Junos Space Network Director

Getting Started With Junos® Space Network Director

Release
3.0

Modified: 2016-12-18

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos Space Introduction to Junos Space Network Director

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

Introduction

Juniper Networks Junos Space Network Director provides a smart, comprehensive, and automated network management solution that enables network and cloud administrators to visualize, build, deploy, analyze, and control their entire enterprise network—data center and campus networks, physical and virtual infrastructure, virtual overlay networks, and wired and wireless networks—through a single pane of glass.

In data center networks, Network Director helps administrators manage, visualize, and troubleshoot physical and virtual environments by providing them correlated visibility between the overlay and the physical network. Network Director also provides flow analysis, visualization, and synchronization of network policies as Virtual Machines (VMs) move from one server to another.

In campus networks, Network Director automates routine management tasks such as network provisioning and troubleshooting, which substantially improves operational efficiency and reliability.

Getting Started with Junos Space Network Director describes a series of steps that you must perform after installing Network Director to be able to manage and troubleshoot your network more efficiently.

Each release of Network Director includes a new set of customer-focused features and enhancements to existing features. To know more about the features that are available with each release of Network Director, use the Juniper Networks Feature Explorer.

Related Documentation

- Junos Space Network Director Documentation
- Juniper Networks Feature Explorer
- Junos Space Network Director Data Sheet

Build Your Network

The first step after you install and log in to Network Director is to build your network. Even with large networks, Network Director has made this step relatively easy and straightforward. The steps that you need to perform depend on whether your network contains legacy devices, or new devices, or a combination of both.

You add legacy devices, which already have some configurations, to Network Director by using a process called *device discovery*. Once such a device is successfully discovered, Network Director reads the device configurations and replicates these configurations in the form of profiles in Network Director. You can use device discovery to add Juniper Networks switches and Wireless LAN Controllers (WLCs) to Network Director. For more details, see "Brownfield Deployment in Network Director" on page 4.

With new devices or devices that are set to factory-default configuration, you can use the *zero touch provisioning (ZTP)* feature to provision the device. ZTP enables you to auto-discover, auto-upgrade, and load the requisite default configuration on Juniper Networks switches in your network automatically—without manual intervention. When

you physically connect a switch that has the factory-default configuration to a network and boot the switch, the switch attempts to upgrade Junos OS automatically and autoinstall a configuration file from the network.

Discovering Devices

The first step to manage your existing network devices using Network Director is to discover these devices from Network Director. You can discover devices from Network Director using an easy-to-use wizard-based workflow.

To discover devices in Network Director:

1. Log in to Network Director.

   Network Director user interface opens with Dashboard View selected.

2. Select **Logical View** from the View selector in the Network Director banner to open the Logical View.

3. Click **Discover Devices** from the Device Discovery menu in the Tasks pane.

   The Discovery Devices wizard opens.

4. Do one of the following:

   - Click **Add** in the Device Targets window. You can add a single device IP address, a range of IP addresses, an IP subnet, or a hostname.
   - To add devices in bulk, click **Import from CSV** and select a CSV file that has details about the devices that you want to add to Network Director. You can download a sample CSV to understand the format of the CSV file by clicking **CSV Sample**.

5. Click **Next** and then click **Add** in the Device Credentials table to add the device credentials.

6. Specify the device administrator username and password for the device that you want to discover, and confirm the password. The username and password must match the name and password configured on the device that is to be discovered.

7. Click **Add** to save the username and password that you specified or click **Add More** to add another username and password. Click **Add** after you have finished adding all login credentials. The Device Credentials table displays the usernames that you configured.

8. In the Specify Probes section, select both the **Use Ping** and the **Use SNMP** check boxes to enable Network Director for faster discovery of the target devices, provided the device is pingable and also SNMP is enabled on the device. Specify the SNMP settings and click **Next**.

9. Do one of the following:

   - Click **Run Now** to discover the devices immediately.
   - Use the scheduling option if you want the discovery job to be run at a later time.

Click **Next** to review the discovery options.

10. Click **Finish**. If you chose to discover the devices immediately, Network Director starts the discovery process.
    A message window opens, displaying the status of the device discovery job name and job ID. Click **OK**.
    The Device Discovery Jobs page opens, displaying a list of scheduled jobs.

Adding Devices Using Zero Touch Provisioning

Zero touch provisioning (ZTP) simplifies the deployment of networks without requiring user intervention, providing policy-driven plug-and-play provisioning and network bring-up operations for both fabrics and individual devices.

To add devices using ZTP, follow the steps mentioned here or watch this video-based tutorial:

Video: Zero Touch Provisioning using Network Director

Before you begin:

Ensure that the switch has access to the following network resources:

- The DHCP server that provides the location of the software image and configuration files on the network

  See your DHCP server documentation for configuration instructions.

- The anonymous FTP server, the HTTP server, or the Trivial File Transfer Protocol (TFTP) server on which the software image and configuration files are stored. If you are using an FTP server, ensure that the FTP server is configured to enable anonymous access. Refer to your FTP server documentation to know more about this.

NOTE: **Although TFTP is supported, we recommend that you use FTP or HTTP, because these transport protocols are more reliable.**

- (Optional) A Network Time Protocol (NTP) server to perform time synchronization on the network.
- (Optional) A system log (syslog) server to manage system log messages and alerts.

Identify the type of DHCP server that you will use for zero touch provisioning:

- CentOS DHCP Server—If your DHCP server uses the following command to restart the server, then select **CentOS** as the DHCP server type:

  ```
  service dhcpd restart
  ```

- Ubuntu DHCP Server—If your DHCP server uses the following command to restart the server, then select **Ubuntu** as the DHCP server type:

  ```
  service isc-dhcp-server restart
  ```

- Other—If your server is not an ISC DHCP server running on Linux operating system, then you must select **Other** and configure the DHCP server manually.

To configure ZTP:

1. While in the Deploy mode, select **Zero Touch Provisioning** > **Setup** in the Tasks pane. The Zero Touch Provisioning wizard appears.
2. Specify the server details in the Server Setup wizard page as described in Specifying the Server Details.
3. Click **Next** and proceed to specify the software image, configuration file, and the IP address range to be configured on the DHCP server. For more details, see Specifying the Software Image and Configuration Details.
4. Click **Next** to review the details of the ZTP profile that you created.

   In the Review page, you make changes to or save a ZTP profile:

   - To make changes to the profile, click the **Edit** button associated with the configuration you want to change.

     Alternatively, you can click the appropriate buttons in the ZTP workflow at the top of the page that correspond to the configuration you want to change.

     When you are finished with your modifications, click **Review** to return to the Review page.
   - To save the ZTP profile or to save modifications to the settings of an existing profile, click **Finish**.

You can use the Monitor ZTP Profiles page to view details about the switches that were provisioned using a given ZTP profile and added successfully to the Network Director inventory.

To monitor a ZTP profile:

1. While in the Deploy mode, select **Zero Touch Provisioning** > **Monitor** in the Tasks pane. The Monitor ZTP Profiles page appears.
2. In the Choose ZTP Profile box, select the ZTP profile that you want to monitor.

   Network Director displays the ZTP summary and details of switches that were discovered using the selected profile.

Related Documentation

- Understanding Zero Touch Provisioning

Brownfield Deployment in Network Director

To support rapid network deployment, Junos Space Network Director enables you to define your network configuration in a set of profiles that you can apply to multiple objects in your network. For example, you can define a Port profile to set up class-of-service (CoS), authentication, firewall filters, and Ethernet switching settings that are appropriate for all access ports in your network that connect to employee desktop VoIP phones.

Profiles can be created manually from the Network Director user interface or may be created automatically by Network Director when you discover a device. Once a device, that has network configurations, is discovered, Network Director initiates a *Brownfield* process to read the configuration and create the necessary profiles for all the supported configuration from the discovered device. Network Director initiates the brownfield process immediately after the discovery and the process is transparent to the user. Figure 1 on page 5 displays how the brownfield process works in Network Director.

Figure 1: Brownfield process

Related Documentation

- Understanding Network Configuration Profiles

Profiles in Network Director

Profiles in Network Director are a group of feature-specific configurations that can you assign to devices. For example, you can create a CoS profile that combines all the supported class-of-service configurations for a particular device family, and assign it to a port on a device.

