Release Notes: Junos Space Security Director Release 16.2R1

21April 2017
Revision 3

Contents

Introduction

Junos Space is a comprehensive network management solution that simplifies and automates management of Juniper Networks switching, routing, and security devices.

Junos Space Management Applications optimize network management by extending the breadth of the Junos Space solution for various domains in service provider and enterprise environments.

Release Notes for Junos Space Security Director

The Junos Space Security Director application is a powerful and easy-to-use solution that lets you secure your network by creating and publishing firewall policies, IPsec VPNs, NAT policies, IPS policies, and application firewalls.

NOTE: **You need IPS and application firewall licenses to push IPS and application firewall signatures to a device.**

Supported Platforms

Security Director Release 16.2R1 is supported on the following hardware devices:

- SRX100
- SRX110
- SRX210
- SRX220
- SRX240
- SRX240H
- SRX300
- SRX320

- SRX320-POE
- SRX340
- SRX345
- SRX550
- SRX550M
- SRX650
- SRX1400
- SRX1500
- SRX3400
- SRX3600
- SRX4100
- SRX4200
- SRX5400
- SRX5600
- SRX5800
- MX240
- MX480
- MX960
- MX2010
- MX2020
- LN1000-V
- LN2600
- Kernel-based virtual machine (KVM) server installed on CentOS Release 7.2.1511
- Juniper Secure Analytics (JSA) as Log Collector on JSA Release 2014.8.R4 or later
- QRadar as Log Collector on QRadar Release 7.2.8 or later

Supported Junos OS Releases

- Security Director Release 16.2R1 supports the following Junos OS branches:
  - 10.4
  - 11.4
  - 12.1
  - 12.1X44
  - 12.1X45
  - 12.1X46

  - 12.1X47
  - 12.3X48
  - 15.1x49
  - vSRX 15.1x49
  - 16.1R3-S1.3

- SRX Series devices require Junos OS Release 12.1 or later to synchronize the Security Director description field with the device.
- The logical systems feature is supported on devices running Junos OS Release 11.4 or later.

NOTE: Before you can manage an SRX Series device using Security Director, we recommend that you have the exact matching Junos OS schema installed on the Junos Space Network Management Platform. If there is a mismatch, a warning message is displayed during the publish preview workflow.

Supported Browsers

Security Director Release 16.2R1 is best viewed on the following browsers:

- Mozilla Firefox
- Google Chrome
- Microsoft Internet Explorer 11

Installation and Upgrade Instructions

This section contains the procedures to upgrade Junos Space Security Director and Log Collector.

- Adding Log Collector to Security Director on page 20
- Removing Security Director Log Collector and Adding JSA as a Log Collector on page 22

Installing Junos Space Network Management Platform

Junos Space Security Director Release 16.2R1 is supported only on Junos Space Network Management Platform Release 16.1R2.

CAUTION: Ensure that all data on the node is backed up to a remote server before you install the Junos Space Platform Release 16.1R2 software image as part of the upgrade procedure from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R2. Existing data on the node is deleted when you install Junos Space Platform Release 16.1R2.

To upgrade from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R2, you must follow the procedure outlined in Upgrading to Junos Space Network Management Platform Release 16.1R1.

NOTE: The procedure described for the upgrade from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R1 in Upgrading to Junos Space Network Management Platform Release 16.1R1 is also applicable for the upgrade from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R2.

As part of an initial configuration, you are prompted to choose the backup tgz location to restore the previous version of the Network Management Platform release. Click **N** to continue with the fresh installation of the Network Management Platform.

- For more information on the virtual appliance installation, see Junos Space Virtual Appliance Deployment Overview.

  Download the VISO image for the VM.

- For more information on the appliance installation, see Junos Space Appliance Overview.

  Download the USB image for the JA2500 appliance.

Installing Security Director Release 16.2R1

In Junos Space Security Director Release 16.2R1 a single image installs Security Director, Log Director, and the Security Director Logging and Reporting modules. Installing the Security Director Release 16.2R1, image installs all three applications. You must deploy the Log Collector and then add it to the Junos Space Network Management Platform fabric to view the log data on the Dashboard, Events and Logs, Reports, and Alerts pages.

For more information on adding Junos Space applications, see Adding a Junos Space Application.

Upgrading Security Director Prerequisites

Before you upgrade the Security Director, Log Director, and Security Director Logging and Reporting modules, you must upgrade to Junos Space Network Management Platform Release 16.1R2.

Follow this upgrade sequence if your current Security Director release is earlier than Security Director Release 15.2:

- Upgrade to Junos Space Network Management Platform Release 15.2R1 and Security Director Release 15.2R1.
- Upgrade to Junos Space Network Management Platform Release 15.2R2 and Security Director Release 15.2R2.
- Upgrade to Junos Space Network Management Platform Release 16.1R2 and Security Director Release 16.2R1.

