JUNIPER NETWORKS | Engineering Simplicity

Upgrading Juniper Secure Analytics to 7.4.0

Published
2021-04-07

Release
7.4.0

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

Upgrading Juniper Secure Analytics to 7.4.0
7.4.0

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

IN THIS SECTION

Use this guide to upgrade JSA from earlier version to the current version.

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`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*

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

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		

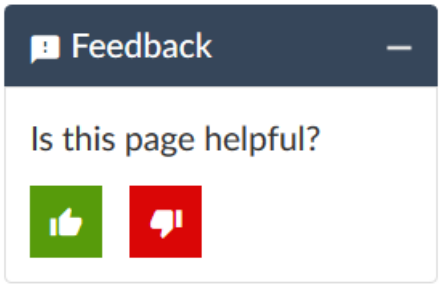
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback 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

JSA Upgrade Types

JSA Upgrade Types

There are two types of JSA upgrades: major OS version upgrades and regular upgrades.

Major OS version upgrades

An upgrade that includes a major operating system version upgrade. These upgrades use an ISO file.

Regular upgrades

An upgrade that doesn't include a major operating system upgrade. These upgrades use an SFS file.

2

CHAPTER

Preparing for the Upgrade

Preparing for the Upgrade

To successfully upgrade an JSA system, verify your upgrade path, especially when you upgrade from older versions that require intermediate steps. You must also review the software, hardware, and high availability (HA) requirements.

Use the following checklist to make sure that you are prepared for an upgrade.

- Review the JSA Release Notes (https://www.juniper.net/documentation/product/en_US/juniper-secure-analytics/).
- Run a health check and fix any failures. See "Running health checks" in the *Juniper Secure Analytics Troubleshooting Guide*.
- Notify users of scheduled maintenance.
- Verify that running scans and reports are complete.
- Request that users close all JSA sessions and **screen** sessions.
- Download the SFS file. See (https://www.juniper.net/documentation/product/en_US/juniper-secure-analytics/).
- Verify the checksum of the SFS file.
- Get a CSV file that contains a list of IP addresses for each appliance in your deployment if you don't already have this information, by typing the following command:

  /opt/qradar/support/deployment_info.sh
- Back up all third-party data, such as:

  - scripts

  - personal utilities

  - important files or exports

  - JAR files or interim fixes that were provided by JSA support

  - static route files for network interfaces
- If you have HA appliances in your deployment, verify that your primary appliances are in the Active state, and your secondary appliances are in the Standby state.
- Ensure that you have direct access to the command line on all appliances. If you are using IMM, iDRAC, Raritan, KVM, or other technology for command line access, ensure that they are configured and functional.
- Back up your custom content by typing the following command:

  /opt/qradar/bin/contentManagement.pl --action export --content-type all

- Confirm that all appliances in your deployment are at the same software version by typing the following commands:

  /opt/qradar/support/all_servers.sh -C -k /opt/qradar/bin/myver > myver_output.txt

  cat myver_output.txt

- Confirm that all previous updates are unmounted by typing the following commands:

  /opt/qradar/support/all_servers.sh -k "umount /media/cdrom"

  /opt/qradar/support/all_servers.sh -k "umount /media/updates"

- If you have HA appliances in your deployment:

  - Verify that the **/store** file system is mounted on the primary appliance and not mounted on the secondary appliance.

  - Verify that the **/transient** file system is mounted on both the primary and secondary appliances.

- Review system notifications for errors and warnings for the following messages before you attempt to update. Resolve these error and warning system notifications before you attempt to update:

  - Performance or event pipeline degradation notifications

  - Memory notifications

  - TX sentry messages or process stopped notifications

  - HA active or HA standby failure system notifications

  - Disk failure system notifications

  - Disk Sentry noticed one or more storage partitions are unavailable notifications

  - Time synchronization system notifications

  - Unable to execute a backup request notifications

  - Data replication experiencing difficulty notifications

  - RAID controller misconfiguration notifications

- Manually deploy changes in the user interface to verify that it completes successfully.
- Verify that the latest configuration backup completed successfully and download the file to a safe location.
- Ensure that all apps on your system are updated. Out-of-date apps might not work after you upgrade JSA.
- Resolve any issues with applications in an error state or not displaying properly.
- App Nodes are no longer supported as of JSA 7.3.2. If you have an App Node in your deployment, follow the steps in "Migrating from an App Node" in the *Juniper Secure Analytics Administration Guide* before you start the upgrade.

