Juniper Secure Analytics Migration Guide

Release
7.3.0

Modified: 2017-09-13

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

Juniper Secure Analytics Migration Guide
7.3.0

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation

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 http://www.juniper.net/techpubs/.

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 http://www.juniper.net/books.

Documentation Conventions

Table 1 on page vi 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 vi 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*
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*

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

Convention	Description	Examples
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		
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, 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: https://prsearch.juniper.net/
- Find product documentation: http://www.juniper.net/documentation/
- 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://entitlementsearch.juniper.net/entitlementsearch/

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.

PART 1

JSA Series Migration

CHAPTER 1

JSA Series Appliance Overview

This chapter includes the following topics:

JSA Series Appliance Overview

The Juniper Secure Analytics (JSA) Series includes the hardware appliances (JSA3500, JSA5500, JSA7500, JSA3800, and JSA5800) and a virtual appliance, which replace Juniper Networks Security Threat Response Manager (STRM) solution for centralized logging, monitoring, and reporting. The JSA Series integrates and automates log management and network behavior analytics and offers increased performance and scaling features.

This guide provides instructions for:

- Migrating the configuration from an existing JSAx500 appliance to a JSAx800 appliance including network settings (for example, IP address). This process replaces the JSAx500 appliances with a similarly configured JSAx800 appliance.

  NOTE:
  - For JSAx500, x is one of the JSA Series appliances 3, 5, or 7 (JSA3500, JSA5500, or JSA7500).
  - For JSAx800, x is one of the JSA Series appliances 3 or 5 (JSA3800 or JSA5800).

- Manually copying JSAx500 event and flow data to the JSAx800 appliance. This step is optional.
- Migrating from a distributed JSAx500 environment to JSAx800.
- Migrating licenses from JSAx500 to JSAx800.

Related Documentation

- JSA Series Migration Overview on page 7
- Configuration and Data Features for JSA Migration on page 4

- Distributed Environment to JSA Migration Overview on page 21
- Migrating Licenses to JSA Series Overview on page 29

Configuration and Data Features for JSA Migration

The following configuration can be migrated from an existing JSAx500 appliance to JSAx800:

NOTE:

- For JSAx500, x is one of the JSA Series appliances 3, 5, or 7 (JSA3500, JSA5500, or JSA7500).
- For JSAx800, x is one of the JSA Series appliances 3 or 5 (JSA3800 or JSA5800).

- Assets
- Custom logos
- Custom rules
- Device Support Modules (DSMs)
- Event categories
- Flow sources
- Flow and event searches
- Groups
- License key information
- Log sources
- Offenses
- User and user roles information
- Custom Dashboards
- Vulnerability data
- Certificates

Optionally, JSAx500 event and flow data can be copied manually to JSAx800.

The following configuration cannot be migrated from JSAx500 to JSAx800:

- Audit log information
- Report data
- Indexes
- Reference set elements

Related Documentation

- JSA Series Appliance Overview on page 3
- JSA Series Migration Overview on page 7
- Distributed Environment to JSA Migration Overview on page 21
- Migrating Licenses to JSA Series Overview on page 29

CHAPTER 2

Migrating a JSAx500 Series Appliance to a JSAx800 Series Appliance

This chapter includes the following topics:

JSA Series Migration Overview

The migration process from JSAx500 Series to JSAx800 Series includes the following steps:

NOTE:

- For JSAx500, x is one of the JSA Series appliances 3, 5, or 7 (JSA3500, JSA5500, or JSA7500).
- For JSAx800, x is one of the JSA Series appliances 3 or 5 (JSA3800 or JSA5800).

1. Perform a pre-upgrade configuration backup of the JSAx500 appliance.
2. Upgrade or patch the JSAx500 appliance to the common image.
3. Perform a configuration backup of the JSAx500 appliance when running the common image.

4. Install the JSAx800 appliance and, if required, reimage the appliance to the common image.
5. Restore an JSAx500 appliance configuration on the JSAx800 appliance.
6. Copy JSAx500 event and flow data to the JSAx800 appliance (optional).
7. Run automatic updates on the JSAx800 appliance.

