

Junos[®] Space Network Director

Network Director Quick Start Guide

Published
2020-12-25

Release
4.1

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos[®] Space Network Director Network Director Quick Start Guide

4.1

Copyright © 2020 Juniper Networks, Inc. All rights reserved.

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 <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation | iv

Documentation and Release Notes | iv

Documentation Conventions | iv

Documentation Feedback | vii

Requesting Technical Support | vii

Self-Help Online Tools and Resources | viii

Creating a Service Request with JTAC | viii

1

Installing and Upgrading Junos Space Network Director

Network Director Installation Overview | 10

Setting up a Junos Space Appliance for Network Director | 10

Upgrading Junos Space Network Management Platform | 11

Installing Network Director | 12

Installing Network Director From Junos Space Store | 13

Installing Network Director by Manually Downloading the Network Director Application Image | 14

Upgrading Network Director | 15

Uploading DMI Schemas | 18

Next Steps | 19

Preparing Devices for Management by Network Director | 20

Discovering Devices | 21

2

Installing Data Learning Engine

Installing and Configuring Data Learning Engine for Network Director | 25

Installing DLE | 25

What to Do Next | 29

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | iv
- Documentation Conventions | iv
- Documentation Feedback | vii
- Requesting Technical Support | vii

Use this guide to install or upgrade Junos Space Network Director, and perform tasks to get the devices ready for management by Network Director.

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 <https://www.juniper.net/documentation/>.

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 <https://www.juniper.net/books>.

Documentation Conventions

[Table 1 on page v](#) 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.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page v 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
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>

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

Convention	Description	Examples
<i>Italic text like this</i>	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 <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> 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)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(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 (<i>string1</i> <i>string2</i> <i>string3</i>)
# (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)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

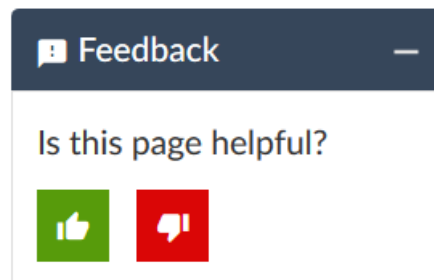
Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> 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 so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software 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 Juniper Care or Partner Support Services 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 <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://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: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- 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 <https://support.juniper.net/support/requesting-support/>.

1

CHAPTER

Installing and Upgrading Junos Space Network Director

Network Director Installation Overview | **10**

Setting up a Junos Space Appliance for Network Director | **10**

Upgrading Junos Space Network Management Platform | **11**

Installing Network Director | **12**

Upgrading Network Director | **15**

Uploading DMI Schemas | **18**

Next Steps | **19**

Preparing Devices for Management by Network Director | **20**

Discovering Devices | **21**

Network Director Installation Overview

Junos Space Network Director enables unified management of EX Series Ethernet Switches, MX Series routers, QFX Series switches, and Junos Fusion Enterprise in your network. It provides for full network life cycle management by simplifying the discovery, configuration, visualization, monitoring, and administration of large networks containing physical and virtual devices.

This chapter describes how you can install Network Director, upgrade Network Director, bring your devices under Network Director management.

These installation steps are intended for network operators and administrators who install, configure, and manage Junos switching with EX Series, QFX Series, and virtualized devices using Network Director.

Before you install Network Director, you must configure the Junos Space Appliance as a Junos Space node.

You can install Network Director in either Juniper Networks JA2500 Junos Space Hardware Appliance or a Junos Space Virtual Appliance. For details, see [“Setting up a Junos Space Appliance for Network Director” on page 10](#).

Setting up a Junos Space Appliance for Network Director

You can install Network Director in one of the following appliances:

- Juniper Networks JA2500 Junos Space Hardware Appliance—The JA2500 appliance is a dedicated hardware device that provides the computing power and specific requirements to run Network Director and the Network Director API as applications.

The JA2500 appliance has a 2-U, rack-mountable chassis with dimensions 17.81 in. x 17.31 in. x 3.5 in. (45.2 cm x 44 cm x 8.89 cm). The JA2500 appliance ships with a single AC power supply module; an additional power supply module can be installed in the power supply slot in the rear panel of the appliance. The JA2500 appliance can also be powered on by using one or two DC power supply modules. The appliance has six 1-TB hard drives arranged in a RAID 10 configuration. Two externally accessible cooling fans provide the required airflow and cooling for the appliance.

