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

ALERT SUMMARY			FIRING				PENDING			RESOLVED		
129	0	829	82	47	0	0	0	0	0	258	228	343
Firing	Pending	Resolved	Critical	Major	Minor	Warning	Critical	Major	Minor	Critical	Major	Minor

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

ALERT SUMMARY			FIRING				PENDING			RESOLVED		
129	0	829	82	47	0	0	0	0	0	258	228	343
Firing	Pending	Resolved	Critical	Major	Minor	Warning	Critical	Major	Minor	Critical	Major	Minor

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

CriticalPodNotHealthy

Alert Details

ALERT INFORMATION

Status	Firing
Severity	Major
Firing Time	Dec 16, 2022 10:42:44 AM
Alert Group	Cluster
Notify Time	Dec 16, 2022 1:47:50 PM
Description	The critical Pod: kube-proxy-fqkfm is not healthy in Cluster: sj-opshub-clust and Hostname: sj-opshub-clust-infra-2.
Summary	The critical Pod: kube-proxy-fqkfm is not healthy.

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

PodNotHealthyHighMEM
Alert Details

Firing Time	Dec 16, 2022 10:42:44 AM
Alert Group	Cluster
Notify Time	Dec 16, 2022 10:47:50 AM
Description	The Pod: robot-cfgsvc-6cfcdc864d-w8r77 is not healthy in Cluster: sj-opshub-clust and Hostname: sj-opshub-clust-ops-2. Container: robot-cfgsvc memory consumption has exceeded the limit specified by the container configuration. usage : limit = 2349.36MB : 1024MB
Summary	High Memory usage on Pod: robot-cfgsvc-6cfcdc864d-w8r77

ACKNOWLEDGE INFORMATION

Acknowledge

Silence (hh:mm) ⓘ

1:0

Expire: Dec 16, 2022 12:48:42 PM

Creator

admin

Comments

ack this alert

Done

Configuring Alerts

KPIs

Key Performance Indicator (KPI) of Operations Hub helps in getting information on the overall system stability and on the components that are not functioning normally and are impacting the system stability.

The Operations Hub supports the following KPI Alert Groups:

- Cluster

- OperationsHubInfra

- DbUpgrade

- InternalUserPasswordExpiry

Configuring Alerts Using SMTP

Use this task to configure alerts globally using Simple Mail Transfer Protocol (SMTP).

1. At main menu, select **System > Email Notifications** view the **Email Notifications** page.

2. You can configure Email Notifications by clicking **Edit** at the bottom right of the page.

3. On the **SMTP Configuration** pane, enter the **SMTP Configuration** details.

SMTP Configuration Details

Field	Description
From Email Address	The default **SMTP From address** header field.
SMTP Server Hostname	The default SMTP smart host used for sending emails, including the port number. The port number is 25 or 587 for SMTP over TLS (STARTTLS). Example: `smtp.example.org:587`

4. Click **Save**.

Configuring Alert groups

Use this task to enable or disable an alert group and add or delete email addresses of receivers for each alert group.

1. At main menu, select **System > Email Notifications** view the **Email Notifications** page.

2. You can configure Email Notifications by clicking **Edit** at the bottom right of the page.

3. Use the **Alert Categories** pane to configure the group or the recipients.

4. Select the toggle button next to the alert category name to **Enable** the alert group.

5. Click the **Alert Category** name to open a sidebar where the recipient email(s) can be configured, so the recipients receive notification when an alert is generated under that respective group.

6. Click **Save**.

Figure 6: Email Notifications

Figure 7: Notification Recipient List

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.