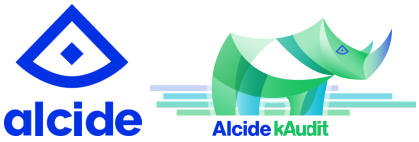


Alcide kAudit and Sumo Logic Integration

This application has been developed and is supported by Alcide.io.
In case of technical questions, please contact Alcide.io's support at support@alcide.io.

Product Description:

Alcide kAudit automatically analyzes Kubernetes audit logs to detect anomalous behavior of users and service accounts. kAudit automatically detects security-related issues related to Kubernetes' administrative actions, especially anomalous behavior that can only be detected from observing extended context over multiple activities. In addition, kAudit supports Audit rules to detect violations of organization compliance policies regarding Kubernetes usage. Incident forensics, along with audit statistics, are presented in graphical and tabular summaries for easy investigation and analysis.

The Alcide kAudit app provides real-time findings including:

- Incidents
- Anomalies
- Audit entries identified by the kAudit policies

Alcide kAudit Page

Alcide kAudit includes a dashboard and several searches for easy access to the findings collected by Alcide kAudit installed in the Kubernetes cluster.

Each kAudit installation handles a single cluster. Note that while the dashboard and searches are designed to present the information collected for a single cluster, they can be easily extended to present information from several clusters using the “cluster” property in the logs.

Log Types

The Alcide kAudit App uses the logs generated by the Alcide kAudit agent that is installed on each Kubernetes cluster.
The kAudit input stream consists of two logs:

- Anomalies and incidents - these logs, marked by ***_sourcecategory="detections"***, include all of the anomalies and incidents identified by the kAudit agent
- Audit entries - these logs, marked by ***_sourcecategory="selections"***, include the findings related to Kubernetes Audit log entries that match one of the kAudit policies.

Sample Log Message

Below is an example of the anomalies and incidents log message:


```
{
"category":"anomaly",
"cluster":"tst",
"etype":"principal",
"reasons":[
{
"values":{
"high":[
1
]
},
"doc":"change in count of unique caller user-agents in write access attempts",
"period":180000,
"direction":"write"
```

```
}
],
"time":1577297340000,
"short-doc":"change in access tool",
"project":"tst-project",
"context":{
"caller-supplied-user-agent":[
"ua1"
]
},
"eid":"180.1.0.4",
"confidence":"high",
"doc":"unusual change in tool used in access attempts"
}
```


Below is an example of the audit entry log message:


```
{
"count-period":1,
"cluster":"tst",
"rule":"pod-creation",
"time":1577293200000,
"caller-ip":"10.1.0.7",
"project":"tst-project",
"count":1,
"principal":"principal1",
"resource-namespace":"kube-system"
}
```

Query sample

Below is an example of a query that filters the anomalies and incidents per principal

```
_source="kaudit-data" and _collector="Kaudit Collector" and
_sourcecategory="detections"  principal | json
"category","etype", "eid" as category, etype, eid | where
etype="principal" | count by eid
```

Below is an example of a query that filters the audit entries by rules:

```
_source="kaudit-data" and _collector="Kaudit Collector" and
_sourcecategory="selections" rule | json "rule"as rule |  count
by rule
```

