Operations Console

Operations Console

Publication Date: 09/08/2022

SUSE LLC
1800 South Novell Place
Provo, UT 84606
USA
https://documentation.suse.com

Contents

1 Alarm Definition

The *Alarm Definition* section under *Monitoring* allows you to define alarms that are useful in generating notifications and metrics required by your organization. By default, alarm definitions are sorted by name and in a table format.

1.1 Filter and Sort

The search feature allows you to search and filter alarm entries by name and description.

The check box above the top left of the table is used to select all alarm definitions on the current page.

To sort the table, click the desired column header. To reverse the sort order, click the column again.

1.2 Create Alarm Definitions

The *Create Alarm Definition* button next to the search bar allows you to create a new alarm definition.

To create a new alarm definition:

1. Click *Create Alarm Definition* to open the *Create Alarm Definition* dialog.
2. In the Create Alarm Definition window, type a name for the alarm in the *Name* text field. The name is mandatory and can be up to 255 characters long. The name can include letters, numbers, and special characters.
3. Provide a short description of the alarm in the *Description* text field (optional).
4. Select the desired severity level of the alarm from the *Severity* drop-down box. The severity level is subjective, so choose the level appropriate for prioritizing the handling of alarms when they occur.
5. Although not required, in order to specify how to receive notifications, you must be able to select the method(s) of notification (Email, Web, API, etc.) from the list of options in the Alarm Notifications area. If none are available to choose from, you must first configure them in the Notifications Methods window. Refer to the Notification Methods help page for further instructions.

6. To enable notifications for the alarm, enable the check box next to the desired alarm notification method.
7. Apply the following rules to your alarm by using the Alarm Expression form:
    - *Function*: determines the output value from a supplied input value.
    - *Metric*: applies a pre-defined means of measuring whatever aspect of the alarm.
    - *Dimension(s)*: identifies which aspect (Hostname, Region, and Service) of the alarm you want to monitor.
    - *Comparator*: specifies the operator for how you want the alarm to trigger.
    - *Threshold*: determines the numeric threshold associated with the operator you specified.
8. *Match By* (optional): group results by a specific dimension that is not part of the Dimension(s) solution.
9. To save the changes and add the new alarm definition to the table, click *Create Alarm Definition*.

2 Alarm Explorer

This page displays the alarms for all services and appliances. By default, alarms are sorted by their state.

2.1 Filter and Sort

Using the *Filter Alarms* button, you can filter the alarms by their IDs and dimensions. The *Filter Alarms* dialog lets you configure a filtering rule using the *Alarm ID* field and options in the *Dimension(s)* section.

You can display the alarms by grid, list or table views by selecting the corresponding icons next to the *Sort By* control.

To sort the alarm list, click the desired column header. To reverse the sort order, click the column again.

2.2 Alarm Table

Each row has a checkbox to allow you to select multiple alarms and set the same condition on them.

The **Status** column displays a graphical indicator that shows the state of each alarm:

- Green indicator: OK. Good operating state.
- Yellow indicator: Warning. Low severity, not requiring immediate action.
- Red indicator: Alarm. Varying severity levels and must be addressed.
- Gray indicator: Unknown.

The **Alarm** column identifies the alarm by the name it was given when it was originally created.

The **Last Check** column displays the date and time the most recent occurrence of the alarm.

The **Dimension** column describes the components to check in order to clear the alarm.

2.3 Notification Methods

The *Notification Methods* section of the Alarm Explorer allows you to define notification methods that are used by the alarms. By default, notification methods are sorted by name.

2.3.1 Filter and Sort

The filter bar allows you to filter the notification methods by specifying a filter criteria. You can sort the available notification methods by clicking on the desired column header in the table.

2.3.2 Create Notification Methods

The *Create Notification Methods* button beside the search bar allows you to create a new notification method.

To create a new notification method:

1. Click the *Create Notification Method* button.
2. In the *Create Notification Method* window, specify a name for the notification in the *Name* text field. The name is required, and it can be up to 255 characters in length, consisting of letters, numbers, or special characters.
3. Select a *Type* in the drop down and select the desired option:
   - *Web Hook* allows you to enter in an internet address, also referred to as a *Web Hook*.
   - *Email* allows you to enter in an email address. For this method to work you need to have a SMTP server specified.
   - *PagerDuty* allows you to enter in a PagerDuty address.
4. In the *Address/Key* text field, provide the required values.
5. Press *Create Notification Method*, and you should see the created notification method in the table.

3 Compute Hosts

This *Compute Hosts* page in the *Compute* section allows you to view your Compute Host resources.

3.1 Filter and Sort

The dedicated bar at the top of the page bar lets you filter alarm entries using the available filtering options.

