JUNIPER NETWORKS

Junos® Space

Network Director Fault Mode User Guide

Release
1.5

Published: 2013-10-15

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® Space Network Director Fault Mode User Guide
1.5

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation vii
Documentation and Release Notes vii
Documentation Conventions vii
Documentation Feedback ix
Requesting Technical Support ix
Self-Help Online Tools and Resources x
Opening a Case with JTAC x

Part 1 Overview

Chapter 1 **Fault Mode Overview 3**

Understanding Fault Mode in Network Director 3
What are Events and Alarms? 3
Alarm Severity 4
Alarm Classification 4
Alarm State 5
Understanding the Fault Mode Tasks Pane 6

Part 2 Administration

Chapter 2 **Viewing and Managing Alarms 9**

Customizing Alarms 9
Changing Alarm State 9
Searching Alarms 10

Chapter 3 **Alarm Monitor Reference 13**

Alarm Detail Monitor 13
Finding Specific Alarms 13
Sorting Alarms 14
Reading Events 16
Investigating Event Attributes 17
Changing the Alarm State 17
Alarms by Category Monitor 17
Alarms by Severity Monitor 18
Alarms by State Monitor 18
Current Active Alarms Monitor 19

List of Tables

About the Documentation vii

Table 1: Notice Icons viii
Table 2: Text and Syntax Conventions viii

Part 1 Overview

Chapter 1 Fault Mode Overview 3

Table 3: Network Director Alarm Classifications 4

Part 2 Administration

Chapter 2 Viewing and Managing Alarms 9

Table 4: Alarm Search Fields 10

Chapter 3 Alarm Monitor Reference 13

Table 5: Alarm Detail Fields 14
Table 6: Sort Options for Alarms 15
Table 7: Event Detail Fields 16
Table 8: Current Active Alarms Monitor 19

About the Documentation

- Documentation and Release Notes on page vii
- Documentation Conventions on page vii
- Documentation Feedback on page ix
- Requesting Technical Support on page ix

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Documentation Conventions

Table 1 on page viii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page viii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub <default-metric** *metric***>;**

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to **techpubs-comments@juniper.net**, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

- Fault Mode Overview on page 3

CHAPTER 1

Fault Mode Overview

- Understanding Fault Mode in Network Director on page 3
- Understanding the Fault Mode Tasks Pane on page 6

Understanding Fault Mode in Network Director

The Fault mode shows you information about the health of your network and changing conditions of your equipment. Use Fault mode to find problems with equipment, pinpoint security attacks, or to analyze trends and categories of errors.

This topic describes:

- What are Events and Alarms? on page 3
- Alarm Severity on page 4
- Alarm Classification on page 4
- Alarm State on page 5

What are Events and Alarms?

Activity on a network device consists of a series of *events*. A software component on the network device, called an *entity*, is responsible for running the Simple Network Management Protocol (SNMP) to log and monitor these events. When certain types of events are persistent, or when the condition causing the event crosses a threshold, SNMP sends a notification, also called a *trap* to Network Director. Network Director correlates traps, describing a condition, into an *alarm* . For example, multiple power supply traps coming from a device are correlated into a single power supply alarm for the device.

There are many types of alarms. An alarm can be as routine as when the device changes state or as serious as when a power supply has failed. When an alarm is sent, or *raised*, it stays raised until the triggering condition is resolved or *cleared*. The system can clear the alarm when the state changes again or an administrator can clear it manually, which indicates that the condition is now resolved.

SNMP also plays another role in Network Director. Enabling devices for SNMP with the appropriate read-only V1/V2/V3 credentials, can speed up device discovery.

Alarm Severity

Alarms are ranked by their impact to the network. The following list shows the ranking in Network Director from most impact to least impact on the network. It also shows the color scheme associated with each level of severity that is reflected in related graphs.

Critical (Red)—A critical condition exists; immediate action is necessary.

Major (Orange)—A major error has occurred; escalate or notify as necessary.

Minor (Yellow)—A minor error has occurred; notify or monitor the condition.

Info (Blue)—An informational message; no action is necessary. Informational alarms do not necessarily indicate an error. It could indicate that a device or entity has changed state.

Administrators can override the default severity of an alarm and set the severity to match their inhouse guidelines. Changing the severity level for an alarm is done on the Alarm Settings page in system Preferences.

Alarm Classification

Network Director organizes alarms into categories so you can view trends in the types of errors occurring on a network. These categories, shown in Table 3 on page 4 are derived from the SNMP Management Information Base (MIB) that is the information database or module containing the trap information for the event.

