

DAY ONE: JSA UP AND RUNNING



Administrators interested in SIEM solutions now have a single set of instructions on how to quickly install, deploy, and configure the Juniper Secure Analytics virtual and physical devices.

By Rethish Vijayakumaran Pillai, Sahithya Asula,
and Sushma Sethuram

DAY ONE: JSA UP AND RUNNING

JSA is a robust Security Information and Event Management (SIEM) solution and one of the best SIEM solutions available. JSA collects, processes, and stores millions of events and flow records from a vast array of vendor devices in near real-time. It then analyzes that information along with latest threat feeds and provides the most relevant and actionable intelligence in real time.

Now there's a one-stop resource to get JSA up and running: *Day One: JSA Up and Running*. The book covers JSA's many capabilities, its hardware and software components, deployment options, and several sections on using the JSA web user interface. Step-by-step instructions allows you to install various JSA appliances that suit their networks, apply licenses, manage data backups, and get your network secure.

"This Day One book provides a comprehensive guide to installing and deploy JSA in your environment as well as excellent step-by-step guidance on how to maintain and troubleshoot your JSA installation. By reading this book you'll be able to provide comprehensive security visibility to detecting and mitigating threats in your network."

Clay Haynes, Sr. Network Engineer, JNCIE-SEC #69, JNCIE-ENT #492

"In today's networks a SIEM is an essential part in event monitoring and analysis. Especially with a larger number of devices and events it is impossible for an operator to correlate all the monitoring and logging data. Juniper Secure Analytics (JSA) is not only a SIEM that collects data but it also helps operators get real insight into what is actually happening in their networks. This very well written book will not only get you up and running but also provides tips and tricks and real-life configuration examples."

Melchior Aelmans, Lead Engineer Cloud Providers, Juniper Networks

IT'S DAY ONE AND YOU HAVE A JOB TO DO, SO LEARN HOW TO:

- Install and configure Juniper Secure Analytics (JSA) hardware appliances
- Install and configure virtual JSA (vJSA) appliances
- Understand basic JSA functions and components
- Understand various JSA hardware models
- Understand JSA software versions
- Understand JSA licensing
- Configure High Availability (HA)
- Understand JSA standalone deployment
- Understand JSA distributed deployment



Juniper Networks Books are focused on network reliability and efficiency. Peruse the complete library at www.juniper.net/books.

JUNIPER
NETWORKS

Day One: JSA Up and Running

by Rethish Vijayakumaran Pillai, Sahithya Asula,
and Sushma Sethuram

Chapter 1: Introduction to JSA. 10

Chapter 2: JSA Software Installation Use Cases 41

Chapter 3: JSA Software Configuration and Troubleshooting Use Case 215

Chapter 4: JSA Hardware Use Cases. 276

Appendices 290



© 2020 by Juniper Networks, Inc. All rights reserved.

Juniper Networks and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo and the Junos logo, are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Published by Juniper Networks Books

Authors: Rethish Vijayakumaran Pillai, Sahithya Asula, Sushma Sethuram

Technical Reviewers: Amitha Kini, Pravin Lokhande, Shailesh Kanyadi

Editor in Chief: Patrick Ames

Copyeditor: Nancy Koerbel

Printed in the USA by Vervante Corporation.

Version History: v1, September, 2020

2 3 4 5 6 7 8 9 10

Comments, errata: dayone@juniper.net

About the Authors

Rethish Vijayakumaran Pillai is an Advanced TAC Engineer at Juniper Networks with over 17 years of experience in Network Security Domain. He is currently a part of Juniper Advanced TAC, providing technical support for Juniper Secure Analytics, SDN, SD-WAN, and Cloud products. Rethish holds a Bachelor of Engineering in Electronics and Communications and has extensive experience in supporting Juniper Network Management products and solutions. With a deep interest in network security, he started his career as a Firewall Administrator and followed his passion to become a network troubleshooter. This is his first Day One, but in his many years of work as a Technical Support Engineer, he's seen how important the Day One series is for newbies.

Sahithya Asula is an Information Development Engineer at Juniper Networks with over 10 years of experience in writing and developing documentation for networking and telecommunications. She contributes to product documentation for JSA, Policy Enforcer, and other network management products. Sahithya holds a Bachelor of Engineering in Information Technology and a Masters Degree in English. She started her career as a software development engineer and then followed her passion to become a Technical Writer.

Sushma Sethuram is an Information Development Engineer at Juniper Networks with over 10 years of experience in writing and developing documentation for networking and telecommunications. She contributes to product documentation for cloud services and network management products. Sushma holds a Bachelor of Engineering in Telecommunication. She started her career as a software development engineer, worked as a Technical Marketing Engineer, and then transitioned to become a Technical Writer.

Authors' Acknowledgments

Writing this JSA *Day One* book as a team has been an exciting and learning experience. The book needed several iterations of cohesive collaboration with cross-functional teams, all of whom added so much value to the effort. Authoring this JSA *Day One* book was volunteer work along with our day jobs, but we are motivated by how the book is helping JSA customers ramp-up quickly.

We would like to thank Patrick Ames and Nancy Koerbel for guidance on writing for the *Day One* series. We would also like to thank the technical reviewers and JTAC for their time and effort in reviewing the content and providing insightful feedback, and getting us going in the right direction. And special thanks to our managers Amitha Kini, Fawn Damitio, Shailesh Kanyadi, and Anand Nair for this wonderful opportunity; their vision, support, and encouragement made this book happen.

Welcome to Day One

This book is part of the *Day One* library, produced and published by Juniper Networks Books. *Day One* books cover the Junos OS and Juniper Networks network-administration with straightforward explanations, step-by-step instructions, and practical examples that are easy to follow.

- Download a free PDF edition at <http://www.juniper.net/dayone>
- PDF books are available on the Juniper app: [Junos Genius](#)
- Purchase the paper edition at Vervante Corporation (www.vervante.com).

What You Need to Know Before Reading This Book

- Basic knowledge of network security, Linux, IT infrastructure, TCP/IP, and virtualization concepts

After Reading This Book You'll Be Able To:

- Install and configure Juniper Secure Analytics (JSA) hardware appliances
- Install and configure virtual JSA (vJSA) appliances
- Understand basic JSA functions and components
- Understand various JSA hardware models
- Understand JSA software versions
- Understand JSA licensing
- Configure High Availability (HA)
- Understand JSA standalone deployment
- Understand JSA distributed deployment

JSA Resources in the Juniper TechLibrary

JSA Software Resources	
<i>Juniper Secure Analytics Getting Started Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-getting-started-guide/information-products/pathway-pages/pathway-page-m-container-qradar-gs.html
<i>Juniper Secure Analytics Installation Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-installation-guide/information-products/pathway-pages/pathway-page-m-container-install.html
<i>Juniper Secure Analytics What's New Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-whats-new-guide/information-products/pathway-pages/pathway-page-m-container-whats-new-guide.html
<i>Juniper Secure Analytics Users Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-users-guide/information-products/pathway-pages/pathway-page-m-container-user-siem.html
<i>Juniper Secure Analytics Administration Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-administration-guide/information-products/pathway-pages/pathway-page-m-container-admin-siem.html
<i>Juniper Secure Analytics Architecture and Deployment Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-arch-deployment-guide/information-products/pathway-pages/pathway-page-m-container-qradar-deployment-guide.html
<i>Juniper Secure Analytics Configuring DSMs Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-configuring-dsm/information-products/pathway-pages/pathway-page-m-dsm-guide-container.html
<i>Juniper Secure Analytics Risk Manager Getting Started Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-risk-manager-getting-started-guide/information-products/pathway-pages/pathway-page-m-container-qrm-gs.html
<i>Migrating Log Manager to Juniper Secure Analytics</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-la-migration/information-products/pathway-pages/pathway-page-m-container-qlm-migration.html
<i>Upgrading Juniper Secure Analytics to 7.4.0</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-upgrade-guide/information-products/pathway-pages/pathway-page-m-container-upgrade.html
<i>Juniper Secure Analytics Application Configuration Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-configuring-applications/information-products/pathway-pages/pathway-page-m-container-defappcfg.html

<i>Juniper Secure Analytics Ariel Query Language (AQL) Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-ariel-query-language-guide/information-products/pathway-pages/pathway-page-m-container-aql-guide.html
<i>Juniper Secure Analytics Configuring Offboard Storage Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-configuring-offboard-storage/information-products/pathway-pages/pathway-page-m-container-offboard.html
<i>Custom Event Properties for IBM Z/OS</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/information-products/pathway-pages/jsa-custom-properties-content-extension.html
<i>Juniper Secure Analytics High Availability Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-high-availability-guide/information-products/pathway-pages/pathway-page-m-container-ha-guide.html
<i>Juniper Secure Analytics Tuning Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-tuning-guide/information-products/pathway-pages/pathway-page-m-container-tuning-guide.html
<i>Juniper Secure Analytics Log Event Extended Format Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-log-event-extended-format-guide/information-products/pathway-pages/pathway-page-m-leef-format-guide.html
<i>Log Source Management App Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-log-source-manager-app-guide/information-products/pathway-pages/pathway-page-m-container-qapps-lsm.html
<i>Juniper Secure Analytics Managing Juniper SRX PCAP Data</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/information-products/pathway-pages/jsa-managing-juniper-pcap-data.html
<i>Juniper Secure Analytics Managing Vulnerability Assessment Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-managing-vulnerability-guide/information-products/pathway-pages/pathway-page-m-container-vuln.html
<i>Mapping Packeteer Applications into JSA</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/information-products/topic-collections/jsa-mapping-packeteer.pdf
<i>Juniper Secure Analytics NSM Plug-In Users Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/information-products/pathway-pages/jsa-nsm-plug-in-guide.html
<i>Partition Splitting</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/information-products/topic-collections/jsa-partition-splitting.pdf
<i>Pulse App Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-pulse-app-guide/information-products/pathway-pages/pathway-page-m-container-qapps-pulsedashboard.html
<i>QRadar Assistant App Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-apps-guide/information-products/pathway-pages/pathway-page-m-assistant-app.html
<i>Juniper Secure Analytics Risk Manager Adapter Configuration Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-risk-manager-adapter-configuration-guide/information-products/pathway-pages/pathway-page-m-container-qrm-adp.html
<i>Juniper Secure Analytics Risk Manager Installation Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-risk-manager-installation-guide/information-products/pathway-pages/pathway-page-m-container-qrm-inst.html

<i>Juniper Secure Analytics Risk Manager Users Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-risk-manager-user-guide/information-products/pathway-pages/pathway-page-m-container-qrm-ug.html
<i>Security Director Application Guide for JSA and IBM QRadar</i>	https://www.juniper.net/documentation/en_US/junos-space19.4/information-products/pathway-pages/security-director-application-guide-for-jsa-and-ibm-qradar.pdf
<i>Juniper Secure Analytics Vulnerability Manager User Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-managing-vulnerability-user-guide/information-products/pathway-pages/pathway-page-m-container-qvm-ug.html
<i>Juniper Secure Analytics WinCollect User Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-wincollect-user-guide/information-products/pathway-pages/pathway-page-m-container-wincollect.html
<i>Juniper Secure Analytics Troubleshooting Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-troubleshooting-guide/information-products/pathway-pages/pathway-page-m-container-qradar-troubleshooting-guide.html
<i>Juniper Secure Analytics API Guide</i>	https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-api-guide/information-products/pathway-pages/pathway-page-m-container-restful-api.html

JSA HARDWARE RESOURCES

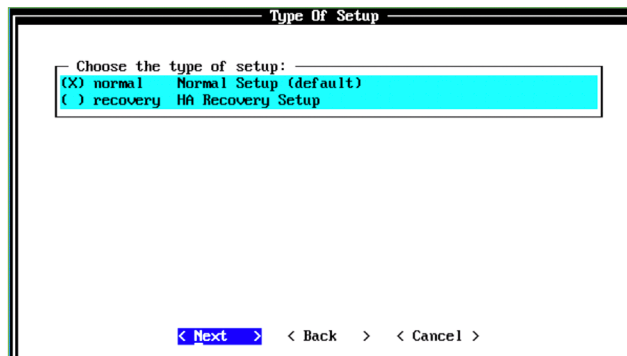
<i>Juniper Secure Analytics 7800 Hardware Guide</i>	https://www.juniper.net/documentation/en_US/release-independent/jsa/information-products/pathway-pages/hardware/jsa7800-hw-guide.html
<i>Juniper Secure Analytics 7800 Quick Start Guide</i>	https://www.juniper.net/documentation/en_US/release-independent/jsa/information-products/topic-collections/jsa-7800-how-to-set-up.pdf
<i>Juniper Secure Analytics 7500 Hardware Guide</i>	https://www.juniper.net/documentation/en_US/release-independent/jsa/information-products/pathway-pages/hardware/jsa-7500-index.html
<i>Juniper Secure Analytics 7500 Quick Start Guide</i>	https://www.juniper.net/documentation/en_US/release-independent/jsa/information-products/topic-collections/jsa-7500-quick-start-guide-new-template.pdf
<i>Juniper Secure Analytics 5800 Hardware Guide</i>	https://www.juniper.net/documentation/en_US/release-independent/jsa/information-products/pathway-pages/hardware/jsa5800-index.html
<i>Juniper Secure Analytics 5800 Quick Start Guide</i>	https://www.juniper.net/documentation/en_US/release-independent/jsa/information-products/topic-collections/jsa-5800-quick-start-guide.pdf
<i>Juniper Secure Analytics 3800 Hardware Guide</i>	https://www.juniper.net/documentation/en_US/release-independent/jsa/information-products/pathway-pages/hardware/jsa3800-index.html
<i>Juniper Secure Analytics 3800 Quick Start Guide</i>	https://www.juniper.net/documentation/en_US/release-independent/jsa/information-products/topic-collections/jsa-3800-quick-start-guide.pdf

How to Navigate the JSA Installation Wizard

The JSA installation wizard allows you to use certain keyboard keys to navigate through the installation options and setup.

Table P.1 JSA Navigation Keys

Keyboard Key	Function
Up	Move UP through the options on the screen.
Down	Move DOWN through the options on the screen.
Space	SELECT an option. When you press space, an X symbol appears beside the selected option.
Enter	Press ENTER to move to the next screen (after moving the cursor to the Next option) or cancel the installation (after moving the cursor to the Cancel option).
Tab	Use the Tab key to MOVE to the Next option.



Chapter 1

Introduction to JSA

This chapter gets you started with Juniper Secure Analytics (JSA). It includes an overview of the concepts of Security Information and Event Management (SIEM) solutions and how JSA incorporates these concepts. It also covers:

- What is JSA?
- Capabilities and functions of JSA
- Software and hardware versions of JSA
- Deployment options of JSA
- Components that make up a JSA installation
- JSA web user interface (UI)

Let's start by briefly introducing JSA.

What is Juniper Secure Analytics (JSA)?

JSA is a SIEM solution. At its core, JSA is a syslog server that can collect security information from almost any type of vendor devices across your network.

Is JSA just another syslog server?

Not at all, JSA is not merely a simple syslog server, it is one of the best SIEM solutions available. JSA collects, processes, and stores millions of events and flow records from a vast array of vendor devices in near real-time. It then analyzes that information along with latest threat feeds and provides the most relevant and actionable intelligence in real time.

What is Security Information and Event Management (SIEM)?

SIEM helps organizations detect and mitigate security threats to their networks with real-time monitoring of suspicious activity across the network.

Traditionally you can define SIEM as a software solution that centrally collects, stores, and analyzes data from various IT components (gateways, servers, firewalls, user workstations, and so on) across your network. By collecting the logs right from user workstations to the entire length and breadth of the organization's network, SIEM has access to entire events and can correlate what's happening on disparate systems to provide insights to security management. Without correlation, these distinct events on different devices can go unnoticed.

While the complete log collection can help address most compliance reporting requirements, parsing and normalization maps log messages from different systems into a common data model and enables analyzing related events, logged in different source formats. Correlation links log events from disparate systems or applications, which can speed the detection and reaction to security threats.

SIEM aggregation reduces the volume of event data by consolidating duplicate event records and reporting on the correlated, aggregated event data in real time, comparing it to long-term summaries. SIEM provides real-time reporting capabilities along with long-term storage and analysis of collected security data.

Why is JSA more than a Traditional SIEM?

Is JSA just another SIEM system? Not at all, JSA is much more than a traditional SIEM solution.

JSA not only collects security events and network flow records, it also provides capabilities such as advanced correlation engines, vulnerability management, and risk management capabilities, along with advanced reporting solutions. JSA has several built-in correlation rules and ready-to-use compliance reports.

Using its extensive API endpoints and extension management capabilities, you can integrate JSA with external devices to automate manual tasks. An example is JSA's integration with Juniper's firewall management solution, Security Director. With this integration, the IP addresses of an attacker caught by JSA can be blocked immediately on the firewalls managed by Security Director with a few clicks.

JSA's integration with X-Force allows X-Force threat intelligence data to be consumed by JSA correlation rules for advanced threat detection. Once enabled,

X-Force feeds are updated multiple times per day with new data. With new IP information provided every two minutes and URL data every five minutes, JSA stays ahead of latest security threats by proactively monitoring the presence of malware hosts, spam sources, and anonymous proxies.

You can scale JSA from a single all-in-one system to a distributed deployment with several hundreds of managed hosts. At scale, a single JSA distributed collector can handle up to around 40,000 events per second or up to 1.2 million flows per minute.

You can install apps (from IBM Security App Exchange) on JSA. Apps can enhance the JSA user interface to deliver new security intelligence capabilities or extend the current functions by providing new tabs, API methods, dashboard items, menus, toolbar buttons, and configuration pages.

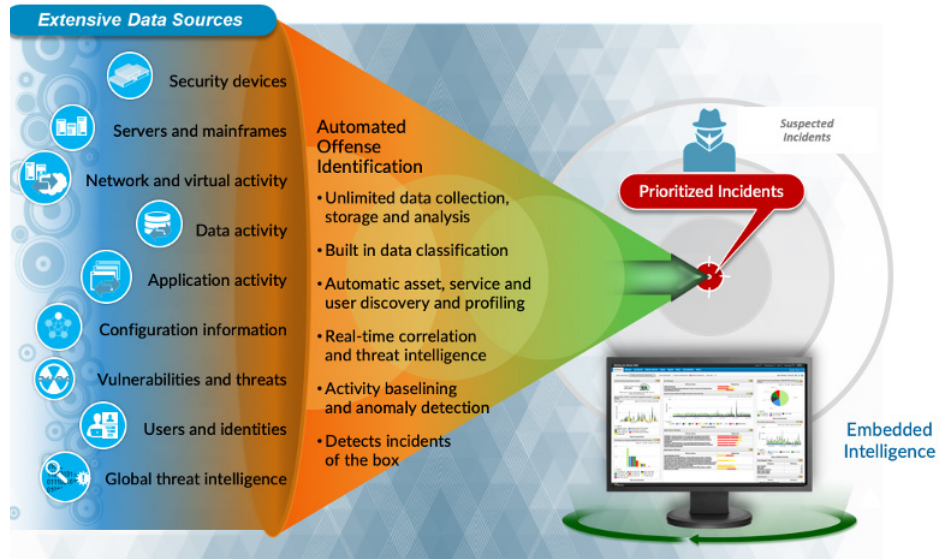
This integrated approach of JSA enables your organization to quickly and easily implement a security management program that delivers security best practices.

JSA combines, analyzes, and manages an unparalleled set of surveillance data – network behavior, security events, vulnerability profiles, and threat information – to empower your network management and analytics.

- **Log Analytics:** JSA provides scalable log analytics by enabling distributed log collection across an organization with a centralized view of the information.
- **Threat Analytics:** JSA provides an advanced network security management solution bridging the gap between network and security operations delivering real-time surveillance and complex IT-based threat detection.
- **Compliance Management:** JSA brings to enterprises, institutions, and agencies the accountability, transparency, and measurability that are critical factors to the success of any IT security program that is required to meet regulatory mandates.
- **Vulnerability Management:** JSA can function as a full-featured vulnerability scanner when deployed as a standalone solution or working in conjunction with Threat Analytics.
- **Risk Management:** JSA helps you stay ahead of advanced threats by proactively quantifying risks from vulnerabilities, configuration errors, and anomalous network activity, preventing attacks that target high value assets and data.

NOTE Threat manager, threat analytics, and log manager, log analytics are terms used interchangeably in this guide.

Figure 1 JSA in a Nutshell



Commonly Used Terms in JSA

There are a few key JSA terms you need to know:

- **Events and Flows:** The core functions of JSA are to manage network security by monitoring events and flows.
- **Events:** An event is typically a log of a specific action, such as a user login or a firewall policy permit or deny action, that occurs at a specific time and the event is logged at that time. JSA accepts these event logs from log sources that are on your network by using protocols such as syslog, SNMP, and so on. JSA can also set up outbound connections to retrieve events by using protocols such as SCP, SFTP, FTP, JDBC, Check Point OPSEC, and SMB/CIFS.
- **Events per second (EPS):** The rate at which events are sent to JSA are measured using EPS. For example, if an SRX Series device is sending 100 events per second to JSA, the EPS value is 100. We recommend that you keep the EPS capacity in mind, while choosing a JSA model. JSA license is based on the EPS. For more information on EPS information for JSA devices, see Table 9 JSA Hardware Information in Chapter 4.
- **Flows:** A flow is a record of network activity that can last for seconds, minutes, hours, or days, depending on the activity within a session. The flow is a record of network activity between two hosts. Flows represent network

activity by normalizing IP addresses, ports, byte and packet counts, and other data, into flow records, which effectively are records of network sessions between two hosts. For example, a Telnet or FTP session that lasts a few minutes or hours.

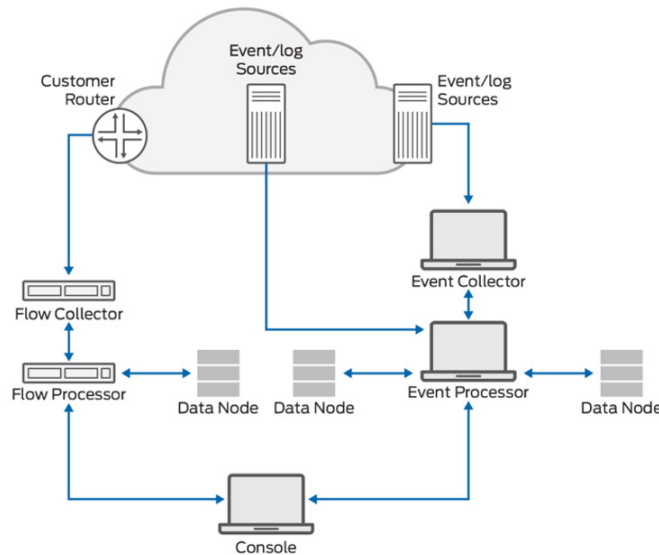
- *Flow source*: A flow source is a data source such as a firewall, router, or switch that creates network flow records. JSA can collect JFlows, NetFlows, and SFlows. JSA supports unlimited number of flow sources.
- *Flows per Minute (FPM)*: The rate at which flows are sent to JSA are measured using FPM. JSA is licensed based on FPM. For more information on FPM information for JSA devices, see Table 9 JSA Hardware Information in Chapter 4.
- *Log Sources*: A log source is a data source such as a firewall or intrusion protection system (IPS) that creates an event log. Any network device (like routers, switches), or servers (DNS /DHCP/AD), or any user workstations are examples. JSA supports an unlimited number of log sources. JSA supports several third-party vendors as log sources such as Microsoft Windows, Oracle, Checkpoint, and Cisco, just to name a few.
- *Offenses*: JSA uses rules to monitor the events and flows in your network to detect security threats. When the events and flows meet the pre-defined rule conditions that are defined in the rules, an offense is created to show that a security attack or policy breach is suspected.

JSA Components

Now that you've had an overview of JSA and its functions, let's learn about the JSA components. Figure 2 illustrates a typical JSA deployment that shows the key components listed here:

- Console
- Event Collector and Event Processor
- Flow Collector and Flow Processor
- Vulnerability Manager (Optional)
- Risk Manager (Optional)
- Data Nodes (Optional)
- App Host (Optional)
- Vulnerability Processor (Optional)
- Vulnerability Scanner (Optional)
- High Availability hosts (Optional)

Figure 2 JSA Components



Console

The console is a pivotal component and hosts the JSA web UI. Using the console, you can view real-time and historical events, flows, graphs, dashboards, reports, offenses, asset information, vulnerabilities, and risks. You can also perform administrative functions.

In a standalone deployment, all JSA components, including console, reside on a single host. In distributed JSA deployments, the JSA console is also used to manage hosts that include other components. Tomcat service (a web server) runs on the console and you can have only one console per deployment. Distributed deployments support multiple JSA devices with different components installed on them, *however there can be only a single console per deployment*.

If a console goes down, the JSA Web UI will not be available. In such a scenario, use the CLI to log in to JSA. In a distributed deployment, even if the console is not up, the events and flows will still be collected by the Event Processor (EP) or Flow Processor (FP). However, you will not be able to log in to JSA Web UI.

For fault tolerance, you can configure high availability for the console. The high availability deployments support a primary console and a secondary console in the active-passive mode.

For more information on JSA deployment models, see JSA Deployment Models later in this chapter.

The console has a magistrate component, which performs the following functions:

- **Offense rules:** Monitors and acts on offenses such as generating email notifications.
- **Offense management:** Updates active offenses, changes status of offenses, and provides user access to offense information from the Offenses tab.
- **Offense storage:** Writes offense data to a Postgres database.

The Magistrate Processing Core (MPC) in the magistrate component is responsible for correlating offenses with event notifications from multiple event processor components.

The main services running on a console are tomcat, accumulator, qvmscanner, qvmprocessor, hostservices, hostcontext, imq, postgresql, ariel_proxy_server, arc_builder, ecs-ep, ecs-ec, ecs-ec-ingress, qflow, vis, assetprofiler, docker, and reporting_executor. See Appendix D for more information.

Here are some common license Stock Keeping Units (SKUs) for console all-in-one (AIO) deployment:

- JSA-LMAIO AIO for hardware
- VJSA-LMAIO AIO for virtual appliance
- JSA-TMAIO AIO for hardware
- VJSA-TMAIO AIO for virtual appliance

And here are some common license SKUs for distributed deployment:

- JSA-LMCON Console for hardware
- VJSA-LMCON Console for virtual appliance
- JSA-TMCON Console for hardware
- VJSA-TMCON Console for virtual appliance

For the complete list of licenses, contact the Juniper Support team (<https://support.juniper.net/support/>).

Event Collector and Event Processor

To view and process events on the JSA console, you must first collect events from the log sources. The event collector collects events from log sources and the event processor processes the collected events.

JSA can collect events by using a dedicated event collector or processor appliance, or by using an AIO appliance. On an AIO appliance, the event collection service and event processing service run on the same device.

Event Collector

The event collector performs the following functions:

- Collects data from log source protocols such as syslog, Java Database Connectivity (JDBC), Operations Security (OPSEC), log file, and Simple Network Management Protocol (SNMP).
- Monitors the number of incoming events to the system to manage the input queues and Events Per Second (EPS) licensing.
- Parses and normalizes the fields of the raw event from the source device into a usable format.
- Applies the parsed and normalized event data to the possible Device Support Modules (DSMs) that support automatic discovery. Events are parsed and then coalesced based on common attributes across events.
- Applies routing rules for the system to forward data to offsite targets, external syslog systems, JavaScript Object Notation (JSON) systems, and other SIEMs.

When the event collector receives the events from log sources such as firewalls, the events are placed into input queues for processing. The queue sizes vary based on the protocol or method. The events are parsed and normalized using these queues. JSA recognizes known log sources using the source IP address or host names in the header. In the normalization process, the raw data is converted into IP addresses, so that JSA can recognize the data.

The event collector parses and coalesces events from known log sources into records. Events from new or unknown log sources that were not detected in the past are redirected to the traffic analysis (auto-detection) engine. When JSA discovers new log sources, a configuration request message to add the log source is sent to the JSA console.

Event Processor

The event processor performs the following functions:

- Custom Rules Engine (CRE): The event processor includes the custom rule engine. The CRE processes events received by JSA and compares them against defined rules, keeps track of systems involved in incidents over time, and generates notifications to users. When the events match a rule, a notification is sent from the event processor to the MPC on the JSA console, that a specific event has triggered a rule. MPC then creates and manages offenses. When rules are triggered, responses or actions such as notifications, syslog, SNMP, email messages, new events, and offenses are generated by the MPC.

- **Event storage (Ariel):** The Ariel database stores events and flows collected by JSA. It is a time-series database for events and flows; data is stored on a minute-by-minute basis. In an AIO deployment, events and flows are stored on the same device. In the distributed deployment with console and event or flow processors, data is stored on event processors and flow processors. The data nodes act as an extended storage for event processors and flow processors.

Table 1 Event Storage for Different Data Types

Type	Event Storage
Raw event data	/store/ariel/events/payloads
Parsed event data	/store/ariel/events/records
Raw flow data	/store/ariel/flows/payloads
Parsed flow data	/store/ariel/flows/records

The events and flows are stored in a `/<Year>/<month>/<day>/<hour>` format. For example, `/store/ariel/events/records/2020/4/5`.

Figure 3 shows the sample data stored in the Ariel database.

Figure 3 Sample Data Stored in Ariel Database

```
[root@TM-jsa 5]# pwd
/store/ariel/events/payloads/2020/4/5
[root@TM-jsa 5]# ls
0 1 10 11 12 13 14 15 16 17 18 19 2 20 21 22 23 3 4 5 6 7 8 9
[root@TM-jsa 5]# cd /store/ariel/events/records/2020/4/5
[root@TM-jsa 5]# ls
0 1 10 11 12 13 14 15 16 17 18 19 2 20 21 22 23 3 4 5 6 7 8 9
[root@TM-jsa 5]# cd /store/ariel/flows/records/2020/4/5
[root@TM-jsa 5]# ls
0 1 10 11 12 13 14 15 16 17 18 19 2 20 21 22 23 3 4 5 6 7 8 9
[root@TM-jsa 5]# cd /store/ariel/flows/payloads/2020/4/5
[root@TM-jsa 5]# ls
0 1 10 11 12 13 14 15 16 17 18 19 2 20 21 22 23 3 4 5 6 7 8 9
```

- **Streaming:** Sends real-time event data to the JSA console when a user is viewing events from the Log Activity tab with the real-time (streaming) option. Streamed events are not provided from the Ariel database. Historical events are pulled from the Ariel database.

The event collector sends normalized event data to the event processor where the events are processed by the CRE. If events are matched to the CRE custom rules that are predefined on the JSA console, the event processor executes the action defined for the rule response.

The main services running on EP are accumulator, qvmscanner, hostservices, hostcontext, imq, postgresql, ariel_query_server, arc_builder, ecs-ep, ecs-ec, ecs-ec-ingress, and vis.

The main services running on EC and SFEC are hostservices, hostcontext, imq, postgresql, ecs-ec, ecs-ec-ingress, and vis. See Appendix D for more information.

Here are common license SKUs for EP distributed deployment:

- JSA-LMEP Event Processor (EP) for hardware
- VJSA-LMEP Event Processor (EP) for virtual appliance
- JSA-TMEP Event Processor (EP) for hardware
- VJSA-TMEP Event Processor (EP) for virtual appliance

Flow Collector and Flow Processor

To view and use the flow data on the JSA console, flows must be first collected from the flow sources and then processed. The flow collector collects flows from the flow sources and then the flow processor processes the collected flows. JSA can collect flows by using a dedicated flow collector or flow processor appliance, or by using an AIO appliance. *Qflow* is the JSA component that collects and creates flow information.

The JSA flow collector does not capture a full packet. For the network sessions that span multiple time intervals (minutes), the flow pipeline reports a record at the end of each minute. The record includes current data for metrics such as bytes and packets. You might see multiple records (per minute) in JSA with the same First Packet Time, but the Last Packet Time values increment through time.

A flow starts when the flow collector detects the first packet that has a unique source IP address, destination IP address, source port, destination port, and other specific protocol options, including 802.1q VLAN fields. Each new packet is evaluated. The bytes and packets counts are added to the statistical counters in the flow record. At the end of an interval, a status record of the flow is sent to a flow processor and statistical counters for the flow are reset. A flow ends when no activity for the flow is detected within the configured time.

The flow collector generates flow data from raw packets collected from the monitor ports such as the Switched Port Analyzer (SPANs), the Test Access Point (TAPs), and from monitor sessions or from the external flow sources such as net-flow, sampled flow (sflow), and jflow. This data is then converted to JSA flow format and sent to the flow processor for processing.

The flow processor performs the following functions:

- **Flow deduplication:** Removes duplicate flows when multiple flow collectors provide data to the flow processors appliances.
- **Asymmetric recombination:** Combines two sides of each flow when data is provided asymmetrically. This process can recognize flows from each side and combine them into one record.
- **License throttling:** Monitors the number of incoming flows to manage input queues and licensing.
- **Forwarding:** Applies routing rules such as sending flow data to offsite targets, external Syslog systems, JSON systems, and other SIEMs.

The flow data passes through the CRE and it is correlated against the configured rules. An offense can be generated based on this correlation.

The main services running on FP are accumulator, hostservices, hostcontext, imq, postgresql, ariel_query_server, ecs-ep, ecs-ec, ecs-ec-ingress, qflow, and vis. See Appendix D for more information.

Here are some common license SKUs for FP distributed deployment:

- JSA-TMFP Flow Processor (FP) for hardware
- VJSA-TMFP Flow Processor (FP) for virtual appliance

Vulnerability Manager

The JSA Vulnerability Manager (VM) provides the following capabilities and specifications:

- Makes JSA a vulnerability scanner.
- Allows third-party vulnerability scanners (such as Qualys, Rapid 7, and tenable) reports to be correlated with other data collected by JSA
- Allows you to install the VM as an add-on to the console or as a standalone node.
- Allows you to install the VM either on a JSA virtual machine or on a hardware appliance.
- With a VM license, allows the console to act as a Vulnerability Processor (VP) and Vulnerability Scanner (VS) by default. Also, any of the JSA components (EP, EC, FP, etc.) can act as a VS.
- Allows you to install the VM as an add-on to the console for small deployments with less than 5K assets, you can install the VM as an add-on to the console. In this case, vulnerability scans can be initiated from the console or from managed hosts.

- Allows you to use the VM on either log analytics or threat analytics.
- If you need to scan 50k assets, we recommend installing VM as a standalone node. In such scenarios, install a VP separately and add it to the deployment. If needed, install a dedicated VS to initiate scans.
- If you are installing the VM on an existing appliance such as a console, use the JSA-ADVM and VJSA-ADVM license SKUs.
- If you are installing VM as a dedicated appliance, use the JSA-VM, VJSA-VM license SKUs.

You must license the assets. An asset is a device, server, or a workstation you want to scan for vulnerabilities. Licensing is based on the number of assets that you want to scan from JSA.

High availability is not required for the VM.

Risk Manager is included with a VM license. When you buy a VM, you will get the risk managers included for fifty sources. However, to add more source devices, you must buy the risk manager sources separately.

Here are some common license SKUs for VM:

- JSA-VM Standalone deployment hardware
- VJSA-VM Standalone deployment virtual appliance
- JSA-ADVM Add-on deployment hardware
- VJSA-ADVM Add-on deployment virtual appliance

Risk Manager

The JSA Risk Manager (RM) is a separately installed appliance to monitor device configurations, simulate changes to your network environment, and prioritize risks and vulnerabilities in your network.

The JSA Risk Manager evaluates the parameters that you define in your question and returns assets in your network to help you assess risk. The questions are based on a series of tests that can be combined and configured as required.

The JSA Risk Manager component provides the following capabilities:

- Risk assessment
- Comparison of firewall configurations
- Network activity monitoring
- Policy monitoring for compliance (for example, firewall rules that are shadowed, redundant, causing compliance issues, and so on.)

- Modelling and simulation of attacks and network configuration changes (what-if scenarios)
- Advanced tools to investigate network topologies and traffic.

The main services running on RM are `hostservices`, `hostcontext`, `imq`, `postgresql`, `ariel_query_server`, `postgresql-rm`, and `ziptie-server`. See Appendix D for more information.

Here are some common license SKUs for RM:

- JSA-RMAD5KSRC (5000 sources)
- JSA-RMAD1KSRC (1000 sources)

Note the following:

- JSA RM must be installed on a dedicated appliance.
- JSA RM supports both the virtual machine and physical appliance.
- You must license the sources. A source is a device on which you want to use RM, such as a firewall, switch, router, and so on.
- RM feature is not available with Log Analytics.

Data Nodes

A data node (DN) is an appliance that you can add to your event and flow processors to increase the storage capacity and improve search performance. You can add an unlimited number of data nodes to your JSA deployment. You can add data nodes at any time.

Data nodes enable new and existing JSA deployments to add storage and processing capacity on demand, as required. You can add data nodes to TA AIO or LA AIO or dedicated event processors and flow processors to increase their storage capacity. You can add any number of data nodes to the same EP or FP. However, you cannot attach the same DN to multiple EPs or FPs. Once a data node is attached, data rebalancing happens between the data node and the host to which it is attached. Data nodes support high availability.

The main services running on a DN appliance are `dataNode`, `accumulator`, `hostservices`, `hostcontext`, `imq`, `postgresql`, and `ariel_query_server`. See Appendix D for more information. Here are some common license SKUs for data node:

- JSA-DN
- vJSA-DNHA
- vJSA-DN
- JSA-DNHA

App Nodes

Apps create or add new functions in JSA by providing new tabs, API methods, dashboard items, menus, toolbar buttons, configuration pages, and so on within the JSA Web UI. When an app is installed on JSA, it is installed on the console and will consume console resources. This is not ideal for large deployments and when there is a possibility for a resource crunch on the console. An app host 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 currently available on the console. You can have only one app host in your deployment.

Here is an App Node license SKU:

- S-JSA-S-P-APPHOST

Vulnerability Processor

JSA can act as a vulnerability processor when you apply a vulnerability manager license to it. The vulnerability processor (VP) is responsible for processing vulnerabilities. There can be only one VP in a deployment. By default, the console will act as a VP and a vulnerability scanner (VS) when there is a vulnerability manager license applied. However, when you need to scan many hosts (for example 50K assets), we recommend using a dedicated VP.

The main services running on a VP appliance are `qvmprocessor`, `hostservices`, `host-context`, `vis imq`, and `postgresql`. See Appendix D for more information.

Vulnerability Scanner

JSA can act as a vulnerability scanner when you apply a vulnerability manager license to it. The vulnerability scanner appliance is a dedicated appliance that scans the target servers (assets). VS can be a hardware or virtual appliance. Any device such as an AIO-console, event processor, SFEC, FP, or RM can act as a VS. However, it may not be feasible to trigger a vulnerability assessment scan from any part of the network for security reasons. You might, therefore, need to add dedicated VS appliances. DMZ is a typical example. A dedicated scanner appliance is placed at the DMZ to scan DMZ servers.

The main services running on a VS appliance are `qvmscanner`, `hostservices`, `host-context`, `vis imq`, and `postgresql`. See Appendix D for more information.

High Availability Hosts

If your hardware or network fails, JSA can continue to collect, store, and process event and flow data by using high availability (HA) appliances. To enable HA, JSA connects a primary HA host with a secondary HA host to create an HA cluster. You can use HA on hardware or virtual appliances. Both primary and secondary HA devices must be the same model and with the same CPU, RAM, and storage resources. The HA console host provides HA for threat analytics or log analytics and the HA non-console host provides high-availability for managed hosts such as flow processor, event processor, SFEC, and so on.

To configure HA you must have an extra IP address. Once you add an HA host (secondary host) to the existing host (primary host), the original IP address of the primary host becomes the virtual IP address for HA, then assign the extra IP address to the primary host.

The main services for high-availability are drbd and ha_manager. See Appendix D for more information.

Here are some common license SKUs for HA:

- vJSA-DNHA
- JSA-DNHA
- JSA-TMAIOHA

JSA Software and Hardware

JSA is available as two options: as a virtual appliance or as a hardware appliance with JSA software pre-installed on it. JSA offers the following hardware models:

- JSA3800 - https://www.juniper.net/documentation/product/en_US/jsa3800
- JSA5800 - https://www.juniper.net/documentation/product/en_US/jsa5800
- JSA7500 - https://www.juniper.net/documentation/product/en_US/jsa7500
- JSA7800 - https://www.juniper.net/documentation/product/en_US/jsa7800

The following JSA software versions are available on both JSA hardware and on JSA virtual appliances:

- JSA 7.3.0 - https://www.juniper.net/documentation/product/en_US/juniper-secure-analytics/7.3.0

- JSA 7.3.1 - https://www.juniper.net/documentation/product/en_US/juniper-secure-analytics/7.3.1
- JSA 7.3.2 - https://www.juniper.net/documentation/product/en_US/juniper-secure-analytics/7.3.2
- JSA 7.3.3 - https://www.juniper.net/documentation/product/en_US/juniper-secure-analytics/7.3.3
- JSA 7.4.0 - https://www.juniper.net/documentation/product/en_US/juniper-secure-analytics/7.4.0

NOTE The JSA software versions mentioned in this section pertain to the releases provided by JSA at the time this book was published. JSA provides newer releases at a regular cadence. See the link for information on the most up-to-date software versions: https://www.juniper.net/documentation/product/en_US/juniper-secure-analytics.

Install and Deploy JSA

Now that you understand how JSA functions, let's get to work and learn how to install and deploy it.

JSA Installation Options

You can install JSA with the following configurations:

- You can deploy (install) JSA on a virtual machine (ESXi / KVM).
- You can buy a JSA hardware appliance pre-installed with JSA software.
- You can access JSA on the cloud via AWS or Azure.
- You can install JSA data nodes on your own hardware. (This is supported only for data nodes installation, from JSA Release 7.3.2 onwards). In this case, first install RHEL on the hardware that you want to install the JSA data node on, and then install JSA software and configure it as a data node. No other roles are supported on this type of installation.

NOTE This book covers JSA installations using ESXi and JSA hardware appliances.

Okay, those are the various JSA installation options, so let's cover the various ways in which you can deploy JSA.

JSA Deployment Models

Before you deploy JSA, consider the following questions:

- Do you need all JSA features or only limited features?
- Do you want to collect only events?
- Do you want to collect events and flows?

A JSA deployment offers the following options that you can choose from:

- *Threat Analytics (TA)* - This option provides all JSA features. It is also called offense management, and it permits you to investigate offenses, behaviors, anomalies, targets, and attackers on your network. TA has the full SIEM capability.
 - TA can collect both events and flows.
- *Log Analytics (LA)* - This option provides basic log collecting and reporting capabilities offered by JSA.
 - LA can collect only events.

Table 2 lists the features available for TA and LA.

Table 2 Supported Features by TA and LA

Capability	JSA TA	JSA LA
Full administrative capabilities	Yes	Yes
Customizable dashboards	Yes	Yes
Custom rules engine	Yes	Yes
Manage network and security events	Yes	Yes
Manage host and application logs	Yes	Yes
Threshold-based alerts	Yes	Yes
Compliance templates	Yes	Yes
Data archiving	Yes	Yes
IBM Security X-Force® Threat Intelligence IP reputation feed integration	Yes	Yes

WinCollect stand-alone deployments	Yes	Yes
WinCollect managed deployments	Yes	Yes
Network activity monitoring (Flows)	Yes	No
Asset profiling	Yes	No
Offenses management	Yes	No
JSA Vulnerability Manager integration	Yes	Yes
JSA Risk Manager integration	Yes	No
Vulnerability assessment scanners	Yes	Yes

Once you decide the JSA deployment type (LA or TA), you must select the scale of deployment. This depends on the following factors:

- Do you want to install JSA on a single device or multiple devices?
- How many branch locations do you have?
- Is there necessary bandwidth available to send events over a WAN link or VPN link?
- Do you have to comply with GDPR or any local government data protection laws?
- How many log sources do you want to collect logs from (Total EPS)?
- How many flow sources do you want to collect flows from (Total FPM)?
- Do you want to collect events from devices that do not have connectivity all the time?
- How long must the events and flows be stored?

Whether TA or LA, you can either deploy on a single device where all services and functions are on a single device installation or deploy on multiple devices where the installation is distributed across multiple devices. For scalability, we recommend you deploy JSA in a distributed model.

JSA architecture supports deployments of varying sizes and topologies, ranging from an all-in-one, or standalone (single host) deployment, to distributed deployment with multiple devices. In distributed deployment, the appliances such as event collectors, flow collectors, data nodes, event processors, and flow processors have specific roles.

Table 3 JSA Deployment Models

All-In-One	Distributed
Event collection, flow collection event processing, flow processing, correlation, analysis, and reporting are embedded within JSA.	Multiple devices to support various tasks such as one device acting as a console, another device as an event processor and another device as a flow processor.
All core functions are available within the system and it is easy for users to deploy and manage in minutes.	JSA can scale to large distributed deployments that can support up to 5 million events per second.
JSA architecture provides a streamlined solution for secure and efficient log analytics.	JSA can be easily deployed in large distributed environments. When there are multiple branches in different geographical locations, distributed deployment helps in conserving the WAN bandwidth and data can be stored locally in branch locations.
Acts as a console and processor in one dedicated device. HA is supported to provide redundancy and fault tolerance.	HA is supported to provide redundancy and fault tolerance.
This is recommended for small environments such as mid-size companies where growth is not anticipated.	Distributed deployments are scalable and are recommended for big-size companies and ISPs, keeping future expansions and scaling in mind. Also, distributed deployment is needed when you have to comply with data regulations (such as, data cannot be moved to another geographical area).

JSA User Interface

After you have installed JSA, you can access the JSA software application using the JSA web UI. This section talks about what the JSA software application looks like and what capabilities it offers. We'll also go over some basic JSA functions along the way.

The JSA console hosts the web UI. You can access the JSA web UI on https port 443. (<https://<JSA-IP-Address>>). If JSA is behind a firewall, make sure that TCP port 443 is allowed from your workstations.

Use the information provided in Table 4 to log in to your JSA console.

Table 4 JSA Login Information

Login Information	Default Value
URL	https://<IP Address>, where <IP Address> is the IP address of the JSA console. To log in to JSA in an IPv6, wrap the IP address in square brackets: https://[<IP Address>]
Username	admin
Password	The password that is assigned to JSA during the installation process.

NOTE The default license key provides you access to the system for five weeks.

The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them before the default license expires. For more information on applying a license to JSA, see the section *Apply a License to JSA*, later in *Chapter 3: JSA Software Configuration and Troubleshooting Use Cases*.

Figure 4 shows the first screen that appears when you access the JSA URL.

Figure 4 JSA Login Page



The default username to log in is `admin`. The admin user has administrative access. The admin password is set while installing JSA.

As an admin user, you can perform administrative tasks such as creating new user accounts after the installation is complete. These new user accounts can be *locally* authenticated (password to be defined in JSA) or can be *remotely* authenticated (JSA to be integrated with Terminal Access Controller Access Control System (TACACS) / Lightweight Directory Access Protocol (LDAP) / Active Directory (AD), and so on).

NOTE You can only use the admin user account from the JSA web UI. Use the root user account for CLI access. The root user has administrative access and the password for this user account is set while installing JSA.

For all the features in JSA to function properly, you must use a supported web browser. Table 5 lists the supported versions of web browsers for JSA.

Table 5 Supported Web Browser Versions for JSA

Web Browser	Supported Versions
4-bit Mozilla Firefox	60 Extended Support Release and later
64-bit Microsoft Edge	38.14393 and later
Microsoft Internet Explorer	11.06
64-bit Google Chrome	Latest

JSA features are organized by tabs in the JSA web UI and the Dashboard tab is displayed first when you log in, so let's take a tour.

Dashboard

The Dashboard tab is a workspace environment that provides summary and detailed information on the events occurring in your network. The Dashboard provides various widgets that allow you to view information about network security, activity, or data that JSA collects.

Figure 5, Figure 6, and Figure 7 show the JSA dashboard.

As shown in Figure 5, you can create new dashboards and share these customized dashboards with other users.

While there are several other predefined widgets that are readily available for use in the Dashboard, Table 6 lists only a few of them as examples and provides more information on those predefined widgets.

Figure 5 JSA Dashboard

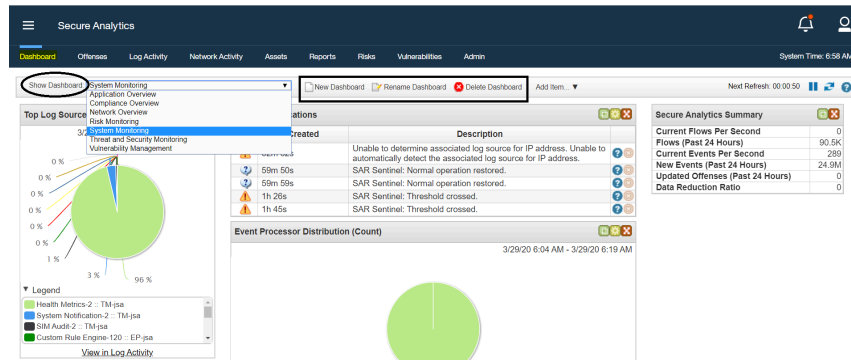


Table 6 Sample JSA Dashboard Widgets

Dashboard Widgets	Description
Most Recent Offenses	The five most recent offenses are identified with a magnitude bar that indicates the importance of the offense. Point to the offense name to view detailed information for the IP address.
Most Severe Offenses	The five most severe offenses are identified with a magnitude bar that indicates the importance of the offense. Point to the offense name to view detailed information for the IP address.
My Offenses	The My Offenses widget displays five of the most recent offenses that are assigned to you. The offenses are identified with a magnitude bar that indicates the importance of the offense. Point to the IP address to view detailed information for the IP address.
Top Sources	The Top Sources widget displays the top offense sources. Each source is identified with a magnitude bar that indicates the importance of the source. Point to the IP address to view detailed information for the IP address.
Top Local Destinations	The Top Local Destinations widget displays the top local destinations. Each destination is identified with a magnitude bar that indicates the importance of the destination. Point to the IP address to view detailed information for the IP.
Categories	The Top Categories Types widget displays the top five categories that are associated with the highest number of offenses.

Figure 6 Web UI for JSA Threat Analytics

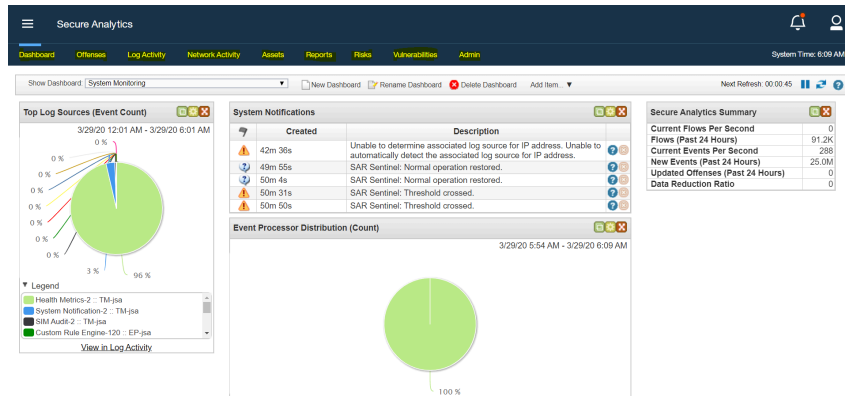
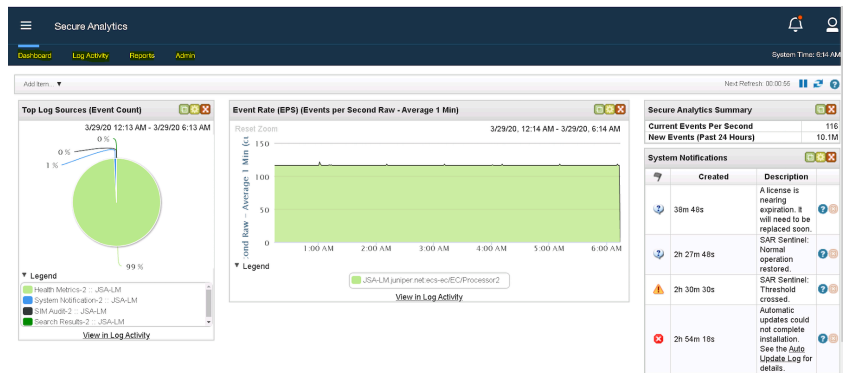
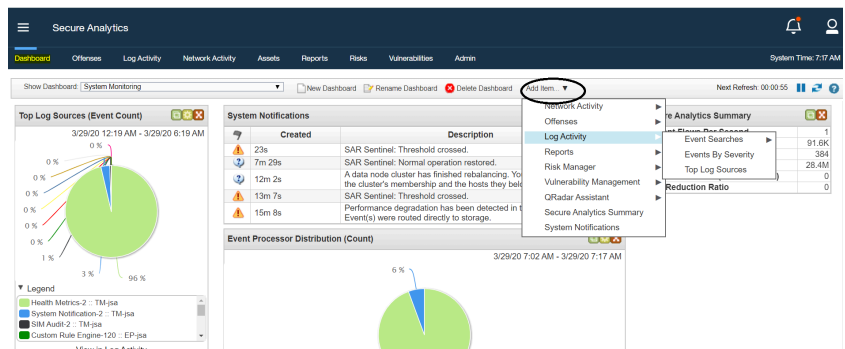


Figure 7 Web UI for JSA Log Analytics



Notice the difference in tabs between the Threat Analytics and Log Analytics windows. You can customize the existing dashboard by creating widgets for the information that you want to view, as shown in Figure 8.