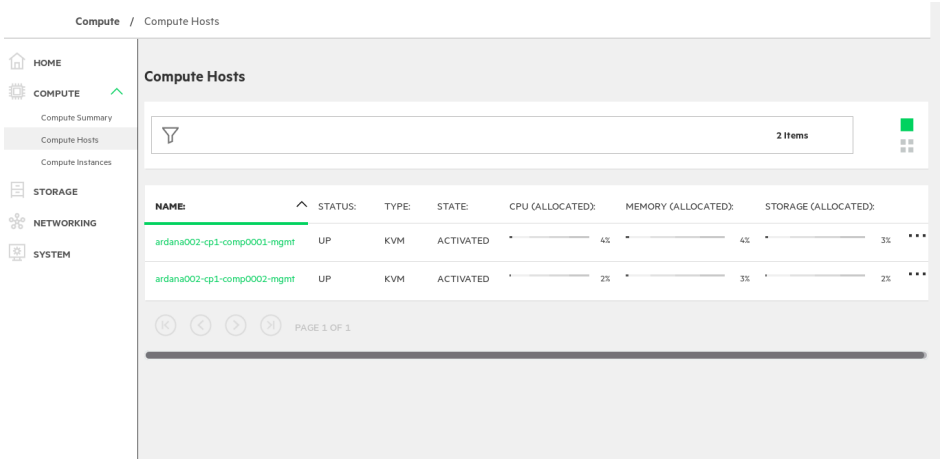


FIGURE 3.1: COMPUTE HOSTS

Click the *Filter* icon to select one of the available options:

- *Any Column* enables plain search across all columns
- *Status* filters alarm entries by status.
- *Type* enables filtering by host type, including Hyper-V, KVM, ESXi, and VMWare vCenter server.
- *State* filters alarm entries by Nova state (for example, Activated, Activating, Imported, etc.).
- *Alarm State* filters entries bay status of the alarms that are triggered on the host.
- *Cluster* returns a filtered list of configured clusters that Compute Hosts belong to.

The alarm entries can be sorted by clicking on the appropriate column header, such as *Name*, *Status*, *Type*, *State*, etc.

To view detailed information (including alarm counts and utilization metrics) about a specific host in the list, click in the host's name in the list.

4 Compute Instances

This Operations Console page allows you to monitor your Compute instances.

4.1 Search and Sort

The search bar allows you to filter the alarm definitions you want to view. Type and Status are examples of alarm criteria that can be specified. Additionally, you can filter by typing in text similar to searching by keywords.

The checkbox allows you to select (or deselect) a group of alarm definitions to delete:

- *Select Visible* allows you to delete the selected alarm definitions from the table.
- *Select All* allows you to delete all the alarms from the table.
- *Clear Selection* allows you to clear all the selections currently selected from the table.

You can display the alarm definitions by grid, list or table views by selecting the corresponding icons next to the *Sort By* control.

The *Sort By* control contains a drop-down list of ways by which you can sort the compute nodes. Alternatively, you can also sort using the column headers in the table.

- *Sort by Name* displays the compute instances by the name assigned to it when it was created.
- *Sort by State* displays the compute instances by their current state.
- *Sort by Status* displays the compute instances by their current status.
- *Sort by Host* displays the compute instances by their host.
- *Sort by Image* displays the compute instances by the image being used.
- *Sort by IP Address* displays the compute instances by their IP address.

5 Compute Summary

The *Compute Summary* page in the *Compute* section gives you access to inventory, capacity, and alarm summaries.

5.1 Inventory Summary

The *Inventory Summary* section provides an overview of compute alarms by status. These alarms are grouped by control plane. There is also information on resource usage for each compute host. Here you can also see alarms triggered on individual compute hosts.