Table 3: Network Director Alarm Classifications

Category	Description
APAndRadio	Indicates alarms for access points and their radios. These alarms are generated from access points.
BFD	Indicates alarms for Bidirectional Forwarding Detection sessions. These alarms are generated from EX Series switches.
BGP	Indicates alarms for Border Gateway Protocol, Version 4.
Chassis	Indicates alarms for switch hardware, in this case, EX Series switches.
ClientAndUserSession	Indicates alarms for wireless clients.
ClusterAndModo	Indicates alarms about wireless network clusters and mobility domains.
Config	Indicates alarms for configuration management.
CoreAndControllers	Indicate device alarms.
CoS	Indicates class of service alarms.
DHCP	Indicates local server DHCP alarms.

Table 3: Network Director Alarm Classifications *(continued)*

Category	Description
DOM	Indicates Digital Optical Monitoring alarms that are generated from optical interfaces.
FlowCollection	Indicates alarms generated when collecting and exporting traffic flows.
General	Indicates alarms that are common to all network devices, such as link up/down or authentication.
GenericEvent	Indicates an alarm that is generated from an Op script or event policies.
L2ALD	Indicates MAC address alarms generated from the Layer 2 Address Learning Daemon (L2ALD).
L2CP	Indicates alarms generated by Layer 2 Control Protocol features.
MACFDB	Indicates an alarm for when MAC addresses are learned or removed from the forwarding database of the monitored device.
Misc	Indicates alarms that do not fit into the other categories.
PassiveMonitoring	Indicates alarms that occur on a passive monitoring interface.
Ping	Indicates alarms that a generated during a Ping request.
RFDETECT	Indicates alarms from radio frequency conditions. These alarms are generated from wireless controllers.
RMON	Indicates RMON alarms
SONET	Indicates a SONET or SDH alarm on an interface.
SONET APS	Indicates alarms generated on a SONET interface that participates in Automatic Protection Switching (APS).
VirtualChassis	Indicates alarms generated from Virtual Chassis members regarding member or port status.
VNETWORK	Indicates virtual networking alarms.

Alarm State

Once an alarm is active, it has one of these states:

- Active—Alarms that are current and not yet acknowledged or cleared.
- Cleared—Alarms that are resolved and the device or entity has returned to normal operation.

Some alarm states go directly from active to cleared state and require little to no administrative effort. However, other alarms with a high severity should be acknowledged and investigated.

In addition to acknowledging and clearing an alarm, you can assign an alarm to someone and you can append a note or annotation to an alarm. Annotations are helpful for documenting the resolution of an alarm or time estimates for a fix. Changes to an alarm's state are made through the Alarm State monitor in Fault mode.

Related Documentation

- *Setting Up User and System Preferences*
- Alarms by Severity Monitor on page 18
- Alarms by Category Monitor on page 17
- Current Active Alarms Monitor on page 19
- Alarms by State Monitor on page 18

Understanding the Fault Mode Tasks Pane

The Tasks pane in Fault mode provides you with a set of tools for effectively managing alarms on your system.

From the Tasks pane, you can filter known alarms to locate a specific alarm or error condition by clicking Search Alarms. Use this task to isolate alarms that occurred during a known time-frame or that have annotations associated with them. Although each of the Fault mode monitors can sort the alarms, Search Alarms enable you to submit multiple search and sort arguments as part of your search query.

In addition, Network Director enables you to group the tasks that you perform frequently and create a list of key tasks. You can add any task from the Tasks pane to the Key Tasks list by selecting a task and clicking the plus (+) sign that appears adjacent to the task. For some modes, you can see that Network Director has predefined some key tasks for you. You can modify this set of tasks to suit your requirements. This feature is available in Task pane irrespective of your current mode, scope, or view.

Related Documentation

- Searching Alarms on page 10
- Changing Alarm State on page 9
- Understanding Fault Mode in Network Director on page 3

PART 2

Administration

- Viewing and Managing Alarms on page 9
- Alarm Monitor Reference on page 13

CHAPTER 2

Viewing and Managing Alarms

- Customizing Alarms on page 9
- Changing Alarm State on page 9
- Searching Alarms on page 10

Customizing Alarms

Ensure that all devices are enabled for SNMP trap forwarding. This task, Set SNMP Trap Configuration, is found in Deploy mode.

Network Director enables you to tailor alarms by:

- Enabling or disabling individual alarms.
- Setting the amount of time alarms are retained in the system.

You can customize alarms using Preferences in the Network Director banner.

