Engineering
Simplicity

Juniper Secure Analytics Installation Guide

Published
2021-03-26

Release
7.4.1

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

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

Juniper Secure Analytics Installation Guide
7.4.1

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About the Documentation

IN THIS SECTION

Use this guide to understand how to install JSA in your network.

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 viii 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 viii 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

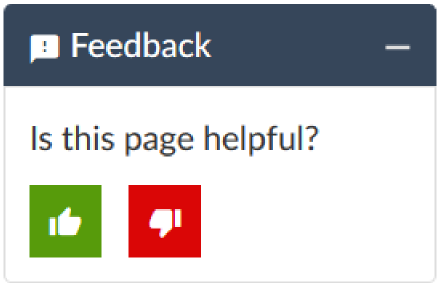
Table 2: Text and Syntax Conventions *(continued)*

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:



Feedback

Is this page helpful?

  - 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 Deployment Overview

JSA Deployment Overview

You can install JSA on a single server for small enterprises, or across multiple servers for large enterprise environments.

For maximum performance and scalability, you must install a high-availability (HA) managed host appliance for each system that requires HA protection. For more information about installing or recovering an HA system, see the *Juniper Secure Analytics High Availability Guide*.

RELATED DOCUMENTATION

License Keys | **14**

JSA Components | **14**

Prerequisite Hardware Accessories for JSA Installations | **17**

Management Controller

The JSA appliances use a management controller for systems-management functions.

JSA appliances contain an integrated service processor, which provides advanced service processor control, monitoring, and alerting functions and consolidates the service processor functionality, super I/O, video controller, and remote presence capabilities into a single chip on the server system board.

For more information about the Lenovo management controller, see Lenovo XClarity Controller.

For instructions on how to configure the Lenovo management controller, see XClarity Controller User Guide.

RELATED DOCUMENTATION

JSA Components | **14**

Prerequisite Hardware Accessories for JSA Installations | **17**

Supported Web Browsers | **18**

License Keys

After you install JSA, you must apply your license keys.

Your system includes a temporary license key that provides you with access to JSA software for five weeks. After you install the software and before the default license key expires, you must add your purchased licenses.

The following table describes the restrictions for the default license key:

Table 3: Restrictions for the Default License Key for JSA Installations

Usage	Limit
Events per second threshold **NOTE:** This restriction also applies to the default license key for Log Manager.	5000
Flows per interval	200000

When you purchase a JSA product, an email that contains your permanent license key is sent from Juniper Networks. These license keys extend the capabilities of your appliance type and define your system operating parameters. You must apply your license keys before your default license expires.

RELATED DOCUMENTATION

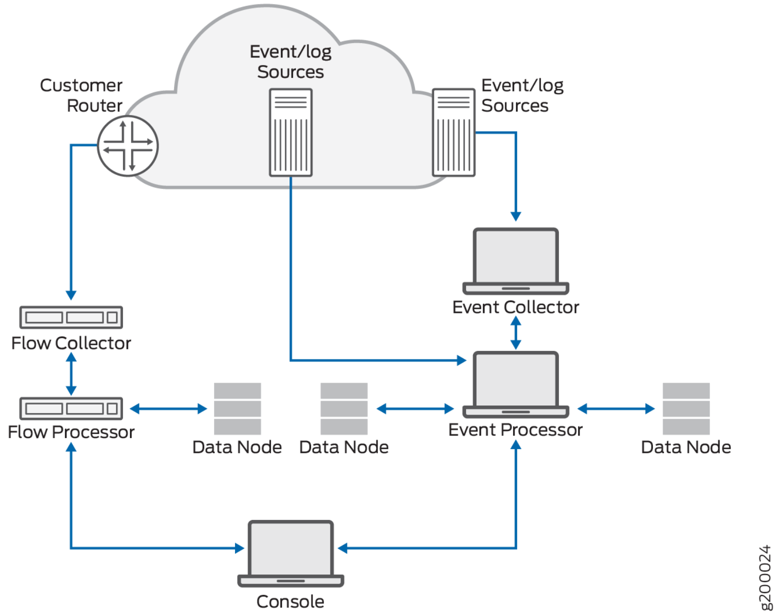
JSA Components | 14
Prerequisite Hardware Accessories for JSA Installations | 17
Supported Web Browsers | 18

JSA Components

JSA consolidates event data from log sources that are used by devices and applications in your network. Figure 1 on page 15 shows JSA components.

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

Figure 1: JSA Components



JSA deployments can include the following components:

JSA Flow Processor

Passively collects traffic flows from your network through span ports or network taps. The JSA Flow Processor also supports the collection of external flow-based data sources, such as NetFlow.

JSA Console

Provides the JSA product user interface. The interface delivers real-time event and flow views, reports, offenses, asset information, and administrative functions.

In distributed JSA deployments, use the JSA console to manage hosts that include other components.

Magistrate

A service running on the JSA console, the Magistrate provides the core processing components. You can add one Magistrate component for each deployment. The Magistrate provides views, reports, alerts, and analysis of network traffic and security events.

The Magistrate component processes events against the custom rules. If an event matches a rule, the Magistrate component generates the response that is configured in the custom rule.

For example, the custom rule might indicate that when an event matches the rule, an offense is created. If there is no match to a custom rule, the Magistrate component uses default rules to process the event. An offense is an alert that is processed by using multiple inputs, individual events, and events that are combined with analyzed behavior and vulnerabilities. The Magistrate component prioritizes the offenses and assigns a magnitude value that is based on several factors, including number of events, severity, relevance, and credibility.

JSA Event Collector

Gathers events from local and remote log sources. Normalizes raw log source events. During this process, the Magistrate component, on the JSA Console, examines the event from the log source and maps the event to a JSA Identifier (QID). Then, the Event Collector bundles identical events to conserve system usage and sends the information to the Event Processor.

JSA Event Processor

Processes events that are collected from one or more Event Collector components. The Event Processor correlates the information from JSA products and distributes the information to the appropriate area, depending on the type of event. The Event Processor can also collect events if you do not have an Event Collector in your deployment.

The Event Processor also includes information that is gathered by JSA products to indicate behavioral changes or policy violations for the event. When complete, the Event Processor sends the events to the Magistrate component.

When to add Event Processors: if you collect and store events in a different country or state, you may need to add Event Processors to comply with local data collection laws.

Data Node

Data Nodes enable new and existing JSA deployments to add storage and processing capacity on demand as required. Data Notes increase the search speed on your deployment by allowing you to keep more of your data uncompressed.

You can scale storage and processing power independently of data collection, which results in a deployment that has the appropriate storage and processing capacity. Data Nodes are plug-n-play and can be added to a deployment at any time. Data Nodes seamlessly integrate with the existing deployment.

Increasing data volumes in deployments require data compression sooner. Data compression slows down system performance as the system must decompress queried data before analysis is possible. Adding Data Node appliances to a deployment allows you to keep data uncompressed longer.

For more information about Data Nodes, see the "Data Node Overview" on page 59.

RELATED DOCUMENTATION

Prerequisite Hardware Accessories for JSA Installations | 17

Supported Web Browsers | 18

USB Flash Drive Installations | 18

Prerequisite Hardware Accessories for JSA Installations

Before you install JSA products, ensure that you have access to the required hardware accessories and desktop software.

Hardware Accessories

Ensure that you have access to the following hardware components:

- Monitor and keyboard, or a serial console
- Uninterrupted Power Supply (UPS) for all systems that store data, such as JSA console, Event Processor components, or JSA flow processor components
- Null modem cable if you want to connect the system to a serial console

> **NOTE:** JSA products support hardware-based Redundant Array of Independent Disks (RAID) implementations, but do not support software-based RAID installations or hardware assisted RAID installations.

RELATED DOCUMENTATION

Supported Web Browsers | 18
USB Flash Drive Installations | 18
Third-party Software on JSA Appliances | 26

Environmental Restrictions

JSA performance can be affected by other devices in your deployment.

For any DNS server that you point a JSA appliance to, you cannot have a DNS registry entry with the hostname set to **localhost**.

Supported Web Browsers

For the features in JSA products to work properly, you must use a supported web browser.

The following table lists the supported versions of web browsers.

Table 4: Supported Web Browsers for JSA Products

Web browser	Supported versions
64 bit Mozilla Firefox	60 Extended Support Release and later
64-bit Microsoft Edge	38.14393 and later
64 bit Google Chrome	Latest

The Microsoft Internet Explorer web browser is no longer supported as of JSA 7.4.0.

Security Exceptions and Certificates

If you are using the Mozilla Firefox web browser, you must add an exception to Mozilla Firefox to log in to JSA. For more information, see your Mozilla Firefox web browser documentation.

Navigate the Web-Based Application

When you use JSA, use the navigation options available in the JSA user interface instead of your web browser **Back** button.

RELATED DOCUMENTATION

USB Flash Drive Installations | 18
Third-party Software on JSA Appliances | 26
JSA Components | 14

USB Flash Drive Installations

You can install JSA software with a USB flash drive.

USB flash drive installations are full product installations. You cannot use a USB flash drive to upgrade or apply product patches. For information about applying patches, see the latest Patch Release Notes.

Supported Versions

The following appliances or operating systems can be used to create a bootable USB flash drive:

- A Linux system that is installed with Red Hat Enterprise Linux V7.7
- Apple Mac OS X
- Microsoft Windows

Installation Overview

Follow this procedure to install JSA software from a USB flash drive:

1. Create the bootable USB flash drive.
2. Install the software for your JSA appliance.
3. Install any product maintenance releases or patches.

   See latest patch Release Notes for installation instructions for patches..

Creating a Bootable USB Flash Drive with Microsoft Windows

Use the Fedora Media Writer app on a Windows system to create a bootable USB flash drive that you can use to install JSA software.

You must have access to an 8 GB or larger USB flash drive.

NOTE: It is recommended to download the latest version of the Fedora Media Writer app.

1. On your Windows system, download and install the Fedora Media Writer app from the Fedora Media Writer GitHub repository.

   Other media creation tools might work to create the bootable flash drive, but the JSA ISO is a modified Red Hat ISO, and Red Hat suggests Fedora Media Writer. For more information, see Making Installation USB Media.

2. On your Windows system, download the JSA ISO image file from https://support.juniper.net/support/downloads/ to a local drive.

3. Insert the USB flash drive into a USB port on your Windows system.

   NOTE: Any files stored on the USB flash drive are overwritten when creating the bootable flash drive.

4. Open Fedora Media Writer and in the main window, click **Custom Image**.

5. Browse to where you downloaded the JSA ISO on your Windows system and select it.

6. Select the USB flash drive from the Fedora Media Writer menu, and then click **Write to disk**.

7. When the writing process is complete, click **Close** and remove the USB flash drive from your system. For more information about installing JSA software, see “Installing JSA with a USB Flash Drive” on page 22.

Creating a Bootable USB Flash Drive on an Apple Mac OS X System

You can use an Apple Mac OS X computer to create a bootable USB flash drive that you can use to install JSA software.

You must have access to the following items:

- A 8 GB or larger USB flash drive
- A JSA 7.3.1 or later ISO image file

When you create a bootable USB flash drive, the contents of the flash drive are deleted.

1. Download the JSA ISO image file from the https://support.juniper.net/support/downloads/.

2. . Insert the USB flash drive into a USB port on your system.

3. Open a terminal and type the following command to unmount the USB flash drive:

   ```
   diskutil unmountDisk /dev/<name_of_the_connected_USB_flash_drive>
   ```

4. Type the following command to write the JSA ISO to your USB flash drive:

   ```
   dd if=/<jsa.iso>of=/dev/ r <name_of_the_connected_USB_flash_drive>bs=1m
   ```

NOTE: The **r** before the name of the connected USB flash drive is for raw mode, which makes the transfer much faster. There is no space between the **r** and the name of the connected USB flash drive.

