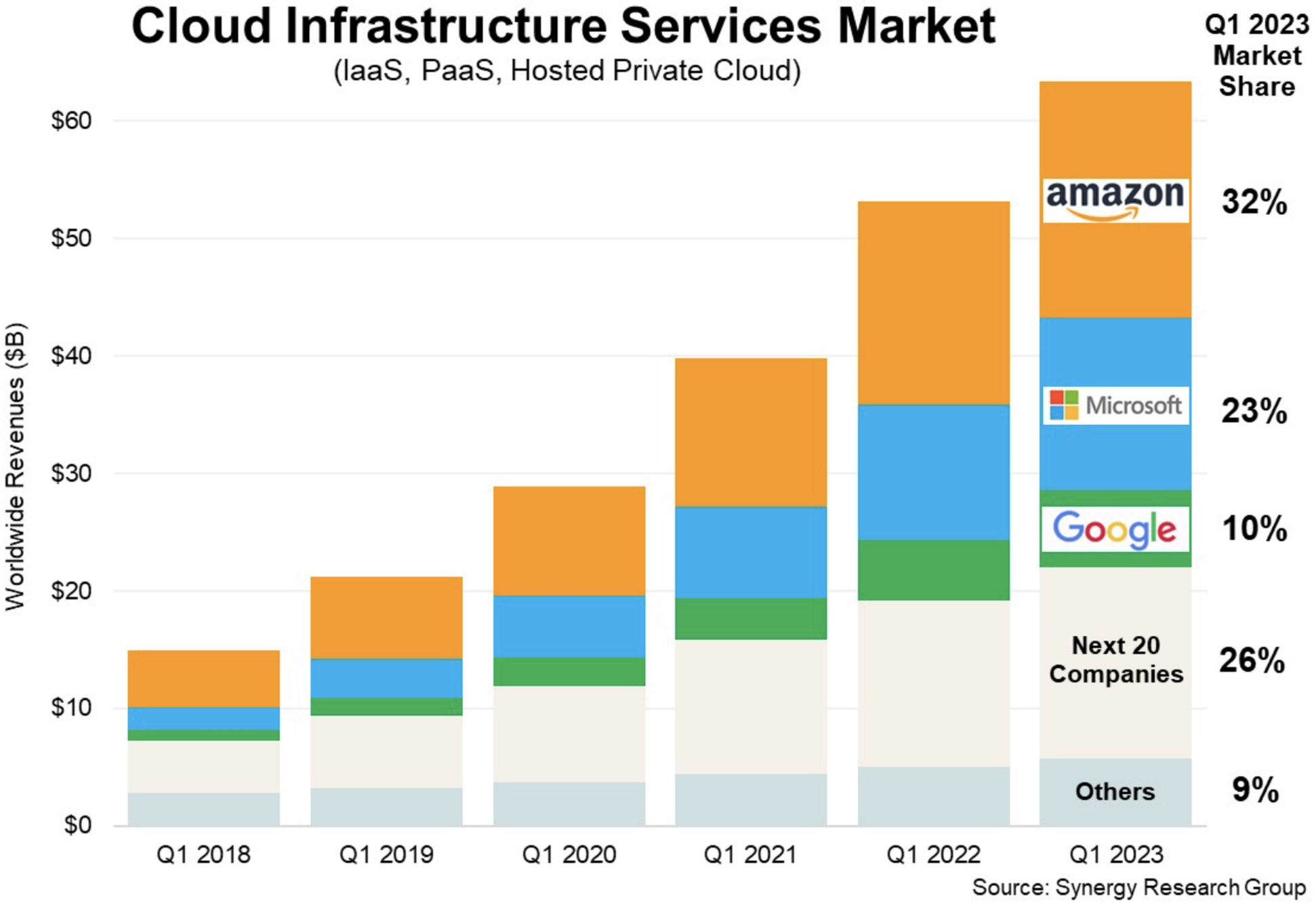
All I see are strange clouds

Korstiaan Stam, Invictus Incident Response

Why this talk?

INVICTUS
INCIDENT RESPONSE


Cloud Infrastructure Services Market
(IaaS, PaaS, Hosted Private Cloud)
Worldwide Revenues ($B)
$60
$50
$40
$30
$20
$10
$0
Q1 2018
Q1 2019
Q1 2020
Q1 2021
Q1 2022
Q1 2023
Q1 2023 Market Share
amazon
32%
Microsoft
23%
Google
10%
Next 20 Companies
26%
Others
9%
Source: Synergy Research Group

market share of leading cloud infrastructure service providers in Q1 2023

 AWS: 32%
 Azure: 23%
 Google Cloud: 10%
 Alibaba Cloud: 4%
 IBM Cloud: 3%
 Salesforce: 3%
 Oracle: 2%
 Tencent Cloud: 2%

INVICTUS
INCIDENT RESPONSE

2.8

The number of cloud providers on average for an enterprise

Why me?

INVICTUS
INCIDENT RESPONSE

Invictus Incident Response (@InvictusIR)

- Founder of the company
- Specializing in cloud incident response services
- Instructor for FOR509 - Cloud Incident Response course
- Big fan of cloud incident response
- Previously held IR roles for large and small organizations

INVICTUS INCIDENT RESPONSE

"Continuously innovate and develop open-source incident response tools and solutions tailored specifically for cloud environments."

Microsoft	Microsoft Extractor Suite https://github.com/invictus-ir/Microsoft-Extractor-Suite
Google Workspace	ALFA https://github.com/invictus-ir/ALFA
aws	Invictus-AWS https://github.com/invictus-ir/Invictus-AWS
Datasets	Microsoft 365: https://github.com/invictus-ir/o365_dataset Google Workspace: https://github.com/invictus-ir/gws_dataset AWS CloudTrail: https://github.com/invictus-ir/aws_dataset

Approach

INVICTUS
INCIDENT RESPONSE

Approach
Research methodology

- Desk research/Researchgate/ChatGPT/Bard etc.
- Determine requirements, what do we need to know?
- Register for trial accounts for cloud provider and start researching

Scoping

1. ~~AWS~~
2. ~~Azure~~
3. ~~Google Cloud~~
4. Alibaba Cloud
5. IBM Cloud
6. Oracle Cloud

No SaaS platforms running on cloud (e.g. Salesforce)

Findings

INVICTUS
INCIDENT RESPONSE

Structure

Hierarchy

Understanding the layout of the cloud is important to scope an incident and the extent of a compromise.

Logging & Acquisition

What logging options are ‘natively’ enabled and can be used for DFIR purposes and can we acquire them?