Related Documentation

- JSA Series Appliance Overview on page 3
- Configuration and Data Features for JSA Migration on page 4
- Distributed Environment to JSA Migration Overview on page 21
- Migrating Licenses to JSA Series Overview on page 29

Pre-Upgrade Configuration Backup Process for a JSAx500 Series Appliance

When you are about to migrate a Juniper Secure Analytics (JSA)x500 Series appliance to a JSAx800 Series appliance, we recommend that you perform a pre-upgrade configuration backup on the JSAx500 appliance. The pre-upgrade backup is not used when you restore the configuration on a JSAx800 appliance. Rather, you should perform the pre-upgrade backup as a best practice in case you encounter errors while upgrading JSAx500 or JSAx800 to a common image.

NOTE:

- For JSAx500, x is one of the JSA Series appliances 3, 5, or 7 (JSA3500, JSA5500, or JSA7500).
- For JSAx800, x is one of the JSA Series appliances 3 or 5 (JSA3800 or JSA5800).

By default, JSAx500 creates a complete backup of the appliance configuration each day at midnight. You can either use the automatic backup or initiate an on-demand backup. Either way, the configuration backup should be downloaded before you upgrade JSAx500 or install the patch on JSAx500.

To create and download an on-demand configuration backup:

1. Log in to the JSAx500 WebUI.
2. Click the Admin tab.
3. On the navigation menu, click **System Configuration**.

4. Click **Backup and Recovery**.

   NOTE: Configuration backup files are located in the /store/backup directory.

5. From the toolbar, click **On Demand Backup**.
6. Enter a name and description to identify the backup.
7. Click **Run Backup**.
8. Click **OK**.
9. Monitor the backup archive process in the Backup Archives window.

   Once complete, the backup will appear in the list of the Existing Backups table.

10. To download the backup, click the backup name.

    NOTE: Double-click in the Existing Backups table to display the Restore a Backup dialog box. Single-click on a backup name to download the backup.

Related Documentation

- JSA Series Appliance Overview on page 3
- JSA Series Migration Overview on page 7
- Upgrading an Existing JSA Appliance on page 9
- Backing Up the Existing JSA Appliance Configuration While Running the Common Image on page 11
- Installing a JSA and a Virtual JSA Appliance on page 11

Upgrading an Existing JSA Appliance

Juniper Secure Analytics (JSA) software will have a version number and a build number.

For example, if the software is 2014.3.r1.931999, then the version number is 2014.3.r1 and the build number is 931999. Both JSAx500 and JSAx800 must run the same version and build for the configuration migration to be successful.

NOTE:

- For JSAx500, x is one of the JSA Series appliances 3, 5, or 7 (JSA3500, JSA5500, or JSA7500).
- For JSAx800, x is one of the JSA Series appliances 3 or 5 (JSA3800 or JSA5800).

Juniper Networks delivers the JSA software in two ways:

- ISO file—used for fresh installs and major upgrades
- SFS file—called a patch and used for minor upgrades

You can replace an existing JSAx500 with JSAx800 by migrating the configuration and data.

The certified image for this migration is 2014.3.r1.931999 or a later version on both JSAx500 and JSAx800; 2014.3.r1.931999 is referred to as the common image in this migration documentation.

Table 3 on page 10 helps you determine the upgrade path to the common image depending on the version that is currently running on the JSAx500 Series or JSAx800 Series appliance.

Table 3: Supported Upgrade Paths to the Common Image

Current Version	Step
2014.1, 2014.2, and 2014.3 ISO	2014.3.r1 patch
2013.2 R3 ISO with 2013.2.r9 patch or later	2014.3.r2 patch
2013.2 R3 ISO to 2013.2.r8 patch	2014.3.r1 patch

For information on upgrading JSA to 2014.3, see *Upgrading JSA to 2014.3*.

Related Documentation

- JSA Series Appliance Overview on page 3
- JSA Series Migration Overview on page 7
- Pre-Upgrade Configuration Backup Process for a JSAx500 Series Appliance on page 8
- Backing Up the Existing JSA Appliance Configuration While Running the Common Image on page 11
- Installing a JSA and a Virtual JSA Appliance on page 11

Backing Up the Existing JSA Appliance Configuration While Running the Common Image

When JSAx500 is running the common image, a new configuration backup must be made. This backup is restored to the JSAx800 appliance. You cannot restore the pre-upgrade backup to JSAx800 because it was made before the JSAx500 was running the common image.