For details about the JA2500 appliance and instructions for installation, see [Juniper Networks JA2500 Junos Space Appliance](#).

- Junos Space Virtual Appliance—The Junos Space Virtual Appliance consists of preconfigured Junos Space Network Management Platform software with a built-in operating system and application stack that is

easy to deploy, manage, and maintain. A Junos Space Virtual Appliance includes the same software and provides all the functionality available in a Junos Space physical appliance. However, you must deploy the virtual appliance on the VMware ESX or ESXi server, which provides a CPU, hard disk, RAM, and a network controller, but requires installation of an operating system and applications to become fully functional.

For information about installing Junos Space appliances in a fabric configuration and installing Junos Space Virtual Appliance on a VMware ESX or ESXi server, see [Junos Space Virtual Appliance](#).

Upgrading Junos Space Network Management Platform

You can install Network Director Release 4.1R1 newly only on Junos Space Network Management Platform Release 20.3R1. If you are using Junos Space Network Management Platform Release 20.3R1, you can skip this procedure and begin installation of Network Director.

If you are using a Junos Space Platform release that is earlier than the supported release, you need to upgrade Junos Space Platform before installing Network Director. To determine the Junos Space Platform release version and to upgrade Junos Space Network Management Platform, follow these steps:

1. Determine the installed Junos Space Platform version:
 - a. Log in to Junos Space by using the default username and password for Junos Space: **super** and **juniper123**.

Junos Space opens the dashboard.
 - b. Click the plus symbol (+) next to Administration to expand the Administration menu.
 - c. Click **Applications** to list all of the applications installed.
 - d. Note the version of the Junos Space Platform or the Network Application Platform. (Some earlier versions of the Network Management Platform were named Network Application Platform.) If the currently installed release is a supported one, you can skip the rest of this procedure; if not, you must upgrade Junos Space Platform to a supported release.
2. Upgrade Junos Space Network Management Platform to 20.3R1. For upgrade steps, see [Junos Space Network Management Platform Upgrade Instructions](#).

NOTE: Make sure that you are running Junos Space Platform Release 19.2R1, Release 19.3R1, Release 19.4R1, or Release 20.1R1. You can upgrade to Junos Space Platform Release 20.3R1 from Junos Space Platform Release 19.2R1, Release 19.3R1, Release 19.4R1, or Release 20.1R1.

If the Junos Space Platform runs a version earlier than Release 17.1R1, you must first upgrade Junos Space Platform to Release 18.1R1. For details about upgrading Junos Space Platform to Release 18.1R1, see [Upgrading to Junos Space Network Management Platform Release 18.1R1](#).

Installing Network Director

IN THIS SECTION

- [Installing Network Director From Junos Space Store | 13](#)
- [Installing Network Director by Manually Downloading the Network Director Application Image | 14](#)

Before you begin:

- Configure a Junos Space Appliance or a Junos Space Virtual Appliance as a Junos Space node or as a specialized node used for fault monitoring and performance monitoring (FMPM). For more information, see [Configuring a Junos Space Appliance as a Junos Space Node](#) for configuring a Junos Space Appliance or see [Configuring a Junos Space Virtual Appliance as a Junos Space Node](#).
- Upgrade Junos Space Platform to Release 20.3R1. For upgrade steps, see “[Upgrading Junos Space Network Management Platform](#)” on page 11.
- Uninstall Connectivity Services Director or Edge Services Director before you install Network Director on your system. Network Director cannot be installed on a system that has Connectivity Services Director or Edge Services Director already installed. For steps to uninstall a Junos Space Application, see [Uninstalling a Junos Space Application](#).

You can install Network Director on Junos Space Network Management Platform by using one of the following methods:

NOTE: OpenNMS is disabled automatically when Network Director is installed in Junos Space Network Management Platform 20.3R1. This is applicable only for a fresh installation.