Figure 8 Customize Dashboard Widgets



Offenses Tab

To detect security threats JSA uses rules to monitor events and flows in your network. When an event or a flow meets the defined test criteria in a rule, an offense is created to show that a security attack or policy breach is suspected. You can investigate these offenses to determine the root cause of a network issue.

Use the Offenses tab (see Figure 9) to view any offenses that occur on your network and then:

- Investigate offenses, source and destination IP addresses, and network behaviors.
- Correlate events and flows that are sourced from multiple networks to the same destination IP address.
- Go to the various pages of the Offenses tab to investigate event and flow details.
- Determine the unique events that caused an offense.

Figure 9

Offense Tab

Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources	Events	Flows	Start Date
CREATE Source IP	192.168.1.1	37	192.168.1.1	192.168.1.2	N/A	Multiple (2)	66	0	Mar 29, 2020, 10:42:37
CREATE Destination IP	192.168.1.2	37	192.168.1.1	192.168.1.2	N/A	Juniper JunOS Plat...	40	0	Mar 29, 2020, 10:42:37

Figure 10 shows how JSA lists those offenses with the events that triggered them.

Figure 10

Offense Tab: Events Associated with Offenses

	Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
RT_FLOW_SESSION_CREATE	RT_FLOW_SESSION_CREATE	Juniper JunOS Platform @ 1...	37	Mar 29, 2020, 10:42:37	Session Opened	192.168.1.1	56040	192.168.1.2	23	N/A	37
RT_FLOW_SESSION_CREATE	RT_FLOW_SESSION_CREATE	Juniper JunOS Platform @ 1...	1	Mar 29, 2020, 10:42:37	Session Opened	192.168.1.1	56040	192.168.1.2	23	N/A	37
RT_FLOW_SESSION_CREATE	RT_FLOW_SESSION_CREATE	Juniper JunOS Platform @ 1...	1	Mar 29, 2020, 10:42:37	Session Opened	192.168.1.1	56040	192.168.1.2	23	N/A	37

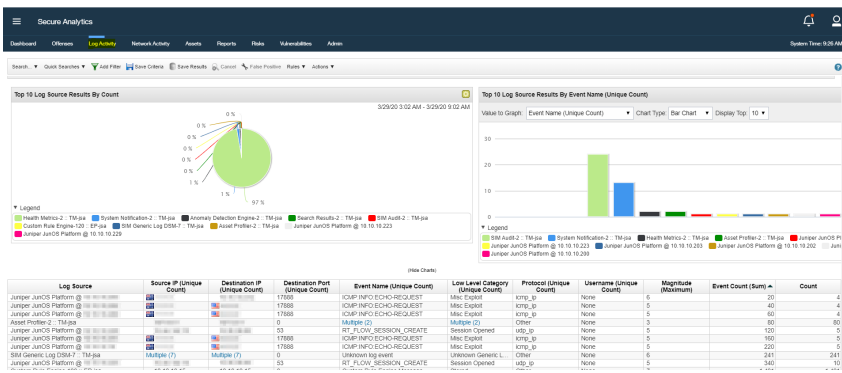
Log Activity Tab

In JSA, you can monitor and display network events in real time or perform advanced searches. The Log Activity tab (see Figure 11) displays event information as records from a log source, such as a firewall or router device. Use the Log Activity tab to:

- Investigate event data
- Investigate event logs that are sent to JSA in real time
- Search event
- Monitor log activity by using configurable time-series charts
- Identify false positives to tune JSA.

Figure 11

Log Activity Tab



Network Activity Tab

Use the Network Activity tab to visually monitor and investigate flow data in real-time or conduct advanced searches to filter displayed flows.

A *flow* is a communication session between two hosts. You can view flow information to determine how the traffic is communicated and what was communicated. Flow information can also include details on protocols, autonomous system number (ASN) values, or Interface Index (IFIndex) values.

By default, the Network Activity tab (see Figure 12) displays flows in the streaming mode. If you have previously configured a saved search as a default, the results of that search are automatically displayed when you access the Network Activity tab.

There's more to the Network Activity tab, of course, such as the ability to:

- Monitor network activity using configurable time-series charts.
- Investigate flows sent to JSA in real time.
- Search network flows.

Figure 12

Network Activity Tab

Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Application	Source Bytes	Destination Bytes	Source Packets	Destination Packets	ICMP Type/Code	Flow Source	Flow Inter
<input type="checkbox"/>	Mar 29, 2...	10.10...	54540	10.10...	443	tcp_ip	Web.SecureWeb	1,024	425	7	4	N/A	TM-isa	TM-js
<input type="checkbox"/>	Mar 29, 2...	10.10...	58050	10.10...	443	tcp_ip	Web.SecureWeb	1,650	3,160	11	9	N/A	TM-isa	TM-js
<input type="checkbox"/>	Mar 29, 2...	10.10...	58058	10.10...	443	tcp_ip	Web.SecureWeb	1,358	4,403	9	7	N/A	TM-isa	TM-js
<input type="checkbox"/>	Mar 29, 2...	10.10...	42196	10.10...	443	tcp_ip	Web.SecureWeb	1,822	3,276	13	11	N/A	TM-isa	TM-js
<input type="checkbox"/>	Mar 29, 2...	10.10...	44191	10.10...	514	tcp_ip	Misc.Syslog	12,124 (C)	2,940	42	42	N/A	TM-isa	TM-js
<input type="checkbox"/>	Mar 29, 2...	10.10...	42252	10.10...	443	tcp_ip	Web.SecureWeb	1,822	3,276	13	11	N/A	TM-isa	TM-js
<input type="checkbox"/>	Mar 29, 2...	10.10...	40288	10.10...	32006	tcp_ip	InnerSystem.Flowgen	58	70	1	1	N/A	TM-isa	TM-js
<input type="checkbox"/>	Mar 29, 2...	10.10...	42338	10.10...	443	tcp_ip	Web.SecureWeb	2,406	3,278	13	11	N/A	TM-isa	TM-js
<input type="checkbox"/>	Mar 29, 2...	10.10...	41040	10.10...	514	udp_ip	Misc.Syslog	5,729 (C)	0	34	0	N/A	TM-isa	TM-js
<input type="checkbox"/>	Mar 29, 2...	10.10...	54530	10.10...	443	tcp_ip	Web.SecureWeb	12,442	96,627	38	48	N/A	TM-isa	TM-js
<input type="checkbox"/>	Mar 29, 2...	10.10...	54552	10.10...	443	tcp_ip	Web.SecureWeb	46,811	137,002	117	96	N/A	TM-isa	TM-js
<input type="checkbox"/>	Mar 29, 2...	10.10...	40208	10.10...	32006	tcp_ip	InnerSystem.Flowgen	58	70	1	1	N/A	TM-isa	TM-js

Receiving an average of less than one result per second.

Assets Tab

JSA automatically discovers assets, servers, and hosts that are operating on your network. Automatic discovery is based on passive flow data and vulnerability data, the combination allowing JSA to build an asset profile. Asset profiles provide information about each known asset in the network, including identity information, if available, and what services are running on each asset. This profile data is used for correlation purposes to help reduce false positives.

For example, an attacker tries to use a specific service that is running on an asset. In this situation, JSA can determine whether the asset is vulnerable to the attack by correlating the attack to the asset profile.

You can use the Assets tab to perform the following tasks as shown in Figure 13:

- Search for assets
- View all learned assets
- View identity information for learned assets
- Tune false positive vulnerabilities

Figure 13

Assets Tab

Id	IP Address	Asset Name	Operating System	Aggregated CVSS	Vulnerabilities	Services	Last User	User Last Seen
1001	192.168.1.101	192.168.1.101		0.0	0	2		
1002	192.168.1.102	192.168.1.102		0.0	0	7		
1003	192.168.1.103	192.168.1.103		0.0	0	0		
1004	192.168.1.104	192.168.1.104		0.0	0	0		
1005	192.168.1.105	192.168.1.105		0.0	0	3		
1006	192.168.1.106	192.168.1.106		0.0	0	1		
1007	192.168.1.107	192.168.1.107		0.0	0	0		
1008	192.168.1.108	192.168.1.108		0.0	0	0		

Displaying 1 to 8 of 8 items (Elapsed time: 0:00:00.321)

Reports Tab

The Reports tab allows you to create, distribute, and manage reports for the data managed by JSA. You can create custom reports or use pre-installed report templates.

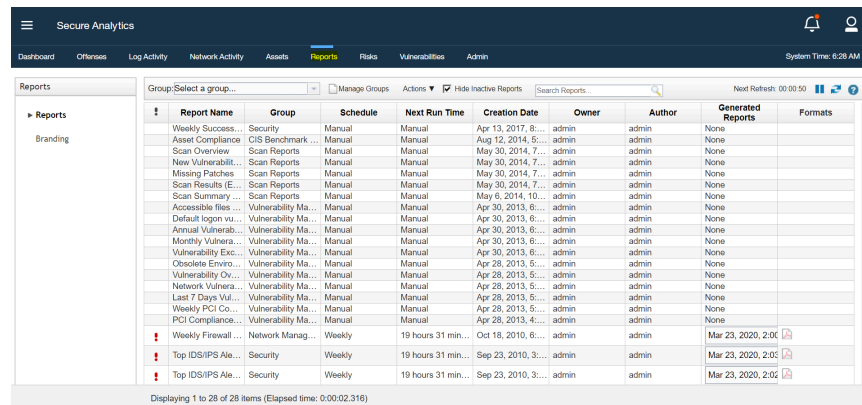
Create a report based on the information you require, such as security or network data. You can also combine different information into a single report, and even brand your reports with customized logos.

Use the Reports tab to perform the following tasks as shown in Figure 14:

- Create, distribute, and manage reports for JSA data
- Create customized reports for operational and executive use
- Combine security and network information into a single report
- Use or edit preinstalled report templates
- Brand your reports with customized logos
- Set a schedule to generate both custom and default reports
- Publish reports in various formats

Figure 14

Reports Tab



Report Name	Group	Schedule	Next Run Time	Creation Date	Owner	Author	Generated Reports	Formats
Weekly Success...	Security	Manual	Manual	Apr 13, 2017, 8...	admin	admin	None	
Asset Compliance	CIS Benchmark ...	Manual	Manual	Aug 12, 2014, 5...	admin	admin	None	
Scan Overview	Scan Reports	Manual	Manual	May 30, 2014, 7...	admin	admin	None	
New Vulnerabil...	Scan Reports	Manual	Manual	May 30, 2014, 7...	admin	admin	None	
Missing Patches	Scan Reports	Manual	Manual	May 30, 2014, 7...	admin	admin	None	
Scan Results (E...	Scan Reports	Manual	Manual	May 30, 2014, 7...	admin	admin	None	
Scan Summary ...	Scan Reports	Manual	Manual	May 6, 2014, 10...	admin	admin	None	
Accessible files	Vulnerability Ma...	Manual	Manual	Apr 30, 2013, 6...	admin	admin	None	
Default logon vu...	Vulnerability Ma...	Manual	Manual	Apr 30, 2013, 6...	admin	admin	None	
Annual Vulnerab...	Vulnerability Ma...	Manual	Manual	Apr 30, 2013, 6...	admin	admin	None	
Monthly Vulnera...	Vulnerability Ma...	Manual	Manual	Apr 30, 2013, 6...	admin	admin	None	
Vulnerability Exc...	Vulnerability Ma...	Manual	Manual	Apr 30, 2013, 6...	admin	admin	None	
Obsolete Enviro...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 5...	admin	admin	None	
Vulnerability Dr...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 5...	admin	admin	None	
Network Vulnera...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 5...	admin	admin	None	
Last 7 Days Vul...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 5...	admin	admin	None	
Weekly PCI Co...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 5...	admin	admin	None	
PCI Compliance...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 4...	admin	admin	None	
Weekly Firewall ...	Network Manag...	Weekly	19 hours 31 min...	Oct 18, 2010, 6...	admin	admin	Mar 23, 2020, 2:0...	
Top IDS/IPS Ale...	Security	Weekly	19 hours 31 min...	Sep 23, 2010, 3...	admin	admin	Mar 23, 2020, 2:0...	
Top IDS/IPS Ale...	Security	Weekly	19 hours 31 min...	Sep 23, 2010, 3...	admin	admin	Mar 23, 2020, 2:0...	

Displaying 1 to 28 of 28 items (Elapsed time: 0:00:02.316)

Risks Tab

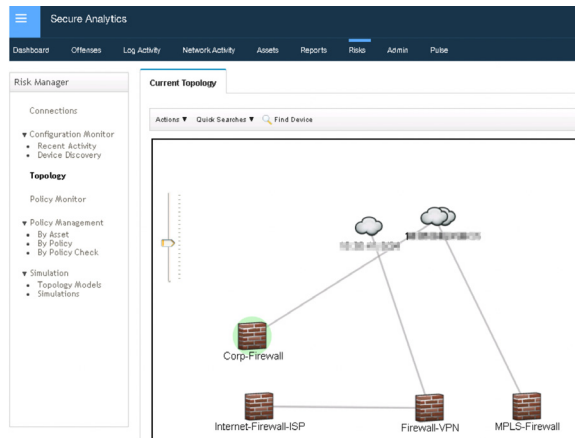
JSA *Risk Manager* is a separately installed appliance that you can use to monitor device configurations, simulate changes to your network environment, and prioritize risks and vulnerabilities in your network.

JSA Risk Manager uses the configuration data from network and security devices, such as firewalls, routers, switches, or IPs, vulnerability feeds, and vendor security sources. This data is used to identify security, policy, and compliance risks within your network security infrastructure and the probability of those risks being exploited.

You can access the JSA Risk Manager by using the Risks tab (Figure 15). JSA Risk Manager provides network topology, active attack paths, and high-risk assets risk-score adjustments on assets based on policy compliance.

NOTE JSA Vulnerability Manager and Risk Manager are combined into one offering and both are enabled through a single base license.

Figure 15 Risks Tab



MORE? For more information, see the Juniper Secure Analytics Risk Manager User Guide at https://www.juniper.net/documentation/en_US/jsa7.3.1/jsa-risk-manager-user-guide/information-products/pathway-pages/pathway-page-m-container-qrm-ug.html.

Vulnerabilities Tab

JSA can function as a full-featured vulnerability scanner. JSA Vulnerability Manager discovers vulnerabilities on your network devices, applications and software adds context to the vulnerabilities, prioritizes asset risk in your network, and supports the remediation of discovered vulnerabilities.

You can access the JSA Vulnerability Manager using the Vulnerabilities tab (see Figure 16). The vulnerability management dashboard items are displayed when you purchase JSA Vulnerability Manager with a valid license. If you install JSA Threat Analytics, the Vulnerabilities tab is enabled by default with a temporary license key. If you install the JSA Log Analytics, the Vulnerabilities tab is *not* enabled. You can purchase the license for JSA Vulnerability Manager separately and enable it by using a license key.

MORE? For more information, see the Juniper Secure Analytics Vulnerability Manager User Guide at https://www.juniper.net/documentation/en_US/jsa7.3.1/jsa-risk-manager-user-guide/information-products/pathway-pages/pathway-page-m-container-qrm-ug.html.

Figure 16

Vulnerabilities Tab

The screenshot shows the JSA Vulnerabilities tab interface. The top navigation bar includes tabs for Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risk, Vulnerabilities (selected), and Admin. The system time is 6:20 AM. The left sidebar shows a tree view with categories like My Assigned Vulnerabilities, Manage Vulnerabilities (By Network, By Asset, By Vulnerability, By Open Service), Scan Results, Vulnerability Exception, Vulnerability Assignment, Research, Administrative (Scan Profiles, Scan Exclusions, Scan Policies, Scheduled Scans, Operational Window, Scanners), and Scanners.

The main content area displays a table of Scan Policies. The table has columns for Name, Description, Enabled, Share With Everyone, and Scan Type. The data is as follows:

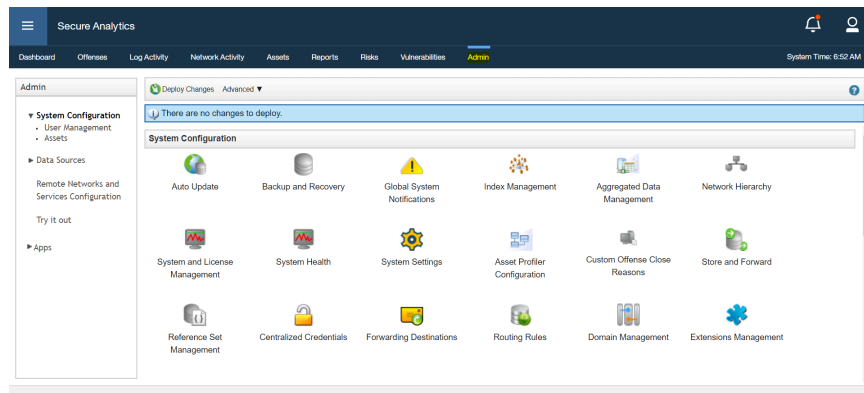
Name	Description	Enabled	Share With Everyone	Scan Type
Web Scan	Scans ports 80, 81, 443, 8080, and 8081 to identify web applications and tests for cross site scripting, sql injection, weak web server settings and vulnerable CGI scripts. Web application scanning is performed on assets where a web application is identified.	●	●	Zero credentialled
PCI Scan	This scan performs a scan required for PCI compliance. This scan performs a Full scan except that it ensures the entire TCP/IP port range (0-65535) is scanned.	●	●	Full scan
Patch Scan	Scouts the network to discover assets then performs a fast port scan and credential scan of the assets.	●	●	Patch scan
Full Scan	Discovers network assets using a fast scan port range. Perform a user configurable port scan and unauthenticated scan of discovered	●	●	Full scan

Admin Tab

As a JSA administrator, you have a variety of tools available to help you configure and manage your JSA deployment on the Admin tab, and you can perform any of the following (see Figure 17):

- Deploy and manage JSA hosts and licenses
- Configure user accounts and authentication
- Build a network hierarchy
- Configure domains and set up a multi-tenant environment
- Define and manage log and flow data sources
- Manage JSA data retention
- Manage assets and reference data
- Schedule regular backups of JSA configuration and data
- Monitor the system health of managed hosts

Figure 17 Admin Tab



More? For more information on the JSA User Interface, see the *JSA Getting Started Guide* at https://www.juniper.net/documentation/en_US/jsa7.3.1/jsa-risk-manager-user-guide/information-products/pathway-pages/pathway-page-m-container-qrm-ug.html.

Chapter 2

JSA Software Installation Use Cases

Let's get hands on with JSA. This chapter provides several sample exercises for you to practice installing the various JSA appliances. After completion you'll be able to:

- Understand the prerequisites for installing JSA
- Create a JSA VM
- Install and configure appliance types
- Add the managed hosts
- Remove managed hosts

Step 1: Prerequisites to Install JSA

JSA appliances come with pre-installed JSA software so that you can directly configure the appliances. You can also install a different version of JSA software using a bootable USB, if required. For more information on that process, see the section, *Reinstall JSA Using Bootable USB*, later in this chapter.

NOTE To ensure proper communication between devices in distributed deployments and to access JSA, you must open the required ports. See Appendix C for more information.

For virtual installations, you must first prepare the VM and then install the JSA software. Ensure that you use a supported virtual appliance that meets the minimum system requirements (see Appendices A and B for more information on system requirements).

A virtual appliance is a JSA system that consists of JSA software installed on a VMWare ESXi or KVM virtual machine. A virtual appliance provides the same visibility and function in your virtual network infrastructure as that of other JSA appliances in your physical environment.

You can install JSA on your virtual appliance using either the software or appliance installation:

- **Software installation:** Uses a Red Hat Enterprise Linux (RHEL) operating system. You must configure partitions and comply with required RHEL specifications before installation. This is supported only for data nodes.
- **Appliance installation:** Uses a version of RHEL included in the JSA software ISO image; no other preparations are required. This is used when you want to install JSA on an ESXi virtual appliance or on any Juniper Networks provided hardware appliances. Here you can install any appliance type as required.

NOTE Juniper Networks provides hardware appliances with pre-installed JSA software, and therefore, Steps 1 and 2 are not be required in the case of hardware appliances.

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

1. Create a virtual machine.
2. Install JSA software on the virtual machine.
3. Configure the roles based on your needs such as, Threat Analytics (TA), Log Analytics (LA), High Availability (HA), or managed hosts.
4. If you are installing a TA or LA All-in-One (AIO or standalone installation), you can directly start using it.
5. If you are installing a managed host, add the appliance (managed host) to the deployment (TM console or LM console).
6. If you are installing a secondary HA host, add the appliance (HA host) to the primary.

NOTE We do not recommend that you install any extra third-party software other than JSA on the virtual machine or appliance. Third party software can take up disk space and interrupt JSA services when a disk space threshold is crossed. This can also cause issues during upgrades, and in general, create security vulnerabilities in the system.

You must also be sure that the virtual appliance complies to the following *minimum* requirements for JSA to work as expected:

- **Memory requirement:** To understand the minimum and suggested *memory* requirements for a virtual appliance, see the Appendix A.
- **Processor requirement:** To understand the minimum and suggested CPU requirements for a virtual appliance, see the Appendix B.
- **Storage requirement:** Virtual appliances must have a minimum of 256 GB storage. But for optimal performance, you need more than 256 GB storage. Use thin provisioning. Before you install your virtual appliance, use the following formula to determine your storage needs:

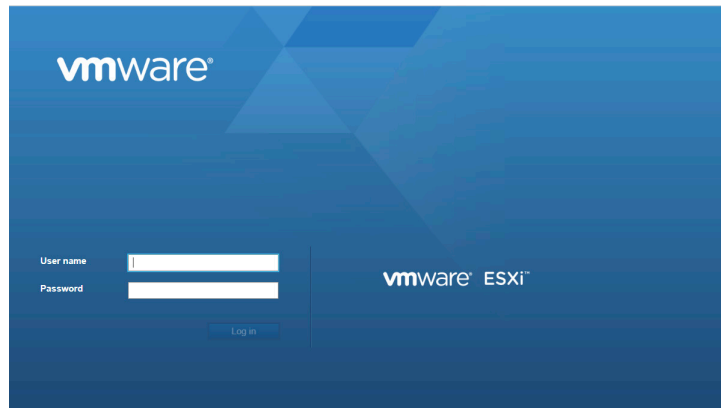
(Number of Days) x (Seconds in a day) x (Events per second rate) x (Average size of a log event x 1.5 JSA normalized event overhead) x 1.05 / (1000 x 1000 x 1000) + 40 GB. For example: 30 x 86,400 x 1,000 EPS x 600 bytes x 1.05 / (1000 x 1000 x 1000) + 40 GB = 1673 GB

Step 2: Create a JSA VM

To create a virtual machine, log in to VMWare ESXi as shown in Figure 18.

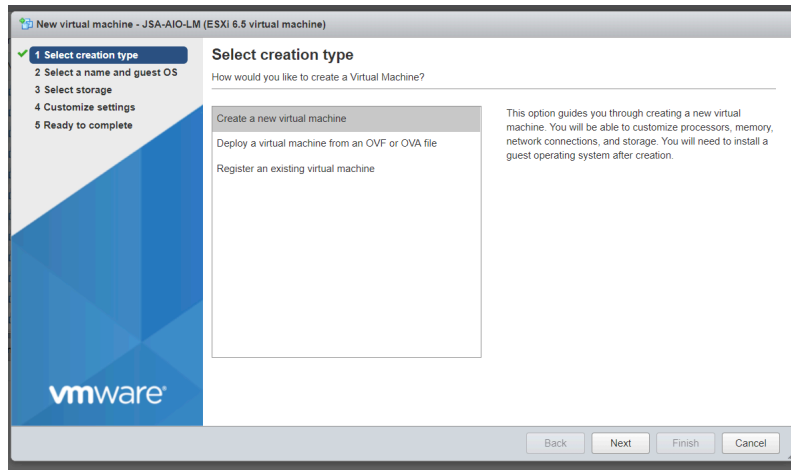
Figure 18

Login to VMWare ESXi



From the VMware vSphere Client, select Virtual Machines, right click and select Create/Register VM, and the New virtual machine page appears as shown in Figure 19.

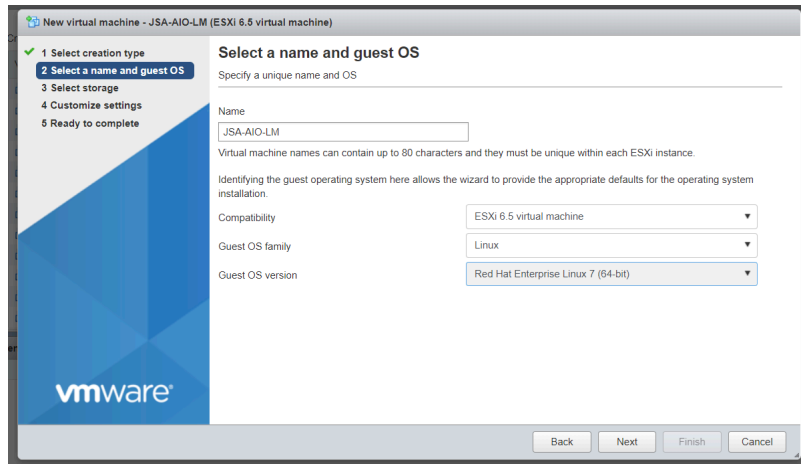
Figure 19 New Virtual Machine Page



You can see the Select creation type page. Now select *Create a new virtual machine* and click Next.

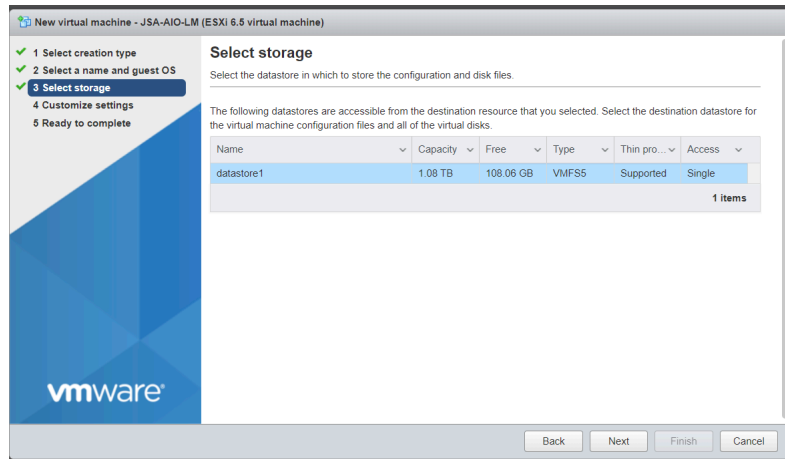
In the Select a name and guest OS page, select the Guest OS family as Linux and Guest OS version as Red Hat Enterprise Linux 7(64-bit), as shown in Figure 20. Click Next.

Figure 20 Select a Name and Guest OS



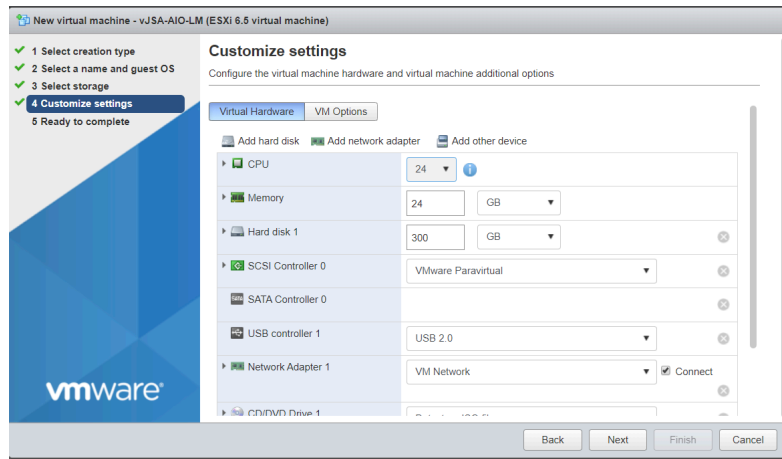
In the Select storage page, select the datastore in which to store the configuration and disk files, shown in Figure 21. Click Next.

Figure 21 Select Storage



In the Customize settings page, configure the CPU, RAM, and the storage that you want for the virtual machine, as shown in Figure 22. For more information about CPU and memory requirements, see Appendix A and Appendix B.

Figure 22 Customize Settings



Select an appropriate virtual network and the JSA ISO image to be installed, and select Next, as shown in Figures 22.

Review the selection, as shown in Figures 23 and 24.

Figure 23

Review Selection

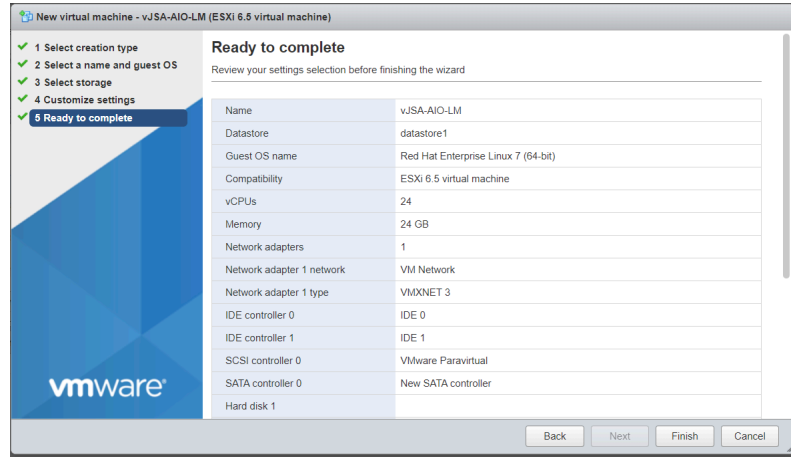
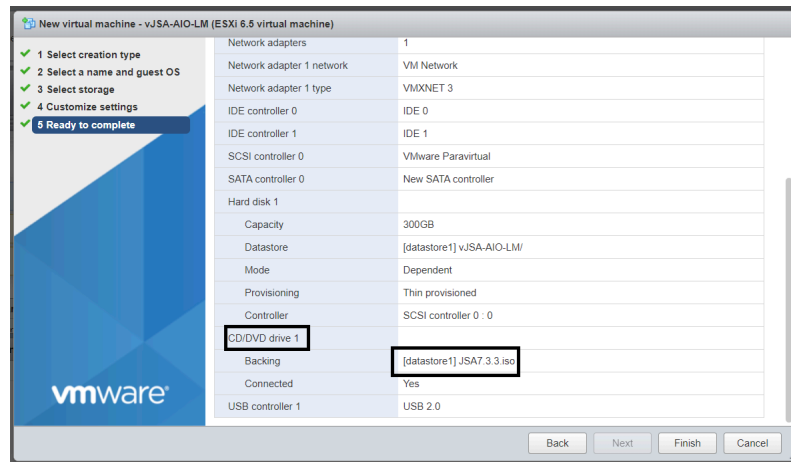


Figure 24

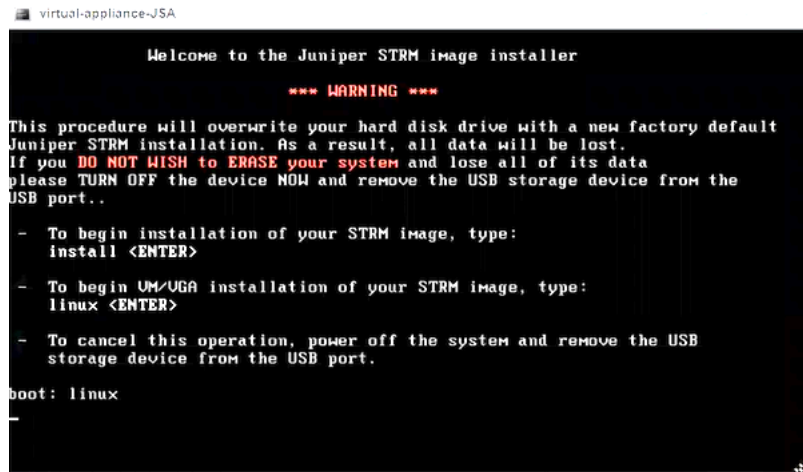
Review Selection



In the Ready to Complete page, review selection and click Finish to complete the process. Restart the virtual machine and the installation will begin, as shown in Figure 25. Type *linux* to continue and complete the installation.

Figure 25

VM Created: Completion



```

virtual-appliance-JSA

Welcome to the Juniper STRM image installer

*** WARNING ***

This procedure will overwrite your hard disk drive with a new factory default
Juniper STRM installation. As a result, all data will be lost.
If you DO NOT WISH to ERASE your system and lose all of its data
please TURN OFF the device NOW and remove the USB storage device from the
USB port..

- To begin installation of your STRM image, type:
  install <ENTER>

- To begin UM/UGA installation of your STRM image, type:
  linux <ENTER>

- To cancel this operation, power off the system and remove the USB
  storage device from the USB port.

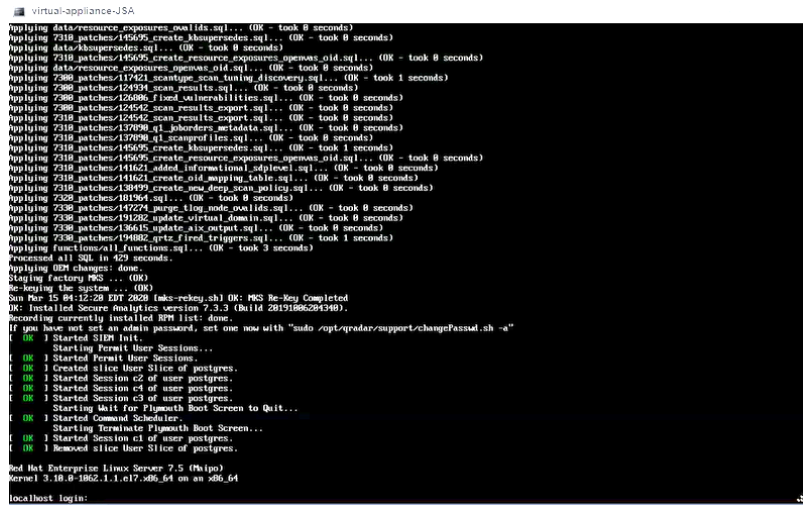
boot: linux

```

Once the installation is complete, a confirmation window appears similar to Figure 26.

Figure 26

Virtual Machine Created: Confirmation



```

virtual-appliance-JSA

Applying data-resource_exposures_gowlids.sql... (OK - took 0 seconds)
Applying 7318_patches/145695_create_khaspersedes.sql... (OK - took 0 seconds)
Applying data/khaspersedes.sql... (OK - took 0 seconds)
Applying 7318_patches/145695_create_resource_exposures_opemaw_old.sql... (OK - took 0 seconds)
Applying data-resource_exposures_opemaw_old.sql... (OK - took 0 seconds)
Applying 7300_patches/117421_scan_type_scan_tuning_discovery.sql... (OK - took 1 seconds)
Applying 7300_patches/124931_scan_results.sql... (OK - took 0 seconds)
Applying 7300_patches/126486_fixd_valuerabilities.sql... (OK - took 0 seconds)
Applying 7300_patches/124542_scan_results_export.sql... (OK - took 0 seconds)
Applying 7318_patches/124542_scan_results_export.sql... (OK - took 0 seconds)
Applying 7318_patches/137090_qi_johnders_metadata.sql... (OK - took 0 seconds)
Applying 7318_patches/137090_qi_scanprofile.sql... (OK - took 0 seconds)
Applying 7318_patches/145695_create_khaspersedes.sql... (OK - took 1 seconds)
Applying 7318_patches/145695_create_resource_exposures_opemaw_old.sql... (OK - took 0 seconds)
Applying 7318_patches/141621_added_informations_adprow.sql... (OK - took 0 seconds)
Applying 7318_patches/141621_create_old_mapping_table.sql... (OK - took 0 seconds)
Applying 7318_patches/130499_create_ssa_deep_scan_policy.sql... (OK - took 0 seconds)
Applying 7320_patches/101964.sql... (OK - took 0 seconds)
Applying 7330_patches/147274_purge_tlog_node_gowlids.sql... (OK - took 0 seconds)
Applying 7330_patches/141282_update_virtual_domain.sql... (OK - took 0 seconds)
Applying 7330_patches/136615_update_aix_output.sql... (OK - took 0 seconds)
Applying 7330_patches/144082_qptz_fixd_triggers.sql... (OK - took 1 seconds)
Applying functions/all_functions.sql... (OK - took 3 seconds)
Processed all SQL in 425 seconds.
Applying ODM changes: done.
Staging factory MRS ... (OK)
Se-seping the system ... (OK)
Sun Mar 15 04:12:29 EDT 2020 (aks-rekey.sh) OK: MRS Re-Key Completed
OK: Installed Secure Analytics version 7.3.3 (Build 281918062894340).
Recording currently installed RPM list: done.
If you have not set an admin password, set one now with "sudo /opt/qradar/support/changePasswd.sh -a"
[ OK ] Started SIGH Init.
[ OK ] Started Permit User Sessions.
[ OK ] Started Permit User Sessions.
[ OK ] Created slice user.slice of user postgres.
[ OK ] Started Session c2 of user postgres.
[ OK ] Started Session c4 of user postgres.
[ OK ] Started Session c3 of user postgres.
[ OK ] Started Session c1 of user postgres.
Starting Wait for Plymouth Boot Screen to Quit...
[ OK ] Started Command Scheduler.
Starting Terminate Plymouth Boot Screen...
[ OK ] Started Session c1 of user postgres.
[ OK ] Removed slice user.slice of postgres.

Red Hat Enterprise Linux Server 7.5 (Maipo)
kernel 3.10.0-1062.1.1.el7.x86_64 on an x86_64

localhost login:

```


Next Steps

You can now configure the desired JSA roles (JSA hardware appliances come with pre-installed software, so you can start directly from here to configure the desired roles). This chapter details these next steps in the order of sections listed here:

Install and Configure JSA as an All-in-One (AIO) Threat Analytics

Install and Configure Log Analytics

Install and Configure an Event Processor

Install and Configure a Flow Processor

Install and Configure a JSA Data Node

Install and Configure Store and Forward Event Collector

Install and Configure High-Availability Appliance for Non-console

Install and Configure High-Availability Appliance for Console

Install and Configure JSA Risk Manager

Install and Configure a Vulnerability Processor

Install and Configure a Vulnerability Scanner

Install and Configure an App Host

Install EP-FP Combo on JSA Appliances

NOTE These sections are applicable to both JSA hardware and virtual appliances.

You can also use the bootable USB to reinstall hardware appliances with a different version of JSA software, if required. For more information, see the section, Reinstall JSA Using Bootable USB, *further along in this chapter*.

Install and Configure JSA as an All-in-One (AIO) Threat Analytics

An all-in-one installation, or a standalone installation, is where all the JSA components are installed on the same device that acts as an independent unit with its own web UI. This installation procedure is applicable to both JSA hardware and virtual appliances.

Before You Begin

Before you start the installation, ensure that:

- The required hardware is installed (in case of appliances).
- You have the required license key for your appliance.
- A keyboard and monitor are connected by using the VGA connection (in case of hardware appliances).
- There are no expired licenses on either the console or the managed hosts.
- Software versions for all JSA appliances in a deployment is the same version and patch level. Note that deployments that use different versions of software are not supported.

Have the following information ready before you begin the installation:

- Hostname
- IP address
- Network mask
- Default gateway address
- Primary Domain Name System (DNS) server address
- Secondary DNS server address (Optional)
- (Optional) Public IP address for networks using Network Address Translation (NAT)
- (Optional) Email server name
- Network Time Protocol (NTP) (for TA/LA Console only) server or time server name

Step-by-Step Procedure

Follow the steps in the installation wizard for the virtual appliance type you are creating.

The JSA installation wizard allows you to use only certain keyboard keys to navigate through the installation options. Table P1 lists these keys along with how you can use them.

Log in as the root user at the prompt (a password is not required). If you are prompted for a password, there is some error with the installation. Contact <https://support.juniper.net/support/>.

Read and accept the EULA license and proceed with the installation.

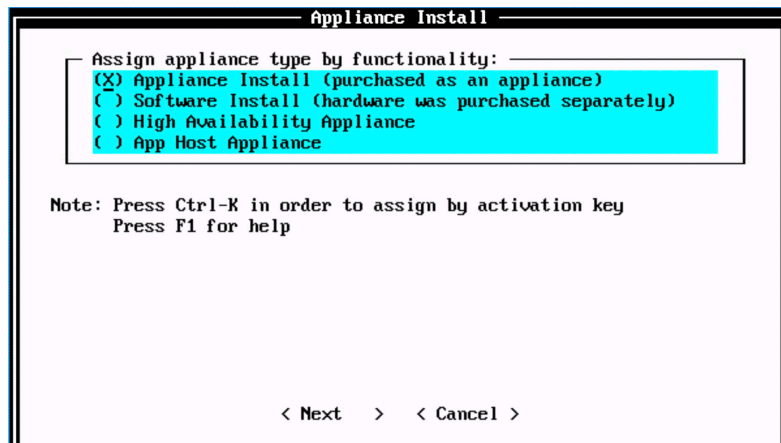
Provide information in the installation wizard when prompted.

After accepting EULA license, the Appliance Install page appears.

Select Appliance Install (purchased as an appliance).

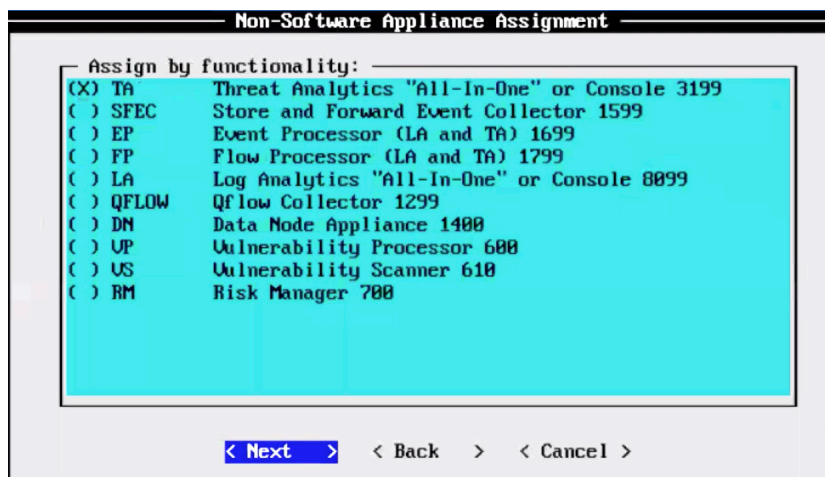
Choose this option if you have purchased JSA appliances or wish to install virtual machines and select Next.

Figure 27 Appliance Install Options



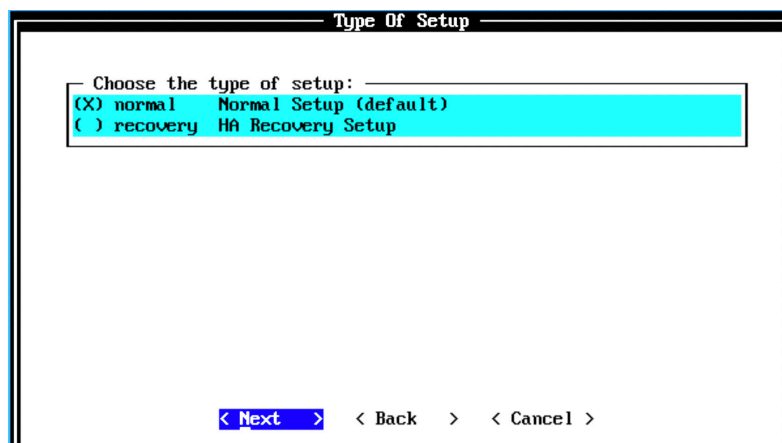
The Non-Software Appliance Assignment page appears. Select the non-software appliance type as Threat Analytics “All-in-One” or Console 3199 and select Next, shown in Figure 28.

Figure 28 Non-Software Appliance Assignment Options



The Type of Setup page appears. Select the Normal Setup (default) option and select Next.

Figure 29 Setup Options



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.

Figure 30 Date/Time Setup Options

Date/Time Setup

Setting the date and time manually or by specifying an NTP/RDate server.

Manual setting:

Current Date (YYY/MM/DD): 2019/12/01

24h Clock Time (HH:MM:SS): 01:30:55

Time Server name or IP address:

Time server:

< Next > < Back > < Cancel >

The Select Continent/Area page appears. Select the time zone continent or area as required and select Next. The default value is America.

Figure 31 Select Continent/Area Options

Select Continent/Area

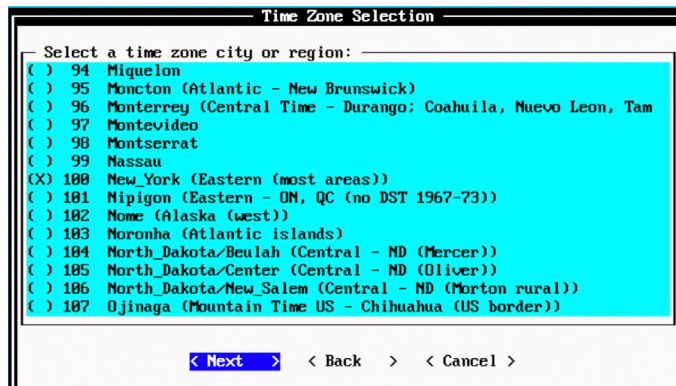
Select a time zone continent/area:

- () 0 Africa
- (X) 1 America
- () 2 Antarctica
- () 3 Arctic
- () 4 Asia
- () 5 Atlantic
- () 6 Australia
- () 7 Europe
- () 8 GMT
- () 9 Indian
- () 10 Pacific
- () 11 UTC

< Next > < Back > < Cancel >

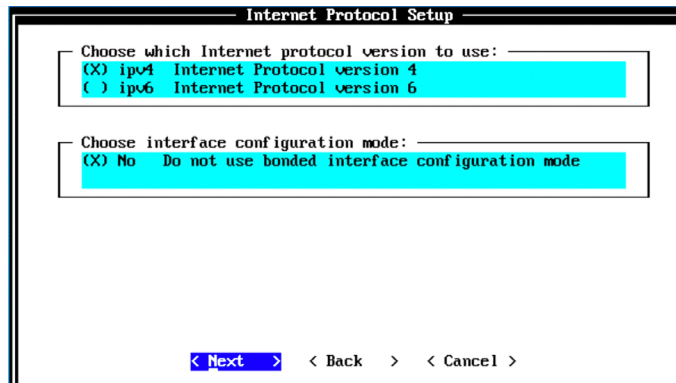
The Time Zone Selection page appears. Select the time zone city or region as required and select Next. The default value is New York (Eastern (most areas)) as shown in Figure 32.

Figure 32 Time Zone Options



The Internet Protocol Setup page appears next. By default, the Internet Protocol version is selected as IPv4 Internet Protocol version 4. You may select IPv6 Internet Protocol version 6, as required. Select No as the value for Do not use bonded interface configuration mode. You might use the bonded interface configuration mode, as required. Select Next in Figure 33.

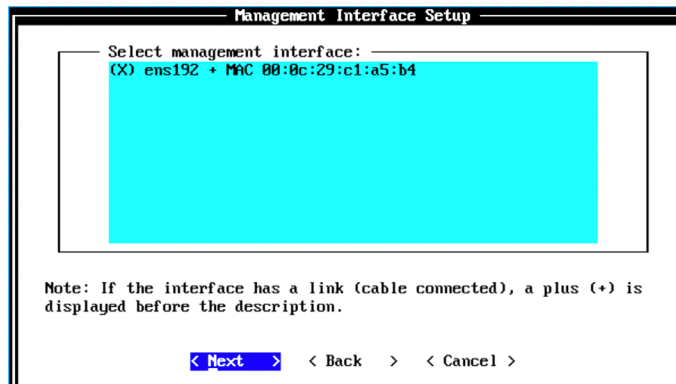
Figure 33 *Internet Protocol Setup Options*



The Management Interface Setup is next. Select the management interface that you want to use and then select Next.

NOTE The list shown depends on the number of NIC Cards in the hardware that you are installing JSA on. All available interfaces will be displayed.

Figure 34 *Management Interface Setup Options*

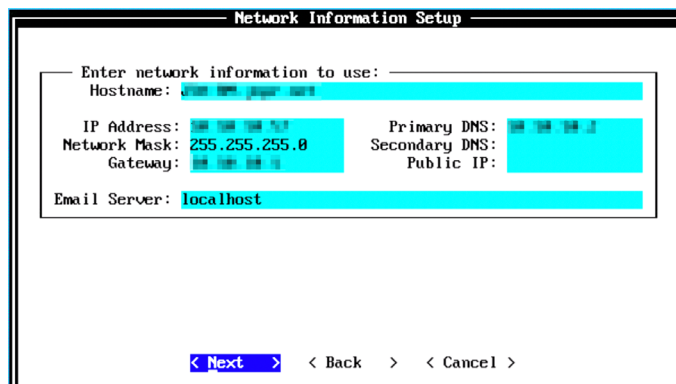


Next is Figure 35 and the Network Information Setup page. Let's configure the following network settings (and then select Next).

- 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.
- Email Server: Enter the email server (if you do not have an e-mail server, type *localhost* in this field).

Figure 35

Network Information Setup Options



This may take a few minutes as the network settings are validated. Once validated successfully, the Admin Password Setup page appears.

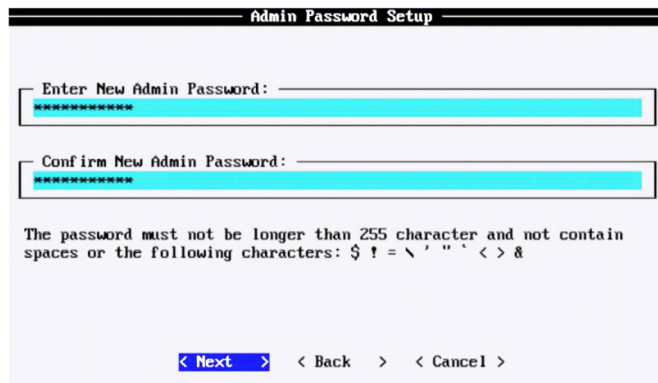
Now configure the administrator password required to login into the JSA web UI.

In the Enter New Admin Password field, enter an admin password that meets the following criteria: contains at least 5 characters; contains no spaces; can include the following special characters: @, #, ^, and *.

Re-enter the admin password in the Confirm New Admin Password field and select Next.

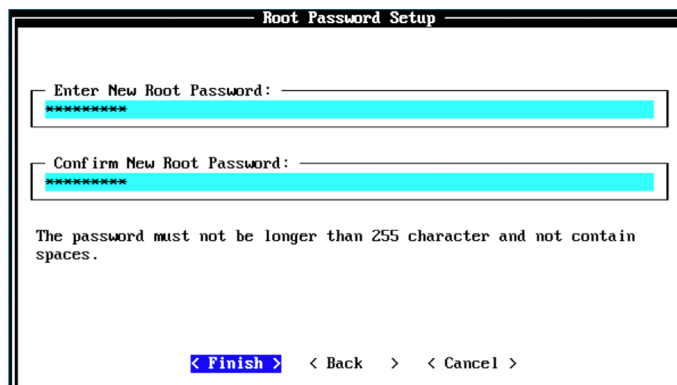
NOTE The option for admin password configuration comes only for LA or TA console installation. This option is not available if you are installing a managed host.

