JUNIPER NETWORKS

Junos® Space

Network Director Administration 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 Administration 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

List of Figures

List of Tables

About the Documentation

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 x 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 x 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

CHAPTER 1

Administration Overview

Understanding Network Director User Administration

Network Director uses the user administration features of the Junos Space platform on which it runs. Use Junos Space for tasks such as adding, deleting, and editing user accounts and roles, and changing user passwords. Refer to the Junos Space documentation for information about user administration.

When Network Director is installed, some additional user administration options are available in Junos Space, which are specific to Network Director:

- In addition to the Super Administrator role, the following predefined roles are available for Network Director users:

  Network Director - Admin—Has complete access to all the Network Director modes and user and system preferences.

  Network Director - Engineer—Has access to all modes except Fault and System modes. Has access to only user preferences, not system preferences.

  Network Director - Monitor—Has access to only Monitor and Report modes. Has access to only user preferences, not system preferences.

- You can create custom roles to grant users different access rights to the Network Director modes. Network Director modes—Report, Deploy, Monitor, Fault, and Build are available to assign to custom user roles in the list of application workspaces and associated tasks.

NOTE: The tasks listed under the Network Director modes do not have any effect. Access is controlled at the mode level, so if you grant a role access to a mode, the role has access to all tasks in that mode, regardless of which tasks you select.

If you try to log in to Network Director using an account that does not have access rights to any Network Director modes, you will be redirected to Junos Space instead.

Access to Network Director system preferences is controlled by user access rights. For more information, see "Setting Up User and System Preferences" on page 9.

Related Documentation

- *Understanding the Network Director User Interface*
- Setting Up User and System Preferences on page 9

Understanding the System Tasks Pane

The System Tasks pane provides tasks for viewing audit logs of Network Director user activities, for managing jobs, and for collecting troubleshooting logs.

To access the System Tasks pane, click **System** in the Network Director banner. The tasks are described in Table 3 on page 4.

Table 3: System Tasks

Task	Description
View Audit Logs	View a history of user activities on Network Director, including log in, log out, and task initiation and completion.
Manage Jobs	View all jobs that are scheduled to run or have been run by Network Director. You can cancel jobs that are in progress or scheduled to run in the future.
Collect Jobs for Troubleshooting	Download a zip file containing logs and troubleshooting data from both Network Director and Junos Space.

Related Documentation

- Viewing Audit Logs From Network Director on page 29
- Managing Jobs on page 30
- Collecting Logs for Troubleshooting on page 35

Audit Logs Overview

Audit logs provide a record of login history and user-initiated tasks that are performed from the user interface. From the Audit Logs page, you can monitor user login–logout activity over time, track device management tasks, view services that were provisioned on devices, and so forth. Audit logging does not record non-user initiated activities, such as device-driven activities, and is not designed for debugging purposes.

Administrators can sort and filter on audit logs to determine which users performed what actions on what objects at what time. For example, an administrator can use audit log filtering to track the user accounts that were added on a specific date, track configuration changes across a particular type of device, view services that were provisioned on specific devices, or monitor user login–logout activity over time.

Over time, Network Director will archive a large volume of log entries. Such log entries might or might not be reviewed, but they must be retained for a period of time.

The audit logs can be saved to a local server (the server that functions as the active node for Network Director) or a remote network host or media.

Related Documentation

- Viewing Audit Logs From Network Director on page 29

PART 2

Configuration

CHAPTER 2

Preferences

Setting Up User and System Preferences

Depending on your system authority, Preferences page can either display user settings or a combination of user settings and system settings. One or more of these preference tabs appear when you open the Preferences page:

- User–All users can choose whether monitors and reports display local time or server time.
- Report–Network Administrators can specifying length of time Network Director reports are retained.
- General–Network Administrators can specifying a RingMaster URL.
- Monitoring–Network Administrators can change the polling interval for data collection for Monitor mode monitors. This page enables the internal processes used for data collection to be enabled or disabled. You can also specify database record retention periods on this tab.
- Fault–Network Administrators can enable or disable alarms. They can also set the retention period for alarms and the number of events per alarm.

This topic describes:

Accessing the Preferences page

To open the Preferences page, click the down arrow next to the System button in the Network Director banner and select **Preferences** as shown in Figure 1 on page 10.

Figure 1: Accessing the Preferences Page

The Preferences page opens with User Preferences as the default tab.

Choosing Server Time or Local Time

All users can specify whether Network Director displays local time or the server's time in monitors and reports on the User Preferences tab. The default setting is to display local time. To change the setting to display the server's time:

1. In the Preferences page, select **Use Server Time** from the list.
2. Click **OK** to save your changes or click **Cancel** to close Preferences.