5. Remove the USB flash drive from your system.

Creating a Bootable USB Flash Drive with Red Hat Linux

You can use a Linux desktop or notebook system with Red Hat V7 or higher to create a bootable USB flash drive that you can use to install JSA software.

You must have access to the following items:

- An 8 GB or larger USB flash drive
- A JSA 7.4.1 or later ISO image file

When you create a bootable USB flash drive, the contents of the flash drive are deleted.

1. Download the JSA ISO image file from the https://support.juniper.net/support/downloads/.

2. Insert the USB flash drive in the USB port on your system.

   It might take up to 30 seconds for the system to recognize the USB flash drive.

3. Open a terminal and type the following command to determine the name of the USB flash drive:

   ```
   dmesg | grep SCSI
   ```

   The system outputs the messages produced by device drivers. The following example shows the name of the connected USB flash drive as sdb.

   ```
   [ 170.171135] sd 5:0:0:0: [sdb] Attached SCSI removable disk
   ```

4. Type the following commands to unmount the USB flash drive:

   ```
   df -h | grep<name_of_the_connected_USB_flash_drive>
   umount /dev/<name_of_the_connected_USB_flash_drive>
   ```

   Example:

```
[root@jsa ~]# dmesg | grep SCSI
[93425.566934] sd 14:0:0:0: [sdb] Attached SCSI removable disk
[root@jsa ~]# df -h | grep sdb
[root@jsa ~]# umount /dev/sdb
umount: /dev/sdb: not mounted
```

5. Type the following command to write the JSA ISO to your USB flash drive:

   ```
   dd if=/<jsa.iso>of=/dev/<name_of_the_connected_USB_flash_drive> bs=512k
   ```

   Example:

   ```
   [root@jsa ~]# dd if=7.4.1.20200716115107.iso of=/dev/sdb bs=512k
   11112+0 records in
   11112+0 records out
   5825888256 bytes (5.8 GB) copied, 1085.26 s, 5.4 MB/s
   ```

6. Remove the USB flash drive from your system. For more information about installing JSA software, see "Installing JSA with a USB Flash Drive" on page 22.

Installing JSA with a USB Flash Drive

Follow this procedure to install JSA from a bootable USB flash drive.

You must create the bootable USB flash drive before you can use it to install JSA software.

This procedure provides general guidance on how to use a bootable USB flash drive to install JSA software.

The complete installation process is documented in the product Installation Guide.

1. Install all necessary hardware.

2. Choose one of the following options:
   - Connect a notebook to the serial port at the back of the appliance.
   - Connect a keyboard and monitor to their respective ports.

3. Insert the bootable USB flash drive into the USB port of your appliance.

4. Restart the appliance.

Most appliances can boot from a USB flash drive by default. If you are installing JSA software on your own hardware (only supported for Data Nodes), you might have to set the device boot order to prioritize USB.

After the appliance starts, the USB flash drive prepares the appliance for installation. This process can take up to an hour to complete.

5. When the login prompt is displayed, type **root** to log in to the system as the root user.

   The user name is case-sensitive.

6. Press **Enter** and follow the prompts to install JSA.

   The complete installation process is documented in the product Installation Guide.

RELATED DOCUMENTATION

Third-party Software on JSA Appliances | 26

JSA Components | 14

Supported Web Browsers | 18

Standard Linux Users | 23

Standard Linux Users

The tables describe the standard Linux user accounts that are created on the JSA console and other JSA product components (All In One console, JSA Risk Manager, QRadar Network Insights, App Host, and all other managed hosts).

The following tables show standard Linux user accounts for RedHat and JSA.

Table 5: Standard Linux User Accounts for RedHat

User Account	Login to the Login Shell	Purpose
root (password required)	Yes	RedHat user
bin	No	Linux Standard Base
daemon	No	Linux Standard Base

Table 5: Standard Linux User Accounts for RedHat *(continued)*

User Account	Login to the Login Shell	Purpose
adm	No	Linux Standard Base
lp	No	Linux Standard Base
sync	No	Linux Standard Base
shutdown	No	Linux Standard Base
halt	No	Linux Standard Base
mail	No	Linux Standard Base
operator	No	Linux Standard Base
games	No	RedHat user
ftp	No	RedHat user
nobody	No	Linux Standard Base
systemd-network	No	RedHat user
dbus	No	RedHat user
polkitd	No	RedHat user
sshd	No	RedHat user
rpc	No	RedHat user
rpcuser	No	RedHat user
nfsnobody	No	RedHat user
abrt	No	RedHat user
ntp	No	RedHat user
tcpdump	No	RedHat user

Table 5: Standard Linux User Accounts for RedHat *(continued)*

User Account	Login to the Login Shell	Purpose
tss	No	RedHat user
saslauth	No	RedHat user
sssd	No	RedHat user

Table 6: Standard Linux User Accounts for JSA

User Account	Login to the Login Shell	Purpose
ziptie	No	Ziptie service used by JSA Risk Manager
si-vault	No	JSA Vault service used by JSA to store secrets and manage internal certificates
vis	No	JSA VIS service used by JSA to process scan results
si-registry	No	JSA Docker Registry Service used by JSA for App Framework
customactionuser	No	JSA Custom Actions used to isolate custom actions into a chroot jail
mks	No	MKS JSA component for handling secrets
qradar	No	General user for JSA
qvmuser	No	JSA Vulnerability Manager
postgres	No (account locked)	PostgreSQL database used by JSA
tlsdated	No	Tlsdate legacy time sync tool that was previously used by JSA
traefik	No	Traefik service proxies Docker Containers for JSA App Framework

Table 6: Standard Linux User Accounts for JSA *(continued)*

User Account	Login to the Login Shell	Purpose
gluster	No	GlusterFS used by JSA HA on event collectors
openvpn	No	OpenVPN optional VPN tool installed by JSA
chrony	No	Chronyd service time sync tool used by JSA
apache	No	Apache Web Server used by JSA
postfix	No	Mail Service used by JSA to send email

RELATED DOCUMENTATION

USB Flash Drive Installations | 18
Third-party Software on JSA Appliances | 26
JSA Components | 14

Third-party Software on JSA Appliances

JSA is a security appliance that is built on Linux, and is designed to resist attacks. JSA is not intended as a multi-user, general-purpose server. It is designed and developed specifically to support its intended functions. The operating system and the services are designed for secure operation. JSA has a built-in firewall, and allows administrative access only through a secure connection that requires encrypted and authenticated access, and provides controlled upgrades and updates. JSA does not require or support traditional anti-virus or malware agents, or support the installation of third-party packages or programs.

RELATED DOCUMENTATION

JSA Components | 14
Supported Web Browsers | 18

2

CHAPTER

Bandwidth for Managed Hosts

Bandwidth for Managed Hosts

To replicate state and configuration data, ensure that you have a minimum bandwidth of 100 Mbps between the JSA console and all managed hosts. Higher bandwidth is necessary when you search log and network activity, and you have over 10,000 events per second (EPS).

An Event Collector that is configured to store and forward data to an Event Processor forwards the data according to the schedule that you set. Ensure that you have sufficient bandwidth to cover the amount of data that is collected, otherwise the forwarding appliance cannot maintain the scheduled pace.

Use the following methods to mitigate bandwidth limitations between data centers:

- Process and send data to hosts at the primary data center-- Design your deployment to process and send data as it's collected to hosts at the primary data center where the console resides. In this design, all user-based searches query the data from the local data center rather than waiting for remote sites to send back data.

  You can deploy a store and forward event collector, such as a JSA physical or virtual appliance, in the remote locations to control bursts of data across the network. Bandwidth is used in the remote locations, and searches for data occur at the primary data center, rather than at a remote location.

- Don't run data-intensive searches over limited bandwidth connections-- Ensure that users don't run data-intensive searches over links that have limited bandwidth. Specifying precise filters on the search limits the amount of data that is retrieved from the remote locations, and reduces the bandwidth that is required to send the query result back.

For more information about deploying managed hosts and components after installation, see the *Juniper Secure Analytics Administration Guide*.

3

CHAPTER

Installing a JSA Console or Managed Host

Installing a JSA Console or Managed Host

Install JSA Console or a managed host on the JSA appliance.

Software versions for all JSA appliances in a deployment must be same version and patch level. Deployments that use different versions of software is not supported.

Ensure that the following requirements are met:

- The required hardware is installed.
- You have the required license key for your appliance.
- A keyboard and monitor are connected by using the VGA connection.
- There are no expired licenses on either the console or the managed hosts.

1. Use SSH to log in as the root user.

2. Accept the **End User License Agreement**.

3. Select the appliance assignment, and then select **Next**.

4. If you selected an appliance for high-availability (HA), select whether the appliance is a console.

5. For the type of setup, select **Normal Setup (default)** or **HA Recovery Setup**, and set up the time.

6. If you selected **HA Recovery Setup**, enter the cluster virtual IP address.

7. Select the Internet Protocol version:

   - Select **ipv4** or **ipv6**.

8. If you selected **ipv6**, select **manual** or **auto** for the **Configuration type**.

9. Select the bonded interface setup, if required.

10. Select the management interface.

11. In the wizard, enter a fully qualified domain name in the **Hostname** field.

12. In the **IP address** field, enter a static IP address, or use the assigned IP address.

> **NOTE:** If you are configuring this host as a primary host for a high availability (HA) cluster, and you selected **Yes** for auto-configure, you must record the automatically-generated IP address. The generated IP address is entered during HA configuration.

For more information, see the *Juniper Secure Analytics High Availability Guide*.

13. If you do not have an email server, enter **localhost** in the **Email server name** field.

14. Enter **root** and **admin** passwords that meet the following criteria:
    - Contains at least 5 characters
    - Contains no spaces
    - Can include the following special characters: @, #, ^, and *.

15. Click **Finish**.

16. Follow the instructions in the installation wizard to complete the installation.

    A series of messages appears as JSA continues with the installation. Based on the appliance ID selected, the installation process may take from several minutes to few hours to complete. TA **All-In-One** or **Console** installation may take up to 2.5 hours. When the JSA installation process is complete, the message window appears.

17. Apply your license key.
    a. Log in to JSA:

       The default user name is **admin**. The password is the password of the admin user account.

    b. Click **Login To JSA**.
    c. Click the **Admin** tab.
    d. In the navigation pane, click **System Configuration**.
    e. Click the **System and License Management** icon.
    f. From the **Display** list box, select **Licenses**, and upload your license key.
    g. Select the unallocated license and click **Allocate System to License**.
    h. From the list of systems, select a system, and click **Allocate System to License**.

18. If you want to add managed hosts, see the *Juniper Secure Analytics Administration Guide*.

Installing a JSA Console or Managed Host (applicable only for JSA 7.3.1 Patch 9, JSA 7.3.2 Patch 2, and JSA 7.3.2 Patch 3)

Install JSA Console or a managed host on the JSA appliance.

Software versions for all JSA appliances in a deployment must be same version and patch level. Deployments that use different versions of software is not supported.

Ensure that the following requirements are met:

- The required hardware is installed.
- You have the required license key for your appliance.
- A keyboard and monitor are connected by using the VGA connection.
- There are no expired licenses on either the console or the managed hosts.

1. Use SSH to log in as the root user.

2. Accept the **End User License Agreement**.

3. Select the appliance type from the following options, and then select **Next**.

   - Appliance Install (purchased as an appliance)—Choose this option if you have purchased JSA appliances or wish to install virtual machines.
   - Software Install (hardware was purchased separately)—Choose this option if you want to install the software on your own hardware.

     > **NOTE:** Software only installations are supported for the 7.3.1 patch 9, 7.3.2 Patch 2, and 7.3.2 Patch 3 releases. Choose **Appliance Install (purchased as an appliance)** for all other implementation choices.

   - High Availability Appliance—Choose this option to use high-availability (HA) appliances.