Related Documentation

- *Setting Up User and System Preferences*

Changing Alarm State

When an alarm becomes active, it remains active until either the system determines that the condition is resolved or system personnel change the status. Critical alarms always need immediate attention and seldom resolve on their own, but informational messages are often expected actions and results. When a condition is severe or persistent and needs attention, follow these steps:

1. Locate the alarm.
   a. Click **Fault** in the Network Director banner to enter Fault mode.
   b. Click the Alarm Details icon on any of the monitors to open the Alarm Details page. Scroll or sort the alarms to find the alarm in question. As an alternate method, click **Search Alarms** in the Tasks pane and filter the active alarm list.

c. Select the alarm.

2. Review the Event Details that triggered the trap for the alarm. These events provide insight into the cause or location of the problem.
3. Click **Acknowledge** to indicate that the problem is now known. You should receive a message saying the alarm is acknowledged.
4. Depending whether you can resolve the alarm with the information at hand or not, either assign the alarm to a member of your staff or clear the alarm. Click **Clear** to clear the alarm or click **Assign** and fill in the assignee's name.

At any time in the life cycle of an alarm, you can attach information about the alarm to the alarm record by clicking **Annotate**. Fill in your name in the **Notes By** field and add the note description in the **Notes** field. Click **Add** to record the annotation.

Related Documentation

- Alarm Detail Monitor on page 13

Searching Alarms

Use Search Alarms, available from the Tasks pane, to filter and isolate information about a specific alarm. Use this page to specify complex sorting and filtering criteria for all alarms.

Each field in the Search Alarm window helps narrow the current list of alarms. The more search items you specify, the more specific your results. All fields are optional.

1. Select or type the known descriptors for the alarm. These fields are described in Table 4 on page 10.
2. Click **Search** to run the query. The Alarms Details page opens with the results of your search.
3. Review the alarm. From this page you can change the state of the alarm, annotate, or assign the alarm to personnel. For more information about changing the state of an alarm, view "Changing Alarm State" on page 9.

Table 4: Alarm Search Fields

Search Criteria	Description
State	Use the list to select which alarm states to search for: • All—Alarms of all states. • Active—Alarms that are current and not yet acknowledged or cleared. • Clear—Alarms that are resolved and the device or entity has returned to normal operation.

Table 4: Alarm Search Fields *(continued)*

Search Criteria	Description
Category	Fill in one of the available alarm categories: • APAndRadio • BFD • BGP • Chassis • ClientAndUserSession • ClusterAndMoDo • Config • CoreAndControllers • CoS • DHCP • DOM • FlowCollection • GENERAL • GenericEvent • L2ALD • L2CP • MACFDB • Misc • PassiveMonitoring • Ping • RFDETECT • RMON • SONET • SONETAPS • VirtualChassis • VNETWORK
Severity	Pull down the list to select the severity level. Not all possible alarm severities are listed. Only the severity levels of your current active alarms are shown. Possible selections are: • Critical • Major • Minor • Info
Advanced Search Criteria	
(from) Date	Pull down the calendar and select the starting date of the search.
(from) Time	Pull down the list to select the starting time of the search. Search times are in military (24-hour) clock format in 30 minute intervals.
(to) Date	Pull down the calendar and select the ending date of the search.

Table 4: Alarm Search Fields *(continued)*

Search Criteria	Description
(to) Time	Pull down the list to select the ending time of the search. Search times are in military (24-hour) clock format in 30 minute intervals.
Notes	Enter any keywords or phases that were listed in an existing annotation.

Related Documentation

- Understanding Fault Mode in Network Director on page 3

CHAPTER 3

Alarm Monitor Reference

- Alarm Detail Monitor on page 13
- Alarms by Category Monitor on page 17
- Alarms by Severity Monitor on page 18
- Alarms by State Monitor on page 18
- Current Active Alarms Monitor on page 19

Alarm Detail Monitor

Use the Alarm Detail monitor to sort alarms, view an alarm in depth, and to assign a disposition to an alarm.

By clicking the Details icon, you can access the Alarm Detail monitor from any of the four alarm monitors available on the main page in Fault mode (Severity, Category, Current, or State). It is also available from the Current Active Monitors available from the Summary tab in Monitor mode.

This topic describes:

- Finding Specific Alarms on page 13
- Sorting Alarms on page 14
- Reading Events on page 16
- Investigating Event Attributes on page 17
- Changing the Alarm State on page 17

Finding Specific Alarms

Use the Alarm Detail monitor to locate a specific alarm, research the events causing the alarm, and to assign a disposition to the alarm. When an alarm is highlighted in the sorting sequence, the events contributing to the alarm are listed in Event Details and the variable settings are shown in Event Attribute Detail.