Upgrading Security Director

NOTE: **If you are upgrading from a previous version of Security Director, clear your browser cache before accessing the Security Director UI.**

To upgrade from a previous version of Security Director to Security Director Release 16.2R1:

1. Download the 16.2R1 file from here.
2. Select **Administration** > **Applications** > **Security Director**. Right-click and select **Upgrade Application**.

   Upload the image using either the **Upload via HTTP** or **Upload via SCP** option.
3. Click **Upgrade**.

   After adding the secondary node under Administration > Fabric, you must manually perform the device load balancing.

   The Job Management tab shows the upgrade status.

If you are upgrading from Security Director Release 15.2R2 to Security Director Release 16.2R1, perform the following steps:

1. Take the back up of Security Director Release 15.2R2.
2. Install Junos Space Network Management Platform Release 16.1R2, and restore the back up.
3. Once the Network Management Platform is up, select **Administration** > **Applications** > **Security Director** and upgrade Security Director to Security Director Release 16.2R1.

NOTE: In Junos Space Security Director Release 16.2R1, all IPS report definitions are consolidated into a single report definition called IPS Report. After upgrading Security Director to 16.2R1, IPS reports for already scheduled IPS report definitions will not be generated because, the individual IPS report definitions does not exist. You must use the consolidated IPS report.

Upgrading Log Collector VM and Integrated Log Collector

NOTE: Before executing the database back up procedure in Junos Space Network Management Platform Release 15.2R2 and Security Director Release 15.2R2, you must delete all the Log Collector nodes from Security Director > Administration > Logging Management > Logging Nodes.

Table 1 on page 8 shows the topology difference between Log Collector Releases 15.2R2, 16.1R1, and 16.2R1 before the upgrade.

Table 1: Understanding the Topology Difference Before Upgrading

Node Type	15.2R2	16.1R1	16.2R1
All-in-One	Yes	Yes	Yes
Log receiver	Yes	Yes	Yes
Log storage	Yes (Log Indexer node and Log Data node)	Yes	Yes
Query node Client node	Yes (20K eps)	No	No
Master node Cluster Manager node	Yes (20K eps)	No	No
Integrated	No	Yes	Yes

In Log Collector Release 16.2R1:

- There can be only one All-in-One node in a deployment and it is a single node deployment.
- Multinode deployment is a combination of log receiver and log storage nodes. You can add a maximum of one log receiver node and three log storage nodes.
- Only one log receiver node is supported for all levels of deployment. If you have multiple log receivers in the Release 15.2R2 setup, upgrade only one log receiver to Release 16.2R1 and delete the other log receivers.
- Log query node and master node are not supported. Delete them in the Release 15.2R2 setup.
- You must delete all the unsupported nodes from Security Director > Administration > Logging Management > Logging Nodes.
- You must run the upgrade script on each of the applicable node to upgrade the nodes to Release 16.2R1.

To upgrade from Log Collector Release 16.1R1 to Log Collector Release 16.2R1:

1. If the log password was changed for the logging nodes in Log Collector Release 15.2R2, perform the following steps. Otherwise, continue to Step 2.
   - Use the **ssh** command to open a connection to Log Query node (Indexer node) or All-in-One node.
   - Edit the **elasticsearch.yml** file, located at vi/etc/elasticsearch/.
   - In the elasticsearch.yml file, search for http.basic.password and replace the changed password with *58dd311734e74638f99c93265713b03c391561c6ce626f8a745d1c7ece7675fa*.
   - Save the changes.
2. Download the Log Collector upgrade script from here.
3. Copy the upgrade script to the /root path of all the applicable nodes that you want to upgrade.
4. Run the **sh Log-Collector-Upgrade-16.2R1.XXX** script.

   The status of the upgrade is shown on the console.

   NOTE:
   - The **Logstash** process does not run on the log receiver node any longer. Instead the **jingest** process will run.
   - You must ensure that the **jingest** and **elasticsearch** processes are running.
5. Add the logging nodes back to Security Director from Security Director > Administration > Logging Management > Logging Nodes.

Upgrading Integrated Log Collector

- Upgrade the Junos Space Network Management Platform Release 16.1R2 from here.
- Upgrade the Junos Space Security Director Release 16.2R1 from here.

To upgrade from integrated Log Collector Release 16.1R1 to integrated Log Collector Release 16.2R1:

1. Download the integrated Log Collector image Integrated-Log-Collector-16.2.R1.xxx.sh from here.
2. Copy the integrated Log Collector script to a JA2500 appliance or virtual appliance.
3. Connect to the CLI of a JA2500 appliance or virtual appliance with admin privileges.
4. Navigate to the location where you have copied the integrated Log Collector script.
5. Install the integrated Log Collector script using the following command: **sh Integrated-Log-Collector-16.2.R1.xxx.sh**.