Specifying Search Preferences

Network Director indexes the device inventory data periodically to enable users to perform efficient searches. You can specify a time interval after which Network Director initiates the next indexing on the Search tab. You can also specify to stop indexing while devices are imported into Network Director. If you are running short of system memory, selecting this option can help save some memory and speed up the discovery and import of new devices. By default this option is selected and the search index update interval is set to 900 seconds.

Retaining Network Director Reports

By default, Network Director keeps reports for 30 days. However, Network Administrators can change the retention period from 0 to 365 days. To change the setting, move the slider right or left on the Report tab of Preferences to the new setting. Click **OK** to save the setting.

Linking to RingMaster

Sites with RingMaster licenses can launch the RingMaster application from within Network Director by supplying the RingMaster URL. After typing the URL on the General Settings tab of Preferences, you can click Launch RingMaster in Build mode to load RingMaster into the main page. To enable launching RingMaster from within Network Director, simply type in the URL and click **OK** to save the setting.

Changing Monitor Mode Settings

The Monitoring tab of Preferences consists of two sub-tabs:

- The Monitor Settings sub-tab enable you to change the default polling interval for data collection for Monitor mode monitors. You can also disable or re-enable the internal processes used for data collection on this sub-tab.
- The Client Session History sub-tab enables you to set the retention period for history records and the frequency that these records are checked for deletion.

This section describes:

Disabling Data Collection for Monitors

Network Director internally gathers data for monitors by using a set of data collector processes. You can disable these data collectors if they do not pertain to your installation. For example, if you do not use Virtual Chassis, you can disable the data collection processes used for Virtual Chassis.

The data collector processes are divided into the following categories:

- Client
- Equipment
- RF
- Traffic

One data collector can be used by multiple monitors. Likewise, some monitors can be supported by multiple data collectors. These data collectors are enabled by default. To ensure proper data collection, if Equipment data collectors are enabled, ensure the Traffic collector is also enabled.

To disable or re-enable a data collector:

1. Determine which monitors are used by the data collectors. Use Table 4 on page 11 to determine the relationship between the data collectors and the monitors.

Table 4: Monitor Mapping for Data Collectors

Monitor	Data Collector	Category
802.11 Packet Error	RFMonitorRadioStatsCollector	RF
AP Interference Source	RFMonitorIntSourcesCollector	RF
AP Status	EquipmentMonitorAPCollector	Equipment
Current Sessions	Client Monitor Collector and SessionCountCollector	Client
Error Trend	PortTrafficMonitorCollector	Traffic
Logical Interfaces	EquipmentMonitorLogicalInterfaceStatusCollector	Equipment
Find End Point	EquipmentMonitorEndPointCollector	Equipment
Percentage of Packets Retransmitted	RFMonitorRadioStatsCollector	RF
Port Status (physical)	EquipmentMonitorControllerCollector	Equipment

Table 4: Monitor Mapping for Data Collectors *(continued)*

Monitor	Data Collector	Category
Radio Status	EquipmentMonitorAPCollector	Equipment
RF Neighborhood	RFMonitorRadioNeighborCollector	RF
RF Throughput or Packet Retransmitted	RFMonitorRadioStatsCollector	RF
Resource Utilization	EquipmentMonitorControllerCollector	Equipment
Session Trend	ClientMonitorCollector and SessionCountCollector	Client
Switch Status	EquipmentMonitorControllerCollector	Equipment
Traffic Trend	PortTrafficMonitorCollector	Traffic
Top Sessions by MAC Address	ClientMonitorCollector	Client
Top Users	ClientMonitorCollector	Client
Unicast vs Broadcast/Multicast	PortTrafficMonitorCollector	Traffic
Unicast vs Broadcast/Multicast Trend	PortTrafficMonitorCollector	Traffic
Virtual Chassis Topology	EquipmentMonitorVCStatsCollector and EquipmentMonitorVCCollector	Equipment
Virtual Chassis Protocol	EquipmentMonitorVCStatsCollector and EquipmentMonitorVCCollector	Equipment
Virtual Chassis Statistics	EquipmentMonitorVCStatsCollector and EquipmentMonitorVCCollector	Equipment

2. Clear the check box to disable the collector or select to enable the collector.
3. Click **Save** and **Close** to save the configuration and to close the window.

Changing the Polling Interval

The frequency that data is collected is determined by the polling interval. Table 5 on page 12 shows the default polling intervals vary by data collector.