NOTE:

- For JSAx500, x is one of the JSA Series appliances 3, 5, or 7 (JSA3500, JSA5500, or JSA7500).
- For JSAx800, x is one of the JSA Series appliances 3 or 5 (JSA3800 or JSA5800).

For the JSAx500 backup process that includes copying the backup to a remote server, see "Pre-Upgrade Configuration Backup Process for a JSAx500 Series Appliance" on page 8.

Related Documentation

- JSA Series Appliance Overview on page 3
- JSA Series Migration Overview on page 7
- Upgrading an Existing JSA Appliance on page 9
- Installing a JSA and a Virtual JSA Appliance on page 11
- Reimaging JSA Series to the Common Image Using the Recovery Partition on page 13
- Restoring Backup on a JSA Appliance on page 14

Installing a JSA and a Virtual JSA Appliance

To install:

- JSA3500, JSA5500, and JSA7500, see the *Juniper Secure Analytics Quick Start Guide*.
- JSA3800, see *How to Set Up Your JSA3800 Appliance*.
- JSA5800, see *How to Set Up Your JSA5800 Appliance*.

These guides provides you the following information:

- Installing a JSA appliance
- Configuring the network settings
- Accessing a JSA appliance

To install a virtual JSA appliance, see the *JSA Virtual Appliance Installation Guide*. This guide provides you the following information:

- Creating a new virtual machine
- Installing the JSA software
- Configuring the network settings
- Accessing a virtual JSA appliance

Assign a temporary IP address when you configure the JSA network settings. When the JSA appliance is installed and active on the network, you must determine the installed version and reimage if necessary.

- Factory Default Version on page 12

Factory Default Version

The physical JSAx800 appliances come with 2014.3.r1.931999 (the common image).

NOTE: **For JSAx800, x is one of the JSA Series appliances 3 or 5 (JSA3800 or JSA5800).**

In the JSA user interface, click **Help** > **About** to view the JSA version information. If the JSA version is 2014.3.r1.931999, there is no need for reimaging. Follow the steps in "Copying Event and Flow Data to JSA" on page 15.

Related Documentation

- JSA Series Appliance Overview on page 3
- JSA Series Migration Overview on page 7
- Pre-Upgrade Configuration Backup Process for a JSAx500 Series Appliance on page 8
- Upgrading an Existing JSA Appliance on page 9
- Backing Up the Existing JSA Appliance Configuration While Running the Common Image on page 11
- Reimaging JSA Series to the Common Image Using the Recovery Partition on page 13

Reimaging JSA Series to the Common Image Using the Recovery Partition

To reimage the JSAx800 appliance to the common image using the recovery partition

NOTE: For JSAx800, x is one of the JSA Series appliances 3 or 5 (JSA3800 or JSA5800).

1. To download the ISO file:
   a. Access the Juniper Customer Support Center (CSC) website (www.juniper.net/support/).
   b. Locate the JSA 2014.3.r1 ISO file on the CSC website.
   c. Save the ISO file on a remote server that supports either SCP or FTP.
2. Using SSH, log in to your JSA system as the root user.
3. Copy the ISO or SFS image from a remote server to the JSA appliance using SCP or FTP.

   For example, if the IP address of the remote server is 10.10.10.1, run the following command to copy the file to the **/root** directory:

   [root@jsa]#scp root@10.10.10.1:/<path>/JSA2014.3.r1.iso /root
4. Run the following command to change to the location of the **recovery.py** script:

   [root@jsa]# cd /opt/qradar/bin
5. Run the following command to execute the recovery script:

   [root@jsa]# ./recovery.py –r --default --reboot /root/JSA2014.3.r1.iso
6. After reboot, when prompted, type **FLATTEN** and then press Enter.

   The JSA appliance is now running the common image.

Related Documentation

- JSA Series Migration Overview on page 7
- Pre-Upgrade Configuration Backup Process for a JSAx500 Series Appliance on page 8
- Upgrading an Existing JSA Appliance on page 9
- Backing Up the Existing JSA Appliance Configuration While Running the Common Image on page 11
- Installing a JSA and a Virtual JSA Appliance on page 11
- Restoring Backup on a JSA Appliance on page 14

Restoring Backup on a JSA Appliance

Because both existing Juniper Secure Analytics (JSA)x500 appliances and JSAx800 appliances are running the common image, the JSAx500 backup (made while running the common image) can be restored to the JSA appliance.