Figure 36 Admin Password Options

The image shows a terminal window titled "Admin Password Setup". It contains two input fields: "Enter New Admin Password:" and "Confirm New Admin Password:". Both fields are filled with red asterisks. Below the fields, a message states: "The password must not be longer than 255 character and not contain spaces or the following characters: \$! = \ ' \" < > &". At the bottom, there are three buttons: "< Next >" (highlighted in blue), "< Back >", and "< Cancel >".

Now configure the root password required to login to the JSA Command Line Interface (CLI). In the Enter New Root Password field, enter a root password that meets the same criteria as before, re-enter the root password in the Confirm New Root Password field, and then select Finish.

Figure 37 Root Password Options

The image shows a terminal window titled "Root Password Setup". It contains two input fields: "Enter New Root Password:" and "Confirm New Root Password:". Both fields are filled with red asterisks. Below the fields, a message states: "The password must not be longer than 255 character and not contain spaces.". At the bottom, there are three buttons: "< Finish >" (highlighted in blue), "< Back >", and "< Cancel >".

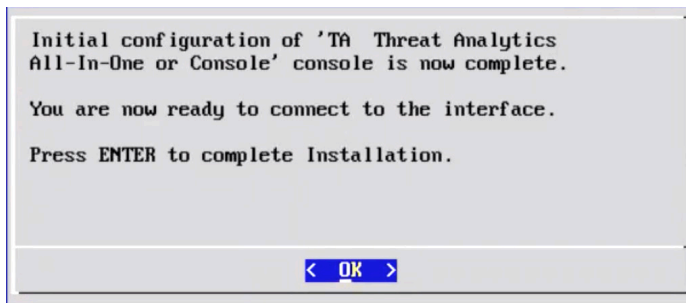
When you select Finish, the installation process starts. This process typically takes a few hours. Although it might appear as if the system is not responding at times, wait for the installation to complete.

Figure 38 *Installing Changes*

```
Installing Qradar changes...
Activating system with key 003U41-5T7A3E-077N7N-54512G.
Appliance ID is 3199.
Installing 'TA Threat Analytics "All-In-One" or Console' with id 3199.
Configuring network...
Setting current date and time.
New date of '2019/12/01 01:30:55' was specified 171 seconds ago...
Setting date and time to '20191201 01:33:46'...
Restarting postgresql-grd
Running changeQradarPassword
Stopping hostcontext
Stopping httpd
Stopping tomcat
Sun Dec 1 01:34:01 EST 2019 [setup-imq.sh] OK: IMQ Setup Completed
Stopping httpd
Stopping tomcat
Updating db user password
```

The output shown in Figure 39 indicates the successful installation of an AIO Threat Analytics console. Once the installation is complete, a final completion message is displayed. Click Ok.

Figure 39 *Installation Complete*



Verification

To verify the successful installation of AIO Threat Analytics console run the following command on the console:

Run `less /etc/.appliance_name`

The output displays 3199 as the appliance installed.

Ping the default gateway to ensure that the connectivity is fine. You can also use the `ifconfig` command to view the IP address details of the appliance.

After the installation is successful, you can log into the JSA web UI.

Next Steps

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received when you purchased JSA from Juniper Networks contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system, *before* the default license expires.

For more information about applying a license, see section *Apply a License to JSA*.

After you complete the TM/TA installation, you can use it either as a standalone all-in-one installation or add managed hosts such as EP, FP, and so on, to TM/TA console (distributed deployment). For more information, see sections *Add an Event Processor to Threat Analytics Console or Log Analytics Console* and *Add a Flow Processor to Threat Analytics*.

Install and Configure a Log Analytics

The Log Analytics hardware or virtual appliance is a log analytics system that manages and stores events from various network devices. Log Analytics includes an on-board event collector, event processor, and internal storage for events. Log Analytics cannot collect and process flows.

NOTE This installation procedure is applicable to both JSA hardware and virtual appliances.

Before You Begin

Before you do the installation, ensure that you have the following in place:

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

- Software versions for all JSA appliances in a deployment are the same version and patch level. Note that deployments that use different versions of software are not supported.

Keep the following information ready before you begin the installation:

- Hostname
- IP address
- Network mask
- Default gateway address
- Primary Domain Name System (DNS) server address
- Secondary DNS server address (Optional)
- (Optional) Public IP address for networks using Network Address Translation (NAT)
- Email server name
- Network Time Protocol (NTP) server (for LA or TA Console only) or time server name

Step-by-Step Procedure

Follow the steps in the installation wizard for the hardware or virtual appliance type you are creating.

The JSA installation wizard allows you to use only certain keyboard keys to navigate through the installation options. Table P1 lists these keys along with how you can use them.

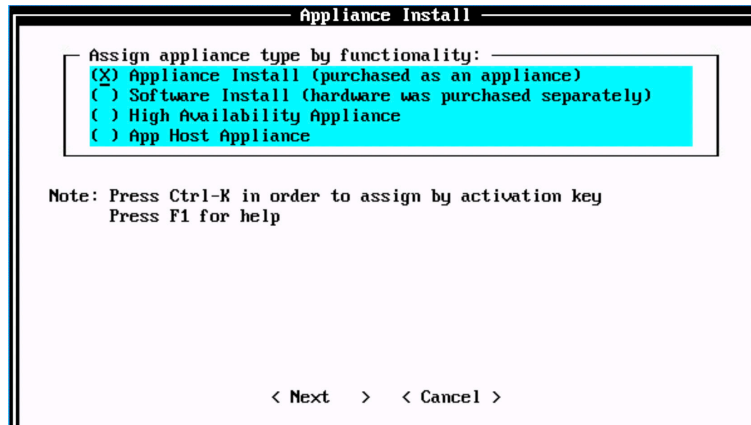
Log in as the root user at the prompt (a password is not required). If you are prompted for a password, there is some error with the installation. Contact <https://support.juniper.net/support/>.

Read and accept the EULA license and proceed with the installation. Provide information in the installation wizard when prompted.

After accepting EULA license, the Appliance Install page appears as shown in Figure 40. Select Appliance Install (purchased as an appliance). Choose this option if

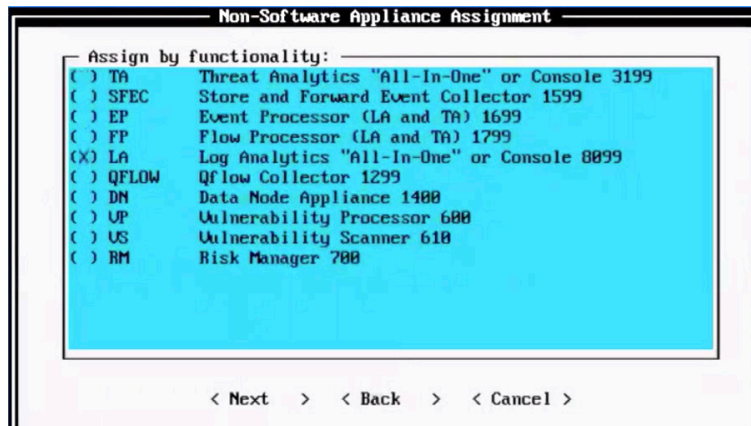
you have purchased JSA appliances or wish to install virtual machines and select Next.

Figure 40 Appliance Install Options



The Non-Software Appliance Assignment page appears. Select the non-software appliance type as LA All-In-One or Console 8099 and select Next.

Figure 41 Non-Software Appliance Assignment Options



The Type of Setup page appears. Select the Normal Setup (default) option and select Next.

Figure 42 Setup Options

Type Of Setup

Choose the type of setup: _____

☒ normal Normal Setup (default)

☐ recovery HA Recovery Setup

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.

Figure 43 Date/Time Setup Options

Date/Time Setup

Setting the date and time manually or by specifying an NTP/RDate server.

Manual setting: _____

Current Date (YYYY/MM/DD): 2019/12/01

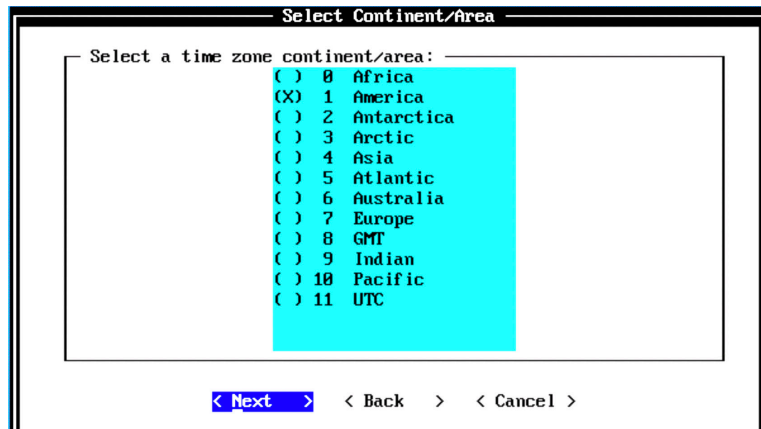
24h Clock Time (HH:MM:SS): 01:30:55

Time Server name or IP address: _____

Time server: _____

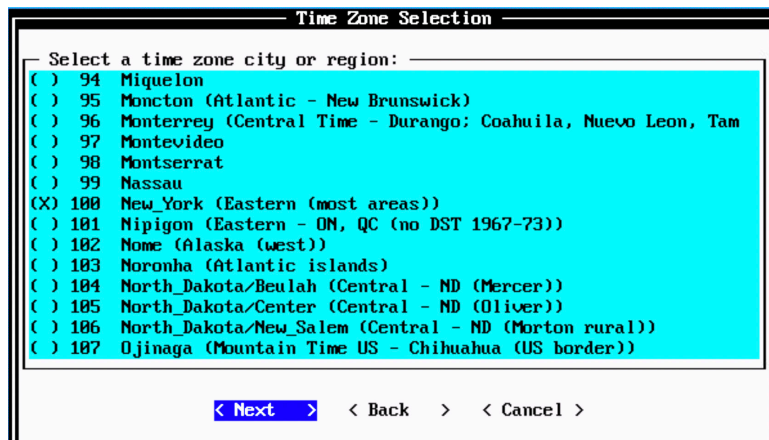
The Select Continent/Area page appears. Select the time zone continent or area as required and select Next. The default value is America.

Figure 44 Select Continent/Area Options



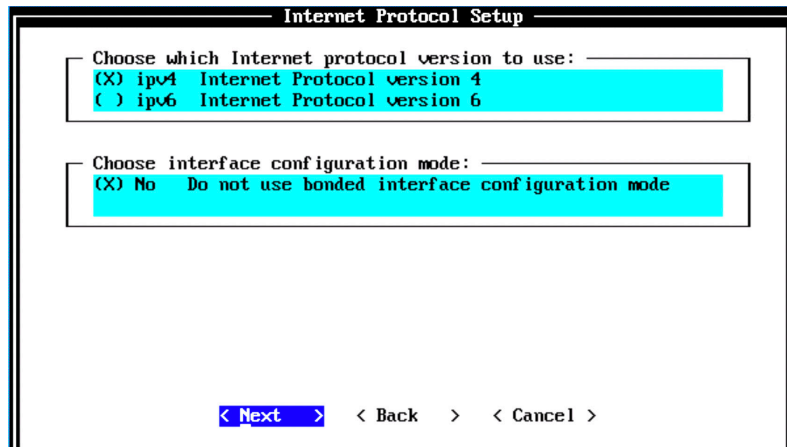
The Time Zone Selection page appears. Select the time zone city or region as required and select Next. The default value is New_York (Eastern (most areas)).

Figure 45 *Time Zone Options*



The Internet Protocol Setup page appears in Figure 46. By default, the Internet Protocol version is selected as IPv4 Internet Protocol version 4. You might select IPv6 Internet Protocol version 6, as required. Select No as the value for Do not use bonded interface configuration mode. You might use the bonded interface configuration mode as required. Select Next.

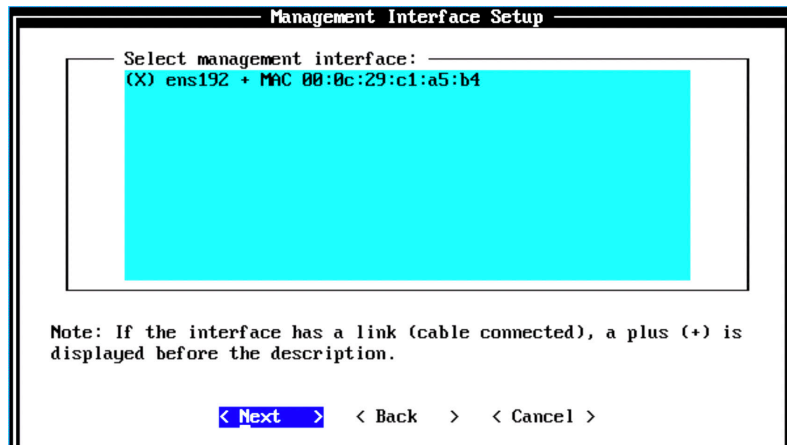
Figure 46 *Internet Protocol Setup Options*



The Management Interface Setup page appears. Select the management interface that you want to use and select Next.

NOTE The list shown depends on the number of NIC Cards in the hardware that you are installing JSA on. All the available interfaces will be displayed in this section.

Figure 47 Management Interface Setup Options



The Network Information Setup page appears. Configure the following network settings:

- 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.
- Email Server—Enter the email server. If you do not have an e-mail server, type localhost in this field.

Select Next. The network settings will be validated. This may take a few minutes.

Figure 48 *Network Information Setup Options*

Network Information Setup

Enter network information to use:

Hostname:

IP Address:

Network Mask: 255.255.255.0

Gateway:

Primary DNS:

Secondary DNS:

Public IP:

Email Server: localhost

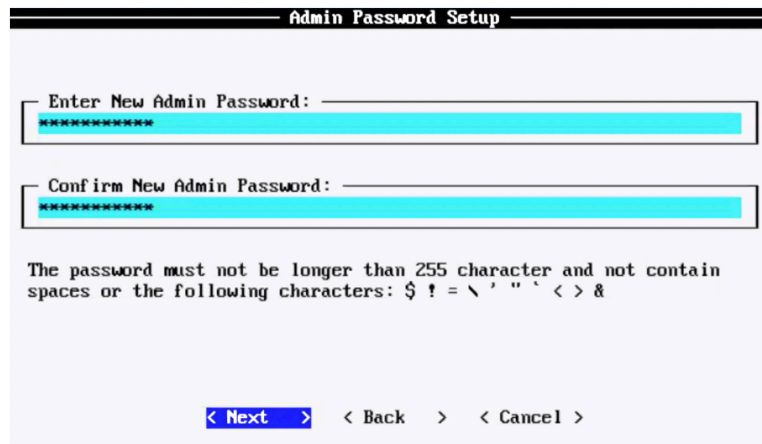
< Next > < Back > < Cancel >

Once the network settings are validated successfully, the Admin Password Setup page appears (Figure 49). In the Enter New Admin Password field, enter an admin password that meets the following criteria: contains at least five characters, contains no spaces, can include the following special characters: @, #, ^, and *.

NOTE The option for admin password configuration comes only for LA or TA console installation. This option is not available if you are installing a managed host.

Re-enter the admin password in the Confirm New Admin Password field and select Next.

Figure 49 Admin Password Options



Admin Password Setup

Enter New Admin Password:

Confirm New Admin Password:

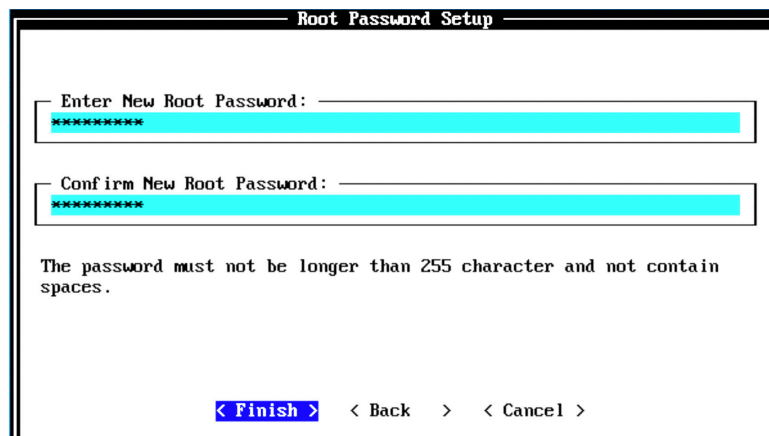
The password must not be longer than 255 character and not contain spaces or the following characters: \$! = \ ' " ' < > &

< Next > < Back > < Cancel >

In the Enter New Root Password field, enter a root password that meets the following criteria: contains at least five characters, contains no spaces, can include the following special characters: @, #, ^, and *.

Re-enter the root password in the Confirm New Root Password field and select Finish.

Figure 50 Root Password Options



Root Password Setup

Enter New Root Password:

Confirm New Root Password:

The password must not be longer than 255 character and not contain spaces.

< Finish > < Back > < Cancel >

When you select Finish, the installation process starts. This process typically takes a few hours. Although it might appear as if the system is not responding at times, wait for the installation to complete.

Figure 51 displays output indicating the ongoing installation process.

Figure 51 Installing Changes

```

Installing Qradar changes...
Activating system with key 1U6E1N-07123Q-5F520A-1D6D4U.
Appliance ID is 8099.
Installing 'LA Log Analytics "All-In-One" or Console' with id 8099.
Configuring network...
Setting current date and time.
New date of '2019/12/01 05:34:21' was specified 259 seconds ago...
Setting date and time to '20191201 05:38:40'...
Restarting postgresql-qrdr
Running changeQradarPassword
Stopping hostcontext
Stopping httpd
Stopping tomcat
Sun Dec 1 05:38:56 EST 2019 [setup-imq.sh] OK: IMQ Setup Completed
Stopping httpd
Stopping tomcat
Updating db user password

```

Once the installation is complete, a final completion message is displayed as shown in Figure 52. Click OK.

Figure 52

Installation Complete



Verification

To verify the successful installation of JSA log analytics, run the following command on the console:

```
Run less /etc/.appliance_name
```

The output displays 8099 as the appliance is installed.

Ping the default gateway to ensure that the connectivity is fine. You can also use the `ifconfig` command to view the IP address details of the appliance. If the installation is successful, you can log in to the JSA web UI.

Next Steps

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system before the default license expires.

For more information about applying a license, see section *Apply a License to JSA*.

After you complete the LA installation, you can use it either as a standalone

all-in-one installation or add managed hosts such as EP, SFEC, and so on, to an LA console (distributed deployment). For more information, see sections *Add an Event Processor to Threat Analytics Console or Log Analytics Console* and *Install and Configure Store and Forward Event Collector*.

Install and Configure an Event Processor

An event processor (EP) processes event and flow data from the event collector (EC). When you install EP (1699), it will also have an EC component.

To complete the installation and configuration of an event processor:

- Install the event processor using the instructions in this section.
- Add the event processor to the threat analytics or log analytics using the instructions provided in section *Add an Event Processor to Threat Analytics or Log Analytics All-in-One Console*.
- Apply a license to the event processor using the instructions *Apply a License to JSA*.

Before You Begin

Before you do the installation, ensure that you have the following in place:

- The required hardware is installed (in case of appliances).
- You have the required license key for your appliance.
- A keyboard and monitor are connected by using the VGA connection (in case of hardware appliances).
- There are no expired licenses on either the console or the managed hosts.
- Software versions for all JSA appliances in a deployment must be the same version and patch level. Note that deployments that use different versions of software are not supported.

Keep the following information ready before you begin the installation:

- Hostname
- IP address
- Network mask
- Default gateway address
- Primary Domain Name System (DNS) server address
- Secondary DNS server address (Optional)

- (Optional) Public IP address for networks using Network Address Translation (NAT)
- Email server name

Step-by-Step Procedure

Follow the steps in the installation wizard for the hardware or the virtual appliance type you are creating.

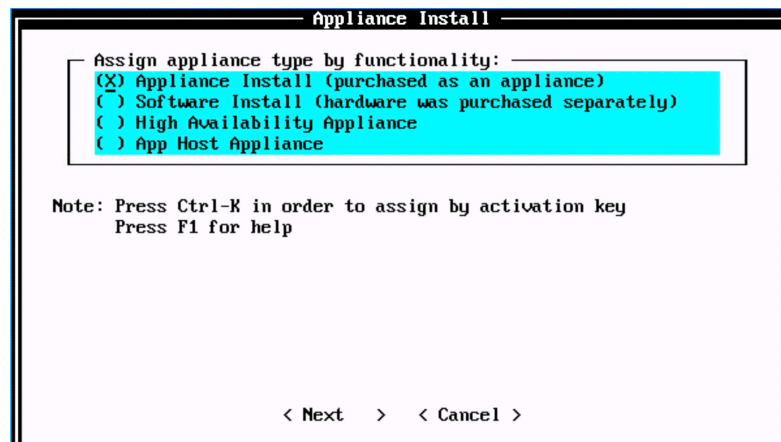
The JSA installation wizard allows you to use only certain keyboard keys to navigate through the installation options. Table P1 lists these keys along with how you can use them.

Log in as the root user at the prompt (a password is not required). If you are prompted for a password, there is some error with the installation. Contact <https://support.juniper.net/support/>.

Read and accept the EULA license and proceed with the installation. Provide information in the installation wizard when prompted. After accepting EULA license, the Appliance Install page appears as shown in Figure 53.

Select Appliance Install (purchased as an appliance). Choose this option if you have purchased JSA appliances or wish to install virtual machines and select Next.

Figure 53 Appliance Install Options



The Non-Software Appliance Assignment page appears. Select the non-software appliance type as EP Event Processor (LA and TA) 1699 and select Next.

Figure 54 Non-Software Appliance Assignment Options

Non-Software Appliance Assignment

Assign by functionality:

<input type="checkbox"/>	TA	Threat Analytics "All-In-One" or Console	3199
<input type="checkbox"/>	SFEC	Store and Forward Event Collector	1599
<input checked="" type="checkbox"/>	EP	Event Processor (LA and TA)	1699
<input type="checkbox"/>	FP	Flow Processor (LA and TA)	1799
<input type="checkbox"/>	LA	Log Analytics "All-In-One" or Console	8899
<input type="checkbox"/>	QFLOW	Qflow Collector	1299
<input type="checkbox"/>	DN	Data Node Appliance	1400
<input type="checkbox"/>	UP	Vulnerability Processor	600
<input type="checkbox"/>	US	Vulnerability Scanner	610

The Type of Setup page appears (Figure 55). Select the Normal Setup (default) option and select Next.

Figure 55 Setup Options

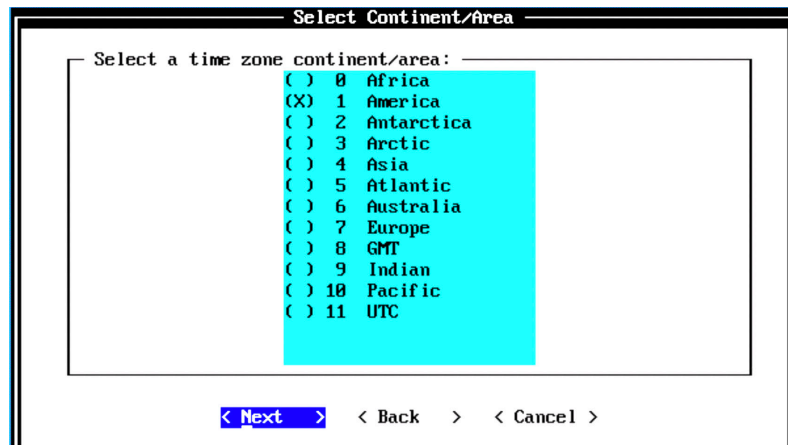
Type Of Setup

Choose the type of setup:

<input checked="" type="checkbox"/>	normal	Normal Setup (default)
<input type="checkbox"/>	recovery	HA Recovery Setup

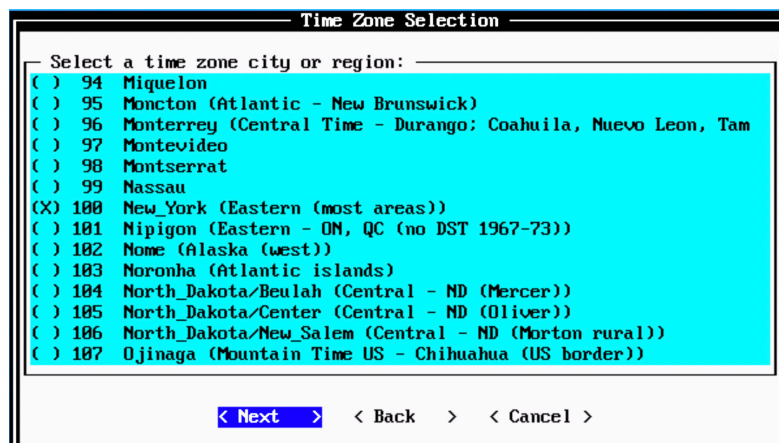
The Select Continent/Area page appears. Select the time zone continent or area as required and select Next. The default value is America.

Figure 56 Select Continent/Area Options



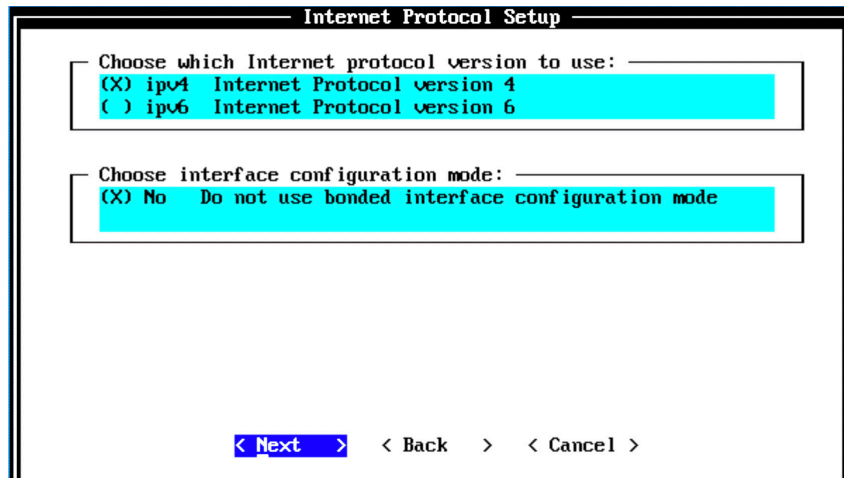
The Time Zone Selection page appears. Select the time zone city or region as required and select Next. The default value is New-York (Eastern (most areas)).

Figure 57 Time Zone Options



The Internet Protocol Setup page appears. By default, the Internet Protocol version is selected as IPv4 Internet Protocol version 4. You might select IPv6 Internet Protocol version 6, as required. Select No as the value for Do not use bonded interface configuration mode. You might use the bonded interface configuration mode, as required. Select Next.

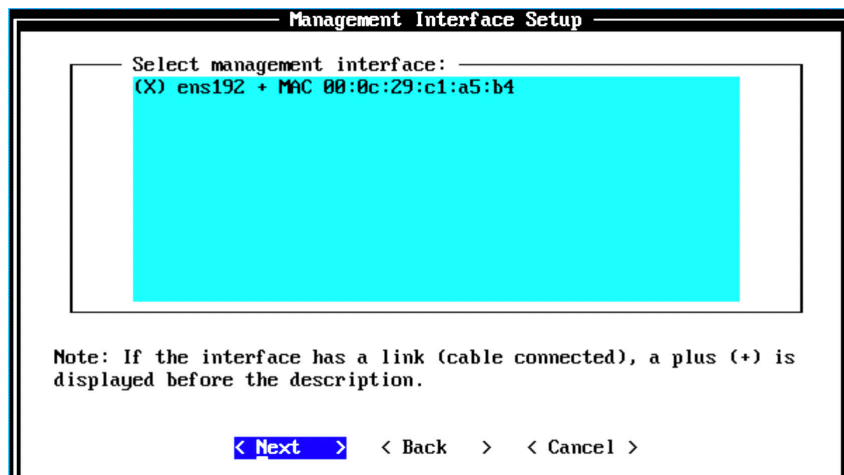
Figure 58 Internet Protocol Setup Options



The Management Interface Setup page appears. Select the management interface that you want to use and select Next.

NOTE The list shown here depends on the number of NIC Cards on the hardware that you are installing JSA. All the available interfaces will be displayed in this section.

Figure 59 Management Interface Setup Options



The Network Information Setup page appears. Configure the following network

settings:

- 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.
- Email Server—Enter the email server. If you do not have an e-mail server, type localhost in this field.

Figure 60

Network Information Setup Options

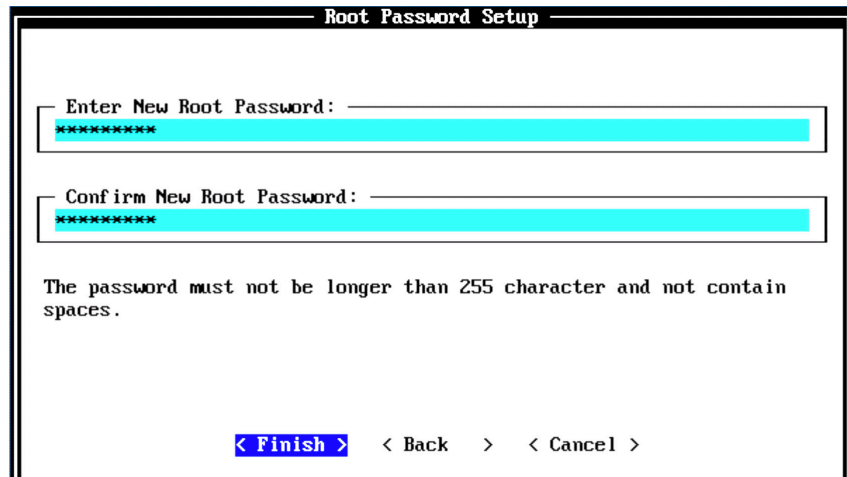
Select Next. The network settings are validated. This may take a few minutes.

Configure the root password required to login to the JSA Command Line Interface (CLI). In the Enter New Root Password field, enter a root password that meets the following criteria: contains at least 5 characters, contains no spaces, can include the following special characters: @, #, ^, and *.

Re-enter the root password in the Confirm New Root Password field and select Finish.

Figure 61

Root Password Options



Root Password Setup

Enter New Root Password:

Confirm New Root Password:

The password must not be longer than 255 character and not contain spaces.

< Finish >
< Back
>
< Cancel >

When you select Finish, the installation process starts. This process typically takes a few hours. Although it might appear as if the system is not responding at times, wait for the installation to complete.

Figure 62

Installing Changes

```

Installing Qradar changes...
Activating system with key 42761B-6T2E38-53845J-2S4172.
Appliance ID is 1699.
Installing 'EP      Event Processor (LA and TA)' with id 1699.
Configuring network...
Setting current date and time.
New date of '2019/12/01 05:13:54' was specified 180 seconds ago...
Setting date and time to '20191201 05:16:54' ...
Running changeQradarPassword
Stopping hostcontext
Sun Dec 1 05:17:10 EST 2019 [setup-imq.sh] OK: IMQ Setup Completed
Updating db user password
Applying replication db file...done!
Running replication setup...done!
Modifying postgresql config...done!
Running changeQUMPPassword
Setting email server to localhost
Running FinalSetup
Updating iptables firewall rules.
Restarting system services:
- syslog-ng
- hostcontext
- hostservices
Running restartServices
Restarting system services: syslog-ng.
Non-console setup, stopping services: hostcontext hostservices java.
Restarting services:
- hostservices
- hostcontext
Failed to start hostcontext!
OK: Configuration of host EP-jsa as a non-console completed.
qradar_setup.py: End: 0
Running: /opt/qradar/bin/after_services_up.sh

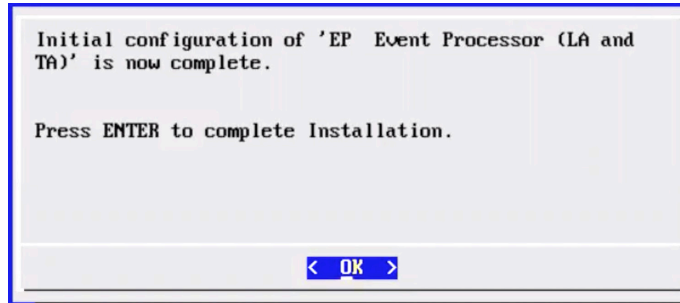
```

The output shown in Figure 62 indicates a successful installation of an event processor is complete. Once the installation is complete, a completion message is dis-

played as in Figure 63. Click OK.

Figure 63

Installation Complete



Verification

To verify the successful installation of an event processor, run the following command on the console:

```
Run less /etc/.appliance_name
```

The output displays 1699 as the appliance installed.

Ping the default gateway to ensure that the connectivity is fine. You can also use the `ifconfig` command to view the IP address details of the appliance.

Next Steps

After you have completed installing the event processor, you can add the event processor to a TA or LA console using the JSA web UI. For more information about adding an event processor, see *Add an Event Processor to Threat Analytics or Log Analytics All-in-One Console*.

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system before the default license expires.

For more information about applying a license, see the section, *Apply a License to JSA*.

Add an Event Processor to the Threat Analytics Console or Log Analytics Console

You can add managed hosts, such as event and flow collectors, event and flow processors, and data nodes, to distribute data collection and processing activities across your JSA deployment.

NOTE Adding an event processor helps in the distributed collection of events. The event collection and the processing load will be on the event processor rather than on the console. Also, when the event collection needs to happen between different geographical locations, event processors conserve the WAN bandwidth by locally storing the events and not sending the entire event data to the console. Another use case for event processor nodes are when you need to comply with data compliance regulations.

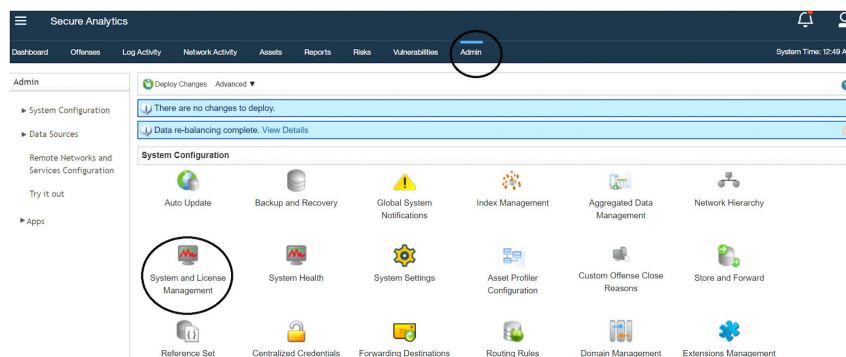
Let's begin by verifying that the managed host has the same JSA version and patch as the JSA console that you are using to manage it. Event processors can be added either to threat analytics (TA) or log analytics (LA) consoles. The same procedure is applicable to TA and LA consoles.

To add an event processor to Threat Analytics host:

Log in to the JSA web UI. On the navigation menu, click Admin and the Admin page appears. In the System Configuration section, click System and License Management.

Figure 64

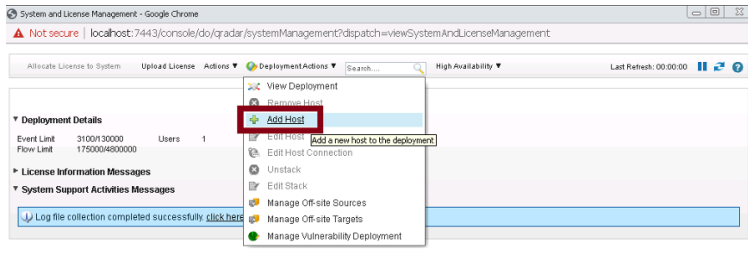
System and License Management



The System and License Management page appears. On the navigation menu, select Deployment Actions > Add Host as shown in Figure 65.

Figure 65

Deployment Actions > Add Host



Add Managed Host appears as shown in Figure 66. Enter the fixed IP address of the event processor host you want to add in the Host IP field. Enter the root password for the host IP in the Host Password field and re-enter the root password in the Confirm Password field.

Click Add.

Figure 66

Add Managed Host

Add Managed Host

Before you add a managed host, make sure the managed host includes the SIEM software. The IP of the host is required as well as the root password. Hover over label fields for more information.

Host IP:

Host Password:

Confirm Password:

Encrypt Host Connections:

☐

Encryption Compression:

☐

Network Address Translation:

☐

NAT Group:

Public IP:

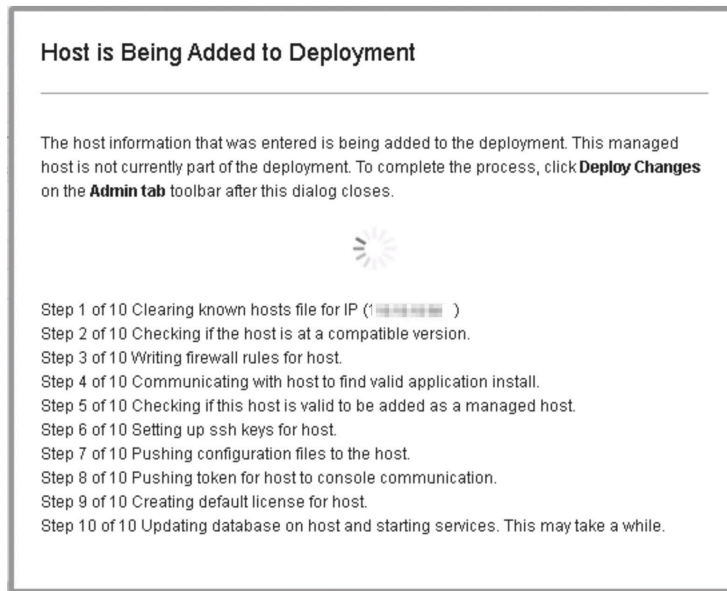
Add

Cancel

NOTE If you are using NAT or want to use encrypted communication between EP and console, select the other options accordingly.

A pop-up appears (Figure 67) displaying the status of the host being added to the network.

Figure 67 Host is Being Added to Deployment



After the host is added successfully, the new host is listed on the System and License Management page.

Figure 68 Host Successfully Added

Allocate License to System Upload License Actions Deployment Actions Search... Last Refresh: 00:00:50							
Display Systems							
Deployment Details Event Limit: 1500130000 Users: 1 Flow Limit: 750004800000							
License Information Messages							
System Support Activities Messages							
Host Name	Host IP	Appliance Type	Version	Serial Number	Host Status	License Expiration Date	License :
FP-isa-new	10.10.10.10	1799 - Flow Processor	7.3.3	VMware-56 4d...	Active	Perpetual	Deployed
EP-isa	10.10.10.10	1699 - Event Processor	7.3.3	VMware-56 4d...	Active	Perpetual	Deployed
TM-isa (console)	10.10.10.10	3199 - Console	7.3.3	VMware-56 4d...	Active	Jan 25, 2020	Deployed

Note that at this point, the new host is not yet deployed. To deploy the changes, go back to the Admin page (Figure 69). The changes that need to be deployed are shown on top of the page. Click View Details to see the changes.

Figure 69 Undeployed Changes

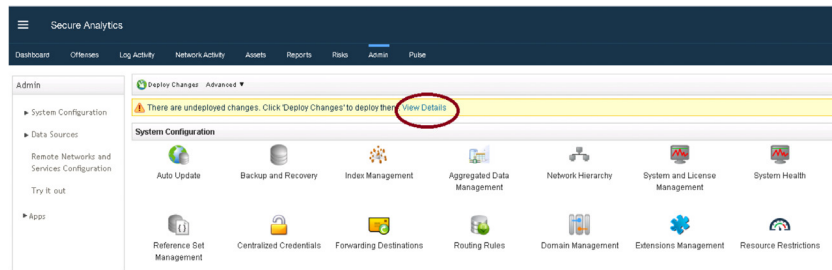
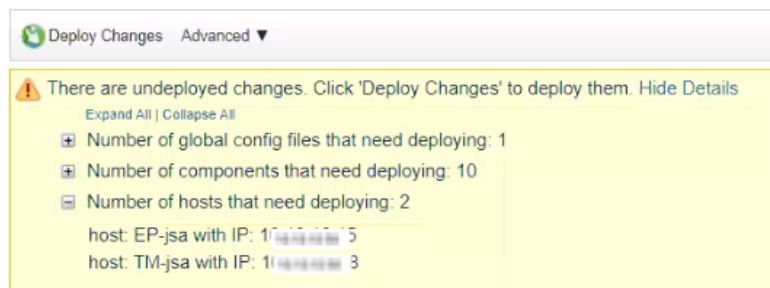


Figure 70 Changes to be Deployed



Click Deploy Changes and a confirmation page appears asking for confirmation to deploy the changes, as shown in Figure 71. Click Continue to deploy the changes.

Figure 71 Deployment Confirmation



The deployment starts. This process typically takes several minutes. Although it might appear as if the system is not responding at times, wait for the deployment to complete. The JSA web UI will display the progress in its deployment process.

When the deployment process is complete, you will see the status as *Success* for all the hosts. This means that the event processor is successfully added to the deployment. You can now point the log sources to send events to the event processor.

Next Step

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your

permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system before the default license expires.

For more information about applying a license, see section *Apply a License to JSA*.

Install and Configure a Flow Processor

The virtual or hardware JSA flow processor appliance provides retention and storage for flows and processes flow data from the flow collector (FC). When you install FP(1799), it also has an FC component. To begin the installation and configuration of a flow processor:

- Install the flow processor using the instructions in this section.
- Add the flow processor to threat analytics using the instructions provided in section *Add a Flow Processor to Threat Analytics*.
- Apply a license to the flow processor using the instructions *Apply a License to JSA*.

Before you start the installation, ensure that you have the following in place:

- The required hardware is installed (in case of appliances).
- You have the required license key for your appliance.
- A keyboard and monitor are connected by using the VGA connection (in case of hardware appliances).
- There are no expired licenses on either the console or the managed hosts.
- Software versions for all JSA appliances in a deployment must be the same version and patch level. Note that deployments that use different versions of software are not supported.

And you'll need the following information for the install:

- Hostname
- IP address
- Network mask
- Default gateway address
- Primary Domain Name System (DNS) server address
- Secondary DNS server address (Optional)

- (Optional) Public IP address for networks using Network Address Translation (NAT)
- Email server name

Step-by-Step Procedure

Follow the steps in the installation wizard for the hardware or virtual appliance type you are creating.

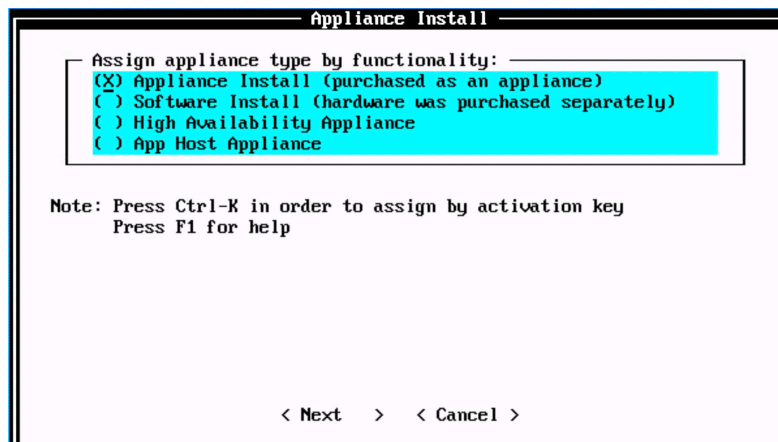
The JSA installation wizard allows you to use only certain keyboard keys to navigate through the installation options. Table P1 lists these keys along with how you can use them.

Log in as the root user at the prompt (a password is not required). If you are prompted for a password, there is some error with the installation. Contact <https://support.juniper.net/support/>.

Read and accept the EULA license and proceed with the installation. Provide information in the installation wizard when prompted.

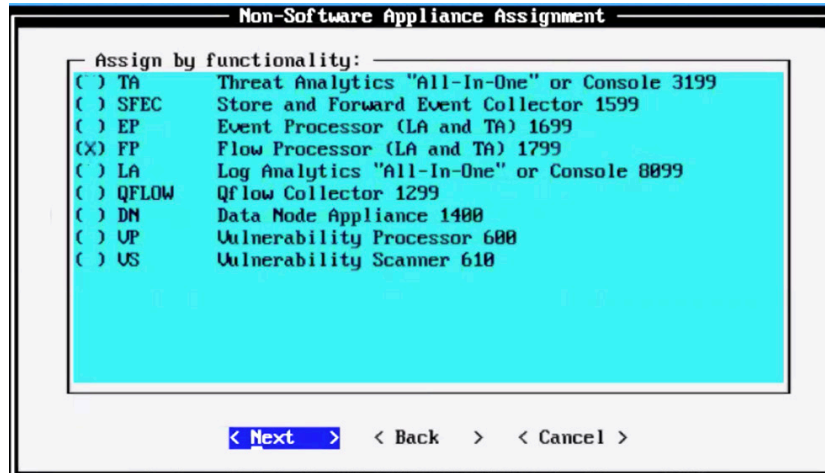
After accepting the EULA license, the Appliance Install page appears. Select Appliance Install (purchased as an appliance). Choose this option if you have purchased JSA appliances or wish to install virtual machines. Select Next as shown in Figure 72.

Figure 72 *Appliance Install Options*



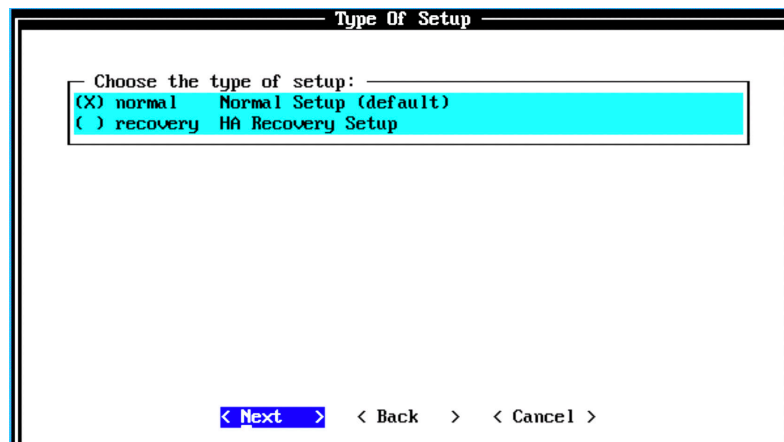
The Non-Software Appliance Assignment page appears (Figure 73). Select the non-software appliance type as FP Flow Processor (LA and TA) 1799 and select Next.

Figure 73 Non-Software Appliance Assignment Options



The Type of Setup page appears. Select the Normal Setup (default) option and select Next.

Figure 74 Setup Options



The Select Continent/Area page appears. Select the time zone continent or area as required and select Next. The default value is America.

Figure 75

Select Continent/Area Options

Select Continent/Area

Select a time zone continent/area: _____

- ☐ 0 Africa
- ☒ 1 America
- ☐ 2 Antarctica
- ☐ 3 Arctic
- ☐ 4 Asia
- ☐ 5 Atlantic
- ☐ 6 Australia
- ☐ 7 Europe
- ☐ 8 GMT
- ☐ 9 Indian
- ☐ 10 Pacific
- ☐ 11 UTC

< Next > < Back > < Cancel >

The Time Zone Options page appears (Figure 76). Select the time zone city or region as required and select Next. The default value is New-York (Eastern (most areas)).

Figure 76

Time Zone Options

Time Zone Selection

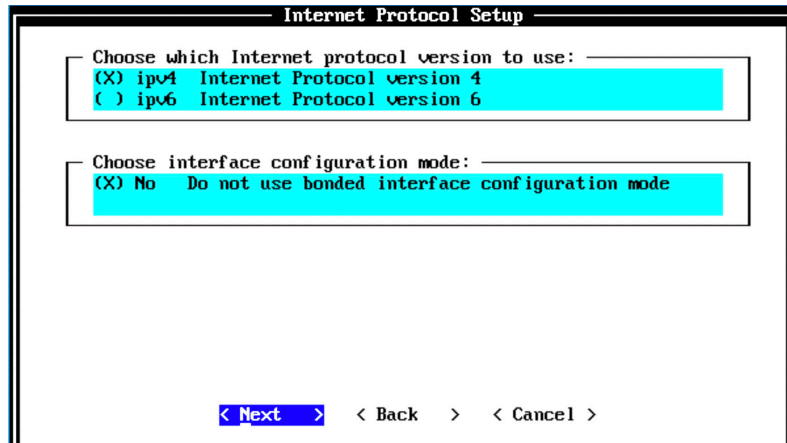
Select a time zone city or region: _____

- ☐ 94 Miquelon
- ☐ 95 Moncton (Atlantic - New Brunswick)
- ☐ 96 Monterrey (Central Time - Durango; Coahuila, Nuevo Leon, Tam)
- ☐ 97 Montevideo
- ☐ 98 Montserrat
- ☐ 99 Nassau
- ☒ 100 New_York (Eastern (most areas))
- ☐ 101 Nipigon (Eastern - ON, QC (no DST 1967-73))
- ☐ 102 Nome (Alaska (west))
- ☐ 103 Noronha (Atlantic islands)
- ☐ 104 North_Dakota/Beulah (Central - ND (Mercer))
- ☐ 105 North_Dakota/Center (Central - ND (Oliver))
- ☐ 106 North_Dakota/New_Salem (Central - ND (Morton rural))
- ☐ 107 Ojinaga (Mountain Time US - Chihuahua (US border))

< Next > < Back > < Cancel >

The Internet Protocol Setup page is next. By default, the Internet Protocol version is selected as IPv4 Internet Protocol version 4. You might select IPv6 Internet Protocol version 6, as required. Then select No as the value for Do not use bonded interface configuration mode. You might use the bonded interface configuration mode, as required. Select Next.

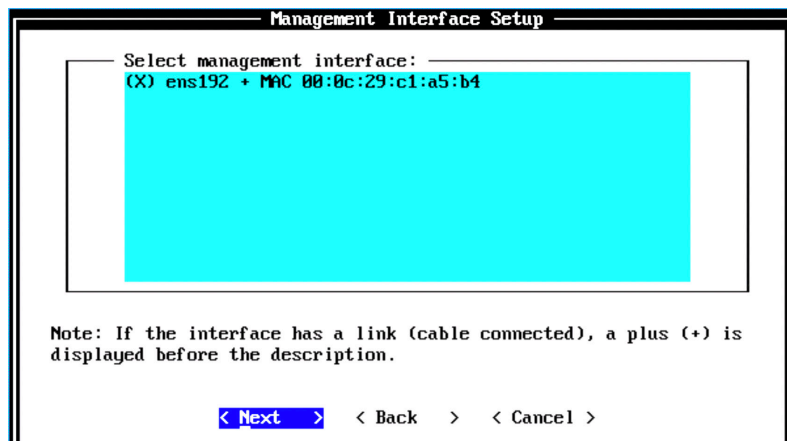
Figure 77 *Internet Protocol Setup Options*



The Management Interface Setup page appears (Figure 78). Select the management interface that you want to use and select Next.

NOTE The list shown will depend on the number of NIC Cards on the hardware that you are installing JSA. All available interfaces will be displayed in this window.

Figure 78 *Management Interface Setup Options*



The Network Information Setup page appears (Figure 79). Configure with the following network settings:

- 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.
- Email Server—Enter the email server. If you do not have an e-mail server, type localhost in this field.