   The integrated Log Collector is successfully upgraded to Log Collector Release 16.2R1.

NOTE:

- The integrated Log Collector does not support high availability (HA) even if it is installed in a Junos Space HA cluster. The integrated Log Collector must be installed only on one of the Junos Space cluster nodes.
- 500 eps is supported for the integrated Log Collector.

Deploying Log Collector

System Requirement

Table 2 on page 10 and Table 3 on page 11 provide the virtual machine (VM) configuration that is recommended for the log collection to work effectively.

Table 2: With SSD Drives

Setup	Number of Nodes (Log Receiver Nodes)	CPU (Log Receiver Nodes)	Memory (Log Receiver Nodes)	Number of Nodes (Log Storage Nodes)	CPU (Log Storage Nodes)	Memory (Log Storage Nodes)	Total Nodes
4K events per second (eps)	1	4	16 GB	-	-	-	1
10K eps	1	8	32 GB	1	8	64 GB	2
20K eps	1	8	32 GB	2	8	64 GB	3

Table 3: With Non-SSD Drives

Setup	Number of Nodes (Log Receiver Nodes)	CPU (Log Receiver Nodes)	Memory (Log Receiver Nodes)	Number of Nodes (Log Storage Nodes)	CPU (Log Storage Nodes)	Memory (Log Storage Nodes)	Total Nodes
3K eps	1	4	16 GB	-	-	-	1
10K eps	1	8	32 GB	2	8	64 GB	3
20K eps	1	8	32 GB	3	8	64 GB	4

NOTE: VMs with 64-GB memory provides better stability for the log collection.

Table 4 on page 11 includes supported node types in which the Log Collector can be deployed.

Table 4: Log Collector Deployment Nodes

Node Type	Description
All-in-One node (combined deployment)	• Both receiver and storage nodes run on the same VM or JA2500 appliance. • Supports up to 3000 eps with spinning disks and 4000 eps with SSD drives. • Suitable for demos and small-scale deployments.
Log Receiver node (Distributed deployment)	This node receives syslogs from SRX Series devices. SRX Series devices must be configured with the Log Receiver node IP address to send syslogs. Upon configuration, this node parses and forwards logs to the Log Storage Node. You must provide the IP address of the Log Storage node while configuring this node.
Log Storage node (Distributed deployment)	This node analyzes, indexes, and stores syslogs. It receives the syslogs from Log Receiver node.

NOTE: You cannot edit the settings of virtual machines using hardware version 10 or earlier, using vSphere Client version 5.5 or earlier. For more details, see VMware Knowledge Base.

Storage Requirements

The total storage required for retaining *X* number of days at a given eps rate is:

eps * 0.155 * *X* = (in GB)

For example, the storage requirement for 7 days at 500 eps is 500 * 0.155 * 7 = 542 GB, with a +20% margin. The storage space is allocated and equally distributed to the Log Indexer nodes.

NOTE: The logs are rolled over in the following scenarios:

- Time-based rollover—Logs that are older than 45 days are automatically rolled over, even if the disk space is available.
- Disk size-based rollover—Older logs are rolled over when the disk size reaches 400 GB.

Deploying Log Collector VM on a KVM Server

Before You Begin

The prerequisites to deploy a Log Collector on a KVM server are as follows:

- Knowledge about configuring and installing a KVM server.
- The KVM server and supported packages must be installed on a machine running CentOS with the required kernels and packages. See http://wiki.centos.org/HowTos/KVM.
- The Virtual Machine Manager (VMM) client must be installed on your local system.
- The bridge interface must be configured according to your environment and you must have at least two static IP addresses that are unused.

NOTE: You can deploy the Log Collector virtual appliance on a KVM server by using virtual machine clients other than VMM. However, Juniper Networks does not provide support for installing the Junos Space virtual appliance using clients other than VMM.

To deploy Log Collector virtual machine (VM) on a KVM server:

1. Download the Log Collector KVM image from the Download Site on the KVM host and extract the tgz file, which contains the **system.qcow2** and **data.qcow2** files.

2. Launch the VMM client by typing **virt-manager** from your terminal or you can search from the System Tools menu.

3. Select **File > New Virtual Machine** to install a new virtual machine.

   The new VM dialog box appears and displays Steps 4 to 8.

4. Select **Import existing disk image** and click **Next**.

5. Click **Browse** and then select the **system.qcow2** file.

6. Select **Linux** as the operating system and the versions as **Red Hat Enterprise Linux 6.6 or later**.

7. Click **Forward**.

8. Set CPU settings as **4**, and then select or enter the memory (RAM) value as **16,384** MB (minimum).

9. Click **Forward**.

10. Edit the Name field, select or set up the network for each bridge or interface configured, and select the **Customize Configuration Before Install** option.