NOTE:

- For JSAx500, x is one of the JSA Series appliances 3, 5, or 7 (JSA3500, JSA5500, or JSA7500).
- For JSAx800, x is one of the JSA Series appliances 3 or 5 (JSA3800 or JSA5800).

This procedure restores the JSAx500 configuration on JSAx800, including network settings like IP address. To avoid a duplicate IP address on the network, the JSAx500 appliance must be turned off before proceeding.

To restore the JSAx500 configuration on the JSAx800 appliance:

1. Log in to the Secure Analytics WebUI.
2. Click the Admin tab.
3. On the navigation menu, click **System Configuration**.
4. Click **Backup and Recovery**.
5. Click **Choose File** to upload the configuration backup.
6. Select the file and then click **Upload**.

   The uploaded backup appears under the Existing Backups table.
7. Select the backup file and then click **Restore**.
8. Select all the check boxes except **Select All Configuration Items** and **License** in the Restore a Backup window, and then click **Restore** to restore the backup.

Special Case for JSA HA Clusters

If the configuration backup was made on a high availability cluster, you must click **Deploy Changes** from the JSAx800 appliance console to restore the HA cluster configuration after the restore is complete and before adding the secondary appliance.

Related Documentation

- JSA Series Migration Overview on page 7
- Backing Up the Existing JSA Appliance Configuration While Running the Common Image on page 11
- Installing a JSA and a Virtual JSA Appliance on page 11
- Reimaging JSA Series to the Common Image Using the Recovery Partition on page 13
- Copying Event and Flow Data to JSA on page 15

Copying Event and Flow Data to JSA

The configuration restore process duplicates only the Juniper Secure Analytics (JSA)x500 configuration to the JSAx800 Series appliance. To copy the event and flow data, several file transfer methods are possible including rsync, SCP, and FTP.

NOTE: All the event and flow data are stored in the /store/ariel directory on both JSAx500 and JSAx800.

NOTE:

- For JSAx500, x is one of the JSA Series appliances 3, 5, or 7 (JSA3500, JSA5500, or JSA7500).
- For JSAx800, x is one of the JSA Series appliances 3 or 5 (JSA3800 or JSA5800).

To copy the JSAx500 event and flow data to a JSAx800 appliance:

1. Using SSH, log in to JSAx500.
2. Run the **rsync** command to copy the event and flow data to JSAx800. If the temporary IP address of the JSAx800 appliance is 10.10.10.1, run the following commands:
   - To copy events, **[root@jsa]# /usr/bin/rsync -azv /store/ariel/events root@10.10.10.1:/store/ariel/events**
   - To copy flows, **[root@jsa]# /usr/bin/rsync -azv /store/ariel/flows root@10.10.10.1:/store/ariel/flows**

NOTE:

- Use the optional v option to view the status of the copy operation. Do not use this option if you are connected to JSAx500 through the serial console or over slow links. Use > to redirect the output to a file, and use the tail command to check the progress periodically.
- If only event or flow data (not both) is desired, specify the directory (either /events or /flows) specifically. For example, run the following command to copy only JSAx500 event data:

  [root@jsa]# /usr/bin/rsync -azv /store/ariel/events root@10.10.10.1:/store/ariel/events

NOTE: To verify that the restored data is available:

a. Log in to the Secure Analytics WebUI.
b. Click the Log Activity or Network Activity tab.
c. Select **Search** > **Edit Search** from the list.
d. In the Time Range box, select **Specific Interval**.
e. Specify the date of the data you just restored.
f. Click **Search**.
g. View the results to verify the restored data.

Related Documentation

- JSA Series Migration Overview on page 7
- Reimaging JSA Series to the Common Image Using the Recovery Partition on page 13
- Restoring Backup on a JSA Appliance on page 14
- Running Automatic Updates on the JSA Appliance on page 16

Running Automatic Updates on the JSA Appliance

After you have verified that the configuration and data are restored to the Juniper Secure Analytics (JSA)x800 appliance, some system components should be updated, including installing new or updated DSMs, vulnerability assessment (VA) scanners, and log source protocols.