Security & Premium features

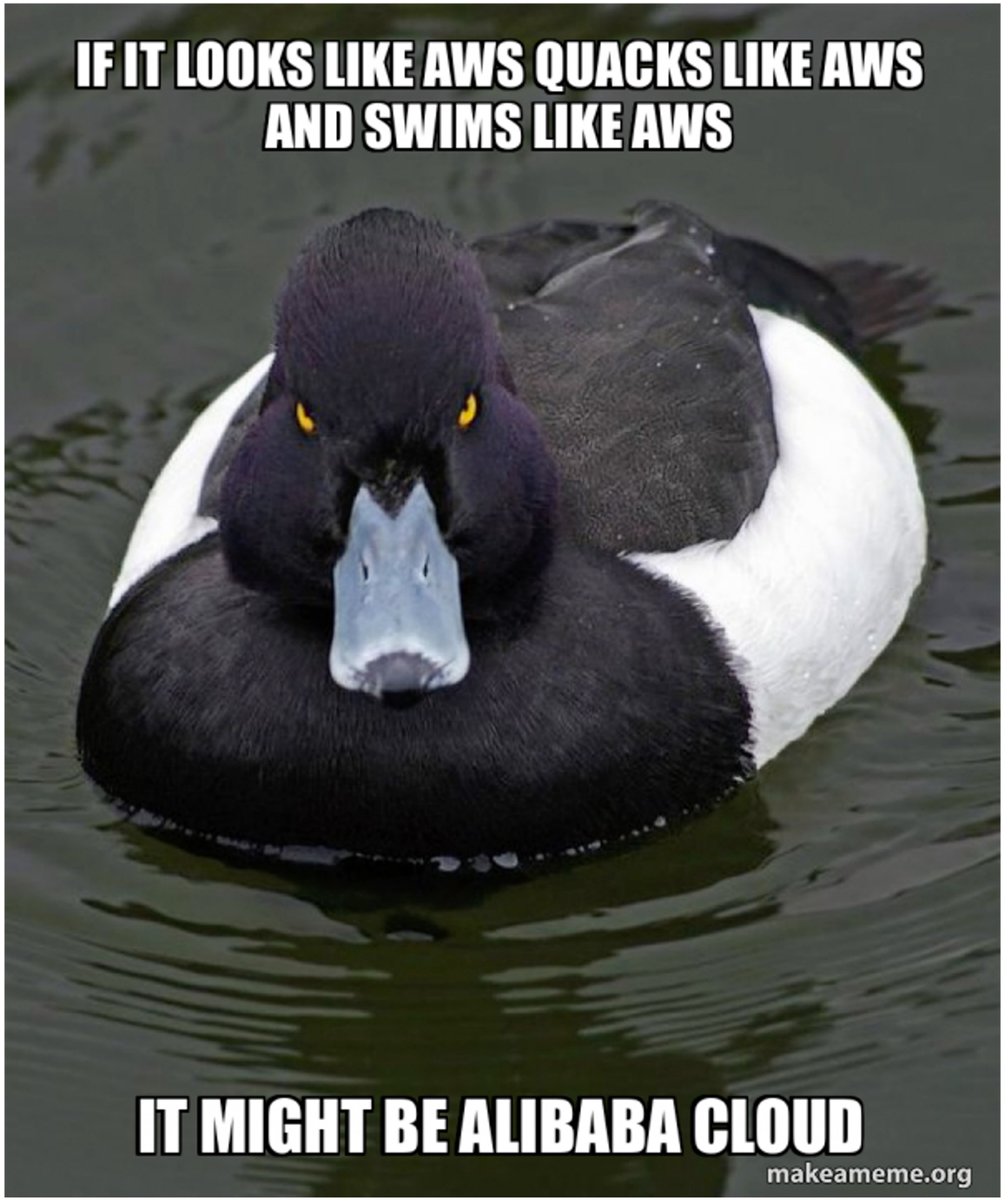
What’s out of the box available from security and anything that’s worth paying for (e.g. E5 in Microsoft).

Challenges and things to know

Other interesting features and findings relevant for DFIR.

Alibaba Cloud

INVICTUS
INCIDENT RESPONSE


IF IT LOOKS LIKE AWS QUACKS LIKE AWS
AND SWIMS LIKE AWS
IT MIGHT BE ALIBABA CLOUD
makeameme.org

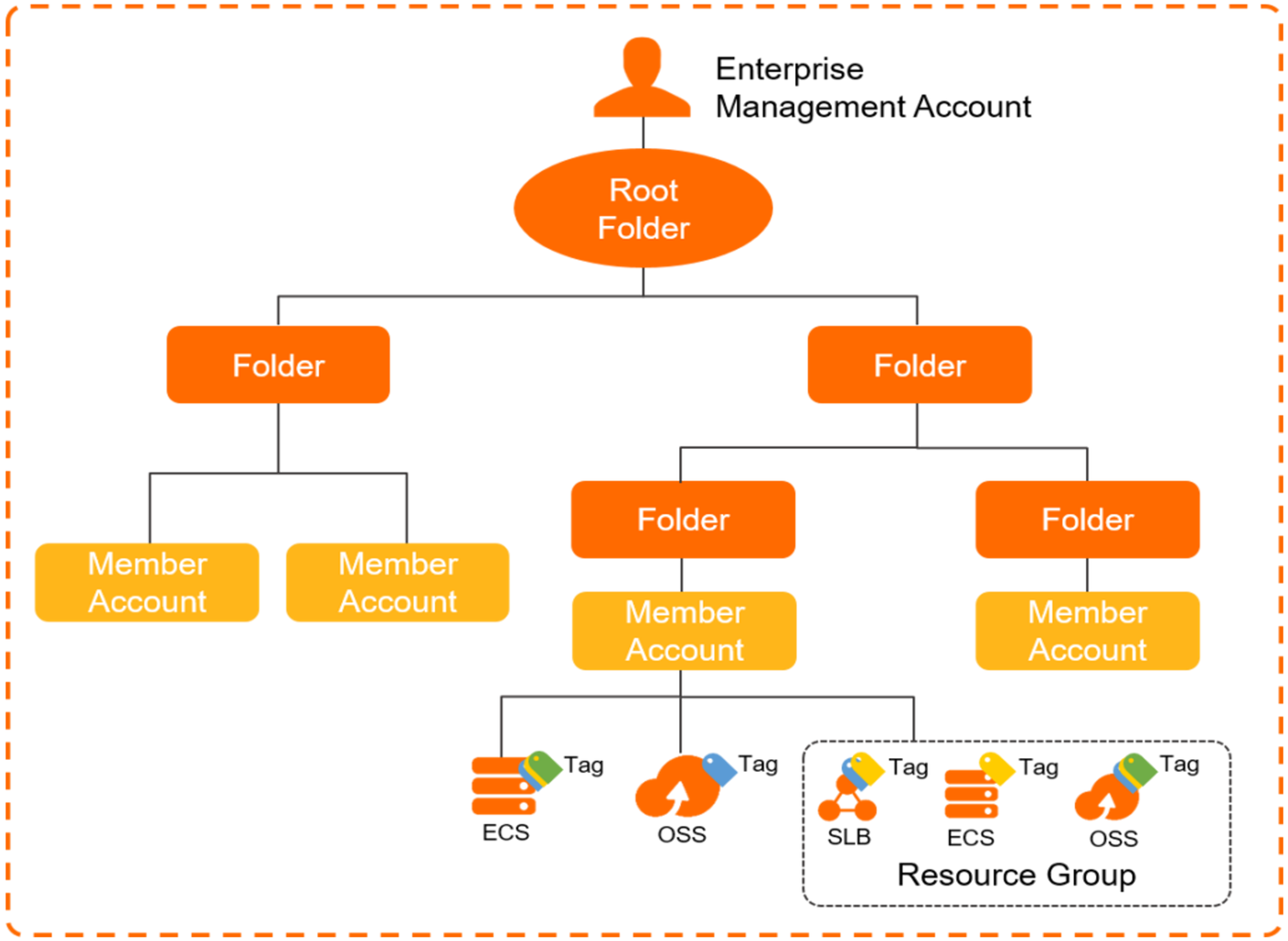
Alibaba Cloud
Introduction

- Also called **Aliyun** or **Ali Cloud**
- It has a lot of similarities with AWS, it also started with e-commerce and now a cloud provider
- Services sound/look very similar

AWS	**Alibaba Cloud**
IAM	RAM
Cloud Object Storage (S3)	Object Storage Service (OSS)
EC2	ECS (!)
CloudTrail	ActionTrail

Alibaba Cloud Hierarchy

- You can enable a Resource Directory which allows you to combine multiple Alibaba accounts, in AWS this is called an Organization
- Everything is RAM instead of IAM
- One root account for each account and normal RAM users