Figure 79 *Network Information Setup Options*

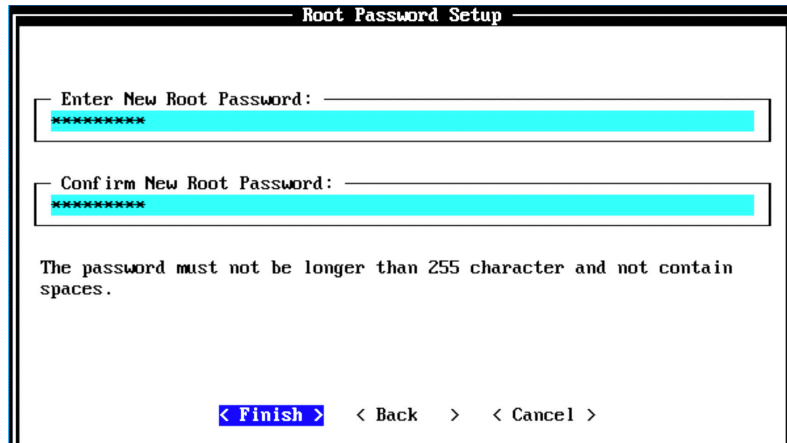
The screenshot shows a window titled "Network Information Setup". Inside, there is a section titled "Enter network information to use:". Below this, there are several input fields with labels: "Hostname:", "IP Address:", "Network Mask:", "Gateway:", "Primary DNS:", "Secondary DNS:", "Public IP:", and "Email Server:". The "Network Mask" field is pre-filled with "255.255.255.0". The "Email Server" field is pre-filled with "localhost". At the bottom of the window, there are three buttons: "< Next >", "< Back", and "< Cancel >".

Select Next to check if the network settings are validated. This may take a few minutes. Once network settings are validated successfully, the Root Password Setup page will appear (Figure 80).

Configure the root password required to log in to the JSA CLI. In the Enter New Root Password field, enter a root password that meets the following criteria: contains at least five characters, contains no spaces, and can include the following special characters: @, #, ^, and *.

Re-enter the root password in the Confirm New Root Password field and select Finish.

Figure 80 Root Password Options



Root Password Setup

Enter New Root Password:

Confirm New Root Password:

The password must not be longer than 255 character and not contain spaces.

< Finish >
< Back
>
< Cancel
>

When you select Finish, the installation process starts. This process typically takes several minutes. Although it might appear as if the system is not responding at times, wait for the installation to complete. The output shown in Figure 81 indicates a successful installation of a flow processor.

Figure 81 Installing Changes

```

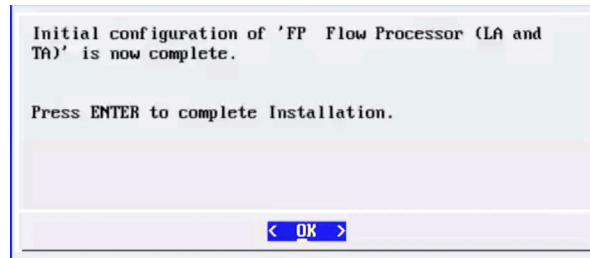
Installing Qradar changes...
Activating system with key 2E253S-5G564H-6L725U-744U0X.
Appliance ID is 1799.
Installing 'FP Flow Processor (LA and TA)' with id 1799.
Configuring network...
Setting current date and time.
New date of '2019/12/01 05:25:27' was specified 169 seconds ago...
Setting date and time to '20191201 05:28:16'...
Running changeQradarPassword
Stopping hostcontext
Sun Dec 1 05:28:32 EST 2019 [setup-imq.sh] OK: IMQ Setup Completed
Updating db user password
Applying replication db file...done!
Running replication setup...done!
Modifying postgresql config...done!
Running changeQUMPPassword
Setting email server to localhost
Running FinalSetup
Updating iptables firewall rules.
Restarting system services:
- syslog-ng
- hostcontext
- hostservices
Running restartServices
Restarting system services: syslog-ng.
Non-console setup, stopping services: hostcontext hostservices java.
Restarting services:
- hostservices
- hostcontext
Failed to start hostcontext!
OK: Configuration of host FP-jsa as a non-console completed.
qradar_setup.py: End: 0
Running: /opt/qradar/bin/after_services_up.sh

```

Once the installation is complete, a final completion message is displayed (Figure 82). Click OK.

Figure 82

Installation Complete



Verification

To verify the successful installation of a flow processor, run the following command on the console:

```
Run less /etc/.appliance_name
```

The output displays 1799 as the appliance installed. Ping the default gateway to ensure that the connectivity is fine. You can also use the `ifconfig` command to view the IP address details of the appliance.

Next Steps

After you have completed installing a flow processor, you can add the flow processor to a Threat Analytics console using JSA web UI. For more information about adding a flow processor, see *Add a Flow Processor to Threat Analytics*.

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system before the default license expires.

For more information about applying a license, see section *Apply a License to JSA*.

Add a Flow Processor to Threat Analytics

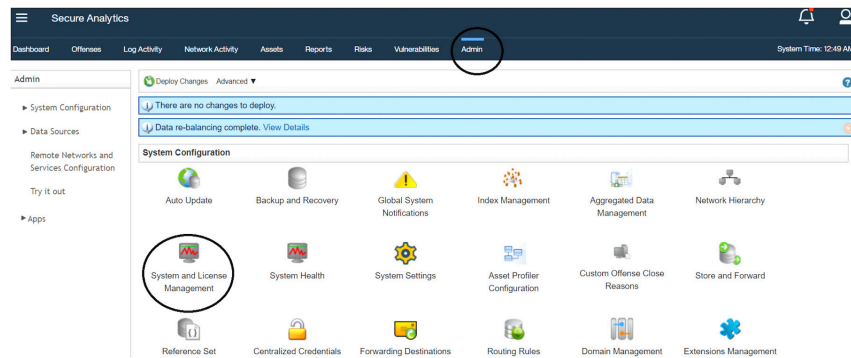
Now let's add managed hosts, such as event and flow collectors, event and flow processors, and data nodes, to distribute data collection and processing activities across your JSA deployment.

NOTE Verify that the managed host has the same JSA version and patch as the JSA console that you are using to manage it and note that flow processors *cannot* be added to LM/LA.

Adding flow processors help to distribute the collection of flows. The flow collection and processing load, will be on the flow processor rather than on console. Also, when flow collection needs to happen between different geographical locations, flow processors conserve WAN bandwidth by locally storing the flows and not sending the entire flow data to the console. Another use case for flow processor nodes are to comply with data compliance regulations.

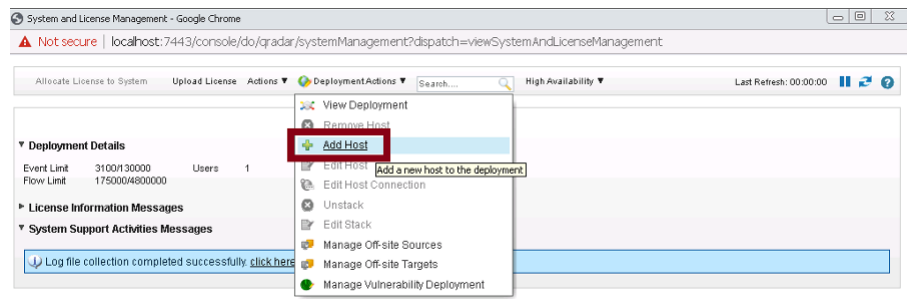
To add a flow processor to *Threat Analytics*, log in to the JSA web UI. On the navigation menu, click Admin. The Admin page appears (Figure 83). In the System Configuration section, click System and License Management. We've done this before.

Figure 83 System and License Management



The System and License Management page appears. On the navigation menu, select Deployment Actions > Add Host.

Figure 84 Deployment Actions > Add Host



Add Management Host appears (Figure 85). Enter the fixed IP address of the flow processor host you want to add in the Host IP field. Enter the root password for the host IP in the Host Password field and re-enter the root password in the Confirm Password field. Click Add when complete.

Figure 85 Add Managed Host

Add Managed Host

Before you add a managed host, make sure the managed host includes the SIEM software. The IP of the host is required as well as the root password. Hover over label fields for more information.

Host IP:

Host Password:

Confirm Password:

Encrypt Host Connections: ☐

Encryption Compression: ☐

Network Address Translation: ☐

NAT Group:

Public IP:

Add **Cancel**

NOTE If you are using NAT or want to use an encrypted communication between FP and console, select the other options accordingly.

A pop-up appears (Figure 86) displaying the status of the host being added to the network.

Figure 86 Host is Being Added to Deployment

Host is Being Added to Deployment

The host information that was entered is being added to the deployment. This managed host is not currently part of the deployment. To complete the process, click **Deploy Changes** on the **Admin tab** toolbar after this dialog closes.

Step 1 of 10 Clearing known hosts file for IP (1.1.1.1)

Step 2 of 10 Checking if the host is at a compatible version.

Step 3 of 10 Writing firewall rules for host.

Step 4 of 10 Communicating with host to find valid application install.

Step 5 of 10 Checking if this host is valid to be added as a managed host.

Step 6 of 10 Setting up ssh keys for host.

Step 7 of 10 Pushing configuration files to the host.

Step 8 of 10 Pushing token for host to console communication.

Step 9 of 10 Creating default license for host.

Step 10 of 10 Updating database on host and starting services. This may take a while.

Add **Cancel**

After the host is successfully added, the new host is listed on the System and License Management page.

Figure 87

Host Successfully Added

Display

Systems

Deployment Details

Event Limit

500/30000

Users

1

Flow Limit

75000/4800000

License Information Messages

System Support Activities Messages

Host Name	Host IP	Appliance Type	Version	Serial Number	Host Status	License Expiration Date	License Status
FP-isa	1799 - Flow Processor	7.3.3	VMware-56 4d...	Active	Perpetual	Deployed	
TM-isa (co...	3199 - Console	7.3.3	VMware-56 4d...	Active	Jan 25, 2020	Deployed	

Note that at this point, the new host is not deployed. To deploy the changes, go back to the Admin page. The changes that need to be deployed are shown on top of the page. Click View Details to see the changes.

Figure 88

Undeployed Changes

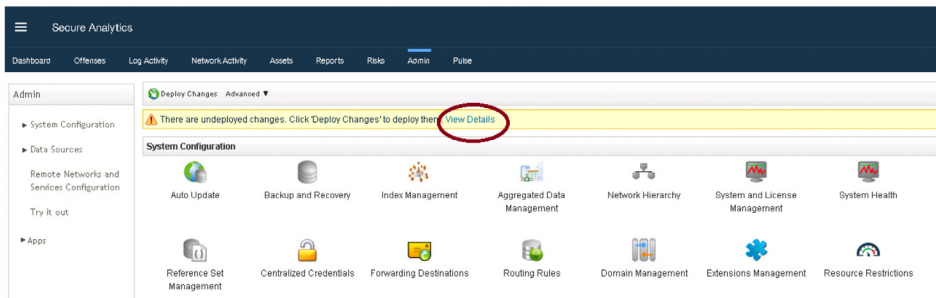
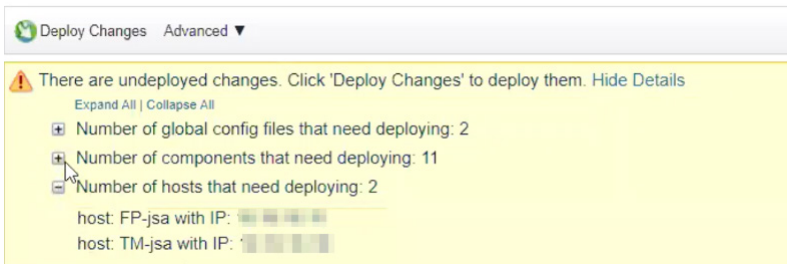


Figure 89

Changes to be Deployed



Click Deploy Changes and a confirmation page appears asking for confirmation to deploy the changes, as shown in Figure 90. Click Continue to deploy the changes.

Figure 90 Deployment Confirmation



The deployment starts. This process typically takes several minutes. Although it might appear as if the system is not responding at times, wait for the deployment to complete. The JSA web UI displays the progress in the deployment process.

When the deployment process is complete, you will see the status as *Success* for all the hosts. This means that the flow processor is successfully added to the deployment. You can now point the flow sources to send flows to the flow processor.

Next Steps

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system before the default license expires.

For more information about applying a license, see section *Apply a License to JSA*.

Install and Configure a JSA Data Node

A data node is an appliance that you can add to your event and flow processors to increase storage capacity and improve search performance. You can add an unlimited number of data nodes to your JSA deployment, and they can be added at any time. Data nodes enable new and existing JSA deployments to add storage and processing capacity on demand, as required. This installation procedure is applicable to both JSA hardware and virtual appliances.

To complete the installation and configuration of a data node:

- Install the data node using the instructions in this section.
- Add the data node to threat analytics or log analytics console using the instructions provided in section *Add Data Nodes to Threat Analytics* or *Log Analytics Deployment*.
- Apply a license to the data node using the instructions *Apply a License to JSA*.

Before You Begin

Before you start the installation, verify:

- The required hardware is installed (in case of appliances).
- You have the required license key for your appliance.
- A keyboard and monitor are connected by using the VGA connection (in case of hardware appliances).
- There are no expired licenses on either the console or the managed hosts.
- Software versions for all JSA appliances in a deployment has the same version and patch level. Note that deployments that use different versions of software are not supported.

Keep the following information at hand for installation:

- Hostname
- IP address
- Network mask
- Default gateway address
- Primary Domain Name System (DNS) server address
- Secondary DNS server address (Optional)
- (Optional) Public IP address for networks using Network Address Translation (NAT)
- (Optional) Email server name

Step-by-Step Procedure

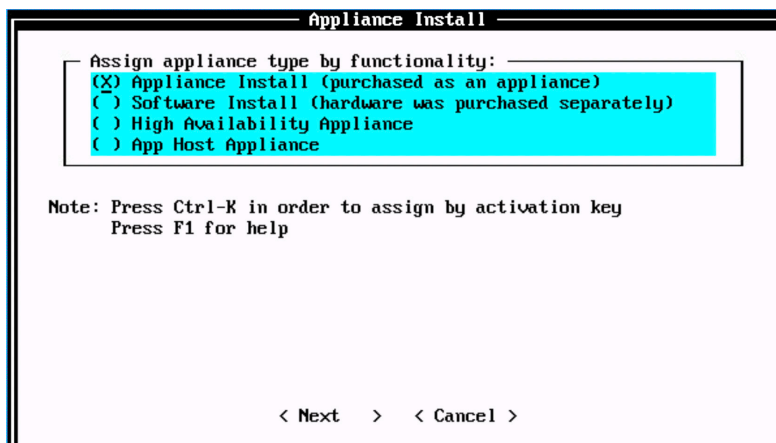
Follow the steps in the installation wizard for the hardware or virtual appliance type you are creating.

The JSA installation wizard allows you to use only certain keyboard keys to navigate through the installation options. Table P1 lists these keys along with how you can use them.

Log in as the root user at the prompt (a password is not required). If you are prompted for a password, there is some error with the installation. Contact <https://support.juniper.net/support/>.

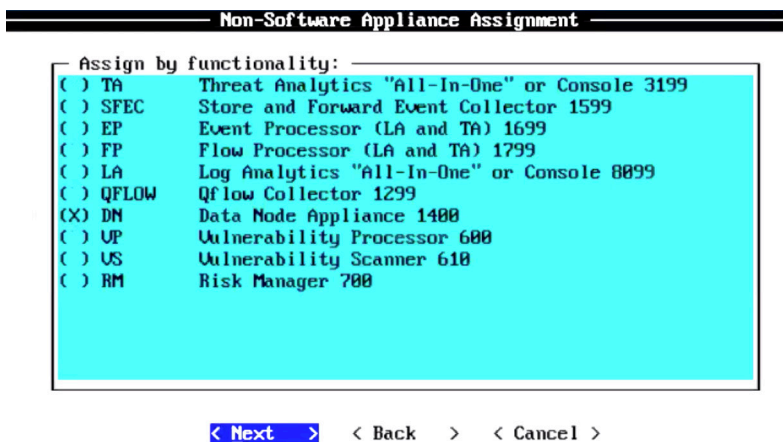
Read and accept the EULA license and proceed providing information in the installation wizard when prompted. After accepting the EULA license, the Appliance Install page appears (Figure 91). Select Appliance Install (purchased as an appliance). Choose this option if you have purchased JSA appliances or wish to install virtual machines and select Next.

Figure 91 *Appliance Install Options*



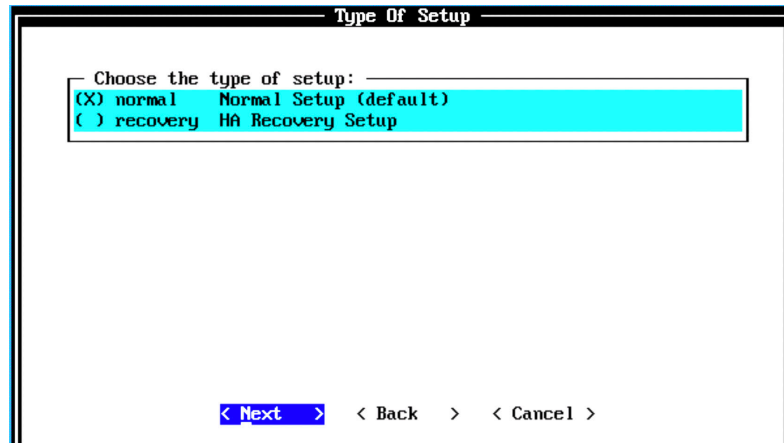
The Non-Software Appliance Assignment page appears. Select the non-software appliance type as DN Data Node Appliance 1400 and select Next.

Figure 92 *Non-Software Appliance Assignment Options*



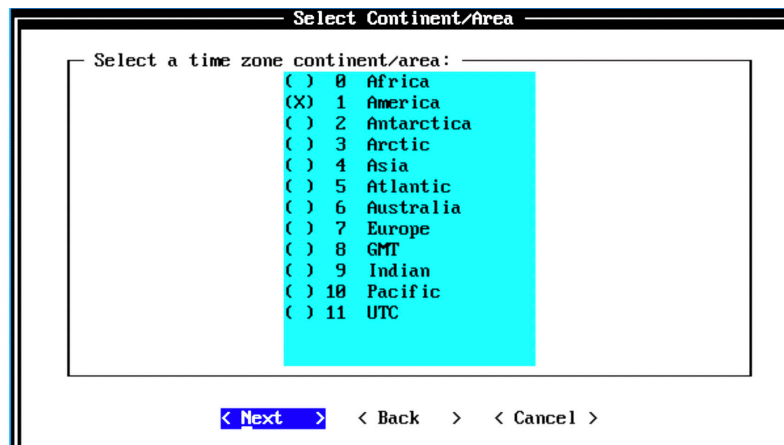
The Type of Setup page appears. Select the Normal Setup (default) option and select Next.

Figure 93 Setup Options



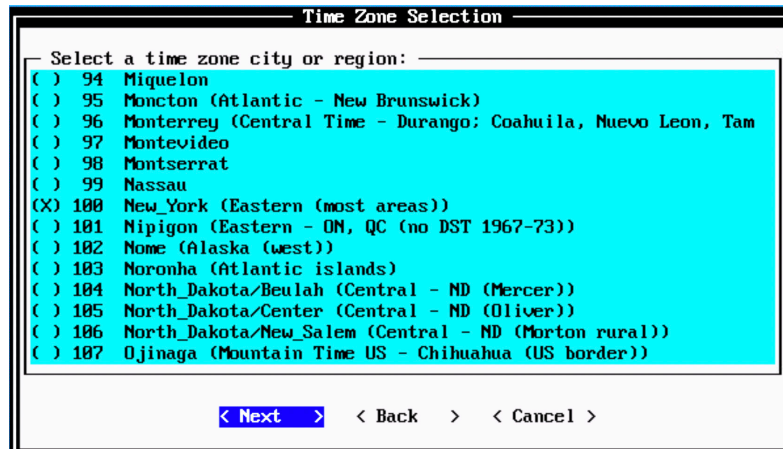
The Select Continent/Area Options page appears. Select the time zone continent or area as required and select Next. The default value is America.

Figure 94 Select Continent/Area Options



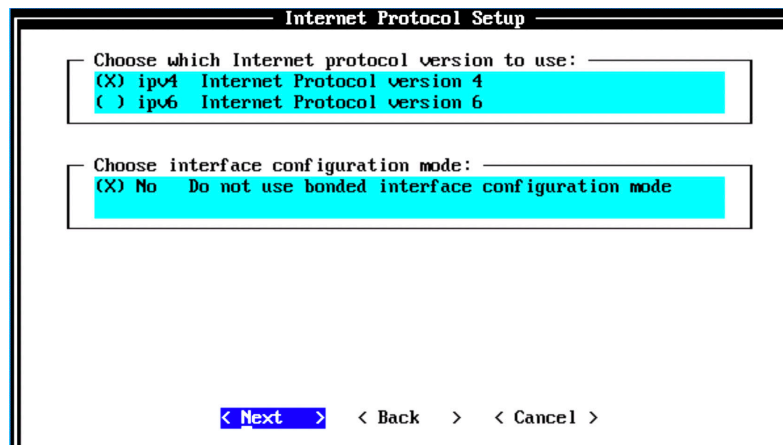
The Time Zone Selection page appears. Select the time zone city or region as required and select Next. The default value is New_York (Eastern (most areas)).

Figure 95 Time Zone Options



The Internet Protocol Setup page appears (Figure 96). By default, the Internet Protocol version is selected as IPv4 Internet Protocol version 4. You can select IPv6 Internet Protocol version 6 if required. Select No as the value for Do not use bonded interface configuration mode. You can use the bonded interface configuration mode if required. Select Next.

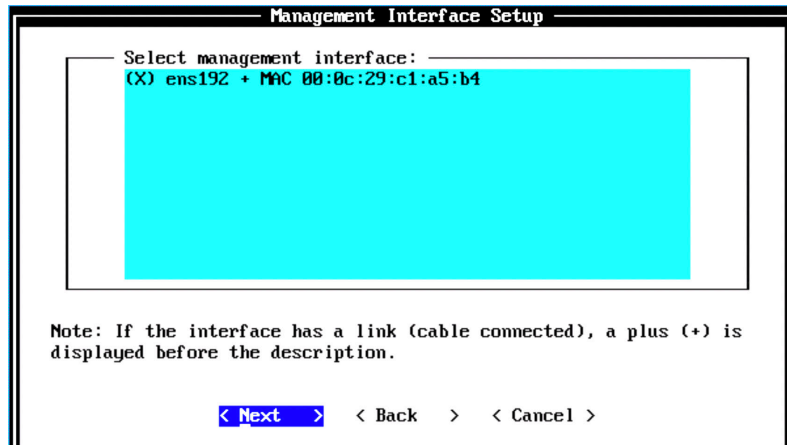
Figure 96 Internet Protocol Setup Options



The Management Interface Setup page appears. Select the management interface that you want to use and select Next.

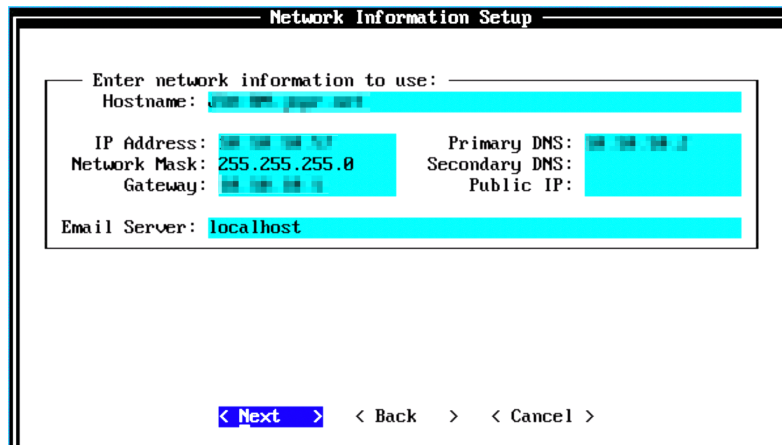
NOTE The list shown depends on the number of NIC Cards on the hardware that you are installing JSA on. All the available interfaces will be displayed in this section.

Figure 97 Management Interface Setup Options



The Network Information Setup page appears. Configure the following settings:

- 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.
- Email Server—Enter the email server. If you do not have an e-mail server, type localhost in this field.

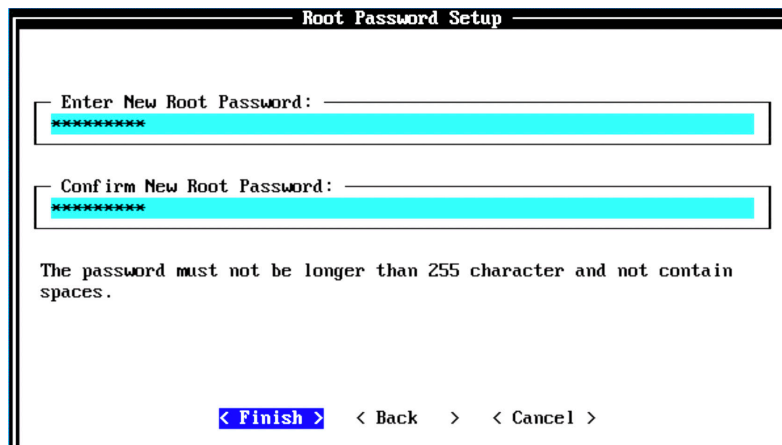
Figure 98 Network Information Setup Options

The dialog box is titled "Network Information Setup". It contains a section titled "Enter network information to use:" with several input fields. The fields are: Hostname (with a blue highlight), IP Address (with a blue highlight), Network Mask (with the value "255.255.255.0"), Gateway (with a blue highlight), Primary DNS (with a blue highlight), Secondary DNS (with a blue highlight), Public IP (with a blue highlight), and Email Server (with the value "localhost"). At the bottom of the dialog box, there are three buttons: "< Next >" (highlighted in blue), "< Back >", and "< Cancel >".

Select Next.

The network settings are validated. This may take a few minutes. Once network settings are validated successfully, the Root Password Setup page appears. Configure the root password required to login to the JSA Command Line Interface (CLI). In the Enter New Root Password field, enter a root password that meets the following criteria: contains at least 5 characters, contains no spaces and can include the following special characters: @, #, ^, and *.

Re-enter the root password in the Confirm New Root Password field and select Finish.

Figure 99 Root Password Options

The dialog box is titled "Root Password Setup". It contains two input fields: "Enter New Root Password:" and "Confirm New Root Password:". Both fields have a blue highlight and contain a series of asterisks. Below the input fields, there is a text message: "The password must not be longer than 255 character and not contain spaces." At the bottom of the dialog box, there are three buttons: "< Finish >" (highlighted in blue), "< Back >", and "< Cancel >".

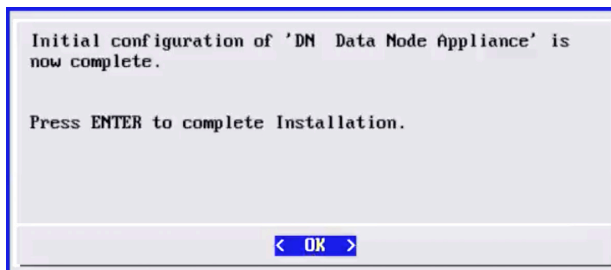
When you select Finish, the installation process starts. This process typically takes several minutes. Although it might appear as if the system is not responding at times, wait for the installation to complete. The output shown in Figure 100 indicates a successful installation of a JSA data node.

Figure 100 *Installing Changes*

```
Installing Qradar changes...
Activating system with key 1X2N3L-664S48-5U1P1M-3B2H1M.
Appliance ID is 1488.
Installing 'DN Data Node Appliance' with id 1488.
Configuring network...
Setting current date and time.
New date of '2019/11/29 07:08:50' was specified 331 seconds ago...
Setting date and time to '20191129 07:14:21'...
Running changeQradarPassword
Stopping hostcontext
Fri Nov 29 07:14:37 EST 2019 [setup-inq.sh] OK: IMQ Setup Completed
Updating db user password
Applying replication db file...done!
Running replication setup...done!
Modifying postgresql config...done!
Running changeQMFPassword
Setting email server to localhost
Running FinalSetup
Updating iptables firewall rules.
Restarting system services:
- syslog-ng
- hostcontext
- hostservices
Running restartServices
Restarting system services: syslog-ng.
Non-console setup, stopping services: hostcontext hostservices java.
Restarting services:
- hostservices
- hostcontext
Failed to start hostcontext!
OK: Configuration of host jsa-dn as a non-console completed.
qradar_setup.py: End: 0
Running: /opt/qradar/bin/after_services_up.sh
```

Once the installation is complete, a final completion message is displayed. Click OK.

Figure 101 *Installation Complete*



Verification

To verify the successful installation of a JSA data node on a virtual machine, run the following command on the console:

```
Run less /etc/.appliance_name
```

The output displays `1400` as the appliance installed. Ping the default gateway to ensure that the connectivity is fine. You can also use the `ifconfig` to view the IP address details of the appliance.

Next Steps

After you have completed installing a data node, you can add the data node to a Threat Analytics or Log Analytics console using JSA web UI. For more information about adding a Data Node, see *Add Data Nodes to Threat Analytics or Log Analytics Deployment*.

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system before the default license expires.

For more information about applying a license, see section *Apply a License to JSA*.

Add Data Nodes to Threat Analytics or Log Analytics Deployment

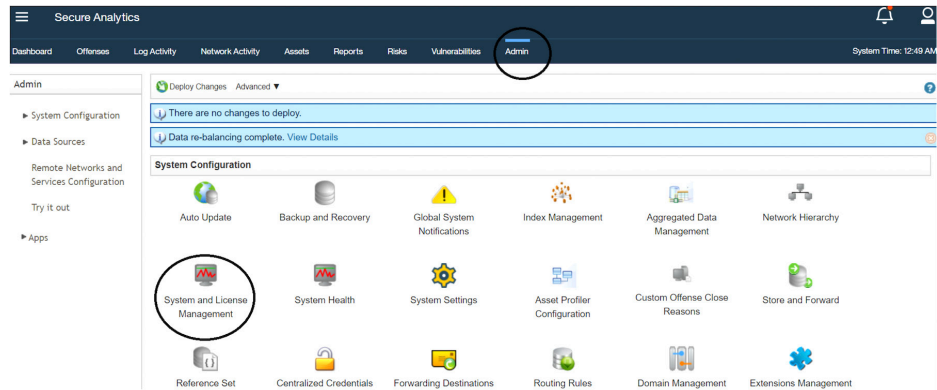
You can add managed hosts, such as event and flow collectors, event and flow processors, and data nodes to distribute data collection and processing activities across your JSA deployment.

First verify that the managed host has the same JSA version and patch as the JSA console that you are using to manage it.

NOTE You can add data nodes to TA AIO or LA AIO or dedicated event processors and flow processors to increase their storage capacity. You can add any number of data nodes to the same EP or FP. However, you cannot attach the same DN to multiple EPs or FPs.

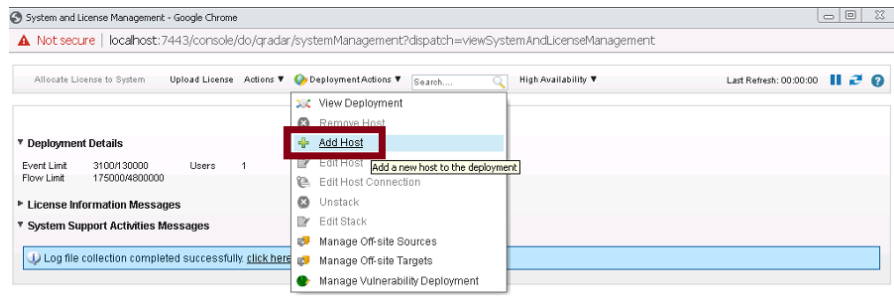
To add data nodes to Threat Analytics, log in to the JSA web UI. On the navigation menu, click Admin. The Admin page appears (Figure 102). In the System Configuration section, click System and License Management.

Figure 102 System and License Management



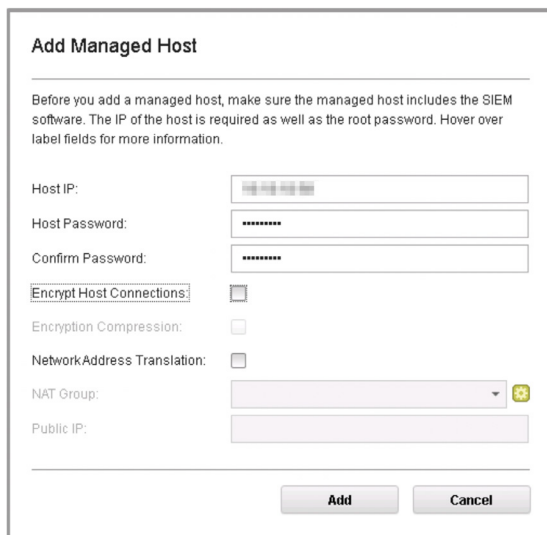
The System and License Management page appears. On the navigation menu, select Deployment Actions > Add Host.

Figure 103 Deployment Actions > Add Host



The Add Management Host page appears (Figure 104). Enter the fixed IP address of the data node you want to add in the Host IP field. Enter the root password for the host IP in the Host Password field and re-enter the root password in the Confirm Password field. When complete click Add.

Figure 104 Add Managed Host



Add Managed Host

Before you add a managed host, make sure the managed host includes the SIEM software. The IP of the host is required as well as the root password. Hover over label fields for more information.

Host IP:


Host Password:

Confirm Password:

Encrypt Host Connections: ☐

Encryption Compression: ☐

NetworkAddress Translation: ☐

NAT Group: 

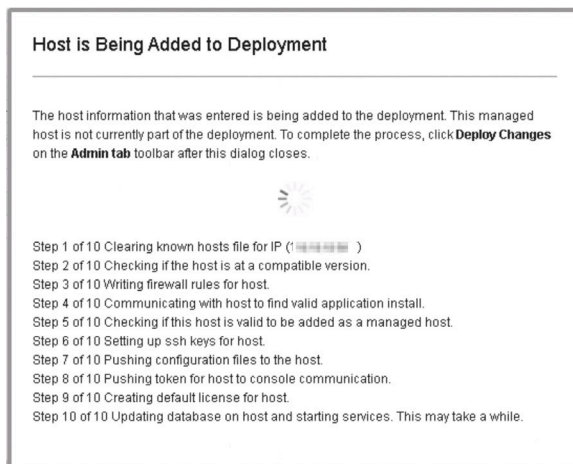
Public IP:

Add **Cancel**

NOTE If you are using NAT or want to use an encrypted communication between DN and EP or FP, select the other options accordingly.


A pop-up appears (Figure 105) displaying the status of the host being added to the network.

Figure 105 Host is Being Added to Deployment



Host is Being Added to Deployment

The host information that was entered is being added to the deployment. This managed host is not currently part of the deployment. To complete the process, click **Deploy Changes** on the **Admin tab** toolbar after this dialog closes.



Step 1 of 10 Clearing known hosts file for IP ()

Step 2 of 10 Checking if the host is at a compatible version.

Step 3 of 10 Writing firewall rules for host.

Step 4 of 10 Communicating with host to find valid application install.

Step 5 of 10 Checking if this host is valid to be added as a managed host.

Step 6 of 10 Setting up ssh keys for host.

Step 7 of 10 Pushing configuration files to the host.

Step 8 of 10 Pushing token for host to console communication.

Step 9 of 10 Creating default license for host.

Step 10 of 10 Updating database on host and starting services. This may take a while.

During the process, the Modify Data Node Appliance Connection page appears, as shown in Figure 106. You must attach the data node to an event processor or a flow processor.

Figure 106 Modify Data Node Appliance Connection Page

Modify Data Node Appliance Connection

Select a Host's Event Processor to connect this Host's Data Node.
NOTE: only eligible hosts will appear in the options.
 The (*) denotes which host contains the destination connection.

EP-isa [1799 - Flow Processor]

Save Cancel

Select the required event processor or flow processor to which you want to attach the data node from the list and click Save. After the host is added successfully, it will be listed on the System and License Management page.

Figure 107 Host Successfully Added

Display Systems ▼

▼ Deployment Details

Event Limit 3100/130000 Users 1

Flow Limit 175000/4800000

▼ License Information Messages

▼ System Support Activities Messages

Host Name	Host IP	Appliance Type	Version	Serial Number	Host Status
vjsaCN (data node)	10.10.10.10	1400 - Data Node	7.3.3	VMware-56 4d 8...	Active
FP-isa-new (HA)	10.10.10.11	1799 - Flow Processor	7.3.3	VMware-56 4d ...	Active
FP-isa-new-primary/juniper.net (prim...	10.10.10.12	1799 - Flow Processor	7.3.3	VMware-56 4d c...	Standby
FP-isa-new-secondary/juniper.net (s...	10.10.10.13	1799 - Flow Processor	7.3.3	VMware-56 4d c...	Active
EP-isa	10.10.10.14	1699 - Event Processor	7.3.3	VMware-56 4d f...	Active
TM-isa (console)	10.10.10.15	3199 - Console	7.3.3	VMware-56 4d 0...	Active

Note that at this point, the new host is not yet deployed. So, close the System and License Management page and go to the Admin page. The changes that need to be deployed are shown on top of the page.

Click View Details to see the changes.

Figure 108 Undeployed Changes

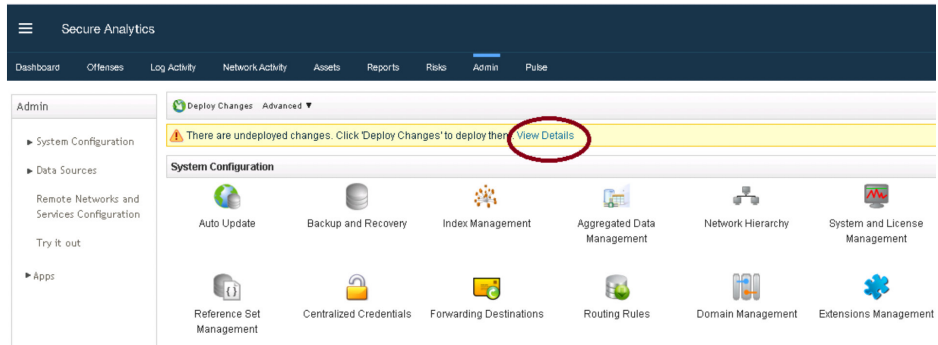
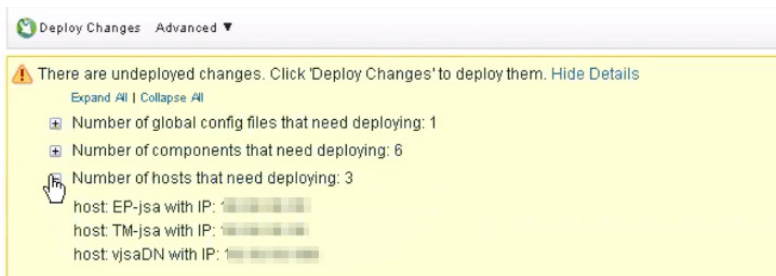


Figure 109 Changes to be Deployed



Click Deploy Changes. A confirmation page appears asking for confirmation to deploy the changes, as shown in figure. Click Continue to deploy the changes.

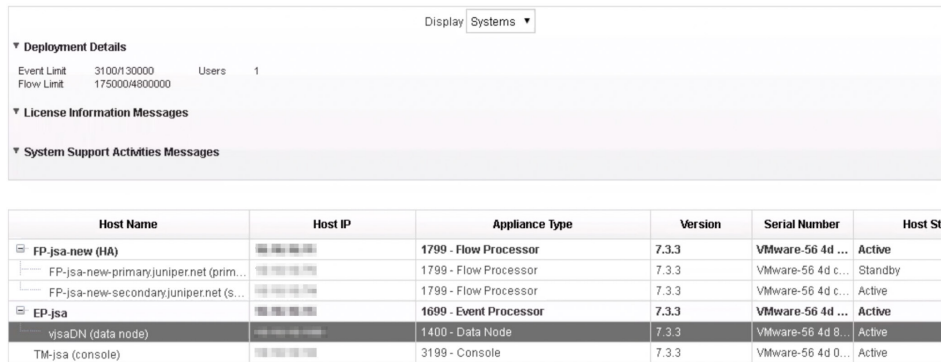
Figure 110 Deployment Confirmation



Okay. The deployment starts. The process can take several minutes. Although it might appear as if the system is not responding at times, wait for the deployment to complete. The JSA web UI will display the progress in the deployment process.

When complete, you will see the status as *Success* for all the hosts. This means that the data nodes are successfully added to the deployment, as shown in Figure 111.

Figure 111 Data Node Added Successfully



Display Systems ▼

▼ Deployment Details

Event Limit 3100/130000 Users 1

Flow Limit 175000/4800000

▼ License Information Messages

▼ System Support Activities Messages

Host Name	Host IP	Appliance Type	Version	Serial Number	Host St
FP-jsa-new (HA)		1799 - Flow Processor	7.3.3	VMware-56 4d ...	Active
FP-jsa-new-primaryjuniper.net (prim...		1799 - Flow Processor	7.3.3	VMware-56 4d c...	Standby
FP-jsa-new-secondaryjuniper.net (s...		1799 - Flow Processor	7.3.3	VMware-56 4d c...	Active
EP-jsa		1699 - Event Processor	7.3.3	VMware-56 4d ...	Active
vjsaDN (data node)		1400 - Data Node	7.3.3	VMware-56 4d 8...	Active
TM-jsa (console)		3199 - Console	7.3.3	VMware-56 4d 0...	Active

Next Steps

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system before the default license expires.

For more information about applying a license, see section *Apply a License to JSA*.

Install and Configure a Store and Forward Event Collector

SFEC is a dedicated event collector that collects only events but does not process those events. This is because it doesn't include an on-board event processor. By default, a dedicated event collector continuously forwards events to the event processor. However, you can use the scheduling feature to store events temporarily on the event collector (during your business hours, for example), or forward the events to an event processor when the transmission does not negatively affect your network bandwidth (for example, such as during non-business hours). Another typical use case for SFEC is on submarines, where the network connectivity or bandwidth is available only for a specific period.

When the events are not forwarded, they are stored locally on the appliance. These events are not accessible on the JSA console web UI. Here's how you can install and configure an SFEC:

- Install the SFEC using the instructions in this section.
- Add the SFEC to threat analytics or log analytics using the instructions provided in section Add SFEC to Threat Analytics or Log Analytics.

- Apply a license to SFEC using the instructions [Apply a License to JSA](#).

Before You Begin

Before installation you'll need the following:

- The required hardware is installed (in case of appliances).
- You have the required license key for your appliance.
- A keyboard and monitor are connected by using the VGA connection (in case of hardware appliances).
- There are no expired licenses on either the console or the managed hosts.
- Software versions for all JSA appliances in a deployment has the same version and patch level. Note that deployments that use different versions of software are not supported.

And you'll need the following information to complete the installation:

- Hostname
- IP address
- Network mask
- Default gateway address
- Primary Domain Name System (DNS) server address
- Secondary DNS server address (Optional)
- (Optional) Public IP address for networks using Network Address Translation (NAT)
- Email server name

Step-by-Step Procedure

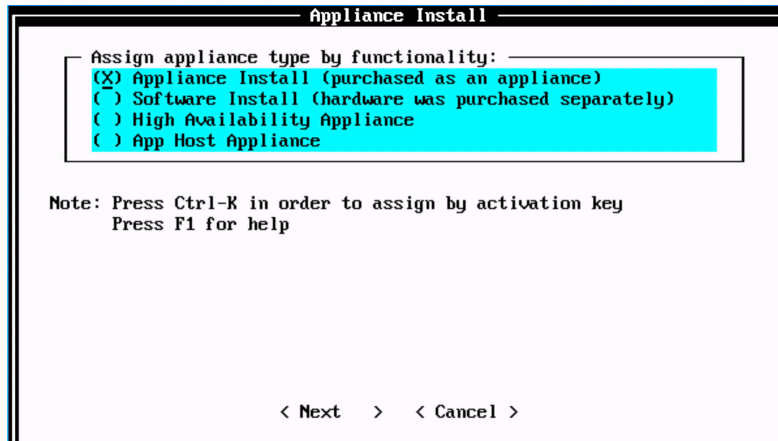
Follow the steps in the installation wizard for the hardware or virtual appliance type you are creating.

The JSA installation wizard allows you to use only certain keyboard keys to navigate through the installation options. Table P1 lists these keys along with how you can use them.

Log in as the root user at the prompt (a password is not required). If you are prompted for a password, there is some error with the installation. Contact <https://support.juniper.net/support/>.

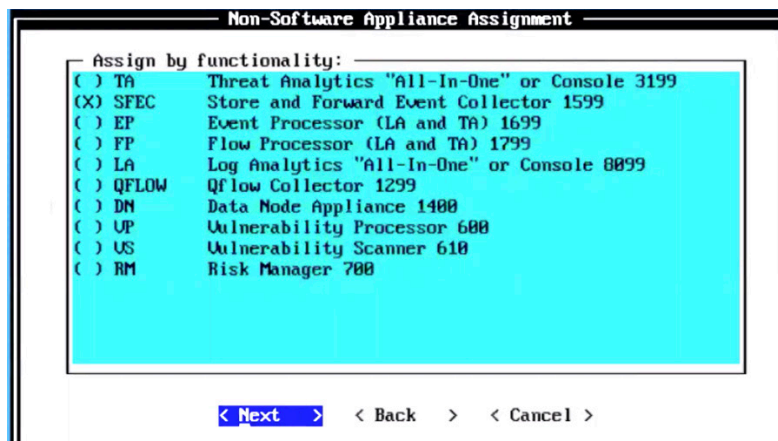
Read and accept the EULA license and the Appliance Install page will appear. Select Appliance Install (purchased as an appliance). Choose this option if you have purchased JSA appliances or wish to install virtual machines. Select Next.

Figure 112 Appliance Install Options



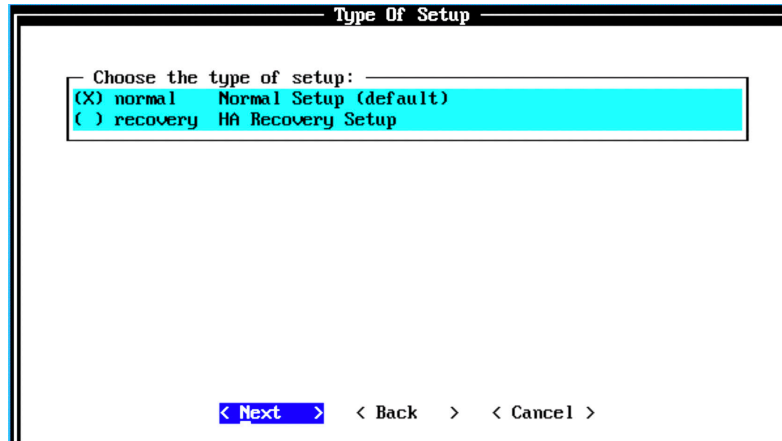
The Non-Software Appliance Assignment page appears (Figure 113). Select the non-software appliance type as SFEC Store and Forward Event Collector 1599 and then select Next.

Figure 113 Non-Software Appliance Assignment Options



The Type Of Setup page appears. Select the Normal Setup (default) option and then select Next.

Figure 114 *Setup Options*



Type Of Setup

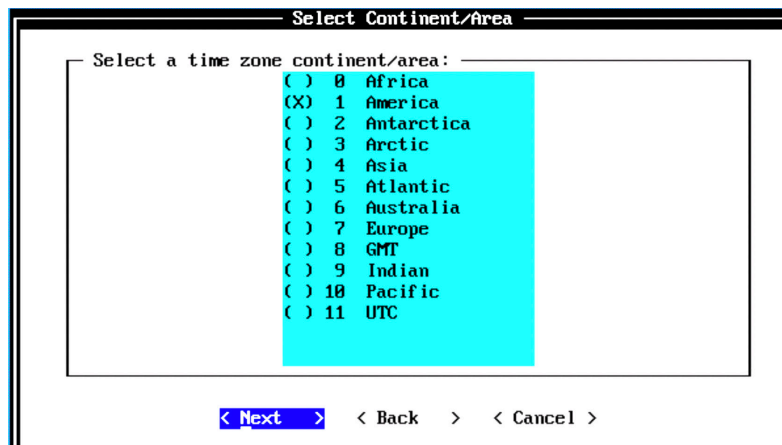
Choose the type of setup: —

- ☒ normal Normal Setup (default)
- ☐ recovery HA Recovery Setup

< Next > < Back > < Cancel >

The Select Continent/Area page appears. Select the time zone continent or area as required and select Next. The default value is America.

Figure 115 *Select Continent/Area Options*



Select Continent/Area

Select a time zone continent/area: —

- ☐ 0 Africa
- ☒ 1 America
- ☐ 2 Antarctica
- ☐ 3 Arctic
- ☐ 4 Asia
- ☐ 5 Atlantic
- ☐ 6 Australia
- ☐ 7 Europe
- ☐ 8 GMT
- ☐ 9 Indian
- ☐ 10 Pacific
- ☐ 11 UTC

< Next > < Back > < Cancel >

The Time Zone Selection page appears. Select the time zone city or region as required and select Next. The default value is New_York (Eastern (most areas)).

Figure 116 Time Zone Options

Time Zone Selection

Select a time zone city or region: _____

- ☐ 94 Miquelon
- ☐ 95 Moncton (Atlantic - New Brunswick)
- ☐ 96 Monterrey (Central Time - Durango: Coahuila, Nuevo Leon, Tam)
- ☐ 97 Montevideo
- ☐ 98 Montserrat
- ☐ 99 Nassau
- ☒ 100 New_York (Eastern (most areas))
- ☐ 101 Nipigon (Eastern - ON, QC (no DST 1967-73))
- ☐ 102 Nome (Alaska (west))
- ☐ 103 Noronha (Atlantic islands)
- ☐ 104 North_Dakota/Beulah (Central - ND (Mercer))
- ☐ 105 North_Dakota/Center (Central - ND (Oliver))
- ☐ 106 North_Dakota/New_Salem (Central - ND (Morton rural))
- ☐ 107 Ojinaga (Mountain Time US - Chihuahua (US border))

The Internet Protocol Setup page appears (Figure 116A). By default, the Internet Protocol version is selected as IPv4 Internet Protocol version 4. You can select IPv6 Internet Protocol version 6 if required. Select No as the value for Do not use bonded interface configuration mode. You can use the bonded interface configuration mode if required. Select Next.

Figure 116A Internet Protocol Setup Options

Internet Protocol Setup

Choose which Internet protocol version to use: _____

- ☒ ipv4 Internet Protocol version 4
- ☐ ipv6 Internet Protocol version 6

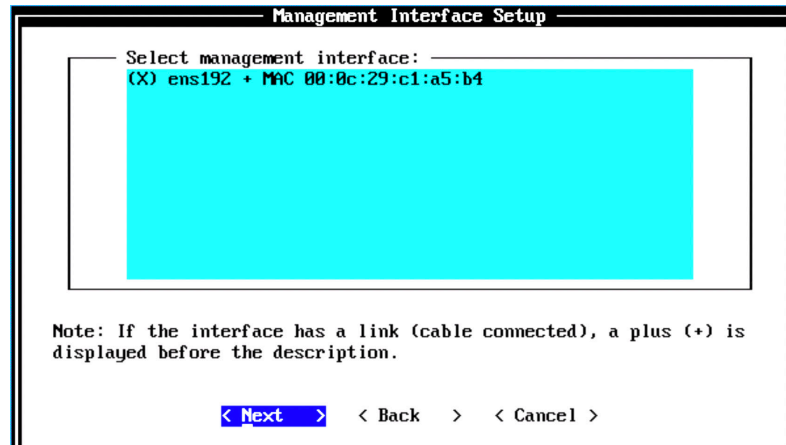
Choose interface configuration mode: _____

- ☒ No Do not use bonded interface configuration mode

The Management Interface Setup page appears. Select the management interface that you want to use and select Next.

NOTE The list shown will depend on the number of NIC Cards on the hardware that you are installing JSA on. All the available interfaces will be displayed in this section.

Figure 116B Management Interface Setup Options



The Network Information Setup page appears. Configure the following settings:

- 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.
- Email Server—Enter the email server. If you do not have an e-mail server, type localhost in this field.

Figure 116C Network Information Setup Options

Network Information Setup

Enter network information to use:

Hostname: [redacted]

IP Address: [redacted] Primary DNS: [redacted]

Network Mask: 255.255.255.0 Secondary DNS: [redacted]

Gateway: [redacted] Public IP: [redacted]

Email Server: localhost

< Next > < Back > < Cancel >

Select Next.

The network settings are being validated. This may take a few minutes. Once network settings are validated successfully, the Root Password Setup page appears (Figure 117). Configure the root password required to login to the JSA Command Line Interface (CLI). In the Enter New Root Password field, enter a root password that meets the following criteria: contains at least five characters, contains no spaces, can include the following special characters: @, #, ^, and *.

