Viewing and Managing System Logs

Operations Hub provides a tool for log aggregation and management leveraging the power of ElasticSearch-Logstash-Fluentd-Kibana (ELFK) stack. The Operations Hub GUI uses Elasticsearch as the data store for logs and Kibana provides meaningful visualization of the raw log data. You can create both macro and micro views using various visualization techniques.

- Enabling Log Management using ELFK stack, on page 1
- Viewing Audit Logs, on page 1
- Viewing Debug Logs, on page 2
- Viewing Logs Using Advanced Option, on page 3

Enabling Log Management using ELFK stack

During deployment, the Operations Hub is configured to forward logs from all the components to ElasticSearch for aggregation and indexing, providing some default visualizations and also available for creating custom visualization, search, and analysis.

Viewing Audit Logs

This procedure enables you to view the audit logs.

Step 1 At the main menu, select **Systems** > **Logs**.

The **Audit Dashboard** page appears.

Step 2 You can view the preconfigured information of audit logs in the following representations:

- Histogram—A view that displays a count of audit logs against time.
- Audit Log Table—A table that displays the audit logs generated based on user-initiated events from UI or using API interface.

  You can view the following information in the audit log table:

Table 1: Audit Log

Field	Description
Time	The time when the event was logged.
User	The user who initiated the event.
API	The API that was called.
Status	The HTTP response status code that is returned on invoking the API.
Response Time	The time taken by the API to execute.
Method	The HTTP method the API used.
Service Host	The application that served the request.

a. You can also search the logs based on following options:

- Kibana Query Language (KQL) query or fields as specified in the logs, and save the search using **Save Current Query**.
- Time duration as absolute time period, relative time, and now.
- Using filter options based on fields and operator enables you to narrow down the search. You can also edit the filter as query DSL and create custom label to the search.

b. Click **Update** to update the query.

c. Click **Refresh** to refresh and add a new search query.

Viewing Debug Logs

This procedure enables you to view the audit logs.

Step 1 At the main menu, select **Systems** > **Logs**.

The **Debug Dashboard** page appears.

Step 2 You can view the preconfigured information of audit logs in the following representations:

- Histogram—A view that displays a count of audit logs against time.
- Debug Log Table—A table that displays the audit logs generated based on user-initiated events from UI or using the API interface.

  You can view the following information in the debug log table:

Table 2: Debug Log

Field	Description
Time	The time when the debug event was logged.
Source	The application (cnBR or Operations Hub) where the event happened.
ContainerName	The microservice in the application that generated the event.
LogLevel	The log level.
Message	The entire log content.

Viewing Logs Using Advanced Option

Advanced options enable you to create and customize the dashboards and visualizations as required.

In the left-side menu, click **Advanced**. You can view the following submenus:

- **Dashboards**—The **Dashboard** page allows you us to view available dashboards or create a new dashboard view using the **Create Dashboard**. To create the new dashboard, add panels from saved 'Search' or 'Visualization', or you can create a new Visualization using available visualization types. Once you save the dashboard, click the **Dashboard** in the left side menu, and you can view the new dashboard.
- **Discover**—The **Discover** page allows you to find logs based on custom search definitions. You can save the search and later access, and use the saved search in the Dashboard. You can perform basic text search and advanced search using the KQL or Lucene Search.
- **Visualize**—The **Visualize** page enables you to view available library of logs or create a new Visualization. To create a new Visualization, click **Create Visualizations**, and select one of the available visualization types such as Lens, Maps, TSVB, Custom Visualization, and Aggregation based in the **New Visualization** page. Enter required search information. Once the visualization is created, you can save and use to create panels in the Dashboard.

Refreshing the Dashboard

You can set the refresh time for each dashboard, choose the time from the drop-down list on the top-right corner of the dashboard. You can select any time from 5 sec to 1 day. If you decide to avoid page refresh, selecting "off" from drop-down menu does not refresh the page.

If data is retrieved, you can choose a time range. It can be absolute time range where you can provide a time interval or you can select the range from a predefined drop down menu.

TAC Debug Package

Feature History

Feature Name	Release Information	Description
TAC Debug Package	Cisco Operations Hub 22.2	You can create TAC debug package for a cluster. The collected information helps the TAC team to debug and troubleshoot the issue at the earliest.

The TAC Debug feature in Operations Hub enables you to create and collect the debug package for a specified time duration. You can download the debug package and attach it to a TAC case.

Once you trigger the create operation on the Operations Hub cluster, you can monitor the status of operation as "ongoing" or "completed". Once the operation is complete, the TAC debug package is available for download.

Note You can perform the TAC debug operations only using API and this feature is not supported in the Operations Hub GUI yet. For more information, see the Cisco Operations Hub and Smart PHY REST API Guide.