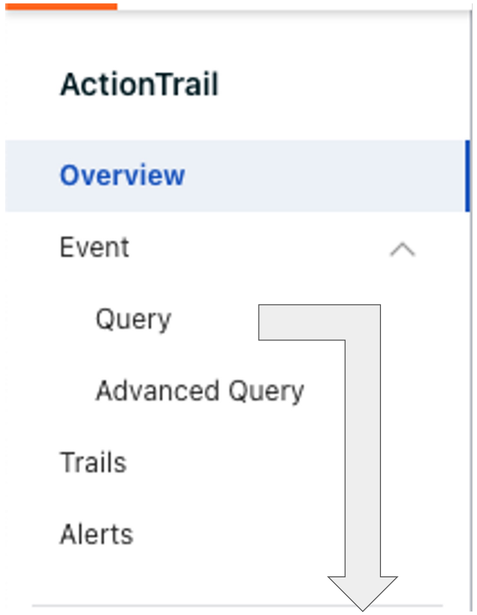


Alibaba Cloud
Logging & Acquisition

ActionTrail is the service for Audit logging in Alibaba Cloud

- You can create one trail for all accounts and regions
- You can perform advanced queries from the interface across regions!
- SLA for event delivery is within 10 minutes
- Retention is 90 days
- **Only** management events
- You can storage the logs in OSS and/or forward them to Log Service

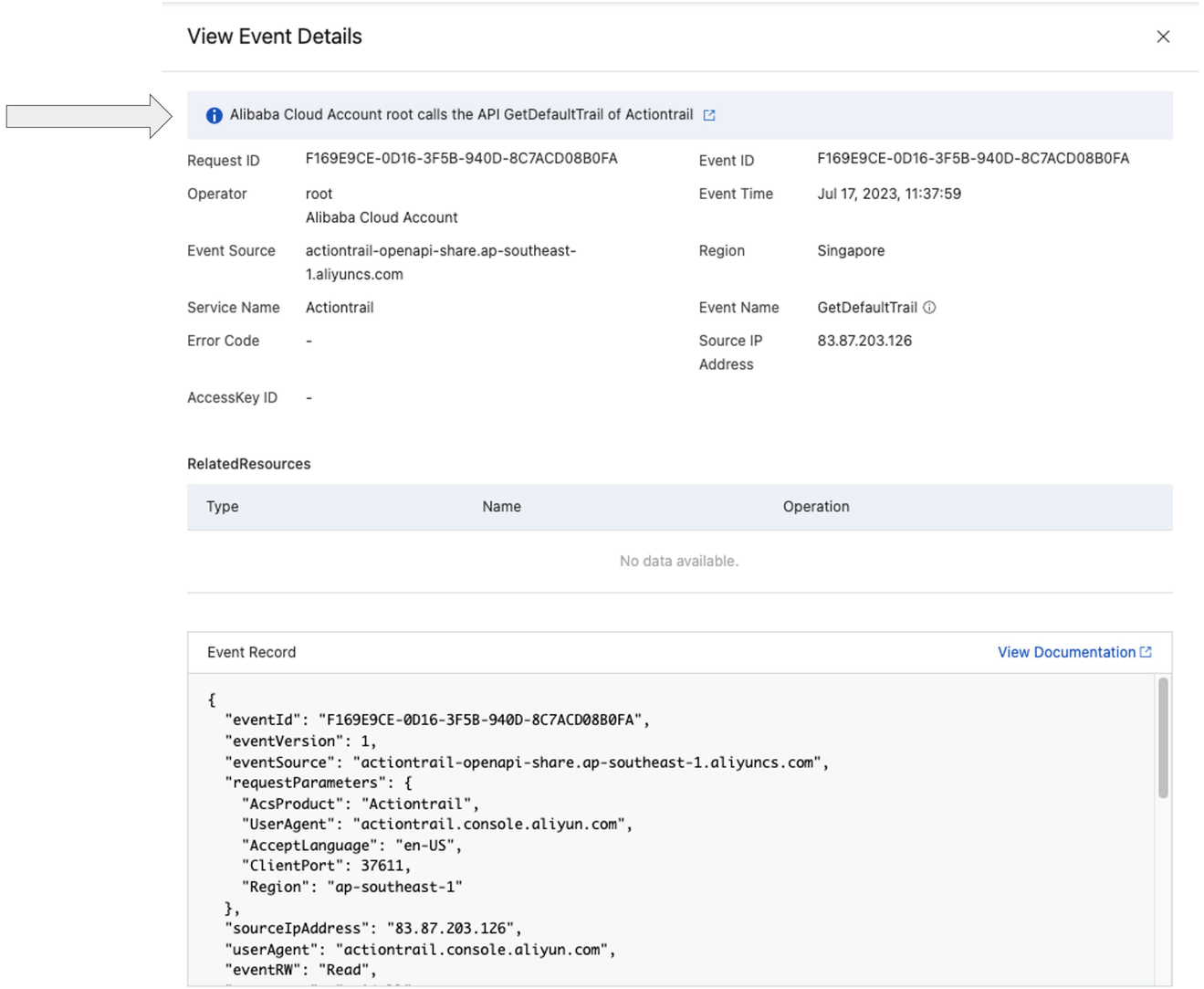
Logging & Acquisition - Example



Read/Write Type | Select a value | 1h | 12h | 1d | 7d | 30d | Custom

Event Time	Operator	Service Name	Event Name	RelatedResources	Operation
Jul 17, 2023, 11:37:59	root Alibaba Cloud Account	Actiontrail	GetDefaultTrail		View Event Details
Jul 17, 2023, 11:37:55	root Alibaba Cloud Account	Actiontrail	DescribeTrails		View Event Details
Jul 17, 2023, 11:37:55	root Alibaba Cloud Account	Actiontrail	LookupInsightEvents		View Event Details

Logging & Acquisition - Example



Logging & Acquisition - Advanced query

Advanced Query

Trail Name management-events | Log Service actiontrail_management-events | Status Enabled | Log Delivery Enabled On Jul 17, 2023, 13:25:18 | Event Type All

Account-related or AccessKey pair-related Events | CIS Standard-related Events | Lifecycle-related Events | **Custom Events**

Please enter a search field or query statement: Example: * and event.eventRW: Write.

Who	What	Which	Where	Other
Alibaba Cloud Account	Service Name	Resource Type	Region	Event ID
AccessKeyId	Read-Write Type	Resource Name	Event Source	Request ID
Principal ID	Event Name		Source IP Address	
Account Type	Event Source			
User Name	API Version			
	Error Message			
	Error Code			

User Name	Service Name	Event Name	Resource Type	Region	Time
root Alibaba Cloud Account	ActionTrail(Actiontrail)	DescribeSearchTemplates	-	China (Hangzhou)	Jul 17, 2023, 15:47:35
aliyunserviceroleforOSS... RAM Role	Object Storage Service(Oss)	GetBucketLocation	-	China (Hangzhou)	Jul 17, 2023, 15:47:32
aliyunserviceroleforSLS... RAM Role	Log Service(SLS)	GetLogStore	-	Singapore	Jul 17, 2023, 15:47:33
root Alibaba Cloud Account	ActionTrail(Actiontrail)	DescribeScenes	-	China (Hangzhou)	Jul 17, 2023, 15:47:32

Alibaba Cloud
Security & Premium features

Cloud Security Center is the security offering, lots of different services ranging from implementation of protective measures to detection response and even setting up honeypots, some highlights:

Access Key Leak detection service

- GitHub scanning
- Threat Intel and crawlers

Cloud Honeypot in a Virtual Private Cloud (VPC)

- Web
- Database
- Custom (based on Docker)

Built-in Log Analysis (like $Sentinel)

- Security logs (alerts, vulnerability)
- Network (DNS, flow logs)
- Host logs (Logon logs, process logs)

Alibaba Cloud
Challenges and things to know

- There’s AliBaba Cloud and AliBaba Cloud for Mainland China users
- The latter requires China Government Issued ID for users
- Feels buggy and throws quite a few errors, but support has been great
- Documentation is really nice within the platform
- Easy to learn/understand if you’re coming from an AWS background.

