SharkFest'24 EUROPE
Vienna, Austria • #sf24eu

~~Logshark~~
~~Logwolf~~
~~Logray~~
Stratoshark

Or how to inspire your DevOps team to use Wireshark

Uli Heilmeier
@uhei@chaos.social


I have seen the light!

Stratoshark

falcodump

extcap interface for falco plugins

k8saudit
cloudtrail
json
dummy
dummy_c
docker
seccompagent
okta
github
k8saudit-eks
nomad
dnscollector
gcpaudit
syslogsrv
salesforce
box
test
k8smeta
k8saudit-gke
journald
kafka
gitlab
keycloak

AWS Cloudtrail

user activity and API usage

Cloudtrail

- Management / Data Events
- Organizational
- S3
- Glue + Athena: Database with dynamic partitioning

Cloudtrail

```
CREATE EXTERNAL TABLE ctrail_pp_ymd_org (eventversion STRING,
useridentity STRUCT<
               type:STRING,
               principalid:STRING,
               arn:STRING,
               accountid:STRING,
               invokedby:STRING,
               accesskeyid:STRING,
               userName:STRING,
sessioncontext:STRUCT<
attributes:STRUCT<
               mfaauthenticated:STRING,
               creationdate:STRING>,
sessionissuer:STRUCT<
               type:STRING,
               principalId:STRING,
               arn:STRING,
               accountId:STRING,
               userName:STRING>>>,
eventtime STRING,
eventsource STRING,
eventname STRING,
awsregion STRING,
sourceipaddress STRING,
useragent STRING,
errorcode STRING,
errormessage STRING,
requestparameters STRING,
responseelements STRING,
additionaleventdata STRING,
requestid STRING,
eventid STRING,
resources ARRAY<STRUCT<
               ARN:STRING,
               accountId:STRING,
               type:STRING>>,
```

```
eventtype STRING,
apiversion STRING,
readonly STRING,
recipientaccountid STRING,
serviceeventdetails STRING,
sharedeventid STRING,
vpcendpointid STRING
)
PARTITIONED BY (account string, region string, year string, month string, day string)
ROW FORMAT SERDE
  'com.amazon.emr.hive.serde.CloudTrailSerde'
STORED AS INPUTFORMAT
  'com.amazon.emr.cloudtrail.CloudTrailInputFormat'
OUTPUTFORMAT
  'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
  's3://doc_example_bucket/AWSLogs/doc_example_orgID/'
TBLPROPERTIES (
  'projection.enabled'='true',
  'projection.day.type'='integer',
  'projection.day.range'='01,31',
  'projection.day.digits'='2',
  'projection.month.type'='integer',
  'projection.month.range'='01,12',
  'projection.month.digits'='2',
  'projection.region.type'='enum',
  'projection.region.values'='us-east-1,us-east-2,us-west-2',
  'projection.year.type'='integer',
  'projection.year.range'='2010,2100',
  'projection.account.type'='enum',
  'projection.account.values'='111122223334444,5555666677778888',
  'storage.location.template'='s3://doc_example_bucket/AWSLogs/doc_example_orgID/${account}/CloudTrail/${region}/${year}/${month}/${day}'
)
```

```
SELECT useridentity.arn, eventtime
FROM "ctrail_pp_ymd”
WHERE eventname = 'GetObject’
and year = '2021'
and month = '05'
and region = 'us-east-1'
and account IN ('234245080893', '531730379764’)
and cast(json_extract(requestparameters,
'$.bucketName')as varchar) ='doc_example_bucket'
```

libcloudtrail Demo

- Log data URL:
  s3://doc_example_bucket/AWSLogs/doc_example_orgID/
  s3://doc_example_bucket/AWSLogs/123456789012/

- S3 Log interval:
  4h
  2024-10-30T18:07:17Z
  5d-2d
  2024-09-05T04:00:00Z-2024-09-05T15:00:10Z

- S3 account list:
  <empty>
  123456789012
  345678901234, 432187650987

- AWS Region:
  where your S3 bucket is located

- S3 download concurrency:
  `64 (32 default)`

falcodump CLI

```
falcodump --capture \
--extcap-interface cloudtrail \
--fifo ~/cloudtrail.pcapng \
--plugin-source s3://my-cloudtrail-bucket/AWSLogs/o-
abc12345/123456789012/ \
--cloudtrail-s3downloadconcurrency 32 \
--cloudtrail-s3interval 5d-2d \
--cloudtrail-aws-region eu-west-1
```

libgcpaudit compile Demo

libgcpaudit

```
git clone https://github.com/falcosecurity/plugins.git
cd plugins/plugins/gcpaudit
make
cp libgcpaudit.so \
/Applications/Stratoshark.app/Contents/PlugIns/stratoshark/fa
lco
```

Cloud be that “Display” is missing for sdk.FieldEntry

Download

https://www.wireshark.org/download/automated/

Questions?

Feedback