11. Click **Finish**.

12. Select the Storage option from the left navigation on the Add New Virtual Hardware window, and then click **Add Hardware**.

13. On the Storage window:
    - Select **Select managed or other existing storage** and choose the **data.qcow2** file.
    - Select the storage format as **qcow2** under Advanced Options.
    - Click **Finish**.

14. Click **Begin Installation** to start the Log Collector VM.

15. After the installation, you can configure the IP address, name server, and time zone.

Add Log Collector Node to Security Director

To add Log Collector to Security Director, see *Adding Log Collector to Security Director*.

Deploying Log Collector VM on an ESX Server

To deploy the Log Collector on an ESX server:

1. Download the latest Log Collector open virtual appliance (OVA) image.

2. Using vSphere or vCenter, deploy the Log Collector OVA image Log-Collector-16.21R1.ova onto the ESX server.

3. Edit the CPU and memory as per the system requirement for the required events per second (eps).

   NOTE: Log Collector virtual machine (VM) contains a Virtual Appliance Management Infrastructure (VAMI) agent. The agent enables the VM to use the required server configuration from the ESX server.

4. Power on the Log Collector VM.

   A configuration script lets you choose the node type and configure the network settings.

5. Use the default credentials to log in to Log Collector. The username is **root** and the password is **juniper123**

6. Change the root password of the VM.

7. Deploy Log Collector as the desired node.

8. Configure your network settings.

Add Log Collector Node to Security Director

To add Log Collector to Security Director, see *Adding Log Collector to Security Director*.

Installing Log Collector on the JA2500 Appliance Using a USB Flash Drive

To install the Log Collector on the JA2500 appliance using a USB flash drive, you must create a bootable USB flash drive, install the Log Collector node using the USB flash drive, and add the Log Collector node to Security Director.

Create a Bootable USB Flash Drive

Before creating a bootable USB flash drive, download and install the Rufus utility on your system.

1. Plug the USB storage device into the USB port of a laptop or PC.

2. Download the Log collector ISO image from here.

If you are using a computer with Microsoft Windows as the operating system, follow these steps to create a bootable USB flash drive:

1. Open the Rufus utility installed on your computer.

   The Rufus window opens.

2. From the Device list, select the USB storage device.

3. In the Format Options section, select the ISO image downloaded in Step 2. To select the ISO image, click the open or browse icon next to the Create a bootable disk using option.

4. Click **Start**.

   A progress bar on the Rufus page indicates the status of the bootable USB flash drive. A success message is displayed once the process completes successfully.

5. Click **Exit** to exit the window.

6. Eject the USB storage device and unplug it from the computer.

If you are using a computer with Linux as the operating system, follow these steps:

NOTE: **While you can use any of the available tools, we recommend that you use the dd command in Linux to create a bootable USB drive.**

1. Open a shell prompt.

2. Use the **cd** command to navigate to the directory containing the software image file.

3. Type the **[user@host ~]$ dd if=Log-collector-version.spinnumber.img of=/dev/usb-drive** command to copy the image file to the USB drive and press Enter.

   Log-Collector-version.spin-number.img is the name of the downloaded Junos Space image file, and /dev/usb-drive is the name of the device drive to which your USB drive is mapped. The image file is copied to the USB drive and you are directed to the command prompt.

4. Eject the USB drive and unplug it from the computer.

Install Log Collector Using USB Flash Drive

1. Plug the USB storage device into the USB port of the JA2500 appliance.

2. Follow these steps to access the JA2500 appliance boot menu:

   a. Power on the JA2500 appliance.

   b. As the JA2500 appliance powers on, press the key mapped to send the DEL character in the terminal emulation utility.

   NOTE: **Typically, the Backspace key is mapped to send the DEL character.**

   c. The boot menu appears after a few minutes.

3. Ensure that the USB boot is at the top of the appliance boot-priority order.

   If USB KEY: CBM USB 2.0 - (USB 2.0) is not at the top of the list, follow these steps:

   a. Use the Down Arrow key to select USB KEY:CBM USB 2.0- (USB 2.0), and use the + key to move the entry to the top of the list.

   b. Press the F4 key to save your changes and exit the BIOS setup.

4. Verify the BIOS setting, and then power off the JA2500 appliance.

5. Power on the appliance again. The boot menu displays the following options:

   a. Install Log Collector on Juniper JA2500 Hardware

   b. Boot from local drive

6. Select **Install Log Collector on Juniper JA2500 Hardware**.

7. Power off the appliance once the installation is completed.

8. Restart the appliance and select **Boot from local drive**.

9. Use the default credentials to log in to the JA2500 appliance; username is **root** and password is **juniper123**.

10. Change the default root password when prompted.

11. After logging in, select the desired node type.

12. Configure the IP address and gateway.

13. Configure settings for the DNS name server and the NTP server.

Add Log Collector Node to Security Director

To add Log Collector to Security Director, see *Adding Log Collector to Security Director*.

