Junos® Space Security Director 16.1 Release Notes

Release 16.1
22 February 2017
Revision 6

Contents

Security Director Release Notes

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: To push IPS and application firewall signatures to a device, you need IPS and application firewall licenses.

Installing Junos Space Network Management Platform

Junos Space Security Director Release 16.1R1 is supported only on Junos Space Network Management Platform Release 16.1. For more information on the Network Management Platform upgrade process, see Upgrading to Junos Space Network Management Platform Release 16.1R1.

At the end of the installation, 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 VM.

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

  Download the USB image for JA2500 appliance.

Installing Security Director Release 16.1

In Junos Space Security Director Release 16.1, a single image installs Security Director, Log Director, and the Security Director Logging and Reporting modules. Installing the Security Director Release 16.1 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 in the dashboard, events and logs, reports, and alerts.

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 16.1.

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 16.1R1 and Security Director Release 16.1R1.

Upgrading Security Director

To upgrade from a previous version of Security Director to Security Director Release 16.1R1:

- Download the 16.1R1 file from the Download Site.
- 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.
- 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.

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

Installing Slipstream Script

NOTE: You must ensure that Security Director is installed or upgraded to the latest version before installing the Slipstream script.

To install the Slipstream script:

1. Download the Slipstream script Slipstream-Framework-T1.xx-x.sh from the Download Site.
2. Copy the downloaded script to the /tmp folder of the Junos Space Network Management Platform server.
3. Use the **chmod 777 Slipstream-Framework-T1.xx-x.sh** command to change the permission of the file to read, write, or execute.
4. Install the Slipstream script by running the following command: **sh Slipstream-Framework-T1.xx-x.sh**.
5. On a multinode Junos Space fabric, you must copy and run the script individually on each node.

Upgrading Log Collector

NOTE: Before creating a backup of Log Collector Release 15.2R2, you must delete all the Log Collector nodes from Security Director > Administration > Logging Management > Logging Nodes.

Table 1 on page 5 shows the topology difference between Log Collector Release 15.2R2 and Log Collector Release 16.1 before the upgrade.

Table 1: Understanding the Topology Difference Before Upgrading

Node Type	15.2R2	16.1R1
All-in-One	Yes	Yes
Log receiver	Yes	Yes
Log storage	Yes (Indexer node)	Yes
Query node	Yes (20K eps)	No
Master node	Yes (20K eps)	No

In Log Collector Release 16.1R1:

- Only one log receiver node is supported for all levels of deployment. If you have multiple log receivers in 15.2R2 setup, upgrade only one log receiver to 16.1R1 and delete the other log receivers.
- Log query node and master node are not supported. If you have query or master node in the 15.2R2 setup, delete them.
- You must delete all the unsupported nodes from Security Director > Administration > Logging Management > Logging Nodes.
- Run the upgrade script on each of the applicable node to upgrade the nodes to 16.1R1.

To upgrade from Log Collector Release 15.2 to Log Collector Release 16.1:

1. If the log password was changed for the logging nodes in the Log Collector Release 15.2R2, perform the following steps. Else, continue with 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/.
   - Inside 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-16.1R1.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 jingest process will run.
- You must ensure that jingest and elasticsearch processes are running.

5. Add the logging nodes back to Security Director from Security Director > Administration > Logging Management > Logging Nodes.

Deploying Log Collector

System Requirement

Table 2 on page 6 and Table 3 on page 6 provide the virtual machine (VM) configuration that we recommend 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 gives better stability for the log collection.

Table 4 on page 7 shows 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 eps of up to 3000 with spinning disks and 4000 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 to send syslogs. Upon configuration, this node parses and forwards logs to 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 the syslogs. It receives the syslogs from Log Receiver Node.

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

Storage Requirements

The total storage required for retaining *X* number of days at a given events-per-second (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 get rolled over under 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 get rolled over when the disk size reaches 400GB.

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-16.1R1.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. username is **root** and 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 on page 13.