4. Select the non-software appliance type and then select **Next**.

5. For the type of setup, select **Normal Setup (default)** or **HA Recovery Setup**, and set up the time.

6. If you selected **HA Recovery Setup**, enter the cluster virtual IP address.

7. Select the Internet Protocol version:

   - Select **ipv4** or **ipv6**.

8. If you selected **ipv6**, select **manual** or **auto** for the **Configuration type**.

9. Select the bonded interface setup, if required.

10. Select the management interface.

11. In the wizard, enter a fully qualified domain name in the **Hostname** field.

12. In the **IP address** field, enter a static IP address, or use the assigned IP address.

    > **NOTE:** If you are configuring this host as a primary host for a high availability (HA) cluster, and you selected **Yes** for auto-configure, you must record the automatically-generated IP address. The generated IP address is entered during HA configuration.

    For more information, see the *Juniper Secure Analytics High Availability Guide*.

13. If you do not have an email server, enter **localhost** in the **Email server name** field.

14. Enter **root** and **admin** passwords that meet the following criteria:

    - Contains at least 5 characters
    - Contains no spaces
    - Can include the following special characters: @, #, ^, and *.

15. Click **Finish**.

16. Follow the instructions in the installation wizard to complete the installation.

    A series of messages appears as JSA continues with the installation. Based on the appliance ID selected, the installation process may take from several minutes to few hours to complete. TA **All-In-One** or **Console** installation may take up to 2.5 hours. When the JSA installation process is complete, the message window appears.

17. Apply your license key.

    a. Log in to JSA:

       The default user name is **admin**. The password is the password of the admin user account.

    b. Click **Login To JSA**.

c. Click the **Admin** tab.

d. In the navigation pane, click **System Configuration**.

e. Click the **System and License Management** icon.

f. From the **Display** list box, select **Licenses**, and upload your license key.

g. Select the unallocated license and click **Allocate System to License**.

h. From the list of systems, select a system, and click **Allocate System to License**.

18. If you want to add managed hosts, see the *Juniper Secure Analytics Administration Guide*.

4

CHAPTER

Virtual Appliance Installations for JSA and Log Manager

Virtual Appliance Installations for JSA and Log Manager

You can install JSA and Log Manager on a virtual appliance. Ensure that you use a supported virtual appliance that meets the minimum system requirements.

You can install JSA on your virtual appliance through an appliance installation.

Appliance installation

An appliance installation is a JSA installation that uses the version of RHEL included on the JSA ISO. An appliance installation requires you purchase an RHEL license. Contact your JSA sales representative for more information about purchasing an RHEL license. You do not need to configure partitions or perform other RHEL preparation as part of an appliance installation. Choose this option if RHEL is not already installed.

NOTE: If the installer does not detect that RHEL is installed, an appliance installation is performed automatically.

To install a virtual appliance, complete the following tasks in sequence:

- Create a virtual machine.
- Install JSA software on the virtual machine.
- If your virtual appliance is a managed host, add your virtual appliance to the deployment.

NOTE: Install no software other than JSA and Red Hat Enterprise Linux on the virtual machine.

RELATED DOCUMENTATION

Overview Of Supported Virtual Appliances | 38

Creating Your Virtual Machine | 48

Installing JSA on a Virtual Machine | 49

Overview Of Supported Virtual Appliances

A virtual appliance provides the same visibility and function in your virtual network infrastructure that JSA appliances provide in your physical environment.

The following virtual appliances are available:

- JSA Threat Analytics “All-in-one” or Console 3199
- JSA Event and Flow Processor Combo
- JSA Flow Processor Virtual 1799
- JSA Event Processor Virtual 1699
- JSA Event Collector Virtual 1599
- JSA Flow Processor
- JSA Flow Processor Virtual 1299
- JSA Risk Manager 700
- JSA Vulnerability Manager Processor 600
- JSA Vulnerability Manager Scanner 610
- JSA App Host 4000

JSA Threat Analytics “All-in-one” or Console 3199

This virtual appliance is a Juniper Secure Analytics system that profiles network behavior and identifies network security threats. The JSA JSA Threat Analytics “All-in-one” or Console 3199 virtual appliance includes an on-board Event Collector, a combined Event Processor and Flow Processor, and internal storage for events.

The JSA Threat Analytics “All-in-one” or Console 3199 virtual appliance supports the following items:

- Up to 1,000 network objects
- 1,200,000 flows per interval, depending on your license
- 30,000 Events Per Second (EPS), depending on your license
- External flow data sources for NetFlow, sFlow, J-Flow, Packeteer, and Flowlog files
- Flow Processor and Layer 7 network activity monitoring

To expand the capacity of the JSA Threat Analytics “All-in-one” or Console 3199 beyond the license-based upgrade options, you can add one or more of the JSA Virtual Event Processor Virtual 1699 or Flow processor Virtual 1799 virtual appliances.

JSA Event and Flow Processor Combo

This virtual appliance is deployed with any JSA Console. The virtual appliance is used to increase storage and includes a combined Event Processor and Flow Processor and internal storage for events and flows.

JSA Event and Flow Processor Combo appliance supports the following items:

- 1,200,000 flows per interval, depending on traffic types
- 30,000 Events Per Second (EPS), depending on your license
- 2 TB or larger dedicated flow storage
- 1,000 network objects
- JSA Flow Collector and Layer 7 network activity monitoring

You can add JSA Event and Flow Processor Combo appliances to any JSA Console to increase the storage and performance of your deployment.

JSA Flow Processor Virtual 1799

This virtual appliance is a dedicated Flow Processor that you can use to scale your JSA deployment to manage higher flows per interval rates. The JSA Flow Processor Virtual 1799 includes an onboard Flow Processor and internal storage for flows.

JSA Flow Processor Virtual 1799 appliance supports the following items:

- 3,600,000 flows per interval, depending on traffic types
- 2 TB or larger dedicated flow storage
- 1,000 network objects
- Flow Processor and Layer 7 network activity monitoring

The JSA Flow Processor Virtual 1799 is a distributed Flow Processor virtual appliance and requires a connection to JSA console. Flow Processor appliance and requires a connection to any series appliance.

JSA Event Processor Virtual 1699

This virtual appliance is a dedicated Event Processor that allows to scale your Juniper Secure Analytics (JSA) deployment to manage higher EPS rates. The JSA Event Processor Virtual 1699 includes an onboard Event Collector, Event Processor, and internal storage for events.

JSA Event Processor Virtual 1699 appliance supports the following items:

- Up to 80,000 events per second
- 2 TB or larger dedicated event storage

The JSA Event Processor Virtual 1699 is a distributed Event Processor virtual appliance and requires a connection to JSA console. Event Processor appliance and requires a connection to any series appliance.

JSA Event Collector Virtual 1599

This virtual appliance is a dedicated Event Collector that you can use to scale your JSA deployment to manage higher EPS rates. The JSA Event Collector Virtual 1599 includes an onboard Event Collector.

JSA Event Collector Virtual 1599 appliance supports the following items:

- Up to 80,000 events per second
- 2 TB or larger dedicated event storage

The JSA Event Collector Virtual 1599 is a distributed Event Collector virtual appliance and requires a connection to JSA console. Event Collector appliance and requires a connection to any series appliance.

JSA Flow Processor

This virtual appliance provides retention and storage for events and flows. The virtual appliance expands the available data storage of Event Processors and Flow Processors, and also improves search performance.

NOTE: Encrypted data transmission between Data Nodes and Event Processors is not supported. The following firewall ports must be opened for Data Node communication with the Event Processor:

- Port 32006 between Flow Processor and the Event Processor appliance
- Port 32006 between Flow Processor and the Event Processor appliance

Size your JSA Flow Processor appliance based on the EPS rate and data retention rules of the deployment.

Data retention policies are applied to a JSA Flow Processor appliance in the same way that they are applied to stand-alone Event Processors and Flow Processors. The data retention policies are evaluated on a node-by-node basis. Criteria, such as free space, is based on the individual JSA Flow Processor appliance and not the cluster as a whole.

JSA Flow Processor can be added to the following appliances:

- Event Processor (16XX)
- Flow Processor (17XX)
- Event/Flow Processor (18XX)
- All-In-One (31XX)

To enable all features included in the JSA Flow Processor appliance, install it by using the Flow Processor appliance type.

JSA Flow Processor Virtual 1299

This virtual appliance provides the same visibility and function in your virtual network infrastructure that a JSA Flow Processor offers in your physical environment. The JSA Flow Processor virtual appliance analyzes network behavior and provides Layer 7 visibility within your virtual infrastructure. Network visibility is derived from a direct connection to the virtual switch.

The JSA Flow Processor Virtual 1299 virtual appliance supports a maximum of the following items:

- 10,000 flows per minute
- Three virtual switches, with one more switch that is designated as the management interface.

JSA Vulnerability Manager Processor

This appliance is used to process vulnerabilities within the applications, systems, and devices on your network or within your DMZ. The vulnerability processor provides a scanning component by default. If required, you can deploy more scanners, either on dedicated JSA Vulnerability Manager managed host scanner appliances or JSA managed hosts. For example, you can deploy a vulnerability scanner on an Event Collector or JSA Flow Processor.

JSA Vulnerability Manager Scanner

This appliance is used to scan for vulnerabilities within the applications, systems, and devices on your network or within your DMZ.

JSA Risk Manager

This appliance is used for monitoring device configurations, simulating changes to your network environment, and prioritizing risks and vulnerabilities in your network.

JSA App Host 4000

This appliance is a managed host that is dedicated to running apps. App Hosts provide extra storage, memory, and CPU resources for your apps without impacting the processing capacity of your JSA Console. Apps such as User Behavior Analytics with Machine Learning Analytics require more resources than are currently available on the Console.

RELATED DOCUMENTATION

Creating Your Virtual Machine | 48

Installing JSA on a Virtual Machine | 49

Adding Your Virtual Appliance to Your Deployment | 51

System Requirements for Virtual Appliances

To ensure that JSA works correctly, you must use virtual appliances that meet the minimum requirements.

For more information about supported hypervisors and virtual hardware versions, see “Creating Your Virtual Machine” on page 48.

NOTE: The minimum requirements support JSA functionality with minimum data sets and performance. The minimum requirements support a JSA system that uses only the default apps. For optimal performance, use the suggested requirements.

Memory Requirements

The following table describes the memory requirements for virtual appliances.

Table 7: Minimum and Suggested Memory Requirements for JSA Virtual Appliances

Appliance	Minimum memory requirement	Suggested memory requirement
JSA Flow Processor Virtual 1299	6 GB	6 GB
JSA Flow Processor	24 GB	48 GB
JSA Event Collector Virtual 1599	12 GB	16 GB
JSA Event Processor Virtual 1699 up to 20,000 EPS	12 GB	48 GB
JSA Event Processor Virtual 1699 20,000 EPS or higher	128 GB	128 GB
JSA Flow Processor Virtual 1799 up to 1,200,000 FPM	12 GB	48 GB
JSA Flow Processor Virtual 1799 1,200,000 FPM or higher	128 GB	128 GB
JSA Event and Flow Processor Combo 5,000 EPS or less 200,000 FPM or less	12 GB	48 GB
JSA Event and Flow Processor Combo 30,000 EPS or less 1,000,000 FPM or less	128 GB	128 GB

Table 7: Minimum and Suggested Memory Requirements for JSA Virtual Appliances *(continued)*

Appliance	Minimum memory requirement	Suggested memory requirement
JSA Threat Analytics “All-in-one” or Console 3199 5,000 EPS or less 200,000 FPM or less	32 GB	48 GB
JSA Threat Analytics “All-in-one” or Console 3199 30,000 EPS or less 1,000,000 FPM or less	64 GB	128 GB
Virtual JSA Log Manager	24 GB	48 GB
JSA Risk Manager	24 GB	48 GB
JSA Vulnerability Manager Processor	32 GB	32 GB
JSA Vulnerability Manager Scanner	16 GB	16 GB
JSA App Host	12 GB	64 GB or more for a medium sized App Host 128 GB or more for a large sized App Host

Processor requirements

The following table describes the CPU requirements for virtual appliances.