Installing Integrated Log Collector on a JA2500 Appliance or Junos Space Virtual Appliance

Before You Begin

The prerequisites to install the integrated Log Collector on a JA2500 appliance or virtual machine (VM) are as follows:

- Install the Junos Space Network Management Platform Release 16.1R2 image on a JA2500 appliance or VM from here.
- Install the Junos Space Security Director Release 16.2R1 image on a JA2500 appliance or VM from here.
- Integrated Log Collector uses the 9200, 514, and 4567 ports.
- The Junos Space Network Management Platform must be configured with Ethernet Interface eth0 and management IP addresses.
- OpenNMS must be disabled on the Junos Space Network Management Platform.

- The Ethernet Interface eth0 on the Junos Space platform must be connected to the network to receive logs.
- /var should have a minimum of 500-GB HDD for the integrated Log Collector installation to complete.

NOTE: **Security Director Logging and Reporting is not supported on a JA1500 appliance.**

Specifications

Table 5 on page 17 shows the specifications for installing the integrated Log Collector on a JA2500 appliance.

Table 5: Specifications for Installing an Integrated Log Collector on a JA2500

Component	Specification
Memory	8 GB Log Collector uses 8 GB of memory of the available 32-GB system RAM.
Disk space	500 GB This is used from the existing JA2500 appliance disk space.
CPU	Single core

NOTE: **These specifications are used internally by the integrated Log Collector on a JA2500 appliance.**

Table 6 on page 17 shows the specifications for installing the integrated Log Collector on Junos Space Virtual Appliance.

Table 6: Specifications for Installing an Integrated Log Collector on a VM

Component	Specification
Memory	8 GB If the integrated Log Collector is running on the Junos Space VM, we recommend adding 8 GB of RAM to maintain the Junos Space performance. It uses 8 GB of system RAM from the total system RAM.
Disk space	500 GB Minimum 500 GB is required. You can add any amount of disk space.
CPU	2 CPUs of 3.20 GHz

NOTE: These specifications are used internally by the integrated Log Collector running on the Junos Space Virtual Appliance.

To install the integrated Log Collector on a JA2500 appliance or virtual appliance:

1. Download the integrated Log Collector image Integrated-Log-Collector-16.2.R1.xxx.sh from here.
2. Copy the integrated Log Collector script to a JA2500 appliance or virtual appliance.
3. Connect to the CLI of a JA2500 appliance or virtual appliance with admin privileges.
4. Navigate to the location where you have copied the integrated Log Collector script.
5. Change the file permission using the following command: **chmod +x Integrated-Log-Collector-16.2.R1.xxx.sh**.
6. Install the integrated Log Collector script using the following command: **sh Integrated-Log-Collector-16.2.R1.xxx.sh**.

   The installation stops if the following error message is displayed while installing the integrated Log Collector on the VM. You must expand the Network Management Platform disk size to proceed with the installation.

   ```
   [root@space-005056b40fef ~]# sh Integrated-Log-Collector-16.2.R1.xxx.sh
   ERROR: Insufficient HDD size, Please upgrade the VM HDD size to minimum 500 GB to install Log Collector
   ```

   To expand the hard disk size for the Junos Space VM:

   1. Add a hard disk with a 500-GB capacity on the Junos Space VM using the vSphere client.
   2. Connect to the console of Junos Space through SSH.
   3. Select **Expand VM Drive Size**.
   4. Enter the admin password and expand /var with 500 GB.
   5. Once /var is expanded, you are prompted for any further HDD expansion. Select **No** and the system reboots.

NOTE: **Junos Space Network Management platform must be active and functioning. You must be able to log into the Junos Space Network Management Platform and Security Director user interfaces before attempting to run the integrated Log Collector setup script again.**

6. After the disk size is expanded and Junos Space Network Management Platform and Security Director user interfaces are accessible, run the **sh Integrated-Log-Collector-16.2.R1.xxx.sh** command.

   The installation stops if the following error message is displayed while installing the integrated Log Collector on the JA2500 appliance or VM. You must disable OpenNMS by following the steps mentioned in the error message to proceed with the installation.

   ```
   [root@space-005056b41440 ~]# sh Integrated-Log-Collector-16.2.R1.157.sh
   ```

   ```
   ERROR: Opennms is running...
   Please try to disable opennms as described below or in document and retry Log Collector installation...
   STEPS: Login to Network Management Platform --> Administration --> Applications
   Right Click on Network Management Platform --> Manage Services --> Select Network Monitoring and click Stop
   Service Status should turn to Disabled
   ```

   After OpenNMS is disabled, run the **sh Integrated-Log-Collector-16.2.R1.xxx.sh** command.

