JUNIPER NETWORKS | Engineering Simplicity

Juniper Secure Analytics Installation Guide

Published
2025-07-01

RELEASE
7.5.0

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

Juniper Secure Analytics Installation Guide
7.5.0

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at 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 This Guide

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

1
CHAPTER

JSA Deployment Overview

IN THIS CHAPTER

JSA Deployment Overview

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

FIPS mode only: (For JSA 7.5.0 GA to JSA 7.5.0 Update Package 7)

NOTE: Upgrading a non-FIPS deployment to a FIPS enabled deployment is not supported.

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*.

FIPS mode only:

Both the primary and secondary HA hosts must be FIPS enabled.

RELATED DOCUMENTATION

License Keys | 2

Prerequisite Hardware Accessories for JSA Installations | 6

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 1: 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

Prerequisite Hardware Accessories for JSA Installations | 6

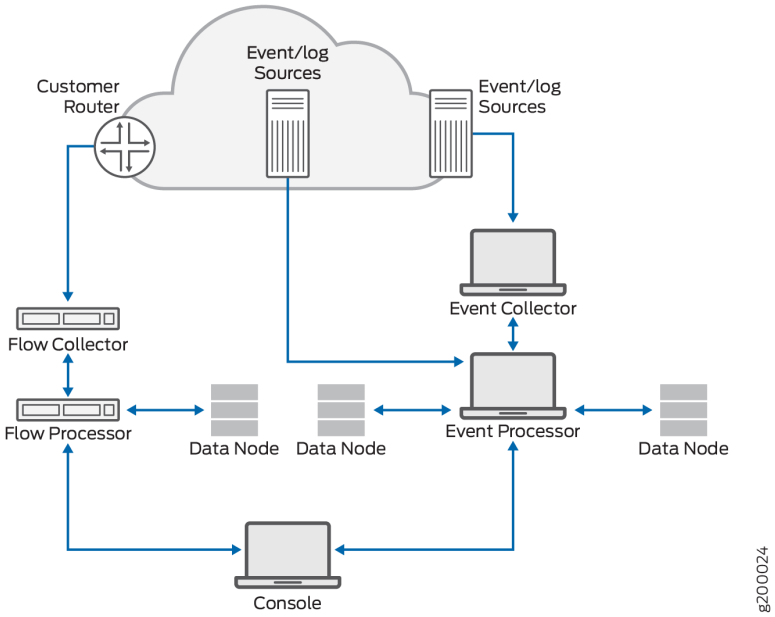
Supported Web Browsers | 7

JSA Components

JSA consolidates event data from log sources that are used by devices and applications in your network. Figure 1 on page 4 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.

RELATED DOCUMENTATION

Prerequisite Hardware Accessories for JSA Installations | 6

Supported Web Browsers | 7

USB Drive Installations | 8

Prerequisite Hardware Accessories for JSA Installations

IN THIS SECTION

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 | 7

USB Drive Installations | 8

Third-party Software on JSA Appliances | 19

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 web browser versions.

Table 2: Supported Web Browsers for JSA Products

Web browser	Supported versions
64-bit Mozilla Firefox	Latest
64-bit Microsoft Edge	Latest
64-bit Google Chrome	Latest

The Microsoft Internet Explorer web browser is no longer supported on JSA 7.4.0 or later.

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 Console instead of your web browser **Back** button.

RELATED DOCUMENTATION

USB Drive Installations | 8

USB Drive Installations

IN THIS SECTION

You can install JSA software with a USB drive.

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

Supported Versions

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

- A Linux system that is installed with:

  Red Hat Enterprise Linux V7.9 for JSA 7.5.0 GA to JSA 7.5.0 Update Package 7

  or

  Red Hat Enterprise Linux V8.8 for JSA 7.5.0 Update Package 8.

- Apple Mac OS X
- Microsoft Windows

Installation Overview

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

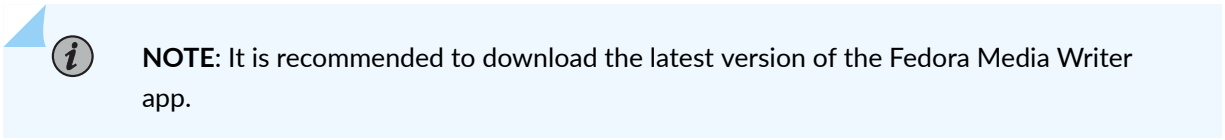
1. Create the bootable USB drive.
2. Install the software for your JSA appliance.
3. Install any product maintenance releases or update packages.

   See latest patch Release Notes for installation instructions for update packages.

Creating a Bootable USB Drive with a Windows System

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 drive.

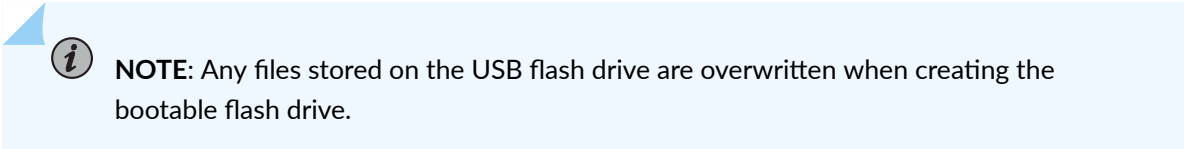


NOTE: It is recommended to download the latest version of the Fedora Media Writer app.

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 Drive" on page 12.

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

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

You must have access to the following items:

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

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

1. Download the JSA ISO image file from the https://support.juniper.net/support/downloads/.
2. Insert the USB drive into a USB port on your system.
3. Open a terminal and type the following command to unmount the USB drive:

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

4. Type the following command to write the JSA ISO to your USB 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 is for raw mode, which makes the transfer much faster. There is no space between the **r** and the name of the connected USB drive.

5. Remove the USB drive from your system.

Creating a Bootable USB 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 drive that you can use to install JSA software.

You must have access to the following items:

- An 8 GB or larger USB drive
- A JSA 7.5.0 or later ISO image file

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

1. Download the JSA ISO image file from the https://support.juniper.net/support/downloads/.
2. Insert the USB drive in the USB port on your system.

   It might take up to 30 seconds for the system to recognize the USB drive.
3. Open a terminal and type the following command to determine the name of the USB drive:

   ```
   dmesg | grep SCSI
   ```

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

   ```
   [ 170.171135] sd 5:0:0:0: [sdb] Attached SCSI removable disk
   ```
4. Type the following commands to unmount the USB 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 drive:

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

Example:

```
[root@jsa ~]# dd if=7.4.2.20201113144954.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 drive from your system. For more information about installing JSA software, see "Installing JSA with a USB Drive" on page 12.

Installing JSA with a USB Drive

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

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.
   - Type "install" for appliances.
   - Type "linux" for virtual machines.

The installation process may take several minutes. After the reboot is complete, the same menu will appear again. You can remove the USB and reboot the appliance. This process can take up to an hour to complete.

5. JSA Console only (For JSA 7.5.0 GA to JSA 7.5.0 Update Package 7): When the **Red Hat Enterprise Linux** menu is displayed, select one of the following options:
   - If you connected a keyboard and monitor, select Install **Red Hat Enterprise Linux 7.9**
   - If you connected a notebook with a serial connection, select **Install Red Hat Enterprise Linux 7.9 using Serial console without format prompt** or **Install Red Hat Enterprise Linux 7.9 using Serial console with format prompt**.
6. JSA Console only (For JSA 7.5.0 Update Package 8): When the **Red Hat Enterprise Linux** menu is displayed, select one of the following options:
   - If you connected a keyboard and monitor, select Install **Red Hat Enterprise Linux 8.8**
   - If you connected a notebook with a serial connection, select **Install Red Hat Enterprise Linux 8.8 using Serial console without format prompt** or **Install Red Hat Enterprise Linux 8.8 using Serial console with format prompt**.
7. FIPS mode only: (For JSA 7.5.0 GA to JSA 7.5.0 Update Package 7): When the **Red Hat Enterprise Linux** menu is displayed, press **Tab** to add `qradar.fips=1` to the appropriate `vmlinuz line`, press **Enter** to select one of the following options.
   - If you connected a keyboard and monitor, modify and select Install Red Hat Enterprise Linux 7.9.
   - If you connected a notebook with a serial connection, modify and select **Install Red Hat Enterprise Linux 7.9 using Serial console without format prompt** or **Install Red Hat Enterprise Linux 7.9 using Serial console with format prompt**.

   The result might look similar to this example:

   ```
   vmlinuz initrd=initrd.img inst.stage2=RHEL-7.9\x20Server.x86_64 live.check quiet qradar.fips=1
   ```
8. FIPS mode only: (For JSA 7.5.0 Update Package 8): When the **Red Hat Enterprise Linux** menu is displayed, press **Tab** to add `qradar.fips=1` to the appropriate `vmlinuz line`, press **Enter** to select one of the following options.
   - If you connected a keyboard and monitor, modify and select Install Red Hat Enterprise Linux 8.8.
   - If you connected a notebook with a serial connection, modify and select **Install Red Hat Enterprise Linux 8.8 using Serial console without format prompt** or **Install Red Hat Enterprise Linux 8.8 using Serial console with format prompt**.

   The result might look similar to this example:

   ```
   vmlinuz initrd=initrd.img inst.stage2=RHEL-7.9\x20Server.x86_64 live.check quiet qradar.fips=1
   ```

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

   The user name is case-sensitive.

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

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

12. Select the **Appliance Install** option on install menu for software installation.

13. Select the appliance ID for the intended appliance functionality, and then select **Next**.

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

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

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

17. Select the Internet Protocol version:

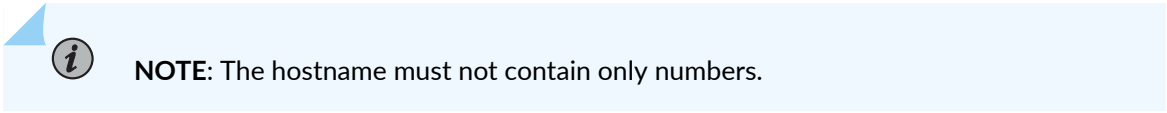
    - Select **ipv4** or **ipv6**.

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

19. Select the bonded interface setup, if required.

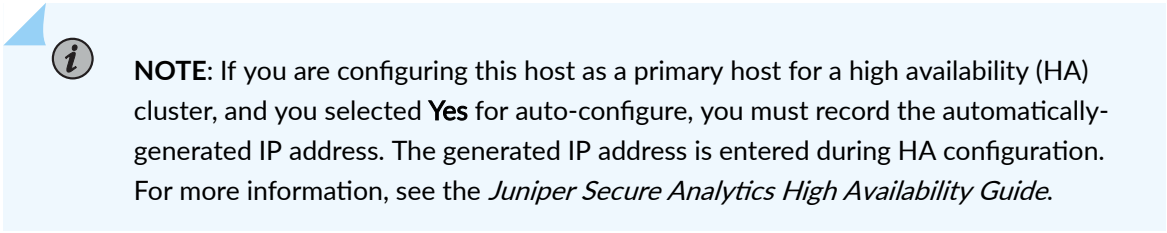
20. Select the management interface.

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

    NOTE: The hostname must not contain only numbers.

22. 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*.

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

24. If you are installing a Console, enter an **admin** password that meets the following criteria:

    - Contains at least 8 characters
    - Contains at least one uppercase character

- Contains at least one lowercase character
- Contains at least one digit
- Contains at least one special character: @, #, ^, or *.

25. Enter **root** password that meets the following criteria:
    - Contains at least 5 characters
    - Contains no spaces
    - Can include the following special characters: @, #, ^, and *.
26. Click **Finish**.

    The installation process might take several minutes. When the installation is complete, if you are installing a JSA Console, proceed to step "27" on page 15. If you are installing a managed host, proceed to "Adding Your Virtual Appliance to Your Deployment" on page 47.
27. 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 that you set during installation.

    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**.

    i. Click **Deploy License Changes**.

RELATED DOCUMENTATION

Third-party Software on JSA Appliances | 19

Supported Web Browsers | 7

Standard Linux Users | 16

Standard Linux Users

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

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

Table 3: Standard Linux User Accounts for Red Hat

User Account	Log in to the Login Shell	Purpose
root (password required)	Yes	Red Hat user
bin	No	Linux Standard Base
daemon	No	Linux Standard Base
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	Red Hat user
ftp	No	Red Hat user

Table 3: Standard Linux User Accounts for Red Hat *(Continued)*

User Account	Log in to the Login Shell	Purpose
nobody	No	Linux Standard Base
systemd-network	No	Red Hat user
dbus	No	Red Hat user
polkitd	No	Red Hat user
sshd	No	Red Hat user
rpc	No	Red Hat user
rpcuser	No	Red Hat user
nfsnobody	No	Red Hat user
abrt	No	Red Hat user
ntp	No	Red Hat user
tcpdump	No	Red Hat user
tss	No	Red Hat user
saslauth	No	Red Hat user
sssd	No	Red Hat user

Table 4: Standard Linux User Accounts for JSA

User Account	Log in to the Login Shell	Purpose
ziptie	No	Ziptie service used by JSA Risk Manager
vis	No	JSA VIS service used by JSA to process scan results
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	Used by 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
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

Table 4: Standard Linux User Accounts for JSA *(Continued)*

User Account	Log in to the Login Shell	Purpose
apache	No	Apache Web Server used by JSA
postfix	No	Mail Service used by JSA to send email
nscd	No	Name Service Cache Daemon used by JSA
qniconfiguser	No	Deployment configuration used by JSA Network Insights
nslcd	No	Used by JSA for LDAP functionality
fusionvm	No	Used by JSA Vulnerability Manager

RELATED DOCUMENTATION

USB Drive Installations | 8

Third-party Software on JSA Appliances | 19

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

Supported Web Browsers | 7

USB Drive Installations | 8

2

CHAPTER

Bandwidth for Managed Hosts

IN THIS CHAPTER

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

IN THIS CHAPTER

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.

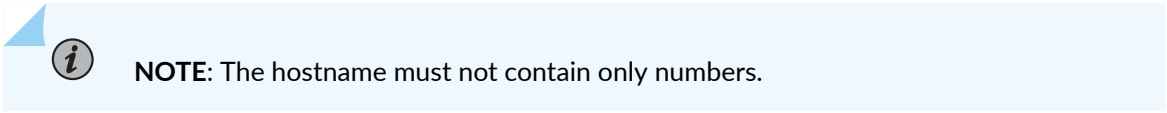
Ensure that the following requirements are met:

- The correct hardware is installed.
- Create a bootable USB flash drive with Red Hat Linux. For more information, see "Creating a Bootable USB Drive with Red Hat Linux" on page 11.
- Install JSA with a USB flash drive. For more information, see "USB Drive Installations" on page 8.
- 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. If you selected **High Availability Appliance** complete the following steps:
   a. Select **HA appliance (All models) 500** as the functionality.
   b. Select whether the high-availability (HA) appliance is a standby for a console or non-console appliance.
   c. Select **Next**.
4. If you did not choose **High Availability Appliance**, select the appliance assignment, 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. If required, select the bonded interface setup,
10. Select the management interface.

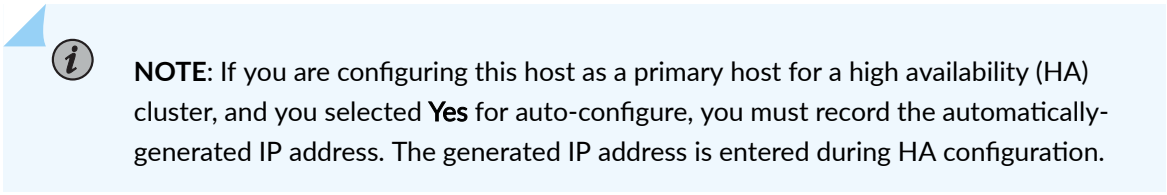
NOTE: If the interface has a link (cable connected), a plus sign (+) is displayed before the description.

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



NOTE: The hostname must not contain only numbers.

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 are installing a Console, enter an **admin** password that meets the following criteria:
    - Contains at least 8 characters
    - Contains at least one uppercase character
    - Contains at least one lowercase character
    - Contains at least one digit
    - Contains at least one special character: @, #, ^, or *.
14. Enter **root** password that meets the following criteria:
    - Contains at least 5 characters
    - Contains no spaces
    - Can include the following special characters: @, #, ^, and *.
15. Click **Finish**.

    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. When the JSA installation process is complete, the message window appears.
16. 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**.

i. Click **Deploy License Changes**.

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

4

CHAPTER

Virtual Appliance Installations for JSA and Log Manager

IN THIS CHAPTER

Virtual Appliance Installations for JSA and Log Manager

You can install JSA Threat Analytics 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. You do not need to configure partitions or perform other RHEL preparation as part of an appliance installation.

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.

RELATED DOCUMENTATION

Overview of Supported Virtual Appliances | 28
Creating Your Virtual Machine | 41
Installing JSA on a Virtual Machine | 43

Overview of Supported Virtual Appliances

IN THIS SECTION

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 Flow Processor Virtual 1799
- JSA Event Processor Virtual 1699
- JSA Event Collector Virtual 1599
- JSA Flow Processor Virtual 1299
- JSA Risk Manager 700
- JSA Vulnerability Manager Processor 600
- JSA Vulnerability Manager Scanner 610
- JSA App Host 4000
- JSA Log Manager Virtual 8099

NOTE: The JSA Vulnerability Manager scanner is end of life (EOL) in 7.5.0 Update Package 6, and is no longer supported in any version of JSA. In JSA 7.5.0 Update Package 6 and later, you can continue to use thirdparty scanners with your JSA Vulnerability Manager platform, but you cannot scan within your DMZ.