Table 5: Default Polling Intervals

Collector	Polling Interval
ClientMonitorCollector	10 minutes
SessionCountCollector	10 minutes

Table 5: Default Polling Intervals *(continued)*

Collector	Polling Interval
EquipmentMonitorVCCollector	30 minutes
EquipmentMonitorVCStatsCollector	30 minutes
EquipmentMonitorLogicalInterfaceStatusCollector	30 minutes
EquipmentMonitorControllerCollector	10 minutes
EquipmentMonitorAPCollector	10 minutes
EquipmentMonitorEndPointCollector	1440 minutes
RFMonitorIntSourcesCollector	15 minutes
RFMonitorRadioNeighborCollector	15 minutes
RFMonitorStatsCollector	10 minutes
PortTrafficMonitorCollector	10 minutes

You can change the interval by:

1. Selecting the polling interval for a data collector in the Monitor Settings table.
2. Typing the new interval level in whole minutes. For example, do not specify 1.5 minutes. Recommended intervals are 5, 10, or 20 minutes.
3. Clicking **OK** and **Yes** to verify the change to the configuration.

Specifying Database History Retention

To keep the database manageable, the system periodically checks the age of the records and retires those that have past an expiration date. By default, Network Director ages database records off at 90 days and runs a database cleanup every 6 hours.

Use the Client Session History sub-tab to change the default values:

1. Select from the lists new values.
   - Age of history records (in days) from 1 to 365 days.
   - Cleanup job frequency (in hours) from 1 through 24 hours.
2. Click **OK** to save the changes.

Changing Alarm Settings

Use Alarm Settings to enable individual alarms, set the retention period for alarms, and to specify the number of events to keep for each alarm. The Alarm Setup tab of Preferences has two sub-tabs:

- Alarms Settings, for enabling alarms and changing the severity setting for the alarm. All of the alarms on this page are preconfigured and enabled by default.
- Retention, for setting the retention period for alarms and for specifying the number of events to keep for each alarm.

This section describes:

- Changing the Severity of Individual Alarms on page 14
- Enabling Alarms on page 14
- Retaining Alarm History on page 25
- Specifying Event History on page 25

Changing the Severity of Individual Alarms

You can change the severity of the alarms to match your corporate procedures and guidelines. For example, at your company a DoS attack might be considered a critical alarm, but Network Director has a default severity for DoS attacks as a major alarm.

To change the severity of an alarm:

1. Select the **Severity** in the specific alarm entry on the Alarm Setup page. A list of the severity levels appear.
2. Select the new severity level for the alarm.
3. Click **OK** and **Yes** to confirm the change to the severity setting.

Enabling Alarms

Ensure all devices are configured to send traps to Network Director. This task is performed for the devices in Deploy mode through Set SNMP Trap Configuration.

Use the Alarm Setup tab on the Alarm Settings page to disable and re-enable individual alarms or all alarms. Fault alarms are preconfigured and initially enabled. To enable or disable alarms:

1. (Optional) Sort the alarms. By default, the list of alarms is sorted alphabetically within each category. You can also sort by description or alarm severity within a category by clicking a column heading.
2. Review the alarms and either select the check box in the heading to select all of the alarms or select the check box for the individual alarms you want to enable. For a full description of each of the alarms, view Table 6 on page 15.
3. Click **OK** and **Yes** to verify the alarm change.

Table 6: Alarm Descriptions

Alarm Name	Description	Device Type
AP and Radio (APAndRadio)		
AP License Limit Exceeded	Generated when the number of wireless LAN access points (WLAs) exceed the number of licenses configured on a wireless switch. The trap occurs when a wireless switch receives a packet from an inactive access point. The switch is unable to attach the access point without exceeding the maximum (licensed) number of active access points.	Wireless LAN controller
AP Manager Changed Alarm	Generated when the access point's secondary link becomes the primary link.	Wireless LAN controller
AP Status Alarm	Generated when an access point changes state.	Wireless LAN controller
AP Tunnel Limit Exceeded	Generated when the number of tunnels per access point are exceeded. This alarm is generated by the access point's Primary Access Manager (PAM) when the access point rejects a tunnel creation request because it has already created the maximum number of tunnels it can support.	Wireless LAN controller
M2U Conversion	Generated when multicast to unicast conversion is enabled on the access point, but cannot be performed.	Wireless LAN controllers
Radio Channel Changed	Generated when autotune changes a radio's channel.	Wireless LAN controller
Radio power changed	Generated when autotune changes a radio's power level.	Wireless LAN controller
Radio Status Alarm	Generated when a radio changes state. It also contains aggregate information about the access point in operational state, its security level and service availability.	Wireless LAN controller
WLC Tunnel Limit Exceeded	Generated when the wireless switch rejects a tunnel creation request because it has reached the maximum number of tunnels supported. When the trap event trpzWsTunnelLimitType equals the platform-tunnel-limit, the wireless switch has reached the maximum tunnel capacity. The actual tunnel limit varies by platform. When the trap trpzWsTunnelLimitType equals ap-ws-tunnel-limit, the wireless switch has reached the access point-to-switch tunnel's limit. The value of that limit depends on the current situation of the wireless switch (mobility domain, network domain, network resiliency status).	Wireless LAN controller