Collect Logs for Alcide kAudit

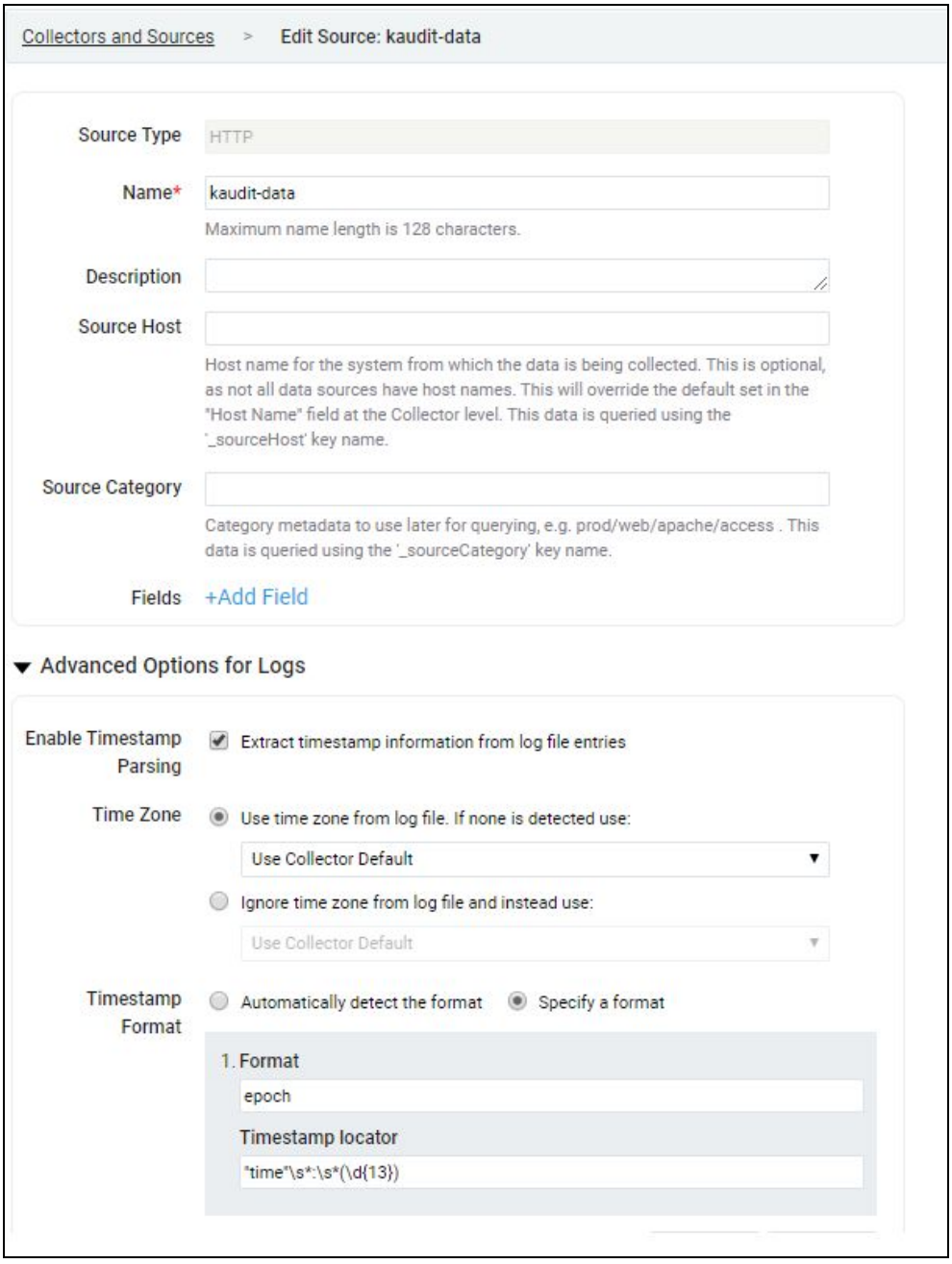
The Alcide kAudit is installed on the Kubernetes cluster. After installation is completed, kAudit integrations with 3rd party systems are configured, including the integration with Sumo Logic. kAudit uses Sumo Logic hosted collector.

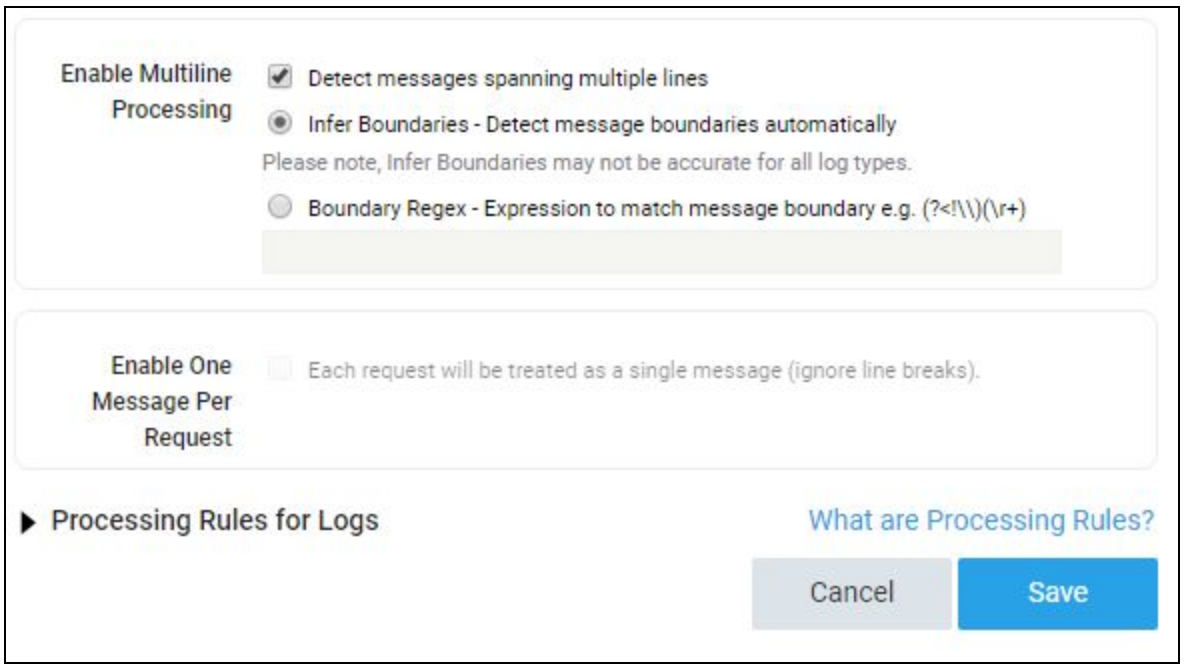
The sections below describe the steps for configuring the kAudit logs collection.