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 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 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 30,000 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 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:

- JSA Console only: Maximum throughput of 1 Gbps

  JSA Console only: If the hardware and software specifications are the same, a virtual appliance can deliver throughput levels that are comparable to JSA supplied appliances.

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

JSA Vulnerability Manager Processor 600

NOTE: The JSA Vulnerability Manager scanner is end of life (EOL) in 7.5.0 Update Package 6, and is no longer supported in any version of JSA. In JSA 7.5.0 Update Package 6 and later, you can continue to use thirdparty scanners with your JSA Vulnerability Manager platform, but you cannot scan within your DMZ.

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 610

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

NOTE: The JSA Vulnerability Manager scanner is end of life (EOL) in 7.5.0 Update Package 6, and is no longer supported in any version of JSA. In JSA 7.5.0 Update Package 6 and later, you can continue to use thirdparty scanners with your JSA Vulnerability Manager platform, but you cannot scan within your DMZ.

JSA Risk Manager 700

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.

JSA Log Manager Virtual 8099

Functions as a Log Manager AIO/Console.

RELATED DOCUMENTATION

- Creating Your Virtual Machine | 41
- Installing JSA on a Virtual Machine | 43
- Adding Your Virtual Appliance to Your Deployment | 47

System Requirements for Virtual Appliances

IN THIS SECTION

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 41.

JSA Console only: JSA virtual appliances require x86 hardware.

JSA Console only: JSA appliances are certified to support certain maximum events per second (EPS) rates. Maximum EPS depends on the type of data that is processed, system configuration, and system load.

NOTE: The minimum requirements support JSA functions 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.

NOTE: You can change the memory or the CPU of your virtual appliance by shutting down the virtual appliance and making the changes. When you restart the virtual appliance, the system detects the changes and adjusts the performance-related configuration.

Memory Requirements

The following table describes the memory requirements for virtual appliances.

Table 5: 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 Event Collector Virtual 1599	12 GB (up to 20,000 EPS) 64 GB (40,000 EPS) 128 GB (80,000 EPS)	16 GB (up to 20,000 EPS) 64 GB (40,000 EPS) 128 GB (80,000 EPS)
JSA Event Processor Virtual 1699 up to 20,000 EPS	JSA Console only: 16 GB FIPS mode only: 12 GB	JSA Console only: 64 GB FIPS mode only: 48 GB
JSA Event Processor Virtual 1699 20,000 EPS or higher	128 GB	128 GB

Table 5: Minimum and Suggested Memory Requirements for JSA Virtual Appliances *(Continued)*

Appliance	Minimum memory requirement	Suggested memory requirement
JSA Flow Processor Virtual 1799 up to 1,200,000 FPM	16 GB	64 GB
JSA Flow Processor Virtual 1799 1,200,000 FPM or higher	128 GB	128 GB
JSA Threat Analytics “All-in-one” or Console 3199 5,000 EPS or less 200,000 FPM or less	32 GB	64 GB
JSA Threat Analytics “All-in-one” or Console 3199 30,000 EPS or less 1,000,000 FPM or less	128 GB	128 GB
JSA Log Manager Virtual 8099	24 GB	48 GB
JSA Risk Manager 700	24 GB	48 GB

Table 5: Minimum and Suggested Memory Requirements for JSA Virtual Appliances *(Continued)*

Appliance	Minimum memory requirement	Suggested memory requirement
JSA Vulnerability Manager Processor 600 **NOTE**: The JSA Vulnerability Manager scanner is end of life (EOL) in 7.5.0 Update Package 6, and is no longer supported in any version of JSA. In JSA 7.5.0 Update Package 6 and later, you can continue to use thirdparty scanners with your JSA Vulnerability Manager platform, but you cannot scan within your DMZ.	32 GB	32 GB
JSA Vulnerability Manager Scanner 610 **NOTE**: The JSA Vulnerability Manager scanner is end of life (EOL) in 7.5.0 Update Package 6, and is no longer supported in any version of JSA. In JSA 7.5.0 Update Package 6 and later, you can continue to use thirdparty scanners with your JSA Vulnerability Manager platform, but you cannot scan within your DMZ.	16 GB	16 GB
JSA App Host 4000	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 6: 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
JSA Event Collector Virtual 1599	5,000 EPS or less	8	16
	20,000 EPS or less 40,000 EPS or less 80,000 EPS or less	19 40 80	19 40 80
JSA Event Processor Virtual 1699	5,000 EPS or less	8	24
	20,000 EPS or less	16	32
	40,000 EPS or less	40	48
	80,000 EPS or less	56	JSA Console only: 80 FIPS mode only: 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	JSA Console only: 32 FIPS mode only: 24
	2,400,000 FPM or less	JSA Console only: 40 FIPS mode only: 48	48
	3,600,000 FPM or less	56	80

Table 6: 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	32
	300,000 FPM or less 15,000 EPS or less	40	48
	1,200,000 FPM or less 30,000 EPS or less	56	80
JSA Log Manager Virtual 8099	2,500 EPS or less	4	16
	5,000 EPS or less	8	16

Table 6: CPU Requirements for JSA Virtual Appliances *(Continued)*

Appliance	Threshold	Minimum number of CPU cores	Suggested number of CPU cores
JSA Vulnerability Manager Processor 600 **NOTE**: The JSA Vulnerability Manager scanner is end of life (EOL) in 7.5.0 Update Package 6, and is no longer supported in any version of JSA. In JSA 7.5.0 Update Package 6 and later, you can continue to use thirdparty scanners with your JSA Vulnerability Manager platform, but you cannot scan within your DMZ.		4	4

Table 6: CPU Requirements for JSA Virtual Appliances *(Continued)*

Appliance	Threshold	Minimum number of CPU cores	Suggested number of CPU cores
JSA Vulnerability Manager Scanner 610 **NOTE**: The JSA Vulnerability Manager scanner is end of life (EOL) in 7.5.0 Update Package 6, and is no longer supported in any version of JSA. In JSA 7.5.0 Update Package 6 and later, you can continue to use thirdparty scanners with your JSA Vulnerability Manager platform, but you cannot scan within your DMZ.		4	4
JSA Risk Manager 700		8	8
JSA App Host 4000		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.

The following table shows the storage requirements for virtual installations.

Table 7: Minimum storage requirements for appliances when you use the virtual installation option.

System classification	IOPS	Data transfer rate (MB/s)
Minimum performance	800	500
Medium performance	1200	1000
High Performance	10,000	2000
Small All-in-One (Console) or 1699	300	300
Event/Flow Processors	300	300

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

RELATED DOCUMENTATION

- Creating Your Virtual Machine | 41
- Installing JSA on a Virtual Machine | 43
- Adding Your Virtual Appliance to Your Deployment | 47

Creating Your Virtual Machine

To install a virtual appliance, you must first use VMware vSphere Client to create a virtual machine.

JSA virtual appliances require x86 hardware.

1. Select the host and choose **File** > **New** > **Virtual Machine**, and then click **Next**.
2. Select **Custom** In the Configuration pane of the Create New Virtual Machine window, and then click **Next**.
3. Enter a name for the virtual machine in the Name and Location pane, and then click **Next**.
4. Select the datastore in which you want to store the virtual machine files, and then click **Next**.

5. Select **Virtual Machine Version: X** in the Virtual Machine Version pane, and then click **Next**. **X** is the software version that is available on the machine. For example, virtual machine version 13 or virtual machine version 7.
6. Select **Linux** under Guest operating System and then select **Linux Red Hat Enterprise Linux 7 (64-bit)** under Version, and then click Next.
7. Configure the number of virtual processors that you want for the virtual machine on the CPUs page, and then click **Next**.

   When you configure the parameters on the CPU page, you must configure a minimum of two processors. The combination of number of virtual sockets and number of cores per virtual socket determines how many processors are configured on your system.

   Table 8 on page 42 provides examples of CPU page settings you can use.

   Table 8: Descriptions for Network Configuration Parameters

Number of Processors	Sample CPU Page Settings
2	Number of virtual sockets = 1 Number of cores per virtual socket = 2
2	Number of virtual sockets = 2 Number of cores per virtual socket = 1
4	Number of virtual sockets = 4 Number of cores per virtual socket = 1
4	Number of virtual sockets = 2 Number of cores per virtual socket = 2

8. In the **Memory Size** field, type or select **24 GB** and then click **Next**.

   Table 5 on page 34 describes the minimum memory requirements for virtual appliances.
9. To configure your network connections, perform the following steps:

   a. Add at least one Network Interface Controller (NIC) for How many NICs do you want to connect.

   b. Select **VMXNET3** for Adapter.

   c. Select **Connect at Power On**.

d. Click **Next**.

10. Select **VMware Paravirtual** in the SCSI Controller pane, and then click **Next**.
11. Select **Create a new virtual disk** in the Select a Disk pane, and then click **Next**.
12. To configure the virtual disk parameters in the Create a Disk pane, perform the following steps:

    a. Select **256 or higher (GB)** in Capacity.

    > **NOTE**: After successful installation, extra disk space cannot be added.

    b. Select **Thin provisioning** in Disk Provisioning.

    c. Select **Store with the virtual machine** in Location.

    d. Click **Next**.

13. In the **Advanced Options** page, do not configure anything.
14. On the Ready to Complete page, review the settings and click **Finish**.

RELATED DOCUMENTATION

Installing JSA on a Virtual Machine | 43

Adding Your Virtual Appliance to Your Deployment | 47

Overview of Supported Virtual Appliances | 28

Installing JSA on a Virtual Machine

Create a virtual machine. For more information, see "Creating Your Virtual Machine" on page 41.

> **NOTE**: The software installation menu will not be visible in the installation wizard by default. If you want to do JSA software installation, refer to JSA Software only Installations.

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

1. FIPS mode only: On the **Red Hat Enterprise Linux 7.9** start menu, click **Tab** to edit the vmlinuz line.
2. FIPS mode only: Add `qradar.fips=1` to the `vmlinuz` line and click **Enter**.

The result might look similar to this example:

```
vmlinuz initrd=initrd.img inst.stage2=hd:LABEl=QRadar-2020_11_0_20201210153453 quiet
inst.text inst.gpt inst.ks=hd:LABEL=QRadar-2020_11_0_20201210153452console=ttyS0,9600
console=tty1 qradar.fips=1
```

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

   The user name is case-sensitive.

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

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

5. Select the appliance type:

   - **Appliance Install (purchased as an appliance)**
   - **High Availability Appliance**
   - **App Host Appliance**
   - **Log Analytics Appliance**

   NOTE: You can select the appliance type based on the intended appliance functionality.

6. If you selected an appliance for high-availability (HA), select whether the appliance is a console.
7. If you selected an appliance for Log Analytics Appliance, select LA (Log Analytics "All-In-One" or Console 8099).
8. For the type of setup, select **Normal Setup (default)** or **HA Recovery Setup**, and select Next.
9. The Date/Time Setup page appears. Enter the current date in the **Current Date (YYYY/MM/DD)** field in the format displayed. A date is also displayed for your reference. Enter the time in 24-hour format in the **24h Clock Time (HH:MM: SS)** field. Alternatively, you can enter the name or the IP address of the time server to which the time can be synced in the **Time Server** field. After entering the date and time details, select Next.
10. The Select Continent/Area page appears. Select the **Time Zone Continent or Area** as required and select Next. The default value is America.
11. The Time Zone Selection page appears. Select the **Time Zone City or Region** as required and select Next. The default value is New York.
12. If you selected **HA Recovery Setup**, enter the cluster virtual IP address.
13. Select the Internet Protocol version:

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

14. If you selected **ipv6**, select **manual** or **auto** for the **Configuration type**.
15. Select the bonded interface setup.
16. Select the management interface.

NOTE: If the interface has a link (cable connected), a plus sign (+) is displayed before the description.

17. In the Network Information Setup window, configure the following network settings and select Next.
    - Hostname: Enter a fully qualified domain name as the system hostname
    - IP Address: Enter the IP address of the system
    - Network Mask: Enter the network mask for the system
    - Gateway: Enter the default gateway of the system
    - Primary DNS: Enter the primary DNS server address
    - Secondary DNS: (Optional) Type the secondary DNS server address
    - Public IP: (Optional) Enter the Public IP address of the server

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*.

18. If you are installing a Console, enter an **admin** password that meets the following criteria:
    - Contains at least 8 characters
    - Contains at least one uppercase character
    - Contains at least one lowercase character
    - Contains at least one digit
    - Contains at least one special character: @, #, ^, or *.
19. Enter **root** password that meets the following criteria:
    - Contains at least 5 characters
    - Contains no spaces
    - Can include the following special characters: @, #, ^, and *.

20. Click **Next**.

    The installation process might take several minutes. When the installation is complete, if you are installing a JSA Console, proceed to step 21. If you are installing a managed host, proceed to "Adding Your Virtual Appliance to Your Deployment" on page 47.

21. 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 that you set during installation.

    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**.

    i. Click **Deploy License Changes**.

22. FIPS mode only: Verify that FIPS mode is enabled by typing the following command.