IBM Cloud

IBM Cloud
Introduction

- IBM Cloud used to be called Bluemix and based on Softlayer
- Only exists since 2021 making it the ‘newest’ cloud in this talk
- Focussed on financial services
- Supports SAP deployments in the cloud
- It has the best dark theme :)

Using Cloud Foundry? Cloud Foundry has been deprecated, but we have you covered with migration paths to Code Engine and other popular services. Learn more.

Dashboard

Edit dashboard | Upgrade account | Create resource +

For you

Select an option

Build

Explore IBM Cloud with this selection of easy starter tutorials and services.

Db2

Get enterprise-level OLTP performance, 99.99% uptime SLA, automatic backups, compliance options and encryption at rest with Db2.

Popular 2 min

Explore IBM Cloud Shell

Try a command-driven approach for creating, developing, and deploying a web project.

Getting started 2 min

Get Started with Watson Studio

Get started with using AI and Cloud Object Storage in 15 minutes.

Popular 2 hr

Build with Watson

Chatbots, insights, recognitizers, and more. Explore the AI platform for business.

Popular 3 min

Use Watson Studio

Watson Studio provides a suite of tools and a collaborative environment for data scientists, developers and domain experts.

Popular 2 min

Use Speech to Text

Easily convert the hum voice into the written v for voice control, transcription, etc. with Speech to Text.

Popular

News

View all

25 IBM Products Win Top Rated Distinction from TrustRadius

IBM Turbonomic SaaS and On-Prem Services Now Available on AWS Marketplace

IBM Spectrum LSF on IBM Cloud: Functional and Performance Updates

IBM Cloud Continuous Delivery Now Supports Event Notifications

Recent support cases

View all

You don't have permission to view the support cases for this account. Learn more about IAM access.

Planned maintenance

View all

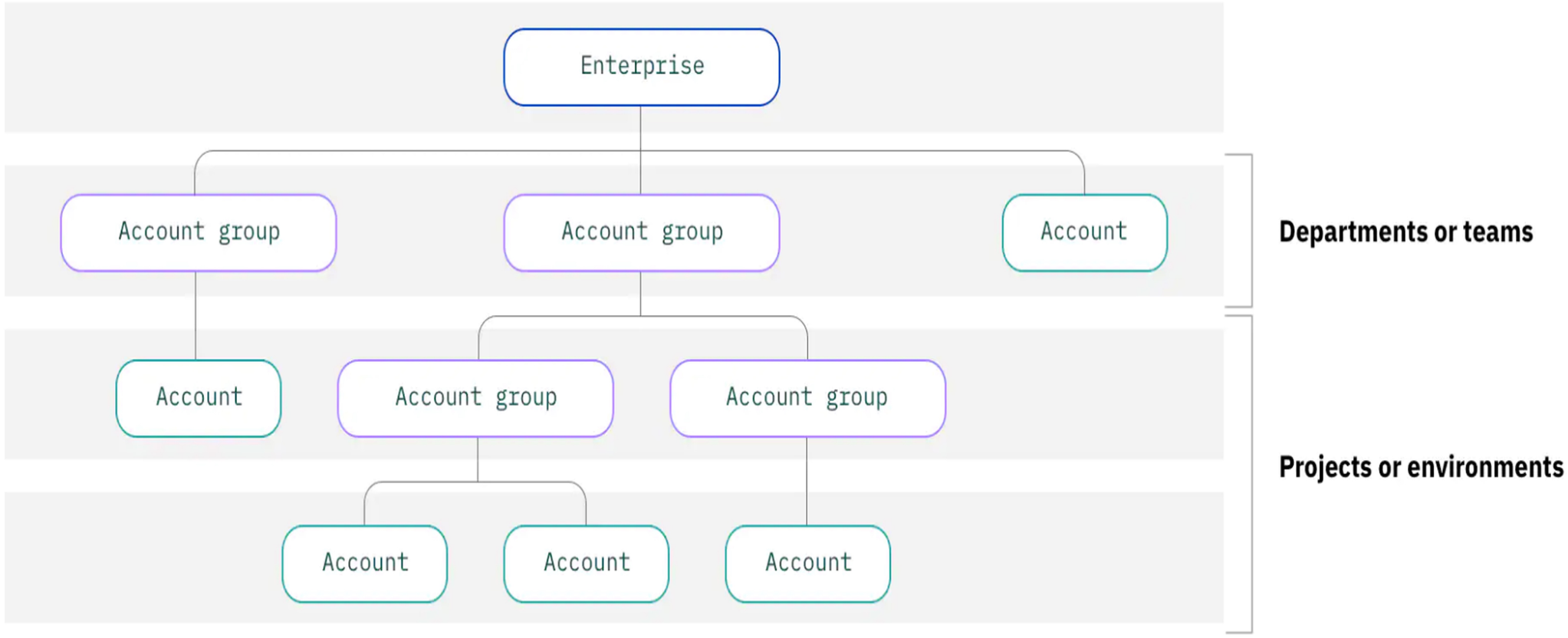
Clear skies!
You can view your scheduled maintenance events here.