Collection process overview

Collection step 1. Add an HTTP Logs & Metrics Source

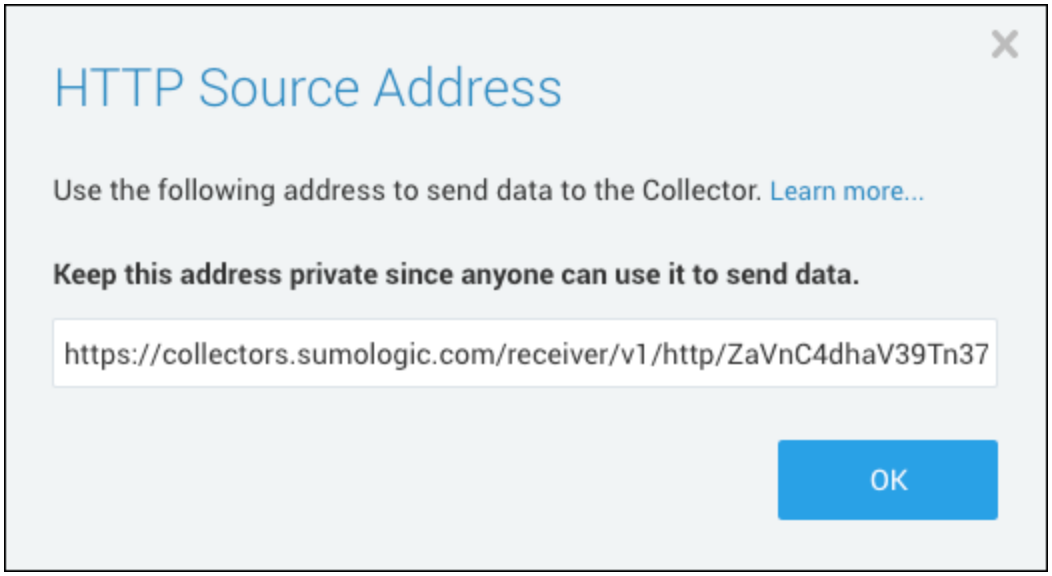
Add an HTTP Logs & Metrics source to the kAudit collector using the instructions outlined here.
Make sure to configure the time stamp extraction and multi-line detection as displayed below:





Collection step 2. Extract the Source URL and Configure kAudit

Once the Sumo Logic HTTP Logs and Metrics source are configured, you will get a popup with the HTTP Source Address as shown below:



You can always get the URL from the source, using the “Show URL” menu option. Configure the URL in kAudit in the HTTP API as detailed in the documentation.

There! You are done!

Install the App

To install the app, do the following:

Locate and install the “Alcide kAudit” app you need from the App Catalog. If you want to see a preview of the dashboards included with the app before installing, click ″Preview Dashboards″.

1. From the App Catalog, search for and select the app.
2. To install the app, click ″Add to Library″ and complete the following fields:
    1. **App Name**
       You can retain the existing name, or enter the name of your choice for the app.
    2. **Data Source**
       Select either of these options for the data source:
        - Choose Source Category, and select a source category from the list.
        - Choose Enter a Custom Data Filter, and enter a custom source category beginning with an underscore. Example: (_sourceCategory=MyCategory).
    3. **Advanced**
       Select the Location in Library (the default is the Personal folder in the library), or click “New Folder” to add a new folder.
3. Click Add to Library.

Once an app is installed, it will appear in your Personal folder, or another folder that you specified. From here, you can share it with your organization.

Panels will start to fill automatically. It's important to note that each panel slowly fills with data matching the time range query and received since the panel was created. Results won't immediately be available, but with a bit of time, you'll see full graphs and maps.