NOTE: For JSAx800, where x is one of the JSA Series appliances 3 or 5 (JSA3800 or JSA5800)

To run automatic updates on the JSAx800 appliance:

1. In the JSAx800 appliance console, click the Admin tab.
2. On the navigation menu, click **System Configuration**.
3. Click the Auto Update icon.
4. Click the Get New Updates button.
5. Select **OK** to download.

NOTE: By default, DSM, scanner, and protocol updates are automatically installed once they are downloaded. This setting is configured through the **Change Settings** pane. For more information, see the *Configuring Automatic Update Settings* section of the *JSA Administration Guide*.

Related Documentation

- Reimaging JSA Series to the Common Image Using the Recovery Partition on page 13
- Restoring Backup on a JSA Appliance on page 14
- Copying Event and Flow Data to JSA on page 15
- JSA Series Migration Overview on page 7
- Distributed Environment to JSA Migration Overview on page 21

PART 2

Distributed Environment to JSA Migration

CHAPTER 3

Migrating a Distributed Existing JSA Environment

This chapter includes the following topics:

Distributed Environment to JSA Migration Overview

The migration of a distributed existing Juniper Secure Analytics (JSA)x500 environment to JSAx800 includes the following steps:

NOTE:

- For JSAx500, x is one of the JSA Series appliances 3, 5, or 7 (JSA3500, JSA5500, or JSA7500).
- For JSAx800, x is one of the JSA Series appliances 3 or 5 (JSA3800 or JSA5800).

1. Migration from the JSAx500 console to a JSAx800 console.
2. Migration of each JSAx500 managed host to a JSAx800 managed host.
3. Adding each new JSAx800 managed host to the JSAx800 console.

Related Documentation

- Migrating to a JSA Console on page 22
- Adding Each New JSA Managed Host to a JSA Console on page 24
- JSA Series Appliance Overview on page 3
- JSA Series Migration Overview on page 7
- Migrating Licenses to JSA Series Overview on page 29

Migrating to a JSA Console

In a distributed existing Juniper Secure Analytics (JSA) environment, managed hosts (distributed event or flow processors) gather and process event and flow data locally, and feed this information into the JSAx500 console. You do not need to change the JSAx500 distributed setup to prepare for the console migration. However, if any managed hosts have been added to the new Juniper Secure Analytics (JSA) console (which will be restored with the JSAx500 backup), the managed hosts must be removed before the restoration process.

NOTE:

- For JSAx500, x is one of the JSA Series appliances 3, 5, or 7 (JSA3500, JSA5500, or JSA7500).
- For JSAx800, x is one of the JSA Series appliances 3 or 5 (JSA3800 or JSA5800).

To migrate the JSAx500 console to a JSAx800 console:

1. If the JSA appliance has managed hosts defined:
   a. On the JSA console, click the Admin tab to launch the Deployment Editor.
   b. Click the System View tab.
   c. Right-click each managed host, and select **Remove host**.

      NOTE: The Remove host option is only available when the JSA appliance has a managed host connected to it.

   d. Click **OK**.
   e. On the Admin tab, select **Advanced** > **Deploy Full Configuration**.
2. For preparing the console, perform the steps as instructed in the following procedures:
   a. Pre-Upgrade Configuration Backup Process for a JSAx500 Series Appliance on page 8
   b. Upgrading an Existing JSA Appliance on page 9
   c. Backing Up the Existing JSA Appliance Configuration While Running the Common Image on page 11
   d. Installing a JSA and a Virtual JSA Appliance on page 11
   e. Reimaging JSA Series to the Common Image Using the Recovery Partition on page 13
   f. Copying Event and Flow Data to JSA on page 15
3. Follow the steps in "Restoring Backup on a JSA Appliance" on page 14.

To successfully restore the JSAx500 backup, you must select **Deploy Full Configuration**. You will be prompted to disable iptables on the JSAx500 managed hosts. You can ignore this prompt because the old managed hosts are being replaced with JSAx800 managed hosts.

4. Once the restore process is complete, log in to the new JSA console.

   Ignore the error messages on the dashboard if you receive any.