Table 8: CPU Requirements for JSA Virtual Appliances

Appliance	Threshold	Minimum number of CPU cores	Suggested number of CPU cores
JSA Flow Processor 1299	10,000 FPM or less	4	4

Table 8: CPU Requirements for JSA Virtual Appliances *(continued)*

Appliance	Threshold	Minimum number of CPU cores	Suggested number of CPU cores
JSA Event Collector Virtual 1599	2,500 EPS or less	4	16
	5,000 EPS or less	8	16
	20,000 EPS or less	16	16
JSA Event Processor Virtual 1699	2,500 EPS or less	4	24
	5,000 EPS or less	8	24
	20,000 EPS or less	16	24
	40,000 EPS or less	40	40
	80,000 EPS or less	56	56
JSA Flow Processor Virtual 1799	150,000 FPM or less	4	24
	300,000 FPM or less	8	24
	1,200,000 FPM or less	16	24
	2,400,000 FPM or less	48	48
	3,600,000 FPM or less	56	56
JSA Event and Flow Processor Combo	200,000 FPM or less 5,000 EPS or less	16	24
	300,000 FPM or less 15,000 EPS or less	48	48
	1,200,000 FPM or less 30,000 EPS or less	56	56

Table 8: CPU Requirements for JSA Virtual Appliances *(continued)*

Appliance	Threshold	Minimum number of CPU cores	Suggested number of CPU cores
JSA Threat Analytics "All-in-one" or Console 3199	25,000 Flows per minute (FPM) or less 500 EPS or less	4	24
	50,000 FPM or less 1,000 EPS or less	8	24
	100,000 FPM or less 1,000 EPS or less	12	24
	200,000 FPM or less 5,000 EPS or less	16	24
	300,000 FPM or less 15,000 EPS or less	48	48
	1,200,000 FPM or less 30,000 EPS or less	56	56
JSA Virtual Log Manager	2,500 Events per second (EPS) or less	4	16
	5,000 EPS or less	8	16
JSA Vulnerability Manager Processor		4	4
JSA Vulnerability Manager Scanner		4	4
JSA Risk Manager		8	8
JSA Flow Processor		4	16

Table 8: CPU Requirements for JSA Virtual Appliances *(continued)*

Appliance	Threshold	Minimum number of CPU cores	Suggested number of CPU cores
JSA App Host		4	12 or more for a medium sized App Host 24 or more for a large sized App Host

Storage Requirements

Your virtual appliance must have at least 256 GB of storage available. Before you install your virtual appliance, use the following formula to determine your storage needs:

(Number of Days) x (Seconds in a day) x (Events per second rate) x (Average size of a log event x 1.5 JSA normalized event overhead) x 1.05 / (1000 x 1000 x 1000) + 40 GB

```
30 x 86,400 x 1,000 EPS x 600 bytes x 1.05 / (1000 x 1000 x 1000) + 40 GB =
1673 GB
```

The following table shows the storage requirements for installing JSA by using the virtual or software only option.

Table 9: Minimum storage requirements for appliances when you use the virtual installation option.

System classification	Appliance information	IOPS	Data transfer rate (MB/s)
Minimum performance	Supports XX05 licensing	800	500
Medium performance	Supports XX29 licensing	1200	1000
High Performance	Supports XX48 licensing	10,000	2000
Small All-in-One or 1600	Event/Flow Processors	300	300
Event/Flow Processors	Event/Flow Collectors	300	300

RELATED DOCUMENTATION

Creating Your Virtual Machine | 48
Installing JSA on a Virtual Machine | 49
Adding Your Virtual Appliance to Your Deployment | 51

Creating Your Virtual Machine

To install a JSA virtual appliance, you must first create a virtual machine.

1. Create a virtual machine by using one of the following hypervisors:

   - VMWare ESXi with hardware version 13
   - KVM on CentOS or Red Hat Enterprise Linux 7.7 with QEMU KVM 1.5.3-141
   - The Hyper-V plugin on Windows Server 2016 with all Windows updates applied

   > **NOTE:** If you are installing a JSA appliance in Hyper-V, you must do a software installation, not an appliance installation. If you are using a version of Hyper-V that includes a secure boot option, secure boot must be disabled.
   >
   > If you are installing JSA on a Unified Extensible Firmware Interface (UEFI) system, secure boot must be disabled.
   >
   > The listed hypervisor versions are tested by Juniper Networks, but other untested versions might also work. If you install JSA on an unsupported version and encounter an issue that can be produced on the listed version of that hypervisor, Juniper Networks supports that issue.

2. Configure your virtual machine to meet the requirements for CPUs, RAM, and storage parameters. See "System Requirements for Virtual Appliances" on page 42.

3. Configure at least one network interface for your virtual machine.

RELATED DOCUMENTATION

Installing JSA on a Virtual Machine | 49
Adding Your Virtual Appliance to Your Deployment | 51

Overview Of Supported Virtual Appliances | 38

Installing JSA on a Virtual Machine

After you create your virtual machine, you must install the JSA software on the virtual machine.

Create a virtual machine. For more information, see “Creating Your Virtual Machine” on page 48.

Determine if you need to do an appliance installation or a software installation. For more information about appliance installations and software installations, see “Virtual Appliance Installations for JSA and Log Manager” on page 37 .

For a software installation, you must install Red Hat Enterprise Linux (RHEL) before you install JSA. For more information about installing RHEL for JSA, see "Installing RHEL on Your System".

1. Log in to the virtual machine by typing **root** for the user name.

   The user name is case-sensitive.

2. Accept the **End User License Agreement**.

3. Select the appliance type:

   - **Non-Software Appliance** for an appliance installation.
   - **Software Appliance** for a software installation.

4. Select the appliance assignment, and then select **Next**.

5. If you selected an appliance for high-availability (HA), select whether the appliance is a console.

6. For the type of setup, select **Normal Setup (default)** or **HA Recovery Setup**, and set up the time.

7. If you selected **HA Recovery Setup**, enter the cluster virtual IP address.

8. Select the Internet Protocol version:

   - Select **ipv4** or **ipv6**.

9. If you selected **ipv6**, select **manual** or **auto** for the **Configuration type**.

10. Select the bonded interface setup, if required.

11. Select the management interface.

12. In the wizard, enter a fully qualified domain name in the **Hostname** field.

13. In the **IP address** field, enter a static IP address, or use the assigned IP address.

    > **NOTE:** If you are configuring this host as a primary host for a high availability (HA) cluster, and you selected **Yes** for auto-configure, you must record the automatically-generated IP address. The generated IP address is entered during HA configuration.

    For more information, see the *Juniper Secure Analytics High Availability Guide*.

14. If you do not have an email server, enter **localhost** in the **Email server name** field.

15. Enter **root** and **admin** passwords that meet the following criteria:

    - Contains at least 5 characters
    - Contains no spaces
    - Can include the following special characters: @, #, ^, and *.

16. Click **Finish**.

17. Follow the instructions in the installation wizard to complete the installation.

    The installation process might take several minutes. When the installation is complete, if you are installing a JSA Console, proceed to step 18. If you are installing a managed host, proceed to "Adding Your Virtual Appliance to Your Deployment" on page 51.

18. Apply your license key.

    a. Log in to JSA.

       The default user name is **admin**. The password is the password of the admin user account.

    b. Click **Login To JSA**.

    c. Click the **Admin** tab.

    d. In the navigation pane, click **System Configuration**.

    e. Click the **System and License Management** icon.

    f. From the **Display** list box, select **Licenses**, and upload your license key.

    g. Select the unallocated license and click **Allocate System to License**.

    h. From the list of systems, select a system, and click **Allocate System to License**.

RELATED DOCUMENTATION

Adding Your Virtual Appliance to Your Deployment | 51

Overview Of Supported Virtual Appliances | 38

Creating Your Virtual Machine | 48

Adding Your Virtual Appliance to Your Deployment

After the JSA software is installed, add your virtual appliance to your deployment.

1. Log in to the JSA console.

2. Click **Admin** tab.

3. In the **Admin** settings, click the **System and License Management** icon.

4. On the **Deployment Actions** menu, click **Add Host**.

5. Configure the settings for the managed host by providing the fixed IP address, and the root password to access the operating system shell on the appliance.

6. Click **Add**.

7. In the **Admin** settings, click **Deploy Changes**.

8. Apply your license key.

   a. Log in to JSA.

      The default user name is **admin**. The password is the password of the root user account.

   b. Click **Login**.

   c. Click the **Admin** tab.

   d. In the navigation pane, click **System Configuration**.

   e. Click the **System and License Management** icon.

   f. From the **Display** list box, select **Licenses**, and upload your license key.

   g. Select the unallocated license and click **Allocate System to License**.

   h. From the list of systems, select a system, and click **Allocate System to License**.

RELATED DOCUMENTATION

Overview Of Supported Virtual Appliances | **38**

Creating Your Virtual Machine | **48**

Installing JSA on a Virtual Machine | **49**

5

CHAPTER

Installations from the Recovery Partition

Installations from the Recovery Partition

When you install JSA products, the installer (ISO image) is copied to the recovery partition. From this partition, you can reinstall JSA products. Your system is restored back to the default configuration. Your current configuration and data files are overwritten.

When you restart your JSA appliance, an option to reinstall the software is displayed. If you do not respond to the prompt within 5 seconds, the system continues to start as normal. Your configuration and data files are maintained. If you choose the reinstall option, a warning message is displayed and you must confirm that you want to reinstall.

> **NOTE:** The retain option is not available on High-Availability systems. See the *Juniper Secure Analytics High Availability Guide* for information on recovering High-Availability appliances.

RELATED DOCUMENTATION

Adding Your Virtual Appliance to Your Deployment | 51

Reinstalling from the Recovery Partition | 54

Installing JSA on a Virtual Machine | 49

Reinstalling from the Recovery Partition

You can reinstall JSA products from the recovery partition.

If your deployment includes offboard storage solutions, you must disconnect your offboard storage before you reinstall JSA. After you reinstall, you can remount your external storage solutions. For more information on configuring offboard storage, see the *Juniper Secure Analytics Configuring Offboard Storage Guide*.

1. Restart your JSA appliance and select **Factory re-install**.

2. Type **flatten** or **retain**.

   The installer partitions and reformats the hard disk, installs the OS, and then re-installs the JSA product. You must wait for the flatten or retain process to complete. This process can take up to several minutes. When the process is complete, a confirmation is displayed.

3. Type **SETUP**.

4. Log in as the root user.

5. Ensure that the **End User License Agreement** (EULA) is displayed.

   > **TIP:** Press the Spacebar key to advance through the document.

6. For JSA console installations, select the **Enterprise** tuning template.

7. Follow the instructions in the installation wizard to complete the installation.

8. Apply your license key.

   a. Log in to JSA:

      The default user name is **admin**. The password is the password of the root user account.

   b. Click **Login To JSA**.

   c. Click the **Admin** tab.

   d. In the navigation pane, click **System Configuration**.

   e. Click the **System and License Management** icon.

   f. From the **Display** list box, select **Licenses**, and upload your license key.

   g. Select the unallocated license and click **Allocate System to License**.

   h. From the list of systems, select a system, and click **Allocate System to License**.

RELATED DOCUMENTATION

Adding Your Virtual Appliance to Your Deployment | 51

Installations from the Recovery Partition | 54

Installing JSA on a Virtual Machine | 49

6

CHAPTER

Reinstalling JSA from Media

Reinstalling JSA from Media

You can reinstall JSA products from media such as the ISO file or a USB flash drive.