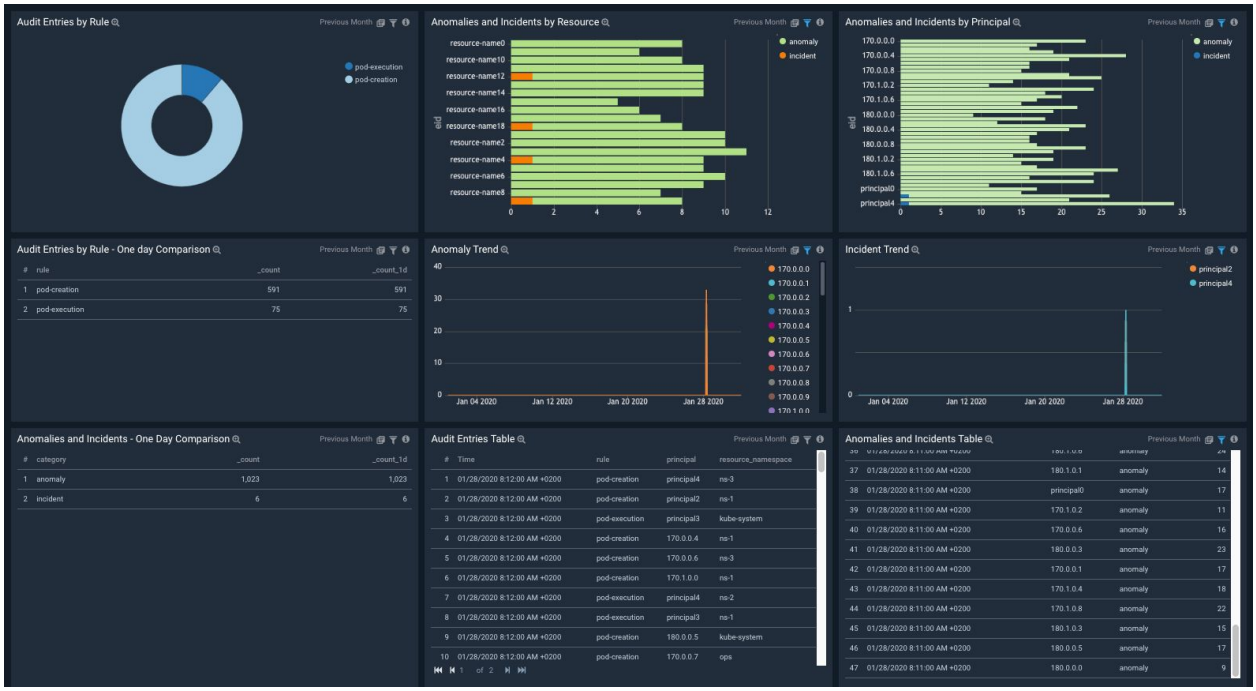
Dashboard filters

Each dashboard has a set of filters that you can apply to the entire dashboard, as shown in the following example. Click the funnel icon in the top dashboard menu bar to display a scrollable list of filters that are applied across the entire dashboard.

NOTE: You can use filters to drill down and examine the data on a granular level, using the funnel icon in each and every panel.

Each panel has a set of filters that are applied to the results for that panel only, as shown in the following example. Click the funnel icon in the top panel menu bar to display a list of panel-specific filters.

Alcide kAudit Overview



Use this dashboard to:

- Closely monitor and track all security-related audit entries, documenting relevant activities by users or service components, filtering events indicating policies violation

- Get a high-level view of tracked anomalies and incidents over time, proactively identifying non-compliant behavior with the ability to configure a set of rules representing the organization’s policies

- Investigate specific operational and security issues, trace back to responsible parties, troubleshoot and identify root cause with ease

The dashboard consists of two sets of panels:

- Anomalies and Incidents findings
- Rule-based findings

The Anomalies and Incidents describe the findings related to the anomalies and incidents detected by Alcide kAudit during the selected time period. The dashboard panels include the aggregation of the findings by a principal (user or a service), by resource and tabular details of the findings.

The Rule-based findings describe the findings of Kubernetes log entries that matched one of the rules configured by the user in the kAudit rules settings during the selected time period. The panels display the aggregation of the findings by rule and tabular details of the findings.

Panel title	Description
Audit Entries by Rule	Number of audit entries per pre-defined rules
Audit Entries Table	Tabular view of listed audit entries
Anomalies and Incidents by Resource	Number of anomalies and incidents per Kubernetes resource
Anomalies and Incidents by Principal	Number of anomalies and incidents per Principal (user or a service)
Anomalies and Incidents Table	Tabular view of listed anomalies and incidents
Anomaly Trend	Number of total anomalies over time
Incident Trend	Number of total incidents over time