Table 6: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
BFD		
BfdSessionDetectionTimeAlarm	Generated when the threshold value for detection time is set and the BFD session detection-time adapts to a value greater than the threshold.	EX Series Switch
BfdSessionTxAlarm	Generated when the threshold value for transmit interval (in microseconds) is exceeded.	EX Series Switch
BGP		
BgpM2BackwardTransitionAlarm	Generated when the BGP FSM moves from a higher-numbered state to a lower-numbered state.	EX Series Switch
BgpM2EstablishedAlarm	Generated when the BGP Finite State Machine (FSM) enters the ESTABLISHED state.	EX Series Switch
Chassis		
FanFailureAlarm	Generated when the specified cooling fan or impeller has failed (not spinning).	EX Series Switch
FEBSwitchoverAlarm	Generated when the Forwarding Engine Board (FEB) has switched over.	EX Series Switch
FRUCheckAlarm	Generated when the device has detected that a Field Replaceable Unit (FRU), has some operational errors and has gone into check state.	EX Series Switch
FRUFailedAlarm	Generated when a FRU has failed.	EX Series Switch
FRUInsertionAlarm	Generated when the system detects that the specified FRU is inserted into the chassis.	EX Series Switch
FRUOfflineAlarm	Generated when the specified FRU goes offline.	EX Series Switch
FRUOnlineAlarm	Generated when the specified FRU goes online.	EX Series Switch
FRUPowerOffAlarm	Generated when the specified FRU is powered off.	EX Series Switch
FRUPowerOnAlarm	Generated when the specified FRU is powered on.	EX Series Switch
FRURemovalAlarm	Generated when the system detects that the specified FRU was removed from the chassis.	EX Series Switch
HardDiskFailedAlarm	Generated when the hard disk for the specified routing engine has failed.	EX Series Switch

Table 6: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
HardDiskMissingAlarm	Generated when the hard disk in the specified routing engine is missing from the boot device list.	EX Series Switch
PowerSupplyFailureAlarm	Generated when the specified power supply has failed (bad DC output).	EX Series Switch
RedundancySwitchOverAlarm	Generated when a Graceful Routing Engine Switchover (GRES) occurs on a switch with dual Routing Engines or on a Virtual Chassis.	EX Series Switch
TemperatureAlarm	Generated when the device has over heated.	EX Series Switch
Client and User Session (ClientAndUserSession)		
Client Association Failure	Generated when a client is unable to associate with an access point.	Wireless LAN controller
Client Authentication Failure	Generated when a client is unable to authenticate.	Wireless LAN controller
Client Authorization Failure	Generated when a client fails authorization.	Wireless LAN controller
Client Authorization Succeeded	Generated when a client authorizes.	Wireless LAN controller
Client Cleared	Generated when a client session is cleared.	Wireless LAN controller
Client Connectivity	Generated when a client session connects.	Wireless LAN controller
Client DeAssociated	Generated when a client de-association occurs.	Wireless LAN controller
Client DeAuthenticated	Generated when a client de-authenticates.	Wireless LAN controller
Client Disconnected	Generated when a client session disconnects administratively.	Wireless LAN controller
Client dot1x Failure	Generated when a client fails 802.1X.	Wireless LAN controller
Client Dynamic Authorization Changed	Generated when the authorization attributes for a user are dynamically changed by a authorized dynamic authorization client.	Wireless LAN controller

