infrastructure

Container Cluster

Deployed and running in
Oracle Kubernetes Engine (OKE)



Audit Log



Available in Oracle Cloud web console

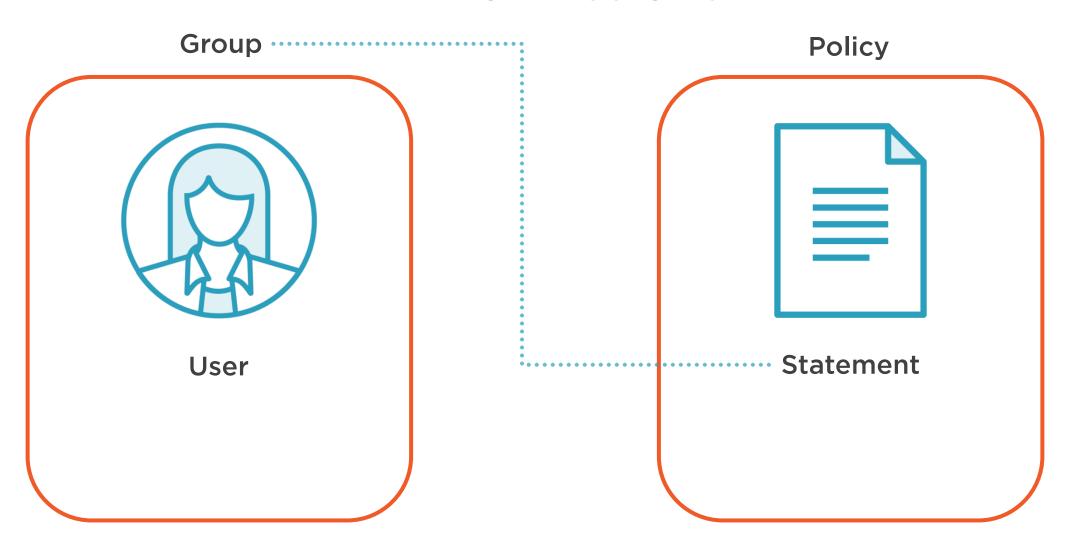
Audit events

- Search
- View
- Copy

User must have permission to view



IAM Permissions



Allow group Auditors to read audit-events in tenancy

Allow group Auditors to read audit-events in compartment Project1

■ Group named "Auditors" can view all audit event logs in the tenancy

■ Group named "Auditors" can view all audit event logs only in the compartment named "Project1"



Audit Log Retention Policy



Default 90 days, can configure up to 365 days



Tenancy level setting



Must be a member of the Administrators group to change



Demo



Audit logs in web console

Permissions to access audit logs

Change retention policy



Audit Log Search





```
"event" : {
    "eventType": "com.oraclecloud.ComputeApi.ListInstances",
    "eventId": "7502c13d-7a74-4676-9f81-0a19b11528f4",
    "eventTime": "2019-10-14T00:00:11.133Z",
    "data": {...}
}
```

Audit Log Event

JSON object

Event envelope is the same for all events

Data varies depending on which service produced event log



Bulk Export Audit Logs



Open a support ticket for bulk export

Support will copy logs to buckets

Must belong to Administrators group to access buckets

Buckets prefixed with oci-logs._audit



```
<region>/<ad>/<YYYY-MM-DDTHH:MMZ>[_<seqNum>].log.gz
```

us-phoenix-1/ad1/2019-10-14T05:30Z.log.gz

us-phoenix-1/ad1/2019-10-14T05:30Z_2.log.gz

Bulk Export Log Files

Organized by region and availability domain

Filename is start time of earliest audit event listed in object

Single audit event per line



Demo



Audit log search options

Explore audit log event



Summary



Search audit logs in web console

Configure access and retention policy

Request and use bulk export log files