- Back up your data.
- On a Unified Extensible Firmware Interface (UEFI) system, remove the Grand Unified Bootloader (GRUB) entries for the existing JSA installation from the UEFI boot loader before you reinstall JSA.
  1. At boot time, press F1 to enter **System Configuration and Boot Management**.
  2. Select **Boot Manager**.
  3. Select **Delete Boot Option**.
  4. Check **grub**, then select **Commit Changes and Exit**.

1. At boot time, press F12 to enter **Boot Devices Manager**.

2. Select your installation media from the list.

3. At the prompt, type **flatten**.

RELATED DOCUMENTATION

Data Node Overview | 59

7

CHAPTER

Data Node Overview

Data Node Overview

Understand how to use Data Nodes in your Juniper Secure Analytics (JSA) deployment.

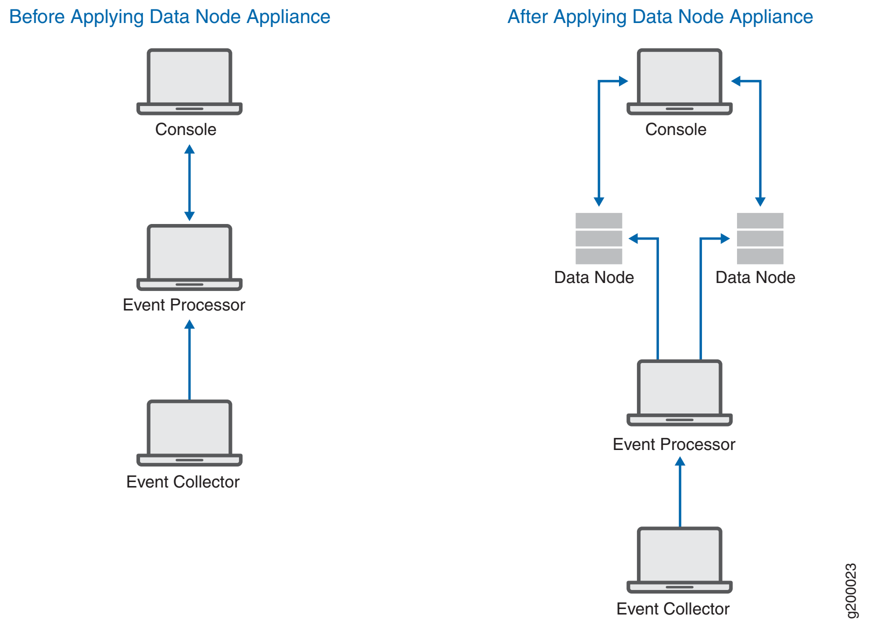
Data Nodes enable new and existing JSA deployments to add storage and processing capacity on demand as required.

Users can scale storage and processing power independently of data collection, which results in a deployment that has the appropriate storage and processing capacity. Data Nodes are plug-n-play and can be added to a deployment at any time. Data Nodes seamlessly integrate with the existing deployment.

Increasing data volumes in deployments require data compression sooner. Data compression slows down system performance as the system must decompress queried data before analysis is possible. Adding Data Node appliances to a deployment allows you to keep data uncompressed longer.

The JSA deployment distributes all new data across the Event and Flow processors and the attached Data Nodes. Figure 2 on page 59 shows the JSA deployment before and after adding Data Node appliances.

Figure 2: JSA deployment before and after adding Data Node appliances



Clustering

Data Nodes add storage capacity to a deployment, and also improve performance by distributing data collected on a processor across multiple storage volumes. When the data is searched, multiple hosts, or a cluster, do the search. The cluster can greatly improve search performance, but do not require the addition of multiple event processors. Data Nodes multiply the storage for each processor.

> **NOTE:** You can connect a Data Node to only one processor at a time, but a processor can support multiple data nodes.

Deployment Considerations

- Data Nodes are available on JSA 2014.2 and later.
- Data Nodes perform similar search and analytic functions as Event and Flow processors in a JSA deployment. Operations on a cluster are affected by the slowest member of a cluster. Data Node system performance improves if Data Nodes are sized similarly to the event and flow processors in a deployment. To facilitate similar sizing between Data Nodes and event and flow processors, Data Nodes are available on core appliances.
- Data Nodes can be installed as VM or on JSA appliances. You can mix these in a single deployment.

Bandwidth and latency

Ensure a 1 GBps link and less than 10 ms between hosts in the cluster. Searches that yield many results require more bandwidth.

Compatibility

Data Nodes are compatible with all existing JSA appliances that have an Event or Flow Processor component, including All-In-One appliances.

Data Nodes support high-availability (HA).

Installation

Data Nodes use standard TCP/IP networking, and do not require proprietary or specialized interconnect hardware. Install each Data Node that you want to add to your deployment as you would install any other JSA appliance. Associate Data Nodes with event or flow processors in the JSA Deployment Editor. See *Juniper Secure Analytics Administration Guide*.

You can attach multiple Data Nodes to a single Event or Flow Processor, in a many-to-one configuration.

When you deploy high availability pairs with Data Node appliances, install, deploy and rebalance data with the high availability appliances before synchronizing the high availability pair. The combined effect of the data rebalancing, and the replication process utilized for high availability results in significant performance degradation. If high availability is present on the existing appliances to which Data Nodes are being introduced, it is also preferable that the high availability connection be broken and reestablished once the rebalance of the cluster is completed.

Decommissioning

Remove Data Nodes from your deployment with the Deployment Editor, as with any other JSA appliance. Decommissioning does not erase balanced data on the host. You can retrieve the data for archiving and redistribution.

Data Rebalancing

Adding a Data Node to a cluster distributes data evenly to each Data Node. Each Data Node appliance maintains the same percentage of available space. New Data Nodes added to a cluster initiate additional rebalancing from cluster event and flow processors to achieve efficient disk usage on the newly added Data Node appliances.

Starting in JSA 2014.3, data rebalancing is automatic and concurrent with other cluster activity, such as queries and data collection. No downtime is experienced during data rebalancing.

Data Nodes offer no performance improvement in the cluster until data rebalancing is complete. Rebalancing can cause minor performance degradation during search operations, but data collection and processing continue unaffected.

Management and Operations

Data Nodes are self-managed and require no regular user intervention to maintain normal operation. JSA manages activities, such as data backups, high availability and retention policies, for all hosts, including Data Node appliances.

Failures

If a Data Node fails, the remaining members of the cluster continue to process data.

When the failed Data Node returns to service, data balancing resumes. During the downtime, data on the failed Data Node is unavailable.

For catastrophic failures requiring appliance replacement or the reinstallation of JSA, decommission Data Nodes from the deployment and replace them using standard installation steps. Copy any data not lost in the failure to the new Data Node before deploying. The rebalancing algorithm accounts for old data and shuffles only data collected during the failure.

For Data Nodes deployed with an high availability pair, a hardware failure causes a failover, and operations continue to function normally.

For more information about each component, see the *Juniper Secure Analytics Administration Guide*.

RELATED DOCUMENTATION

Network Settings Management | 75

Changing the Network Settings in an All-in-one System | 75

Changing the Network Settings Of a JSA Console in a Multi-system Deployment | 76

JSA Software Installations (applicable only for JSA 7.3.1 Patch 9, JSA 7.3.2 Patch 2, and JSA 7.3.2 Patch 3)

A software installation is a JSA installation on your hardware that uses an RHEL operating system that you provide. You must configure partitions and perform other RHEL preparation before a JSA software installation.

Important

- Ensure that your hardware meets the system requirements for JSA deployments. For more information about system requirements, see "Prerequisites for Installing JSA on Your Hardware" and "Appliance Storage Requirements for Virtual and Software Installations".
- Install no software other than JSA and RHEL on your hardware. Unapproved RPM installations can cause dependency errors when you upgrade JSA software and can also cause performance issues in your deployment.
- Do not update your operating system or packages before or after JSA installation.
- If you are installing JSA on a Unified Extensible Firmware Interface (UEFI) system, secure boot must be disabled.

Complete the following tasks in order:

- Installing RHEL on Your System on page 66
- Installing JSA After the RHEL Installation on page 69

Prerequisites for Installing JSA on Your Hardware

Before you install Red Hat Enterprise Linux (RHEL) operating system on your hardware, ensure that your system meets the system requirements.

JSA and RHEL version compatibility

The following table describes the version of Red Hat Enterprise Linux used with the JSA version.

Table 10: Red Hat Version

JSA Version	Red Hat Enterprise Linux Version
JSA 7.4.0	Red Hat Enterprise Linux V7.6 64-bit

Table 10: Red Hat Version *(continued)*

JSA Version	Red Hat Enterprise Linux Version
JSA 7.4.1	Red Hat Enterprise Linux V7.7 64-bit

The following table describes the system requirements:

Table 11: System Requirements for RHEL Installations on your own Appliance

Requirements	Description
Kickstart disks	Not supported
Network Time Protocol (NTP) package	Optional If you want to use NTP as your time server, ensure that you install the NTP package.
Firewall configuration	WWW (http, https) enabled SSH-enabled
Hardware	See the tables below for memory, processor, and storage requirements.

Memory and processor requirements

The following table describes the memory and processor requirements for your hardware.

Table 12: Minimum and Suggested Memory Requirements for JSA Virtual Appliances

Appliance	Minimum memory requirement	Suggested memory requirement	Minimum number of CPU cores	Suggested number of CPU cores
JSA Event Processor 1605	12 GB	48 GB	16	24
JSA Event Processor 1629	128 GB	128 GB	40	40
JSA Event Processor 1648	128 GB	128 GB	56	56
JSA Flow Processor 1705	12 GB	48 GB	16	24

Table 12: Minimum and Suggested Memory Requirements for JSA Virtual Appliances *(continued)*

Appliance	Minimum memory requirement	Suggested memory requirement	Minimum number of CPU cores	Suggested number of CPU cores
JSA Flow Processor 1729	128 GB	128 GB	48	48
JSA Flow Processor 1748	128 GB	128 GB	56	56
JSA Event and Flow Processor 1805			16	24
JSA Event and Flow Processor 1829			48	48
JSA Event and Flow Processor 1829			56	56
JSA 3105 “All-in-one” or Console	32 GB	48 GB	16	24
JSA 3129 “All-in-one” or Console				
JSA 3148 “All-in-one” or Console	64 GB	128 GB	56	56
JSA Flow Processor 1202/1301	64 GB		14	
JSA Flow Processor 1310	64 GB		14	
JSA Flow Processor 1501	64 GB		8	

Storage requirements

Your appliance must have at least 256 GB of storage available.

The following table shows the storage requirements for installing JSA on your hardware.

Table 13: Minimum Storage Requirements for Appliances when you use the Virtual or Software Installation Option

System classification	Appliance Information	IOPS	Data transfer rate (MB/s)
Minimum performance	Supports XX05 licensing	800	500
Medium performance	Supports XX29 licensing	1200	1000
High Performance	Supports XX48 licensing	10,000	2000
Small All-in-One or 1600	Less than 500 EPS	300	300
Event/Flow Processors	Events and flows	300	300

Appliance Storage Requirements for Virtual and Software Installations

To install JSA using virtual or software options, the device must meet minimum storage requirements.

The following table shows the recommended minimum storage requirements for installing JSA by using the virtual or software only option.

NOTE: The minimum required storage size will vary, based in factors such as event size, event per second (EPS), and retention requirements.

Table 14: Minimum Storage Requirements for Appliances When You Use the Virtual or Software Installation Option

System classification	Appliance Information	IOPS	Data transfer rate (MB/s)
Minimum performance	Supports XX05 licensing	800	500
Medium performance	Supports XX29 licensing	1200	1000
High Performance	Supports XX48 licensing	10,000	2000
Small All-in-One or 1600	Less than 500 EPS	300	300

Table 14: Minimum Storage Requirements for Appliances When You Use the Virtual or Software Installation Option *(continued)*

System classification	Appliance Information	IOPS	Data transfer rate (MB/s)
Event/Flow Processors	Events and flows	300	300

Installing RHEL on Your System

You can install the Red Hat Enterprise Linux (RHEL) operating system on your own system to use with JSA.