When the integrated Log Collector is installed on the JA2500 appliance or VM, the following message is displayed:

```
Shutting down system logger: [ OK ]
Starting jingest ... jingest started.
{"log-collector-node": {"id":376,"ip-address":"x.x.x.x","priority":0,"node-type":
"INTEGRATED","cpu-usage":0,"memory-usage":0, "fabric-id":0,"display-name":
"Integrated","timestamp":0}}
```

Once the installation is complete, a logging node is automatically added in Administration > Logging Management > Logging Nodes.

Configuring Log Collector Using Scripts

If you have used the standard setup menu to configure Log Collector, then you can use the script described in Table 7 on page 20 to reconfigure it.

```
“jnpr-” <TAB>
[root@NWAPPLIANCE25397 ~]# jnpr- jnpr-configure-node jnpr-configure-ntp
jnpr-configure-timezone jnpr-network-script healthcheckOSLC
```

Table 7: Description of the Log Collector Script

Script	Description
jnpr-configure-node	Master script for the node configuration and network settings.
jnpr-configure-ntp	Script for NTP configuration.
jnpr-configure-timezone	Script for time zone configuration.
jnpr-network-script	Script for interface configuration.
healthcheckOSLC	Script for checking the issues with logging infrastructure.

Adding Log Collector to Security Director

You must deploy either Security Director Log Collector or Juniper Secure Analytics (JSA) as a log collector and then add it to Security Director to view the log data in the Dashboard, Events and Logs, Reports, and Alerts pages.

Before You Begin

- Configure system log and security logging configuration from **Devices** > **Security Devices** > **Modify Configuration**.
- Security Director Log Collector is supported on both the VM and JA2500 appliance.
- For information on JSA, see Juniper Secure Analytics documentation.

To add Log Collector to Security Director:

1. From the Security Director user interface, select **Administration** > **Logging Management** > **Logging Nodes**, and click the plus sign (+).

   The Add Logging Node page appears.

2. Choose the Log Collector type as Security Director Log Collector or Juniper Secure Analytics.

   If you select the Log Collector type as Security Director Log Collector, then select the deployment.

3. Click **Next**.

4. Provide the root credentials for the Security Director Log Collector node. For JSA, provide the admin credentials that is used to login to the JSA console.

5. Verify the corresponding job status.

   The Log Collector node appears in the Logging Nodes page with the status UP.

6. Complete the configuration for Add Collector/JSA Node.

7. If the Log Collector type is Security Director Log Collector, then Add Another Node is displayed to add multiple nodes as needed.

8. Click **Next**.

   The certificate details are displayed.

9. Click **Finish**.

10. Review the summary of configuration changes from the summary page and click Edit to modify the details, if required.

11. Click **OK** to add the node.

    A new logging node with your configurations is added. To verify if the node is configured correctly, click **Logging Management > Logging Nodes** to check the status of the node.

NOTE:

- JSA node sends many maintenance logs from its own IP address to localhost (127.0.0.1). These system logs are displayed in the Event Viewer page. You can disable these maintenance logs.

  To disable the maintenance logs:

  1. Log in to the JSA console.
  2. Select Admin > Routing Rules.
  3. Add a rule: Destination IP - Equals - 127.0.0.1
  4. Select the Drop routing option.
  5. Uncheck the Forward routing option.
  6. Click Save.

- The status, application, version, and last boot time are not displayed for the JSA node.
- The Log Forwarding and Change Log Password options are not available for the JSA node.
- The statistics and troubleshooting information is not displayed for the JSA Node.

Removing Security Director Log Collector and Adding JSA as a Log Collector

To remove the existing Security Director Log Collector and add JSA as a Log Collector:

1. Select **Administration** > **Logging Management** > **Logging Nodes**.

2. Select the existing Security Director Log Collector and click the delete icon to delete Security Director Log Collector node.

   This removes the Security Director Log Collector.

3. Click the **+** icon to add JSA as a Log Collector.

   You can either add All-in-One node for the standalone deployment, or Console node for the distributed deployment.

4. You must configure the SRX Series devices to stop sending logs to Security Director Log Collector, and ensure that logs are sent to the JSA node.

Loading Junos OS Schema for SRX Series Releases

You must download and install the matching Junos OS schema to manage SRX Series devices. To download the correct schema, under the Network Management Platform list, select **Administration** > **DMI Schema**, and click **Update Schema**. See Updating a DMI Schema.