There are three ways in which profiles can be created in Network Director:

- You can create a new profile for an interface or device by defining the custom configuration. You can use the Tasks pane in Build mode to manually create profiles. For more details, see "Create Profiles" on page 6.
- Network Director automatically creates profiles based on the configuration information read by the brownfield process. This is applicable when a device with supported configuration is discovered in Network Director. For more information, see "Brownfield Deployment in Network Director" on page 4.
- Network Director automatically creates profiles when a supported configuration of a device that is already discovered and managed by Network Director is modified outside Network Director (also known as out-of-band configuration changes). For more information, see Understanding Resynchronization of Device Configuration.

Following are some advantages of using profiles:

- Bulk provisioning—You can combine a group of configurations as a profile and apply it to one or more ports or devices in one go, thereby saving a lot of time and effort. Profiles ensure that the configurations are error-free as most configuration value ranges

are set in the profile workflow. Network Director prompts the user if there are any errors. You must fix the errors before you can create a profile.

- Editing—For profiles that are already deployed on devices, if you want to make changes to the configuration values, you can modify the configuration values in the profile and redeploy the profile. Network Director updates the new configuration value on each device where the profile is deployed.
- Cloning—If you already have a set of profiles defined for your network and want to apply a different configuration for a set of devices or ports in your network, you use the clone feature. The clone feature enables you to make a copy of any profile and make the necessary modifications. You can then apply these to devices and ports that require the different set of configuration.

Related Documentation

- Create Profiles on page 6

Create Profiles

You can create profiles for the various configurations that you want to apply to your network devices. The profile configuration settings might vary depending upon the device family (hardware family of the device) you select. The device families for which you can create profiles in Network Director are:

- Switching (EX)
- Campus Switching ELS (Enhanced Layer 2 Software)
- Data Center Switching Non-ELS
- Data Center Switching ELS

After you create the necessary profiles, you can associate these profile with devices by either directly assigning a profile to a device (or to ports or radios on the device) or by referencing the profile in another profile.

When you assign a profile to a device, you can configure certain device-specific parameters. For example, when you assign a VLAN profile to a device, you can configure the IP address for that VLAN on that device. Similarly when you assign a Port profile for a Layer 3 interface to the interface, you can configure the IP address for that interface.

Watch this video-based tutorial to know more about how profiles are created in Network Director.

Video: Building and Deploying VLAN Profiles in Network Director.

When you assign a profile through referencing, that is, you do not assign them directly to network devices, instead they are referenced from other profiles that are, in turn, assigned

to network devices. For example, the settings in the CoS, Filter, and Authentication profiles are assigned indirectly to a port by the including these profiles in the Port profile.

Creating and Managing Profiles

Creating and managing profiles involves the following tasks:

1. Creating a new profile by clicking **Add**, and selecting the device family for which you want to create the profile, and clicking **OK**.
2. Modifying an existing profile by selecting it and clicking **Edit**.
3. Associating a profile to specific interfaces by selecting it and clicking **Assign**. During the assignment process, you can choose to configure interface-specific settings, such as IP address.
4. Changing a profile's current interface assignments by selecting it and clicking **Edit Assignments**. This opens the Edit assignments for profile-name page, which displays the assignment state and other details of the interfaces in a grid layout. After editing an assignment, click **Apply**.
5. Viewing information about a profile, including the interfaces it is associated with, by selecting the profile and clicking **Details** or by clicking the profile name, which opens the Profiles Details page. This page displays the profile details and the interface associations in a grid layout. It also has an option using which you can search for the profiles associated with a device and filter interfaces. Click **Show Filters** to filter an interface based on its IP address, serial number, type, or location or custom group.
6. Deleting profiles by selecting the profiles and clicking **Delete**.
7. Cloning a profile by clicking the profile and clicking **Clone**.

For detailed steps for profile management tasks, see Assigning Profiles to an Interface, Device, or a Group of Devices.

Creating Device Profiles

Network Director enables you to configure device-level settings for switches in the Device Common Settings profile page. Once you create the profiles, you can,

- assign the profiles to a single switch or multiple switches.
- assign the profiles to a single controller or multiple controllers.
- deploy the profiles by using the Deploy mode tasks.

Network Director also creates Device Common Settings profiles when it discovers devices. It creates a Device Common Settings profile for each device it discovers, importing the

device-level settings from the device into the profile. While configuring a profile, you can specify the basic settings, which include the profile name, device user list, and time settings. Apart from the basic settings, you can optionally specify the management and protocol settings too.

Device profile creation and management involves the following tasks:

1. Completing the management settings and protocol settings for the selected device family described in Creating and Managing Device Common Settings.
2. Once a Device Common Settings profile is created or discovered (system-created profile), assigning it to devices by using the steps described in Assigning Device Common Settings to Devices.

Creating and Managing Port Profiles

Port profiles provide a way to provision multiple switch interfaces, including Ethernet interfaces on EX Series switches, Campus Switching ELS, Data Center Switching devices, and Fibre Channel (FC) interfaces on Data Center Switching devices. In a Port profile, you can define a set of attributes to be shared by multiple interfaces and configure as well as select the in-line profiles such as the VLAN, CoS, Authentication, Filter, and VRRP profiles.

Port profiles define only shared attributes. To enable you to configure specific attributes for an interface or a switch during the process of assigning a Port profile to an interface, the Create Port profile wizard provides two setup options: Quick Setup and Custom Setup.

1. Use the Quick Setup option to:
   - Create the default configuration settings for a Port profile.
   - Select or create an in-line VLAN profile.
   - Configure advanced settings and other profiles, such as CoS, Authentication, Filter, and VRRP profiles with their default values.
2. Use the Custom Setup option to further configure the advanced settings and modify the default configuration settings of the other profiles.

NOTE: **While configuring the in-line profiles in Port profiles, you can either configure or select a CoS profile, VLAN profile, and Authentication profile; however you will be only able to select a Filter and the VRRP profile.**

Creating Access and RADIUS Profiles

Once you configure or select the in-line profiles in the Port profile, configure the Access and RADIUS profiles to provide centralized access to the network.

1. Create and manage RADIUS profiles to configure RADIUS server settings by selecting the **RADIUS** option under Profiles.

2. Create and manage Access profiles and specify servers to be used by the user accounting purposes by selecting the **Access** option under Profiles.
3. Assign these profiles to the Port profiles by clicking **Edit Assignment** in Port profiles.

Viewing Assigned Profiles to a Device

The View Assigned Profiles page lists all the profiles associated with a selected device or with an object such as ports, access points, or radios within that device. To view the profiles assigned to a device, you must have the profiles already assigned to the devices, ports, access points, or radios within that device. Only those profiles that are assigned to a specified object are displayed in the Profiles Assigned to the Device page.

In addition to displaying profiles assigned to objects, the Profiles Assigned to Device page also shows link aggregation groups (LAGs) assigned to devices.

To view the assigned profiles to a particular device:

1. While in Build mode, select an EX Series switch from the Switching Network cabinet in the left navigation tree.
2. Select **Logical**, **Location**, or **Device** under **Views**.
3. Select **View Assigned Profiles** under **Tasks > Device Management**.

   The Profiles Assigned to the Device page displays a list of profiles that are already assigned to the selected device.

Related Documentation

- Profiles in Network Director on page 5
- Creating and Managing VLAN Profiles.
- Creating and Managing Access Profiles.
- Creating and Managing Authentication Profiles.
- Creating and Managing RADIUS Profiles.
- Creating and Managing VRRP Profiles.
- Creating and Managing Wired CoS Profiles
- Creating and Managing Wired Filter Profiles.

Create Fibre Channel Gateway Service and Fabric Profiles

You can configure Fibre Channel (FC) gateways on data center switching devices by using an FC Gateway Service profile or by using a combination of other profiles.

An FC Gateway Service profile provides a quick way to configure FC gateways on data center switching devices. An FC gateway configuration has some default settings that cannot be modified. For example, you cannot specify any CoS settings for the FC gateway; only the default settings are available.

If you want to configure an FC gateway that does not meet the requirements of the FC Gateway Service profile, you can use a combination of other profiles to configure the components of the FC gateway and assign them to the appropriate devices, ports, and profiles. These configurations might include, CoS on the FC gateway, FCoE VLANs, FC and Ethernet ports as FC gateway, and FC Gateway Fabric profiles.