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.

To create a bootable USB flash drive, follow these steps in Microsoft Windows:

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. Click the open or browse icon next to the Create a bootable disk using option to select the ISO image.
4. Click **Start**.

   A progress bar on the Rufus page indicates the status of the bootable USB flash drive creation. 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 go 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 taken 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. While 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 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 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 on page 13.

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

Prerequisites

The prerequisites for installing integrated log collector on a JA2500 appliance or virtual machine (VM) are as follows:

- Install the Junos Space Network Management Platform Release 16.1R1 image on a JA2500 appliance or VM from the download site.
- Install the Junos Space Security Director Release 16.1R1 image on a JA2500 appliance or VM from the download site.
- Integrated Log Collector uses the 9200, 514, and 4567 ports.
- Junos Space Network Management Platform must be configured with Ethernet Interface eth0 and management IP addresses.
- OpenNMS must be disabled on Junos Space Network Management Platform.
- Ethernet Interface eth0 on 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 11 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 11 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 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-16.1.R1.xxx.sh from the Download Site.
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 permission of the **Chmod +x Integrated-Log-Collector-16.1.R1.xxx.sh** file.
6. Install the integrated Log Collector script using the following command: **sh Integrated-Log-Collector-16.1.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-16.1.R1.157.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 Junos Space VM:

  1. Add a hard disk of 500 GB capacity on the Junos Space VM through 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 up and running. You must be able to log into the Junos Space Network Management Platform and Security Director user interfaces before attempting again to run the integrated Log Collector setup script.

  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-16.1.R1.xxx.sh** command.

- The installation stops if the following error message is displayed while installing 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-16.1.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-16.1.R1.xxx.sh** command.

When 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 used the standard setup menu to configure Log Collector, then you can use the following script, described in Table 7 on page 13, 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 of time zone configuration.
jnpr-network-script	Script for interface configuration.
healthcheckOSLC	Script of checking the issues with logging infrastructure.

Adding Log Collector to Security Director

Once Log Collector is configured, you can add it to Security Director.

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 (+).
2. Provide the root credentials of the Log Collector node.
3. Verify the corresponding job status.

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

For more information on increasing the disk size of your VM when log files are too large, see Expanding the Size of the VM Disk for Log Collector.

For more information configuring vMotion, see Creating a VMkernel port and enabling vMotion on an ESXi/ESX host and Set Up a Cluster for vMotion.

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 VM setup must have 32 GB of RAM and must stop running OpenNMS (in a single or a two-node fabric) on it. 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 in 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 the 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, performance of publish and update is better compared with the normal two-node Junos Space fabric setup.

Supported Devices

Security Director Release 16.1 is supported on the following SRX Series and LN Series 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
- LN1000-V
- LN2600

Supported Junos OS Releases

- Security Director Release 16.1 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

- 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 16.1 is best viewed on the following browsers:

- Mozilla Firefox
- Google Chrome
- Microsoft Internet Explorer 11

New Features

This section describes the new features available in Security Director Release 16.1.

- **Threat Map Enhancements**—On the Threats Map (Live) page, when you click a country, a tooltip displays the total threat events for that country since midnight, followed by the number of inbound and outbound threat events. You can also see top five IP addresses, either inbound or outbound, whichever is higher. You can choose one or more IP addresses and block them.

  You can use Block all traffic, Block inbound, or Block outbound traffic for selected countries. You can click **View details** from the tooltip to view additional details for the selected country, displayed on the right panel with the selected country zoomed-in.

  

  NOTE: You must use Sky Advanced Threat Protection (ATP) service.

- **Application and User Visibility Enhancements**—You can see the IP address of a user, if username is not available, and you can block the IP address similar to blocking the username. This is supported in both chart view and grid view.