Download the Red Hat Enterprise Linux Server ISO x86_64 Boot ISO from https://access.redhat.com.

Refer to the Red Hat version table to choose the correct version.

Table 15: Red Hat Version

JSA Version	Red Hat Enterprise Linux version
7.4.0	Red Hat Enterprise Linux Server V7.6 x86_64 Boot ISO
7.4.1	Red Hat Enterprise Linux Server V7.7 x86_64 Boot ISO

You can provide your own RHEL, or acquire entitlement to a JSA Software Node. To acquire entitlement to a JSA Software Node, contact your JSA Sales Representative.

If there are circumstances where you need install to RHEL separately, proceed with the following instructions.

1. Map the ISO to a device for your appliance by using the bootable USB flash drive with the ISO.

   For information about creating a bootable USB flash drive, see "USB Flash Drive Installations" on page 18.

2. Insert the portable storage device into your appliance and restart your appliance.

3. From the starting menu, do one of the following options:

   - Select the device that you mapped the ISO to, or the USB drive, as the boot option.
   - To install on a system that supports Extensible Firmware Interface (EFI), you must start the system in **legacy** mode.

4. When prompted, log in to the system as the root user.

5. Follow the instructions in the installation wizard to complete the installation:
    a. Set the language to English (US).
    b. Click **Date & Time** and set the time for your deployment.
    c. Click **Software selection** and select **Minimal Install**.
    d. Click **Installation Destination** and select the **I will configure partitioning** option.
    e. Select **LVM** from the list.
    f. Click the **Add** button to add the mount points and capacities for your partitions, and then click **Done**. For more information about RHEL7 partitions, see "Linux Operating System Partition Properties for JSA Installations on Your Own Hardware".
    g. Click **Network & Host Name**.
    h. Enter a fully qualified domain name for your appliance host name.
    i. Select the interface in the list, move the switch to the **ON** position, and click **Configure**.
    j. On the **General** tab, select **Automatically connect to this network when it is available** option.
    k. On the **IPv4 Settings** tab, select **Manual** in the **Method** list.
    l. Click **Add** to enter the IP address, Netmask, and Gateway for the appliance in the **Addresses** field.
    m. Add two DNS servers.
    n. Click **Save > Done > Begin Installation**.
6. Set the root password, and then click **Finish configuration**.
7. After the installation finishes, disable SELinux by modifying the **/etc/selinux/config** file, and restart the appliance.

Linux Operating System Partition Properties for JSA Installations on Your Own System

If you use your own appliance hardware, you can delete and re-create partitions on your Red Hat Enterprise Linux operating system rather than modify the default partitions.

Use the values in the following table as a guide when you re-create the partitioning on your Red hat Enterprise Linux Operating system.

The file system for each partition is XFS.

Table 16: Partitioning Guide for RHEL

Mount Path	LVM Supported?	Exists on Software Installation	Size
/boot	No	Yes	1 GB

Table 16: Partitioning Guide for RHEL *(continued)*

Mount Path	LVM Supported?	Exists on Software Installation	Size
/boot/efi	No	Yes	200 MB
/recovery	No	No	8 GB
/var	Yes	Yes	5 GB
/var/log	Yes	Yes	15 GB
/var/log/audit	Yes	Yes	3 GB
/opt	Yes	Yes	13 GB
/home	Yes	Yes	1 GB
/storetmp	Yes	Yes	15 GB
/tmp	Yes	Yes	3 GB
swap	N/A	Yes	swap formula: Configure the swap partition size to be 75 percent of RAM, with a minimum value of 12 GB and a maximum value of 24 GB
/	Yes	Yes	Upto 15 GB
/store	Yes	Yes	80% of remaining space
/transient	Yes	Yes	20 % of remaining space

Console Partition Configurations for Multiple Disk Deployments

For systems with multiple disks, configure the following partitions for JSA.

Disk 1

boot, swap, OS, JSA temporary files, and log files

Remaining Disks

- Use the default storage configurations for JSA appliances as a guideline to determine what RAID type to use.
- Mounted as **/store**
- Store JSA data

The following table shows the default storage configuration for JSA appliances.

Table 17: Default Storage Configurations for JSA Appliances

JSA host role	Storage Configuration
Flow processor QRadar Network Insights (QNI)	RAID1
Data Node Event processor Flow processor Event and flow processor All-in-one console	RAID6
Event collector	RAID10

Installing JSA After the RHEL Installation

Install Security JSA on your own device after you install RHEL.

A fresh software install erases all data in **/store** as part of the installation process. If you want to preserve the contents of **/store** when performing a software install (such as when performing a manual retain), back up the data you want to preserve apart from the host where the software is to be installed.

1. Copy the JSA ISO to **/root** or **/storetmp** directory of the device.

2. Create the **media/cdrom** directory by typing the following command:

   ```
   mkdir/media/cdrom
   ```

3. Mount the JSA ISO by using the following command:

mount - o loop <path_to_iso>/<qradar.iso> / media/cdrom

4. Run the JSA setup by using the following command:

   /media/cdrom/setup

   > **NOTE:** A new kernel might be installed as part of the installation, which requires a system restart. Repeat the commands in steps 3 and 4 after the system restart to continue the installation.

5. Select the appliance type:
   - **Software Install**
   - **High Availability Appliance**
6. Select the appliance assignment, and then select **Next**.
7. If you selected an appliance for high-availability (HA), select whether the appliance is a console.
8. For the type of setup, select **Normal Setup (default)** or **HA Recovery Setup**, and set up the time.
9. If you selected **HA Recovery Setup**, enter the cluster virtual IP address.
10. Select the Internet Protocol version.
11. If you selected **ipv6**, select **manual** or auto for the **Configuration type**.
12. Select the bonded interface setup, if required.
13. Select the management interface.
14. In the wizard, enter a fully qualified domain name in the **Hostname** field.
15. In the IP address field, enter a static IP address, or use the assigned IP address.

NOTE: If you are configuring this host as primary host for a high availability (HA) cluster, and you selected **Yes** for auto-configure, you must record the automatically-generated IP address. The generated IP address is entered during HA configuration.

For more information, see *Juniper Security Analytics High Availability Guide*.

16. If you do not have a email server, enter **localhost** in the **Email server name** field.

17. Leave the **root** password as it is.

18. If you are installing a Console, enter an **admin** password that meets the following criteria:
    - Contains at least 5 characters
    - Contains no spaces
    - Can include the following special characters: @, #, ^, and *.
19. Click **Finish**.

20. Follow the instructions in the installation wizard to complete the installation.

    The installation process might take several minutes.

21. If you are installing a Console, apply your license key.
    a. Log in to JSA as the **admin** user:
    b. Click **Login**.
    c. In the navigation menu, click **Admin**.
    d. In the navigation pane, click **System configuration**.
    e. Click the **System and License Management** icon.
    f. From the **Display** list box, select **Licenses**, and upload your license key.
    g. Select the unallocated license and click **Allocate System to License**.
    h. From the list of systems, select a system, and click **Allocate System to License**.
22. If you want to add managed hosts, see *Juniper Security Analytics Administration Guide*.

8

CHAPTER

Configuring Bonded Management Interfaces

Configuring Bonded Management Interfaces

You can bond the management interface on JSA hardware.

You can bond the management interfaces during the JSA installation process, or after installation by following these steps.

You can bond non-management interfaces in the JSA user interface after installation. See “Configuring network interfaces” in *Juniper Secure Analytics Administration Guide* for more information about configuring non-management interfaces.

Bonding modes 1 and 4 are supported. Mode 4 is the default.

> **NOTE:** You must be physically logged in to your appliance, for example through IMM or iDRAC, for these steps. Do not use **ssh** for these steps.

1. Change your network setup by typing the command **qchange_netsetup**:

   > **NOTE:** If you attempt to run **qchange_netsetup** over a serial connection, the connection can be misidentified as a network connection. To run over a serial connection use **qchange_netsetup -y** . This command allows you to bypass the validation check that detects a network connection.

2. Select the protocol version that is used for the appliance.

3. Select **Yes** to continue with bonded network interface configuration.

4. Select interfaces to configure as bonded interfaces. The interfaces that you select must not already be configured.

5. Enter the bonding options. For more information about configuring specific bonding options, see your vendor-specific operating system documentation.

6. Update any network information settings as needed. Your appliance restarts automatically.

7. Log in to the appliance and verify the configuration.

9

CHAPTER

Network Settings Management

Network Settings Management

Use the **qchange_netsetup script** to change the network settings of your JSA system. Configurable network settings include host name, IP address, network mask, gateway, DNS addresses, public IP address, and email server.

RELATED DOCUMENTATION

Changing the Network Settings in an All-in-one System

You can change the network settings in your All-in-one system. An All-in-one system has all JSA components that are installed on one system.

- You must have a local connection to your JSA console
- Confirm that there are no undeployed changes.
- If you are changing the IP address host name of a box in the deployment you must remove it from the deployment.
- If this system is part of an HA pair you must disable HA first before you change any network settings.
- If the system that you want to change is the console, you must remove all hosts in the deployment before proceeding.

1. Log in to as the root user.

2. Type the following command:

   qchange_netsetup

   > NOTE: If you attempt to run **qchange_netsetup** over a serial connection, the connection can be misidentified as a network connection. To run over a serial connection use **qchange_netsetup -y**. This command allows you to bypass the validation check that detects a network connection.

3. Follow the instructions in the wizard to complete the configuration.

   The following table contains descriptions and notes to help you configure the network settings.

   Table 18: Description Of Network Settings for an All-in-one JSA Console

Network Setting	Description
Internet Protocol	**IPv4** or **IPv6**
Host name	Fully qualified domain name
Secondary DNS server address	Optional
Public IP address for networks that use Network Address Translation (NAT)	Optional Used to access the server, usually from a different network or the Internet. Configured by using Network Address Translation (NAT) services on your network or firewall settings on your network. (NAT translates an IP address in one network to a different IP address in another network).
Email server name	If you do not have an email server, use **localhost**.

   A series of messages are displayed as JSA processes the requested changes. After the requested changes are processed, the JSA system is automatically shutdown and restarted.

RELATED DOCUMENTATION

Network Settings Management | 75

Changing the Network Settings Of a JSA Console in a Multi-system Deployment | 76

Changing the Network Settings Of a JSA Console in a Multi-system Deployment

To change the network settings in a multi-system JSA deployment, remove all managed hosts, change the network settings, add the managed hosts again, and then reassign the component.

- You must have a local connection to your JSA console

1. To remove managed hosts, log in to JSA.

   The **Username** is **admin**.

   a. Click the **Admin** tab.

   b. Click the **System and License Management** icon.

   c. Select the managed host that you want to remove.

   d. Select **Deployment Actions >Remove Host**.

   e. In the **Admin** tab, click **Deploy Changes**.

2. Type the following command: **qchange_netsetup**.

   > NOTE: If you attempt to run **qchange_netsetup** over a serial connection, the connection can be misidentified as a network connection. To run over a serial connection use **qchange_netsetup -y**. This command allows you to bypass the validation check that detects a network connection.

3. Follow the instructions in the wizard to complete the configuration.

   The following table contains descriptions and notes to help you configure the network settings.

Table 19: Description Of Network Settings for a Multi-system JSA Console Deployment

Network Setting	Description
Internet Protocol	**IPv4** or **IPv6**
Host name	Fully qualified domain name
Secondary DNS server address	Optional
Public IP address for networks that use Network Address Translation (NAT)	Optional Used to access the server, usually from a different network or the Internet. Configured by using Network Address Translation (NAT) services on your network or firewall settings on your network. (NAT translates an IP address in one network to a different IP address in another network).
Email server name	If you do not have an email server, use **localhost**.