Table 6: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
Client IP Address Changed	Generated when a client's IP address changes, normally when the client first connects to the network.	Wireless LAN controller
Client Roamed	Generated when a client roams from one location to another.	Wireless LAN controller
Dynamic Authorization Client Alarm	Generated when the authorization attributes for a user are dynamically changed by an authorized dynamic authorization client.	Wireless LAN controller
ClusterAndMoDo		
Cluster Sync Failure	Generated when the cluster configuration failed to apply.	Wireless LAN controller
Mobility Domain Failback	Generated when the mobility domain fails back to the primary seed.	Wireless LAN controller
Mobility Domain Failover	Generated when the mobility domain fails back to the secondary seed.	Wireless LAN controller
Mobility Domain Join	Generated when a member joins the mobility domain.	Wireless LAN controller
Mobility Domain Resiliency Status	Generated when a mobility domain seed changes resilient capacity.	Wireless LAN controller
Mobility Domain Timeout	Generated when a mobility domain member times out.	Wireless LAN controller
Configuration (Config)		
CmCfgChangeAlarm	Generated when the jnxCMCfgChgEventTable records a configuration management event.	EX Series Switch and wireless LAN controller
CMRescueChangeAlarm	Generated when a change is made to the rescue configuration.	EX Series Switch and wireless LAN controller
Core and controllers (CoreAndControllers)		
Device alarm	Generated when the device status changes (up to down or down to up).	EX Series Switch and wireless LAN controller
CoS		

Table 6: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
CoSAlmostOutOfDedicatedQueuesAlarm	Generated when only 10% of CoS queues are available.	EX Series Switch
CoSOutOfDedicatedQueuesAlarm	Generated when there are no more available dedicated CoS queues.	EX Series Switch
DHCP		
JdhcpLocalServerDupClientAlarm	Generated when a DHCP client is detected changing interfaces.	EX Series Switch
JdhcpLocalServerIfLimitExceededAlarm	Generated when the client limit is reached on an interface.	EX Series Switch
Jdhcpv6LocalServerLimitExceededAlarm	Generated when the client limit is reached on an interface for DHCPv6.	EX Series Switch
DOM		
DomAlertSetAlarm	Generated when an interface detects Digital Optical Monitor (DOM) alarm conditions.	EX Series Switch
Flow Collection (FlowCollection)		
CollFlowOverloadAlarm	Generated when a collector PIC detects a hard or soft flow overload.	EX Series Switch
CollFtpSwitchOverAlarm	Generated when an FTP server switchover occurs.	EX Series Switch
CollMemoryUnavailableAlarm	Generated when a PIC is out of memory or the memory is unavailable.	EX Series Switch
CollUnavailableDestAlarm	Generated when a file transfer destination is unavailable.	EX Series Switch
CollUnsuccessfulTransferAlarm	Generated when a collector file is unable to transfer because the destination is unavailable.	EX Series Switch
General		
Authentication Failure Alarm	Generated when a protocol message is received that is not properly authenticated.	EX Series Switch and wireless LAN controller
Cold Start Alarm	Generated when a device is re-initializing and its configuration might have changed.	EX Series Switch and wireless LAN controller

Table 6: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
Link Down Alarm	Generated when a link is down. The trap is generated when the ifOperStatus object for a communication link is about to enter the down state from another state other than notPresent. This other state is indicated by the included value of ifOperStatus.	EX Series Switch and wireless LAN controller
Link Up Alarm	Generated when a link comes up that was previously in the down state. The trap is generated when the ifOperStatus object for a communication link left the down state and transitioned into another state other than notPresent state. This other state is indicated by the included value of ifOperStatus.	EX Series Switch and wireless LAN controller
Warm Start Alarm	Generated when a device is re-initializing and its configuration has not changed.	EX Series Switch and wireless LAN controller
Generic (GenericEvent)		
GenericEventTrapAlarm	Generated by an Op script or event policies. This notification can include one or more attribute-value pairs. The pairs are identified by the jnxEventAvAttribute and jnxEventAvValue objects.	EX Series Switch
L2ALD		
L2aldGlobalMacLimitAlarm	Generated when the MAC limit is reached for the entire system. This trap is sent only once, when the limit is reached.	EX Series Switch
L2aldInterfaceMacLimitAlarm	Generated when the given interface reaches the MAC limit (jnxl2aldInterfaceMacLimit).	EX Series Switch
L2aldRoutingInstMacLimitAlarm	Generated when the MAC limit is reached for a given routing instance (jnxl2aldRoutingInst).	EX Series Switch
L2CP		
LacpTimeOutAlarm	Generated when LACP has timed out.	EX Series Switch
PortBpduErrorStatusChangeTrapAlarm	Generated when the port's BPDU error state (no-error or detected) changes.	EX Series Switch
PortLoopProtectStateChangeTrapAlarm	Generated when the port's loop-protect state (no-error or loop-prevented) changes.	EX Series Switch
PortRootProtectStateChangeTrapAlarm	Generated when the port's root-protect state (no-error or root-prevented) changes.	EX Series Switch