Installing Network Director From Junos Space Store

Starting Release 18.2R1, Junos Space Platform provides Junos Space store from where you can download and install or upgrade Network Director in a single operation. On the Junos Space store page, you can view the versions of Network Director that are compatible with the currently installed version of Junos Space Platform.

NOTE: Before you install or upgrade Network Director by using Junos Space store, you must configure the credentials to access Junos Space Store. For information see, *Configuring and Managing Junos Space Store*.

To install Network Director from Junos Space Store:

1. Click **Administration > Applications > Junos Space Store**.

The Junos Space Store opens. Junos Space Store lists all the applications that can be installed on the Junos Space Platform.

2. Click **Network Director**.

The right-side of the page lists the Network Director versions that can be installed on Junos Space Platform.

3. (Optional) Select the **Show only compatible version** check box to list only the compatible versions of Network Director that can be installed on the current installed version of Junos Space Platform.

4. Click **Next** to install Network Director.

The end user license agreement page appears.

5. Click **Accept and install** to install Network Director.

The Network Director installation job status appears. The status indicates each step that is completed while Network Director is getting installed.

Once installed successfully, Network Director is listed on the Applications page (**Administration > Applications**).

Installing Network Director by Manually Downloading the Network Director Application Image

Download the Junos Space Network Director Release 4.1R1 software image to the hard disk or to an SCP server. The SCP server where you download the Network Director image should be a Linux server. You can download the Network Director Software image from the [Network Director Download Software](#) page.

To install Junos Space Network Director:

1. Log in to Junos Space.
2. Click the add symbol (+) adjacent to the Administration and click **Applications**.

The Administration > Applications page opens.

3. Click add symbol (+) symbol to add the Network Director application.

The Add Application page opens.

4. You can upload the Network Director release image file by using HTTP or by using SCP:

To upload the image file using HTTP:

- a. Click **Upload via HTTP**.

The Upload Software via HTTP page opens.

- b. Click **Browse** to select the Network Director image file. You can either navigate to the local directory and select the Network Director software image, or copy and paste the download URL in the **Software File** if the image is not already downloaded to the local directory.

Your browser opens a dialog box to browse the Network Director image file.

- c. Click **Open** to download the image file.
- d. Click **Upload** to upload the image file.

A notification about the progress in the upload is displayed.

To upload the image file using SCP if you have a Linux server:

- a. Click **Upload via SCP**.

The Upload Software via SCP page opens.

Enter the following secure copy credentials to upload the image from a remote server to Junos Space.

- Enter the user name of the remote server.
- Enter the password of the remote server and reenter the password in the Confirm Password field.
- Enter the host IP address of the remote server.
- Enter the path of the remote server to which you have copied the Network Director image file.

- b. Click **Upload** to load the Network Director image file into Junos Space.

The Upload Application Job Information dialog opens.

5. Click **OK** to skip viewing the job results and to take you back to the Administration > Applications > Add Application page.

6. Select Network Director and click **Install**.

7. Click **OK** in the Application Configuration window dialog box.

You can check the Job Status page to view the progress of the installation job. Once the installation completes, Network Director appears on the Applications page. The Network Director application also appears in the Application Chooser (at the upper-left corner).

8. (Optional) Bookmark this page in your browser for future use.

You can use the bookmarked URL to log in to Network Director without logging in to Junos Space first.

Upgrading Network Director

You can upgrade to Network Director Release 4.1R1 from the following Network Director releases:

- Upgrading from Network Director 4.0R1
- Upgrading from Network Director 3.9R1

- Upgrading from Network Director 3.8R1
- Upgrading from Network Director 3.7R1

If you do not have a supported version of Network Director, upgrade to Release 3.7R1, 3.8R1, 3.9R1, or Release 4.0R1. For instructions on upgrading to Network Director Releases 3.7R1, 3.8R1, 3.9R1, or 4.0R1, see the following:

- [Network Director Release 3.7 Quick Start Guide](#)
- [Network Director Release 3.8 Quick Start Guide](#)
- [Network Director Release 3.9 Quick Start Guide](#)
- [Network Director Release 4.0 Quick Start Guide](#)

Before you start the upgrade, ensure that you have:

- Disabled monitoring for all categories in the Monitoring tab of the Preferences page. For more details, see [Disabling Data Collection for Monitors](#).
- Taken a back up of your database using the Junos Space backup feature. For more details, see [Executing the Data Back Up Procedure](#).
- Junos Space Release 20.3R1 running on your appliance. If your appliance is running an unsupported release of Junos Space Platform, you must upgrade Junos Space Platform before installing Network Director. For step-by-step instructions on upgrading Junos Space, see [“Upgrading Junos Space Network Management Platform” on page 11](#).