Re-enter the root password in the Confirm New Root Password field and select Finish.

Figure 117 Root Password Options

Root Password Setup

Enter New Root Password: [redacted]

Confirm New Root Password: [redacted]

The password must not be longer than 255 character and not contain spaces.

< Finish > < Back > < Cancel >

When you select Finish, the installation process starts. This process typically takes several minutes. Although it might appear as if the system is not responding at times, wait for the installation to complete. Figure 118 indicates that the installation process of an SFEC is underway.

Figure 118 *Installing Changes*

```
Installing Qradar changes...
Activating system with key 2F3C5Q-2H7534-6Q700N-711S1S.
Appliance ID is 1599.
Installing 'SFEC Store and Forward Event Collector' with id 1599.
Configuring network...
Setting current date and time.
New date of '2019/12/01 01:18:23' was specified 320 seconds ago...
Setting date and time to '20191201 01:15:43'...
Running changeQradarPassword
Stopping hostcontext
Sun Dec 1 01:15:58 EST 2019 [setup-img.sh] OK: IMQ Setup Completed
Updating db user password
Applying replication db file...done!
Running replication setup...done!
Modifying postgresql config...done!
Running changeQMPassword
Setting email server to localhost
Running FinalSetup
Updating iptables firewall rules.
Restarting system services:
- syslog-ng
- hostcontext
- hostservices
Running restartServices
Restarting system services: syslog-ng.
Non-console setup, stopping services: hostcontext hostservices java.
```

Once the installation is complete, a final completion message is displayed as shown in Figure 119. Click Ok.

Figure 119 *Installation Complete*

```
Initial configuration of 'SFEC Store and Forward Event
Collector' is now complete.
```

```
Press ENTER to complete Installation.
```

< OK >

Verification

To verify the successful installation of an SFEC, run the following command on the console:

```
Run less /etc/.appliance_name
```

The output displays 1599 as the appliance installed. Ping the default gateway to ensure that the connectivity is fine. You can also use the `ifconfig` command to view the IP address details of the appliance.

Next Steps

After you have completed installing an SFEC, you can add the SFEC to a Threat Analytics or Log Analytics console using JSA web UI. For more information about adding an SFEC, see the next section: *Add SFEC to Threat Analytics or Log Analytics*.

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system, before the default license expires.

For more information about applying a license, see section *Apply a License to JSA*.

Add SFEC to Threat Analytics or Log Analytics

SFEC is a dedicated event collector that collects only events and does not process those events. This is because it doesn't include an on-board event processor. By default, a dedicated event collector continuously forwards events to the event processor. However, you can use the scheduling feature to store events temporarily on the event collector (during your business hours, for example), or forward the events to an event processor when the transmission does not negatively affect your network bandwidth (for example, such as during non-business hours). Another typical use case for SFEC is on submarines, where the network connectivity or bandwidth is available only for specific period.

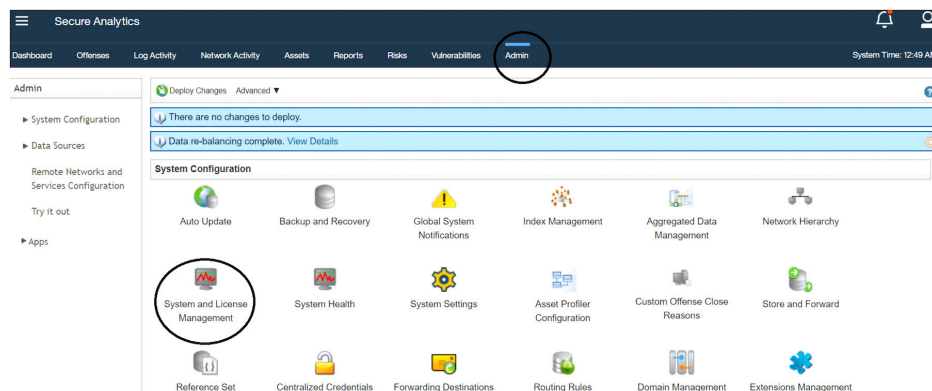
When the events are not forwarded, they are stored locally on the appliance. These events are not accessible on the JSA console web UI.

Ensure that the managed host has the same JSA version and patch as the JSA console that you are using to manage it.

NOTE SFEC can be attached to only event processors. You can attach multiple SFECs to the same event processors. However, you cannot attach the same SFEC to multiple event processors.

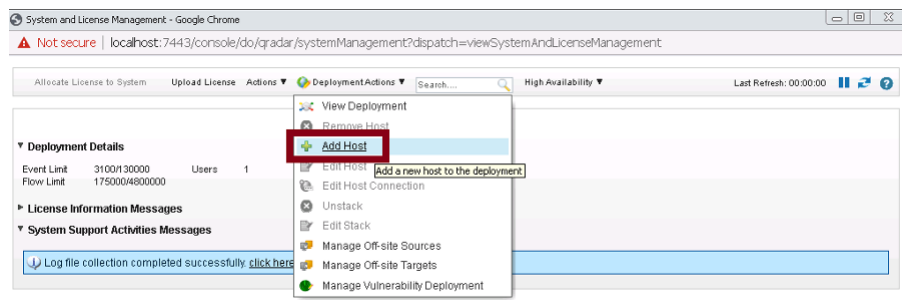
To add SFEC to Threat Analytics or Log Analytics, log in to the JSA web UI. On the navigation menu, click Admin. The Admin page appears (Figure 120). In the System Configuration section, click System and License Management.

Figure 120 System and License Management



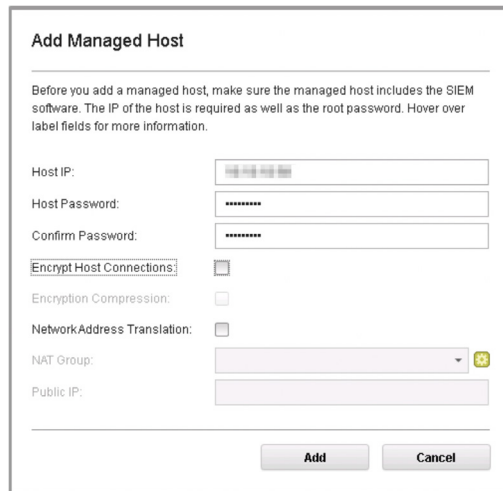
The System and License Management page appears. On the navigation menu, select Deployment Actions > Add Host.

Figure 121 Deployment Actions > Add Host



The Add Management Host page appears. Enter the fixed IP address of the SFEC host you want to add in the Host IP field. Enter the root password for the host IP in the Host Password field and re-enter the root password in the Confirm Password field, then click Add.

Figure 122 Add Managed Host



Add Managed Host

Before you add a managed host, make sure the managed host includes the SIEM software. The IP of the host is required as well as the root password. Hover over label fields for more information.

Host IP:


Host Password:

Confirm Password:

Encrypt Host Connections: ☐

Encryption Compression: ☐

NetworkAddress Translation: ☐

NAT Group: 

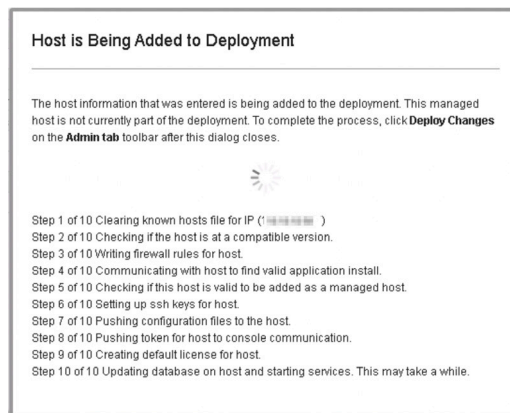
Public IP:

Add **Cancel**

NOTE If you are using NAT or want to use encrypted communication between SFEC and EP, select the other options accordingly.


A pop-up appears (Figure 123) displaying the status of the host being added to the network.

Figure 123 Host is Being Added to Deployment



Host is Being Added to Deployment

The host information that was entered is being added to the deployment. This managed host is not currently part of the deployment. To complete the process, click **Deploy Changes** on the **Admin tab** toolbar after this dialog closes.



Step 1 of 10 Clearing known hosts file for IP (192.168.1.100)

Step 2 of 10 Checking if the host is at a compatible version.

Step 3 of 10 Writing firewall rules for host.

Step 4 of 10 Communicating with host to find valid application install.

Step 5 of 10 Checking if this host is valid to be added as a managed host.

Step 6 of 10 Setting up ssh keys for host.

Step 7 of 10 Pushing configuration files to the host.

Step 8 of 10 Pushing token for host to console communication.

Step 9 of 10 Creating default license for host.

Step 10 of 10 Updating database on host and starting services. This may take a while.

During the process, the Modify Event Collector Appliance Connection page appears, as shown in Figure 124. You must attach the SFEC to an event processor to receive events from SFEC.

Figure 124 Modify Event Collector Appliance Connection Page

Modify Event Collector Appliance Connection

Select a Host's Event Processor to receive events from this Host.
NOTE: only eligible hosts will appear in the options.

The (*) denotes which host contains the destination connection.

EP-Jsa (*)

Save

Cancel

Select the required event processor to which you want to attach SFEC, from the list and click Save. After the host is added successfully, the new host is now listed on the System and License Management page (Figure 125).

Figure 125 Host Successfully Added

Display Systems

Deployment Details

Event Limit 3100/130000 Users 1

Flow Limit 175000/4800000

License Information Messages

System Support Activities Messages

Host Name	Host IP	Appliance Type	Version	Serial Number	Host Status
Jsa-SFEC		1599 - Event Collector	7.3.3	VMware-56 4d 6...	Active
FP-Jsa-new (HA)		1799 - Flow Processor	7.3.3	VMware-56 4d ...	Active
FP-Jsa-new-primary.juniper.net (prim...		1799 - Flow Processor	7.3.3	VMware-56 4d c...	Standby
FP-Jsa-new-secondary.juniper.net (s...		1799 - Flow Processor	7.3.3	VMware-56 4d c...	Active
EP-Jsa		1699 - Event Processor	7.3.3	VMware-56 4d ...	Active
vjsaDN (data node)		1400 - Data Node	7.3.3	VMware-56 4d 8...	Active
TM-Jsa (console)		3199 - Console	7.3.3	VMware-56 4d 0...	Active

Note that at this point, the new host is not deployed. Close the System and License Management page and to deploy the changes, go to the Admin page.

The changes that need to be deployed are shown on top of the page (Figure 126). Click View Details to see the changes.

Figure 126 Undeployed Changes

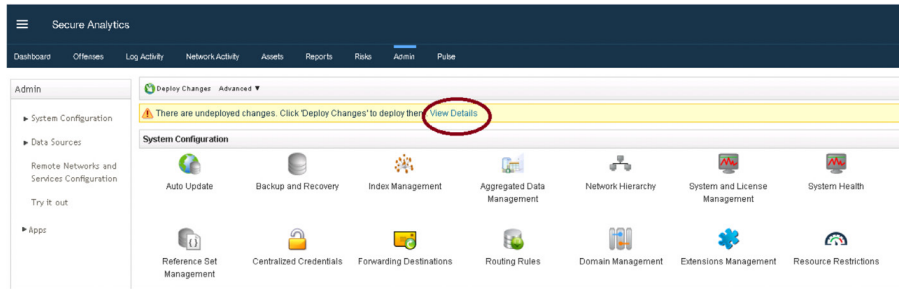
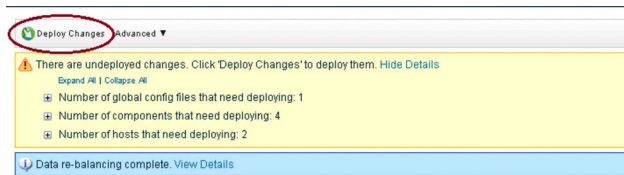


Figure 127 Changes to be Deployed



Click Deploy Changes. A confirmation page appears asking for confirmation to deploy the changes, as shown in Figure 128. Click Continue to deploy the changes.

Figure 128 Deployment Confirmation



The deployment starts. This process typically takes several minutes. Although it might appear as if the system is not responding at times, wait for the deployment to complete. The JSA web UI displays the progress in the deployment process. When the deployment process is complete, you will see the status as Success for all the hosts. This means that the SFEC is successfully added to the deployment. You can now point the log sources to send events to SFEC.

Next Step

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system, before the default license expires.

For more information about applying a license, see the section *Apply a License to JSA*.

Install and Configure High-Availability Appliance for Non-console

If your hardware or network fails, JSA can continue to collect, store, and process event and flow data by using high-availability (HA) appliances. To enable HA, JSA connects a primary HA host with a secondary HA host to create an HA cluster. You can use HA on hardware or virtual appliances. Both primary and secondary HA devices must be the same model and with the same CPU, RAM, and storage resources.

NOTE If you want high-availability for threat analytics or log analytics, use HA console. If you want high-availability for managed hosts such as flow processor, event processor, SFEC and so on, use HA non-console.

To configure HA, you must have an extra IP address. Once you add an HA host (secondary host) to the existing host (primary host), the original IP address of the primary host becomes the virtual IP address for HA and the extra IP address must be assigned to the primary host.

To complete the installation and configuration of an HA non-console:

- Install the HA non-console using the instructions in this section.
- Add this HA host to the primary non-console using the instructions provided in the section *Add High Availability (HA) Host*.
- Apply a license to the HA non-console using the instructions *Apply a License to JSA*.

Before You Begin

Before you begin the installation have the following in place:

- The required hardware is installed (in case of appliances).
- You have the required license key for your appliance.
- Add A keyboard and monitor are connected by using the VGA connection (in case of hardware appliances).
- There are no expired licenses on either the console or the managed hosts.
- Software versions for all JSA appliances in a deployment must be the same version and patch level. Note that deployments that use different versions of software are not supported.

Keep the following information ready before you begin the installation:

- Hostname
- IP address
- Network mask
- Default gateway address
- Primary Domain Name System (DNS) server address
- Secondary DNS server address (Optional)
- (Optional) Public IP address for networks using Network Address Translation (NAT)
- Email server name

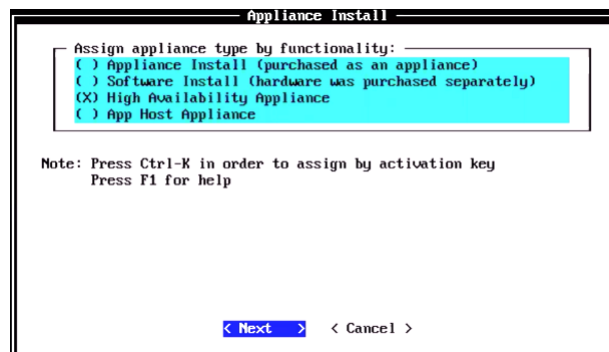
Step-by-Step Procedure

Follow the steps in the installation wizard for the hardware or virtual appliance type you are creating. Log in as the root user at the prompt (a password is not required). If you are prompted for a password, there is some error with the installation. Contact <https://support.juniper.net/support/>.

Read and accept the EULA license and proceed with the installation. Provide information in the installation wizard when prompted.

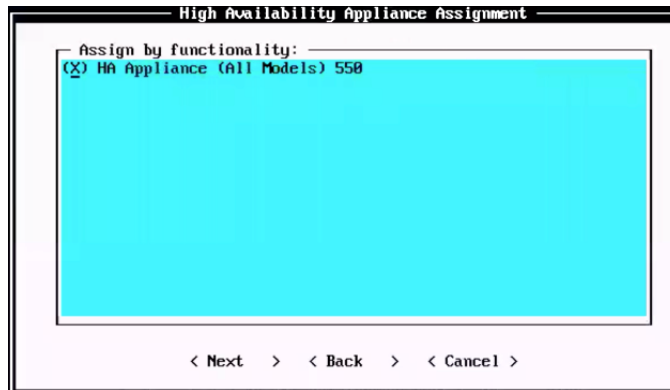
After accepting EULA license, the Appliance Install page appears (Figure 129). Select High Availability Appliance. Choose this option if you have purchased JSA appliances or wish to install virtual machines and select Next.

Figure 129 Appliance Install Options



The High Availability Appliance Assignment page appears. Select the appliance type as HA Appliance (All Models) 550 and select Next.

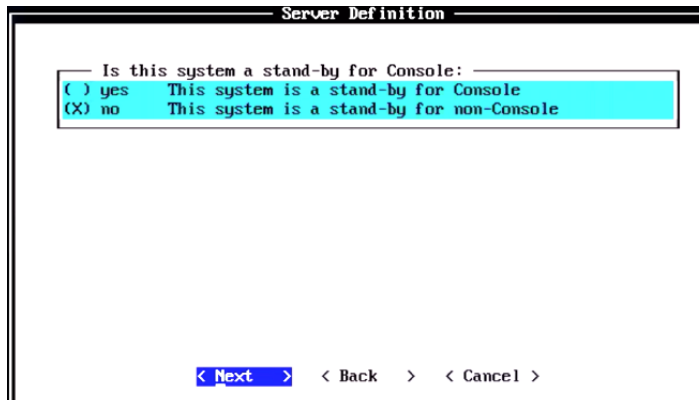
Figure 130 High Availability Appliance Assignment



The Server Definition page appears. Choose whether the stand-by appliance is for console or not and select Next. Select *No This system is a stand-by for non-console* and select Next.

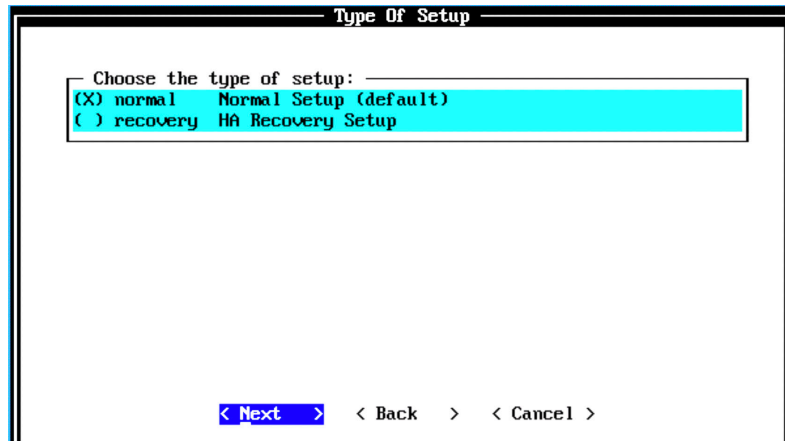
NOTE If you are installing an HA host for TA or LA console, you must select the *yes* option.

Figure 131 Server Definition Options



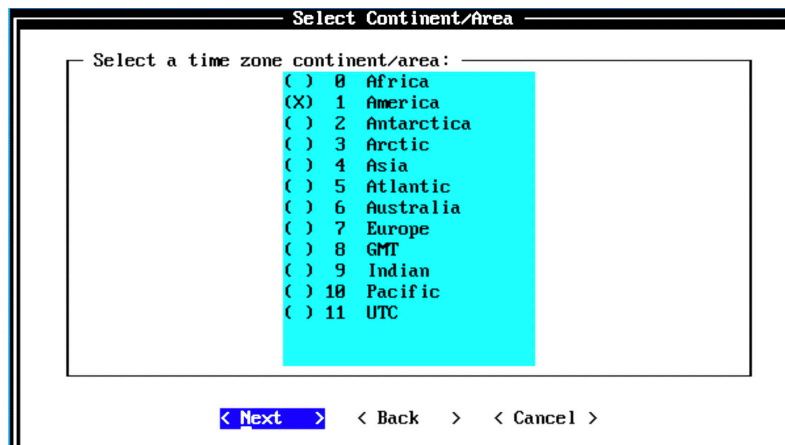
The Type of Setup page appears. Select the Normal Setup (default) option and select Next.

Figure 132 Setup Options



The Select Continent/Area page appears. Select the time zone continent or area as required and select Next. The default value is America.

Figure 133 Select Continent/Area Options



The Time Zone Selection page appears. Select the time zone city or region as required and select Next. The default value is New_York (Eastern (most areas)).

Figure 134 Time Zone Options

Time Zone Selection

Select a time zone city or region: —

- ☐ 94 Miquelon
- ☐ 95 Moncton (Atlantic - New Brunswick)
- ☐ 96 Monterrey (Central Time - Durango; Coahuila, Nuevo Leon, Tam)
- ☐ 97 Montevideo
- ☐ 98 Montserrat
- ☐ 99 Nassau
- ☒ 100 New_York (Eastern (most areas))
- ☐ 101 Nipigon (Eastern - ON, QC (no DST 1967-73))
- ☐ 102 Nome (Alaska (west))
- ☐ 103 Noronha (Atlantic islands)
- ☐ 104 North_Dakota/Beulah (Central - ND (Mercer))
- ☐ 105 North_Dakota/Center (Central - ND (Oliver))
- ☐ 106 North_Dakota/New_Salem (Central - ND (Morton rural))
- ☐ 107 Ojinaga (Mountain Time US - Chihuahua (US border))

< Next > < Back > < Cancel >

The Internet Protocol Setup page appears (Figure 135).

By default, the Internet Protocol version is selected as IPv4 Internet Protocol version 4. You can select IPv6 Internet Protocol version 6, if required. Select No as the value for Do not use bonded interface configuration mode. You can use the bonded interface configuration mode, if required. Select Next.

Figure 135 Internet Protocol Setup Options

Internet Protocol Setup

Choose which Internet protocol version to use: —

- ☒ ipv4 Internet Protocol version 4
- ☐ ipv6 Internet Protocol version 6

Choose interface configuration mode: —

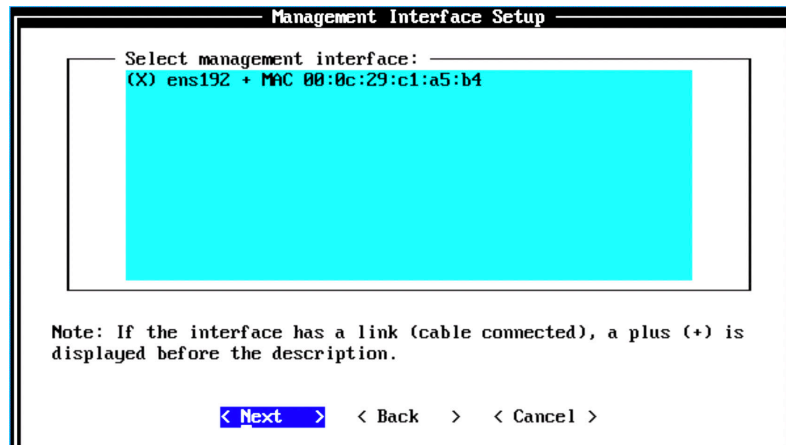
- ☒ No Do not use bonded interface configuration mode

< Next > < Back > < Cancel >

The Management Interface Setup page appears (Figure 136). Select the management interface that you want to use and select Next.

NOTE The list shown will depend on the number of NIC Cards on the hardware that you are installing JSA on. All the available interfaces will be displayed in this section.

Figure 136 Management Interface Setup Options



The Network Information Setup page appears. Configure the following network settings:

- 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.
- Email Server—Enter the email server. If you do not have an e-mail server, type localhost in this field.

Select Next.

Figure 137 *Network Information Setup Options*

Network Information Setup

Enter network information to use:

Hostname: [REDACTED]

IP Address: [REDACTED] Primary DNS: [REDACTED]

Network Mask: 255.255.255.0 Secondary DNS: [REDACTED]

Gateway: [REDACTED] Public IP: [REDACTED]

Email Server: localhost

< Next > < Back > < Cancel >

The network settings are validating. This may take a few minutes. Once network settings are validated successfully, the Root Password Setup page appears. Configure the root password required to login to the JSA Command Line Interface (CLI). In the Enter New Root Password field, enter a root password that meets the following criteria: contains at least 5 characters, contains no spaces, can include the following special characters: @, #, ^, and *. Re-enter the root password in the Confirm New Root Password field and select Finish.

Figure 138 *Root Password Options*

Root Password Setup

Enter New Root Password: [REDACTED]

Confirm New Root Password: [REDACTED]

The password must not be longer than 255 character and not contain spaces.

< Finish > < Back > < Cancel >

When you select Finish, the installation process starts.

This process typically takes several minutes. Although it might appear as if the system is not responding at times, wait for the installation to complete. Figure 139 shows that the installation process of a HA non-console is underway.

Figure 139 *Installing Changes*

```
Installing Qradar changes...
Activating system with key 3W5E1Q-2W4M2E-7D8X2A-6U8U7Y.
Appliance ID is 550.
Installing 'HA Appliance (All Models)' with id 550.
Configuring network...
Setting current date and time.
New date of '2020/02/19 00:15:20' was specified 379 seconds ago...
Setting date and time to '20200219 00:21:39'...
Setting email server to localhost
Running FinalSetup
Updating iptables firewall rules.
Restarting system services:
- syslog-ng
- hostcontext
- hostservices
Running restartServices
Restarting system services: syslog-ng.
HA Stand-by for Non-console setup, stopping services: hostcontext hostservices java.
OK: Configuration of host FP-HA as HA non-console stand-by completed.
qradar_setup.py: End: 0
Running: /opt/qradar/bin/after_services_up.sh
```

Once the installation is complete (Figure 140), a final completion message is displayed. Click OK.

Figure 140 *Installation Complete*



Verification

To verify the successful installation of an HA non-console, run the following command on the console:

Run `less /etc/.appliance_name`

The output displays 550 as the appliance installed. Ping the default gateway to ensure that the connectivity is fine. You can also use the `ifconfig` command to view the IP address details of the appliance.

Next Steps

After you have completed installing an HA non-console, you can add it to a primary non-console host (for example, EP,FP, and so on). For more information about adding an HA host, see *Add High Availability (HA) Host*.

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system, before the default license expires.

For more information about applying a license, see section *Apply a License to JSA*.

Install and Configure High-Availability Appliance for Console

If your hardware or network fails, JSA can continue to collect, store, and process event and flow data by using high-availability (HA) appliances. To enable HA, JSA connects a primary HA host with a secondary HA host to create an HA cluster. You can use HA on hardware or virtual appliances. Both primary and secondary HA devices must be the same model and with the same CPU, RAM, and storage resources.

NOTE If you want high-availability for threat analytics or log analytics, use HA console. If you want high-availability for managed hosts such as flow processor, event processor, SFEC and so on, use HA *non-console*.

To configure HA, you must have an extra IP address. Once you add an HA host (secondary host) to the existing host (primary host), the original IP address of the primary host becomes the virtual IP address for HA and the extra IP address must be assigned to the primary host.

To complete the installation and configuration of an HA console:

- Install the HA console using the instructions in this section.
- Add this HA host to the primary device using the instructions provided in the section *Add High Availability (HA) Host*.
- Apply a license to the HA console using the instructions provided in the section *Apply a License to JSA*.

Before You Begin

Before you start the installation, ensure that you have the following in place:

- The required hardware is installed (in case of appliances).
- You have the required license key for your appliance.
- A keyboard and monitor are connected by using the VGA connection (in case of hardware appliances).
- There are no expired licenses on either the console or the managed hosts.
- Software versions for all JSA appliances in a deployment must be the same version and patch level. Note that deployments that use different versions of software are not supported.

Keep the following information ready before you begin the installation:

- Hostname
- IP address
- Network mask
- Default gateway address
- Primary Domain Name System (DNS) server address
- Secondary DNS server address (Optional)
- (Optional) Public IP address for networks using Network Address Translation (NAT)
- Email server name

Step-by-Step Procedure

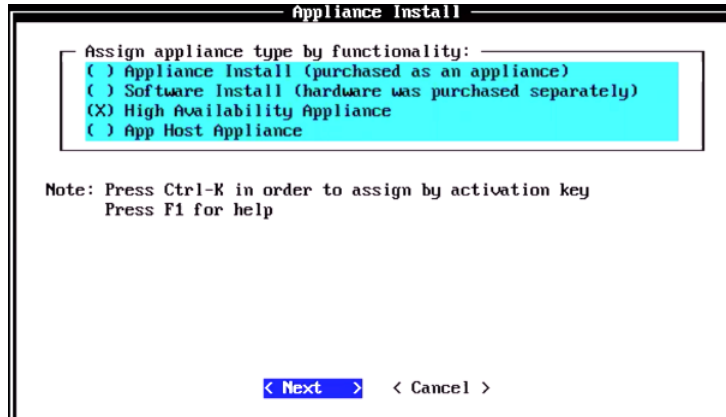
Follow the steps in the installation wizard for the hardware or virtual appliance type you are creating.

Log in as the root user at the prompt (a password is not required). If you are prompted for a password, there is some error with the installation. Contact <https://support.juniper.net/support/>.

The JSA installation wizard allows you to use only certain keyboard keys to navigate through the installation options. Table P1 lists these keys along with how you can use them.

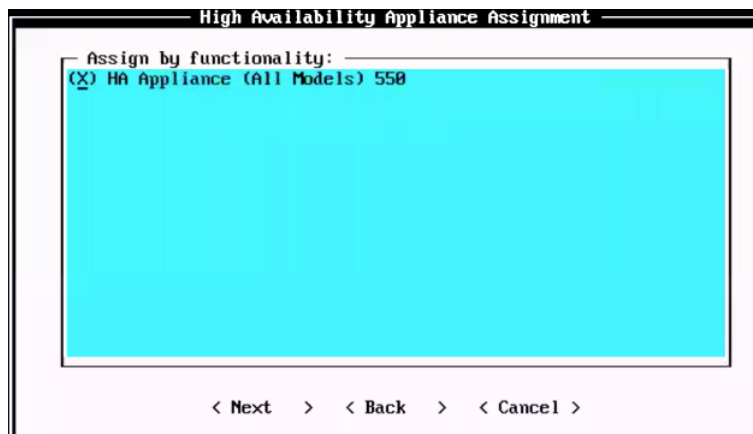
Read and accept the EULA license and proceed with the installation. Provide information in the installation wizard when prompted. After accepting EULA license, the Appliance Install page appears (Figure 141). Select High Availability Appliance. Choose this option if you have purchased JSA appliances or wish to install virtual machines. Select Next to continue.

Figure 141 *Appliance Install Options*



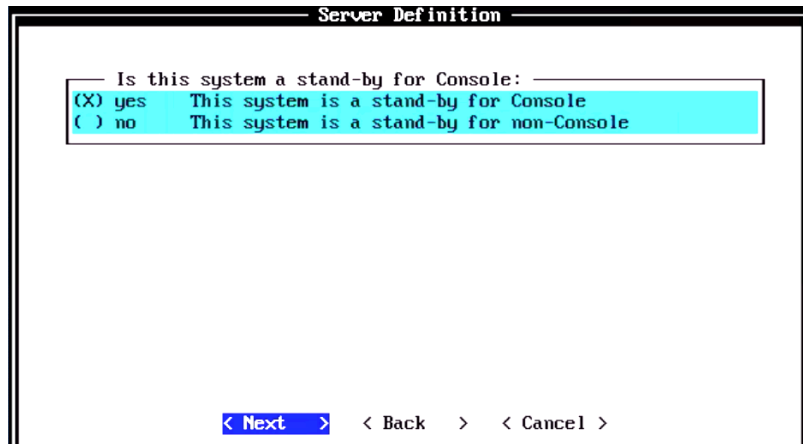
The High Availability Appliance Assignment page appears. Select the appliance type as HA Appliance (All Models) 550 and select Next.

Figure 142 *High Availability Appliance Options*



The Server Definition page appears. Choose whether the stand-by appliance is for console or not and select Next. Select yes This system is a stand-by for Console and select Next.

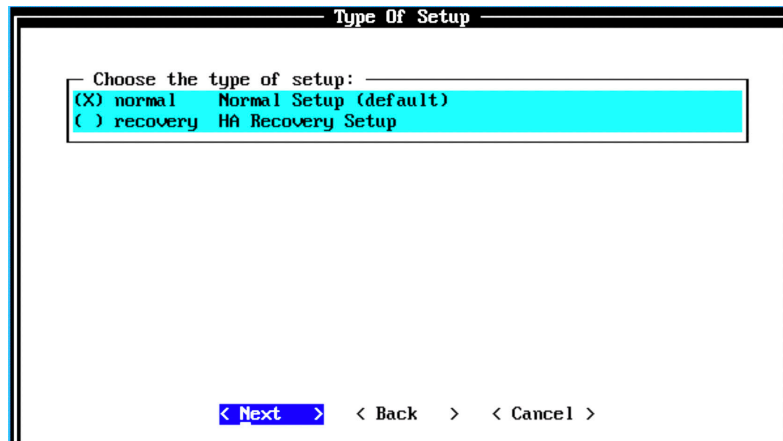
Figure 143 Server Definitions Options



The screenshot shows a dialog box titled "Server Definition". Inside, there is a text prompt "Is this system a stand-by for Console:". Below the prompt, there are two radio button options: "(X) yes This system is a stand-by for Console" and "() no This system is a stand-by for non-Console". The "yes" option is selected. At the bottom of the dialog, there are three buttons: "< Next >", "< Back", and "< Cancel >". The "< Next >" button is highlighted in blue.

The Type of Setup page appears. Select the Normal Setup (default) option and select Next.

Figure 144 Setup Options



The screenshot shows a dialog box titled "Type Of Setup". Inside, there is a text prompt "Choose the type of setup:". Below the prompt, there are two radio button options: "(X) normal Normal Setup (default)" and "() recovery HA Recovery Setup". The "normal" option is selected. At the bottom of the dialog, there are three buttons: "< Next >", "< Back", and "< Cancel >". The "< Next >" button is highlighted in blue.

The Date/Time Setup page appears (Figure 145). 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.

Figure 145 Date/Time Setup Options

Date/Time Setup

Setting the date and time manually or by specifying an NTP/RDate server.

Manual setting:

Current Date (YYYY/MM/DD): 2019/12/01

24h Clock Time (HH:MM:SS): 01:30:55

Time Server name or IP address:

Time server:

< Next > < Back > < Cancel >

The Select Continent/Area page appears. Select the time zone continent or area as required and select Next. The default value is America.

Figure 146 Select Continent/Area Options

Select Continent/Area

Select a time zone continent/area:

- ☐ 0 Africa
- ☒ 1 America
- ☐ 2 Antarctica
- ☐ 3 Arctic
- ☐ 4 Asia
- ☐ 5 Atlantic
- ☐ 6 Australia
- ☐ 7 Europe
- ☐ 8 GMT
- ☐ 9 Indian
- ☐ 10 Pacific
- ☐ 11 UTC

< Next > < Back > < Cancel >

The Time Zone Selection page appears. Select the time zone city or region as required and select Next. The default value is New_York (Eastern (most areas)).

Figure 147 Time Zone Options

Time Zone Selection

Select a time zone city or region: _____

- ☐ 94 Miquelon
- ☐ 95 Moncton (Atlantic - New Brunswick)
- ☐ 96 Monterrey (Central Time - Durango; Coahuila, Nuevo Leon, Tam)
- ☐ 97 Montevideo
- ☐ 98 Montserrat
- ☐ 99 Nassau
- ☒ 100 New_York (Eastern (most areas))
- ☐ 101 Nipigon (Eastern - ON, QC (no DST 1967-73))
- ☐ 102 Nome (Alaska (west))
- ☐ 103 Noronha (Atlantic islands)
- ☐ 104 North_Dakota/Beulah (Central - ND (Mercer))
- ☐ 105 North_Dakota/Center (Central - ND (Oliver))
- ☐ 106 North_Dakota/New_Salem (Central - ND (Morton rural))
- ☐ 107 Ojinaga (Mountain Time US - Chihuahua (US border))

The Internet Protocol Setup page appears (Figure 148). By default, the Internet Protocol version is selected as IPv4 Internet Protocol version 4. You can select IPv6 Internet Protocol version 6, if required. Select No as the value for Do not use bonded interface configuration mode. You can use the bonded interface configuration mode, if required. Select Next.

Figure 148 Internet Protocol Setup Options

Internet Protocol Setup

Choose which Internet protocol version to use: _____

- ☒ ipv4 Internet Protocol version 4
- ☐ ipv6 Internet Protocol version 6

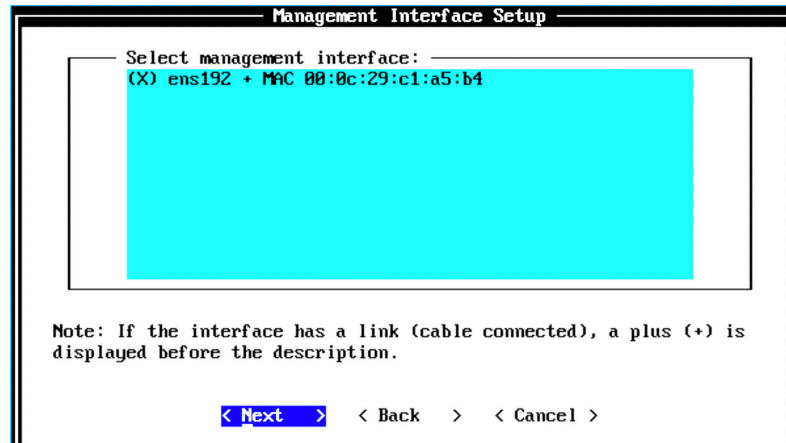
Choose interface configuration mode: _____

- ☒ No Do not use bonded interface configuration mode

The Management Interface Setup page appears (Figure 149). Select the management interface that you want to use and select Next.

NOTE The list shown will depend on the number of NIC Cards on the hardware that you are installing JSA on. All the available interfaces will be displayed in this section.

Figure 149 *Management Interface Setup Options*



The Network Information Setup page appears. Configure the following network settings:

- 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.
- Email Server—Enter the email server. If you do not have an e-mail server, type localhost in this field.

Select Next.

Figure 150 Network Information Setup Options

Network Information Setup

Enter network information to use:

Hostname:

IP Address: Primary DNS:

Network Mask: 255.255.255.0 Secondary DNS:

Gateway: Public IP:

Email Server: localhost

< Next > < Back > < Cancel >

The network settings will start validating. This may take a few minutes. Once network settings are validated successfully, the Root Password Setup page appears (Figure 151). Configure the root password required to login to the JSA Command Line Interface (CLI).

In the Enter New Root Password field, enter a root password that meets the following criteria: contains at least five characters, contains no spaces, can include the following special characters: @, #, ^, and *.

Re-enter the root password in the Confirm New Root Password field and select Finish.

Figure 151 Root Password Options

Root Password Setup

Enter New Root Password:

Confirm New Root Password:

The password must not be longer than 255 character and not contain spaces.

< Finish > < Back > < Cancel >

When you select Finish, the installation process starts. This process typically takes several minutes. Although it might appear as if the system is not responding at times, wait for the installation to complete. Figure 152 indicates that the installation process of a HA console is underway.

Figure 152 *Installing Changes*

```
Installing Qradar changes...
Activating system with key 3W5E1Q-2W4M2E-7D8X2A-6U0U7Y.
Appliance ID is 550.
Installing 'HA Appliance (All Models)' with id 550.
Configuring network...
Setting current date and time.
New date of '2020/02/22 15:44:28' was specified 15145 seconds ago...
Setting date and time to '20200222 19:56:53'...
Setting email server to localhost
Running FinalSetup
Updating iptables firewall rules.
Running restartServices
Restarting system services: syslog-ng.
HA Stand-by for Console setup, stopping services: hostcontext httpd tomcat hostservices java.
OK: Configuration of host TM-HA as HA console stand-by completed.
qradar_setup.py: End: 0
Running: /opt/qradar/bin/after_services_up.sh
_
```

Once the installation is complete, a final completion message is displayed. Click Ok.

Figure 153 *Installation Complete*

```
Initial configuration of 'HA Appliance (All Models)' is
now complete.

Press ENTER to complete Installation.

< OK >
```

Verification

To verify the successful installation of an HA console, run the following command on the console:

```
Run less /etc/.appliance_name
```

The output displays 550 as the appliance installed. Ping the default gateway to ensure that the connectivity is fine. You can also use the `ifconfig` command to view the IP address details of the appliance.

Next Steps

After you have completed installing an HA console, you can add it to the primary device. For more information about adding an HA host, see *Add High Availability (HA) Host*.

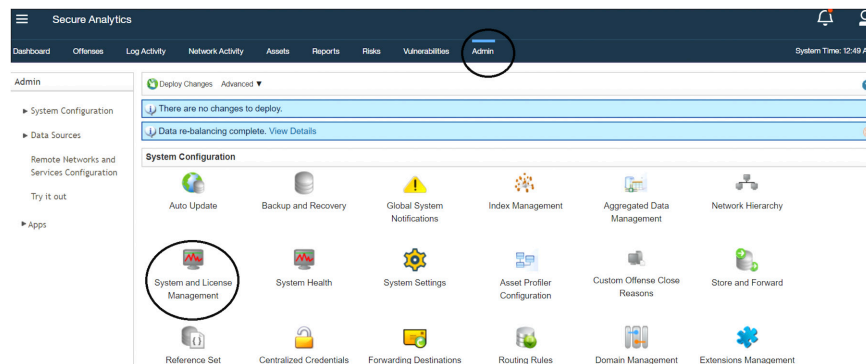
When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system, before the default license expires.

For more information about applying a license, see section *Apply a License to JSA*.

Add High Availability (HA) Host

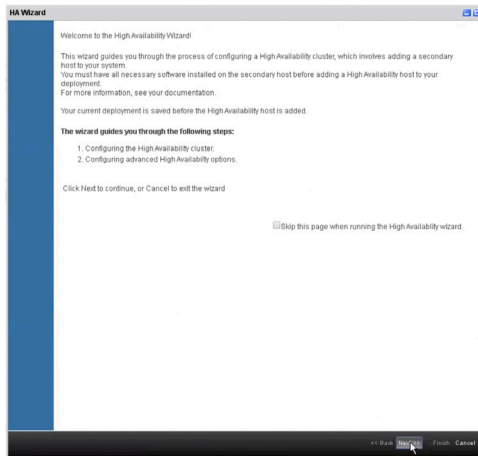
To add the HA console or non-console host, log in to the JSA web UI. On the navigation menu, click Admin. The Admin page appears (Figure 154). In the System Configuration section, click System and License Management.

Figure 154 System and License Management



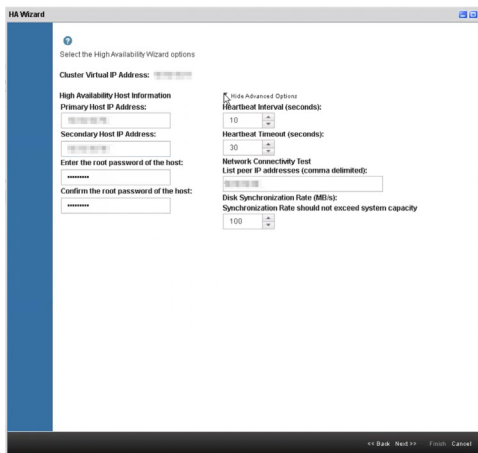
The System and License Management page appears. Right-click on the host that you want to configure HA on and select Add HA Host. The HA Wizard page appears, as shown in Figure 155.

Figure 155 HA Wizard



Read the introductory text and click Next. The High Availability Wizard Options page appears, as shown in Figure 156.

Figure 156 High Availability Wizard Options



In the Primary Host IP Address, enter a new primary HA host IP address. The new IP address replaces the previous IP address. The current IP address of the primary HA host becomes the Cluster Virtual IP address. The new primary HA host IP address must be on the same subnet as the virtual host IP address.

In the Secondary Host IP Address, enter the IP address of the secondary HA host. The secondary HA host must be on the same subnet as the primary HA host.

Enter the root password for the secondary HA host. Enter the root password for the secondary HA host again for confirmation.

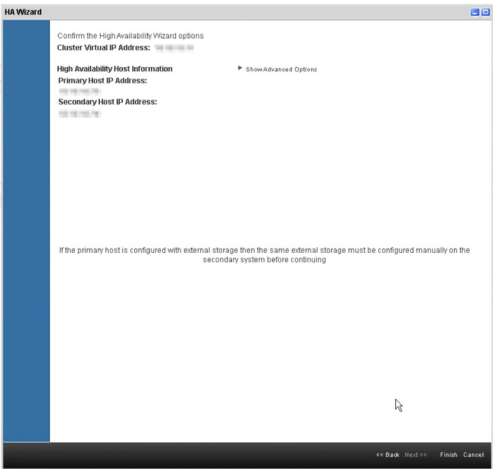
Under the Show Advanced Options, you can configure the following advanced parameters (Table 7):

Table 7 Advanced Options for the HA Host

Option	Description
Heartbeat Interval (seconds)	The time, in seconds, that you want to elapse between heartbeat pings. The default is 10 seconds.
Heartbeat Timeout (seconds)	The time, in seconds, that you want to elapse before the primary HA host is considered unavailable if no heartbeat is detected. The default is 30 seconds.
Network Connectivity Test List peer IP addresses (comma delimited)	The IP addresses of the hosts that you want the secondary HA host to ping. The default is to ping all other managed hosts in the JSA deployment.
Disk Synchronization Rate (MB/s)	The disk synchronization rate. The default is 100 MB/s.

Review the configured parameters. If you need to edit any fields, click Back. If all parameter values are correct, click Next, and then click Finish.

Figure 157 High Availability Wizard Options – Finish



Click on the host name to view the primary and secondary HA details, as shown in Figure 158.

Figure 158 High Availability Details Page

The screenshot shows the 'High Availability' section of the JSA Risk Manager interface. It includes tabs for 'Display' and 'Systems'. Below the tabs, there are sections for 'Deployment Details', 'License Information Messages', and 'System Support Activities Messages'. The 'Deployment Details' section shows 'Event Limit: 3100/130000' and 'Flow Limit: 175000/4800000'. The 'License Information Messages' section is empty. The 'System Support Activities Messages' section is also empty. Below these sections is a table with the following data:

Host Name	Host IP	Appliance Type	Version	Serial Number	Host Status	License Expiration Date	License Status	Event Rate
FP-JSA-new (JSA)	1799	Flow Processor	7.3.3	VMware-56 4d c...	Adding Secondary	Perpetual	Deployed	N/A
FP-JSA-new(juniper.net) (primary)	1799	Flow Processor	7.3.3	VMware-56 4d c...	Installing	Perpetual	Deployed	N/A
FP-JSA-new(juniper.net) (secondary)	1799	Flow Processor	7.3.3	VMware-56 4d f...	Active	Perpetual	Deployed	1000/10000
EP-JSA	3199	Event Processor	7.3.3	VMware-56 4d 0...	Active	Aug 10, 2020	Deployed	500/30000
TM-JSA (console)	3199	Console	7.3.3	VMware-56 4d 0...	Active	Aug 10, 2020	Deployed	500/30000

NOTE Devices will reboot during HA configuration process.

As data must be synced between primary and stand-by systems, HA configuration can take several hours to complete. You can view the status in the System and License Management page.

Install and Configure JSA Risk Manager

JSA Risk Manager evaluates the parameters that you define in your question and returns assets in your network to help you assess risk. The questions are based on a series of tests that can be combined and configured as required.

JSA Risk Manager is a separately installed appliance for monitoring device configurations, simulating changes to your network environment, and prioritizing risks and vulnerabilities in your network.

To complete the installation and configuration of Risk Manager:

- Install Risk Manager using the instructions in this section.
- Add Risk Manager to the deployment using the instructions provided in the section *Add Risk Manager to Deployment*.
- Apply a license to the risk manager console using the instructions provided in section *Apply a License to JSA*.

Before You Begin

Before you do the installation, ensure that you have the following in place:

- The required hardware is installed (in case of appliances).
- You have the required license key for your appliance.
- A keyboard and monitor are connected by using the VGA connection (in case of hardware appliances).
- There are no expired licenses on either the console or the managed hosts.
- Software versions for all JSA appliances in a deployment must be the same version and patch level. Note that deployments that use different versions of software are not supported.

Keep the following information ready before you begin the installation:

- Hostname
- IP address
- Network mask
- Default gateway address
- Primary Domain Name System (DNS) server address
- Secondary DNS server address (Optional)
- (Optional) Public IP address for networks using Network Address Translation (NAT)
- (Optional) Email server name

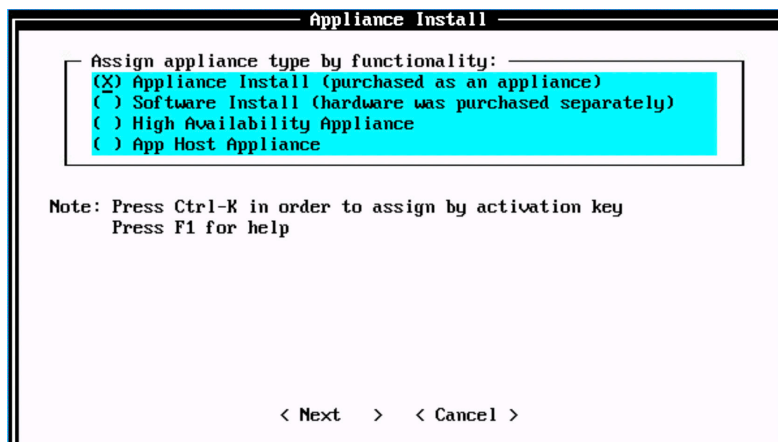
Step-By-Step Procedure

Follow the steps in the installation wizard for the virtual appliance type you are creating. Log in as the root user at the prompt (a password is not required). If you are prompted for a password, there is some error with the installation. Contact <https://support.juniper.net/support/>.

The JSA installation wizard allows you to use only certain keyboard keys to navigate through the installation options. Table P1 lists these keys along with how you can use them.

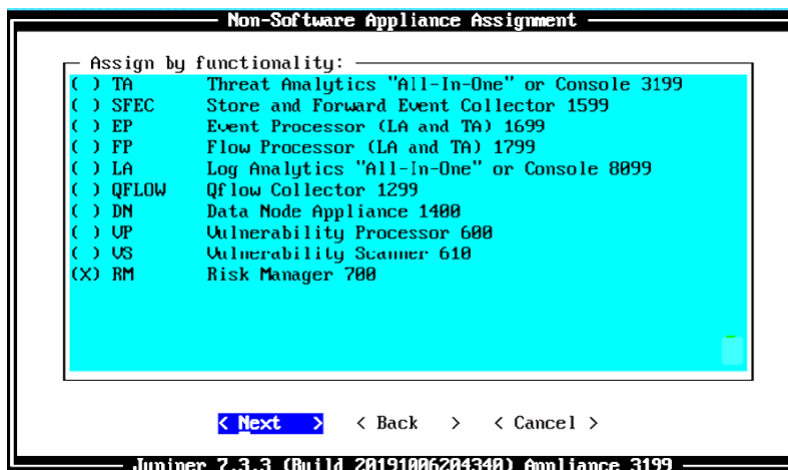
Read and accept the EULA license and proceed with the installation. Provide information in the installation wizard when prompted. After accepting EULA license, the Appliance Install page appears (Figure 159). Select Appliance Install (purchased as an appliance). Choose this option if you have purchased JSA appliances or wish to install virtual machines. Select Next.

Figure 159 Appliance Install Options



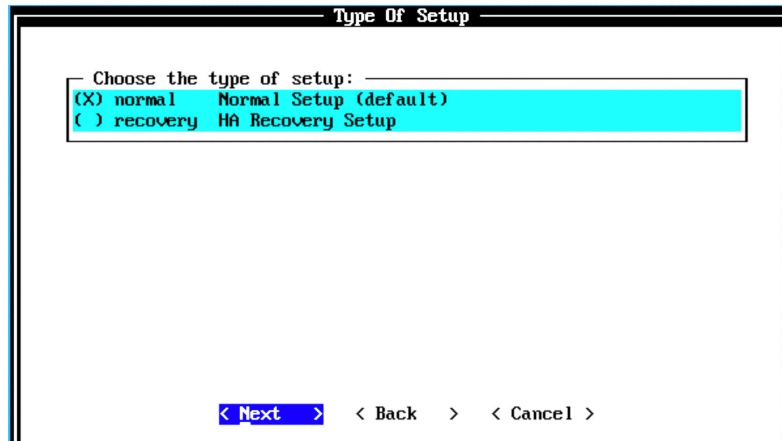
The Non-Software Appliance Assignment page appears. Select the Non-Software Appliance type as Risk Manager and select Next.