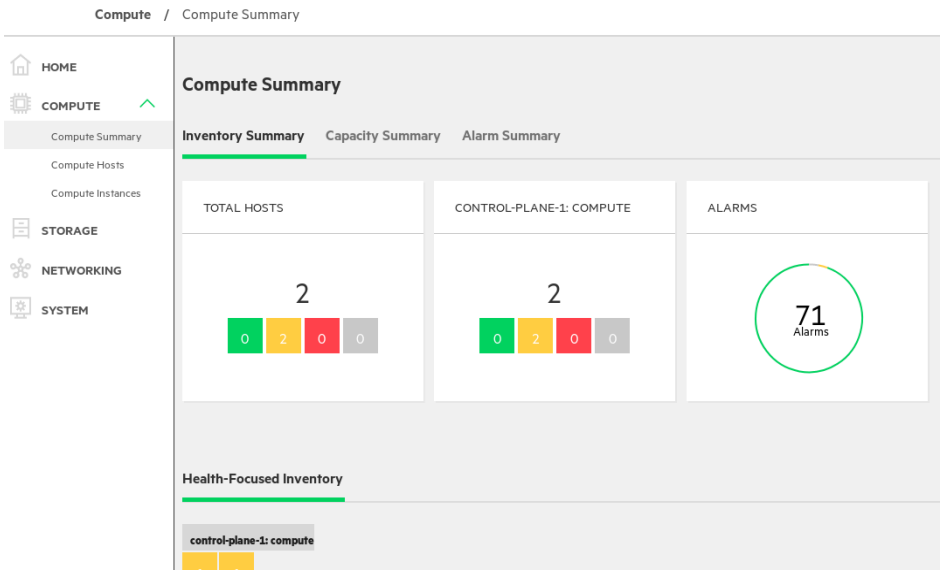


FIGURE 5.1: COMPUTE SUMMARY

5.2 Capacity Summary

Capacity Summary offers an overview of the utilization of physical resources and allocation of virtual resources among compute nodes. Here you will also find a break-down of CPU, memory, and storage usage across all compute resources in the cloud.

5.3 Compute Summary

The *Compute Summary* show overviews of new alarms as well as a list of all alarms that can be filtered and sorted. For more information on filtering alarms, see *Chapter 2, Alarm Explorer*.

6 Appliances

This page displays details of an appliance.

Search and Sort

- The search bar allows you to filter the appliances you want to view. **Role** and **Status** are examples of criteria that can be specified. Additionally, you can filter by selecting **Any Column** and typing in text similar to searching by keywords.
- You can sort using the column headers in the table.

Actions

Click the Action icon (three dots) to view details of an appliance.

More Information

HPE Helion CloudSystem Network Planning Guide (http://www.hpe.com/info/cloudsystem/docs)

7 Block Storage Summary

This page displays the alarms that have triggered since the timeframe indicated.

Search and Sort

- The search bar allows you to filter the alarms you want to view. **State** and **Service** are examples of criteria that can be specified. Additionally, you can filter by typing in text similar to searching by keywords.
- You can sort alarm entries using the column headers in the table.

New Alarms: Block Storage

The New Alarms section shows you the alarms that have triggered since the timeframe indicated. You can select the timeframe using the Configure control with options ranging from the Last Minute to Last 30 Days. This section refreshes every 60 seconds.

The new alarms will be separated into the following categories:

Category	Description
Critical	Open alarms, identified by red indicator.
Warning	Open alarms, identified by yellow indicator.
Unknown	Open alarms, identified by gray indicator. Unknown will be the status of an alarm that has stopped receiving a metric. This can be caused by the following conditions: • An alarm exists for a service or component that is not installed in the environment. • An alarm exists for a virtual machine or node that previously existed but has been removed without the corresponding alarms being removed. • There is a gap between the last reported metric and the next metric.
Open	Complete list of open alarms.
Total	Complete list of alarms, may include Acknowledged and Resolved alarms.

More Information

- *Chapter 2, Alarm Explorer*
- *Book “Operations Guide”, Chapter 15 “Troubleshooting Issues”, Section 15.1 “General Troubleshooting”, Section 15.1.1 “Alarm Resolution Procedures”*

8 Logging

This page displays the link to the Logging Interface, known as Kibana.

Important: Accessing Kibana

The Kibana logging interface only runs on the management network. You need to have access to that network to be able to use Kibana.

8.1 View Logging Interface

To access the logging interface, click the *Launch Logging Interface* button, which will open the interface in a new window.

For more details about the logging interface, see *Book "Operations Guide", Chapter 12 "Managing Monitoring, Logging, and Usage Reporting", Section 12.2 "Centralized Logging Service"*.

9 My Dashboard

This page allows you to customize the dashboard by mixing and matching graphs and alarm cards.

My Dashboard allows you to customize the dashboard by mixing and matching graphs and alarm cards. Since different operators may be interested in different metrics and alarms, the configuration for this page is tied to the login account used to access Operations Console. Charts available here are based on metrics collected by the Monasca monitoring component.

10 Networking Alarm Summary

This page displays the alarms for the Networking (Neutron), DNS, Firewall, and Load Balancing services. By default, alarms are sorted by State.

10.1 Filter and Sort

The filter bar allows you to filter the alarms by the available criteria, including *Dimension*, *State*, and *Service*. The dimension filter accepts key/value pairs, while the State filter provides a selection of valid values.

You can sort alarm entries using the column headers in the table.

10.2 Alarm Table

You can select one or multiple alarms using the check box next to each entry.