You can upgrade to Network Director Release 4.1R1 either by using the Junos Space Store option under **Administration > Applications** task or by manually downloading the Network Director software image.

To upgrade Network Director by using Junos Space Store, see [“Installing Network Director From Junos Space Store” on page 13](#).

To upgrade Network Director from a previous version by manually downloading the software image:

1. Download the Network Director Release 4.1R1 software image to the hard disk or to an SCP server. You can download the Network Director Software image from the [Network Director Download Software](#) page.
2. Log in to Junos Space Platform.
3. Click the add symbol (+) adjacent to the Administration and click **Applications**.
The Applications page opens.
4. Click add symbol (+) symbol to add the Network Director application.
The Add Application page opens.

5. Select Network Director from the list of installed applications and click **Upgrade Application** from the Actions menu.

6. In the Upgrade Application page, click either **Upload via HTTP** or **Upload via SCP** and navigate to the location where you saved the Network Director image.

To upload Network Director by using HTTP:

- a. Click **Upload via HTTP**.

The Upload Software via HTTP page opens.

- b. Click **Browse** to select the Network Director image file. You can either navigate to the local directory and select the Network Director software image, or copy and paste the download URL in the **File name** if the image is not already downloaded to the local directory.

- c. Click **Open** to download the image file.

- d. Click **Upload** to load the image file into Junos Space.

To upload Network Director by using SCP if you have a Linux server:

- a. Click **Upload via SCP**.

The Upload Software via SCP page opens.

Enter the following secure copy credentials to upload the image from a remote server to Junos Space.

- Enter the user name of the remote server.
- Enter the password of the remote server and reenter the password in the Confirm Password field.
- Enter the host IP address of the remote server.
- Enter the path of the remote server to which you have copied the Network Director image file.

Click **Upload** to load the image file into Junos Space.

The Upload Application Job Information dialog opens.

7. Click **OK** to skip viewing the job results.

8. Select Network Director and click **Upgrade**.

You can check the Job Status page to see the progress of the upgrade job. Once the upgrade completes, Network Director appears on the Applications inventory page. The new or upgraded application also appears in the Application Chooser (at the upper-left corner).

9. (Optional) Bookmark this page in your browser for future use.

You can use the bookmarked URL to log in to Network Director without logging in to Junos Space first.

Uploading DMI Schemas

Junos Space Network Management Platform interfaces with network devices using an open API called the Device Management Interface (DMI), which is a standard interface used by Juniper Networks devices. Each device type is described by a unique data model (DM) that contains all the configuration data of the device. The DMI schema lists all the possible fields and attributes for a type of device. The newer schemas describe the new features coming out with recent device releases. It is important that you load all your device schemas into Junos Space Network Management Platform; otherwise only a default schema is applied when you try to edit a device configuration by using the device configuration edit action in the Devices workspace.

Typically, when you perform a clean installation of Junos Space Platform, a schema (usually the latest one) is automatically set as the default for each device family. If an exact matching schema is not available, the default schema for the device family is used.

For the list of DMI schema that you can obtain and upload in Junos Space before you start working on Network Director 4.1R1 Release, see [Junos Space DMI Schema Requirements for Network Director](#).

If you cannot find the schema equivalent, use the latest DMI schema from the main release or contact the [Juniper Support](#). For example, for an EX4500 switch running Junos OS Release 13.2X51-D20, you must use the Junos OS Release 13.2X51-D20 schema. If this is not available, you can use the latest schema available from the Junos OS Release 13.2X51 releases.

You can download the schema from [Schema Repository](#).

To install or update a DMI schema on Junos Space Platform, see [Adding Missing DMI Schemas or Updating Outdated DMI Schemas by Using the Update Schema Menu](#).