- Creating FC Gateway Service Profiles on page 10
- Creating Fabric Profiles on page 10

Creating FC Gateway Service Profiles

To create an FC Gateway Service profile:

1. While in Build mode, select **Wired > System > FC Gateway Service** from the Tasks pane.
2. Click **Add**.
3. Enter the settings for the FC Gateway Service profile as described in Specifying Settings for an FC Gateway Service Profile.
4. Click **Done**.

After you create an FC Gateway Service profile, you must assign it to ports on the data center switching devices that you want to include in an FC gateway. You must assign the profile to at least one FC port and at least one Ethernet or aggregated Ethernet interface on the device. In a QFabric fabric, an FC gateway cannot span multiple nodes. For information about the FC Gateway Service profile assignment, see Assigning an FC Gateway Service Profile to Ports.

Creating Fabric Profiles

A Fabric profile contains configuration settings for a gateway FC fabric. You assign Fabric profiles to QFX Series devices that act as an FCoE-FC gateway, to configure gateway FC fabrics.

A gateway FC fabric is a QFX Series configuration construct. It is not the same thing as an FC fabric in the storage area network (SAN); the gateway FC fabric is local to the switch. It creates associations that connect FCoE devices with converged network adapters (CNAs) on the Ethernet network to an FC switch on the Fibre Channel network. A gateway FC fabric consists of:

- A unique fabric name and a unique fabric ID.
- At least one dedicated VLAN for FCoE traffic.
- At least one FCoE VLAN interface (Layer 3 VLAN interface) that includes one or more 10-Gigabit Ethernet interfaces connected to FCoE devices.
- One or more native FC interfaces.

To create a Fabric profile:

1. From the Network Director Banner, select **Build** mode.
2. In the Tasks pane, select **Wired > System > Fabric**.

3. Click **Add**.

   The Create Fabric Profile page appears.

4. Enter settings for the Fabric profile as described in Specifying Settings for a Fabric profile and click **Done**.

After you create a Fabric profile, you can assign it to a QFX3500 device in standalone mode or to a QFabric Node. A Fabric profile contains configuration settings for a gateway Fibre Channel (FC) fabric. You can assign an existing user-created or system-created Fabric profile to devices and FC ports to configure FC fabrics, using the steps described in Assigning a Fabric Profile to Devices and Ports topic.

Related Documentation

- Configuring Fibre Channel Gateways
- Creating and Managing Fabric Profiles

Manage Software Images using Network Director

As a Network Administrator, you can store different versions of Junos OS software images in the Network Director image repository. You can then deploy these images on one or more managed devices manually or have the system deploy the images by using zero touch provisioning (ZTP).

To manage the image repository:

1. Click **Deploy** in the Network Director banner.
2. In the Tasks pane, select **Image Management** > **Manage Image Repository**. The Device Image Repository page opens in the main window. This page displays a table that lists the software images in the repository.
3. From the Device Image Repository page, you can:
   - Add a software image to the repository. For detailed steps, see Adding Software Images to the Repository.
   - View details about a software image. For detailed steps, see Viewing Software Image Details.
   - Delete software images from the repository. For detailed steps, see Deleting Software Images.
4. You can choose to deploy the images in the repository to the managed devices by using one of the following methods depending on your network requirement:
   - To deploy software images to devices that are already managed by Network Director, use the **Image Management** > **Deploy Images to Devices** option available in the Tasks pane in the Deploy mode. For detailed steps, see Deploying Software Images.
   - To deploy software images on new devices, use the **Zero Touch Provisioning** > **Setup** option available in the Tasks pane in the Deploy mode. For detailed steps, see "Adding Devices Using Zero Touch Provisioning" on page 3.

Related Documentation

- Configuring and Monitoring Zero Touch Provisioning

Configure Approval Modes for Device Configurations

When you make configuration changes in Build mode, the changes are not deployed to devices automatically. You must manually deploy the changes to devices in Deploy mode. When you deploy configuration changes to a device, all pending configuration changes for that device are deployed. You can deploy the device configurations in the following two ways:

- Auto Approval—In this mode, the device configuration changes are approved automatically by the system and do not require explicit (manual) approval by a configuration approver before they can be deployed. This is the default approval mode.
- Manual Approval—In this mode, the device configuration changes must be explicitly approved by a configuration approver before the changes can be deployed to the device. An operator performs device configurations and creates a change request for that configuration and submits it for approval to one or more approvers. The approvers are notified by e-mail whenever a change request is created. If a configuration or a change to it is approved by an approver, then the operator is able to deploy it. If a configuration is rejected, the operator must make the necessary changes, resubmit the change request, and procure an approval before the configuration can be deployed. For manual approval, the **Network Director - Configuration Approver** role is available in Junos Space, which is specific to Network Director. A user with this role reviews device configurations and proposed changes to device configurations and can either approve or reject them.

- Setting up the Approval Mode Type on page 12
- Deploying Configuration Changes on page 13

Setting up the Approval Mode Type

Use the Config & Deploy tab of System Preferences to configure the approval mode:

1. Select the **Manual Approval** mode if you want an approver to review and approve the changes before they are deployed. By default, the Auto Approval mode is selected. Use this mode if you want to deploy the configuration changes without a prior approval.
2. If you select the Manual Approval mode, add the e-mail addresses of one or more approvers, who are notified every time a change request is submitted.
3. Specify the rollback limit, which is the number of change requests that can be rolled back. The default value is 50. You can roll back a maximum of 1000 change requests.
4. Specify the time after which a change request elapses after the time it was created.

   The minimum and maximum number of days that you can specify after which a change request elapses is 1 day and 365 days respectively.
5. Click **OK** to save the changes.

Deploying Configuration Changes

Based on the approval mode, you can choose to deploy the device configuration changes in the following ways:

From the Devices with Pending Changes page, you can select Auto Approval mode or Manual Approval mode.

If you select the auto approval mode, you can deploy configuration changes for devices without an approval from the configuration approver. In the auto approval mode, you can do the following configuration deployment tasks on devices that have pending changes.

1. Run configuration deployment jobs immediately or schedule them for future times by clicking the **Deploy Now** or the **Schedule Deploy** options respectively.
2. Preview, validate, or discard the pending configuration changes.

If you select Manual Approval mode, the Devices with recent configuration changes and Change Requests pages open. You can do the following configuration deployment tasks on devices that have pending changes in manual approval mode:

1. Create a device configuration change request approval and submit it for approval. Upon submission, all device changes made by an operator are validated and all the approvers are notified of the details of the proposed change request by e-mail.
2. An approver either approves or rejects the change requests. See Approving Change Requests for more information.
3. After the successful approval, you can deploy the device configurations immediately or schedule the deployment for a later period.
4. Preview, validate, or discard the pending configuration changes.

Related Documentation

- Deploying Configuration to Devices

Resynchronize Device Configuration

In a network managed by Network Director, the following three separate repositories about device configuration are maintained:

- The configuration information about the devices themselves.
- The configuration information maintained by the Junos Space Network Management Platform. When a device is discovered, either by Junos Space or Network Director, Junos Space stores a record of the configuration on that device.
- The configuration information maintained by Network Director in Build mode. This information is in the form of the profiles assigned to the device, and additional configurations, such as LAG and access point configurations, that you create for device management.

When the configuration information in all the three repositories match, the configuration state of the device is shown as In Sync. If there is a conflict in the configuration information in any one or all of the repositories, the configuration state of the device is shown as Out of Sync. You cannot deploy configuration on a device when the device configuration state is Out of Sync.

To deploy the device configuration in Network Director, the configuration information state of the device must be In Sync. If there are conflicting device configurations, these conflicts need to be resolved by the resynchronization process.

When out-of-band changes occur on a device, the auto-resync operation is triggered. If there are no conflicting changes, the state of the device is shown as In-Sync. If there are conflicting changes, the status of the device is shown as Conflict, in which case you must perform manual resynchronization of the device.