  When you mouse over a bubble in the Application Visibility page, you can click the **View All Users** link in the tooltip to navigate to the User Visibility page with correct filters applied. When you mouse over a bubble in the User Visibility page, you can click the **View All Applications** link in the tooltip to navigate to the Application Visibility page with correct filters applied. Also, you can attach a schedule to the autocreated rule when you perform the block operation.

- **IP Address Visibility**—You can use the Source IP Visibility page to view information related to bandwidth consumption, session establishment, and the risks associated with the source IP addresses.

- **Drag and Drop of Policy Rules**—You can select one or more objects to drag and drop into the columns in the policy tabular view. Security Director ensures that objects can be dropped only into the columns that support the drag and drop feature. Columns that support this feature are the Source Address, Destination Address, and Service columns.

  You can drag and drop objects across the rules. The new objects are copied to the rule. This feature is supported for firewall and NAT policies.

- **Integrated Log Collector**—You can collect system logs from the SRX Series devices without deploying an additional virtual machine or JA2500 as a log collector.

  To install the log collector in an integrated mode on a JA2500 or virtual machine, OpenNMS must be disabled. For more information, see the Known Behavior section.

- **JA2500 Distributed Log Collectors**—You can deploy the distributed Log Collector on JA2500 appliance.

- **User Firewall Management**—You can create an access directory and an access profile, update them to SRX Series devices, and use them later in firewall policies.

- **Alert Enhancements**—You can use the Time Span field to specify the time and duration to trigger an alert when you create or edit an alert. The default duration is 30 minutes and the maximum duration is 24 hours.
- **Device Inventory Page Enhancements**—On the Security Devices page, you can drill down on the CPU meter to view additional details on the usage of each CPU on the SRX Series device.
- **Exporting and Importing Security Policies to ZIP**—You can export policies (firewall, IPS, or NAT) in a ZIP file from their respective Policies landing page or import policies from a ZIP file to Security Director. The supported file type is XML.
- **General IKE ID Option**—You can now provide a generic peer IKE ID when you create a VPN profile. This enables you to bypass the validation of an IKE ID.
- **Reporting Enhancements**—You can run a report immediately on demand and download the report in PDF using the Run Now option.

  The following predefined report definitions are available:

  - Top Destination Countries—Displays a report on top destination IP addresses by countries.
  - Top Source Countries—Displays a report on top source IP addresses by countries.
  - Top IPS Attacks By Source Countries—Displays a report on top IPS attacks by source countries.
  - Top IPS Attacks by Destination Countries—Displays a report on top IPS attacks by destination countries.

Known Issues

- After upgrading to Security Director 16.1R1, dashboard widgets are not seen in the user interface, though the widgets were added prior to upgrading.

  [Workaround] Add the widgets again from the dashboard widgets palette.
- When you unassign a device from an access profile and do not deploy the access profile, the delete CLI command is generated. [PR 1210093]
- In the firewall or NAT rules page, the grid separator adjustments between the rule grid and the drag-and-drop panel varies each time you navigate to different pages and come back to the rules page.

  Workaround: Install the Slipstream script to address this issue. See Installing Slipstream Script on page 4. [PR 1225754]
- The drag-and-drop window adjustments made on the Firewall Rules page is not remembered by Security Director. You must adjust the drag and drop grid width every time you come back to the Firewall Rules page. [PR 1235942]
- Adding more than one Log Collector by selecting the Node Count drop-down list fails to add nodes beyond a single node. You must add nodes sequentially by selecting the Single Node option. [PR 1234680]

- The size of all the screens and grids is not aligned with the resolution of the monitor. [PR 1217274]
- The context menu options are sometimes disabled in the right-click option, but appears properly from the More link. [PR 1234802]
- The traffic passing through the logical systems is not captured in the device widgets. [PR 1137173]
- If you perform a column filter by name or IP address in the Security Devices landing page, result shows empty at the first instance.

  Workaround: Install the Slipstream script to address this issue. See Installing Slipstream Script on page 4. [PR 1239170]
- In the Security Devices landing page, if you have selected all of the column filtered values, removing the selection for one or multiple values does not work.