To locate an alarm and to assign a disposition to the alarm:

1. Sort the list using the Display list. Sorting choices vary depending on how you arrived here. View "Sorting Alarms" on page 14 for details on sorting options.

2. Review the sorted list. Each entry shows a minimum of one to a maximum of nine fields. These fields are described in Table 5 on page 14.
3. Examine the events and event attributes that contributed to sending the alarm. Events and event attributes are discussed in "Reading Events" on page 16 and "Investigating Event Attributes" on page 17.

Table 5: Alarm Detail Fields

Field	Value	Shown in Detailed View by Default
Name	The alarm name.	Yes
ID	A system and sequentially-generated identification number.	No
Assigned To	If assigned to an individual, it shows the name of the person assigned; otherwise, it shows System to mark that the alarm is still unassigned.	Yes
Severity	The severity of the alarm. Severity levels are: • Critical—A critical condition exists; immediate action is necessary. • Major—A major error has occurred; escalate or notify as necessary. • Minor—A minor error has occurred; notify or monitor the condition. • Info—An informational message; no action is necessary.	Yes
Acknowledged	Indicates if the alarm has been acknowledged.	Yes
Entity ID	The identification of the entity responsible for causing this alarm. The Entity ID is the key for correlation of events into an alarm. The Entity ID could be a MAC address of a radio or an IP address of the device.	Yes
Source	The IP address of the device or network element that generated the alarm. The SNMP agent is located at the source IP. In most cases, the source IP is the IP address of the switch or controller.	No
Reporting Device	The hostname of the reporting device.	Yes
Creation Date	The date and time the alarm was first reported.	No
Last Updated	The date and time that the information for the alarm was last modified.	Yes
Updated By	Either the system or the last user who modified the alarm.	No

Sorting Alarms

Depending on the monitor you chose to access Alarm Detail, your sorting options change to reflect the summary monitor. The different sort options are listed in Table 6 on page 15.

Table 6: Sort Options for Alarms

Alarms by Severity Sort	Alarms by Category Sort	Alarms by State and Current Active Alarms Sort
All	APAndRadio	Active
Info	BFD	Clear
Minor	BGP	
Major	Chassis	
Critical	ClientandUserSession	
	ClusterAndModDo	
	Config	
	CoreAndControllers	
	CoS	
	DHCP	
	DOM	
	FlowCollection	
	GENERAL	
	GenericEvent	
	L2ALD	
	L2CP	
	MACFDB	
	Misc.	
	PassiveMonitoring	
	Ping	
	RFDetect	
	RMON	
	SONET	

Table 6: Sort Options for Alarms *(continued)*

Alarms by Severity Sort	Alarms by Category Sort	Alarms by State and Current Active Alarms Sort
	SONETAPS	
	VirtualChassis	
	VNETWORKS	

You can also use Searching Alarms in the Tasks pane to perform searches using multiple arguments. With multiple arguments, you can isolate a single alarm from a long alarm list.

Reading Events

When you select an alarm in Alarm Detail, the Event Detail table updates with information about the events that are associated with the alarm. Table 7 on page 16 lists the fields in Event Detail.

Table 7: Event Detail Fields

Field	Value
Name	The event name; also known as the SNMP trap name.
ID	A system-generated, hexadecimal code that uniquely identifies the event.
Description	If the event is an SNMP event, it is shown as a system-generated event.
Type	The type of event, either fault or system alert.
Category	The category of the event message. The category corresponds to the alarm categories shown in the Alarms by Category monitor and the Alarm Settings window. These categories are: • RFDetect • General • Chassis • APandRadio • BFD • CoreandControllers • Misc.
Source	The identification of the entity that is the cause of this event ; it is not necessarily the ID of the event that generated the event.
Originator	The identification of the entity that generated this event, for example, the switch IP or controller IP address.
Time Updated	The date and time of the last update to the event.

Investigating Event Attributes

The Event Attribute Detail window reflects the variables set during the event. In SNMP terminology, these attributes are known as variable bindings or varbinds. These attributes can provide key information about triggers. For example, if a fan fails, the attribute field could indicate the location of the fan in the chassis.

Changing the Alarm State

When an alarm is first reported, it is considered an active alarm. To change the alarm state, to assign the alarm to a person, or simply to record notes about the alarm, use the buttons on Alarm Details. These buttons are:

- Acknowledge—Use this button to acknowledge or record that the alarm is known and is being addressed.
- Clear—Use this button to clear or remove the alarm. The clear state says that the issue sending the alarm has been resolved and no long requires attention.
- Annotate—Use this button to record actions taken to resolve the alarm.
- Assign—Use this button to assign active or acknowledged alarms to staff.