Figure 160 Non-Software Appliance Assignment Options



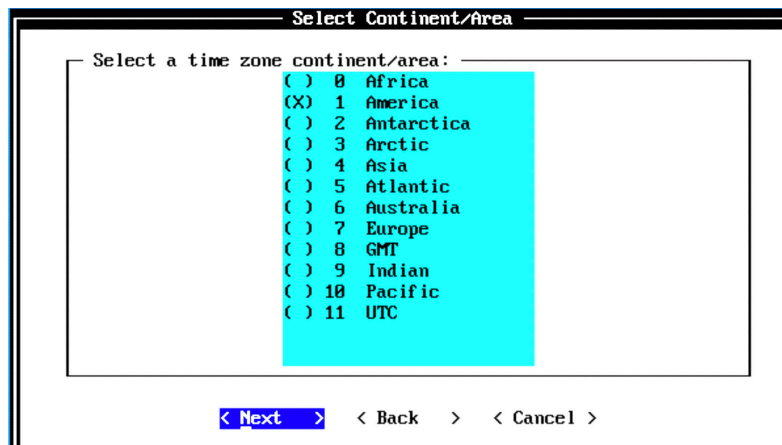
The Type of Setup page appears. Select the Normal Setup (default) option and select Next.

Figure 161 Setup Options



The Select Continent/Area page appears. Select the time zone continent or area as required and select Next. The default value is America.

Figure 162 Select Continent/Area Options



The Time Zone Selection page appears. Select the time zone city or region as required and select Next. The default value is New_York (Eastern (most areas)).

Figure 163 Time Zone Options

Time Zone Selection

Select a time zone city or region: _____

- ☐ 94 Miquelon
- ☐ 95 Moncton (Atlantic - New Brunswick)
- ☐ 96 Monterrey (Central Time - Durango; Coahuila, Nuevo Leon, Tam)
- ☐ 97 Montevideo
- ☐ 98 Montserrat
- ☐ 99 Nassau
- ☒ 100 New_York (Eastern (most areas))
- ☐ 101 Nipigon (Eastern - ON, QC (no DST 1967-73))
- ☐ 102 Nome (Alaska (west))
- ☐ 103 Noronha (Atlantic islands)
- ☐ 104 North_Dakota/Beulah (Central - ND (Mercer))
- ☐ 105 North_Dakota/Center (Central - ND (Oliver))
- ☐ 106 North_Dakota/New_Salem (Central - ND (Morton rural))
- ☐ 107 Ojinaga (Mountain Time US - Chihuahua (US border))

< Back > < Cancel >

The Internet Protocol Setup page appears (Figure 164). By default, the Internet Protocol version is selected as IPv4 Internet Protocol version 4. You can select IPv6 Internet Protocol version 6, if required. Select No as the value for Do not use bonded interface configuration mode. You can use the bonded interface configuration mode, if required. Select Next.

Figure 164 Internet Protocol Setup Options

Internet Protocol Setup

Choose which Internet protocol version to use: _____

- ☒ ipv4 Internet Protocol version 4
- ☐ ipv6 Internet Protocol version 6

Choose interface configuration mode: _____

- ☒ No Do not use bonded interface configuration mode

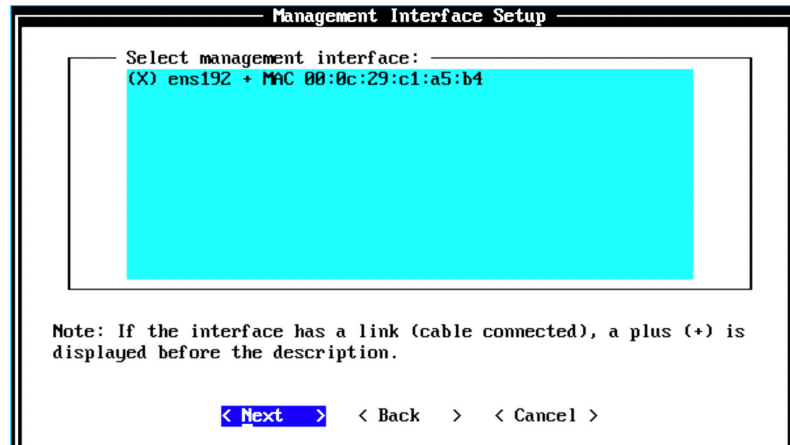
< Back > < Cancel >

The Management Interface Setup page appears.

Select the management interface that you want to use and select Next.

NOTE The list shown here depends on the number of NIC Cards on the hardware that you are installing JSA on. All the available interfaces will be displayed in this section.

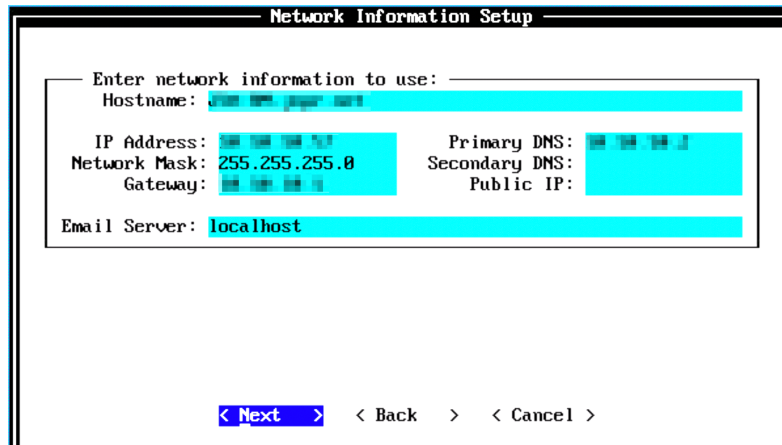
Figure 165 Management Interface Setup Options



The Network Information Setup page appears. Configure the following network settings:

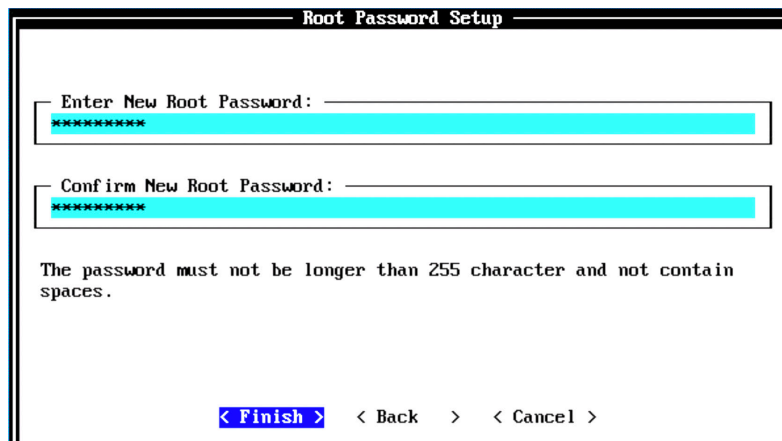
- Hostname—Enter a fully qualified domain name as the system hostname.
- IP Address—Enter the IP address of the system.
- Network Mask—Enter the network mask for the system.
- Gateway—Enter the default gateway of the system.
- Primary DNS—Enter the primary DNS server address.
- Secondary DNS—(Optional). Type the secondary DNS server address.
- Public IP—(Optional). Enter the Public IP address of the server.
- Email Server—Enter the email server. If you do not have an e-mail server, type localhost in this field.

When complete select Next.

Figure 166 *Network Information Setup Options*

The screenshot shows a window titled "Network Information Setup". Inside, there is a section titled "Enter network information to use:". Below this, there are several input fields: "Hostname:" followed by a redacted field, "IP Address:" followed by a redacted field, "Network Mask:" with the value "255.255.255.0", "Gateway:" followed by a redacted field, "Primary DNS:" followed by a redacted field, "Secondary DNS:" followed by a redacted field, "Public IP:" followed by a redacted field, and "Email Server:" with the value "localhost". At the bottom of the window, there are three buttons: "< Next >", "< Back", and "< Cancel >".

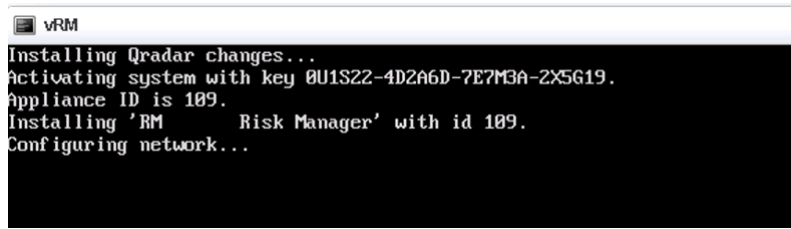
The network settings will validate. This may take a few minutes. Once network settings are validated successfully, the Root Password Setup page appears (Figure 167). Configure the root password required to login to the JSA Command Line Interface (CLI). In the Enter New Root Password field, enter a root password that meets the following criteria: contains at least 5 characters, contains no spaces, can include the following special characters: @, #, ^, and *. Re-enter the root password in the Confirm New Root Password field and select Finish.

Figure 167 *Root Password Options*

The screenshot shows a window titled "Root Password Setup". Inside, there are two input fields: "Enter New Root Password:" followed by a redacted field, and "Confirm New Root Password:" followed by a redacted field. Below these fields, there is a message: "The password must not be longer than 255 character and not contain spaces." At the bottom of the window, there are three buttons: "< Finish >", "< Back", and "< Cancel >".

When you select Finish, the installation process starts. This process typically takes several minutes. Although it might appear as if the system is not responding at times, wait for the installation to complete. Figure 168 indicates that the installation process of Risk Manager is underway.

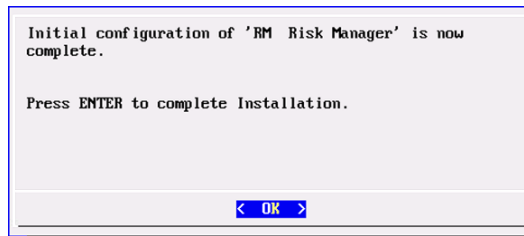
Figure 168 Installing Changes

A terminal window titled 'vRM' with a black background and white text. The text shows the installation progress of Risk Manager, including activating the system with a key and configuring the network.

```
vRM
Installing Qradar changes...
Activating system with key 0U1S22-4D2A6D-7E7M3A-2X5G19.
Appliance ID is 109.
Installing 'RM Risk Manager' with id 109.
Configuring network...
```

The output shown in Figure 169 indicates the successful installation of Risk Manager. Once the installation is complete, a final completion message is displayed. Click Ok.

Figure 169 Installation Complete



Verification

To verify the successful installation of Risk Manager run the following command on the console:

Run `less /etc/.appliance_name`

The output displays `700` as the appliance installed. Ping the default gateway to ensure that the connectivity is fine. You can also use the `ifconfig` command to view the IP address details of the appliance.

Next Steps

After you complete the Risk Manager installation, you can add it to the deployment. For more information, see section *Add Risk Manager to Deployment*.

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system, before the default license expires.

For more information about applying a license, see section *Apply a License to JSA*.

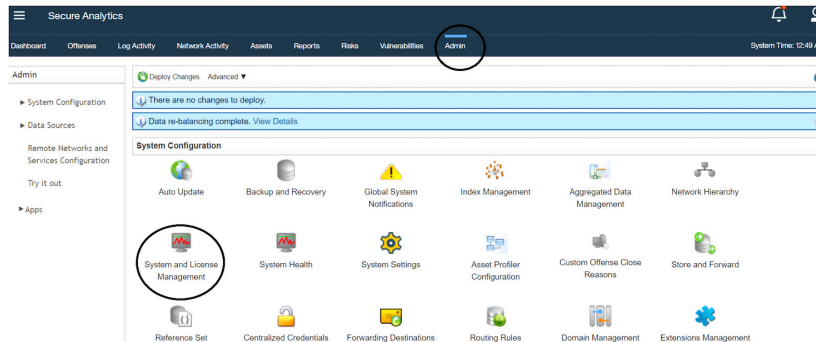
Add Risk Manager to Your Deployment

To use the Risk Manager features and functionality you must add a risk manager hardware/virtual appliance to the JSA deployment. Here's how you can add a Risk Manager to the deployment.

NOTE You must apply the Risk Manager license to enable this feature. Without the license, the Risks tab will not be available in the JSA Web UI.

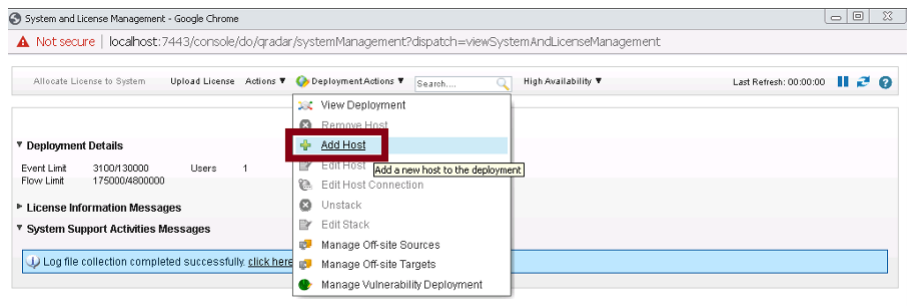
To add Risk Manager to the deployment, log in to the JSA web UI. On the navigation menu, click Admin. The Admin page appears (Figure 170). In the System Configuration section, click System and License Management.

Figure 170 System and License Management



The System and License Management page appears (Figure 171). On the navigation menu, select Deployment Actions > Add Host.

Figure 171 Deployment Actions > Add Host



The Add Management Host page appears (Figure 172). Enter the fixed IP address of the Risk Manager host you want to add in the Host IP field. Enter the root password for the host IP in the Host Password field and re-enter the root password in the Confirm Password field. Click Add.

Figure 172 Add Managed Host

Add Managed Host

Before you add a managed host, make sure the managed host includes the SIEM software. The IP of the host is required as well as the root password. Hover over label fields for more information.

Host IP:

Host Password:

Confirm Password:

Encrypt Host Connections:

☐

Encryption Compression:

☐

Network Address Translation:

☐

NAT Group:

Public IP:

Add

Cancel

NOTE If you are using NAT or want to use encrypted communication between the Risk Manager and the console, select the other options accordingly.

A pop-up appears (Figure 173) displaying the status of the host being added to the network.

Figure 173 Host is Being Added to Deployment

Host is Being Added to Deployment

The host information that was entered is being added to the deployment. This managed host is not currently part of the deployment. To complete the process, click **Deploy Changes** on the **Admin** tab toolbar after this dialog closes.

Step 1 of 10 Clearing known hosts file for IP ()

Step 2 of 10 Checking if the host is at a compatible version.

Step 3 of 10 Writing firewall rules for host.

Step 4 of 10 Communicating with host to find valid application install.

Step 5 of 10 Checking if this host is valid to be added as a managed host.

Step 6 of 10 Setting up ssh keys for host.

Step 7 of 10 Pushing configuration files to the host.

Step 8 of 10 Pushing token for host to console communication.

Step 9 of 10 Creating default license for host.

Step 10 of 10 Updating database on host and starting services. This may take a while.

After the host is added successfully, the new host is now listed on the System and License Management page. Note that at this point the new host is *not* deployed. So, close the System and License Management page and go to the Admin page to deploy the changes (Figure 174). The changes that need to be deployed are shown on top of that page. Click View Details to see the changes.

Figure 174 Undeployed Changes

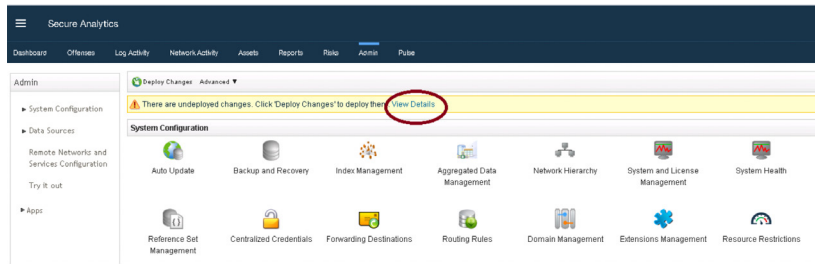
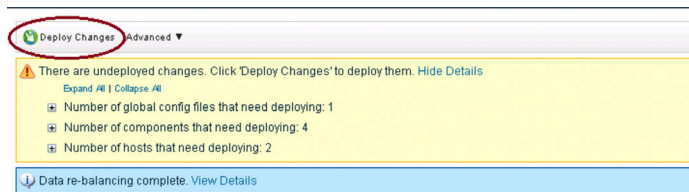


Figure 175 Changes to be Deployed



Click Deploy Changes and a confirmation page will appear asking for confirmation to deploy the changes, as shown in Figure 176. Click Continue to deploy the changes.

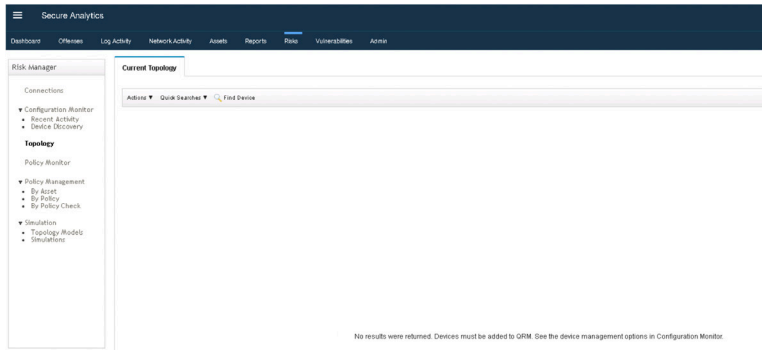
Figure 176 Deployment Confirmation



The deployment starts. This process typically takes several minutes. Although it might appear as if the system is not responding at times, wait for the deployment to complete.

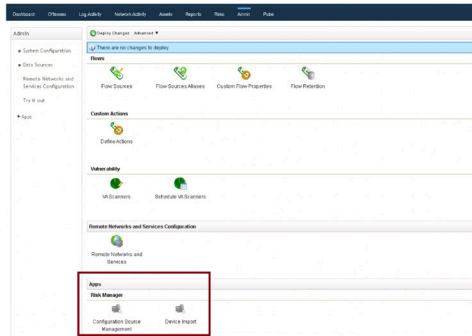
The JSA web UI will display the progress in the deployment process. When the deployment is complete, the Risks tab is displayed, as shown in Figure 177.

Figure 177 Risks Tab



You can now add security or firewall devices for risk management using Configuration Source Management or Device Import using the Risk Manager in the Admin tab, as shown in Figure 178.

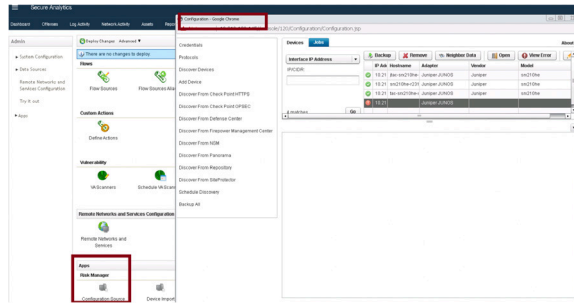
Figure 178 Risk Manager Options



Use Configuration Source Management (Figure 179) to configure credentials, add or discover devices, view device configurations, and back up device configurations in JSA Risk Manager. The data that is obtained from devices in your network is used to populate the topology. You must have administrative privileges to access Configuration Source Management functions from the Admin tab in JSA.

NOTE For more detailed information, go to the Juniper Networks TechLibrary: https://www.juniper.net/documentation/en_US/jsa7.3.1/jsa-risk-manager-user-guide/topics/concept/jsa-rm-user-configuration-source-management.html.

Figure 179 Risks Manager - Configuration Source Management



Use the Device Import (Figure 180) feature to add a list of adapters and their network IP addresses to the Configuration Source Manager using a comma-separated value file (.csv). You can easily do a bulk upload by using the CSV file. The device import list can contain up to 5000 devices, but the list must contain one line for each adapter and its associated IP address in the import file.

MORE? For more information on importing devices into Risk Manager, visit the Juniper Networks TechLibrary: https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-risk-manager-user-guide/topics/concept/concept-jsa-rm-user-import-devices.html.

Figure 180 Risks Manager - Device Import

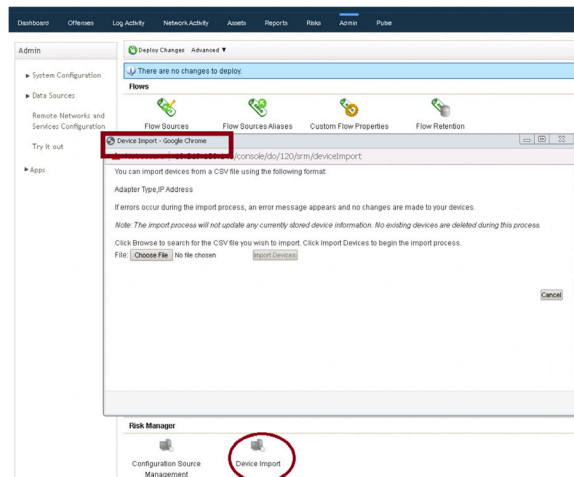
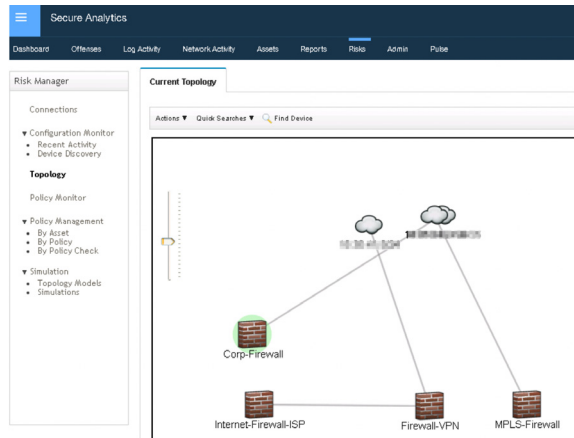


Figure 181 Risks Tab - After Device Import



Next Steps

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system before the default license expires.

For more information about applying a license, see section *Apply a License to JSA*.

Install and Configure a Vulnerability Processor

Locate and manage the vulnerabilities in your network by deploying JSA Vulnerability Manager. JSA Vulnerability Manager discovers vulnerabilities on your network devices, applications and software adds context to the vulnerabilities, prioritizes asset risk in your network, and supports the remediation of discovered vulnerabilities.

To deploy a dedicated JSA vulnerability manager processor or vulnerability processor (VP) appliance you must complete the followings tasks:

- Install a dedicated JSA vulnerability manager processor appliance or VP using the instructions provided in this section.
- Add the vulnerability processor appliance to your deployment using the instructions provided in the section *Add a Dedicated Vulnerability Processor*.
- Apply a license to the vulnerability processor using the instructions *Apply a License to JSA*.

Before You Begin

Make sure you have the following:

- The required hardware is installed (in case of appliances).
- You have the required license key for your appliance.
- A keyboard and monitor are connected by using the VGA connection (in case of hardware appliances).
- There are no expired licenses on either the console or the managed hosts.
- Software versions for all JSA appliances in a deployment must be the same version and patch level. Note that deployments that use different versions of software are not supported.

And keep the following information ready at hand:

- Hostname
- IP address
- Network mask
- Default gateway address
- Primary Domain Name System (DNS) server address
- Secondary DNS server address (Optional)
- (Optional) Public IP address for networks using Network Address Translation (NAT)
- Email server name

Step-by-Step Procedure

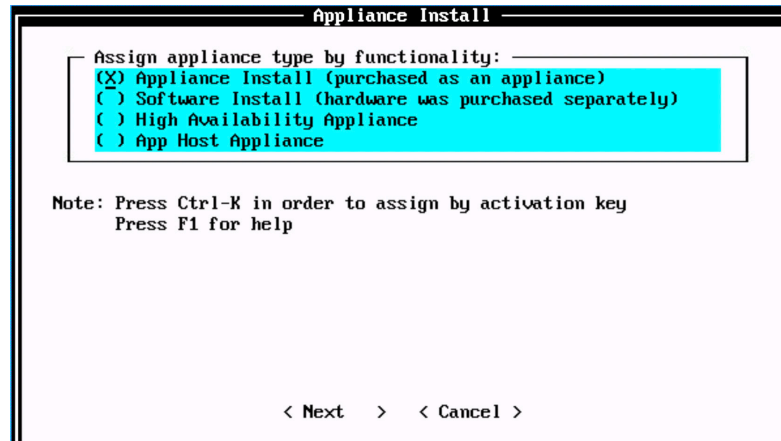
Follow the steps in the installation wizard for the hardware or the virtual appliance type you are creating. Log in as the root user at the prompt (a password is not required). If you are prompted for a password, there is some error with the installation. Contact <https://support.juniper.net/support/>.

The JSA installation wizard allows you to use only certain keyboard keys to navigate through the installation options. Table P1 lists these keys along with how you can use them.

Read and accept the EULA license and proceed with the installation providing information for the installation wizard when prompted.

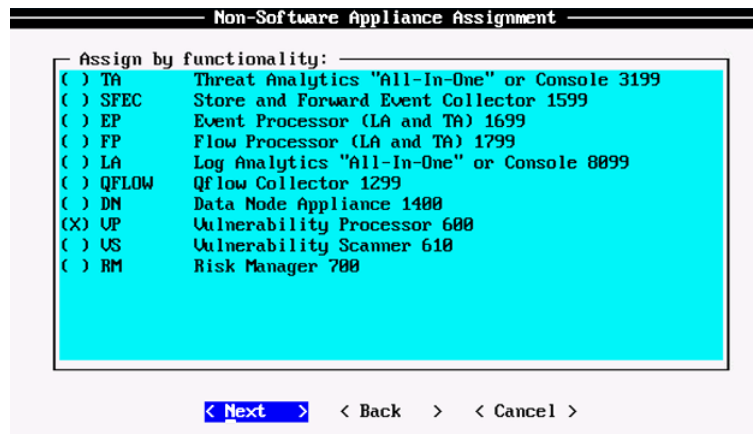
After accepting EULA license, the Appliance Install page appears (Figure 182). Select Appliance Install (purchased as an appliance). Choose this option if you have purchased JSA appliances or wish to install virtual machines. Select Next.

Figure 182 Appliance Install Options



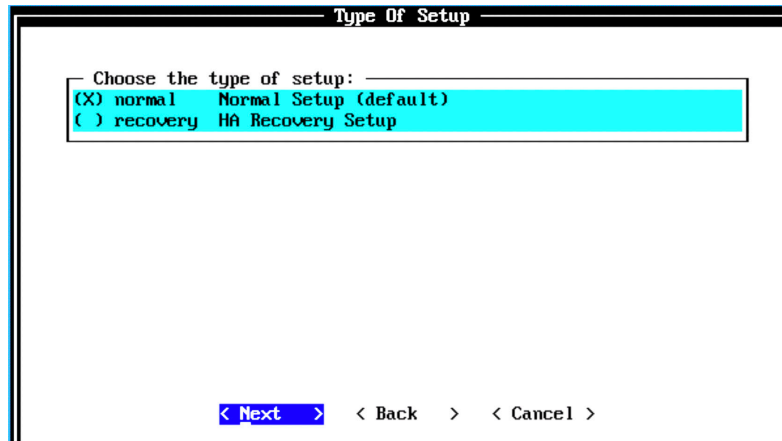
The Non-Software Appliance Assignment page appears (Figure 183). Select the non-software appliance type as *Vulnerability Processor 600* and select Next.

Figure 183 Non-Software Appliance Assignment Options



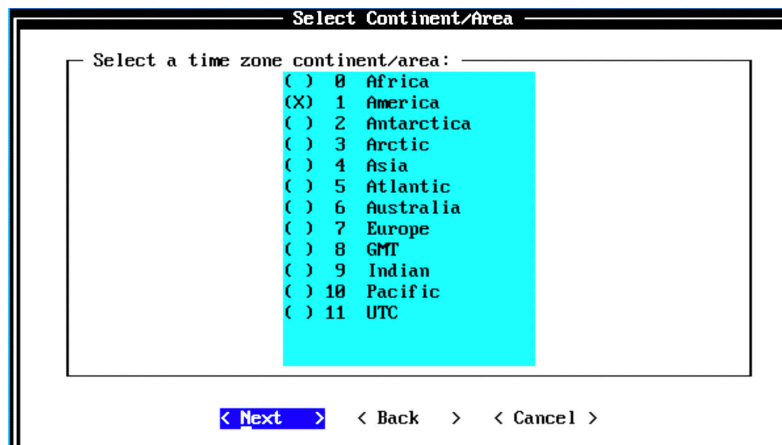
The Type of Setup page appears. Select the Normal Setup (default) option and select Next.

Figure 184 Setup Options



The Select Continent/Area page appears (Figure 185). Select the time zone continent or area as required and select Next. The default value is America.

Figure 185 Select Continent/Area Options



The Time Zone Selection page appears (Figure 186). Select the time zone city or region as required and select Next. The default value is New_York (Eastern (most areas)).

Figure 186 Time Zone Options

Time Zone Selection

Select a time zone city or region: _____

- ☐ 94 Miquelon
- ☐ 95 Moncton (Atlantic - New Brunswick)
- ☐ 96 Monterrey (Central Time - Durango: Coahuila, Nuevo Leon, Tam)
- ☐ 97 Montevideo
- ☐ 98 Montserrat
- ☐ 99 Nassau
- ☒ 100 New_York (Eastern (most areas))
- ☐ 101 Nipigon (Eastern - ON, QC (no DST 1967-73))
- ☐ 102 Nome (Alaska (west))
- ☐ 103 Noronha (Atlantic islands)
- ☐ 104 North_Dakota/Beulah (Central - ND (Mercer))
- ☐ 105 North_Dakota/Center (Central - ND (Oliver))
- ☐ 106 North_Dakota/New_Salem (Central - ND (Morton rural))
- ☐ 107 Ojinaga (Mountain Time US - Chihuahua (US border))

< Next > < Back > < Cancel >

The Internet Protocol Setup page appears (Figure 187). By default, the Internet Protocol version is selected as IPv4 Internet Protocol version 4. You can select IPv6 Internet Protocol version 6, if required. Select No as the value for Do not use bonded interface configuration mode (you can use the bonded interface configuration mode, if required). Select Next.

Figure 187 Internet Protocol Setup Options

Internet Protocol Setup

Choose which Internet protocol version to use: _____

- ☒ ipv4 Internet Protocol version 4
- ☐ ipv6 Internet Protocol version 6

Choose interface configuration mode: _____

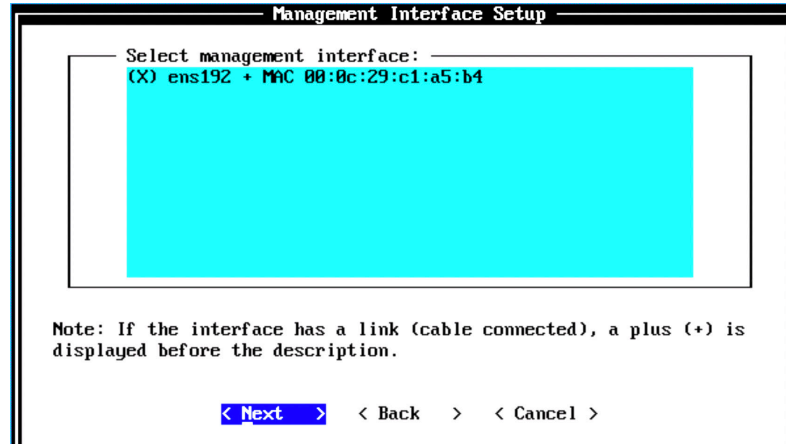
- ☒ No Do not use bonded interface configuration mode

< Next > < Back > < Cancel >

The Management Interface Setup page appears (Figure 188). Select the management interface that you want to use and select Next.

NOTE The list shown will depend on the number of NIC cards on the hardware that you are installing JSA upon. All available interfaces will be displayed here.

Figure 188 *Management Interface Setup Options*



The Network Information Setup page appears (Figure 189). Configure the following network settings here:

- 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.
- Email Server—Enter the email server. If you do not have an e-mail server, type localhost in this field.

Once complete, select Next.

Figure 189 Network Information Setup Options

Network Information Setup

Enter network information to use:

Hostname:

IP Address: Primary DNS:

Network Mask: 255.255.255.0 Secondary DNS:

Gateway: Public IP:

Email Server: localhost

< Next > < Back > < Cancel >

The network settings are validating and may take a few minutes.

It's time to configure the root password required to log in to the JSA CLI. In Root Password Setup (Figure 190), enter a root password that meets the following criteria: contains at least 5 characters, contains no spaces, can include the following special characters: @, #, ^, and *.

Re-enter the root password in the Confirm New Root Password field and select Finish.

Figure 190 Root Password Options

Root Password Setup

Enter New Root Password:

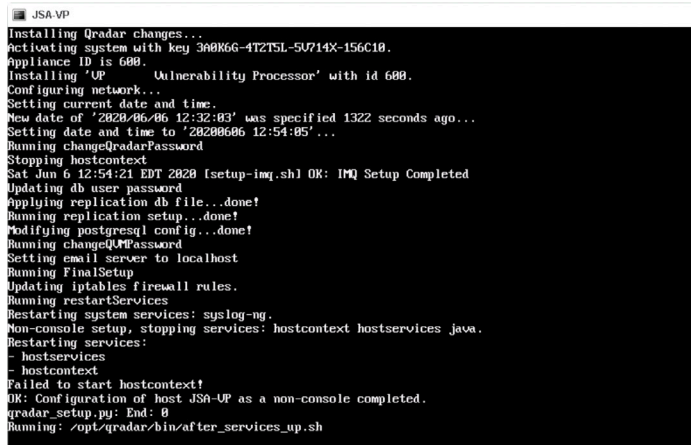
Confirm New Root Password:

The password must not be longer than 255 character and not contain spaces.

< Finish > < Back > < Cancel >

When you select Finish, the installation process begins, and it typically takes several minutes. Although it might appear as the system is not responding at times, wait for the installation to complete.

Figure 191 Installing Changes



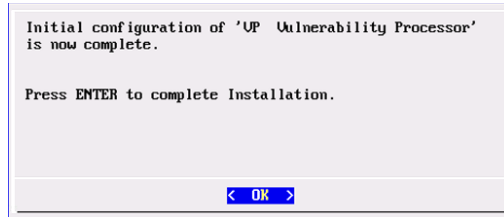
```

JSA-VP
Installing Qradar changes...
Activating system with key 3a0866-4T2TSL-5U714X-156C10.
Appliance ID is 600.
Installing 'UP Vulnerability Processor' with id 600.
Configuring network...
Setting current date and time.
New date of '2020/06/06 12:32:03' was specified 1322 seconds ago...
Setting date and time to '20200606 12:54:05'...
Running changeQradarPassword
Stopping hostcontext
Sat Jun 6 12:54:21 EDT 2020 [setup-imq.sh] OK: IMQ Setup Completed
Updating db user password
Applying replication db file...done!
Running replication setup...done!
Modifying postgresql config...done!
Running changeQUPPassword
Setting email server to localhost
Running FinalSetup
Updating iptables firewall rules.
Running restartServices
Restarting system services: syslog-ng.
Non-console setup, stopping services: hostcontext hostservices java.
Restarting services:
+ hostservices
+ hostcontext
Failed to start hostcontext!
OK: Configuration of host JSA-UP as a non-console completed.
qradar_setup.py: End: 0
Running: /opt/qradar/bin/after_services_up.sh

```

The output shown in Figure 192 indicates a successful installation of a vulnerability processor. Once the installation is complete, a completion message is displayed. Click OK.

Figure 192 Installation Complete



Verification

To verify the successful installation of a vulnerability processor, run the following command on the console:

Run `less /etc/.appliance_name`

The output displays 600 as the appliance installed. Ping the default gateway to ensure that the connectivity is fine. You can also use the `ifconfig` command to view the IP address details of the appliance.

Next Steps

After installing the vulnerability processor, you can add it to the deployment using JSA web UI. For more information about adding a vulnerability processor, see *Adding a Dedicated Vulnerability Processor*.

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system, before the default license expires. For more information about applying a license, see section *Apply a License to JSA*.

Add a Dedicated Vulnerability Processor

JSA supports only one vulnerability processor (VP) in a deployment. By default, the console acts as the VP and vulnerability scanner (VS) when you apply a vulnerability manager license. However, when you need to scan a high number of hosts (for example, 50K assets), it is recommended that you use a dedicated VP.

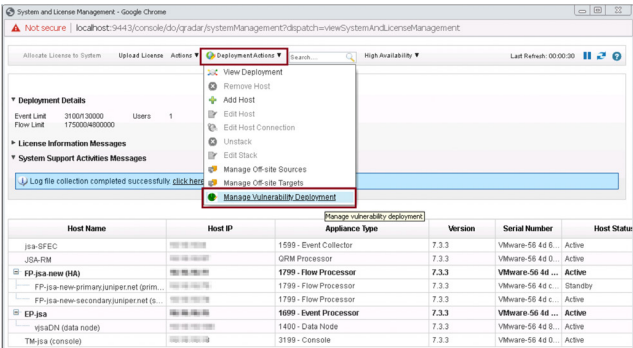
NOTE For more information about vulnerability scanner, see section *Install and Configure a Vulnerability Scanner*.

After you install the VP, you can add it to the deployment. Since there can be only one VP in a deployment, you need to first remove the existing VP (console) and then add the new dedicated VP to the deployment.

To Remove the Existing VP (Console)

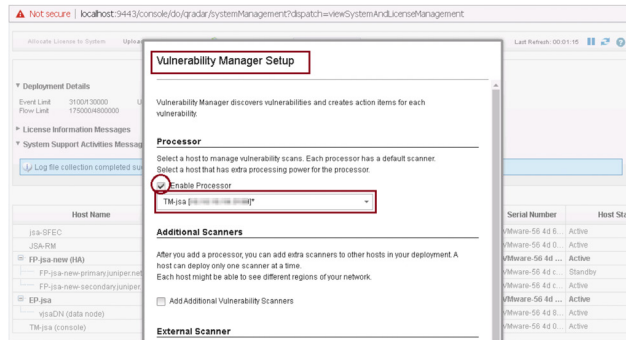
Log in to the JSA web UI. On the navigation menu, click Admin. The Admin page appears. In the System Configuration section, click System and License Management. The System and License Management page appears. Select Manage Vulnerability Deployment and the Vulnerability Manager Setup (Figure 194) window appears.

Figure 193 Manage Vulnerability Deployment



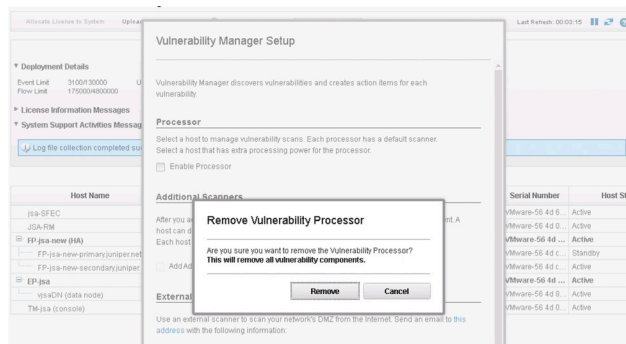
Uncheck the Enable Processor, as shown in Figure 194.

Figure 194 Vulnerability Manager Setup



The Remove Vulnerability Processor pop-up appears asking for confirmation to remove the vulnerability processor (console). Click Remove, as shown in Figure 195.

Figure 195 Remove Vulnerability Processor



Now scroll to the bottom if necessary and click Save to save the changes to the vulnerability manager settings, as shown in Figure 196.

Figure 196 Save Vulnerability Manager Settings

Vulnerability Manager Setup

Vulnerability Manager discovers vulnerabilities and creates action items for each vulnerability.

Processor

Select a host to manage vulnerability scans. Each processor has a default scanner. Select a host that has extra processing power for the processor.

☐ Enable Processor

Additional Scanners

After you add a processor, you can add extra scanners to other hosts in your deployment. A host can deploy only one scanner at a time. Each host might be able to see different regions of your network.

☐ Add Additional Vulnerability Scanners

External Scanner

Use an external scanner to scan your network's DMZ from the Internet. Send an email to this address with the following information:

- Your organization's external IP address
- The IP address range of the assets that are in your DMZ

You must allow outbound Internet access on port 443. You must configure the external IP address before you can run external scans.

☐ Use External Scanner

SiteProtector™

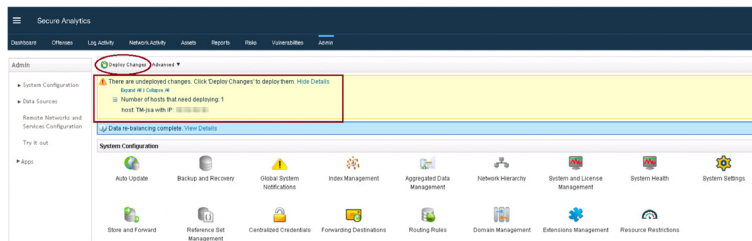
You can forward detected vulnerabilities to SiteProtector™ for analysis.

☐ Use SiteProtector™

Save **Close**

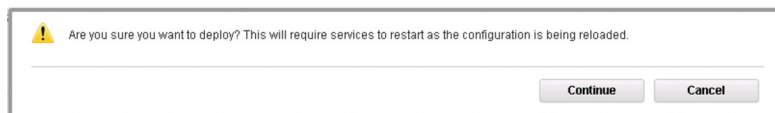
You must now deploy these changes. To do so, go to the Admin tab to see the changes that need to be deployed, as shown in Figure 197.

Figure 197 Deploy Vulnerability Manager Settings



Click Deploy Changes. The deployment process starts as shown in Figure 198. This process might take a few minutes. Please wait for the deployment process to complete.

Figure 198 Deployment Confirmation

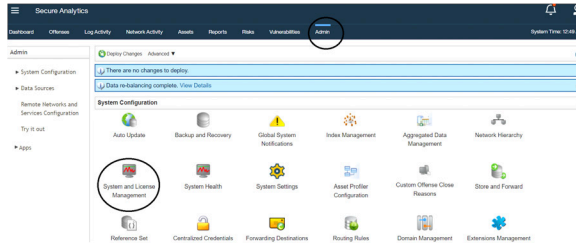


After the deployment process is complete, the console is removed from the role of VP in the deployment.

Add the Dedicated VP

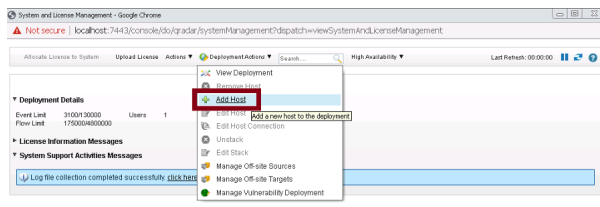
You can now add the dedicated VP by logging in to the JSA web UI. On the navigation menu, click Admin. The Admin page appears (Figure 199). In the System Configuration section, click System and License Management.

Figure 199 System and License Management



The System and License Management page appears. On the navigation menu, select Deployment Actions > Add Host.

Figure 200 Deployment Actions > Add Host



The Add Managed Host page appears (Figure 201). Enter the fixed IP address of the VP node you want to add in the Host IP field. Enter the root password for the host IP in the Host Password field and re-enter the root password in the Confirm Password field. When complete, click Add.

Figure 201 Add Managed Host

Add Managed Host

Before you add a managed host, make sure the managed host includes the SIEM software. The IP of the host is required as well as the root password. Hover over label fields for more information.

Host IP:

Host Password:

Confirm Password:

☐
Encrypt Host Connections:

☐
Encryption Compression:

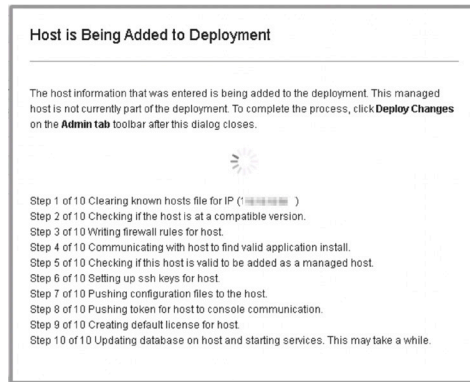
☐
Network Address Translation:

NAT Group:

Public IP:

A pop-up appears displaying the status of the host being added to the network.

Figure 202 *Host is Being Added to Deployment*



After the host is added successfully, the new host is now listed on the System and License Management page. Note that at this point, the new host is *not* deployed. Close the System and License Management page and go to the Admin page to deploy the changes. The changes that need to be deployed are shown on top of the page (Figure 203). Click View Details to see the changes.

Figure 203 *Undeployed Changes*

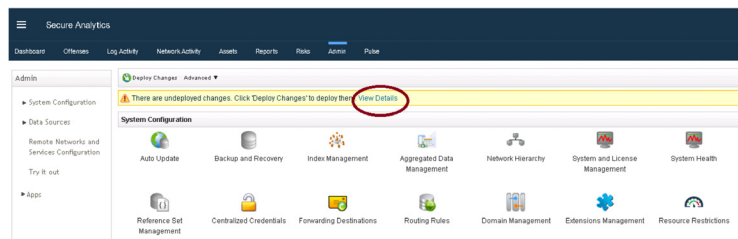
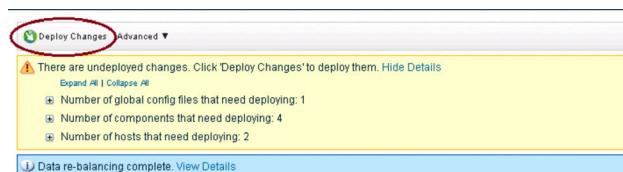


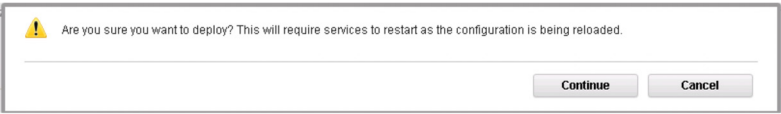
Figure 204 *Changes to be Deployed*



Click Deploy Changes.

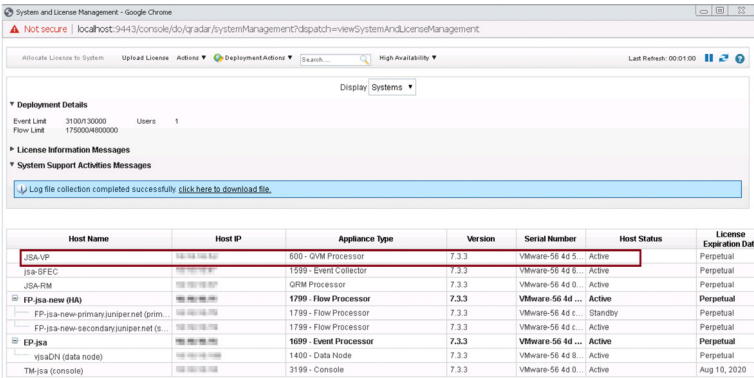
A confirmation page appears asking for confirmation to deploy the changes, as shown in Figure 205. Click Continue to deploy the changes.

Figure 205 Deployment Confirmation



The deployment starts and typically takes several minutes. Although it might appear as if the system is not responding at times, wait for the deployment to complete. The JSA web UI will display the progress in the deployment process. After the deployment is complete, you can see the new VP node that you have added in the System and License Management page, as shown in Figure 206.

Figure 206 Dedicated VP Added to Deployment

A screenshot of the 'System and License Management' page in a web browser. The page shows deployment details, license information, and a table of systems. A red box highlights the 'JSA-VP' row in the table.

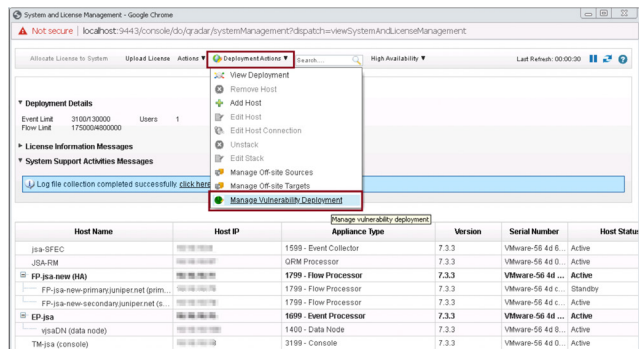
Host Name	Host IP	Appliance Type	Version	Serial Number	Host Status	License Expiration Date
JSA-VP	192.168.1.100	800 - QRM Processor	7.3.3	Vmware-56 4d 5	Active	Perpetual
JSA-SEC	192.168.1.101	1599 - Event Collector	7.3.3	Vmware-56 4d 5	Active	Perpetual
JSA-RM	192.168.1.102	QRM Processor	7.3.3	Vmware-56 4d 0	Active	Perpetual
FP-JSA-new (HA)	192.168.1.103	1799 - Flow Processor	7.3.3	Vmware-56 4d ...	Active	Perpetual
FP-JSA-new-primaryjuniper.net (prim...	192.168.1.104	1799 - Flow Processor	7.3.3	Vmware-56 4d c	Standby	Perpetual
FP-JSA-new-secondaryjuniper.net (s...	192.168.1.105	1799 - Flow Processor	7.3.3	Vmware-56 4d c	Active	Perpetual
EP-JSA	192.168.1.106	1699 - Event Processor	7.3.3	Vmware-56 4d ...	Active	Perpetual
visaCN (data node)	192.168.1.107	1400 - Data Node	7.3.3	Vmware-56 4d 0	Active	Perpetual
TM-JSA (console)	192.168.1.108	3199 - Console	7.3.3	Vmware-56 4d 0	Active	Aug 10, 2020

Enable the New VP

You must enable the newly added VP node and deploy the changes to the deployment, so that it can act as the VP of the deployment.

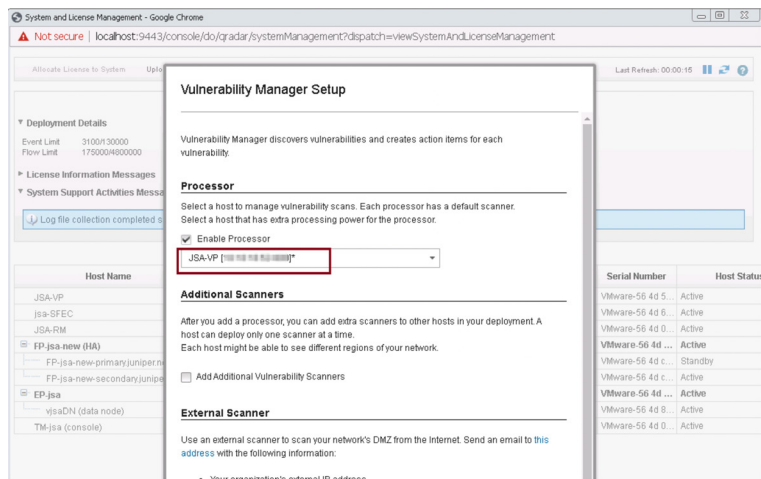
Log in to the JSA web UI. On the navigation menu, click Admin. The Admin page appears. In the System Configuration section, click System and License Management. The System and License Management page appears. Select Manage Vulnerability Deployment and the Vulnerability Manager Setup window appears (Figure 207).

Figure 207 Manage Vulnerability Deployment



Check Enable Processor and select the newly added VP in the drop-down, as shown in Figure 208.

Figure 208 Vulnerability Manager Setup



Click Save to save the changes to the vulnerability manager settings, as shown in Figure 209.

Figure 209 Save Vulnerability Manager Settings

Vulnerability Manager Setup

Vulnerability Manager discovers vulnerabilities and creates action items for each vulnerability.

Processor

Select a host to manage vulnerability scans. Each processor has a default scanner. Select a host that has extra processing power for the processor.

☒ Enable Processor

JSA-IP [10.10.10.10]

Additional Scanners

After you add a processor, you can add extra scanners to other hosts in your deployment. A host can deploy only one scanner at a time. Each host might be able to see different regions of your network.

☐ Add Additional Vulnerability Scanners

External Scanner

Use an external scanner to scan your network's DMZ from the Internet. Send an email to this address with the following information:

- Your organization's external IP address
- The IP address range of the assets that are in your DMZ

You must allow outbound internet access on port 443. You must configure the external IP address before you can run external scans.