Table 6: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
MAC Forwarding Database (MACFDB)		
MacChangedNotificationAlarm	Generated when MAC addresses of the monitored devices are learned or removed from the forwarding database (FDB).	EX Series Switch and wireless LAN controller
Misc.		
Counter Measures Alarm	Generated when counter measures are started against a rogue.	Wireless LAN controller
Device Configuration Saved	Generated when the running configuration of the switch is written to the configuration file.	Wireless LAN controller
Multimedia Call Failure	Generated when a multimedia call fails.	Wireless LAN controller
PoE failure	Generated when Power over Ethernet (PoE) has failed on the indicated port.	EX Series Switch
Passive Monitoring (PassiveMonitoring)		
PMonOverloadSetAlarm	Generated when an overload condition is detected on a Passive Monitoring Interface.	EX Series Switch
Ping		
PingEgressJitterThresholdExceededAlarm	Generated when egress time jitter (jnxPingMaxEgressUs minus jnxPingResultsMinEgressUs) exceeds the configured threshold (jnxPingCtlEgressJitterThreshold) causing the egressJitterThreshold bit to be set.	EX Series Switch and wireless LAN controller
PingEgressStdDevThresholdExceededAlarm	Generated when the standard deviation of the egress time (jnxPingResultsStddevEgressUs) exceeds the configured threshold (jnxPingCtlEgressTimeThreshold) and the causes the egress bit to be set.	EX Series Switch and wireless LAN controller
PingEgressThresholdExceededAlarm	Generated when the egress time (jnxPingResultsStdevEgressUs) exceeds the configured threshold (jnxPingCtlEgressTimeThreshold) and the egress threshold bit is set in jnxPingCtlTrapGeneration.	EX Series Switch and wireless LAN controller

Table 6: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
PingIngressJitterThresholdExceededAlarm	Generated when ingress time jitter (jnxPingResultsMaxIngressUs minus jnxPingResultsMinIngressUs) exceeds the configured threshold (jnxPingCtlIngressJitterThreshold) and the ingressJitterThreshold bit is set in jnxPingCtlTrapGeneration.	EX Series Switch and wireless LAN controller
PingIngressStddevThresholdExceededAlarm	Generated when the standard deviation of the ingress time (jnxPingResultsStdDevIngressUs) exceeds the configured threshold (jnxPingCtlIngressStddevThreshold) and the ingress StdDevThreshold bit is set in jnxPingCtlTrapGeneration.	EX Series Switch and wireless LAN controller
PingIngressThresholdExceededAlarm	Generated when the ingress time jitter (jnxPingResultsIngressUs) exceeds the configured threshold (jnxPingCtlIngressTimeThreshold) and the ingress threshold bit (jnxPingIngressThresholdExceeded) is set in jnxPingCtlTrapGeneration.	EX Series Switch and wireless LAN controller
PingRttJitterThresholdExceededAlarm	Generated when the round trip time jitter (jnxPingResultsMaxRttUs minus jnxPingResultsMinRttUs) exceeds the configured threshold (jnxPingCtlRttJitterThreshold) and the rttJitterThreshold bit is set in jnxPingCtlTrapGeneration.	EX Series Switch and wireless LAN controller
PingRttStdDevThresholdExceededAlarm	Generated when the standard deviation of the round trip time (jnxPingResultsStdDevRttUs) exceeds the configured threshold (jnxPingCtlRTTStdDev) and the rttStdDevThreshold bit is set in jnxPingCtlTrapGeneration.	EX Series Switch and wireless LAN controller
PingRttThresholdExceededAlarm	Generated when the round trip time (jnxPingCtlRttThreshold) exceeds the configured threshold (jnxPingCtlRttThreshold) and the rttThreshold bit is set in jnxPingCtlTrapGeneration.	EX Series Switch and wireless LAN controller
RF Detect (RFDETECT)		
Adhoc user detected	Generated when RF detection sweep finds an ad hoc user or if previously found ad hoc user disappears.	Wireless LAN controller
Client Blacklisted	Generated when an association, re-association, or de-association request is detected from a blacklisted transmitter.	Wireless LAN controller
DoS Attack Detected	Generated when RF detection finds a denial of service (DoS) occurring.	Wireless LAN controller