After you configure the installation parameters, a series of messages are displayed. The installation process might take several minutes.

4. To re-add and reassign the managed hosts, log in to JSA.

   The **Username** is **admin**.

   a. Click the **Admin** tab.

   b. Click the **System and License Management** icon.

   c. Click **Deployment Actions >Add Host**.

   d. Follow the instructions in the wizard to add a host.

      Select the **Network Address Translation** option to configure a public IP address for the server. This IP address is a secondary IP address that is used to access the server, usually from a different network or the Internet. The Public IP address is often configured by using Network Address Translation (NAT) services on your network or firewall settings on your network. NAT translates an IP address in one network to a different IP address in another network.

5. Reassign all components that are not your JSA console to your managed hosts.

   a. Click the **Admin** tab.

   b. Click the **System and License Management** icon.

   c. Select the host that you want to reassign.

   d. Click **Deployment Actions >Edit Host Connection**.

   e. Enter the IP address of the source host in the **Modify Connection** window.

RELATED DOCUMENTATION

Network Settings Management | 75

Changing the Network Settings in an All-in-one System | 75

Updating Network Settings After a NIC Replacement

If you replace your integrated system board or stand-alone (Network Interface Cards) NICs, you must update your JSA network settings to ensure that your hardware remains operational.

The network settings file contains one pair of lines for each NIC that is installed and one pair of lines for each NIC that was removed. You must remove the lines for the NIC that you removed and then rename the NIC that you installed.

NOTE: In previous releases of JSA, interfaces were named in the following format: **eth0**, **eth1**, **eth4**, and so on. JSA 7.3.0 interface naming includes a greater range of possible interface names. For example, **ens192**, **enp2s0**, and so on.

Your network settings file might resemble the following example, where ***NAME="<old_name>"*** is the NIC that was replaced and ***NAME="<new_name>"*** is the NIC that was installed.

```
# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"
```

```
# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0
```

```
# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth4
```

```
# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth4
```

1. Use SSH to log in to the JSA product as the root user.

   The user name is **root**.

2. Type the following command:

```
cd /etc/udev/rules.d/
```

3. To edit the network settings file, type the following command:

```
vi 70-persistent-net.rules
```

4. Remove the pair of lines for the NIC that was replaced: **NAME=”<*old_name*>”**.

5. Rename the **Name=<*name*>** values for the newly installed NIC.

6. Save and close the file.

7. Type the following command: **reboot**.

RELATED DOCUMENTATION

Changing the Network Settings in an All-in-one System | 75

Changing the Network Settings Of a JSA Console in a Multi-system Deployment | 76

10

CHAPTER

Troubleshooting Problems

Troubleshooting Problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem.

Review the following table to help you or customer support resolve a problem.

Table 20: Troubleshooting Actions to Prevent Problems

Action	Description
Apply all known patches, service levels, or program temporary fixes (PTF).	A product fix might be available to fix the problem.
Ensure that the configuration is supported.	Review the software and hardware requirements.
Check kb.juniper.net for known issues/fixes.	Error messages give important information to help you identify the component that is causing the problem.
Reproduce the problem to ensure that it is not just a simple error.	If samples are available with the product, you might try to reproduce the problem by using the sample data.
Check the installation directory structure and file permissions.	The installation location must contain the appropriate file structure and the file permissions. For example, if the product requires write access to log files, ensure that the directory has the correct permission.
Review relevant documentation, such as release notes, tech notes, and proven practices documentation.	Search the Juniper Networks knowledge bases to determine whether your problem is known, has a workaround, or if it is already resolved and documented.
Review recent changes in your computing environment.	Sometimes installing new software might cause compatibility issues.

If you still need to resolve problems, you must collect diagnostic data. This data is necessary for an Juniper Networks technical-support representative to effectively troubleshoot and assist you in resolving the problem. You can also collect diagnostic data and analyze it yourself.

RELATED DOCUMENTATION

Troubleshooting Resources | 83

Troubleshooting Resources

Troubleshooting resources are sources of information that can help you resolve a problem that you have with a product.

Find the Juniper Secure Analytics (JSA) content that you need by selecting your products from the https://support.juniper.net/support/downloads/.

RELATED DOCUMENTATION

JSA Log Files | 83

Common Ports and Servers Used by JSA | 84

JSA Log Files

Use the JSA log files to help you troubleshoot problems.

You can review the log files for the current session individually or you can collect them to review later.

Follow these steps to review the JSA log files.

1. To help you troubleshoot errors or exceptions, review the following log files.
   - **/var/log/qradar.log**
   - **/var/log/qradar.error**
2. If you require more information, review the following log files:
   - /var/log/qradar-sql.log
   - /opt/tomcat6/logs/catalina.out
   - /var/log/qflow.debug
3. Review all logs by selecting **Admin >System & License Mgmt >Actions >Collect Log Files**.

RELATED DOCUMENTATION

Common Ports and Servers Used by JSA | 84
Troubleshooting Resources | 83

Common Ports and Servers Used by JSA

JSA requires that certain ports are ready to receive information from JSA components and external infrastructure. To ensure that JSA is using the most recent security information, it also requires access to public servers and RSS feeds.

SSH Communication on Port 22

All the ports that are used by the JSA console to communicate with managed hosts can be tunneled, by encryption, through port 22 over SSH.

The console connects to the managed hosts using an encrypted SSH session to communicate securely. These SSH sessions are initiated from the console to provide data to the managed host. For example, the JSA console can initiate multiple SSH sessions to the Event Processor appliances for secure communication. This communication can include tunneled ports over SSH, such as HTTPS data for port 443 and Ariel query data for port 32006. Flow Processors that use encryption can initiate SSH sessions to Flow Processor appliances that require data.

Open Ports That Are Not Required by JSA

You might find additional open ports in the following situations:

- When you mount or export a network file share, you might see dynamically assigned ports that are required for RPC services, such as **rpc.mountd** and **rpc.rquotad**.

JSA Port Usage

Review the list of common ports that JSA services and components use to communicate across the network. You can use the port list to determine which ports must be open in your network. For example, you can determine which ports must be open for the JSA console to communicate with remote event processors.

WinCollect Remote Polling

WinCollect agents that remotely poll other Microsoft Windows operating systems might require additional port assignments.

For more information, see the *Juniper Secure Analytics WinCollect User Guide*.

JSA Listening Ports

The following table shows the JSA ports that are open in a **LISTEN** state. The **LISTEN** ports are valid only when iptables is enabled on your system. Unless otherwise noted, information about the assigned port number applies to all JSA products.

Table 21: Listening Ports That Are Used by JSA Services and Components

Port	Description	Protocol	Direction	Requirement
22	SSH	TCP	Bidirectional from the JSA console to all other components.	Remote management access. Adding a remote system as a managed host. Log source protocols to retrieve files from external devices, for example the log file protocol. Users who use the command-line interface to communicate from desktops to the Console. High-availability (HA).

Table 21: Listening Ports That Are Used by JSA Services and Components *(continued)*

Port	Description	Protocol	Direction	Requirement
25	SMTP	TCP	From all managed hosts to the SMTP gateway.	Emails from JSA to an SMTP gateway. Delivery of error and warning email messages to an administrative email contact.
111	Port mapper	TCP/UDP	Managed hosts (MH) that communicate with the JSA console. Users that connect to the JSA console.	Remote Procedure Calls (RPC) for required services, such as Network File System (NFS).
123	Network Time Protocol (NTP)	UDP	Outbound from the JSA Console to the NTP Server Outbound from the MH to the JSA Console	Time synchronization via Chrony between: • JSA Console and NTP server • Managed Hosts and JSA Console
135 and dynamically allocated ports above 1024 for RPC calls.	DCOM	TCP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events. Bidirectional traffic between JSA console components or JSA event collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter. **NOTE:** DCOM typically allocates a random port range for communication. You can configure Microsoft Windows products to use a specific port. For more information, see your Microsoft Windows documentation.

Table 21: Listening Ports That Are Used by JSA Services and Components *(continued)*

Port	Description	Protocol	Direction	Requirement
137	Windows NetBIOS name service	UDP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events. Bidirectional traffic between JSA console components or JSA Event Collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
138	Windows NetBIOS datagram service	UDP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events. Bidirectional traffic between JSA console components or JSA Event Collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
139	Windows NetBIOS session service	TCP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events. Bidirectional traffic between JSA console components or JSA Event Collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.

Table 21: Listening Ports That Are Used by JSA Services and Components *(continued)*

Port	Description	Protocol	Direction	Requirement
162	NetSNMP	UDP	JSA managed hosts that connect to the JSA console. External log sources to JSA Event Collectors.	UDP port for the NetSNMP daemon that listens for communications (v1, v2c, and v3) from external log sources. The port is open only when the SNMP agent is enabled.
199	NetSNMP	TCP	JSA managed hosts that connect to the JSA console. External log sources to JSA Event Collectors.	TCP port for the NetSNMP daemon that listens for communications (v1, v2c, and v3) from external log sources. The port is open only when the SNMP agent is enabled.
443	Apache/HTTPS	TCP	Bidirectional traffic for secure communications from all products to the JSA console. Unidirectional traffic from the App Host to th JSA Console.	Configuration downloads to managed hosts from the JSA console. JSA managed hosts that connect to the JSA console. Users to have log in access to JSA. JSA console that manage and provide configuration updates for WinCollect agents. Apps that require access to the JSA API.

Table 21: Listening Ports That Are Used by JSA Services and Components *(continued)*

Port	Description	Protocol	Direction	Requirement
445	Microsoft Directory Service	TCP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events. Bidirectional traffic between JSA console components or JSA Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events. Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
514	Syslog	UDP/TCP	External network appliances that provide TCP syslog events use bidirectional traffic. External network appliances that provide UDP syslog events use uni-directional traffic. Internal syslog traffic from JSA hosts to the JSA console.	External log sources to send event data to JSA components. Syslog traffic includes WinCollect agents, event collectors, and Adaptive Log Exporter agents capable of sending either UDP or TCP events to JSA.
762	Network File System (NFS) mount daemon (mountd)	TCP/UDP	Connections between the JSA console and NFS server.	The Network File System (NFS) mount daemon, which processes requests to mount a file system at a specified location.
1514	Syslog-ng	TCP/UDP	Connection between the local Event Collector component and local Event Processor component to the syslog-ng daemon for logging.	Internal logging port for syslog-ng.

Table 21: Listening Ports That Are Used by JSA Services and Components *(continued)*

Port	Description	Protocol	Direction	Requirement
2049	NFS	TCP	Connections between the JSA console and NFS server.	The Network File System (NFS) protocol to share files or data between components.
2055	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the JSA Flow Processor.	NetFlow datagram from components, such as routers.
2375	Docker command port	TCP	Internal communications. This port is not available externally.	Used to manage JSA application framework resources.
3389	Remote Desktop Protocol (RDP) and Ethernet over USB is enabled	TCP/UDP		If the Microsoft Windows operating system is configured to support RDP and Ethernet over USB, a user can initiate a session to the server over the management network. This means the default port for RDP, 3389 must be open.
4333	Redirect port	TCP		This port is assigned as a redirect port for Address Resolution Protocol (ARP) requests in JSA offense resolution.
5000	Used to allow communication to the docker si-registry running on the Console. This allows all managed hosts to pull images from the Console that will be used to create local containers.	TCP	Unidirectional from the JSA managed host to the JSA Console. The port is only opened on the Console. Managed hosts must pull from the Console.	Required for apps running on an App Host.