IBM Cloud status

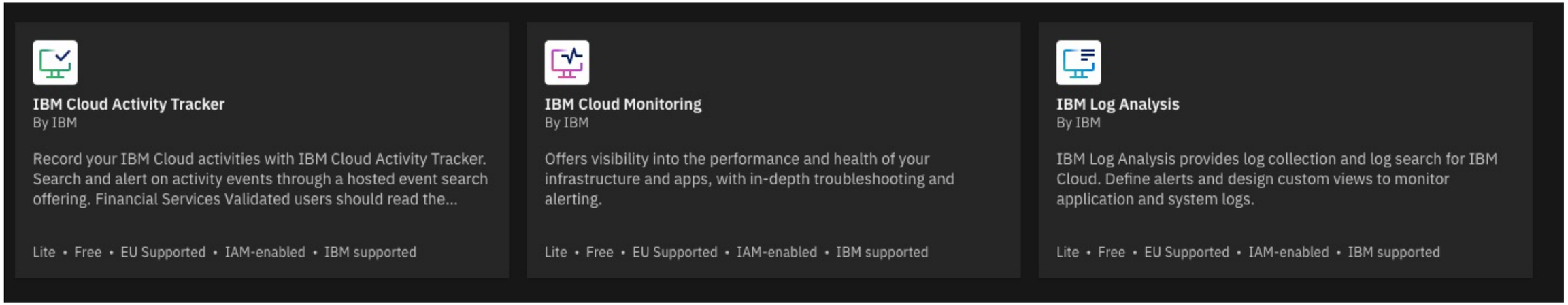
View all

No issues

IBM Cloud Hierarchy

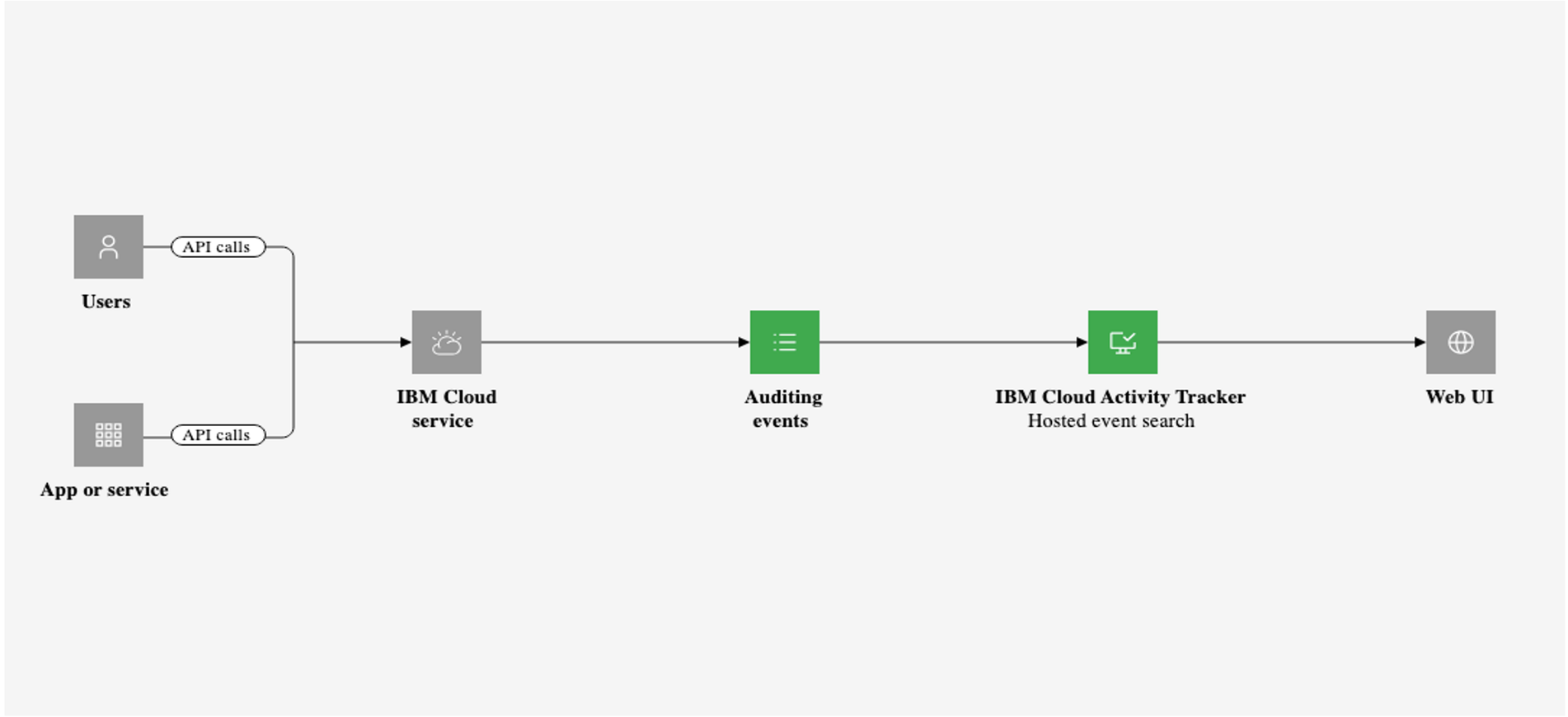


IBM Cloud
Logging & Acquisition



IBM Cloud
Logging & Acquisition

Cloud Activity tracker is the most important service for forensics



IBM Cloud Activity Tracker

- **Off** by default
- Global events (IAM) recorded in Frankfurt
- To collect and view global events, you must provision an instance of the Activity Tracker service in Frankfurt
- By default the Cloud Activity tracker only allows live analysis, you have to pay for storing and searching capabilities
- Dashboarding with Kibana
- Max 30 day retention period!

IBM Cloud Activity Tracker offers ready to run event search offerings to simplify configuration and expedite your time to greater insights. You can choose to retain your events for 7, 14, or 30 days. A 30 day HIPAA compliant offering is also available.

IBM Cloud Activity Tracker
What is logged?

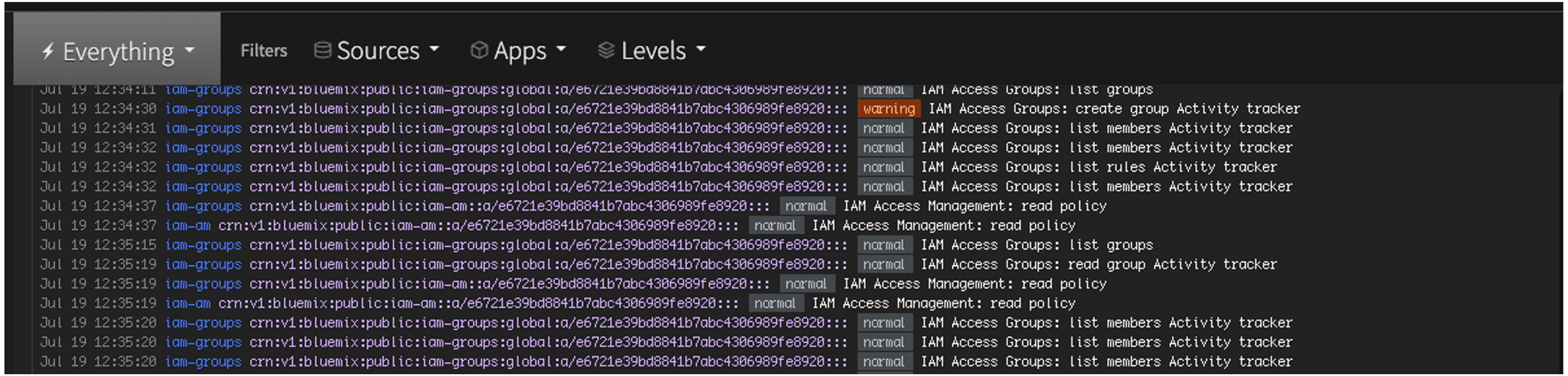
- Management events via GUI, API or CLI
- Additional data events need to be enabled:

Service	Upgrade plan	Configure the service	More info
IBM Cloud® App ID	✓	✓	Monitoring runtime activity
IBM Cloud® Object Storage		✓	Enabling Activity Tracker Event Routing
IBM® Cloudant® for IBM Cloud®		✓	Configuring data events for an IBM Cloudant instance
IBM® Event Streams for IBM Cloud®	✓	✓	Enabling message audit events
Watson services	✓		