5. 

   NOTE: Connections to the JSAx500 managed hosts are restored along with the configuration. These connections must be removed before you complete the configuration. Before removing each managed host, make a note of the processes assigned to that managed host. After adding corresponding new managed host, remove default processes added by the new host and then assign the corresponding old processes to the new managed host. These old processes should have a red outline as they are currently unassigned. We recommend you to migrate managed hosts one at a time.

   To disconnect each managed host:

   a. On the JSA console, click the Admin tab to launch the Deployment Editor.

   b. Click the System View tab.

   c. Right-click each managed host, and select **Remove host**.

      

      NOTE: This option is available only when the JSA appliance is connected to a managed host.

   d. Click **OK**, and then save and close the Deployment Editor.

   e. On the Admin tab, select **Advanced** > **Deploy Full Configuration**.

6. Follow the steps in "Running Automatic Updates on the JSA Appliance" on page 16 to complete the configuration of the new JSA console.

Related Documentation

- Adding Each New JSA Managed Host to a JSA Console on page 24
- Distributed Environment to JSA Migration Overview on page 21
- JSA Series Appliance Overview on page 3
- JSA Series Migration Overview on page 7
- Migrating Licenses to JSA Series Overview on page 29

Adding Each New JSA Managed Host to a JSA Console

After the successful migration of JSAx500 console to JSAx800, you can connect the managed hosts to the new JSAx800 console.

NOTE:

- For JSAx500, x is one of the JSA Series appliances 3, 5, or 7 (JSA3500, JSA5500, or JSA7500).
- For JSAx800, x is one of the JSA Series appliances 3 or 5 (JSA3800 or JSA5800).

To add the JSA managed hosts to the JSA console:

1. On the JSA console, click the Admin tab to launch the Deployment Editor.
2. Click the System View tab.
3. From the menu, select **Actions** > **Add a Managed Host**.
4. Click **Next**.
5. Enter the values for the following parameters:
   - **Enter the IP of the server or appliance to add**—Type the IP address of the host you want to add to your system view.
   - **Enter the root password of the host**—Type the root password for the host.
   - **Confirm the root password of the host**—Type the password again.
   - **Host is NATed**—Select the check box to use an existing Network Address Translation (NAT) on this managed host.
   - **Enable Encryption**—Select the check box to create an SSH encryption tunnel for the managed host.
   - **Enable Compression**—Select the check box to enable data compression to the managed hosts.
6. Click **Next**.
7. If you select the Host is NATed check box, the Configure NAT Settings page is displayed. Otherwise, continue to Step 9.
8. To configure NAT settings, enter the values for the following parameters:

a. **Enter public IP of the server or appliance to add**—Type the public IP address of the managed host. The managed host uses this IP address to communicate with other managed hosts in different networks using NAT.

b. **Select NATed network**—From the list box, select the network you want this managed host to use:

   a. If the managed host is on the same subnet as the console, select the console of the NATed network.

   b. If the managed host is not on the same subnet as the console, select the managed host of the NATed network.

   c. Click **Next**.

   d. Click **Finish**.

9. Click **Finish**.

10. After adding corresponding new managed host, remove default processes added by the new host and then assign the corresponding old processes to the new managed host. These old processes should have a red outline as they are currently unassigned.

11. From the menu, select **File** > **Save and Close**.

12. On the Admin tab, select **Advanced** > **Deploy Full Configuration**.

Related Documentation

- Distributed Environment to JSA Migration Overview on page 21
- Migrating to a JSA Console on page 22
- Migrating Licenses to JSA Series Overview on page 29
- JSA Series Appliance Overview on page 3

PART 3

JSA Series License Migration

This chapter includes the following topics:

CHAPTER 4

Migrating Licenses to JSA Series

Migrating Licenses to JSA Series Overview

Juniper Networks supports the migration of licenses from existing JSAx500 Series to the JSAx800 Series appliances.

NOTE:

- For JSAx500, x is one of the JSA Series appliances 3, 5, or 7 (JSA3500, JSA5500, or JSA7500).
- For JSAx800, x is one of the JSA Series appliances 3 or 5 (JSA3800 or JSA5800).

