Monitoring Operations Hub

Alerts

All alerts are built based on the KPI metrics and divided into several alert groups. Each KPI metric generates one alert that belongs to a predefined alert group.

Alert Record

The **Alert Management Dashboard** captures all alerts that are generated in the Cisco Operations Hub cluster. This dashboard displays alert summary and detailed information about those alerts.

Viewing Alert Summary

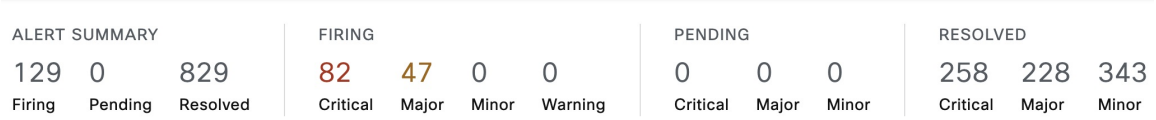
The **Alerts** page displays a summary of total number of firing, pending, and warning alerts based on alert severity. You can access the alert overview page from the main menu.

1. At the main menu, select **Alerts**. The **Alerts** page appears.
2. View **Alert Summary**.

Cisco Operations Hub supports the following alert severity:

- Critical
- Major
- Minor
- Warning

Figure 1: Alerts Summary



Viewing Alert Information

You can view a list of firing alerts that are currently active and a list of resolved alerts. At the main menu, select **Alerts** to view the alerts.

Alerts Summary Total count of firing, pending and resolved alerts. Count of alerts are based on severity.

Figure 2: Alerts Summary

You can filter alerts on any of the following conditions:

Table 1: Filter condition

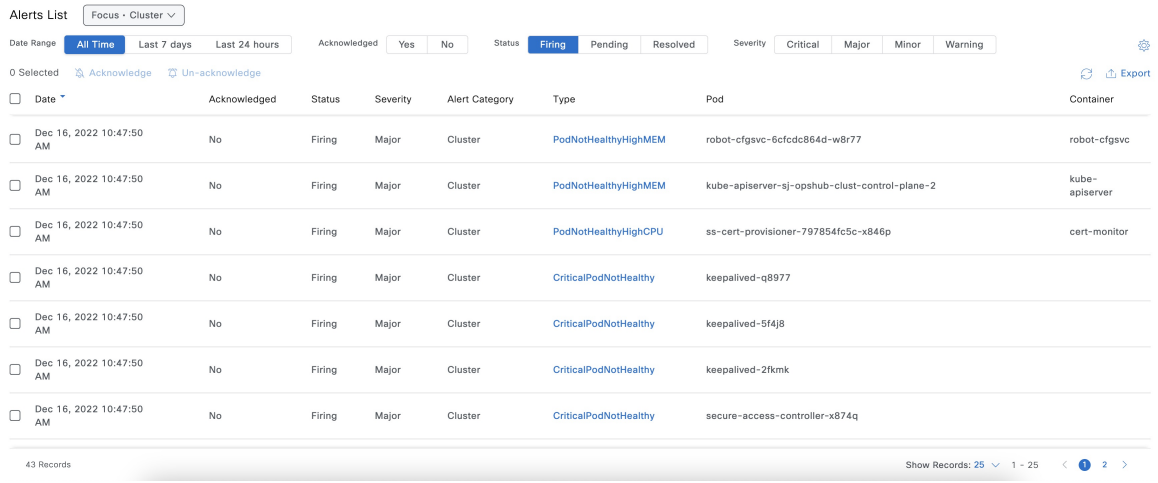
Filter condition	Description	Options
Focus filter	List of Alert categories	**Cluster** (default), **Operations Hub Infrastructure**, **DB Upgrade**, **Internal User Password Expiration**, **System**
Date Range	Filter alerts in a specific time window	**All Time** (default), **Last 7 days**, **Last 24 hours**
Acknowledged	Filter using acknowledgement status	**Yes**, **No**
Status	Status of an alert	**Firing** (default), **Pending**, **Resolved**
Severity	Severity of the alerts	**Critical**, **Major**, **Minor**, **Warning**