  Workaround: Install the Slipstream script to address this issue. See Installing Slipstream Script on page 4. [PR 1239172]
- If you search for a firewall policy in the All Events page, under the Detail View tab, the Show firewall policy option does not point to the appropriate zone-based rule in the firewall rules page.

  Workaround: Install the Slipstream script to address this issue. See Installing Slipstream Script on page 4 [PR 1239124]
- If you change the Policy Enforcer VM password, the Policy Enforcer VM still communicates with Security Director even though you did not update the Policy Enforcer password in the Administration > PE Settings window in Security Director. [PR 1235683]
- When changing the mode from Sky ATP to Sky ATP with Policy Enforcer within Security Director, SRX Series devices previously enrolled with Sky ATP realms are removed and disenrolled. The enroll configuration is not removed from the SRX Series devices when you change the Policy Enforcer password immediately after changing the mode type. Instead, change the Policy Enforcer password at the same time that you change the mode type. [PR 1238810]
- Alarms are not seen in Security Director on a four-node Junos Space setup installed with Network Director, Service Now, and Service Insight.

  Workaround: Restart JBoss services on all the Junos Space nodes. [PR 1237877]
- In the integrated Log Collector setup, once the syslog forwarding is configured and saved, the user interface does not display the configuration on next edit. Syslog is forwarded to the configured destination, but editing the configuration is not possible. [PR 1240001]
- On the Secure Fabric landing page, the tool tip for SkyATP Enroll Status always says Device failed to enroll. Instead, refer to the icon. A green icon indicates success; a red icon indicates failure. [PR 1239977]
- Enrolling devices to Sky ATP through Policy Enforcer takes an average of four minutes to complete. [PR 1222713]
- The policy publish fails after upgrading to Security Director 16.1.

[Workaround] You must edit the firewall policy and publish again. [PR 1242966]

- The links in the Getting Started panel are inactive. [PR 1240636]
- If you enter multiple tokens in a filter bar or search bar and leave that page and come back again, only the first token is persisted.

  Workaround: Install the Slipstream script to address this issue. See Installing Slipstream Script on page 4. [PR 1239158]
- Firewall policy rules page width is not sufficient to show rules with many objects. You must use the scroll bar to reach to the end of the page.

Known Behavior

- 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 the **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 Networking 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 it 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 the policies and publish them. 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.
- SRX Series High Availability is not supported in this release of Policy Enforcer.

Documentation Updates

This section lists the errata and changes in Security Director Release 16.1R1 documentation:

- In the Security Director user interface, the following corrections apply to the *Getting Started* panel content, under the *Configure Logging and Reporting* step:

  The following sentence is incorrect:

  Log Collector is supported only as a VM that can be deployed on VMWare ESX and KVM Hypervisor. Log Collector cannot be installed on any physical device. For more details, see Security Director Release Notes.

  The correct description is as follows:

  You can deploy Log Collectors in both VM and JA2500 appliance. You can deploy Log Collector as All in One node for small-scale deployments. For easy scaling, begin with a single Log Receiver node and Log Storage node, and incrementally add Log Storage nodes as your needs expand. You can add a maximum of one Log Receiver node and three Log Storage nodes.

  In case of VM environment, a single OVA image is used to deploy All in One, Log Receiver, and Log Storage nodes. The image presents a configuration script after you login. At deployment, you must select appropriate memory and CPU configuration values, as appropriate for the role of the VM.

  In case of JA2500 deployment, a single ISO image is used to install All in One, Log Receiver, and Log Storage nodes. The image presents a configuration script after you login. For more details, see Security Director Release Notes.

Junos Space Documentation and Release Notes

For a list of related Junos Space documentation, see http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the *Junos Space Release Notes*.

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

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at http://www.juniper.net/books.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/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 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

21 December 2016—

5 January 2017—

9 January 2017—

18 January 2017—

2 February 2017—

22 February 2017—