Table 21: Listening Ports That Are Used by JSA Services and Components *(continued)*

Port	Description	Protocol	Direction	Requirement
5432	Postgres	TCP	Communication for the managed host that is used to access the local database instance.	Required for provisioning managed hosts from the **Admin** tab.
6514	Syslog	TCP	External network appliances that provide encrypted TCP syslog events use bidirectional traffic.	External log sources to send encrypted event data to JSA components.
7676, 7677, and four randomly bound ports above 32000.	Messaging connections (IMQ)	TCP	Message queue communications between components on a managed host.	Message queue broker for communications between components on a managed host. **NOTE:** You must permit access to these ports from the JSA console to unencrypted hosts. Ports 7676 and 7677 are static TCP ports, and four extra connections are created on random ports. For more information about finding randomly bound ports, see "Viewing IMQ Port Associations".
7777, 7778, 7779, 7780, 7781, 7782, 7783, 7788, 7790, 7791, 7792, 7793, 7795, 7799, and 8989.	JMX server ports	TCP	Internal communications. These ports are not available externally.	JMX server (Java Management Beans) monitoring for all internal JSA processes to expose supportability metrics. These ports are used by JSA support.

Table 21: Listening Ports That Are Used by JSA Services and Components *(continued)*

Port	Description	Protocol	Direction	Requirement
7789	HA Distributed Replicated Block Device (DRBD)	TCP/UDP	Bidirectional between the secondary host and primary host in an HA cluster.	Distributed Replicated Block Device (DRBD) used to keep drives synchronized between the primary and secondary hosts in HA configurations.
7800	Apache Tomcat	TCP	From the Event Collector to the JSA console.	Real-time (streaming) for events.
7801	Apache Tomcat	TCP	From the Event Collector to the JSA console.	Real-time (streaming) for flows.
7803	Anomaly Detection Engine	TCP	From the Event Collector to the JSA console.	Anomaly detection engine port.
7804	JSA Risk Manager Arc builder	TCP	Internal control communications between JSA processes and ARC builder.	This port is used for JSA Risk Manager only. It is not available externally.
7805	Syslog tunnel communication	TCP	Bidirectional between the JSA Console and managed hosts	Used for encrypted communication between the console and managed hosts.
8000	Event Collection service (ECS)	TCP	From the Event Collector to the JSA console.	Listening port for specific Event Collection Service (ECS).
8001	SNMP daemon port	TCP	External SNMP systems that request SNMP trap information from the JSA console.	Listening port for external SNMP data requests.
8005	Apache Tomcat	TCP	Internal communications. Not available externally.	Open to control tomcat. This port is bound and only accepts connections from the local host.

Table 21: Listening Ports That Are Used by JSA Services and Components *(continued)*

Port	Description	Protocol	Direction	Requirement
8009	Apache Tomcat	TCP	From the HTTP daemon (HTTPd) process to Tomcat.	Tomcat connector, where the request is used and proxied for the web service.
8080	Apache Tomcat	TCP	From the HTTP daemon (HTTPd) process to Tomcat.	Tomcat connector, where the request is used and proxied for the web service.
8082	Secure tunnel for JSA Risk Manager	TCP	Bidirectional traffic between the JSA Console and JSA Risk Manager	Required when encryption is used between JSA Risk Manager and the JSA Console.
8413	WinCollect agents	TCP	Bidirectional traffic between WinCollect agent and JSA console.	This traffic is generated by the WinCollect agent and communication is encrypted. It is required to provide configuration updates to the WinCollect agent and to use WinCollect in connected mode.
8844	Apache Tomcat	TCP	Unidirectional from the JSA console to the appliance that is running the JSA Vulnerability Manager processor.	Used by Apache Tomcat to read RSS feeds from the host that is running the JSA Vulnerability Manager processor.
9000	Conman		Unidirectional from the JSA Console to a JSA App Host.	Used with an App Host. It allows the Console to deploy apps to an App Host and to manage those apps.
9090	XForce IP Reputation database and server	TCP	Internal communications. Not available externally.	Communications between JSA processes and the XForce Reputation IP database.

Table 21: Listening Ports That Are Used by JSA Services and Components *(continued)*

Port	Description	Protocol	Direction	Requirement
9381	Certificate files download	TCP	Unidirectional from JSA managed host or external network to JSA Console.	Downloading JSA CA certificate and CRL files, which can be used to validate JSA generated certificates.
9913 plus one dynamically assigned port	Web application container	TCP	Bidirectional Java Remote Method Invocation (RMI) communication between Java Virtual Machines	When the web application is registered, one additional port is dynamically assigned.
9995	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the JSA flow processor.	NetFlow datagram from components, such as routers.
9999	JSA Vulnerability Manager processor	TCP	Unidirectional from the scanner to the appliance running the JSA Vulnerability Manager processor	Used for JSA Vulnerability Manager command information. The JSA console connects to this port on the host that is running the JSA Vulnerability Manager processor. This port is only used when JSA Vulnerability Manager is enabled.
10000	JSA web-based, system administration interface	TCP/UDP	User desktop systems to all JSA hosts.	In JSA 2014.5 and earlier, this port is used for server changes, such as the hosts root password and firewall access. Port 10000 is disabled in 2014.6.
10101, 10102	Heartbeat command	TCP	Bidirectional traffic between the primary and secondary HA nodes.	Required to ensure that the HA nodes are still active.

Table 21: Listening Ports That Are Used by JSA Services and Components *(continued)*

Port	Description	Protocol	Direction	Requirement
12500	Socat binary	TCP	Outbound from MH to the JSA Console	Port used for tunneling chrony udp requests over tcp when JSA Console or MH is encrypted
15432				Required to be open for internal communication between JSA Risk Manager and JSA.
15433	Postgres	TCP	Communication for the managed host that is used to access the local database instance.	Used for JSA Vulnerability Manager configuration and storage. This port is only used when JSA Vulnerability Manager is enabled.
20000-23000	SSH Tunnel	TCP	Bidirectional from the JSA Console to all other encrypted managed hosts.	Local listening point for SSH tunnels used for Java Message Service (JMS) communication with encrypted managed hosts. Used to perform long-running asynchronous tasks, such as updating networking configuration via System and License Management.
23111	SOAP web server	TCP		SOAP web server port for the Event Collection Service (ECS).
32000	Normalized flow forwarding	TCP	Bidirectional between JSA components.	Normalized flow data that is communicated from an off-site source or between JSA Flow Processors.

Table 21: Listing Ports That Are Used by JSA Services and Components *(continued)*

Port	Description	Protocol	Direction	Requirement
32004	Normalized event forwarding	TCP	Bidirectional between JSA components.	Normalized event data that is communicated from an off-site source or between JSA Event Collectors.
32005	Data flow	TCP	Bidirectional between JSA components.	Data flow communication port between JSA Event Collectors when on separate managed hosts.
32006	Ariel queries	TCP	Bidirectional between JSA components.	Communication port between the Ariel proxy server and the Ariel query server.
32007	Offense data	TCP	Bidirectional between JSA components.	Events and flows contributing to an offense or involved in global correlation.
32009	Identity data	TCP	Bidirectional between JSA components.	Identity data that is communicated between the passive Vulnerability Information Service (VIS) and the Event Collection Service (ECS).
32010	Flow listening source port	TCP	Bidirectional between JSA components.	Flow listening port to collect data from JSA Flow Processor.
32011	Ariel listening port	TCP	Bidirectional between JSA components.	Ariel listening port for database searches, progress information, and other associated commands.
32000-33999	Data flow (flows, events, flow context)	TCP	Bidirectional between JSA components.	Data flows, such as events, flows, flow context, and event search queries.

Table 21: Listening Ports That Are Used by JSA Services and Components *(continued)*

Port	Description	Protocol	Direction	Requirement
ICMP	ICMP		Bidirectional traffic between the secondary host and primary host in an HA cluster.	Testing the network connection between the secondary host and primary host in an HA cluster by using Internet Control Message Protocol (ICMP).

Viewing IMQ Port Associations

Several ports that are used by JSA allocate extra random port numbers. For example, Message Queues (IMQ) open random ports for communication between components on a managed host. You can view the random port assignments for IMQ by using telnet to connect to the local host and doing a lookup on the port number.

Random port associations are not static port numbers. If a service is restarted, the ports that are generated for the service are reallocated and the service is provided with a new set of port numbers.

1. Using SSH, log in to the JSA console as the root user.

2. To display a list of associated ports for the IMQ messaging connection, type the following command:

   telnet localhost 7676

   The results from the telnet command might look similar to this output:

   ```
   [root@domain ~]# telnet localhost 7676 Trying 127.0.0.1... Connected to
   localhost. Escape character is '^]'. 101 imqbroker 4.4 Update 1 portmapper
   tcp PORTMAPPER 7676
   [imqvarhome=/opt/openmq/mq/var,imqhome=/opt/openmq/mq,sessionid=<session_id>]
   cluster_discovery tcp CLUSTER_DISCOVERY 44913 jmxrmi rmi JMX 0
   [url=service:jmx:rmi://domain.ibm.com/stub/<urlpath>] admin tcp ADMIN 43691
   jms tcp NORMAL 7677 cluster tcp CLUSTER 36615
   ```

   The telnet output shows 3 of the 4 random high-numbered TCP ports for IMQ. The fourth port, which is not shown, is a JMX Remote Method Invocation (RMI) port that is available over the JMX URL that is shown in the output.

   If the telnet connection is refused, it means that IMQ is not currently running. It is probable that the system is either starting up or shutting down, or that services were shut down manually.

Searching for Ports in Use by JSA

Use the **netstat** command to determine which ports are in use on the JSA Console or managed host. Use the **netstat** command to view all listening and established ports on the system.

1. Using SSH, log in to your JSA console, as the root user.

2. To display all active connections and the TCP and UDP ports on which the computer is listening, type the following command:

   ```
   netstat -nap
   ```

3. To search for specific information from the netstat port list, type the following command:

   ```
   netstat -nap | grep port
   ```

   - To display all ports that match 199, type the following command:

     ```
     netstat -nap | grep 199
     ```

   - To display information on all listening ports, type the following command:

     ```
     netstat -nap | grep LISTEN
     ```

JSA Public Servers

To provide you with the most current security information, JSA requires access to a number of public servers and RSS feeds.

Public Servers

Table 22: Public Servers That JSA Must Access

IP address or hostname	Description
194.153.113.31	JSA Vulnerability Manager DMZ scanner
194.153.113.32	JSA Vulnerability Manager DMZ scanner
download.juniper.net	JSA auto-update servers.

Table 22: Public Servers That JSA Must Access *(continued)*

IP address or hostname	Description
www.iss.net	Juniper X-Force Threat Intelligence Threat Information Center dashboard item
update.xforce-security.com	X-Force Threat Feed update server
license.xforce-security.com	X-Force Threat Feed licensing server

RSS Feeds for JSA Products

Table 23: RSS feeds

Title	URL	Requirements
Security Intelligence	http://feeds.feedburner.com/SecurityIntelligence	JSA and an Internet connection
Security Intelligence Vulns / Threats	http://securityintelligence.com/topics/vulnerabilities-threats/feed	JSA and an Internet connection
Juniper My Notifications		JSA and an Internet connection
Security News	*http://IP_address_of_QVM_processor* :8844/rss/research/news.rss	JSA Vulnerability Manager processor is deployed
Security Advisories	*http://IP_address_of_QVM_processor* :8844/rss/research/news.rss	JSA Vulnerability Manager processor is deployed
Latest Published Vulnerabilities	*http://IP_address_of_QVM_processor* :8844/rss/research/vulnerabilities.rss	JSA Vulnerability Manager processor deployed
Scans Completed	*http://IP_address_of_QVM_processor* :8844/rss/scanresults/completedScans.rss	JSA Vulnerability Manager processor is deployed
Scans In Progress	*http://IP_address_of_QVM_processor* :8844/rss/scanresults/runningScans.rss	JSA Vulnerability Manager processor is deployed

RELATED DOCUMENTATION

Troubleshooting Resources | 83

JSA Log Files | 83