Table 2: Alerts table

Field	Description	Options
Date	Date and Time when the alert is fired	**Date and Time**
Acknowledged	Shows whether an alert is acknowledged or not	**Yes, No**
Status	Status of the alert	**Firing, Pending, Resolved**
Severity	Severity of the alert	**Critical, Major, Minor, Warning**
Alert Category	Category of the alert	**Cluster, OperationsHubInfra, DbUpgrade, InternalUserPasswordExpiry, System**

Field	Description	Options
Type	Type of the alert	**High CPU, High Memory**
Pod	Details of the pod generating an alert	**Pod-Details**
Container	Details of the container generating an alert	**Container-Details**

Figure 3: Alerts List



You can view the details of an alert by clicking the Alert Type. The alert details panel captures the following fields:

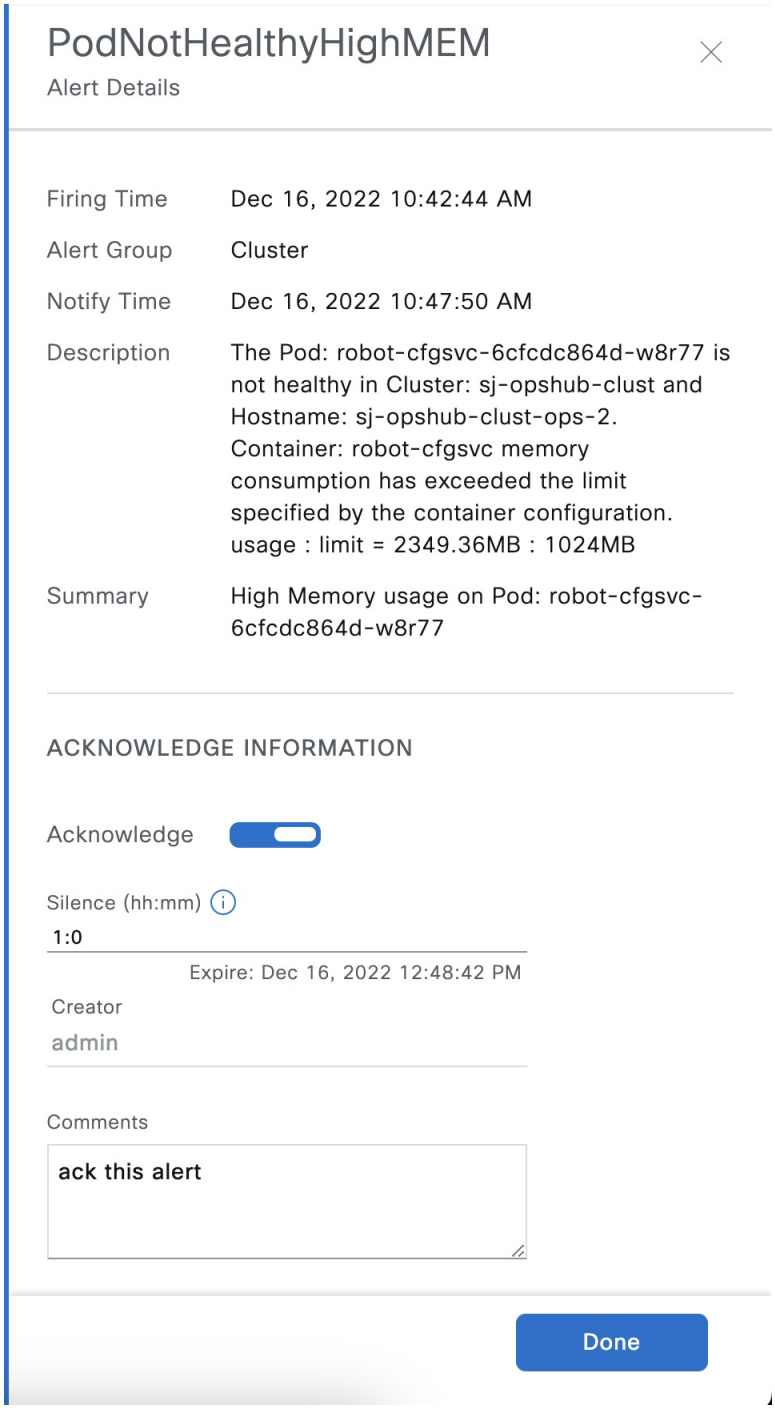
Field	Description
Status	Status of the alert
Firing Time	Time when alert is raised
Alert Category	Category of the alert
Notify Time	Displays alert notify time
Description	Description of the alert
Summary	A short summary of the alert