To migrate an existing Juniper Secure Analytics (JSAx500) licenses to JSAx800, you need to access License Management System (LMS) or access LMS through the Juniper Customer Support Center (CSC). For more information, see "JSA Series License Migration Assistance" on page 30.

Juniper Networks also supports the migration of licenses from the JSAx500 Series to the JSA virtual appliances. To migrate from the JSAx500 Series to the JSA virtual appliances, you need to purchase the virtual appliance license.

Related Documentation

- Obtaining the Serial Number of a JSA Series Appliance on page 30
- JSA Series License Migration Assistance on page 30
- JSA Series Appliance Overview on page 3
- JSA Series Migration Overview on page 7
- Configuration and Data Features for JSA Migration on page 4
- Distributed Environment to JSA Migration Overview on page 21

Obtaining the Serial Number of a JSA Series Appliance

The serial number for a JSA appliance is a 16-digit number, for example, 0249032008000081. You can locate the serial number label on the back of the appliance.

NOTE:

- For JSAx500, x is one of the JSA Series appliances 3, 5, or 7 (JSA3500, JSA5500, or JSA7500).
- For JSAx800, x is one of the JSA Series appliances 3 or 5 (JSA3800 or JSA5800).

To obtain the serial number of an JSAx500 or a JSA appliance remotely:

1. Using SSH, log in to your JSA appliance as the root user.
2. Run the following **dmidecode** command to retrieve the serial number of the appliance:
   # dmidecode -s system-serial-number

Related Documentation

- Migrating Licenses to JSA Series Overview on page 29
- JSA Series License Migration Assistance on page 30
- JSA Series Appliance Overview on page 3
- JSA Series Migration Overview on page 7
- Distributed Environment to JSA Migration Overview on page 21

JSA Series License Migration Assistance

If you need assistance while migrating a JSA appliance, open a support case using the Case Manager link at http://www.juniper.net/support/, or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).

To migrate an existing Juniper Secure Analytics (JSAx500) licenses to JSAx800:

NOTE:

- For JSAx500, x is one of the JSA Series appliances 3, 5, or 7 (JSA3500, JSA5500, or JSA7500).
- For JSAx800, x is one of the JSA Series appliances 3 or 5 (JSA3800 or JSA5800).

1. Go to License Management System (LMS) or access LMS through the Juniper Customer Support Center (CSC).
2. Log in to LMS with your username and password.
3. Under Generate Licenses, select **Secure Analytics (STRM)** from the list and then click **GO**.
4. Select **Secure Analytics (STRM) Appliance** and then click **Continue**.
5. To transfer unlocking keys to a JSA appliance:
   a. Click **Transfer unlocking keys to Secure Analytics devices**.
   b. Enter the serial number of the JSAx500 appliance in **Transfer From Serial Number** and the serial number of the JSA appliance in **Transfer To Serial Number**.

      After the availability of the software licenses to transfer is confirmed, LMS starts transferring the license and generates new unlocking keys.
   c. Go to Step 7.
6. To transfer unlocking keys to the multiple JSA appliances:
   a. Click **Transfer unlocking keys to Secure Analytics devices**.
   b. Click **Transfer unlocking keys to multiple Secure Analytics devices** to transfer license keys from multiple JSAx500 appliances to JSA appliances, and then follow the instructions provided on the page.

      LMS initiates the license transfer in the background. Once the license transfer is complete, you will receive an e-mail notification.
7. Click **Review**.
8. Click **Continue**.

NOTE: If the JSA appliance has the capacity already, then the capacity/key is archived. A new key is generated for the JSA appliance with the transferred capacity.

9. To enter the new license keys in your Secure Analytics appliances:
   a. Log in to the JSA WebUI.
   b. Click the Admin tab.
   c. On the navigation menu, click **System Configuration**.
   d. Click **System and License Management**.
   e. Click the Upload License tab.
   f. Allocate the license to appropriate hosts once the license file is uploaded.
   g. Click **Deploy License Changes** after the license is allocated to hosts.

Related Documentation

- Migrating Licenses to JSA Series Overview on page 29
- Obtaining the Serial Number of a JSA Series Appliance on page 30
- JSA Series Appliance Overview on page 3
- JSA Series Migration Overview on page 7
- Distributed Environment to JSA Migration Overview on page 21