Management Scalability

The supported management scalability is:

- The VM setup must have 32 GB of RAM and must stop running OpenNMS (in a single or a two-node fabric). Security Director supports 15K firewall rules per policy. In concurrent cases, a maximum of 40K firewall rules per policy can be processed at a time with different publish, preview, and update jobs (in a two-node VM or a JA2500 fabric setup).
- By default, the monitor polling is set to 15 minutes and resource usage polling is set to 10 minutes. This polling time changes to 30 minutes for a large-scale data center setup such as one for 200 high-end SRX Series devices managed in Security Director.

  NOTE: You can manually configure the monitor polling on the Administration > Monitor Settings page.

- Security Director supports a maximum of 10K SRX Series devices in a six-node Junos Space fabric (four JBoss servers and two database nodes). In a 10K SRX Series setup, all settings for monitoring polling must be set to 60 minutes. If monitoring is not required, disable it to improve your publish or update job performance.

- To improve the performance further, increase the Update sub-jobs thread number in the database. To increase the Update sub-jobs thread in the database, run the following command:

  ```
  #mysql -pnetscreen
  mysql> update RuntimePreferencesEntity SET value=20 where
  name='UPDATE_MAX_SUBJOBS_PER_NODE';
  mysql> exit
  ```

- Security Director supports 100K firewall rules concurrently with delta publish and update.

  The following system configuration is required for delta publish and update support:

  - Two-node Junos Space fabric VM. The VM must have an SSD hard disk with 32 GB of RAM.
  - The OpenNMS must be stopped in the setup. You must restart the JBoss application after stopping OpenNMS.

  NOTE: **If you use the database dedicated setup (SSD hard disk VMs) for this deployment, the performance of publish and update is better compared with the normal two-node Junos Space fabric setup.**

New and Changed Features

This section describes the new features and enhancements to existing features in Junos Space Security Director Release 16.2R1.

- **MX Series firewall capability support**—Security Director now supports managing MX Series routers. You can discover them along with SRX Series devices and perform the following actions:

  - Create and manage firewall policies
  - Create and manage firewall policy rules
  - Publish and update policies

  Starting in Junos OS Release 16.1R3-S1.3, you can use the Screens section on the Modify Configuration page to modify the security screen configuration for MX Series routers.

  [See Creating Firewall Policies, Creating Firewall Policy Rules, and Modifying the Screens Configuration for Security Devices.]

- **Migrating content from NSM to Security Director**—You can migrate the NSM database from NSM Releases 2010.3 through 2012.2 into Security Director.

  The following features are supported during the NSM migration:

  - Firewall policies with global rules (including support for the global address book)
  - NAT policies with support for the global address book

  - Nested address group support (Junos OS Release 11.2 and later)
  - Negate address group support in firewall rules
  - Service offload support in firewall rules
  - Source address or source port option in static NAT
  - Source port option in source NAT

  [See NSM Migration.]

- **Using JSA as a log collector**—Starting in Security Director Release 16.2R1, you can use Juniper Secure Analytics (JSA) as a log collector to view log data in Security Director. From the JSA console, Security Director supports SRX Series logs only. Security Director can use JSA3800, JSA5800, JSA7500, or virtual JSA for log collection. You must add JSA as a logging node in Security Director to view the log data on the Dashboard, Events and Logs, Reports, and Alerts pages.

  After JSA is deployed as a VM or hardware appliance, you can configure the network devices to send system logs to JSA. It collects the logs in a standalone or clustered setup. For more details on deploying and configuring JSA, see Juniper Secure Analytics.

  NOTE: You can use either Security Director log collector or JSA as a log collector.

  [See Using JSA as a Log Collector.]

- **SSL forward proxy URL category**—The whitelisting feature is extended to include URL categories supported by Enhanced Web filtering in the whitelist configuration of SSL forward proxy. These URL categories are exempted during the SSL inspection.

  [See Creating SSL Forward Proxy Profiles.]

- **Suite B and PRIME cryptographic suites support**—Suite B and PRIME-128 and PRIME-256 cryptographic suites are supported.

Known Behavior

This section contains the known behavior and limitations in Junos Space Security Director Release 16.2R1.

- You must disable OpenNMS before installing integrated Log Collector.

  To disable OpenNMS :

  1. Select **Network Management Platform** > **Administration** > **Applications**.

     The Applications page appears.

  2. Right-click **Network Management Platform** and select **Manage Services**.

     The Manage Services page appears.

  3. Select **Network Monitoring** and click the Stop Service icon.

     The network monitoring service is stopped and the status is changed to Disabled.

  NOTE: You must ensure that the Network Management Platform and Security Director are already installed on a JA2500 or virtual machine.