How Network Director performs resynchronization depends on the system of record (SOR) mode set for the Junos Space Network Management Platform. There are two possible modes:

- Network as system of record (NSOR)—In NSOR mode, the network device is considered the system of record for device configuration, which means the configuration maintained by the device takes precedence over the configuration maintained by Junos Space and Network Director. Thus, when you perform a resynchronization, the Junos Space configuration record and the Network Director Build mode configuration are updated to match the device configuration. This is the default mode. This modes supports both auto-resynchronization and manual resynchronization.
- Junos Space as system of record (SSOR)—When Junos Space is in SSOR mode, Junos Space is considered the system of record for device configuration. In this mode, when you make an out-of-band configuration change on a device, you can choose whether to accept the change or to overwrite the change with the configuration maintained by Junos Space. This mode supports only manual resynchronization.

- Setting up Auto Resynchronization Preferences on page 14
- Manually Resynchronizing Device Configurations on page 15

Setting up Auto Resynchronization Preferences

In Network Director, the automatic resynchronization feature is enabled by default and cannot be disabled. However, you can enable or disable the purging of unassigned system profiles. Purging of unassigned system profiles removes unassigned profiles generated by Network Director after resynchronization or deletion of a device.

You can enable or disable the purge option under auto-synchronization preferences settings:

1. Select the **Config & Deploy** tab in the Preferences window.
2. Select the option **Purge unassigned system profiles after resynchronizing configuration** to remove unassigned profiles that were generated by Network Director after resynchronization or deletion of a device.
3. Specify the time interval in **Auto Resync TriggerWait Interval(sec)**.

Network Director waits for this time interval before triggering auto-resynchronization. The default time interval is 120 seconds.

4. Click **OK**.

Manually Resynchronizing Device Configurations

When the device out-of-band changes conflict with the changes made in Network Director, Network Director does not automatically resynchronize the device changes into Network Director. The device is marked as Conflict. You must manually resynchronize the changes by using the Resynchronize Configuration task. After this, the local changes are discarded and are replaced by the latest network configuration.

How Network Director performs resynchronization depends on the system of record (SOR) mode (either network as system of record (NSOR) or Junos Space as system of record (SSOR)) set for the Junos Space Network Management Platform.

To resynchronize devices when the Junos Space Network Application Platform is in NSOR mode:

1. In the Resynchronization Device Configuration page, select the device or devices that you want to resynchronize.
2. (Optional) View any pending changes to a device's configuration in Network Director by clicking **View** in the Local Changes column.

   These pending changes are deleted when you resynchronize the device.
3. Click **Resynchronize Configuration**.

To resynchronize devices when the Junos Space Network Management Platform is in SSOR mode:

1. In the Resynchronization Device Configuration page, select the device or devices that you want to resynchronize.
2. (Optional) View any pending changes to a device's configuration in Network Director by clicking **View** in the Local Changes column.

   These pending changes are deleted if you accept the out-of-band changes when you resynchronize the device.
3. Click **Resynchronize Configuration**.
4. In the confirm dialog box, click **Accept device changes** or **Reject device changes** depending upon status of the out-of-band changes.
5. Click **Submit**.

Related Documentation

- Understanding Resynchronization of Device Configuration
- The Resynchronize Device Configuration Task

Create Baseline Configuration

You can create a baseline of configuration and the Junos OS version of the devices on the Network Director server. By creating a baseline configuration file for a device you define a reference point to save the device configuration and its Junos OS version to a particular known state and later restore the configuration to that known state.

- Creating and Managing Baseline Configuration of Devices on page 16

Creating and Managing Baseline Configuration of Devices

You can select the devices at the scope level, custom grouping, or for individual devices and create baseline configuration files and images for all or for selected devices. The baseline configuration file includes all of the configuration and image files. When you restore a device configuration, you restore both the baseline configuration file and the image of the file. However, restoring the image file is optional.

To start baseline file management:

1. Click **Deploy** in the Network Director banner.
2. Select the following baseline creation and management tasks, which are described in the respective topics:
   - Baselining Device Configuration Files
   - Restoring Baseline Device Configuration Files
   - Viewing Baseline Configuration Files
   - Comparing Baseline Configuration with Current Configuration
   - Deleting Baseline
   - Managing Baseline Management Jobs

Related Documentation

- Understanding Deploy Mode in Network Director
- Creating and Managing Baseline of Device Configuration Files

Viewing Current Configuration

From Network Director, you can view the configuration running on a device and those that are pending deployment by using the following options respectively:

- Show Current Configuration
- Configuration or Pending Configuration Window

- Using the Show Current Configuration on page 17
- Using the Configuration or Pending Configuration Window on page 17

Using the Show Current Configuration

The Show Current Configuration task shows the entire running configuration of the selected device in Network Director. This task is available in the Logical, Location, and Device panes.

To view a device's current configuration:

1. Click **Build** or **Deploy** in the Network Director banner.
2. Select the device in the View pane.
3. Select **Device Management > Show Current Configuration** in the Tasks pane.

   The device's current configuration displays in the main window.

Using the Configuration or Pending Configuration Window

Use the Pending Configuration window to view the configuration changes that will be deployed to a device when a job runs. This task is available under Deploy Configuration Changes when you are in Deploy mode.

After an operator creates change request for a device configuration, the change request is submitted to the approvers mentioned in the approvers list. To view the pending configuration of the device:

1. Approver selects the change request and clicks on **Approve Change Requests** .

   The Change Request Details page opens.
2. Clicking **View** under Configuration column shows the device pending configuration changes in XML and CLI format:
   - Select the XML View tab to view the configuration changes in XML format. This view shows the configuration (XML format) that will be deployed to the device's Device Management Interface (DMI), which is used to remotely manage devices.
   - Select the CLI View tab to view the configuration changes in CLI format. This view shows the Junos configuration statements that will be deployed to the device.

     In both views, the content is color-coded for easier interpretation:
     - Black text indicates configuration that is already active on the device, and which will not be changed if you deploy.
     - Green text indicates configuration that will be added if you deploy.
     - Red text indicates configuration that will be removed if you deploy.

Related Documentation

- Understanding the Network Director User Interface
- Deploying Configuration to Devices

Monitor your Network using the Monitor Mode

Monitor mode in Network Director provides you visibility into your network status and performance. You can also use the Dashboard widgets to monitor your network performance.

Network Director monitors the devices it manages and maintains the information it collects from the devices in a database. You can view this data as easy-to-understand graphs and tables—known as monitoring widgets—to quickly visualize the state of your network, spot trends developing over time, and view important details.

Monitor mode divides the monitoring activity into the following categories:

- Traffic—Provides information about traffic on QFabric systems, switches, routers, Virtual Chassis, Virtual Chassis Fabrics (VCFs), Layer 3 Fabrics, and wireless controllers.
- Client—Provides session information about clients connected to wireless access points and to 802.1X authenticator switch ports.
- RF—Provides information about the wireless environment and signal performance.
- Equipment—Provides information about the state of switches, wireless LAN controllers, interfaces, wireless access points, and radios.
- Fabric Analysis—Displays the results of running the Run Fabric Analyzer task on a QFabric or VCF. It shows information about the health, connectivity, and topology of the fabric.

To view the state and performance of your network:

1. Click **Monitor** in the Network Director banner.
2. Use the various monitor widgets to view the status and performance of your network. The most commonly used monitoring widgets are described in the following table:

Category	Purpose	How to access
Traffic	To monitor port traffic statistics on a device.	a. Select a node in the View pane that contains the port traffic you want to monitor. b. Select the **Traffic** tab. c. In the Tasks pane, select **View** > **Port Statistics**. The Port Traffic Stats window opens. For information about this window, click the Help icon in the title bar of the window or see Port Traffic Stats Window.

Category	Purpose	How to access
Traffic	To monitor Layer 3 VLAN traffic statistics on a device.	a. Select a node in the View pane that contains the Layer 3 VLAN traffic you want to monitor. b. Select the **Traffic** tab. c. In the Tasks pane, select **View > L3 VLAN Statistics**. The L3 VLAN Traffic Stats window opens. For information about this window, click the Help icon in the title bar of the window or see L3 VLAN Traffic Stats Window.
Traffic	To monitor routing instances on MX Series routers.	a. In the View pane, select the MX Series whose routing instances you want to monitor. b. In the Tasks pane, select **Tasks > Show Routing Instances**. The Show Routing Instances window opens. For information about this window, click the Help icon in the title bar of the window or see Show Routing Instances Window.