☐ Use External Scanner

SiteProtector™

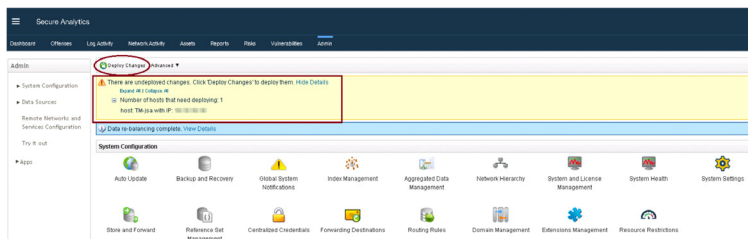
You can forward detected vulnerabilities to SiteProtector™ for analysis.

☐ Use SiteProtector™

Save Close

You must now deploy these changes for the changes to come into effect in the deployment. To do so, go to the Admin tab to see the changes that need to be deployed, as shown in Figure 210.

Figure 210 Deploy Vulnerability Manager Settings



Click Deploy Changes. A confirmation page appears asking for confirmation to deploy the changes (Figure 211). Click Continue to deploy the changes.

Figure 211 Deployment Confirmation

Are you sure you want to deploy? This will require services to restart as the configuration is being reloaded.

Continue Cancel

The deployment starts and can take several minutes. Although it might appear as if the system is not responding at times, wait for the deployment to complete. The JSA web UI displays the progress in the deployment process. After the deployment is complete, the newly added VP acts as the dedicated VP for your deployment.

Next Steps

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system, before the default license expires.

For more information about applying a license, see section *Apply a License to JSA*.

Install and Configure a Vulnerability Scanner

Any device such as an AIO-console, event processor, SFEC, FP, or RM can act as a vulnerability scanner. A VS can be any appliance from where a vulnerability assessment scan is triggered towards a target machine.

However, it may not be feasible to trigger a vulnerability assessment scan from any part of the network due to security reasons. You may, therefore, need to add dedicated VS appliances for this purpose.

To deploy a dedicated VS appliance in your deployment you must complete the following tasks:

- Install a dedicated VS using the instructions provided in this section.
- Add the VS to your deployment using the instructions provided in section *Add a Dedicated Vulnerability Scanner*.
- Apply a license to the vulnerability scanner using the instructions *Apply a License to JSA*.

Before You Begin

Before you start the installation, ensure that you have the following in place:

- The required hardware is installed (in case of appliances).
- You have the required license key for your appliance.

- A keyboard and monitor are connected by using the VGA connection (in case of hardware appliances).
- There are no expired licenses on either the console or the managed hosts.
- Software versions for all JSA appliances in a deployment must be the same version and patch level. Note deployments that use different versions of software are not supported.

Keep the following information ready for the installation:

- Hostname
- IP address
- Network mask
- Default gateway address
- Primary Domain Name System (DNS) server address
- Secondary DNS server address (Optional)
- (Optional) Public IP address for networks using Network Address Translation (NAT)
- Email server name

Step-by-Step Procedure

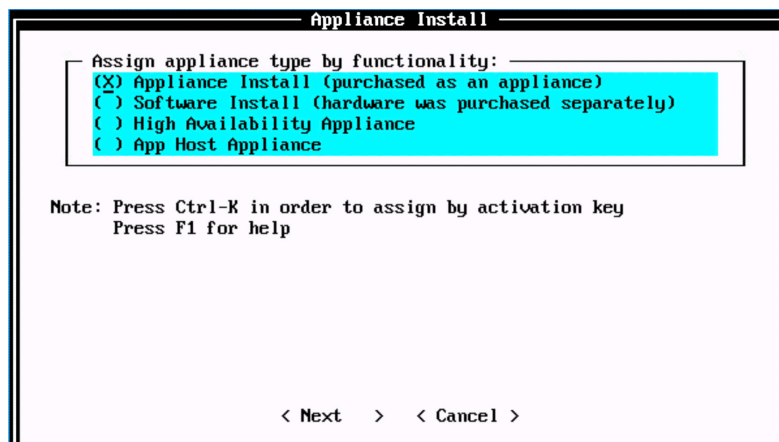
Follow the steps in the installation wizard for the hardware or the virtual appliance type you are creating.

The JSA installation wizard allows you to use only certain keyboard keys to navigate through the installation options. Table P1 lists these keys along with how you can use them.

First of all, log in as the root user at the prompt (a password is not required). If you are prompted for a password, there is some error with the installation. Contact <https://support.juniper.net/support/>.

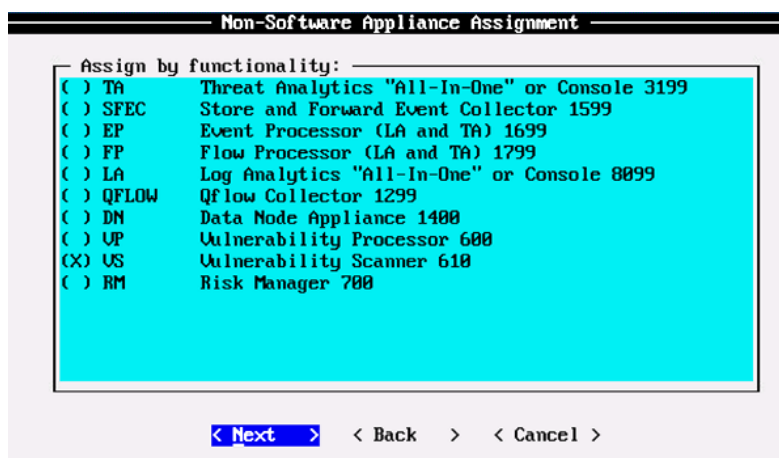
Read and accept the EULA license and proceed with the installation. After accepting EULA license, the Appliance Install page appears (Figure 212). Select Appliance Install (purchased as an appliance). Choose this option if you have purchased JSA appliances or wish to install virtual machines. Select Next.

Figure 212 Appliance Install Options



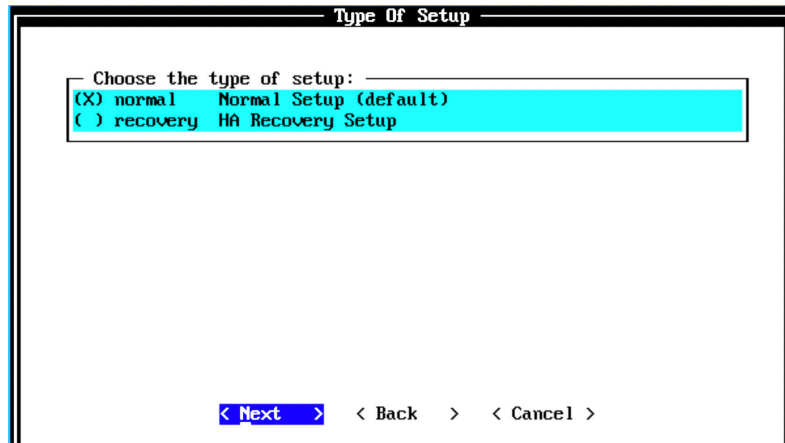
The Non-Software Appliance Assignment page appears. Select the non-software appliance type as Vulnerability Scanner and select Next.

Figure 213 Non-Software Appliance Assignment Options



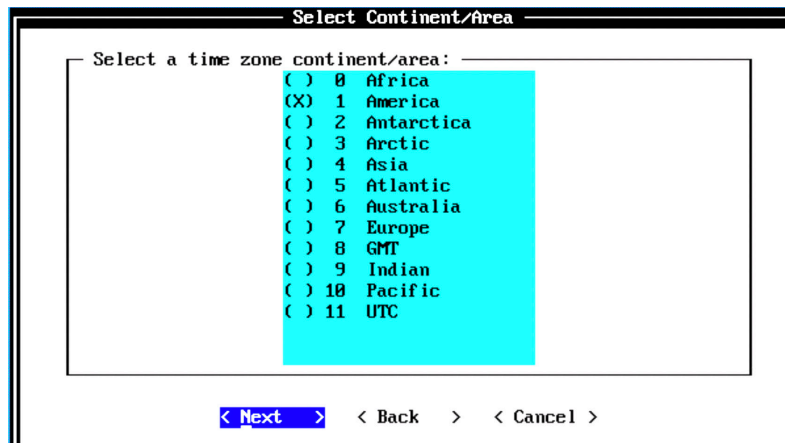
The Type Of Setup page appears (Figure 214). Select the Normal Setup (default) option and select Next.

Figure 214 Setup Options



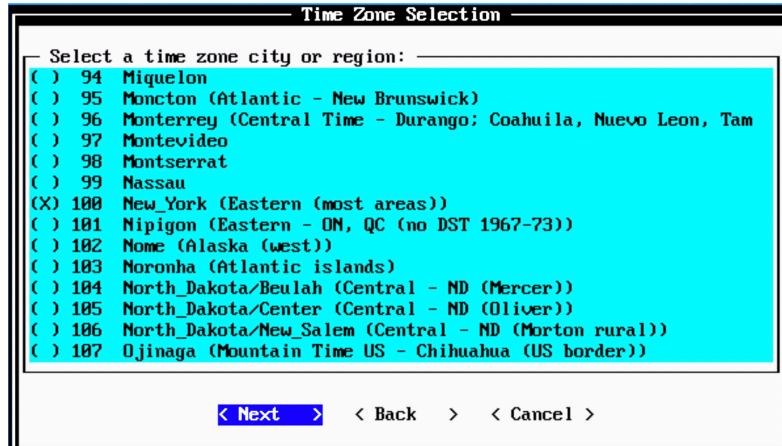
The Select Continent/Area page appears. Select the time zone continent or area as required and select Next. The default value is America.

Figure 215 Select Continent/Area Options



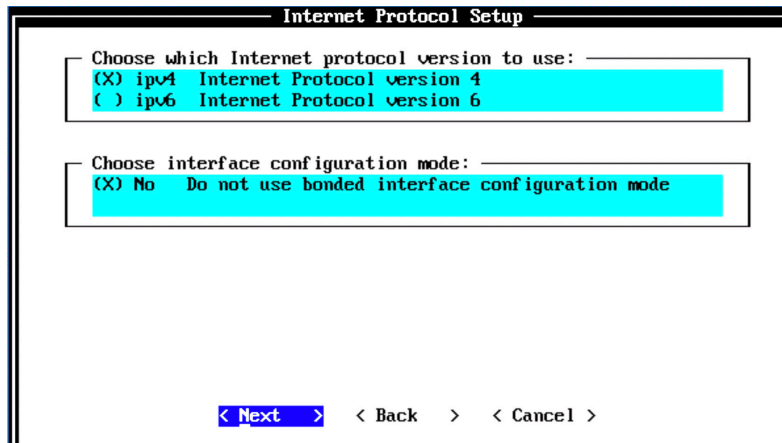
The Time Zone Selection page appears. Select the time zone city or region as required and select Next. The default value is New-York (Eastern (most areas)).

Figure 216 Time Zone Options



The Internet Protocol Setup page appears (Figure 217). By default, the Internet Protocol version is selected as IPv4 Internet Protocol version 4. You can select IPv6 Internet Protocol version 6, if required. Select No as the value for Do not use bonded interface configuration mode. You can use the bonded interface configuration mode, if required. Select Next.

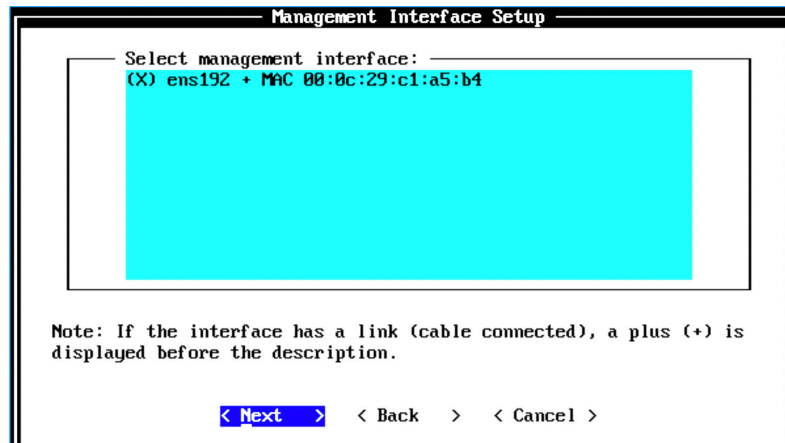
Figure 217 Internet Protocol Setup Options



The Management Interface Setup page appears (Figure 218). Select the management interface that you want to use and select Next.

NOTE The list shown will depend on the number of NIC Cards on the hardware that you are installing JSA on. All the available interfaces will be displayed in this section.

Figure 218 *Management Interface Setup Options*



The Network Information Setup page appears. Configure the following network settings:

- 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.
- Email Server—Enter the email server. If you do not have an e-mail server, type localhost in this field.

Select Next.

Figure 219 Network Information Setup Options

Network Information Setup

Enter network information to use:

Hostname: [redacted]

IP Address: [redacted] Primary DNS: [redacted]

Network Mask: 255.255.255.0 Secondary DNS: [redacted]

Gateway: [redacted] Public IP: [redacted]

Email Server: localhost

< Next > < Back > < Cancel >

The network settings are validating and it may take a few minutes.

Next configure the root password required to log in to the JSA Command Line Interface (CLI). In the Enter New Root Password field, enter a root password that meets the following criteria: contains at least 5 characters, contains no spaces, can include the following special characters: @, #, ^, and *. Re-enter the root password in the Confirm New Root Password field and select Finish.

Figure 220 Root Password Options

Root Password Setup

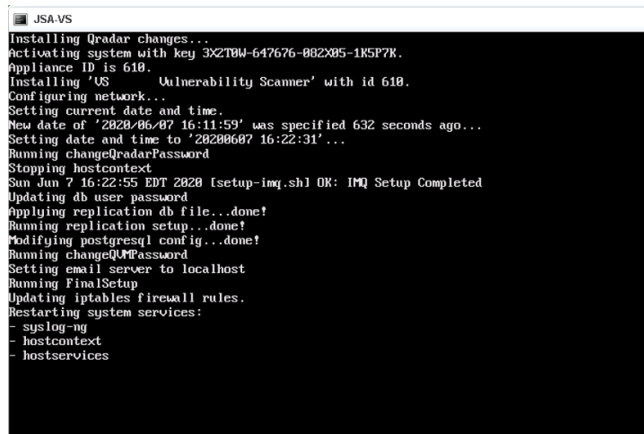
Enter New Root Password: [redacted]

Confirm New Root Password: [redacted]

The password must not be longer than 255 character and not contain spaces.

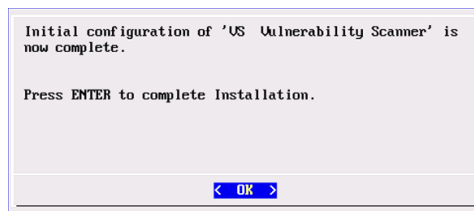
< Finish > < Back > < Cancel >

When you select Finish, the installation process starts. This process typically takes several minutes. Although it might appear as if the system is not responding at times, wait for the installation to complete.

Figure 221 *Installing Changes*A terminal window titled 'JSA-VS' showing the output of a script. The text is as follows:

```
Installing Qradar changes...
Activating system with key 3XZT8W-647676-882X85-1K5P7K.
Appliance ID is 610.
Installing 'US Vulnerability Scanner' with id 610.
Configuring network...
Setting current date and time.
New date of '2020/06/07 16:11:59' was specified 632 seconds ago...
Setting date and time to '20200607 16:22:31' ...
Running changeQradarPassword
Stopping hostcontext
Sun Jun 7 16:22:55 EDT 2020 [setup-imq.sh] OK: IMQ Setup Completed
Updating db user password
Applying replication db file...done!
Running replication setup...done!
Modifying postgresql config...done!
Running changeQUPPassword
Setting email server to localhost
Running FinalSetup
Updating iptables firewall rules.
Restarting system services:
- syslog-ng
- hostcontext
- hostservices
```

The output shown in Figure 222 indicates a successful installation of a vulnerability scanner. Once the installation is complete, a completion message is displayed. Click OK.

Figure 222 *Installation Complete*

Verification

To verify the successful installation of the VS, run the following command on the console:

Run `less /etc/.appliance_name`

The output displays 610 as the appliance installed. Ping the default gateway to ensure that the connectivity is fine. You can also use the `ifconfig` command to view the IP address details of the appliance.

Next Steps

After you have completed installing the VS, you can add it to the deployment using JSA web UI. For more information about adding a vulnerability scanner, see the next section, *Adding a Dedicated Vulnerability Scanner*.

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system, before the default license expires. For more information about applying a license, see section *Apply a License to JSA*.

Add a Vulnerability Scanner to Deployment

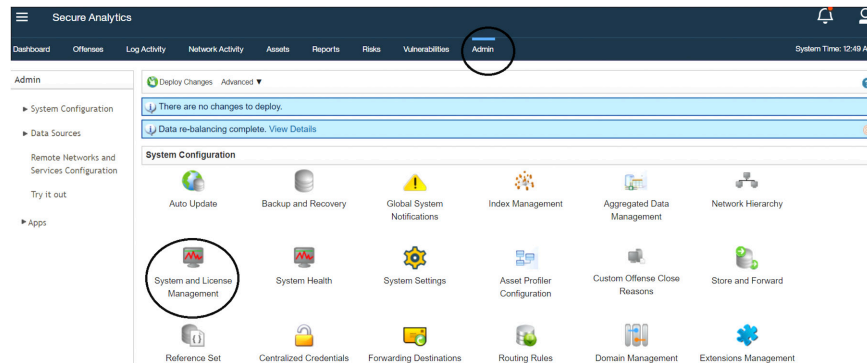
Now that you have installed a vulnerability scanner (VS), let's add it to the deployment.

NOTE Ensure that the VS has the same JSA version and patch, as the JSA console that you are using to manage it.

To add a VS to your deployment, log in to the JSA web UI. On the navigation menu, click Admin. The Admin page appears (Figure 223). In the System Configuration section, click System and License Management.

Figure 223

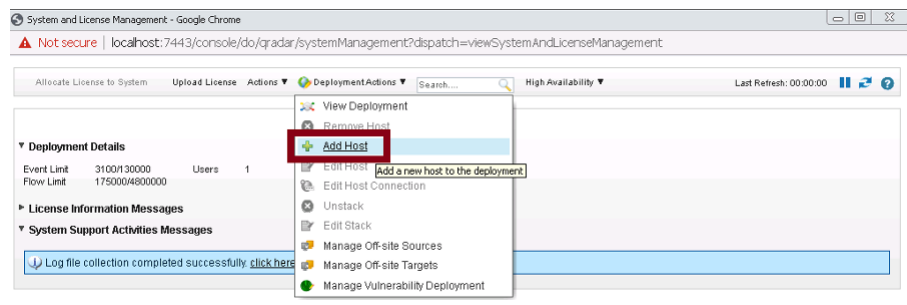
System and License Management



The System and License Management page appears. On the navigation menu, select Deployment Actions > Add Host.

Figure 224

Deployment Actions > Add Host



The Add Management Host page appears. Enter the fixed IP address of the VS node you want to add in the Host IP field. Enter the root password for the host IP in the Host Password field and re-enter the root password in the Confirm Password field. When complete, click Add.

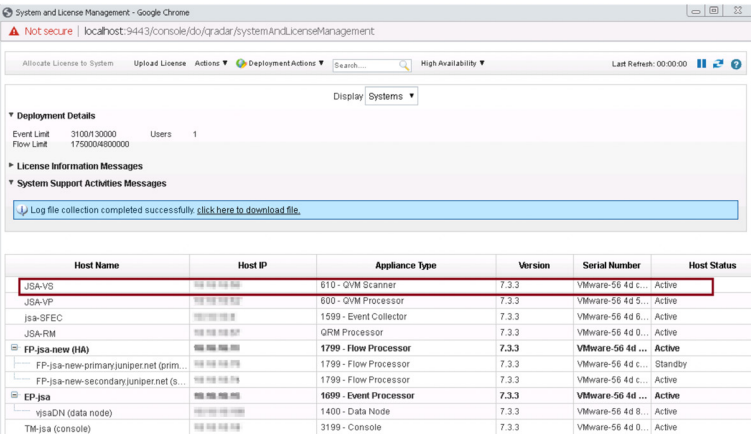
Figure 225 Add Managed Host

A pop-up appears displaying the status of the host being added to the network.

Figure 226 Host is Being Added to Deployment

After the host is added successfully, the VS node appears in the System and License Management page, as shown in Figure 227.

Figure 227 New Vulnerability Scanner



The screenshot shows the 'System and License Management' console. It includes sections for 'Deployment Details' (Event Limit: 31000/30000, Flow Limit: 175000/480000, Users: 1), 'License Information Messages', and 'System Support Activities Messages' with a message about log file collection. Below is a table of systems:

Host Name	Host IP	Appliance Type	Version	Serial Number	Host Status
JSA-VS	192.168.1.100	610 - QVM Scanner	7.3.3	VMware-56 4d c...	Active
JSA-VP	192.168.1.101	600 - QVM Processor	7.3.3	VMware-56 4d 5...	Active
JSA-SFEC	192.168.1.102	1599 - Event Collector	7.3.3	VMware-56 4d 8...	Active
JSA-RM	192.168.1.103	QRM Processor	7.3.3	VMware-56 4d 0...	Active
EP-JSA-new (HA)	192.168.1.104	1799 - Flow Processor	7.3.3	VMware-56 4d ...	Active
FP-JSA-new-primaryjuniper.net (prim...	192.168.1.105	1799 - Flow Processor	7.3.3	VMware-56 4d c...	Standby
FP-JSA-new-secondaryjuniper.net (s...	192.168.1.106	1799 - Flow Processor	7.3.3	VMware-56 4d c...	Active
EP-JSA	192.168.1.107	1699 - Event Processor	7.3.3	VMware-56 4d ...	Active
visaDN (data node)	192.168.1.108	1400 - Data Node	7.3.3	VMware-56 4d 8...	Active
TM-JSA (console)	192.168.1.109	3199 - Console	7.3.3	VMware-56 4d 0...	Active

Close the System and License Management page. At this point, the new host is not yet deployed. To deploy the changes, go back to the Admin page (Figure 228). The changes that need to be deployed are shown on top of the page. Click View Details to see the changes.

Figure 228 Undeployed Changes

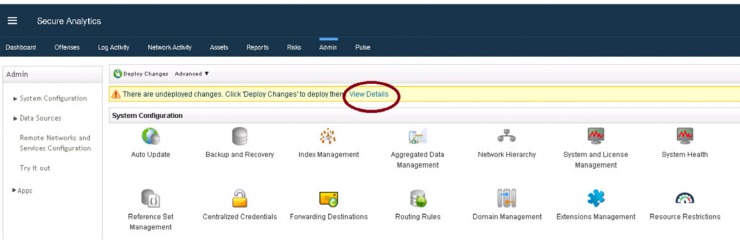


Figure 229 Changes to be Deployed



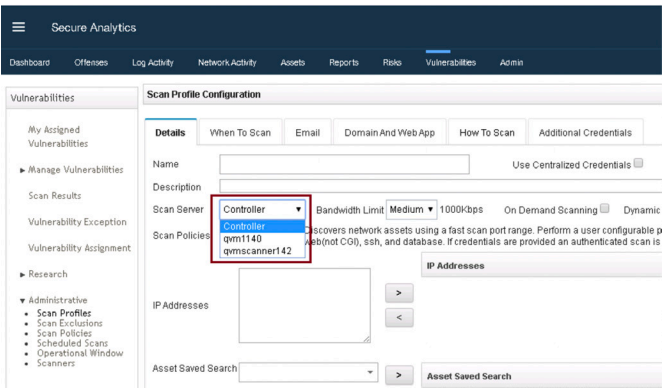
Click **Deploy Changes**. A confirmation page appears asking for confirmation to deploy the changes, as shown in Figure 230. Click **Continue** to deploy the changes.

Figure 230 Deployment Confirmation



The deployment starts. This process typically takes several minutes. Although it might appear as if the system is not responding at times, wait for the deployment to complete. The JSA web UI will display the progress in the deployment process. After the deployment is complete, the newly added VS will be available in the Vulnerabilities tab for VA scan, as shown in Figure 231.

Figure 231 VS Available for Scan



Next Steps

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system, before the default license expires.

For more information about applying a license, see section *Apply a License to JSA*.

Install and Configure an App Host

An app host 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.

NOTE You can have only one app host in your deployment. If you have an environment that uses Network Address Translation (NAT), both the console and the app host must exist within the same NAT group. Port 5000 must be open on your console. For more information, see *Appendix C*.

To complete the installation and configuration of an app host:

- Install an app host using the instructions in this section.
- Add the app host to a deployment using the instructions provided in the section *Add App Hosts to Deployment*.
- Apply a license to the app host using the instructions provided in section *Apply a License to JSA*.

Before You Begin

Before you start the installation, ensure that you have the following in place:

- The required hardware is installed (in case of appliances).
- You have the required license key for your appliance.
- A keyboard and monitor are connected by using the VGA connection (in case of hardware appliances).
- There are no expired licenses on either the console or the managed hosts.
- Software versions for all JSA appliances in a deployment must be the same version and patch level. Note deployments that use different versions of software are not supported.

Keep the following information ready before you begin the installation:

- Hostname
- IP address
- Network mask
- Default gateway address

- Primary Domain Name System (DNS) server address
- Secondary DNS server address (Optional)
- (Optional) Public IP address for networks using Network Address Translation (NAT)
- Email server name

Step-by-Step Procedure

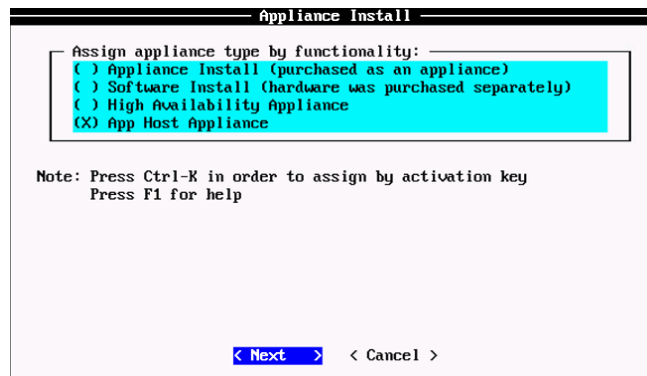
Follow the steps in the installation wizard for the hardware or virtual appliance type you are creating.

The JSA installation wizard allows you to use only certain keyboard keys to navigate through the installation options. Table P1 lists these keys along with how you can use them.

Log in as the root user at the prompt (a password is not required). If you are prompted for a password, there is some error with the installation. Contact <https://support.juniper.net/support/>.

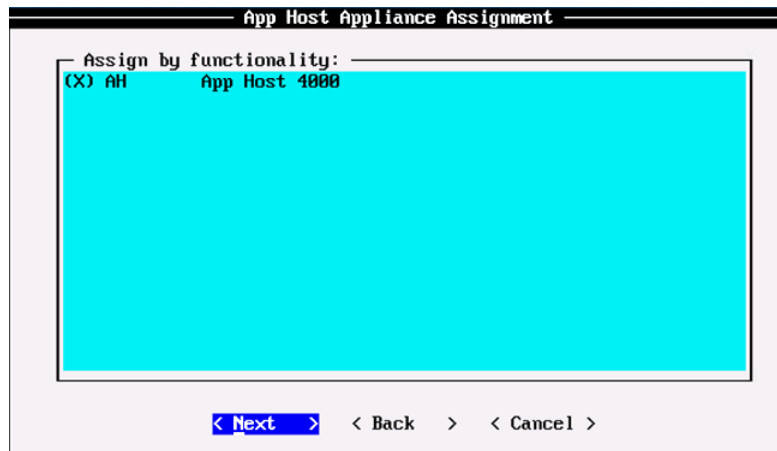
Read and accept the EULA license and proceed with the installation. Provide information in the installation wizard when prompted. After accepting EULA license, the Appliance Install page appears (Figure 232). Select App Host Appliance. Choose this option if you have purchased JSA appliances or wish to install virtual machines. Select Next.

Figure 232 *Appliance Install Options*



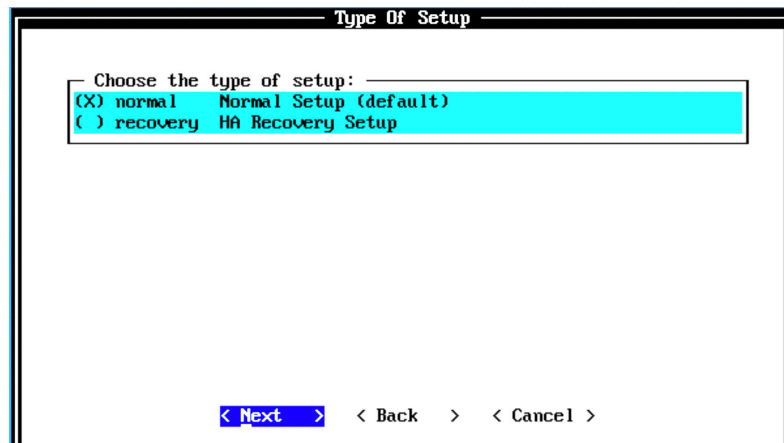
The App Host Appliance Assignment page appears. (Figure 233). Select the appliance type as App Host 4000 and select Next.

Figure 233 App Host Appliance Assignment Options



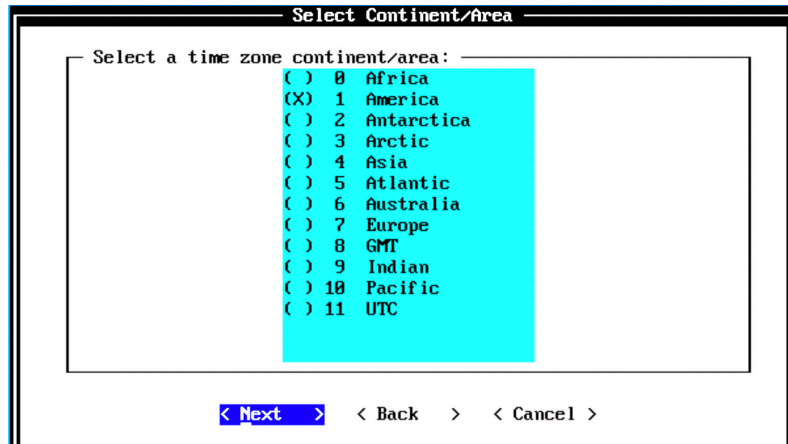
The Type of Setup page appears (Figure 234). Select the Normal Setup (default) option and select Next.

Figure 234 Setup Options



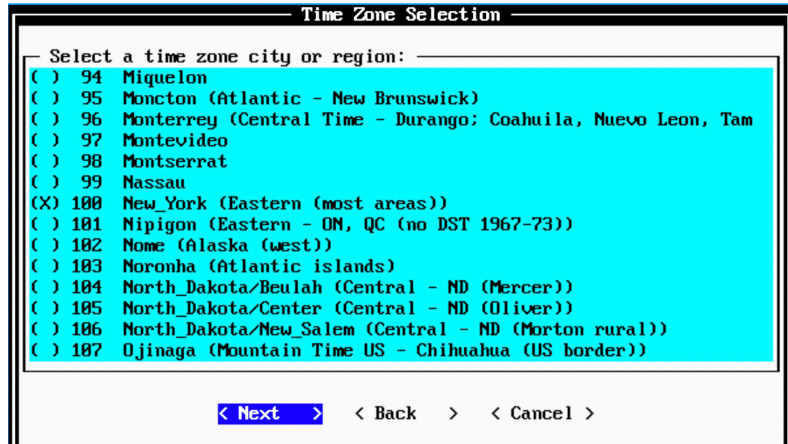
The Select Continent/Area page appears. Select the time zone continent or area as required and select Next. The default value is America.

Figure 235 Select Continent/Area Options



The Time Zone Selection page appears. Select the time zone city or region as required and select Next. The default value is New_York (Eastern (most areas)).

Figure 236 Time Zone Options



The Internet Protocol Setup page appears (Figure 237). By default, the Internet Protocol version is selected as IPv4 Internet Protocol version 4. You can select IPv6 Internet Protocol version 6, if required. Select No as the value for Do not use bonded interface configuration mode. You can use the bonded interface configuration mode, if required. When complete, select Next.

Figure 237 Internet Protocol Setup Options

Internet Protocol Setup

Choose which Internet protocol version to use: _____

☒ ipv4 Internet Protocol version 4

☐ ipv6 Internet Protocol version 6

Choose interface configuration mode: _____

☒ No Do not use bonded interface configuration mode

< Next > < Back > < Cancel >

The Management Interface Setup page appears (Figure 238). Select the management interface that you want to use and select Next.

NOTE The list shown will depend on the number of NIC Cards on the hardware that you are installing JSA upon. All available interfaces will be displayed in this section.

Figure 238 Management Interface Setup Options

Management Interface Setup

Select management interface: _____

☒ ens192 + MAC 08:0c:29:c1:a5:b4

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

< Next > < Back > < Cancel >

The Network Information Setup page appears (Figure 239). Configure the following network settings:

- 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.
- Email Server—Enter the email server. If you do not have an e-mail server, type localhost in this field.

Now select Next.

Figure 239 *Network Information Setup Options*

Network Information Setup

Enter network information to use:

Hostname: <input type="text"/>	
IP Address: <input type="text"/>	Primary DNS: <input type="text"/>
Network Mask: <input type="text"/>	Secondary DNS: <input type="text"/>
Gateway: <input type="text"/>	Public IP: <input type="text"/>
Email Server: <input type="text"/>	

The network settings are validated. This may take a few minutes. Once network settings are validated successfully, the Root Password Setup page appears (Figure 240).

Configure the root password required to login to the JSA Command Line Interface (CLI). In the Enter New Root Password field, enter a root password that meets the following criteria: contains at least 5 characters, contains no spaces, can include the following special characters: @, #, ^, and *. Re-enter the root password in the Confirm New Root Password field and then select Finish.

Figure 240 Root Password Options

Root Password Setup

Enter New Root Password:

Confirm New Root Password:

The password must not be longer than 255 character and not contain spaces.

< Finish >

< Back >

< Cancel >

When you select Finish, the installation process starts. This process can typically take several minutes. Although it might appear as if the system is not responding at times, wait for the installation to complete. Figure 241 indicates that the installation process of an application host is underway.

Figure 241 Installing Changes

```
JSA-AppHost
Installing Qradar changes...
Activating system with key 1U1W1Y-5S783L-1R3B12-8T6Q6Z.
Appliance ID is 4000.
Installing 'AH' App Host' with id 4000.
Configuring network...
Setting current date and time.
New date of '2020/06/06 06:56:34' was specified 1321 seconds ago...
Setting date and time to '20200606 07:18:35'...
Running changeQradarPassword
Stopping hostcontext
Sat Jun 6 07:18:50 EDT 2020 [setup-imq.sh] OK: IMQ Setup Completed
Updating db user password
Applying replication db file...done!
Running replication setup...done!
Modifying postgresql config...done!
Running changeQUTPassword
Setting email server to localhost
Running FinalSetup
Updating iptables firewall rules.
Restarting system services:
- syslog-ng
- hostcontext
- hostservices
Running restartServices
Restarting system services: syslog-ng.
Non-console setup, stopping services: hostcontext hostservices java.
Restarting services:
- hostservices
Failed to start hostservices!
OK: Configuration of host AppHost as a non-console completed.
qradar_setup.py: End: 0
Running: /opt/qradar/bin/after_services_up.sh
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 294 100 294 0 0 1910 0 --:--:-- --:--:-- --:--:-- 1921
```

Once the installation is complete, a final completion message is displayed. Click Ok. This output indicates a successful installation of an application host virtual/hardware appliance.

Figure 242 *Installation Complete*



Verification

To verify the successful installation of an application host, run the following command on the console:

```
Run less /etc/.appliance_name
```

The output displays 4000 as the appliance installed. Ping the default gateway to ensure that the connectivity is fine. You can also use the `ifconfig` command to view the IP address details of the appliance.

Next Steps

After you have completed installing an application host, you can add it to a deployment. For more information about adding an App host, see *Add App Hosts to Deployment*.

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system, before the default license expires.

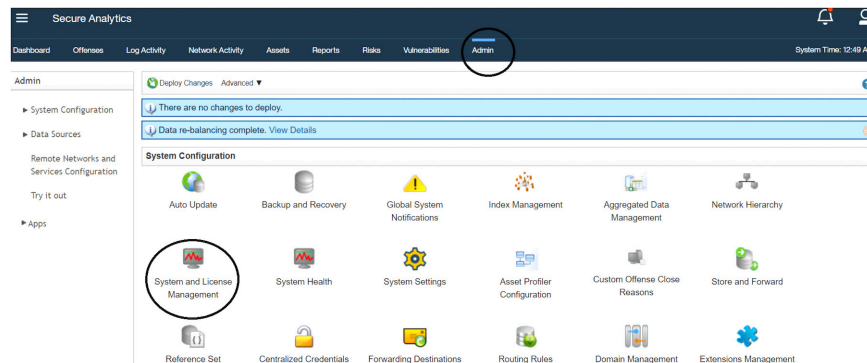
For more information about applying a license, see section *Apply a License to JSA*.

Add App Hosts to Deployment

This section shows how you can add an app host to the deployment.

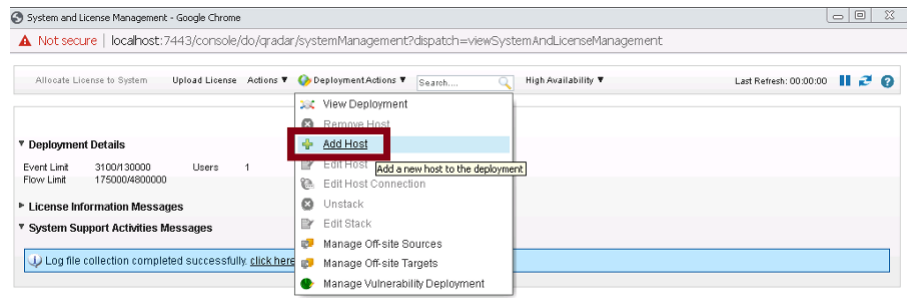
To add an application host to a deployment, log in to the JSA web UI. On the navigation menu, click Admin. The Admin page appears (Figure 243). In the System Configuration section, click System and License Management.

Figure 243 System and License Management



The System and License Management page appears. On the navigation menu, select Deployment Actions > Add Host as shown in Figure 244.

Figure 244 Deployment Actions > Add Host



The Add Managed Host page appears (Figure 245). Enter the fixed IP address of the App Host you want to add in the Host IP field. Enter the root password for the host IP in the Host Password field and re-enter the root password in the Confirm Password field. When complete, click Add.

Figure 245 Add Managed Host

Add Managed Host

Before you add a managed host, make sure the managed host includes the SIEM software. The IP of the host is required as well as the root password. Hover over label fields for more information.

Host IP:

Host Password:

Confirm Password:

Encrypt Host Connections:

☐

Encryption Compression:

☐

Network Address Translation:

☐

NAT Group:

Public IP:

Add

Cancel

NOTE If you are using NAT or want to use an encrypted communication between the app host and the console, select the other options accordingly.

A pop-up appears (Figure 246) displaying the status of the host being added to the network.

Figure 246 Host is Being Added to Deployment

Host is Being Added to Deployment

The host information that was entered is being added to the deployment. This managed host is not currently part of the deployment. To complete the process, click **Deploy Changes** on the **Admin tab** toolbar after this dialog closes.

Step 1 of 10 Clearing known hosts file for IP ()
Step 2 of 10 Checking if the host is at a compatible version.
Step 3 of 10 Writing firewall rules for host.
Step 4 of 10 Communicating with host to find valid application install.
Step 5 of 10 Checking if this host is valid to be added as a managed host.
Step 6 of 10 Setting up ssh keys for host.
Step 7 of 10 Pushing configuration files to the host.
Step 8 of 10 Pushing token for host to console communication.
Step 9 of 10 Creating default license for host.
Step 10 of 10 Updating database on host and starting services. This may take a while.

After the host is added successfully, the new host is listed on the System and License Management page.

Figure 247 Host Successfully Added

Allocate License to System: Upload License Actions Deployment Actions Search... High Availability Last Refresh: 00:00:35					
Display Systems					
Deployment Details					
Apps are set to run on the Console					
There is no app migration in progress					
Click to change where apps are run					
License Information Messages					
System Support Activities Messages					
Host Name	Host IP	Appliance Type	Version	Serial Number	Host Status
jss-SFEC		1599 - Event Collector	7.3.3	VMware-56 4d 6...	Active
FP-jss-new (HA)		1799 - Flow Processor	7.3.3	VMware-56 4d ...	Active
FP-jss-new-primaryjuniper.net (prim...		1799 - Flow Processor	7.3.3	VMware-56 4d c...	Standby
FP-jss-new-secondaryjuniper.net (s...		1799 - Flow Processor	7.3.3	VMware-56 4d c...	Active
EP-jss		1699 - Event Processor	7.3.3	VMware-56 4d ...	Active
vsasDN (Data node)		1400 - Data Node	7.3.3	VMware-56 4d 8...	Active
AppHost		4000 - App Host	7.3.3	VMware-56 4d c...	Active
TM-jss (console)		3199 - Console	7.3.3	VMware-56 4d 0...	Active

Note that at this point, the new host is not deployed. Close the System and License Management page and go to the Admin page to deploy the changes. The changes that need to be deployed are shown on top of the page. Click View Details to see the changes.

Figure 248 Undeployed Changes

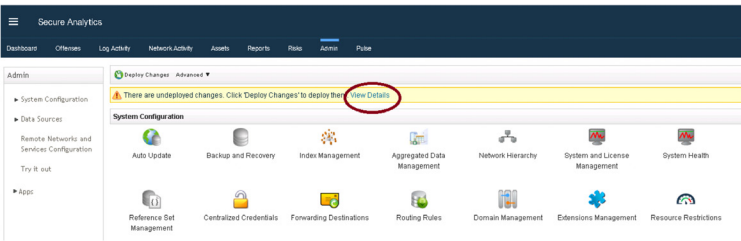
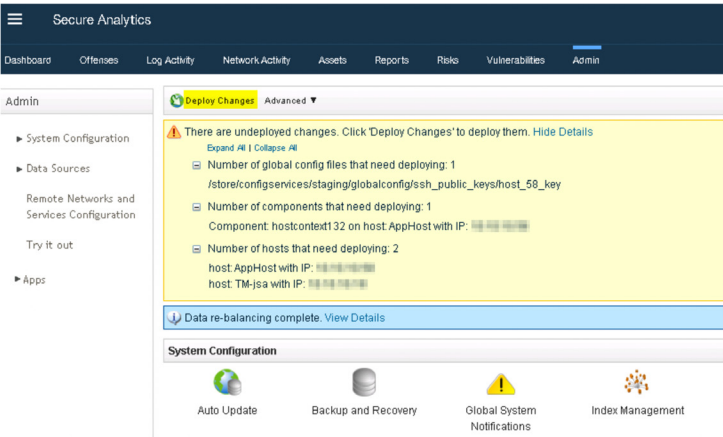
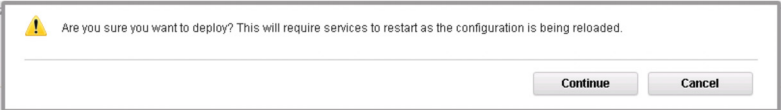


Figure 249 Changes to be Deployed



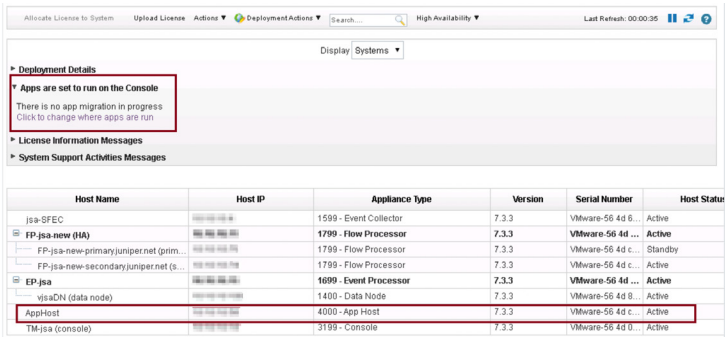
Click **Deploy Changes**. A confirmation page appears asking for confirmation to deploy the changes (Figure 250). Click **Continue** to deploy the changes.

Figure 250 Confirmation for Deployment



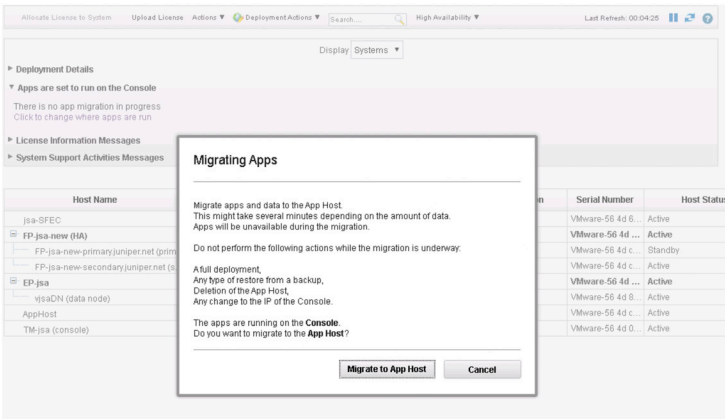
The deployment starts. This process can typically take several minutes. Although it might appear as if the system is not responding at times, wait for the deployment to complete. The JSA web UI will display the progress in the deployment process. After the deployment is complete, you can migrate the apps running on the console to run on the app hosts. To do so, click to change where the apps are run, as shown in Figure 251.

Figure 251 Deployment Details



The apps will be migrated to the app host, as shown in Figure 252.

Figure 252 Migrating Apps



Install EP-FP Combo on JSA Appliances

The event processor (EP)-flow processor (FP) combo functions as an event processor plus flow processor. It can collect both events and flows. Only the console component is absent. This combo is useful when you do not want to install separate EP devices and FP devices, and to avoid buying two separate devices. The installation process is the same for all JSA appliances. However, this section deals with the installation of the EP-FP combo on JSA5800.

To complete the installation and configuration of EP-FP combo:

- Install the EP-FP combo using the instructions in this section.
- Add EP-FP combo console to the deployment. For more information, see the section *Add EP-FP Hosts to Deployment*.
- Apply a license to the EP-FP combo console using the instructions *Apply a License to JSA*.

Before You Begin

Before you do the installation, ensure that you have the following in place:

- The required hardware is installed (in case of appliances).
- You have the required license key for your appliance.
- A keyboard and monitor are connected by using the VGA connection (in case of hardware appliances).
- There are no expired licenses on either the console or the managed hosts.
- Software versions for all JSA appliances in a deployment must be the same version and patch level. Note deployments that use different versions of software are not supported.

Keep the following information handy for the installation:

- Hostname
- IP address
- Network mask
- Default gateway address
- Primary Domain Name System (DNS) server address

- Secondary DNS server address (Optional)
- (Optional) Public IP address for networks using Network Address Translation (NAT)
- Email server name

Step-By-Step Procedure

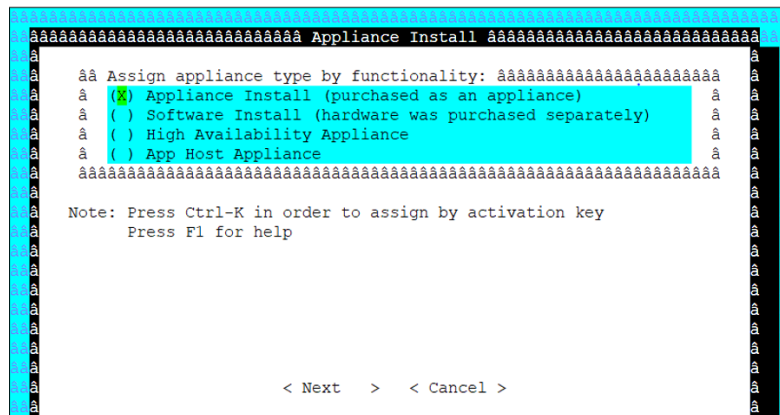
Follow the steps in the installation wizard for the hardware appliance type you are creating.

The JSA installation wizard allows you to use only certain keyboard keys to navigate through the installation options. Table P1 lists these keys along with how you can use them.

First log in as the root user at the prompt (a password is not required). If you are prompted for a password, there is some error with the installation. Please contact <https://support.juniper.net/support>.

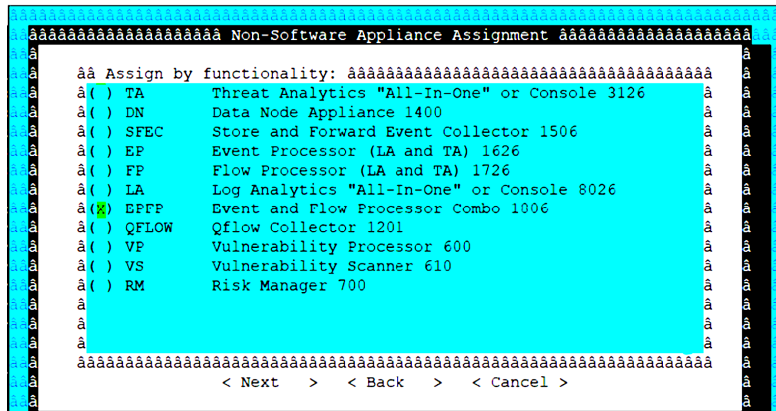
Read and accept the EULA license and proceed with the installation. After accepting EULA license, the Appliance Install page appears (Figure 253). Select Appliance Install (purchased as an appliance). Choose this option if you have purchased JSA appliances or wish to install a virtual machine. Then select Next.

Figure 253 Appliance Install Options



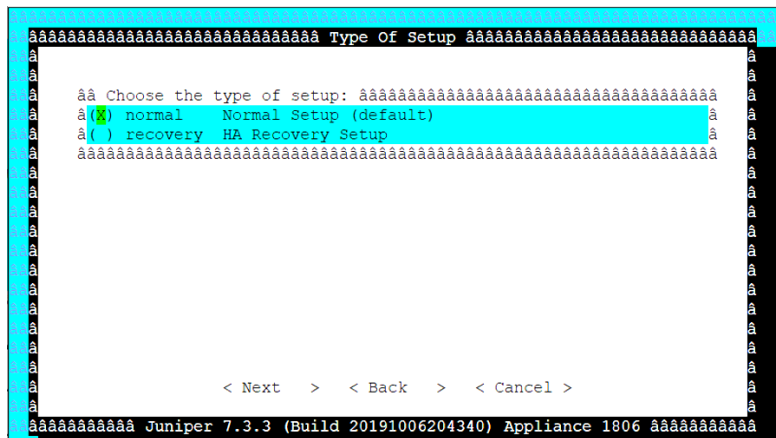
The Non-Software Appliance Assignment page appears (Figure 254). Select the non-software appliance type as EPFP Event and Flow Processor Combo 1806 and then select Next.

Figure 254 Non-Software Appliance Assignment Options



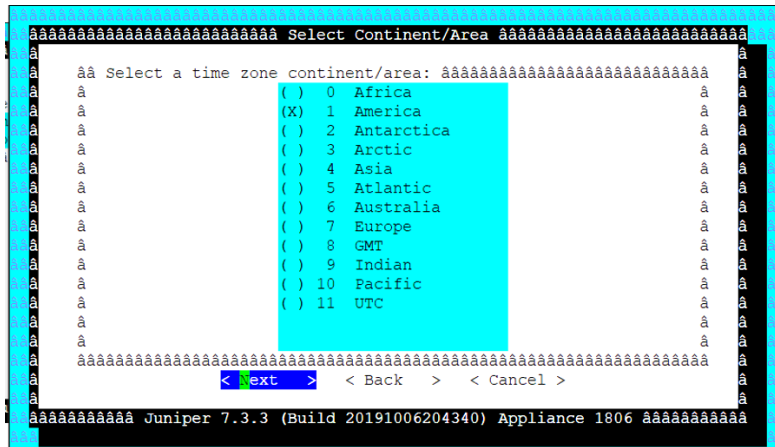
The Type of Setup page will appear (Figure 255). Select the Normal Setup (default) option, and select Next.