Figure 4: Alerts Details

Acknowledging Alerts

Once an alert is raised, you can acknowledge the firing alert. You have an option to put a comment before you acknowledge. You can also silence alerts for a predefined time in case you wish to ignore the alert during that time. By default, every three hours you are notified about the firing alerts by email.

Figure 5: Acknowledging Alerts



Monitoring Cluster Health

Table 3: Feature History

Feature Name	Release Information	Description
Cluster Health Monitoring	Cisco Operations Hub 22.2	Cisco Operations Hub supports viewing and monitoring of the cluster health using the alert management feature. An alert is raised when there is an issue and you can take necessary action based on the severity of the alert. You can view the cluster health information using the **Kubernetes Cluster Health** dashboard.
Alert UI	Cisco Operations Hub, Release 22.4	Alert UI is introduced.

Operations Hub enables you to view and monitor the cluster health using the alert management feature. For each cluster, you can map an alert-group to check the cluster health status and take required action. Each alert is categorized based on severity which helps you prioritize the action for taken for that alert. If you do not specify any alert-group for the cluster, then all available alert-groups are added to the cluster

A cluster can have the following types of health alerts:

- **Clear** - Indicates that the cluster has no alerts and everything is working as expected.
- **Minor** - Indicates that a few nonessential pods are not running in the cluster. If you see this alert, then rectify the problem at the earliest.
- **Critical** - Indicates that the cluster has critical problems. Take immediate action before the service degrades further.

Each alert-group is independent in nature, and therefore it is important to review all the alert-groups. Ensure that you take corrective actions that are based on the overall cluster health and not just for an individual alert-group.

For example, an essential pod such as **timescaledb** can have high CPU usage, which causes it to raise a **Critical** alert. This is part of the *Cluster* alert-group for which the cluster health severity is **Critical**.

Similarly, if there are no critical alerts for the *InternalUserPasswordExpiry* alert-group and all the pods are running in the cluster, then the cluster health severity is **Clear**.

For more information regarding *Operations Hub Infra Alert Management API*, see Cisco Operations Hub and Smart PHY REST API Guide

1. At the main menu, choose **Dashboards**. The **Dashboard Gallery** page appears.
2. Click **Kubernetes Cluster Health**.

   The **Kubernetes Cluster Health** dashboard displays.
3. At the main menu, select **Alerts** .

   The **Alerts** page displays.

Viewing and Managing System Logs

Feature History

Feature Name	Release Information	Description
Dedicated Application Debug Logs	Cisco Operations Hub 22.3	You can view application-specific debug logs using the Debug Dashboard.

Operations Hub provides a tool for log aggregation and management, leveraging the power of ElasticSearch-Logstash-Fluentd-Kibana (ELK) 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 ELK 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 4: Audit Log

Field	Description
Time	The time when the event is logged.
User	The user who initiated the event.
API	The API that is called.
Status	The HTTP response status code that is returned on invoking the API.
Response Time	The time taken by the API to execute.

Field	Description
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 5: Debug Log

Field	Description
Time	The time when the event is logged.
User	The user who initiated the event.
API	The API that is 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.

Field	Description
Service Host	The application that served the request.

Viewing Logs Using Advanced Option

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

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

The **Debug Dashboard** page displays.

Step 2 At the left-side menu, click **Advanced**. You can view the following submenus:

- **Dashboards**—The **Dashboard** page allows you 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.

Dedicated Application Debug Logs

If you have installed applications such as Smart PHY on Operations Hub, you can view the application-specific debug logs.

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

Step 2 At the left-side menu, click **Debug Dashboard** option under the application header to view application-specific debug logs.

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.