Category	Purpose	How to access
Traffic Summary	To access information about port utilization in either one of two places, depending on the node you select in the View pane: • Port Utilization monitor—This monitor, available in the Summary tab, provides a bar chart that shows the aggregate utilization of the ports on a device or devices over a period of time that you select. • Port Utilization task—This task, available from View > Port Utilization in the Tasks pane of the Summary or Traffic tabs, provides a bar chart similar to the Port Utilization monitor bar chart. Unlike the Port Utilization monitor, it also enables you to obtain information about individual port utilization over time when you have selected an individual device or Layer 3 Fabric in the View pane.	a. Select a node in the View pane that contains the ports whose utilization you want to monitor. b. Select the **Summary** or **Traffic** tab. c. In the Tasks pane, select **View > Port Utilization**. If you select a node that contains more than one device, the Port Utilization Details window opens. For information about this window, see Port Utilization Details Window. If you select an individual device, the Utilization for Device window opens. For information about this window, see Utilization for Device Window. If you select a Layer 3 Fabric, the Utilization for IP Fabric window opens. For information about this window, see Utilization for IP Fabric Window.
Traffic	To monitor Virtual Chassis protocol statistics on a device. NOTE: This task is applicable only for Virtual Chassis and Fabric devices that are managed by Network Director.	a. Select a node in the View pane that contains the Virtual Chassis protocol traffic you want to monitor. b. Select the **Traffic** tab. c. In the Tasks pane, select **View > VC Protocol Statistics**. The Virtual Chassis Protocol Statistics window opens. For information about this window, click the Help icon in the title bar of the window or see Virtual Chassis Protocol Statistics Window.
All	To find user sessions on the network.	In the Tasks pane, select **Tasks > Find User Session**. The Search User Session window opens. For information about this window, click the Help icon in the title bar of the window or see Search User Session Window. NOTE: You can search for user sessions in any tab in Monitor mode.
All	To find end points on the network. End points are computing devices that are connected to the network.	In the Tasks pane, select **Tasks > Find Endpoint**. The Find End Point window opens. For information about this window, click the Help icon in the title bar of the window or see Find End Point Window. NOTE: You can search for end points in any tab in Monitor mode except the Fabric Analysis tab.

Category	Purpose	How to access
Client	To access information about clients and sessions on the network such as the session count and session trend over a period of time. The data can also be categorized based on VLANs.	a. Select a node in the View pane that contains the client sessions you want to monitor. b. Select the **Client** tab. For information about a monitor, click the Help icon in its title bar or see Monitoring Client Sessions.
All	To view the Address Resolution Protocol (ARP) table information for a device.	a. Select the device in the View pane that you want to monitor. b. Select **Tasks > Show ARP Table** in the Tasks pane. The Show ARP Table Information window opens. For information about this window, click the Help icon in the title bar of the window or see Show ARP Table Information Window. You can click the Refresh button below the table to refresh the data from the device. NOTE: You can view ARP table from any tab in Monitor mode except the Fabric Analysis tab.
Equipment	To access real-time statistics on logical Ethernet switching interfaces for switches, routers, Virtual Chassis, QFabric systems, and Layer 3 Fabrics.	a. Select a node in the View pane that contains the logical interface you want to monitor. b. Select the **Equipment** tab. c. Click **Logical Interfaces** in the Tasks pane to open the Show Logical Interface Information table in main window. For more details, see Show Logical Interface Information Table.
Equipment	To obtain at-a-glance information about the status and performance of Virtual Chassis.	a. Expand the network tree to display the Virtual Chassis nodes. Select the Virtual Chassis in the network tree. b. Click the Equipment tab to display the four monitors. c. Click the Help icon on the monitor to learn more about the purpose or fields on a monitor. For more details, see Monitoring the Status of a Virtual Chassis. To view details of the Virtual Chassis members, follow the procedure given in Monitoring the Status of Virtual Chassis Members.
All	To analyze QFabric devices. The Run Fabric Analyzer task analyzes a QFabric device and provides information about its health, connectivity, and topology.	a. Select the QFabric device to analyze in the View pane. b. In the Tasks pane, select **Tasks > Run Fabric Analyzer**. The results of the analysis appear on the Fabric Analysis tab in Monitor mode when the QFabric device is selected in the View pane. For information about using the tabs within this tab, see Using the Fabric Health Check Tab and Using the Topology Tab.

3. To know more about the Monitor mode in Network Director, see Understanding Monitor Mode in Network Director.

Related Documentation

- Changing Monitor Polling Interval and Data Collection

Monitor Your Network Using the Dashboard View

Dashboard View is a customizeable page that displays information about the network, and is the default page that opens when you log in.

You select monitoring widgets to display on the Dashboard that show various information about the network.

You can add widgets to the Dashboard:

1. To add a widget to the Dashboard:
   a. Select **Add Widgets**. Thumbnails of the available widgets appear.
   b. To add a widget to the Dashboard, mouse over the widget's thumbnail, then click the **Add** button that appears on the widget.
   c. When you are finished adding widgets, click **Done**. The new widgets appear on the Dashboard.

Table 1 on page 22 lists the dashboard widgets that are currently available in Network Director and their purpose. With each release, Juniper Networks adds new widgets to assist you to monitor your network more efficiently. See the Network Director release notes and documentation to know about new or modified dashboard widgets.

Table 1: List of Dashboard widgets

Name of the Dashboard widget	Purpose
Alarms widget	The Alarms widget provides summary and detailed information about network alarms. The summary view of the Alarms widget displays summary information about network alarms and their location. The number of active alarms of each severity is shown in colored circles on the left side of the widget. The distribution of alarms by site is shown on a map. The alarms count for each site is shown as a pie chart. The color of each pie chart segment indicates severity level. The colored circles to the left of the map also serve as the legend for the color coding. Mouse over a pie chart to see more information about the alarms for that site. For more information, see Alarms Widget.
Config Deployment Jobs Status widget	The Config Deployment Jobs Status widget provides summary and detailed information about the status of configuration deployment jobs. The information appears in a table. The vertical axis lists the job statuses. The horizontal axis shows the times when job status data was collected. For more information, see Config Deployment Jobs Status Widget.

Table 1: List of Dashboard widgets *(continued)*

Name of the Dashboard widget	Purpose
Config Deployment Jobs Status widget	The Device & Port Latency widget provides a graphical view of latency on devices. The heat map represents each device as a color-coded box. The color coding indicates the level of latency on a device. Cooler colors (for example, green) indicate lower latency, while hotter colors (for example, red) indicate higher latency. The Device & Port Latency widget can show information only for devices that support Cloud Analytics Engine and that have the high-frequency traffic statistics feature enabled in Network Director. For more information, see Device & Port Latency Widget.
Device & Port Utilization widget	The Device & Port Utilization Heatmap widget provides a graphical view of device port utilization percentage. The heat map represents each device as a color-coded box. The color coding indicates the overall level of port utilization on a device. Cooler colors (for example, green) indicate lower port utilization , while hotter colors (for example, red) indicate higher port utilization. For more information, see Device & Port Utilization Widget.
Equipment By Type widget	The Equipment By Type widget provides summary and detailed information about the types of devices Network Director is managing. The diagram represents the managed devices as a set of nested rings. The circle in the center of the diagram shows information about the ring segments when you mouse over them. The inner ring divides the devices into segments that represent wired and wireless device types. The outer ring divides each of those types into more specific device-type segments. Mouse over any diagram segment to see the device type and number of those devices that it represents in the center circle. For more information, see Equipment By Type Widget.
Port Status - Physical widget	The Port Status - Physical widget provides summary and detailed information about the status of physical ports on managed devices. For more information, see Port Status - Physical Widget.
Recent Flow Analysis widget	The Recent Flow Analysis widget enables you to view the results of all analyses of application flows that have been initiated by Network Director in your network. It also enables you simulate and analyze a flow between virtual machines (VMs) and between bare-metal servers (BMSs) to determine the best placement for a new application in your data center. For more information, see Recent Flow Analysis Widget.
Top Talker - Wired Devices widget	The Top Talker - Wired Devices widget provides summary and detailed information about the hosts that are using the most bandwidth. Hosts are endpoints that are directly connected to access ports of wired switches. For more information, see Top Talker - Wired Devices Widget.
Top Virtual Machines by Bandwidth widget	The Top Virtual Machines by Bandwidth widget displays a bar chart of the virtual machines that are using the most bandwidth. Each horizontal bar represents a virtual machine. The horizontal axis shows the bandwidth utilization of the virtual machines in kilobits per second. You can mouse over a bar to see more information about that virtual machine.