Table 6: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
DoS Port Detected	Generated when RF detection finds a denial of service (DoS) occurring. This trap collects port and access point information instead of information about the listener.	Wireless LAN controller
RF Interference Detected	Generated when a new noise source appears. A given combination of noise source ID, listener, and channel triggers this trap. It is normally not triggered more than once every 15 minutes.	Wireless LAN controller
RF Detect Classification Changed	Generated when the RF detection classification rules change.	Wireless LAN controller
Rogue Device Detected	Generated when RF detection finds a rogue device.	Wireless LAN controller
Rogue Wired WLA Client Detected	Generated when a client is detected that connected through a rogue access point that is attached to a wired port.	Wireless LAN controller
Rogue WLA Client Detected	Generated when RF detection finds a suspect device.	Wireless LAN controller
Rogue WLA Interference Detected	Generated when RF detection finds an interfering rogue access point.	Wireless LAN controller
Spoofed MAC Detected	Generated when RF detection finds an access point using the MAC of the listener.	Wireless LAN controller
Spoofed SSID Detected	Generated when RF detection finds an access point using the SSID of the listener, and the access point is not in the mobility domain.	Wireless LAN controller
Suspected Device Detected	Generated when RF detection finds a suspect device.	Wireless LAN controller
Unauthorized AP Detected	Generated when RF detection discovers an unauthorized access point being used.	Wireless LAN controller
Unauthorized OUI Detected	Generated when RF detection finds an unauthorized OUI being used.	Wireless LAN controller
Unauthorized SSID Detected	Generated when RF detection finds an unauthorized SSID being used.	Wireless LAN controller
RMON		
RmonAlarmGetFailureAlarm	Generated when a GET request for an alarm variable returns an error. The specific error is identified by a varbind in jnxRmonAlarmGetFailReason.	EX Series Switch

Table 6: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
SONET		
SonetAlarmSetAlarm	Generated when there is a notification of a recently set SONET or SDH alarm on an interface.	EX Series Switch
SONET APS (SONETAPS)		
APSEventChannelMismatchAlarm	Generated when the value of an instance of apsStatusChannelMismatches increments.	EX Series Switch
APSEventFEPLFAlarm	Generated when the value of an instance of apsEventFEPLFs increments.	EX Series Switch
APSEventModeMismatchAlarm	Generated when the value of an instance of apsEventModeMismatch increments.	EX Series Switch
APSEventPSBFAlarm	Generated when the value of an instance of apsStatusPSBFs increments.	EX Series Switch
APSEventSwitchoverAlarm	Generated when the value of an instance of apChanStatusSwitchover increments.	EX Series Switch
Virtual Chassis (VirtualChassis)		
VccpMemberDownAlarm	Generated when a member is about to enter the down state.	EX Series Switch
VccpMemberUpAlarm	Generated when a member has completed transition from the down state to another state.	EX Series Switch
VccpPortDownAlarm	Generated when one of the member's communication links is about to enter the down state.	EX Series Switch
VccpPortUpAlarm	Generated when one of the member's communication links has completed transition from the down state to another state.	EX Series Switch
VNetwork		
HostConnectivityLostAlarm	Generated when all the uplink ports of a virtual switch residing in a host loses network connectivity.	Host
HostNetworkRedundancyLostAlarm	Generated when some uplink ports of a virtual switch residing in a host loses network connectivity. It indicates that there are one or more ports that still has network connectivity.	Host

Table 6: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
VNetworkConnectivityLostAlarm	Generated when Network Director loses network connectivity with the vCenter server.	Virtual Network

Retaining Alarm History

Use the Retention tab on the Alarm Settings page to specify the number of days to keep alarm history. The default retention time is 120 days; but you can specify a period of 7 through 1000 days. Specifying a longer retention time consumes more database resources. To change the alarm retention duration, type a new value and click **OK** and **Yes** to verify the change.

Specifying Event History

The Events per Alarm field enables you specify the number of event entries that are kept in the alarm history. This field is found on the Retention tab on the Alarm Settings page. The default setting for events is 20. To change the setting, type a new value and click **OK** and **Yes** to verify the change.

Related Documentation

- *Understanding the Network Director User Interface*
- *Enabling SNMP Categories and Setting Trap Destinations*
- *Understanding Fault Mode in Network Director*

PART 3

Administration

CHAPTER 3

Audit Logs and Jobs

Viewing Audit Logs From Network Director

Audit logs are generated for login activity and tasks that are initiated from the Network Director application. The Audit Logs page displays the logs for all user-initiated activities.

You can do the following on the Audit Logs page:

- Sort, filter, and search the log entries using the standard table manipulation features in Network Director.
- Obtain more information about a log entry by double-clicking the entry or by selecting the entry and clicking **Show Details**. The Audit Log Details window is displayed.
- For a user-initiated task that runs as a job, you can obtain more information about the job by clicking the job ID in the Job ID column.

To display the Audit Logs page:

1. Click **System** in the Network Director banner.
2. Select **View Audit Logs** from the Tasks pane.

   The Audit Logs page is displayed with the fields listed in Table 7 on page 29.