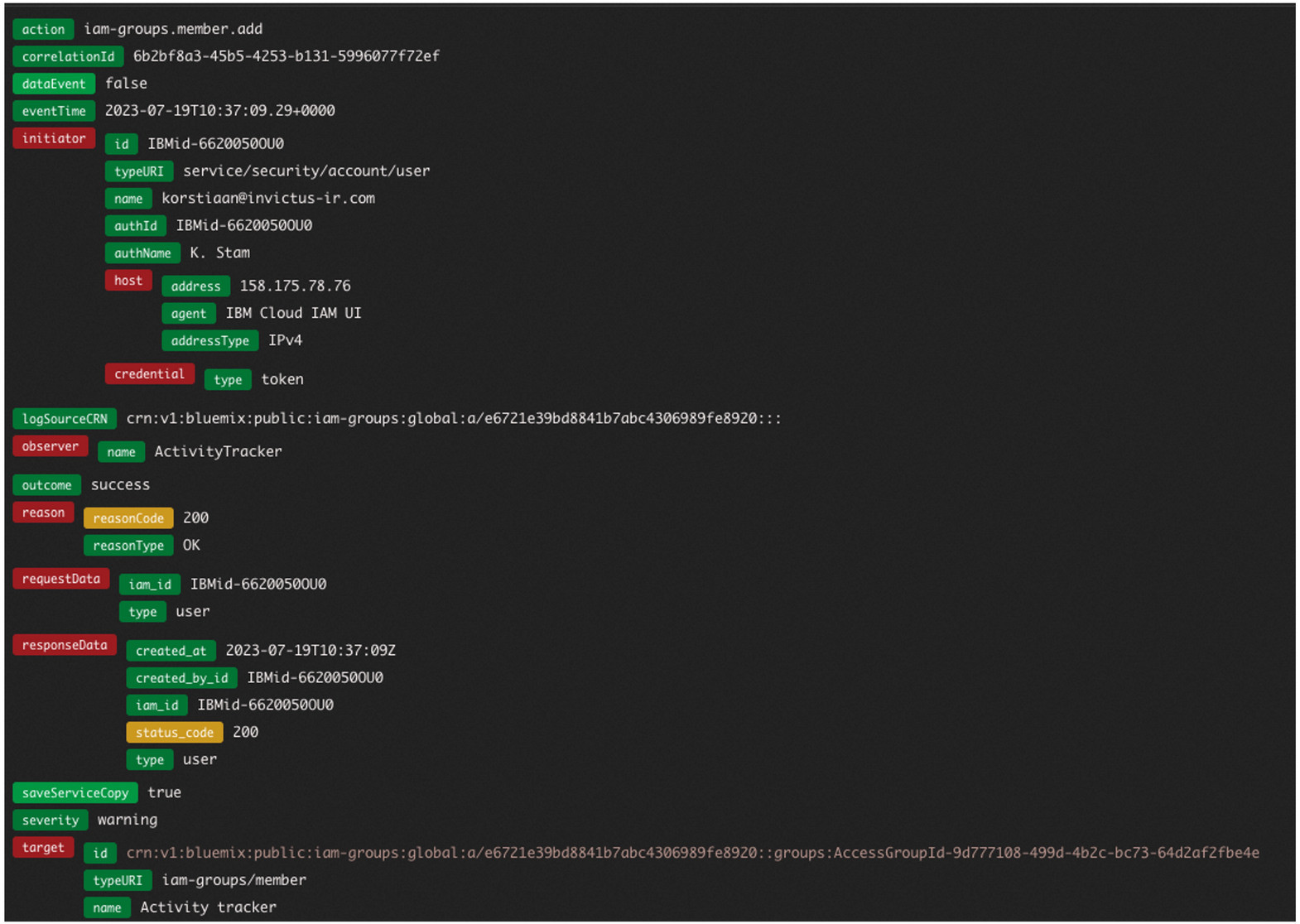
Table 2. IBM Cloud services that require actions for data events

- SLA not documented
- You can disable logging through exclusion rules

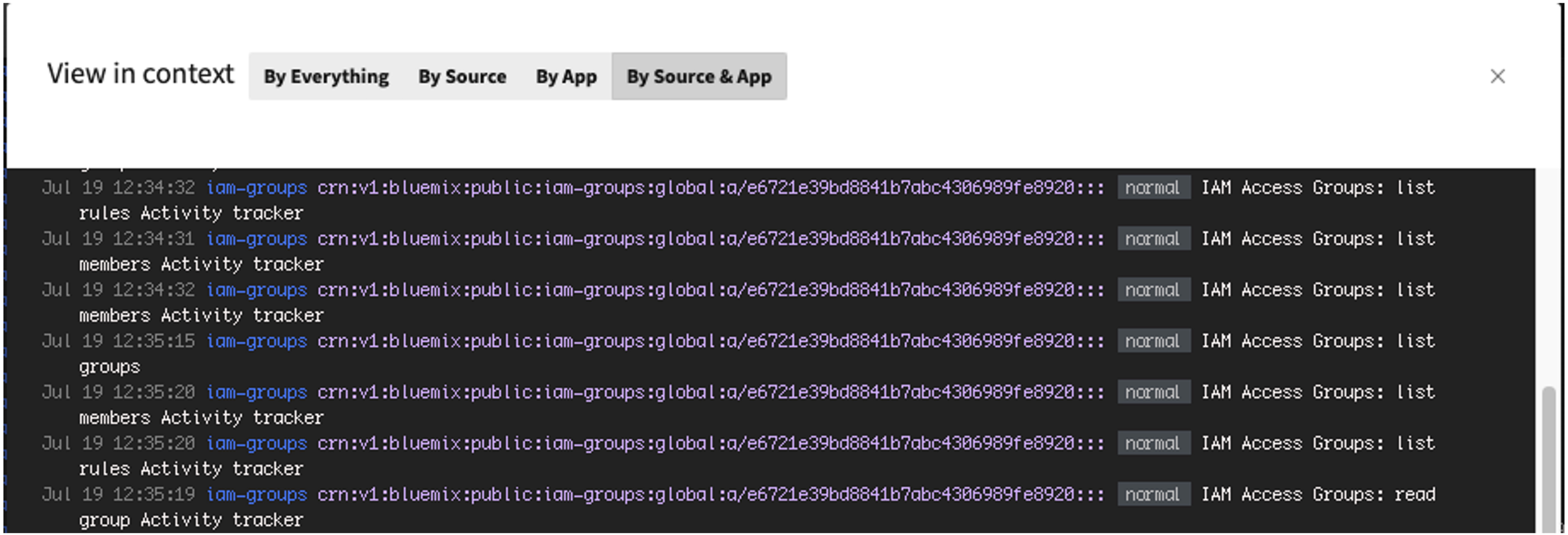
Example #1


Everything
Filters
Sources
Apps
Levels
Jul 19 12:34:11 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Groups: list groups
Jul 19 12:34:30 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: warning IAM Access Groups: create group Activity tracker
Jul 19 12:34:31 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Groups: list members Activity tracker
Jul 19 12:34:32 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Groups: list members Activity tracker
Jul 19 12:34:32 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Groups: list rules Activity tracker
Jul 19 12:34:32 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Groups: list members Activity tracker
Jul 19 12:34:37 iam-groups crn:v1:bluemix:public:iam-am::a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Management: read policy
Jul 19 12:34:37 iam-am crn:v1:bluemix:public:iam-am::a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Management: read policy
Jul 19 12:35:15 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Groups: list groups
Jul 19 12:35:19 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Groups: read group Activity tracker
Jul 19 12:35:19 iam-groups crn:v1:bluemix:public:iam-am::a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Management: read policy
Jul 19 12:35:19 iam-am crn:v1:bluemix:public:iam-am::a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Management: read policy
Jul 19 12:35:20 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Groups: list members Activity tracker
Jul 19 12:35:20 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Groups: list members Activity tracker
Jul 19 12:35:20 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Groups: list members Activity tracker

Example #2


action iam-groups.member.add
correlationId 6b2bf8a3-45b5-4253-b131-5996077f72ef
dataEvent false
eventTime 2023-07-19T10:37:09.29+0000
initiator
id IBMid-6620050OU0
typeURI service/security/account/user
name korstiaan@invictus-ir.com
authId IBMid-6620050OU0
authName K. Stam
host
address 158.175.78.76
agent IBM Cloud IAM UI
addressType IPv4
credential
type token
logSourceCRN crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920:::
observer
name ActivityTracker
outcome success
reason
reasonCode 200
reasonType OK
requestData
iam_id IBMid-6620050OU0
type user
responseData
created_at 2023-07-19T10:37:09Z
created_by_id IBMid-6620050OU0
iam_id IBMid-6620050OU0
status_code 200
type user
saveServiceCopy true
severity warning
target
id crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::groups:AccessGroupId-9d777108-499d-4b2c-bc73-64d2af2fbe4e
typeURI iam-groups/member
name Activity tracker