Table 1: List of Dashboard widgets *(continued)*

Name of the Dashboard widget	Purpose
Top vNetwork Hosts by Bandwidth widget	The Top vNetwork Hosts by Bandwidth widget displays a bar chart of the virtual hosts that are using the most bandwidth. Each horizontal bar represents a virtual host. The horizontal axis shows the percentage of bandwidth utilization. Mouse over a bar to see more information about that host.
Virtual Machines & Bare Metal Servers widget	The Virtual Machines & Bare Metal Servers widget provides information about the application flows on virtual machines (VMs) and bare-metal servers (BMSs) in your data center. Use the widget to start flow analysis on selected active flows on a specific VM or a BMS and to view the analysis results. You can also use this widget to place a critical VM or BMS on a watchlist. Network Director automatically initiates analysis on all flows on that VM or BMS. For more information, see Virtual Machines & Bare Metal Servers Widget.
Top Overlay Networks widget	The Top Overlay Networks widget displays a summary of the VXLANs in your network in a table. For more information, see Top Overlay Networks Widget.

Related Documentation

- Using Dashboard Widgets

Set Up Network Traffic Analysis and Analyze Traffic

Network Traffic Analysis is a monitoring technology for high-speed switched or routed networks. Network Director uses Cloud Analytics Engine to perform flow analysis. The Compute Agent component of Cloud Analytics Engine creates a probe, or synthetic packet that traces the path of the application flow through the network. When a device detects the probe, it collects various metrics that are sent to the Compute Agent, which then sends the metrics to the Data Learning Engine (DLE) component of the Cloud Analytics Engine. Network Director, in turn, obtains this information from DLE. For more information about Cloud Analytics Engine, see Understanding Cloud Analytics Engine and Network Director.

After you install and configure Cloud Analytics Engine, you can enable network traffic analysis on all devices except wireless devices that are managed by Network Director.

Installing and Configuring Cloud Analytics Engine Compute Agent

To install and configure Cloud Analytics Engine:

1. Download the *Cloud Analytics Engine* **.rpm** package from the Software Download page.

   You install it using the operating system's standard package installation procedure.

2. After installing Compute Agent, run the interactive setup program and enter configuration parameters. For step-by-step instructions, see Configuring Compute Agent by Running the Interactive Setup Program.

   Alternatively, you can create a configuration file that the Compute Agent installer will use to configure Compute Agent during installation. For more details, see Creating a Compute Agent Configuration File and Configuring Compute Agent Initial Configuration by Using a Configuration File. The Compute Agent installer detects the configuration file and use the configuration defined in it instead of running the interactive setup program.

3. Install the DLE. For step-by-step instructions, see Installing and Configuring Cloud Analytics Engine Data Learning Engine.

4. By default, supported networking devices accept and process the network probes that the Compute Agent sends to communicate with networking devices. To enable Cloud Analytics Engine probes on the device, run the following command from the device CLI:

   set services analytics probe enable

Integrating Cloud Analytics Engine with Network Director

Cloud Analytics Engine can integrate with Junos Space Network Director (Network Director) to enable Network Director to configure analytics data collection and visualize network analytics data.

To integrate Cloud Analytics Engine with Network Director:

1. Click  in the Network Director banner and select **Preferences** as shown in Figure 2 on page 25.

   Figure 2: Accessing the Preferences Page

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

2. Click the **Monitor** tab and select the **Data Learning Engine Settings** sub-tab.

3. Enter the IP address of the DLE server.

4. If you want to change the ports used by the DLE, click **View/Edit DLE Ports** to edit the ports and then click **OK**.

   Table 2 on page 26 describes the DLE ports.

Table 2: DLE Port Descriptions

Port	Description
Flow Analysis API Port	Used by the flow path analysis feature and network traffic analysis feature to communicate with the DLE. Port 8082 is the default port.
HFS API Port	Used by the high-frequency statistics feature to communicate with the DLE. Port 8081 is the default port.
HFS Control Channel Port	Used by the high-frequency statistic feature for communication with the DLE about threshold-related events. Port 50006 is the default port.

NOTE: **If you change the default DLE ports, you must ensure that the new ports are open between the DLE and the Junos Space Network Management Platform.**

5. Click **Add Another** to add a new DLE server.
6. Click **OK** to save the DLE settings.

Configuring High-Frequency Statistics and Flow Analysis in Network Director

To configure high-frequency statistics and perform network traffic and flow analysis:

1. To configure high-frequency statistics, you must enable the collection of statistics on specific devices or ports. In Deploy mode, select **Configuration Deployment** > **Enable High Frequency Stats** in the Tasks pane. For more information, see "Enabling High-Frequency Traffic Statistics Monitoring on Devices" on page 27.
2. To perform network traffic analysis using the high-frequency statistics, follow the steps given in "Performing Network Traffic Analysis and Viewing Results" on page 27.
3. To configure flow analysis, you must enable LLDP on the bare-metal servers (BMSs), on the servers hosting the virtual machines (VMs), and on the connecting switches. In addition, the switches must be discovered by using the SNMP option in Network Director. For more information about discovering devices using the SNMP option, see "Discovering Devices" on page 2.

   To perform a flow analysis, follow the steps given in "Performing Flow Analysis and Viewing Results" on page 28.

Enabling High-Frequency Traffic Statistics Monitoring on Devices

To use Network Director monitoring analytics features such as latency heat maps and congestion monitoring on devices, you must enable high-frequency traffic statistics monitoring on the devices.

To enable high-frequency traffic statistics monitoring on devices:

1. Click **Deploy** in the Network Director banner to open Deploy mode.
2. Select the task **Configuration Deployment** > **Enable High Frequency Stats** in the Tasks pane.

   The Enable High Frequency Stats page opens. It displays a table that lists the devices in inventory that support high-frequency traffic statistics monitoring.
3. You can enable high-frequency traffic statistics monitoring on a device as a whole or on selected ports of a device. For more details, see Enabling High-Frequency Traffic Statistics Monitoring on Devices.

Performing Network Traffic Analysis and Viewing Results

Network Traffic Analysis is a monitoring technology for high-speed switched or routed networks. Once enabled, Network Director randomly samples network packets and sends the samples to the DLE for analysis. Network traffic analysis uses packet-based sampling. Network Director samples one packet out of a specified number of packets from an interface enabled for network traffic analysis and sends the packet to the DLE. The DLE uses this sampling information to create a picture of the network traffic, which includes the applications that contribute to the traffic, traffic statistics, and the top applications.

To perform network traffic analysis and view the results:

1. Click **Deploy** in the Network Director banner.
2. In the Tasks pane, select **Configuration Deployment** > **Enable Network Traffic Analysis**.

   The Enable Network Traffic Analysis page opens.
3. Select the check box adjacent to **Enable Traffic Analysis on Devices when Port Utilization exceeds certain percentage** to enable network traffic analysis. The default port utilization percentage value is 90%. You can change the default value to a value that is appropriate for your network.
4. Enter the number of packets from which a packet must be sampled in the Sample rate field.
5. Click **Add Devices** to add new devices for network traffic analysis.

   The Add Devices window opens.
6. In the Add Devices window, select the devices for which you want to enable network traffic analysis.
7. Click **Add**.

Network Director adds the selected devices to the list in the Enable Network Traffic Analysis page.

To remove a device, select a device from the list and click **Remove**.

8. Click **Save** to save the network traffic analysis configuration details.

   Network Director initiates traffic analysis when traffic utilization on any interface of the devices added to the Enable Network Traffic Analysis page exceeds the port utilization that you specified. You can view the traffic analysis details from the **Monitor** mode > **Traffic Analysis** or the Device & Port Utilization dashboard widget.

   For more details, see Monitoring Port Traffic Statistics and Device & Port Utilization Widget.