RELATED DOCUMENTATION

Software Version Requirements for Upgrades | 14

Software Version Requirements for Upgrades

To ensure that JSA upgrades without errors, ensure that you use only the supported versions of JSA software:

- Ensure that JSA 7.3.0 or later is installed.
- Check the software version in the software by clicking **Help >About**.

> **NOTE:** Software versions for all JSA appliances in a deployment must be the same version and build. Deployments that use different JSA versions of software are not supported.

RELATED DOCUMENTATION

Upgrade Sequence in Distributed Deployments | 14

Upgrade Sequence in Distributed Deployments

When you upgrade JSA systems, you must complete the upgrade process on your JSA Console first. You must be able to access the user interface on your desktop system before you upgrade your secondary JSA Console and managed hosts.

Upgrade your JSA systems in the following order:

1. Console
2. The following JSA systems can be upgraded concurrently:
   - Event Processors/ Collectors
   - Flow Processors
   - App Hosts

3

CHAPTER

Upgrading JSA to 7.4.0

Upgrading JSA to 7.4.0

You must upgrade all of the JSA products in your deployment to the same version.

Ensure that JSA 7.3.0 or later is installed.

Upgrade your JSA Console first, and then upgrade each managed host. In high-availablity (HA) deployments, upgrade the HA primary host first, and then upgrade the HA secondary host.

1. Run the **aqlValidator** script to determine whether any Ariel queries must be updated before you upgrade JSA:
   - If auto-updates are enabled, run **aqlValidator** by typing the following command:

     /opt/qradar/support/apar/aqlValidator
   - If auto-updates are not enabled:
     a. Download the latest autoupdates bundle from Juniper Customer Support https://support.juniper.net/support/downloads/.
     b. Install the autoupdates bundle by following the instructions in JSA. See *Juniper Secure Analytics Administration Guide*/Set Up JSA/Automatic update. Juniper Secure Analytics Administration Guide.
     c. Run **aqlValidator** by typing the following command:

        /opt/qradar/support/apar/aqlValidator
2. Download the *<qradar>.sfs* file from Juniper Customer Support https://support.juniper.net/support/downloads/.
3. Use SSH to log in to your system as the root user.
4. Copy the SFS file to the **/root** or **/var/log** directory or to another location that has sufficient disk space.

   NOTE: Do not copy the file to an existing JSA system directory, such as **/store**.
5. To create the **/media/updates** directory, type the following command:

   mkdir -p /media/updates
6. Use the **cd** command to change to the directory where you copied the SFS file.
7. Unzip the patch file using the bunzip utility:

bunzip2 <patchfilename>.bz2

8. To mount the SFS file to the **/media/updates** directory, type the following command:

   mount -o loop <qradar>.sfs /media/updates/

9. To run the patch installer, type the following command:

   /media/updates/installer

What to do next:

1. **Unmount /media/updates** by typing the following command:

   umount /media/updates

2. Delete the SFS file.
3. Perform an automatic update to ensure that your configuration files contain the latest network security information. For more information, see the *Juniper Secure Analytics Administration Guide*.
4. Delete the patch file to free up space on the partition.
5. Clear your web browser cache. After you upgrade JSA, the **Vulnerabilities** tab might not be displayed. To use JSA Vulnerability Manager after you upgrade, you must upload and allocate a valid license key. For more information, see the *Juniper Secure Analytics Administration Guide* for your product.
6. Determine if there are changes that must be deployed. For more information see “Deploying Changes” in *Juniper Secure Analytics Administration Guide*.