Table 7: Audit Logs Page Fields

Field	Description
User Name	The login ID of the user that initiated the task
User IP	The IP address of the client computer from which the user initiated the task
Task	The name of the task that triggered the audit log
Time	The data and time when the user initiated the task

Table 7: Audit Logs Page Fields *(continued)*

Field	Description
Result	The execution result of the task that triggered the audit log: • Success—Job completed successfully • Failure—Job failed and was terminated • Job Scheduled—Job is scheduled but has not yet started
Description	A description of the audit log
Job ID	The job ID for any task that runs as a job

Related Documentation

- Audit Logs Overview on page 4
- Managing Jobs on page 30

Managing Jobs

Network Director allows you to view and manage jobs. You can view the status of completed jobs and cancel the jobs that are scheduled to execute at a later time or jobs that are in progress.

The Job Management page, accessible as a System task, allows you to view and manage all jobs. In addition, Network Director enables you to view special pre-filtered versions of this page from various other tasks, such as View Discovery Status or View Image Deployment Jobs. These pages contain the same fields (although some fields might be hidden) and have the same functionality as the Job Management page, but they list only those jobs relevant to particular tasks.

To display the Job Management page:

1. Click **System** on the Network Director banner.
2. Select **Manage Jobs** from the Tasks pane. The Job Management page appears.
3. To view the details of a job, select a row and click **Show Details** or double-click on a row.
4. To cancel a scheduled job, select a job that is scheduled for a later time or a job that is in progress and click **Cancel**.

The fields in the Job Management page are described in Table 8 on page 30. To view any hidden column, keep the mouse on any column heading and select the down arrow and then click Columns. Select the check box to display the hidden columns.

Table 8: Job Management Page Fields

Field	Description
Job ID	The unique ID assigned to the job

Table 8: Job Management Page Fields *(continued)*

Field	Description
Name	The name of the job
Percent	The percentage of completion of the job
State	The status of the job: • Success—Job completed successfully • Failure—Job failed and was terminated • Job Scheduled—Job is scheduled but has not yet started • In progress—Job is has started, but not completed • Cancelled—Job is cancelled
Job Type	The type of the job
Summary	Summary of the job scheduled and executed with status
Scheduled Start Time	The time when the job is scheduled to start
Actual Start Time	The actual time when the job started
End Time	The time when the job was completed
User	The login ID of the user that initiated the task
Recurrence	The recurrent time when the job will be restarted.

Related Documentation

- Audit Logs Overview on page 4
- Viewing Audit Logs From Network Director on page 29

PART 4

Troubleshooting

CHAPTER 4

Collecting Logs

Collecting Logs for Troubleshooting

Network Director enables you to collect logs and other data from both Network Director and Junos Space that can assist in managing and monitoring Network Director servers.

Network Director collects the logs and troubleshooting data into a compressed file that you can download. This file is named **troubleshoot_yyyy-mm-dd_hh-mm-ss.zip**—for example, **troubleshoot_2012-12-21_11-25-12.zip**. The date and time in the file name is the server Coordinated Universal Time (UTC) date and time.

To retrieve troubleshooting data and log files, follow these steps:

1. Click **System** on the Network Director banner.
2. From the Tasks pane, click **Collect Logs for Troubleshooting**. The Collect Logs for Troubleshooting page appears.
3. Click the **Download troubleshooting data and logs from Network Director and Junos Space** link.

   Network Director begins collecting the logs and data. It can take a few minutes for Network Director to collect the information and create the zip file.
4. When the standard file download window for your browser opens, save the **troubleshoot_yyyy-mm-dd_hh-mm-ss.zip** file.
5. When you contact the Juniper Technical Assistance Center, describe the problem you encountered and provide the JTAC representative with the **troubleshoot.zip** file.

   Table 9 on page 35 lists the files included in the **troubleshoot_yyyy-mm-dd_hh-mm-ss.zip** file.

Table 9: Log Files in troubleshooting.zip File

Description	Location
Jboss log files	**/var/log/jboss/**
MSS OS adapter log files	**/home/jmp/mssosadpater/var/errorLog/**

Table 9: Log Files in troubleshooting.zip File *(continued)*

Description	Location
Daemon log files	**/opt/opennms/logs/daemon/**
Platform log files	**/var/log/platform**
Access Log Files	**/var/log/httpd**
Log files for Apache, NMA, Webproxy	**/var/log/httpd/**
Watchdog log file	**/var/log/**

Related Documentation

- Managing Jobs on page 30
- Audit Logs Overview on page 4
- Viewing Audit Logs From Network Director on page 29