```
/opt/qradar/bin/myver -fips
```

    The output is 'true' on a FIPS mode enabled system and 'false' when FIPS mode is not enabled.

    If the result is false, try to reinstall with FIPS mode enabled.

RELATED DOCUMENTATION

- Adding Your Virtual Appliance to Your Deployment | 47
- Overview of Supported Virtual Appliances | 28
- Creating Your Virtual Machine | 41

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 admin user account that you set during installation.

   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**.

   i. Click **Deploy License Changes**.

RELATED DOCUMENTATION

Overview of Supported Virtual Appliances | 28

Creating Your Virtual Machine | 41

Installing JSA on a Virtual Machine | 43

5
CHAPTER

Installations from the Recovery Partition

IN THIS CHAPTER

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 | 47

Reinstalling from the Recovery Partition | 49

Installing JSA on a Virtual Machine | 43

Reinstalling 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*.

You can reinstall JSA products from the recovery partition.

1. Restart your JSA appliance.
2. Select **Factory re-install**. This process can take up to several minutes.
3. Log in as the root user.
4. Ensure that the **End User License Agreement** (EULA) is displayed.

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

5. For JSA console installations, select the **Enterprise** tuning template.
6. Follow the instructions in the installation wizard to complete the installation.
7. 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**.

   i. Click **Deploy License Changes**.

RELATED DOCUMENTATION

Adding Your Virtual Appliance to Your Deployment | 47

Installations from the Recovery Partition | 49

Installing JSA on a Virtual Machine | 43

CHAPTER 6

Reinstalling JSA from Media

IN THIS CHAPTER

Reinstalling JSA from Media

You can reinstall JSA products from media such as the ISO file or a USB flash drive. For more information about reinstalling JSA, see "Installing JSA with a USB Drive" on page 12.

CHAPTER 7

JSA Software only Installations

IN THIS CHAPTER

JSA Software only Installations

IN THIS SECTION

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

Important

- Ensure that your hardware meets the system requirements for JSA deployments.
- JSA Software node license comes with the default Red Hat entitlement. You can provide your own RHEL, or acquire entitlement to a JSA Software Node. For the vulnerability updates, you must purchase RHEL entitlement from the satellite server.
- 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.
- It is not possible to do a factory reset from the recovery partition when you do a software only installation.

NOTE: Software installations do not come with the recovery partition available, and also these instructions do not apply.

Complete the following tasks in order:

- "Installing RHEL on Your Own System" on page 57
- "Installing JSA After the RHEL Installation" on page 64

Prerequisites for Installing JSA on Your Hardware

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.

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 versions.

Table 9: Red Hat Version

JSA Version	Red Hat Enterprise Linux Version
JSA 7.5.0 GA to JSA 7.5.0 Update Package 7	Red Hat Enterprise Linux V7.9 64-bit
JSA 7.5.0 Update Package 8	Red Hat Enterprise Linux V8.8 64-bit

The following table describes the system requirements:

Table 10: System Requirements for RHEL Installations on your own Hardware

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. Optional If you want to use NTP as your time server, ensure that you install the Chrony package.

Table 10: System Requirements for RHEL Installations on your own Hardware *(Continued)*

Requirements	Description
Firewall configuration	WWW (http, https) enabled SSH-enabled
Hardware	See the tables below for memory, processor, and storage requirements.

Memory and CPU Requirements

If you use hardware not provided by Juniper, ensure that your hardware meets or exceeds the specifications for memory and CPU of the corresponding JSA appliance.

NOTE: You can change the memory or the CPU of your appliance by shutting down the appliance and making the changes. When you restart the appliance the system detects the changes and adjusts the performance related configuration. You must maintain the minimum requirements.

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.

NOTE: The minimum required storage size varies, based on factors such as event size, events per second (EPS), and retention requirements.

Table 11: Minimum Storage Requirements for Software Only Installations

System classification	IOPS	Data transfer rate (MB/s)
Minimum performance	800	500
Medium performance	1200	1000
High Performance	10,000	2000

Table 11: Minimum Storage Requirements for Software Only Installations *(Continued)*

System classification	IOPS	Data transfer rate (MB/s)
All Platforms Event Processor	300	300
Event/Flow Processors	300	300

Installing RHEL on Your Own System

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.

Download the Red Hat Enterprise Linux Server Binary DVD from https://access.redhat.com.

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

Table 12: Red Hat Version

JSA Version	Red Hat Enterprise Linux version
JSA 7.5.0 GA to JSA 7.5.0 Update Package 7	Red Hat Enterprise Linux Server V7.9 Binary DVD
JSA 7.5.0 Update Package 8	Red Hat Enterprise Linux Server V8.8 Binary DVD

JSA Software node license comes with the default Red Hat entitlement. You can provide your own RHEL, or acquire entitlement to a JSA Software Node. For the vulnerability updates, you must purchase RHEL entitlement from the satellite server.

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

NOTE: FIPS mode only (For JSA 7.5.0 GA to JSA 7.5.0 Update Package 7): To install RHEL in FIPS mode, add `qradar.fips=1` to the `vmlinuz`.

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 Drive Installations" on page 8.

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

3. FIPS mode only (For JSA 7.5.0 GA to JSA 7.5.0 Update Package 7): From the Red Hat Enterprise Linux 7.9 installer start menu, click Tab.

4. FIPS mode only (JSA 7.5.0 GA to JSA 7.5.0 Update Package 7): Add `qradar.fips=1` to the `vmlinuz` line and press Enter.

   The result might look similar to this example:

   ```
   vmlinuz initrd=initrd.img inst.stage2=RHEL-7.9\x20Server.x86_64 live.check quiet
   qradar.fips=1
   ```

5. 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.

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

7. 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 System" on page 60.

      To encrypt data complete the following steps:

      i. Select one of the LVM partitions created.

      ii. Select **Modify** under the **Volume Group** section. A pop up console opens for further configuration options.

iii. Select **Encrypt**.

iv. Save the changes.

> **NOTE**: Upgrading to RHEL-8 on systems with LUKS encrypted partitions is not supported. Ensure that your deployment does not include hosts with LUKS encrypted partitions to successfully upgrade your system. For more information, see Upgrading Juniper Secure Analytics to 7.5.0.

g. Click **Network & Host Name**.

h. Enter a fully qualified domain name for your appliance hostname.

> **NOTE**: JSA Console Only: The Console and managed host (MH) cannot have the same hostname.

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**.

8. Set the root password, and then click **Finish configuration**.

9. After the installation is complete, disable SELinux by modifying the **/etc/selinux/config** file, and restart the appliance.

   To modify the **/etc/selinux/config** file, complete the following steps:

   a. Open the **/etc/selinux/config** file using the following command:

```
# vi /etc/selinux/config
```

   b. Configure the `SELINUX=disabled` option:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
```

```
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected,
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

c. Save the file and restart the appliance.

```
# :wq
```

```
# reboot
```

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

If you use your own disk drive 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. You must use these partition names. Using other partition names can cause the installation to fail and other issues.

Table 13: Partitioning Guide for RHEL for JSA 7.5.0 Update Package 8

Mount Path	LVM Supported?	Size	File System
/boot	No	1 GB	XFS
/boot/efi	No	200 MB	VFAT
/var	Yes	5 GB	XFS
/var/log	Yes	15 GB	
/var/log/audit	Yes	3 GB	

Table 13: Partitioning Guide for RHEL for JSA 7.5.0 Update Package 8 *(Continued)*

Mount Path		LVM Supported?	Size	File System
/opt		Yes	13 GB	
/home		Yes	1 GB	
/storetmp		Yes	15 GB	
/tmp		Yes	3 GB	
swap		N/A	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	Upto 15 GB	
JSA Console App Host	/transient	Yes	20 % of remaining space	
	/store	Yes	80% of remaining space	
Processors and Collectors	/transient	Yes	The lesser of 20% of the remaining space and 500 GB	
	/store	Yes	The remaining space after / transient allocation	

Table 13: Partitioning Guide for RHEL for JSA 7.5.0 Update Package 8 *(Continued)*

Mount Path		LVM Supported?	Size	File System
Data Nodes	/transient	Yes	The lesser of 10% of the remaining space and 100 GB	
	/store	Yes	The remaining space after / transient allocation	

Table 14: Partitioning Guide for RHEL for JSA 7.5.0 GA to JSA 7.5.0 Update Package 7

Mount Path	LVM Supported?	Size	File System
/boot	No	1 GB	XFS
/boot/efi	No	200 MB	
/var	Yes	5 GB	
/var/log	Yes	15 GB	
/var/log/audit	Yes	3 GB	
/opt	Yes	13 GB	
/home	Yes	1 GB	
/storetmp	Yes	15 GB	
/tmp	Yes	3 GB	

Table 14: Partitioning Guide for RHEL for JSA 7.5.0 GA to JSA 7.5.0 Update Package 7 *(Continued)*

Mount Path	LVM Supported?	Size	File System
swap	N/A	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	Upto 15 GB	
/transient	Yes	20% of remaining space	
/store	Yes	80% 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.

Table 15: Default Storage Configurations for JSA

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 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 installation, manually 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. JSA Console Only:
   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" on page 64 and "4" on page 64 after the system restart to continue the installation.

5. FIPS mode only (For JSA 7.5.0 GA to JSA 7.5.0 Update Package 7): When the OS installation finishes run the QRadar setup by typing the following command:`/media/cdrom/setup --fips`. The --fips option verifies that the OS is FIPS enabled so that you can proceed with the installation. If RHEL is not FIPS enabled, the installation fails with the following error message:

```
"** ERROR: Installing QRadar in FIPS mode requires the operating system to be running in
FIPS
mode."
```

NOTE: A new kernel might be installed as part of the installation, which requires a system restart. Repeat the commands in steps "3" on page 64 and "4" on page 64 after the system restarts.

6. Select the disk drive type:

NOTE: The software installation menu will not be visible in the installation wizard by default.

- **Software Install**
- **High Availability Appliance**

7. Select the disk drive assignment, and then select **Next**.
8. If you selected an disk drive for high-availability (HA), select whether the disk drive is a console.
9. For the type of setup, select **Normal Setup (default)** or **HA Recovery Setup**, and set up the time.
10. If you selected **HA Recovery Setup**, enter the cluster virtual IP address.
11. Select the Internet Protocol version.
12. If you selected **ipv6**, select **manual** or auto for the **Configuration type**.
13. Select the bonded interface setup, if required.

14. Select the management interface.
15. In the wizard, enter a fully qualified domain name in the **Hostname** field.

    NOTE: The hostname must not contain only numbers.

    NOTE: JSA Console only: The console and managed host (MH) cannot share the have hostname.

16. 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*.

17. If you do not have a email server, enter `localhost` in the **Email server name** field.
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. Leave the `root` password as it is.
20. Click **Finish**.
21. Follow the instructions in the installation wizard to complete the installation.

    The installation process might take several minutes.

22. 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**.

i. Click **Deploy License Changes**.

23. If you want to add managed hosts, see *Juniper Security Analytics Administration Guide*.

RELATED DOCUMENTATION

Prerequisite Hardware Accessories for JSA Installations | 6

8
CHAPTER

Setting up a JSA Silent Installation

IN THIS CHAPTER

Setting up a JSA Silent Installation

JSA Console only Install IBM JSA "silently," or perform an unattended installation.

- You must have the JSA ISO for the release that you want to install.
- Modify the SELINUX value in the `/etc/sysconfig/selinux` file to `SELINUX=disabled`, and restart the system.
- You must install Red Hat Enterprise Linux (RHEL) on the system where you want to install JSA. For more information, see "Installing RHEL on your own appliance" on page 57. The following table describes the version of Red Hat Enterprise Linux used with the JSA version.

Table 16: Red Hat version

JSA Version	Red Hat Enterprise Linux Version
JSA 7.5.0 GA to JSA 7.5.0 Update Package 7	Red Hat Enterprise Linux V7.9 64-bit
JSA 7.5.0 Update Package 8	Red Hat Enterprise Linux V8.8 64-bit

1. As the root user, use SSH to log on to the host where you want to install JSA.
2. In the root directory of the host where you want to install JSA, create a file that is named AUTO_INSTALL_INSTRUCTIONS and contains the following content:

   Table 17: Silent Install File parameters. Parameters that are listed as "Optional" are required in the AUTO_INSTALL_INSTRUCTIONS file, but can have no value.

Parameter	Value Required?	Description	Permitted values
`force`	Required	Forces the installation of the appliance despite any hardware issues.	`true or false`

Table 17: Silent Install File parameters. Parameters that are listed as "Optional" are required in the AUTO_INSTALL_INSTRUCTIONS file, but can have no value. *(Continued)*

Parameter	Value Required?	Description	Permitted values
`api_auth_token`	Optional	An authorization token. For more information about managing authorized services, see the *Juniper Secure Analytics Administration Guide*	Authorization token
`appliance_number`	Optional	The identifier for the appliance	0, 3105, 1201, and so on.
`appliance_oem`	Required	Identifies the appliance provider.	`JSA and so on`
`appliance_filter`	Required	The appliance name or identifier.	`vmware, na`
`bonding enabled`	Required	Specifies whether you are using bonded interfaces.	`true or false`
`bonding_interface`	If using bonded interfaces, then required.	The MAC addresses for the interfaces that you are bonding, separated by commas.	*<interface_name =mac_address><seconda ry_interface_name*=mac_ address>
`bonding_interface_name`	If using bonded interfaces, then required.	Identifies the bonding interface.	bond0
`bonding_options`	If using bonded interfaces, then required.	The Linux options for bonded interfaces.	Example: miimon=100 mode=4 lacp_rate=1
`ha_cluster_virtual_ip`	Optional	Specifies the IP address for the HA cluster	ip_address

Table 17: Silent Install File parameters. Parameters that are listed as "Optional" are required in the AUTO_INSTALL_INSTRUCTIONS file, but can have no value. *(Continued)*

Parameter	Value Required?	Description	Permitted values
`hostname`	Required	The fully qualified host name for JSA system	
`ip_protocol`	Required	The IP protocol for this host.	ipv4, ipv6
`ip_dns_primary`	If ip_protocol is set to IPv4, then required	The primary DNS server.	A valid IPv4 address
`ip_dns_secondary`	If ip_protocol is set to IPv4, then required	The secondary DNS server.	A valid IPv4 address
`ip_management_interface`	Required	The interface name, and the MAC address of the management interface. You can use either, or both separated by "=".	
`ipv4_address`	If ip_protocol is set to IPv4, then required	The IP address of the host that you are installing the software on.	A valid IPv4 address
`ipv4_address_public`	If ip_protocol is set to IPv4, and NATed, then required	The public IP address of the host that you are installing the software on.	A valid IPv4 address
`ipv4_gateway`	If ip_protocol is set to IPv4, then required	The network gateway for this host	A valid IPv4 address
`ipv4_network_mask`	If ip_protocol is set to IPv4, then required	The netmask for this host	

Table 17: Silent Install File parameters. Parameters that are listed as "Optional" are required in the AUTO_INSTALL_INSTRUCTIONS file, but can have no value. *(Continued)*

Parameter	Value Required?	Description	Permitted values
`ip_v6_address`	If ip_protocol is set to IPv6, then required	The IPv6 address of the JSA installation if required.	A valid IPv6 address
`ip_v6_address_public`	If ip_protocol is set to IPv6, and NATed, then required	The public IP address of the host that you are installing the software on.	A valid IPv6 address
`ip_v6_autoconf`	Required	Specifies whether IPv6 is autoconfigured.	`true or false`
`ip_v6_gateway`	Not Required	Leave empty.	
`is_console`	Required	Specifies whether this host is the console within the deployment	`true` - This host is the console in the deployment `false` - This is not the console and is another type of managed host (Event or Flow Processor, and so on)
`is_console_standby`	Required	Specifies whether this host is an HA console standby	`true or false`

Table 17: Silent Install File parameters. Parameters that are listed as "Optional" are required in the AUTO_INSTALL_INSTRUCTIONS file, but can have no value. *(Continued)*

Parameter	Value Required?	Description	Permitted values
admin_password	Optional	The password for the administrator account. You can encrypt the password if required. If you leave this parameter blank, the password is not updated.	<password> Important: Your company's security policies can prevent you from entering a password in a static file on theappliance. Defined, or leaving the value empty to use a previously entered password on an upgrade.
root_password	Required	The password for the root account. You can encrypt the password, if required. If you leave this parameter blank, the password is not updated.	<password> Important: Your company's security policies can prevent you from entering a password in a static file on the appliance. Defined, or leaving the value empty uses a previously entered password on an upgrade.
security_template	If isconsole is set to Y, then required	The security template This value must be consistent with the value entered in appliance_number.	Enterprise - for all SIEM-based hosts Logger - for Log Manager

Table 17: Silent Install File parameters. Parameters that are listed as "Optional" are required in the AUTO_INSTALL_INSTRUCTIONS file, but can have no value. *(Continued)*

Parameter	Value Required?	Description	Permitted values
`time_current_date`	Required	The current date for this host. Use the following format: YYYY/MM/DD format	
`time_current_time`	Required	The time for the host in the 24 hour format HH:MM:SS.	
`time_ntp_server`	Optional	The FQHN or IP address of the network time protocol (NTP) server.	
`timezone`	Required	The time zone from the TZ database.	Europe/London GMT America/Montreal America/New_York America/Los_Angeles Asia/Tokyo, and so on.
`type_of_setup`	Required	Specifies the type of installation for this host	normal- A standard JSA managed host or console deployment. recovery - A High Availability (HA) recovery installation on this host.

Example:

```
#0.0.1
ai_force=<true_false>
ai_api_auth_token= <certificate>
ai_appliance_number= <####>
ai_appliance_oem= <qradar_forensics_or_oem>
ai_appliance_filter= <appliance_number_or_identifier>
ai_bonding_enabled= <true_or_false>
ai_bonding_interfaces= <mac_address>
ai_bonding_interface_name= <interface_identifier>
ai_bonding_options= <bonding_option_identifiers>
ai_gateway_setup_choice= <true_or_false>
ai_ha_cluster_virtual_ip= <IP_address>
ai_hostname= <hostname_with_FQDN>
ai_ip_dns_primary= <IP_address_of _primary_DNS>
ai_ip_dns_secondary= <IP_address_of_secondary DNS>
ai_ip_management_interface= <MAC_address>
ai_ip_protocol= <ipv4_or_ipv6>
ai_ip_v4_address= <IP_address>
ai_ip_v4_address_public= <public_IP_address>
ai_ip_v4_gateway= <IP_address_of_gateway>
ai_ip_v4_network_mask= <network_mask>
ai_ip_v6_address= <IPv6_address>
ai_ip_v6_address_public= <IPv6_public_address>
ai_ip_v6_autoconf= <true_false>
ai_ip_v6_gateway= <IP_address>
ai_is_console= <true_or_false>ai_is_console_standby= <true_or_false>
ai_root_password= <password_for_root_account>
ai_security_template= <enterprise_or_logger>
ai_time_current_date= <yyyy-mm-dd>
ai_time_current_time= <hh:mm:ss>
ai_time_ntp_server= <ntpserver_hostserver>
ai_timezone= <EST_or_PST_or_timezone>
ai_type_of_setup= <normal_or_recovery>
ai_console_host= <IP_address_or_identifier_for_SIOC_7000_host>
ai_http_proxy_host= <SIOC_7000_proxy_hostname>
ai_http_proxy_password= <SIOC_7000_proxy_password>
ai_http_proxy_port= <SIOC_7000_proxy_port>
ai_http_proxy_user= <SIOC_7000_proxy_user_name>
ai_internet_access_mode= <SIOC_7000_direct_or_proxy>
```

Replace the configuration settings in the file with ones that are suitable for your environment.

NOTE: Ensure that the `AUTO_INSTALL_INSTRUCTIONS` file has no extension, such as .txt, or .doc. The installation does not succeed if the file has an extension.

3. Using an SFTP program copy the JSA ISO to the host where you want to install JSA.
4. On the host where you are installing, create a **/media/cdrom** directory on the host by using the command:

   ```
   mkdir /media/cdrom
   ```

5. Mount the JSA ISO by using the command:

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

6. Run the JSA setup by using the command:

   ```
   /media/cdrom/setup
   ```

7. Open the End User License Agreement (EULA) at /media/cdrom/EULA.txt and review.
8. To agree to the EULA, `add --accept-eula` to the /media/cdrom/setup command.

   When you add `--accept-eula`, you bypass the EULA prompt.

CHAPTER 9

Configuring Bonded Management Interfaces

IN THIS CHAPTER

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” bonding 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.

   NOTE: JSA Console only: Verify all external storage that is not **/store/ariel** or **/store** is not mounted.

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.

10
CHAPTER

Network Settings Management

IN THIS CHAPTER

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 | 80

Changing the Network Settings Of a JSA Console in a Multi-system Deployment | 82

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.

JSA Console only:

NOTE: You cannot change the IP address of any host to the IP address of a previously deleted Managed Host.

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.

NOTE: JSA Console only: Verify all external storage which is not **/store/ariel** or **/store** is not mounted.

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

   The following table contains information to help you configure the network settings.

Table 18: Description Of Network Settings for an JSA 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 | 80

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
- JSA Console only: If you are adding a network adapter to either physical appliance or a virtual machine, you must shut down the appliance before you add the network adapter. Power on the appliance before you follow this procedure.

JSA Console only:

NOTE: You cannot change the IP address of any host to the IP address of a previously deleted Managed Host.

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.

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.

NOTE: JSA Console only: Verify all external storage which is not **/store/ariel** or **/store** is not mounted.

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 | 80

Changing the Network Settings in an All-in-One System | 80

CHAPTER 11

Troubleshooting Problems

IN THIS CHAPTER

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 JSA update packages, 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 | 87

JSA Log Files | 87

Common Ports and Servers Used by JSA | 88

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 | 87

Common Ports and Servers Used by JSA | 88

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 | 88

Troubleshooting Resources | 87

Common Ports and Servers Used by JSA

IN THIS SECTION

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.

NOTE: If you change any common ports, your JSA deployment might break.

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 by 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.

NOTE: If you change any common ports, your JSA deployment might break.

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).
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 and random generated port	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).

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

Port	Description	Protocol	Direction	Requirement
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.

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

Port	Description	Protocol	Direction	Requirement
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.
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.

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

Port	Description	Protocol	Direction	Requirement
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.
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.

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

Port	Description	Protocol	Direction	Requirement
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.
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.
2376	Docker command port	TCP	Internal communications. This port is not available externally.	Used to manage JSA application framework resources.

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

Port	Description	Protocol	Direction	Requirement
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 Console to JSA App Host.	Used with an App Host. It allows the Console to deploy apps to an App Host and to manage those apps.
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.

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

Port	Description	Protocol	Direction	Requirement
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".

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

Port	Description	Protocol	Direction	Requirement
JSA Console only: 5791, 7700, 7777, 7778, 7779, 7780, 7781, 7782, 7783, 7787, 7788, 7790, 7791, 7792, 7793, 7794, 7795, 7799, 8989, and 8990. FIPS mode only: 7777, 7778, 7779, 7780, 7781, 7782, 7783, 7788, 7790, 7791, 7792, 7793, 7795,	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
7799, and 8989				
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.

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

Port	Description	Protocol	Direction	Requirement
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.
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.

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

Port	Description	Protocol	Direction	Requirement
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 information from the host that is running the JSA Vulnerability Manager processor. **NOTE**: The JSA Vulnerability Manager scanner is end of life (EOL) in 7.5.0 Update Package 6, and is no longer supported in any version of JSA. In JSA 7.5.0 Update Package 6 and later, you can continue to use third-party scanners with your JSA Vulnerability Manager platform, but you cannot scan within your DMZ.
JSA Console only: 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.
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.

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

Port	Description	Protocol	Direction	Requirement
9381	localca-server	TCP	Bidirectional between JSA components.	Used to hold JSA local root and intermediate certificates, as well as associated CRLs.
9393, 9394	vault-qrd	TCP	Internal communications. Not available externally.	Used to hold secrets and allow secure access to them to services.
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.

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

Port	Description	Protocol	Direction	Requirement
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. **NOTE**: The JSA Vulnerability Manager scanner is end of life (EOL) in 7.5.0 Update Package 6, and is no longer supported in any version of JSA. In JSA 7.5.0 Update Package 6 and later, you can continue to use third-party scanners with your JSA Vulnerability Manager platform, but you cannot scan within your DMZ.
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.

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

Port	Description	Protocol	Direction	Requirement
10101, 10102	Heartbeat command	TCP	Bidirectional traffic between the primary and secondary HA nodes.	Required to ensure that the HA nodes are still active.
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
14433	traefik	TCP	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.
15432				Required to be open for internal communication between JSA Risk Manager and JSA.

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

Port	Description	Protocol	Direction	Requirement
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. **NOTE**: The JSA Vulnerability Manager scanner is end of life (EOL) in 7.5.0 Update Package 6, and is no longer supported in any version of JSA. In JSA 7.5.0 Update Package 6 and later, you can continue to use third-party scanners with your JSA Vulnerability Manager platform, but you cannot scan within your DMZ.
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.

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

Port	Description	Protocol	Direction	Requirement
23111	SOAP web server	TCP		SOAP web server port for the Event Collection Service (ECS).
23333	Emulex Fibre Channel	TCP	User desktop systems that connect to JSA appliances with a Fibre Channel card.	Emulex Fibre Channel HBAnywhere Remote Management service (elxmgmt).
26000	traefik	TCP	Bidirectional between JSA components.	Used with an App Host that is encrypted. Required for app services discovery.
26001	Conman	TCP	Unidirectional from the JSA Console to a JSA App Host.	Used with an App Host that is encrypted. It allows the Console to deploy apps to an App Host and to manage those apps.
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.
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.

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

Port	Description	Protocol	Direction	Requirement
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.

Table 22 on page 110 lists descriptions for the IP addresses or hostnames that JSA accesses.

Public Servers

Table 22: Public Servers That JSA Must Access

IP address or hostname	Description
194.153.113.31	JSA Vulnerability Manager DMZ scanner **NOTE**: The JSA Vulnerability Manager scanner is end of life (EOL) in 7.5.0 Update Package 6, and is no longer supported in any version of JSA. In JSA 7.5.0 Update Package 6 and later, you can continue to use third-party scanners with your JSA Vulnerability Manager platform, but you cannot scan within your DMZ.
194.153.113.32	JSA Vulnerability Manager DMZ scanner **NOTE**: The JSA Vulnerability Manager scanner is end of life (EOL) in 7.5.0 Update Package 6, and is no longer supported in any version of JSA. In JSA 7.5.0 Update Package 6 and later, you can continue to use third-party scanners with your JSA Vulnerability Manager platform, but you cannot scan within your DMZ.
download.juniper.net	JSA auto-update servers.
update.xforce-security.com	X-Force Threat Feed update server
license.xforce-security.com	X-Force Threat Feed licensing server

RELATED DOCUMENTATION

Troubleshooting Resources | 87

JSA Log Files | 87