The **State** column displays a graphical indicator that shows the state of each alarm:

- Green indicator: OK. Good operating state.
- Yellow indicator: Warning. Low severity, not requiring immediate action.
- Red indicator: Alarm. Varying severity levels and must be addressed.
- Gray square (or gray indicator): Undetermined.

The **Alarm** column identifies the alarm by its name.

The **Last Check** column displays the date and time the most recent occurrence of the alarm.

The **Dimension** column shows the components to check in order to clear the alarm.

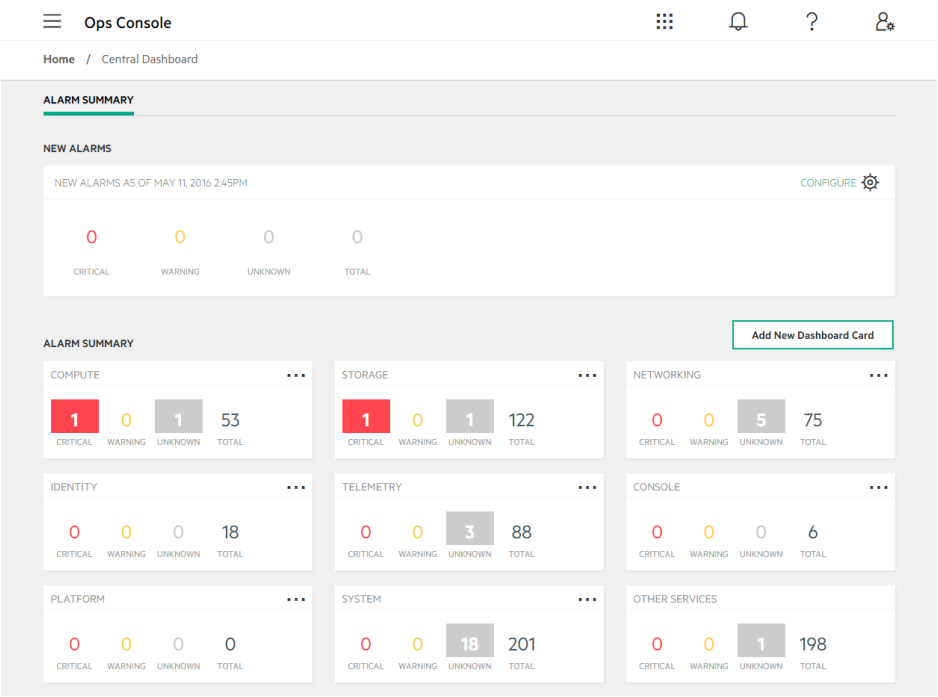
The last column, depicted by three dots, reveals an **Actions** menu gives you access to the following options:

- *View Details* opens a separate window with the information from the table view and the alarm history.
- *View Alarm Definition* allows you to view and edit the selected alarm definition.
- *Delete* is used to delete the currently selected alarm entry.

11 Central Dashboard

This page displays a high level overview of all cloud resources and their alarm status.

11.1 Central Dashboard



11.2 New Alarms

The New Alarms section shows you the alarms that have triggered since the timeframe indicated. You can select the timeframe using the *View* control with options ranging from the Last Minute to Last 30 Days. This section refreshes every 60 seconds.

The new alarms will be separated into the following categories:

- *Critical* - Open alarms, identified by red indicator.
- *Warning* - Open alarms, identified by yellow indicator.

- *Unknown* - Open alarms, identified by gray indicator. Unknown will be the status of an alarm that has stopped receiving a metric. This can be caused by the following conditions:
  - An alarm exists for a service or component that is not installed in the environment.
  - An alarm exists for a virtual machine or node that previously existed but has been removed without the corresponding alarms being removed.
  - There is a gap between the last reported metric and the next metric.
- *Open* - Complete list of open alarms.
- *Total* - Complete list of alarms, may include Acknowledged and Resolved alarms.

11.3 Alarm Summary

Each service or group of services have a dedicated card displaying related alarms.

- *Critical* - Open alarms, identified by red indicator.
- *Warning* - Open alarms, identified by yellow indicator.
- *Unknown* - Open alarms, identified by gray indicator. Unknown will be the status of an alarm that has stopped receiving a metric. This can be caused by the following conditions:
  - An alarm exists for a service or component that is not installed in the environment.
  - An alarm exists for a virtual machine or node that previously existed but has been removed without the corresponding alarms being removed.
  - There is a gap between the last reported metric and the next metric.
- *Open* - Complete list of open alarms.
- *Total* - Complete list of alarms, may include Acknowledged and Resolved alarms.