Example #3


View in context
By Everything
By Source
By App
By Source & App
Jul 19 12:34:32 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Groups: list rules Activity tracker
Jul 19 12:34:31 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Groups: list members Activity tracker
Jul 19 12:34:32 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Groups: list members Activity tracker
Jul 19 12:35:15 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Groups: list groups
Jul 19 12:35:20 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Groups: list members Activity tracker
Jul 19 12:35:20 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Groups: list rules Activity tracker
Jul 19 12:35:19 iam-groups crn:v1:bluemix:public:iam-groups:global:a/e6721e39bd8841b7abc4306989fe8920::: normal IAM Access Groups: read group Activity tracker

IBM Cloud
Exporting the logs

- Exporting via the GUI uses the V1 API

Plan	Limit
7-day plan	10.000 lines
All other plans	20.000 lines

- Export is done per endpoint (region)

- The V2 API limit is also 10.000 lines, but supports pagination so you can acquire all data

IBM Cloud
Security & Premium features

- *IBM Cloud Security and Compliance Center*, name of the security offering
- It is **not** detection/response focussed more on Cloud Security Posture Management
- The idea is to protect your workloads/instances look for misconfigurations and vulnerabilities
- Very much focused on Compliance & Risk not forensics/IR

IBM Cloud
Challenges and things to know

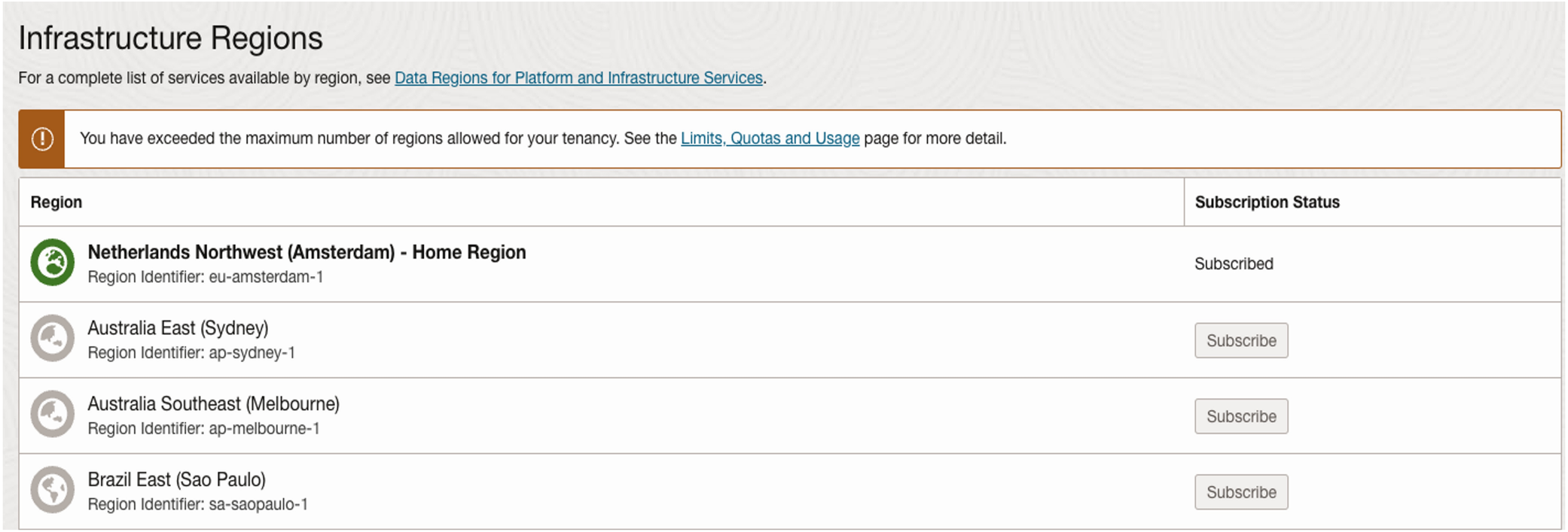
- Logging is **off** by default this is the only cloud that does that
- Limited retention (30 days)
- EU focus, Frankfurt is the default platform region also for US/APAC customers
- Very AI focussed (Watson)
- Built-in VMware solution can be useful for deploying forensic VMs (bring your own image)

Oracle Cloud

INVICTUS
INCIDENT RESPONSE

Oracle Cloud
Introduction

- Oracle Cloud also called OCI (Oracle Cloud Infrastructure)
- Allows you to have a ‘private cloud’ in your own datacenter
- You set main region (us-east-1) when signing up can’t change afterwards



Oracle Cloud Hierarchy

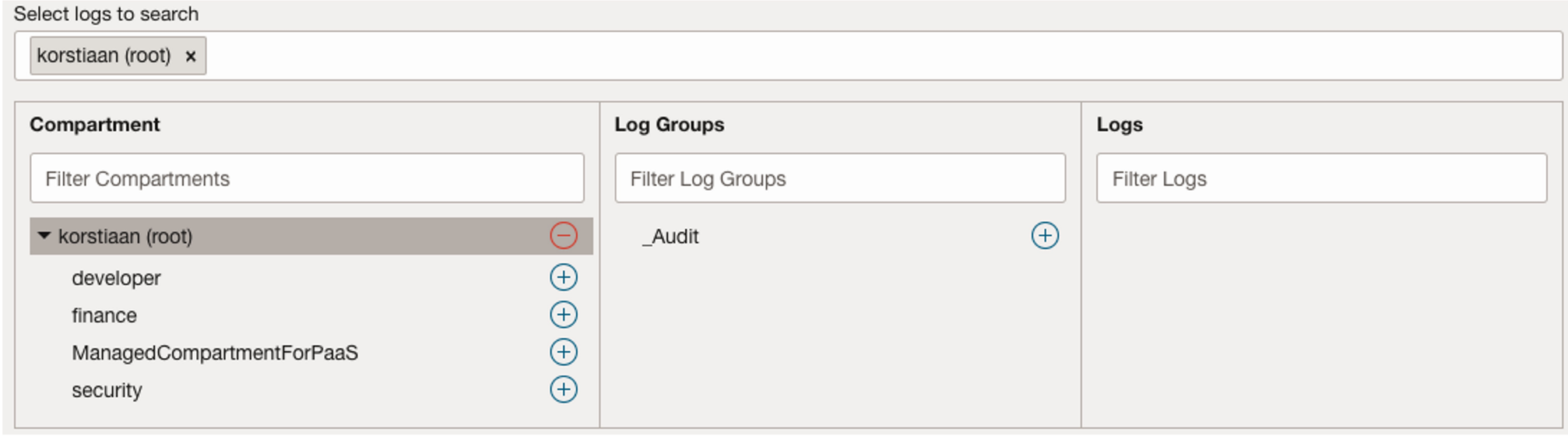
- Oracle is different then other clouds they use something called Compartments to structure resources
- The highest Compartment is called the root compartment
- Compartments are cross region, access to root Compartment provides you access to all underlying compartments

Create Compartment

Name	Status	OCID	Authorized	Security Zone	Subcompartments
korstiaan	Active	...qys3nq	Yes	-	4
developer	Active	...hj7bwa	Yes	-	0
finance	Active	...tpc2jq	Yes	-	0
ManagedCompartmentForPaaS	Active	...g7m52q	Yes	-	0
security	Active	...n4tysq	Yes	-	0

Oracle Cloud
Logging & Acquisition

- Oracle Logging Service responsible for logging
  - Audit Logs
  - Service Logs
  - Custom Logs
- You can search cross Compartments from the GUI