Related Documentation

- Alarms by Category Monitor on page 17
- Alarms by Severity Monitor on page 18
- Alarms by State Monitor on page 18
- Current Active Alarms Monitor on page 19

Alarms by Category Monitor

Alarms by Category is a table of all active alarms sorted by category. Use this monitor to view where errors are trending. These categories are the same categories shown in the Alarm Settings page.

This monitor is available in all views in the main window when in Fault mode.

The table shows the active categories and the number of alarms per category. Clicking the Details icon on Alarms by Category opens Alarm Details where you can sort these categories and change the state of the alarms.

To create a similar report for a specific period of time, use the Alarm Summary report in Report mode.

Related Documentation

- Alarm Detail Monitor on page 13
- Understanding the Fault Mode Tasks Pane on page 6
- *Setting Up User and System Preferences*
- *Alarm Summary Report*

Alarms by Severity Monitor

Alarms by Severity is a pie-chart that shows the breakdown of all alarms since the last system restart. It is available on the main page when in Fault mode.

If you mouse over each segment, the total number of alerts for those alarms is shown. Alarm severity levels are:

- Critical (Red)—A critical condition exists; immediate action is necessary.
- Major (Orange)—A major error has occurred; escalate or notify as necessary.
- Minor (Yellow)—A minor error has occurred; notify or monitor the condition.
- Info (Wedgewood Blue)—An informational message; no action is necessary. Informational alarms do not necessarily indicate an error. It could indicate that a device or entity has changed state.

Clicking the Details icon on Alarms by Severity opens Alarm Details where you can sort and disposition individual.

Related Documentation

- Alarm Detail Monitor on page 13
- Understanding the Fault Mode Tasks Pane on page 6
- *Setting Up User and System Preferences*

Alarms by State Monitor

The Alarms by State monitor is a pie-chart representation of the states of an alarm: active and cleared. Use this graph to get an overall perspective of the amount of alarms that are active compare to those that are cleared. The Alarms by State monitor is on the main pane when in Fault mode.

Mouse over each segment of the pie-chart shows the number of alarms in these states:

- Active—Alarms that are current and not yet cleared.
- Cleared—Alarms that are resolved and the device or entity has returned to normal operation.

You can create an Alarms by State report for a specified node or a period of time using the Alarms Summary Report in Repot mode.

Changing the state of an alarm using Network Director is performed on the Alarm Detail page. Clicking the Details icon on Alarms by State opens Alarm Details where you can sort and set the disposition of the alarms.

Related Documentation

- Alarm Detail Monitor on page 13
- Understanding the Fault Mode Tasks Pane on page 6
- *Setting Up User and System Preferences*

- *Alarm Summary Report*

Current Active Alarms Monitor

The Current Active Alarms monitor shows any active alarm that has not yet been cleared. It is one of the four standard monitors available in Alarm mode. Current Active Alarms is a table that has four fields and appear by default. However, nine fields are available for selection. View Table 8 on page 19 for a description of the table.

Table 8: Current Active Alarms Monitor

Table Column	Description	Shown in Summary by Default	Shown in Detailed View by Default
Name	The alarm name.	Yes	Yes
ID	A system and sequentially-generated identification number.	No	No
Assigned To	If assigned to an individual, it shows the name of the person assigned; otherwise, it shows System to mark that the alarm is still unassigned.	No	Yes
Severity	The severity of the alarm. Severity levels are: • Critical—A critical condition exists; immediate action is necessary. • Major—A major error has occurred; escalate or notify as necessary. • Minor—A minor error has occurred; notify or monitor the condition. • Info—An informational message; no action is necessary.	Yes	Yes
Entity ID	The identification of the entity responsible for causing this alarm. The Entity ID is the key for correlation of events into an alarm. The Entity ID could be a MAC address of a radio or an IP address of the device.	Yes	Yes
Source	The IP address of the device or network element that generated the alarm. The SNMP agent is located at the source IP. In most cases, the source IP is the IP address of the switch or controller.	No	No
Reporting Device	The hostname or IP address of the reporting device.	Yes	Yes
Creation Date	The date and time the alarm was first reported.	No	No
Last Updated	The date and time that the information for the alarm was last modified.	Yes	Yes
Updated By	Either the system or the last user who modified the alarm.	No	No

Clicking the Details icon opens Alarm Details where you can sort and disposition alarms by state (Acknowledged, Clear, Active).

Related Documentation

- Alarm Detail Monitor on page 13
- Understanding Fault Mode in Network Director on page 3