Next Steps

After your devices are up and synchronized, much of the function in Network Director is automatically enabled. However, there are a few additional tasks that you will need to perform to use all the features of Network Director. We suggest that you explore:

- Set up a Location View

Location View is one of seven different views, or perspectives, in your network. In Location View, you can manage devices based on a site. Here you define the buildings, floors, wiring closets, and outdoor areas. You can upload floor maps for easy reference and assign devices to a specific spot.

To set up a Location View:

1. Click **Build** in the Network Director banner.
2. Select **Location View** in the View pane to the left of the screen.
3. Click **Setup Locations** in the Tasks pane to start setting up your location, buildings, floors, racks, wiring closets, and outdoor areas.

- Enable Trap Forwarding and Alarms for Fault Management

A key component of Network Director is to diagnose problems with precision and ease. Network Director correlates multiple traps from the same device to a single alarm.

You must complete device discovery and the devices must be up before you can enable trap forwarding. Traps are not enabled by default; you need to enable them after device discovery.

1. Use **Set SNMP Trap Configuration** in the Tasks pane of Deploy mode to configure your device to send SNMP traps to Network Director.
2. Review the list of alarms in Preferences, located in the Network Director banner. All alarms are enabled by default, but you might want to disable those alarms that are not pertinent to your installation. You can also change the severity of an alarm by using Preferences.

- Set up users

After you install Network Director, there is only one username defined: *super* with the default password, *juniper123*.

You have the ability to set up users with different Network Director privileges. New Network Director users are set up in Junos Space and follow the roles and privileges as defined in Junos Space. For a complete discussion on how to properly set up users, see [Understanding Network Director User Administration](#).

- Configure Network Director API—The Network Director API is a set of Representational State Transfer (REST) APIs that enable network management functions and is installed when you install Network Director. To know more about configuring Network Director API, see [Network Director API Guide](#).

- Learn what you can do with Network Director

There are two ways you can become familiar with the functions and features of Network Director:

- Use the extensive online help system that guides you through Network Director. Clicking the main Help icon provides a top-down view into the help system; clicking a Help icon on a pane or window provides context-sensitive information. Use the help system to familiarize yourself with Network Director and the different modes and panes in the interface.
- Refer to the [Network Director User Guide](#).

Preparing Devices for Management by Network Director

To discover and manage devices, Network Director requires the following minimum device configuration as a prerequisite. Ensure that the device:

- Has a static management IP address. The address can be in-band or out-of-band, but must be reachable from the Junos Space server.
- Is enabled for SSH v2. On wireless LAN controllers, SSH is enabled by default. However, on EX Series switches you need to enable SSH. Issue the **set system services ssh protocol-version v2** command to enable SSH v2 on EX Series switches.
- Has a user ID with the superuser class configured. Junos Space and Network Director uses this user ID to authenticate the SSH connection with the device.
- Is enabled for SNMP with the appropriate read-only V1, V2, and V3 credentials created. You do not need to configure SNMP trap receivers; Network Director configures traps as a deployment task.

In addition, the following protocol ports must be open for Network Director communication:

- Port 22 for SSH connections. If you have changed the SSH port to a port other than port 22 on your Network Management Platform, you must change the SSH ports on your managed devices to the port that the Network Management Platform is using.
- Port 443 for virtualization and RingMaster import support. Use port 443 for outbound traffic to vCenter servers.

NOTE: If your RingMaster server uses any port other than port 443, then you must open that port from the Junos Space Network Management Platform server.

- Port 10162 for SNMP traps. Network Director receives traps from managed devices on this port. (After you install Network Director, use Network Director to configure SNMP on your devices to send traps to Network Director on this port.)
- Port 8889 for the management of wireless LAN controllers.
- Port 21 (TCP) and port 69 (UDP) for uploading the software image and configuration file to the FTP server.
- Ports 8774, 9696, 9292, 8777, 35357, and 8776 for accessing OpenStack and VMware NSX APIs.