Oracle Cloud
Logging & Acquisition

- Basic and advanced searching in the console
- Format is in .json
- Great level of detail
- Listing of objects via GUI and searches performed are logged

datetime	type	data.message	
Jul 17, 2023, 14:37:56 UTC	LogSearch.SearchLogs	SearchLogs succeeded	⌄

JSON | Before & After


```
{
  "datetime": 1689604676813
  "logContent": {
    "data": {
      "additionalDetails": NULL
      "availabilityDomain": "AD1"
      "compartmentId": "ocid1.tenancy.oc1..aaaaaaaalnkcon5h3lky44htf5z2xetbjoh7p4hbsbkiotcz6vv6oeqys3nq"
      "compartmentName": "korstiaan"
      "definedTags": NULL
      "eventGroupingId": NULL
      "eventName": "SearchLogs"
      "freeformTags": NULL
      "identity": {...}
      "message": "SearchLogs succeeded"
      "request": {...}
      "resourceId": NULL
      "response": {...}
      "stateChange": {...}
    }
    "dataschema": "2.0"
    "id": "6a6078ad-b9cc-4512-87d5-13d05605f9a0"
    "oracle": {
      "compartmentid": "ocid1.tenancy.oc1..aaaaaaaalnkcon5h3lky44htf5z2xetbjoh7p4hbsbkiotcz6vv6oeqys3nq"
      "ingestedtime": "2023-07-17T14:37:57.952Z"
      "loggroupid": "_Audit"
      "tenantid": "ocid1.tenancy.oc1..aaaaaaaalnkcon5h3lky44htf5z2xetbjoh7p4hbsbkiotcz6vv6oeqys3nq"
    }
    "source": ""
    "specversion": "1.0"
    "time": "2023-07-17T14:37:56.813Z"
    "type": "com.oraclecloud.LogSearch.SearchLogs"
  }
  "regionId": "eu-amsterdam-1"
}
```

Oracle Cloud
Logging & Acquisition

- On by default
- Default retention = 30 days
- Time is in UTC (w00t)

- Each event has fields prefixed with *event* that will give you metadata about the event such as the time and source of the event

- Each event has fields prefixed with *data* that contain the payload of the event and all of its details such as the identity that made the call the name of the API that was called


```
{
  "datetime": 1689613785846
  ⊖"logContent": {
    ⊕"data": {...}
    "dataschema": "2.0"
    "id": "d6e29866-7739-43ef-8527-320bd99880d3"
    ⊕"oracle": {...}
    "source": ""
    "specversion": "1.0"
    "time": "2023-07-17T17:09:45.846Z"
    "type": "com.oraclecloud.LogSearch.SearchLogs"
  }
  "regionId": "eu-amsterdam-1"
}
```

Oracle Cloud
Logging & Acquisition

INVICTUS INCIDENT RESPONSE

"Identity" contains details on credentials, user-agent and IP-address of request


```
"identity": {
  "authType": "natv"
  "callerId": NULL
  "callerName": NULL
  "consoleSessionId": "csid1068b4c64da98601565debdb22a8"
  "credentials": "ST$eyJraWQiOiJhc3dfb2MxX2o0eGQiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJvY2lkMS51c2VyLm9jMS4uYWFhYWFhYWFiNDZ
  "ipAddress":
  "principalId": "ocid1.user.oc1..aaaaaaaab46rafwq3wvtrtpguf7o6b2fo5nynvdfehwj4dd5ykgu67hhcaza"
  "principalName": "K Stam"
  "tenantId": "ocid1.tenancy.oc1..aaaaaaaalnkcon5h3lky44htf5z2xetbjoh7p4hbsbkiotcz6vv6oeqys3nq"
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36"
```

Oracle Cloud
Logging & Acquisition

- Export can be made in .json format from the GUI

- GUI very limited in results size and time

You have reached the search results limit (500 results). Please adjust the query time range to refine your search results.

- The search results are limited to 10.000 results, via GUI/API which is also the export limit.

- Scripts to search and acquire logs available on the Oracle website see references.

https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/bulkexport.htm
https://docs.oracle.com/en-us/iaas/Content/Logging/Concepts/loggingoverview.htm
https://docs.oracle.com/en-us/iaas/Content/Logging/Concepts/using_the_api_searchlogs.htm

Oracle Cloud
Security & Premium features

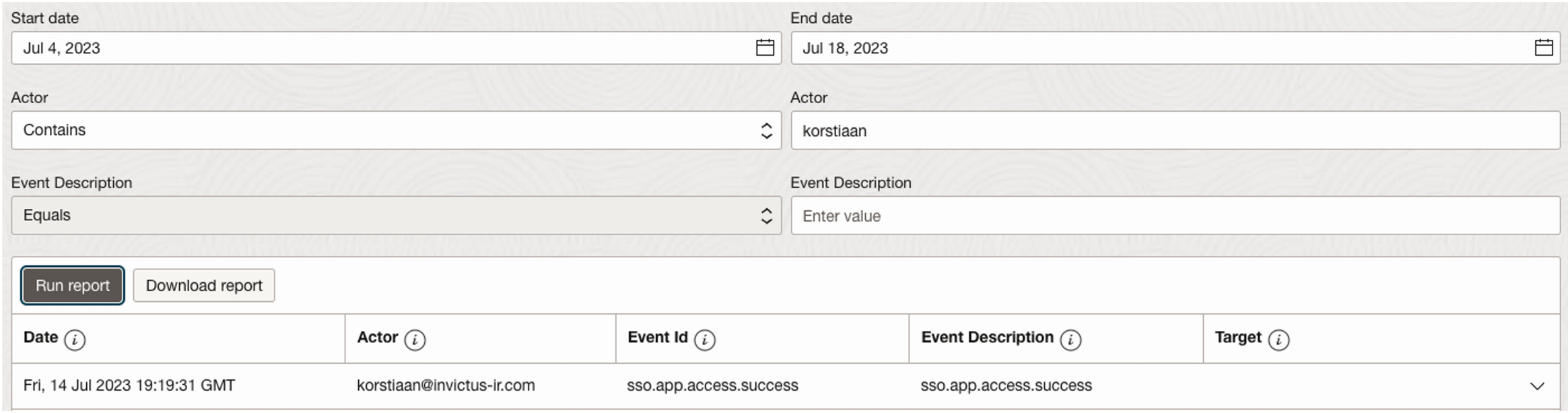
- Oracle Cloud Guard is the premium security feature more a CSPM tool than a detection/response tool

- There seems to be no real native security solution that alerts on attacks similar to GuardDuty or Defender

- The closest is Cloud Guard Threat Detector which is also fed by Threat Intelligence

Oracle Cloud
Challenges and things to know

- Audit Log Report can be useful for IR to know what actions an has performed



- Maximum period for log searches is 14 days via all methods (GUI/API/CLI)

Conclusion &Takeaways

INVICTUS INCIDENT RESPONSE

- 35 minutes is not enough time to give a comprehensive overview of three clouds :)
- Alibaba Cloud seems to be the most mature from a security perspective, mostly by mimicking and improving on AWS
- IBM Cloud, the audit logging is off by default and limited retention, no easy way around this
- Oracle Cloud, audit logging provides lots of details, but their security offering is lacking
- For the ‘other’ clouds there are almost no tools available that will help you in acquisition and analysis of cloud data

Questions?
Let’s connect

LinkedIn: To stay in touch and our latest offerings: **https://www.linkedin.com/company/invictus-incident-response**

Medium: We publish our research here: **https://invictus-ir.medium.com/**

Twitter: updates on our latest tools and research: **https://twitter.com/InvictusIR**

GitHub: this is where the magic happens: **https://github.com/invictus-ir**