Performing Flow Analysis and Viewing Results

The Recent Flow Analysis dashboard widget enables you to view the results of all analyses of application flows that have been initiated by Network Director in your network. It also enables you to simulate and analyze a flow between VMs and between BMSs to determine the best placement for a new application in your data center.

Flow analysis provides you with the number of hops, latency per hop, and end-to-end latency. For each hop, you can view information about the device—for example, CPU utilization, traffic statistics, and ingress and egress ports used. The information provided enables you to determine congestion points in the network that might be affecting application performance.

To perform flow analysis by using Network Director, you must:

- Ensure that the components of Cloud Analytics Engine are installed on your network devices and that the Compute Agent discovery file has been created and uploaded to the DLE.
- Specify the DLE server IP address under **Preferences** > **Monitoring** > **Data Learning Engine Settings**.
- Enable LLDP on the servers hosting the VMs, on the BMSs, and on the connecting switches. In addition, the switches must be discovered by using the SNMP option in Network Director. For more information about discovering devices using the SNMP option, see “Discovering Devices” on page 2.

To perform flow analysis and view the results:

1. Click **Dashboard** in the Network Director banner.

   The Dashboard view opens. You can customize the Dashboard view for viewing information about the network. You select monitoring widgets to display on the Dashboard that show various information about the network.

2. If the Recent Flow Analysis monitor widget is not available in the dashboard, you must add it to the dashboard.

   To add a monitor widget to the dashboard:

   a. Select **Add Widgets**. Thumbnails of the available widgets appear.

   b. To add a widget to the Dashboard, mouse over the widget's thumbnail, then click the **Add** button that appears on the widget.

   c. When you are finished adding widgets, click **Done**. The new widgets appear on the Dashboard page.

3. Follow the instructions given in Recent Flow Analysis Widget or watch this video-based tutorial.

Video: Juniper CAE Application flow path analysis

Related Documentation

- Cloud Analytics Engine Documentation
- Understanding Cloud Analytics Engine and Network Director

Manage Network Faults and Notifications in Fault Mode

In Fault mode, Network Director informs you of unexpected, significant events happening in your network. Examples of such events include link up or link down, power supply failure, client authentication failure, detection of an unauthorized access point, and so on.

Network Director receives information about events from its managed devices in the form of SNMP notifications. A single event can often generate multiple SNMP notifications. To simplify management of events, Network Director correlates these notifications, creating high-level alarms of different severity levels for the events. For example, a power supply failure might generate a number of notifications. Network Director correlates these notifications and raises a single power supply failure alarm for the device. Network Director also automatically clears an alarm if it receives notification from the device that the error condition has been resolved.

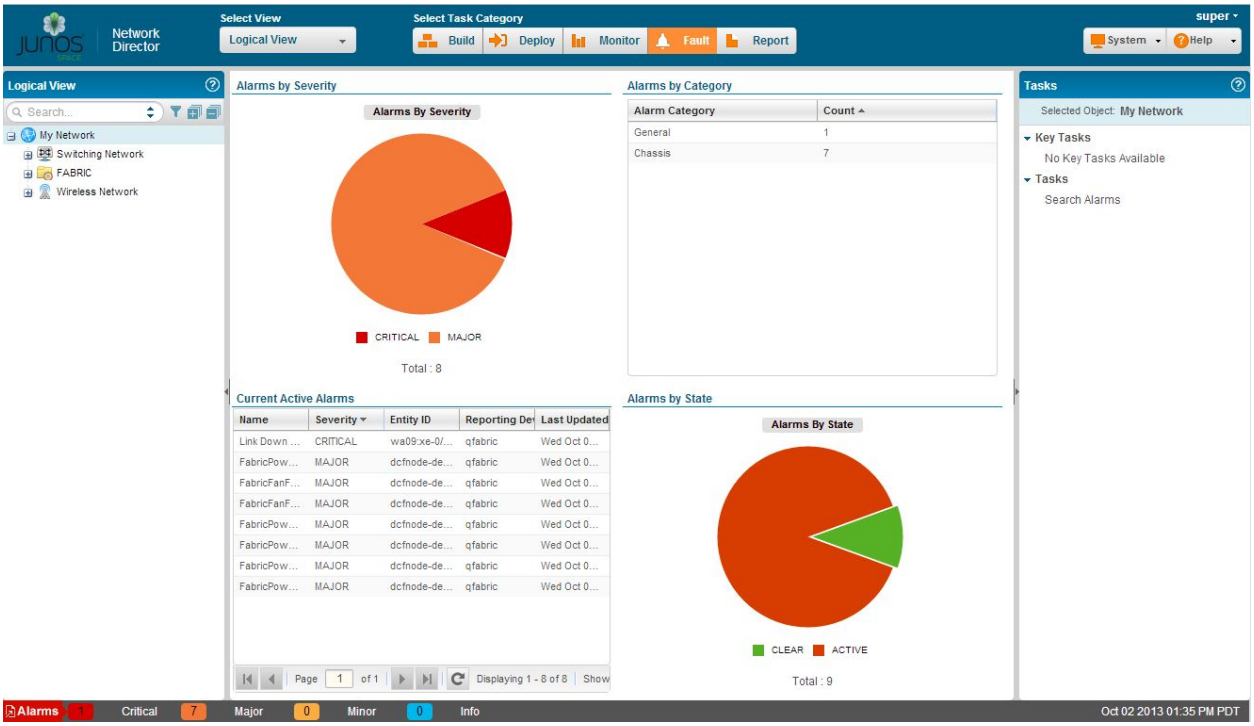
To tailor Network Director fault management to your organization's requirements, you can enable or disable the receipt of specific alarms and change the default severity level of alarms.

- Alarm Monitors—Alarm Status At-a-Glance on page 30
- Alarm Detailed View—Managing Individual Alarms on page 30
- Alarms Pane—Available in Every Mode and Scope on page 31

Alarm Monitors—Alarm Status At-a-Glance

When you enter Fault mode, Network Director displays four alarm monitors in the main window, as shown in Figure 3 on page 30. These monitors enable you to view at a glance the alarm status of the scope currently selected in the View pane. Alarms are organized by severity, category, and state. By selecting different scopes in the View pane, you can see the alarms being generated from different portions of your network—for example, alarms from all devices in your wireless network, alarms from all devices on a particular floor, or the alarms from a specific device.

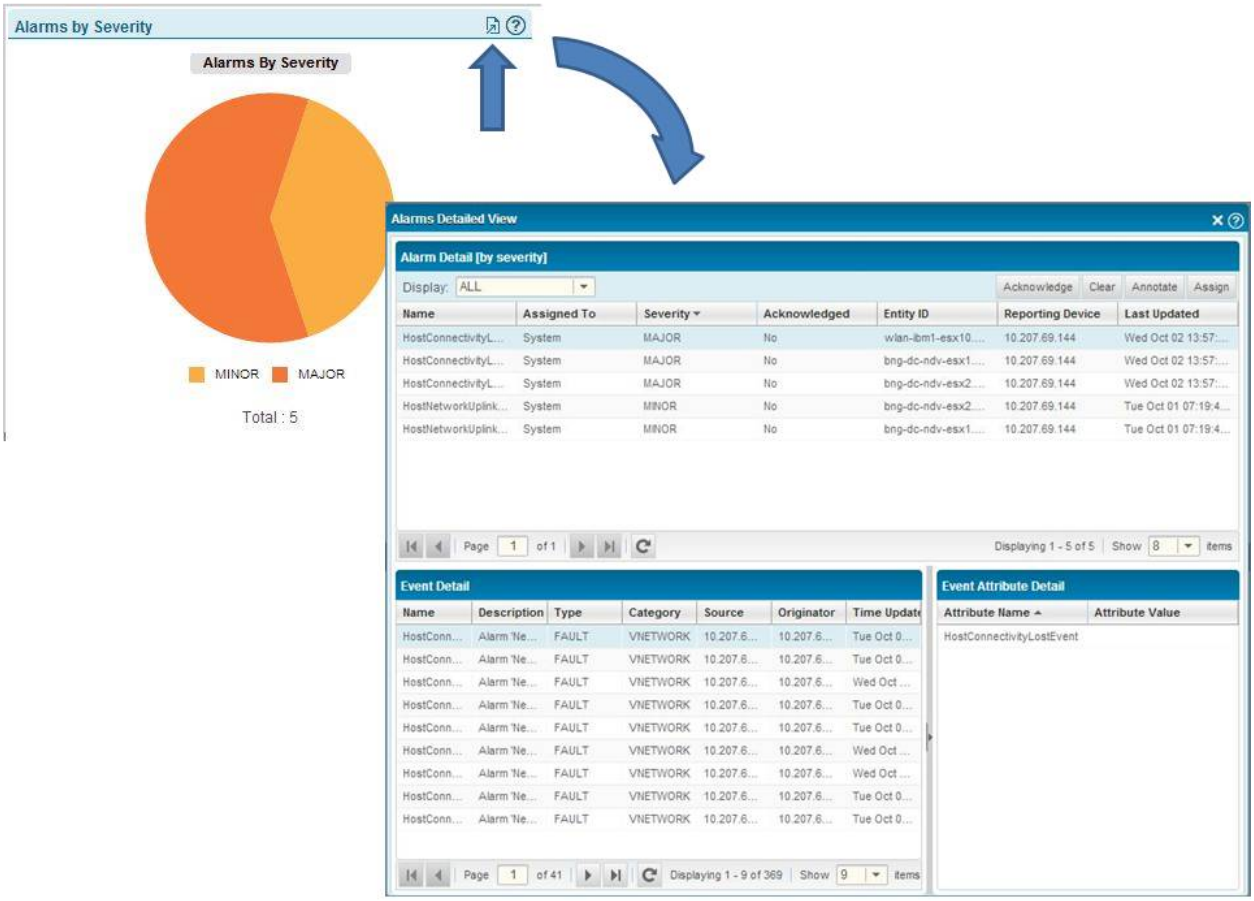
Figure 3: Alarm Monitors Provide a High-Level View of Alarm Status