You can verify whether a port is open by logging in to the Junos Space CLI and using the **nmap** command. For example, to determine whether port 8889 is open on a controller, issue this command:

```
root@space# nmap <IP address of controller> -p 8889
```

Discovering Devices

When you start Network Director for the first time, the system does not have any devices. The first step is to build your network. Even with large networks, Network Director has made this step relatively easy and straightforward. You will add devices to Network Director and the database by using a process called *device discovery*. Once a device is discovered, it shows in the interface and Network Director begins to monitor the device.

Network Director provides a wizard for device discovery. The following example shows the path for device discovery through the wizard. For an alternate path, you can get a step-by-step instruction from the help system.

In this example, we provide an IP address range, and Network Director populates the database with all supported devices within that range.

1. While in the **Build** mode, select **Logical View**, **Location View**, **Device View**, or **Custom Group View** from the View selector.

NOTE: Select **Datacenter View** if you want to view and manage data centers by using Network Director. You must set up a data center from the Datacenter View. Network Director automatically discovers and adds devices that are part of the data center set up to its inventory. There is no separate device discovery task for the Datacenter View. You can also add devices that are discovered from the other views to a data center by editing a data center in the Datacenter View.

2. To discover physical devices, click **Discover Devices** in the Tasks pane. Each mode has a Tasks Pane that displays the actions you can take while in that mode and that particular network view.
3. (Optional) Type a name for the discovery job. The default name is ND Discovery.
4. 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. In this example, we select an IP address range.
5. Provide the initial or the lowest IP address value and the ending or highest IP address value for the range and click **Add**. You can have up to 1024 devices in a range. After you click Add, the address range is listed in the Device Targets window.
6. Click **Next** or click **Discovery Options** to proceed to specify the device credentials and method of discovery.
7. Click **Add** in the Device Credentials window and enter the username and password assigned for administrative access.
8. Select **Ping**, **SNMP**, or both as the method of device discovery. Selecting both is the preferred method if the device is configured for SNMP.

If you select SNMP, the Add SNMP Settings dialog box is displayed. In this example, because we run SNMP version 2, we need to provide the community string. Click **Add** to save the setting.

NOTE: You cannot choose a method for device discovery for virtual network discovery.

9. Click **Next** or **Schedule Options** to proceed to schedule the time when discovery is run.

NOTE: Scheduling options are not available for virtual network discovery.

10. Indicate whether to run the device discovery now or set up a schedule to minimize network traffic. In this example, we set the schedule to run during off hours.
11. Click **Review** to review the settings before you exit the wizard.
12. Click **Finish** to complete the discovery setup and to save the settings.
13. Click **View Discovery Status** to view all scheduled and completed jobs. After a job completes, you can click **Show Details** to view further information on any unexpected results.

2

CHAPTER

Installing Data Learning Engine

Installing and Configuring Data Learning Engine for Network Director | 25

Installing and Configuring Data Learning Engine for Network Director

IN THIS SECTION

- [Installing DLE | 25](#)
- [What to Do Next | 29](#)

Data Learning Engine (DLE) enables Network Director to collect and analyze high-frequency statistics and sFlow data for devices that are managed by Network Director. Only the QFX Series devices support the analytics feature that is required for generating high-frequency statistics data. Network Director uses high-frequency statistics data to create network heat maps and to monitor latency in QFX devices and sFlow data to monitor network traffic in EX and QFX devices.

This topic contains the following sections:

Installing DLE

DLE runs on a dedicated CentOS server. You can install DLE either directly on a CentOS server or on a virtual machine (VM) that runs CentOS. Following are the system requirements to install DLE:

- The server or the VM on which you install DLE must have:
 - CentOS version 6.10, 64 bit or CentOS version 7.6, 64 bit
 - 16 GB RAM
 - 8 CPUs
 - 100 GB of hard disk space
- The Network Director server, the DLE server, and all the devices that are to be monitored using the analytics feature must be connected over a network, and have the following system time configurations:
 - Configured with the same time zone.
 - System clocks synchronized with a Network Time Protocol (NTP) server.