- The Enable preview and import device change option is disabled by default. You must enable by clicking **Network Management Platform** > **Administration** > **Applications**. Right-click **Security Director** and click **Modify Application Settings**. Under Update-Device, select the **Enable preview and import device change** option.
- If you restart the JBoss application server manually in a six-node setup one-by-one, the Junos Space Network Management Platform and the Security Director user interface launch quickly, within 20 minutes, and the device reconnects to the Junos Space Network Management Platform. You can edit and publish the policies. Once the connection status and the configuration status of all devices are UP and IN SYNC respectively, click **Update Changes** to update all security-specific configurations or pending services on SRX Series devices.
- To generate reports in the local time zone of the server, you must modify /etc/sysconfig/clock to configure the time zone. Changing the time zone on the server by modifying /etc/localtime is not sufficient.
- High availability for SRX Series devices is not supported in Release 16.2R1 of Policy Enforcer.

Known Issues

This section lists the known issues in Junos Space Security Director Release 16.2R1.

For the most complete and latest information about known defects Junos Space Security Director defects, use the Juniper Networks online Junos Problem Report Search application.

- The Modify Configuration overlay does not fetch configurations such as hostname, domain, and time zone when specified under Groups. PR1240434
- Custom column is not visible in the firewall policy rule grid after the upgrade.

  Workaround:

1. Open the Junos Space Network Management Platform command line and run the **redis-cli** command.

   The command line prompt to execute Redis commands is now available.

2. Run the **get <userid>** command, where <userid> is the name of the user who is not able to see the custom column.

   This command retrieves the following response which includes all the preferences for the specified user.

   "{\"juniper.net\":{\"fw-policy-management\":{\"firewall-rule-grid\":{\"elements\":{\"columns\": [{\"index\":\"id\",\"name\":\"id\",\"hidden\":true,\"width\":50}, {\"index\":\"disabled\",\"name\":\"disabled\"...

3. Copy this string to a text editor and modify the information available after **\"firewall-rule-grid\":{\"elements\":{\"columns\":...**. Delete the following firewall policies rule grid information:

   \"fw-policy-management\": {\"firewall-policies-grid\":{\"elements\":{\"columns\": [{\"index\":\"id\",\"name\":\"id\",\"hidden\":true,\"width\":50}, {\"index\":\"icons\",\"name\":\"icons\",\"label\":\"\",\"width\": 30,\"fixed\":true,\"resizable\":false,\"sortable\":false}, {\"index\":\"sequenceNumber\",\"name\":\"sequence-number\",\"classes\":\"rule-grid-group-object\"...

4. At the Redis command prompt, execute the **set <username> <modified_string>** command, where <username> is the name of the user and <modified_string> is the firewall rule grid information, as shown in Step 2.

   For example:

   set super "{\"juniper.net\":{\"fw-policy-management\":{\"firewall-rule-grid:{}}}}".

5. Type **quit** to exit the Redis command prompt. PR1256789

- In the NSM Release 2012.2.R12 XDIFF files, the source NAT, destination NAT, mapped ports, and protocols are not imported into Security Director.

  Workaround: You must manually configure these values after importing the XDIFF file. PR1261791

- Filter bar in JSA is case sensitive. PR1261805

- Mismatched results are shown when a filter is loaded.

  Workaround: Click the left pane for the filter effect to take place. PR1262071

- Predefined report definitions cannot be deleted, scheduled, or updated with e-mail address though the UI menu icons are enabled.

  Workaround: Predefined reports can be cloned and later scheduled and updated with the e-mail address. PR1257172

- Enrolling devices to Sky ATP through Policy Enforcer takes an average of four minutes to complete. [PR 1222713]

- The first time you open the Monitoring pages, you will receive an **Error occurred while requesting the data message**. This also happens the first time you open the Top

Compromised Host dashboard widget. As a workaround, click your browser refresh button to refresh the page and display the information. [PR 1239956]

- The top compromised hosts widget in the dashboard does not list all the realms. As a workaround, drag and drop another top compromised host widget to the dashboard to display all realms. [PR 1262410]

Resolved Issues

- The traffic passing through the logical systems is not captured in the device widgets. PR1137173
- Generating the delete command for the entire zone address book, though the addresses are used in the firewall policies. PR1256457
- Publish and upgrade are causing random reordering of rules for the All Device policies attached to a device. PR1243761

Finding More Information

For the latest, most complete information about known and resolved issues with Junos Space Network Management Platform and Junos Space Management Applications, see the Juniper Networks Problem Report Search application at: http://prsearch.juniper.net.

Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: http://pathfinder.juniper.net/feature-explorer/.

Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at: http://www.juniper.net/techpubs/content-applications/content-explorer/.

Documentation Feedback

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

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

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post sales technical support, you can access our tools and resources online or open a case with JTAC.

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.

- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

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

Revision History

3 April 2017—

21 April 2017—

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.