Alarm Detailed View—Managing Individual Alarms

From any alarm summary, open the Alarms Detailed View, shown in Figure 4 on page 31, which provides more information about the alarms. You can view the events that make up an alarm and, for each event that sends attributes, you can view attributes that help describe the event.

Figure 4: Alarm Detailed View for Individual Alarm Management



In addition, you can acknowledge an alarm, assign an alarm to a person for resolution, annotate an alarm with the actions taken on the alarm, or clear an alarm.

Alarms Pane—Available in Every Mode and Scope

The Alarms pane, shown in Figure 5 on page 31, is always displayed in the Network Director user interface. It provides a count of the number of critical, major, minor, and info alarms that are active in the entire network. Because this information is displayed in every working mode and scope, you can quickly respond to problems in the network. Click the Expand icon or any of the colored numbers to enter the Fault mode directly.

Figure 5: The Alarms Pane Shows the Number of Alarms Active in the Network

Related Documentation

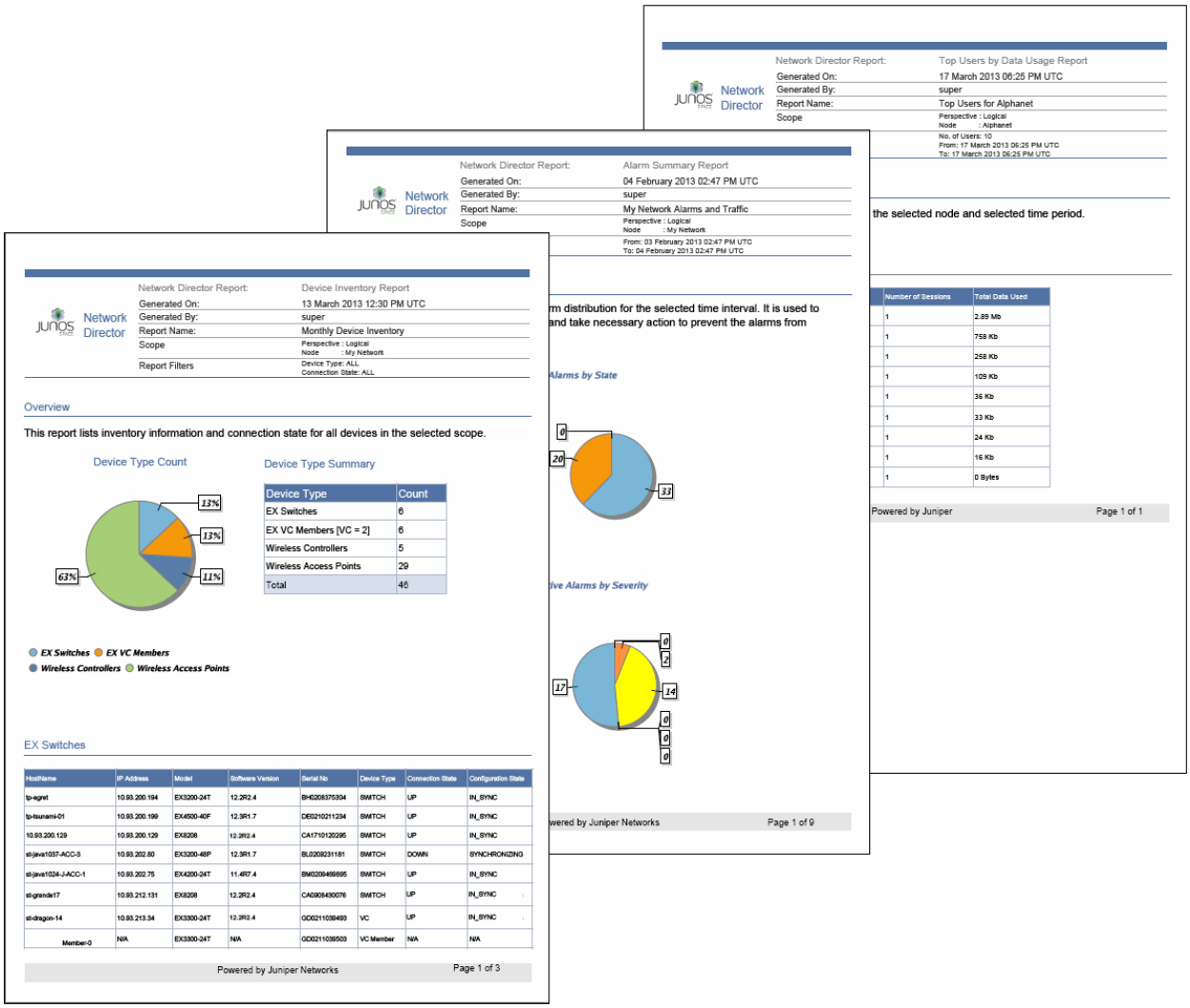
- Understanding Fault Mode in Network Director
- Searching Alarms
- Changing Alarm State

Generate Network Reports in Report Mode

Use the Report mode in Network Director to create standardized reports from the monitoring and fault data collected by Network Director. An essential part of the network management life cycle, reporting provides administrators and management insight into the network for maintenance, troubleshooting, trend and capacity analysis, and provides records that can be archived for compliance requirements.

Network Director provides reports in PDF and HTML formats that use graphs and tables to clearly convey data. Reports are also available in CSV format for importing into spreadsheets. Figure 6 on page 33 shows some examples of PDF reports.

Figure 6: Examples of Network Director Reports



In addition to choosing the formats for your reports, you can:

- Run reports on-demand or schedule them to run at a specific time or on a recurring schedule.
- Select the portion of network you want the report to cover by selecting a scope in the View pane when you create a report definition. For example, you can run a Device Inventory report on your entire network, on all devices in a wiring closet, or on all EX4200 switches.
- Select the report options—for example, the historical time frame you want an Audit Trail report to cover or the type of devices you want to include in a Device Inventory report.
- Have reports sent to an e-mail address or automatically archived on a file server.

The process for generating reports is simple. Select a scope in the View pane and then create a report definition by using the Create Report Definition wizard. When you complete the report definition, the reports are immediately scheduled to run according to the scheduling choices you have made.

Related Documentation

- *Managing Reports in Network Director*
- *Creating Reports*

For More Information

This Getting Started guide provides an overview of the features and capabilities of Network Director. It does not describe every feature that Network Director offers. For more information about Network Director features, see:

- Junos Space Network Director documentation at www.juniper.net/techpubs/
- The online help provided with the Network Director user interface
- Juniper Networks on YouTube