Before you install DLE make sure you have:

For CentOS Version 6.10

- Verified that CentOS version 6.10 is installed on the server as shown in the following example:

```
[root@user ~]# rpm --query centos-release  
centos-release-6-10.el6.centos.11.1.x86_64
```

Or

```
[root@user ~]# lsb_release -d  
Description: CentOS release 7.6 (Final)
```

For CentOS Version 7.6

- Verified that CentOS version 7.6 is installed on the server as shown in the following example:

```
[root@user ~]# rpm --query centos-release  
centos-release-7-6.1810.2.el7.centos.x86_64
```

Or

```
[root@user ~]# grep OS /etc/centos-release  
CentOS Linux release 7.6.1810 (Core)
```

- Synchronized the time on the DLE server, Network Director server, and the devices using a common NTP server as shown in the following example:

```
[root@user log]# ntpdate -u ntp.example.net  
13 Jan 12:51:02 ntpdate[11386]: adjust time server 192.0.2.1 offset -0.101819  
sec
```

NOTE: You can either specify the domain name/host name or IP address of the server.

NOTE: Juniper Networks recommends that you use an NTP server to synchronize the time between DLE, Network Director, and devices. However, if you do not use an NTP server, you need to synchronize the time manually.

- Verified that the network ports 8080, 4242, 50005, 8282, 8081, 50006, 50009, 9160, 7000, and 9042 are in listening mode by entering the **netstat -anp | grep <port number>** command as shown in the following example:

```
[root@user] # netstat -anp | grep 8282
```

```
tcp        0      0 0.0.0.0:8282          0.0.0.0:*             LISTEN
           1839/java
```

Alternatively, you can disable firewall on the DLE server to make sure that all the network ports are accessible as shown in the following example:

```
[root@user log]# service iptables stop
```

```
iptables: Setting chains to policy ACCEPT: filter      [ OK ]
iptables: Flushing firewall rules:                    [ OK ]
iptables: Unloading modules:                          [ OK ]
```

- Noted down the CentOS server IP address for configuring DLE in Network Director.

To install DLE:

1. Download the DLE RPM package version 14.1X53-D30 or later from the [Cloud Analytics Engine software download page](#) to your CentOS server.

The RPM file name has the following format:

dle-all-release-identifier.x86_64.rpm—for example, **dle-all-14.1X53-D30.1.x86_64.rpm**

2. Install the DLE RPM package on the CentOS server.

If you have downloaded the DLE RPM package to the tmp folder and you are installing the DLE package from the same (tmp) location, enter the command as shown in the following example:

```
[root@user tmp]# rpm -ivh dle-all-14.1X53-D30.1.x86_64.rpm
```

If you have downloaded the DLE RPM package to the tmp folder and you are installing the DLE package from a different location, enter the command as shown in the following example:

```
[root@user]# rpm -ivh /tmp/dle-all-14.1X53-D30.1.x86_64.rpm
```

A successful installation displays the output as shown in the following example:

```
warning: dle-all-14.1X53-D30.1.x86_64.rpm: Header V3 RSA/SHA256 Signature, key
ID dc466ab6:
NOKEY
Preparing...                               ##### [100%]

1:dle-all                                ##### [100%]
Starting Cassandra DB: [ OK ]
Starting KairosDB:      [ OK ]
Starting Data Learning Engine: [ OK ]
Starting cae monitor [ OK ]
```

3. Verify the status of DLE and the database processes by entering the service status commands as shown in the following example:

- [root@user]# service cassandra status

```
cassandra (pid 1483) is running...
```

- [root@user]# service kairosdb status

```
kairosdb (pid 1779) is running...
```

- [root@user]# service dle status

```
dle (pid 1862) is running...
```

4. Verify the DLE version installed on the CentOS server as shown in the following example:

```
[root@user]# rpm -qa |grep dle
```

```
dle-all-14.1X53-D30.1.x86_64
```

NOTE: You can view the DLE log file at `/opt/cae/dle/log/dle.log` file.

You can run the following commands to view the DLE log file:

```
[root@user tmp]# cd /opt/cae/dle/log
[root@user log]# tail -f dle.log
```

What to Do Next

After you have installed DLE on the CentOS server, you must perform the following operations to identify the applications that contribute to the traffic, traffic statistics, and the top applications:

- [Configuring the DLE IP in Network Director](#)
- [Enabling the high-freq statistics on the devices](#)
- [Enabling the network traffic analysis](#)
- [Viewing the traffic on a device](#)