Figure 255 Setup Options



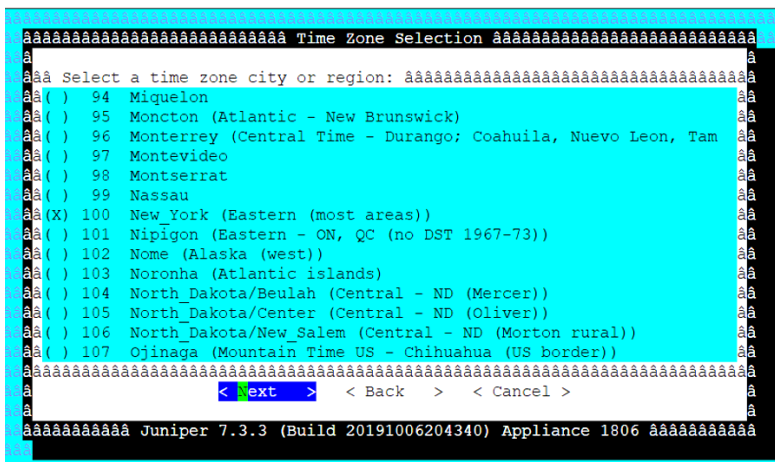
The Select Continent/Area page appears. Select the time zone continent or area as required and select Next. The default value is America.

Figure 256 Area Options



The Time Zone Selection page appears. Select the time zone city or region as required and select Next. The default value is New_York (Eastern (most areas)).

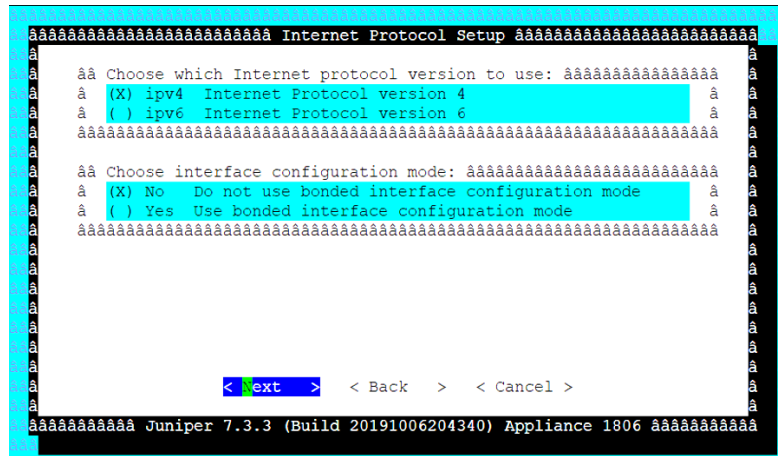
Figure 257 Time Zone Options



The Internet Protocol Setup page appears (Figure 258). Select the Internet Protocol version as IPv4 Internet Protocol version 4. Select No as the value for Do not use bonded interface configuration mode. When complete, select Next.

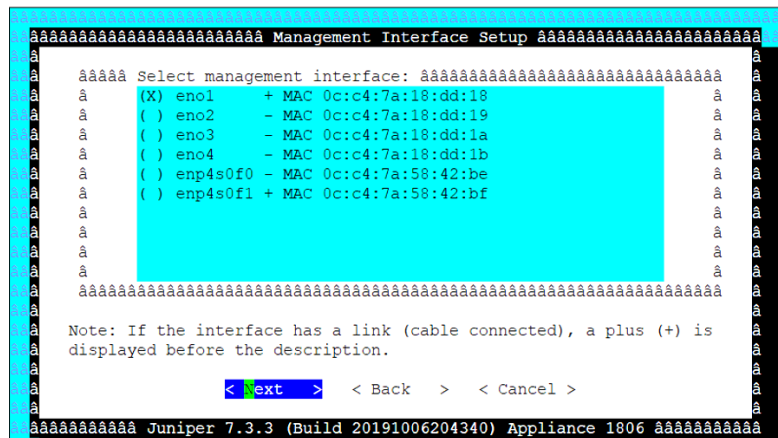
NOTE Select IPv6 Internet Protocol version 6 and Yes Do not use bonded interface configuration mode, as you require.

Figure 258 Internet Protocol Options



The Management Interface Setup page appears (Figure 259). Select the management interface that you want to use and select Next.

Figure 259 Management Interface Options



The Network Information Setup page appears (Figure 260). Configure the following network settings:

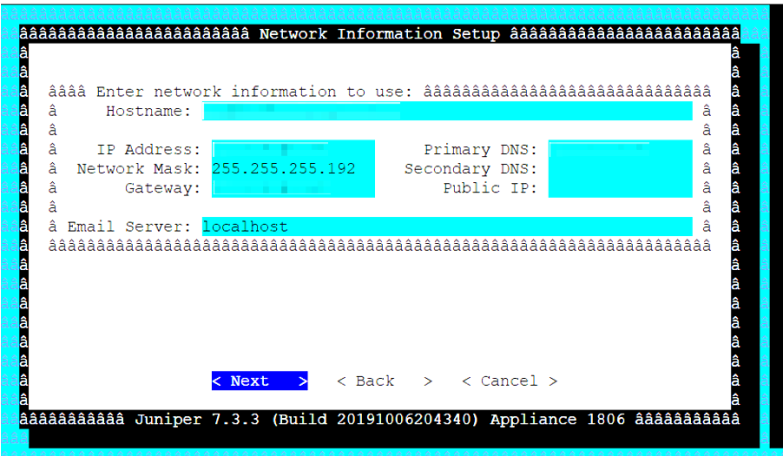
- Hostname—Enter a fully qualified domain name as the system hostname.
- IP Address—Enter the IP address of the system.
- Network Mask—Enter the network mask for the system.
- Gateway—Enter the default gateway of the system.

- 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.
- Email Server—Enter the e-mail server. If you do not have an e-mail server, type localhost in this field.

Select Next.

Figure 260

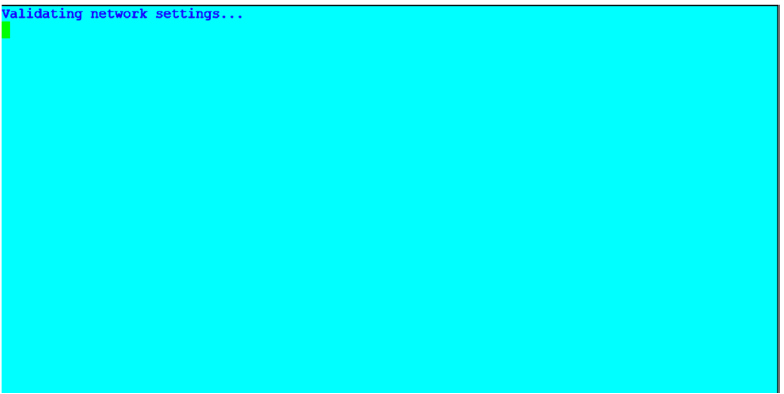
Network Information Options



The network settings are being validated. This may take a few minutes.

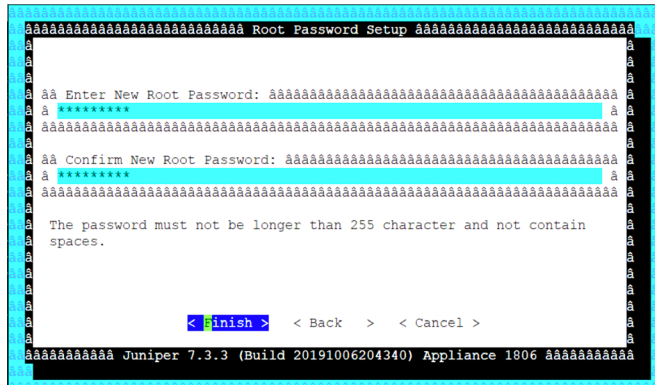
Figure 261

Validating Network Settings



Once network settings are validated successfully, the Root Password Setup page appears (Figure 262). In the Enter New Root Password field, enter a root password that meets the following criteria: contains at least 5 characters, contains no spaces, can include the following special characters: @, #, ^, and *. Re-enter the root password in the Confirm New Root Password field, and select Finish.

Figure 262 Root Password Setup



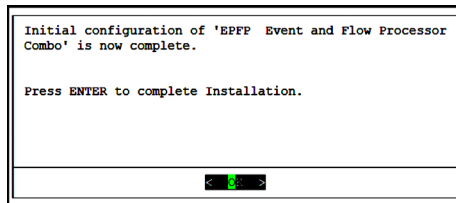
After you select Finish, the installation process starts. This process typically takes several minutes. Although it might appear as if the system is not responding at times, wait for the installation to complete.

Figure 263 Installing Changes

```
Installing Qradar changes...
Activating system with key 3D1B4K-1Q6J62-3Y6F34-684H49.
Appliance ID is 1806.
Installing 'EPFP Event and Flow Processor Combo' with id 1806.
Configuring network...
Setting current date and time.
New date of '2020/03/18 09:31:51' was specified 1471 seconds ago...
Setting date and time to '20200318 09:56:22'...
Running changeQradarPassword
Stopping hostcontext
Wed Mar 18 09:56:33 EDT 2020 [setup-imq.sh] OK: IMQ Setup Completed
Updating db user password
Applying replication db file...done!
Running replication setup...done!
Modifying postgresql config...done!
Running changeQVMPPassword
Setting email server to localhost
Running FinalSetup
Updating iptables firewall rules.
Restarting system services:
- syslog-ng
- hostcontext
- hostservices
Running restartServices
Restarting system services: syslog-ng.
Non-console setup, stopping services: hostcontext hostservices java.
Restarting services:
- hostservices
- hostcontext
Failed to start hostcontext!
OK: Configuration of host jsaEP-FP as a non-console completed.
qradar_setup.py: End: 0
Running: /opt/qradar/bin/after_services_up.sh
```

Figure 264 indicates a successful installation of the JSA Event and Flow Processor Combo. Click OK.

Figure 264 Installation Complete



Verification

You can verify the installation and completion of the Event and Flow Processor Combo by running the following command:

Run `less /etc/.appliance.name`

The output displays 1806 as the appliance installed. Ping the default gateway to ensure that connectivity is fine. You can also use the `ifconfig` to view the IP address details of the appliance.

Next Steps

Add EP-FP combo to the deployment. For more information, see section *Add EP-FP Hosts to Deployment*.

When you install JSA, you can use it with the temporary default license key. It gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them to the system, before the default license expires.

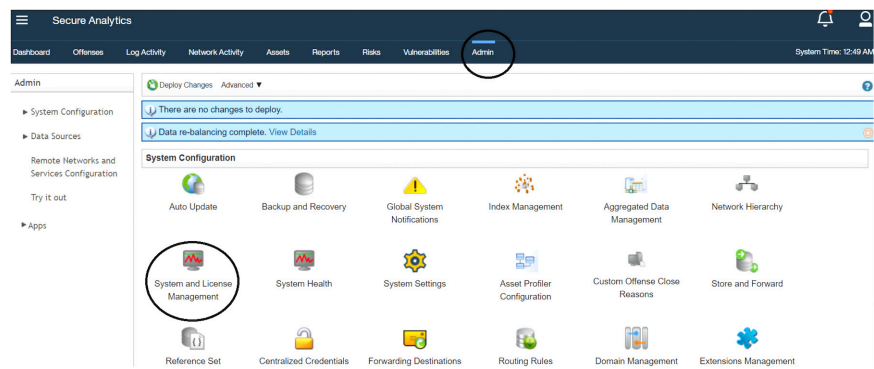
For more information about applying a license, see section *Apply a License to JSA*.

Add EP-FP Hosts to Deployment

This section includes instructions to add an EP-FP host to the deployment. Note that you can add an EP-FP host only to a threat analytics deployment.

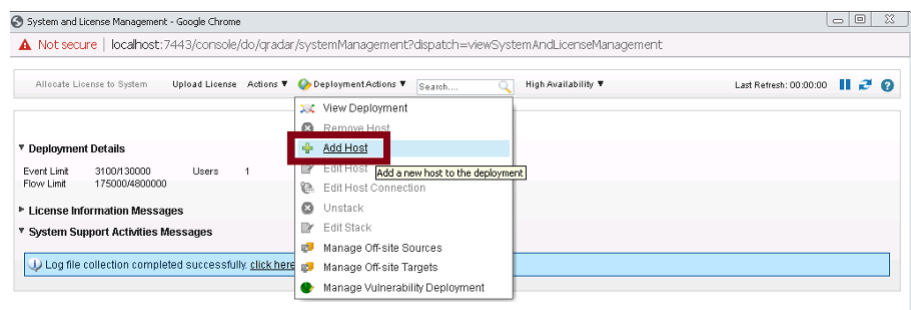
To add an EP-FP host to a deployment, log in to the JSA web UI. On the navigation menu, click Admin. The Admin page appears. In the System Configuration section, click System and License Management and the System and License Management page appears (Figure 265).

Figure 265 System and License Management



Select Deployment Actions > Add Host on the navigation menu (Figure 266).

Figure 266 Deployment Actions > Add Host



The Add Management Host page appears, as shown in Figure 267.

Figure 267 Add Managed Host

Add Managed Host

Before you add a managed host, make sure the managed host includes the SIEM software. The IP of the host is required as well as the root password. Hover over label fields for more information.

Host IP:

Host Password:

Confirm Password:

Encrypt Host Connections: ☐

Encryption Compression: ☐

Network Address Translation: ☐

NAT Group:

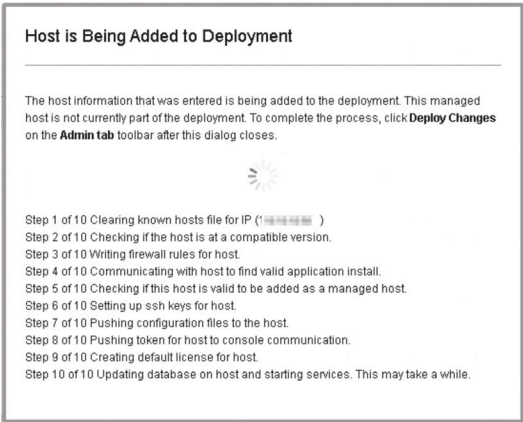
Public IP:

In the Host IP field, enter the fixed IP address of the EP-FP host you want to add. In the Host Password field, enter the root password for the host IP. In the Confirm Password field, re-enter the root password. When complete, click Add.

NOTE If you are using NAT, or want to use an encrypted communication between the EP-FP host and the console, select the options accordingly.

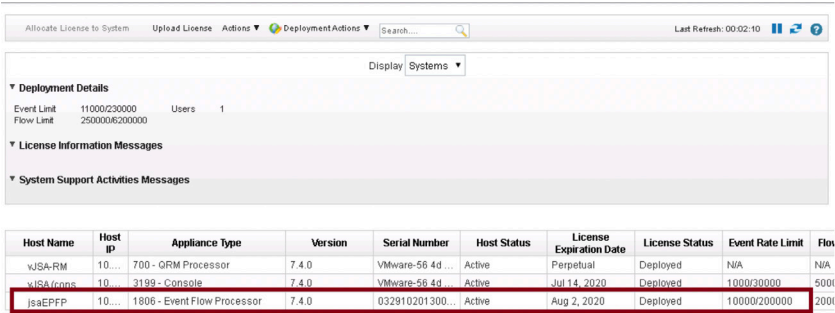
A pop-up message appears (Figure 268) showing the status of the host being added to the network.

Figure 268 Host is Being Added to Deployment



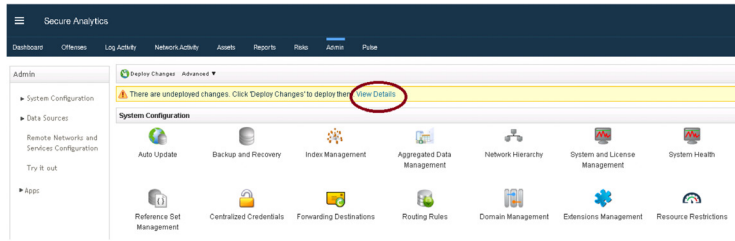
After the host is added successfully, the new host is listed on the System and License Management page (Figure 269).

Figure 269 Host Successfully Added



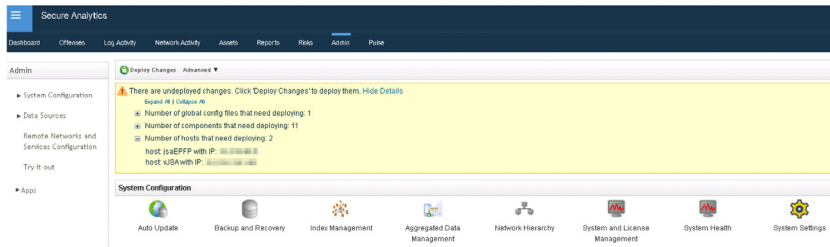
Note that at this point, the new host is not deployed. So, close the System and License Management page and go to the Admin page to deploy the changes. The changes that need to be deployed are shown on top of the page (Figure 270).

Figure 270 Undeployed Changes



Click View Details to see the changes, as shown in Figure 271.

Figure 271 Details of Undeployed Changes



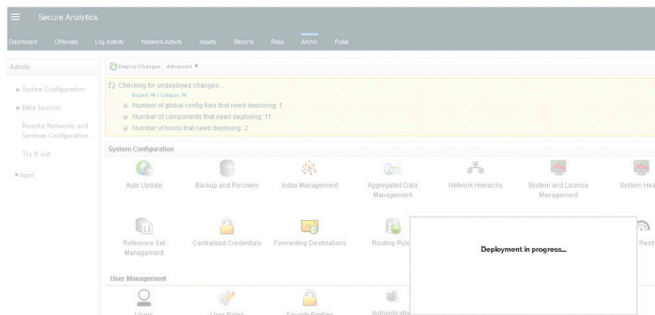
Click Deploy Changes. A confirmation page appears (Figure 272) asking for confirmation to deploy the changes. Click Continue to deploy.

Figure 272 Confirm Deployment of Changes



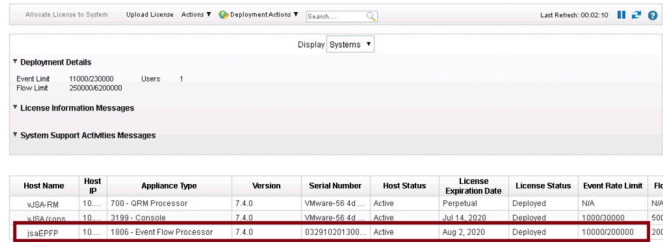
The deployment starts. This process typically takes several minutes. Although it might appear the system is not responding at times, wait for the deployment to complete. The JSA web UI will display the progress in the deployment process.

Figure 273 Deployment Confirmation



Wait for the deployment to complete. Once the deployment is completed successfully, you'll see that EP-FP host has been added to the deployment, as shown in Figure 274. You can now send flows or events to the EP-FP combo host.

Figure 274 EP-FP Host Added Successfully



The screenshot shows the Juniper JSA web interface. At the top, there are tabs for 'Allocate License to System', 'Upload License', 'Actions', and 'Deployment Actions'. Below these, there's a 'Display' dropdown set to 'Systems'. The main content area shows 'Deployment Details' with 'Event Limit' at 11000020000 and 'Flow Limit' at 2500006200000. Below that, there are sections for 'License Information Messages' and 'System Support Activities Messages'. At the bottom, there's a table of hosts.

Host Name	Host ID	Appliance Type	Version	Serial Number	Host Status	License Expiration Date	License Status	Event Rate Limit	Flow Rate Limit
vJSA-RM	10...	700 - QRM Processor	7.4.0	VMware-56 48...	Active	Perpetual	Deployed	N/A	N/A
vJSA-CP	10...	3199 - Console	7.4.0	VMware-56 48...	Active	Jul 14, 2020	Deployed	10000/20000	5000
jseFP	10...	1806 - Event Flow Processor	7.4.0	832910201300...	Active	Aug 2, 2020	Deployed	10000/200000	2000

Upgrade JSA

Typically, a JSA upgrade is needed when you want to use the latest features and to fix issues in older versions. The process to upgrade JSA devices is straightforward. To upgrade JSA, first download the following types of files from the Juniper Networks download site.

- ISO files - ISO files are normally used for clean installations only. Clean installations erase the existing configuration and data. ISO files are used for upgrades when there are major upgrades that involve the underlying RedHat OS changes. Such instances are documented in JSA Release Notes.
- SFS files - SFS files are used to upgrade from one version to another version.

The upgrade is triggered from the CLI. A new screen session is created, and the upgrade will run there. This ensures that the session remains active even if the SSH connection drops, and therefore, it is very important not to trigger multiple upgrades.

Before You Begin

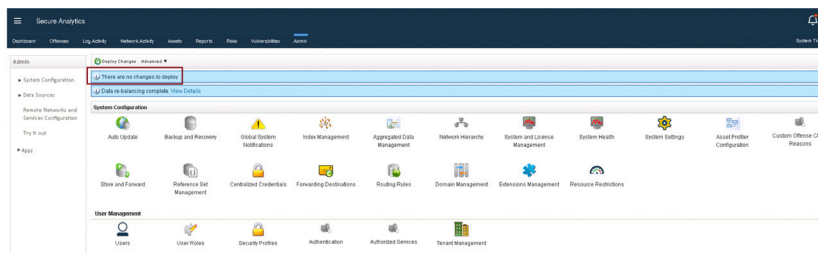
Before you begin make sure that you have completed the following:

- Read the JSA Release notes before planning an upgrade.
- Take a data backup. Move the backup file to a remote server.
- For VMs, we recommend that you to take a snapshot.
- Take configuration backup just before the upgrade. Move the backup file to a remote server.

- Ensure you have access to the console port on all devices in deployment.
- Ensure there is no third-party software on devices.
- Ensure enough disk space is available on all devices in deployment.
- Ensure HA status is correct. The primary should be active and the secondary should be in standby status, for upgrades to proceed.
- Ensure the JSA software version is the same on all devices.
- Ensure the status of all devices in deployment is active (there are no connectivity issues), no unknown or failed status.
- Inform JSA users about the planned upgrade activity.
- Ensure all licenses are active.
- Ensure there are no undeployed changes.
- Ensure hardware health checks for JSA appliances are done.
- If there are any hard disk issues, rectify them before upgrading. RAID should be optimal.
- Ensure you can ssh to all devices using root password.
- Do not reboot devices while they are upgrading.
- For critical log sources, to not to lose events, you can redirect logs to another syslog server or to another event processor which is not being upgraded at the moment. Managed hosts will still collect logs until the upgrade is triggered on them.

Let's check that there are no pending deploy changes, as shown in Figure 275.

Figure 275 Check Pending Deploy Changes



Verify that the current version is a supported version from where you can upgrade to the latest version. Figure 276 shows how we can verify the current JSA version.

Figure 276 Verify Current JSA Version

```
[root@vJSA storetmp]# su
This server has Secure Analytics 7.4.0 (Build 20200304205308) installed on Tue Jun 9 01:11:26 EDT 2020.
[root@vJSA storetmp]#
```

To upgrade the JSA Software version, download the required software from the Juniper support site and move the file to /storetmp.

NOTE Typically, the upgrade files size will be around 3GB to 5GB. Make sure there is enough disk space on the device.

Figure 277 Move the File to /storetmp

```
[root@vJSA storetmp]# cd /storetmp/
[root@vJSA storetmp]# ls
7.4.0.20200409095210.sfs.bz2  backup  geodata  report_runner
```

Unzip the file in the /storetmp directory using the bunzip utility:

bunzip2 <SFS File Name>

Figure 278 Unzip File in /storetmp

```
[root@vJSA storetmp]#
[root@vJSA storetmp]# bunzip2 7.4.0.20200409095210.sfs.bz2
```

Create the /media/updates directory by using the following command:

mkdir -p /media/updates

Mount the patch file to the /media/updates directory by using the following command:

mount -o loop -t squashfs /storetmp/<FileName>.sfs /media/updates

Figure 279 Mount Patch File to /media/updates

```
[root@vJSA storetmp]# mkdir -p /media/updates
[root@vJSA storetmp]#
[root@vJSA storetmp]# mount -o loop -t squashfs /storetmp/7.4.0.20200409095210.sfs /media/updates/
[root@vJSA storetmp]#
```

Run the patch installer by using the following command:

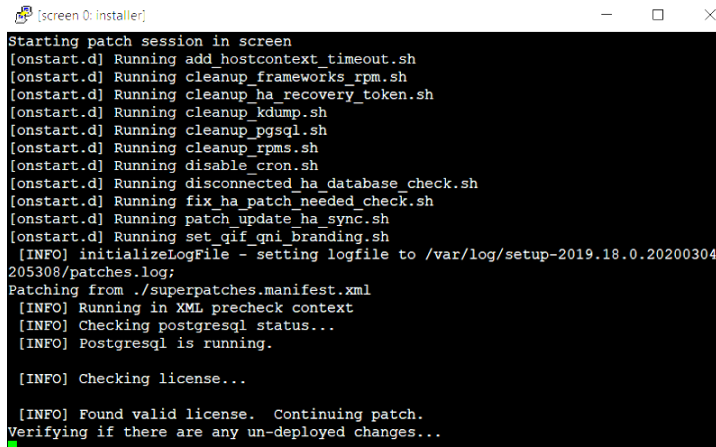
/media/updates/installer

Figure 280 Run Patch Installer

```
[root@vJSA storetmp]# mount -o loop -t squashfs /storetmp/7.4.0.20200409095210.sfs /media/updates/
[root@vJSA storetmp]#
[root@vJSA storetmp]# /media/updates/installer
```

A separate screen session is started for the upgrade and a series of checks happens, such as undeployed changes, expired license, and so on, as shown in Figure 281.

Figure 281 Starting Patch Session



```

[screen 0: installer]
Starting patch session in screen
[onstart.d] Running add_hostcontext_timeout.sh
[onstart.d] Running cleanup_frameworks_rpm.sh
[onstart.d] Running cleanup_ha_recovery_token.sh
[onstart.d] Running cleanup_kdump.sh
[onstart.d] Running cleanup_pgsql.sh
[onstart.d] Running cleanup_rpms.sh
[onstart.d] Running disable_cron.sh
[onstart.d] Running disconnected_ha_database_check.sh
[onstart.d] Running fix_ha_patch_needed_check.sh
[onstart.d] Running patch_update_ha_sync.sh
[onstart.d] Running set_gif_qni_branding.sh
[INFO] initializeLogFile - setting logfile to /var/log/setup-2019.18.0.20200304
205308/patches.log;
Patching from ./superpatches.manifest.xml
[INFO] Running in XML precheck context
[INFO] Checking postgresql status...
[INFO] Postgresql is running.

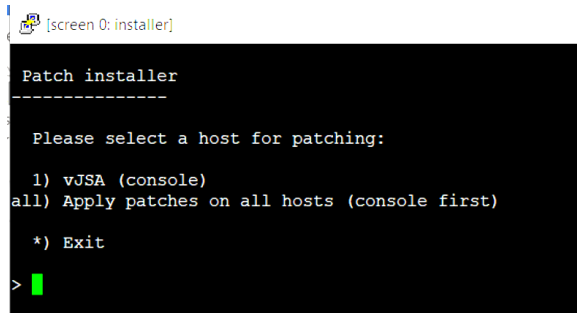
[INFO] Checking license...

[INFO] Found valid license. Continuing patch.
Verifying if there are any un-deployed changes...

```

Once all pre-tests have passed, the hosts to be upgraded are listed, as shown in Figure 282.

Figure 282 Patch Installer



```

[screen 0: installer]

Patch installer
-----

Please select a host for patching:

1) vJSA (console)
all) Apply patches on all hosts (console first)

*) Exit

>

```

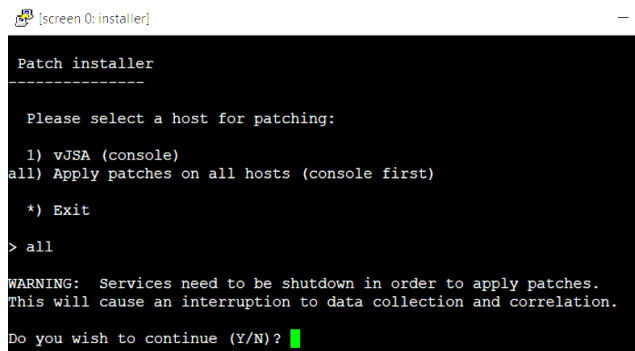
In the case of AIO or standalone deployments, there is only one server to upgrade. In the case of HA systems, upgrades take care of both primary and secondary hosts as a single entity. In the case of distributed deployments, you must upgrade the console first and then the managed hosts.

The *all* option in Figure 282 updates the software on all appliances (console first). If you do not select the *all* option, you must select your console appliance. Managed hosts are not displayed in the installation menu to ensure that the console is patched first. After the console is patched, a list of managed hosts that can be updated is displayed in the installation menu.

If you want to patch systems in a sequence, you can update the console first, copy the patch to all other appliances, and then run the software update installer individually on each managed host. You must patch the console before you run the installer on managed hosts. When updating in parallel, you don't need an order to update appliances after the console is updated. Even if your SSH session is disconnected while the upgrade is in progress, the upgrade continues.

Type *all*. Confirm if the services can be stopped and proceed with the upgrade, as shown in Figure 283.

Figure 283 All Option Confirmation



```

[screen 0: installer]

Patch installer
-----

Please select a host for patching:

1) vJSA (console)
all) Apply patches on all hosts (console first)

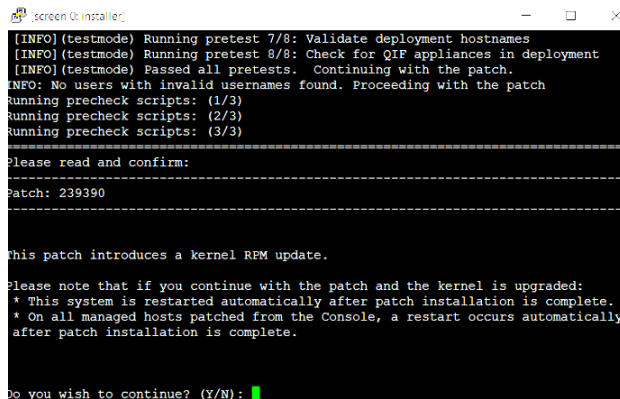
*) Exit

> all

WARNING: Services need to be shutdown in order to apply patches.
This will cause an interruption to data collection and correlation.
Do you wish to continue (Y/N)? █
  
```

Type Y to proceed. The upgrade begins and for any reboot, a confirmation message is shown, as shown in Figure 284.

Figure 284 Reboot Confirmation



```

[screen 0: installer]

(INFO)(testmode) Running pretest 7/8: Validate deployment hostnames
(INFO)(testmode) Running pretest 8/8: Check for QIP appliances in deployment
(INFO)(testmode) Passed all pretests. Continuing with the patch.
INFO: No users with invalid usernames found. Proceeding with the patch
Running precheck scripts: (1/3)
Running precheck scripts: (2/3)
Running precheck scripts: (3/3)

=====
Please read and confirm:

Patch: 239390

=====

This patch introduces a kernel RPM update.

Please note that if you continue with the patch and the kernel is upgraded:
* This system is restarted automatically after patch installation is complete.
* On all managed hosts patched from the Console, a restart occurs automatically
after patch installation is complete.

Do you wish to continue? (Y/N): █
  
```

Type Y to proceed. Confirm the ECS upgrade, as shown in Figure 285 (the option that you choose is applicable to managed hosts as well).

Figure 285 Confirm ECS Upgrade

```

[screen 0: installer]
Patch: 140059
-----
An update for the event collection service is available.

Currently Running Version: 2019.18.0.20200304205308
New Available Version: 2019.18.1.20200409095210

Applying the update requires the event collection service to restart, which could result in a gap in data collection.
You can continue to use the version that you are currently running, and update to the new version later.
For more information about manually updating the event collection service, see the IBM Security QRadar Administration Guide.

Note: The option that you choose is applied to all managed hosts that are patched from this QRadar console.

Choices:
1) Update and restart the event collection service now.
2) Continue using the current version of the event collection service for now. Update the event collection service during the next restart.
3) Abort patch
>

```

Choose the appropriate option and proceed. Ensure that all applications on your system are updated before you upgrade JSA, as shown in Figure 286.

Figure 286 Confirm Application Upgrade

```

[screen 0: installer]
>1
-----
Patch: 192175
-----
Ensure that all apps on your system are updated before you update QRadar. Out-of-date apps might not work after you install this update.

Do you want to continue, or abort the patch?
Choices:
1) Yes, my apps are up-to-date and I want to continue.
2) No, abort the patch so I can update my apps.
>1
-----
[INFO](testmode) Inspecting 1 patches for files to patch
[INFO](testmode) Found 1 patches, and 54 files to patch
[INFO](testmode) Inspected patch '2019.18.1.20200409095210-2019181_patchupdate-2019.18.1.20200409095210'; added 69 install packages and 4 upgrade packages
[INFO](testmode) Test upgrading 4 and test installing 69 packages.

[INFO](testmode) 4 packages to upgrade
[INFO](testmode) 69 packages to install
>

```

Choose the appropriate option and proceed. The upgrade continues, as shown in Figure 287.

Figure 287 Upgrade Continues

```

[INFO] (patchmode) Updating : kernel-tools-libs-3.10.0-1062.12.1.el7.x86_64 24/117
[INFO] (patchmode) Updating : openssh-qconf-1.0-11.el7.x86_64 25/117
[INFO] (patchmode) Detecting SSH installation ... (OK)
[INFO] (patchmode) Backing-up SSH configuration ... (OK)
[INFO] (patchmode) Updating SSH configuration
[INFO] (patchmode) - sshd_config defaults ... (OK)
[INFO] (patchmode) - sshd_config disallowed ... (OK)
[INFO] (patchmode) Setting QRadar SSH configuration ... (OK)
[INFO] (patchmode) Setting SSH public key options ... (OK)
[INFO] (patchmode) Reloading SSH service ... (OK)
[INFO] (patchmode) Sun Jun 28 13:04:17 EDT 2020 [setup-ssh.sh] OK: SSH Setup Completed
[INFO] (patchmode) Updating : qllabs mpe-2019.18.1-20200409095210.noarch 26/117
[INFO] (patchmode) Updating : jars-icu4j-charset-65.1-1.noarch 27/117
[INFO] (patchmode) Updating : qllabs uiframeworks-2019.18.1-20200409095210.noarch 28/117
[INFO] (patchmode) Updating : qllabs configservices common-2019.18.1-20200409095210. 29/117
[INFO] (patchmode) Updating : forensics html-7.4.0.2-20200326125359.el7.x86_64 30/117
[INFO] (patchmode) Updating : jars-icu4j-65.1-1.noarch 31/117
[INFO] (patchmode) Updating : qllabs application-2019.18.1-20200409095210.noarch 32/117
[INFO] (patchmode) Updating : ecs-ec-ingress-systemd-2019.18.1-20200409095210-1.noar 33/117
[INFO] (patchmode) Updating : ecs-sp-systemd-2019.18.1-20200409095210-1.noarch 34/117
[INFO] (patchmode) Updating : qllabs ecingress-2019.18.1-20200409095210.noarch 35/117
[INFO] (patchmode) Updating : forensics analysis-7.4.0.2-20200326125359.el7.x86_64 36/117
[INFO] (patchmode) Updating : forensics-setup-2019.18.1-20200409095210.el7.x86_64 37/117

```

The JSA software patch is applied successfully and the services are started. Deployment is initiated, as shown in Figure 288.

Figure 288 Deployment Initiated

```

[INFO] (patchmode) recording patch 7.4.0 FixPack 1 (Build 20200409095210) was applied
Upgraded Secure Analytics to 7.4.0 FixPack 1 (Build 20200409095210) from 7.4.0 (Build )
[INFO] (patchmode) Running postpatch scripts
Applying postpatch script: (16/16)
[INFO] (patchmode) Running pre_services_up scripts
Applying pre_services_up script: (16/16)

[INFO] (patchmode) All patches applied successfully. Restarting processes
[INFO] (patchmode) Starting process "tomcat"
Checking that tomcat is running and ready: (attempt 1/120) (0 seconds)

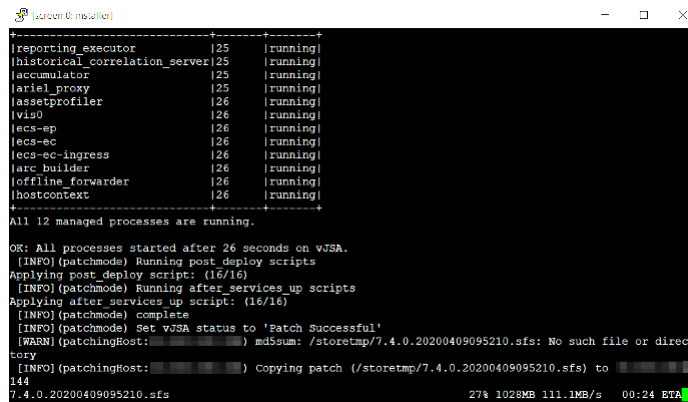
[INFO] (patchmode) Tomcat started and ready after 126 seconds.

[INFO] (patchmode) Starting process "hostcontext"
[INFO] (patchmode) Waiting for hostcontext to fully start
[INFO] (patchmode) Running post_services_up scripts
Applying post_services_up script: (16/16)
[INFO] (patchmode) One of the patches required a deployment be performed after restarting services.
Checking that tomcat is running and ready: 300
Tomcat started and ready after 9 seconds.
Triggering deployment of : 300
Waiting for deployment to commence: started.
0.219.130.145: In Progress.
Waiting for deployment to complete: 825

```

The upgrade of the console is completed. As you previously selected the *all* option, the SFS file is moved to the managed host to start the upgrade of managed hosts.

Figure 289 Console Upgraded



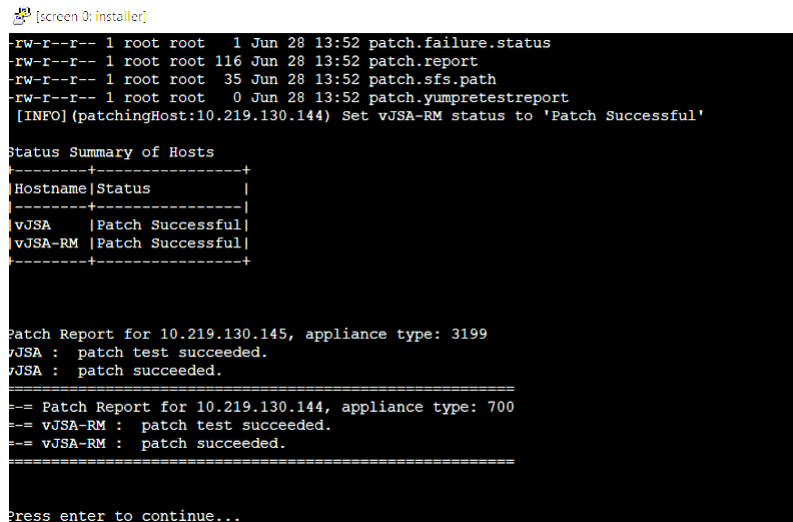
```

[reporting_executor] 125 [running]
[historical_correlation_server] 125 [running]
[accumulator] 125 [running]
[ariel_proxy] 125 [running]
[assetprofiler] 126 [running]
[viso] 126 [running]
[iecs-ep] 126 [running]
[iecs-ec] 126 [running]
[iecs-ec-ingress] 126 [running]
[iars builder] 126 [running]
[offline_forwarder] 126 [running]
[hostcontext] 126 [running]
+-----+
All 12 managed processes are running.
OK: All processes started after 26 seconds on vJSA.
[INFO] (patchmode) Running post deploy scripts
Applying post deploy script: (15/16)
[INFO] (patchmode) Running after_services up scripts
Applying after_services up script: (16/16)
[INFO] (patchmode) complete
[INFO] (patchmode) Set vJSA status to 'Patch Successful'
[WARN] (patchingHost: 10.219.130.144) md5sum: /storetmp/7.4.0.20200409095210.sfs: No such file or directory
[INFO] (patchingHost: 10.219.130.144) Copying patch (/storetmp/7.4.0.20200409095210.sfs) to 10.219.130.144
7.4.0.20200409095210.sfs 27% 1028MB 111.1MB/s 00:24 ETA

```

The software update installation summary shows managed hosts that are not updated. If the software update fails to update a managed host, you can copy the software update to the host and run the installation locally.

Figure 290 Software Update Installation Summary



```

-rw-r--r-- 1 root root 1 Jun 28 13:52 patch.failure.status
-rw-r--r-- 1 root root 116 Jun 28 13:52 patch.report
-rw-r--r-- 1 root root 35 Jun 28 13:52 patch.sfs.path
-rw-r--r-- 1 root root 0 Jun 28 13:52 patch.yumpretestreport
[INFO] (patchingHost:10.219.130.144) Set vJSA-RM status to 'Patch Successful'

Status Summary of Hosts
+-----+
|Hostname|Status|
+-----+
|vJSA    |Patch Successful|
|vJSA-RM |Patch Successful|
+-----+

Patch Report for 10.219.130.145, appliance type: 3199
vJSA : patch test succeeded.
vJSA : patch succeeded.

=====
== Patch Report for 10.219.130.144, appliance type: 700
== vJSA-RM : patch test succeeded.
== vJSA-RM : patch succeeded.
=====

Press enter to continue...

```

Reinstall JSA Using Bootable USB

You can re-install JSA hardware appliances using a bootable USB. This is required when you want a specific OS to be installed on the hardware appliance.

WARNING! This procedure erases the entire configuration and data on the JSA appliance. You can use this procedure for clean installations only. You must physically access the JSA hardware appliance to plug-in the USB.

To reinstall JSA using bootable USB: prepare the bootable USB using the JSA ISO, plug-in the USB to the JSA hardware appliance, and reboot the JSA hardware appliance.

The following options are available to prepare a bootable USB using the JSA ISO:

- Create a bootable USB flash drive with Red Hat Linux.
- Create a bootable USB flash drive with Microsoft Windows.
- Create a bootable USB flash drive with another JSA hardware appliance.
- Create a bootable USB flash drive with Mac OS.

This example shows the procedure to create a bootable USB using a Linux workstation. For more details, see the JSA Installation guides: https://www.juniper.net/documentation/product/en_US/juniper-secure-analytics.

You can use a Linux desktop or notebook system with Red Hat V7.3 to create a bootable USB flash drive to install JSA software. Before you create a bootable USB flash drive, you must have access to an 8GB USB flash drive and the JSA 7.3.0 or later ISO image file.

To Create a Bootable USB Flash Drive

Download the required JSA ISO image file from the Juniper Networks Support Website. Insert the USB flash drive in the USB port on your Linux system. Open a terminal and type the following command to determine the name of the USB flash drive:

```
dmesg | grep SCSI
```

The system displays the messages produced by device drivers, as shown in Figure 291. The following example shows the name of the connected USB flash drive as `sdb`:

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


Figure 291 Device Driver Output

```

root@:/ # dmesg | grep -i scsi
10.021902] SCSI subsystem initialized
29.169326] Block layer SCSI generic (bsg) driver version 0.4 loaded (major 240)
43.754450] scsi host1: iscsi
43.760067] scsi host2: ahci
43.760264] scsi host3: ahci
43.760454] scsi host4: ahci
43.760642] scsi host5: ahci
43.760912] scsi host6: ahci
43.769150] scsi host7: ahci
43.792046] scsi host0: Avago SAS based MegaRAID driver
43.831230] scsi 0:2:0:0: Direct-Access Intel RM325PB080 3.24 PQ: 0 ANSI
44.190140] sd 0:2:0:0: [sda] Attached SCSI disk
51.104377] sd 0:2:0:0: Attached scsi generic sg0 type 0
39025.399359] scsi host8: usb-storage 2-1.7:1.0
39031.792041] scsi host9: usb-storage 2-1.6:1.0
39037.046157] scsi 9:0:0:0: Direct-Access Unigen PQS4000 1100 PQ: 0 ANSI
39037.046774] scsi 9:0:0:0: alua: supports implicit and explicit TPGS
39037.046782] scsi 9:0:0:0: alua: No target port descriptors found
39037.046788] scsi 9:0:0:0: alua: not attached
39037.047215] sd 9:0:0:0: Attached scsi generic sg1 type 0
39037.058590] sd 9:0:0:0: [sdb] Attached SCSI removable disk
45252.643296] scsi host10: usb-storage 2-1.6:1.0
45253.961410] scsi 10:0:0:0: Direct-Access JetFlash Transcend 16GB 1100 PQ: 0 ANSI
45253.961878] scsi 10:0:0:0: alua: supports implicit and explicit TPGS
45253.961885] scsi 10:0:0:0: alua: No target port descriptors found
45253.961891] scsi 10:0:0:0: alua: not attached
45253.962410] sd 10:0:0:0: Attached scsi generic sg1 type 0
45253.976625] sd 10:0:0:0: [sdb] Attached SCSI removable disk

```

Type the following commands to unmount the USB flash drive:

```
umount /dev/sdb
```

Assume that sdb is the USB drive that you attached.

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

```
dd if=<jsa-iso-file> of=/dev/sdb bs=512k
```

Figure 292 JSA ISO to your USB

```

[root@ /]# dd if=/JSA7.3.1.iso of=/dev/sdb bs=512k
9212+0 records in
9212+0 records out
4829741056 bytes (4.8 GB) copied, 209.986 s, 23.0 MB/s

```

Assume that sdb is the USB drive and you have copied the JSA ISO file in /.

Remove the USB flash drive from your system. Now that the USB is ready, use that USB drive to install the JSA appliance.

Access the console port (serial port access) of the JSA hardware appliance, and insert the bootable USB flash drive into the USB port of your appliance.

Restart the appliance.

After the appliance restarts, the USB flash drive prepares the appliance for installation and the Juniper STRM image installer appears, as shown in Figure 293.

Figure 293 Juniper STRM Image Installer

```

Welcome to the Juniper STRM image installer

*** WARNING ***

This procedure will overwrite your hard disk drive with a new factory default
Juniper STRM installation. As a result, all data will be lost.
If you DO NOT WISH to ERASE your system and lose all of its data
please TURN OFF the device NOW and remove the USB storage device from the
USB port..

- To begin installation of your STRM image, type:
install <ENTER>

- To begin UM/UGA installation of your STRM image, type:
linux <ENTER>

- To cancel this operation, power off the system and remove the USB
storage device from the USB port.

boot: _

```

Type *install* and press enter to begin installation of your STRM image, as shown in Figure 294.

Figure 294 Install STRM Image

```

Welcome to the Juniper STRM image installer

*** WARNING ***

This procedure will overwrite your hard disk drive with a new factory default
Juniper STRM installation. As a result, all data will be lost.
If you DO NOT WISH to ERASE your system and lose all of its data
please TURN OFF the device NOW and remove the USB storage device from the
USB port..

- To begin installation of your STRM image, type:
install <ENTER>

- To begin UM/UGA installation of your STRM image, type:
linux <ENTER>

- To cancel this operation, power off the system and remove the USB
storage device from the USB port.

boot: install_

```

The installation process can take up to an hour to complete. When the login prompt is displayed, type *root* to log in to the system as the root user. The user name is case-sensitive.

NOTE You need not enter any password to log in to the system during this step.

Press Enter and follow the prompts to install JSA. You can now configure different JSA roles such as threat analytics, log analytics, event processors, flow processors, and so on, as covered earlier in this chapter.

Reinstall JSA Using Factory Reinstall Method

You can restart and reinstall your JSA hardware or virtual appliance by using the factory installation option.

NOTE This procedure erases the entire configuration and data on the JSA appliance. You can use this procedure for only clean installs.

To reinstall JSA hardware or virtual appliance, first log in to your JSA hardware or a virtual appliance. Enter *reboot* in the console and press Enter to reboot your JSA hardware or virtual appliance, as shown in Figure 295.

Figure 295 Reboot Command

```
JSA-AppHost login: root
Password:
Last login: Mon Nov 18 01:51:21 on tty1
This server has Secure Analytics 7.3.3 (Build [REDACTED]) installed on Sun Nov 17 05:40:42 EST 2019.
[root@JSA-AppHost ~]# reboot
[ OK ] Started Show Plymouth Reboot Screen.
[ OK ] Stopped Docker Application Container Engine.
[ OK ] Started Restore /run/initramfs.
[ OK ] Stopped LSB: Starts the Spacewalk Daemon.
      Stopping SYSU: elxsnmpd is the snmp extension agent required to monitor Emulex OneConnect hardware...
[ OK ] Stopped SYSU: elxsnmpd is the snmp extension agent required to monitor Emulex OneConnect hardware.
      Stopping LSB: Start/stop pf_ring...
[ OK ] Stopped IRQ.
```

During device boot up, select Factory re-install, as shown in Figure 296.

Figure 296 Factory Re-Install Option

```
Normal System
Factory re-install [Secure Analytics 7.3.3 (Build [REDACTED])]

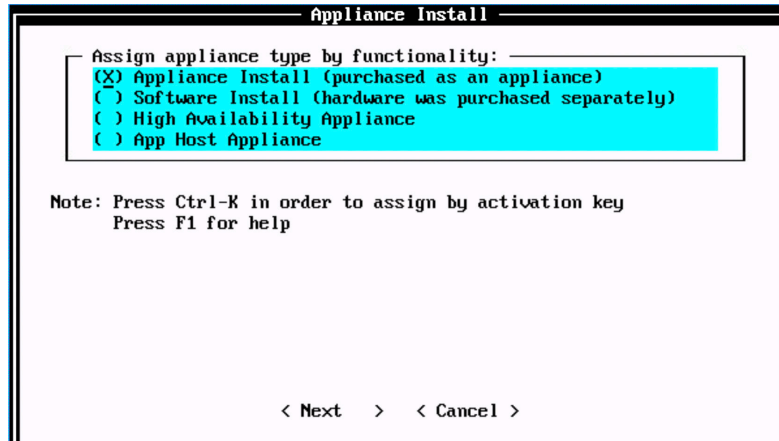
Use the ↑ and ↓ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
```

The hard disk is partitioned and reformatted, the OS is installed, and then the JSA hardware or virtual appliance is reinstalled. You must wait for the process to complete and it can take up to several hours, depending on your system.

When completed, log in to the JSA hardware or virtual appliance as the root user. The JSA installation wizard allows you to use only certain keyboard keys to navigate through the installation options. Table P1 lists these keys along with how you can use them.

Read the license information in the window. Press the spacebar to advance each window until you reach the end of the document. Type *yes* to accept the license agreement, and then press *Enter*. And the wizard to begin to install the appliance appears, as shown in Figure 297.

Figure 297 Appliance Installation



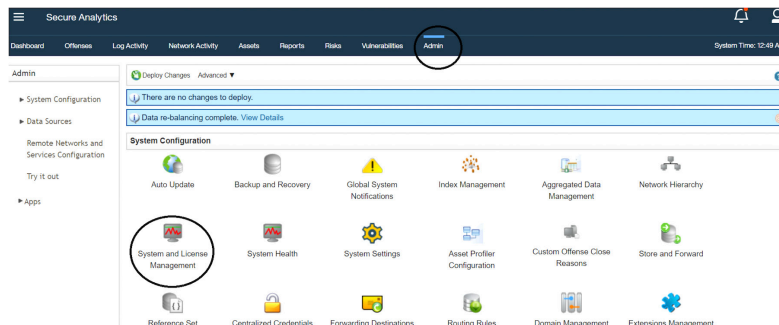
You can now configure different JSA roles such as threat analytics, log analytics, event processors, flow processors, and so on, as covered earlier in this chapter.

Remove a Managed Host

In some network scenarios you may need to remove a managed host from the deployment. For example, decommissioning an old site where a managed host is placed, or relocation of a site where a managed host is physically located.

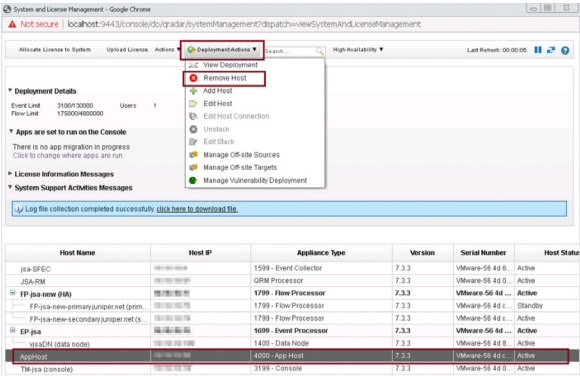
To remove a managed host from your deployment, log in to the JSA web UI. On the navigation menu, click *Admin*. The *Admin* page appears (Figure 298). In the *System Configuration* section, click *System and License Management*.

Figure 298 System and License Management



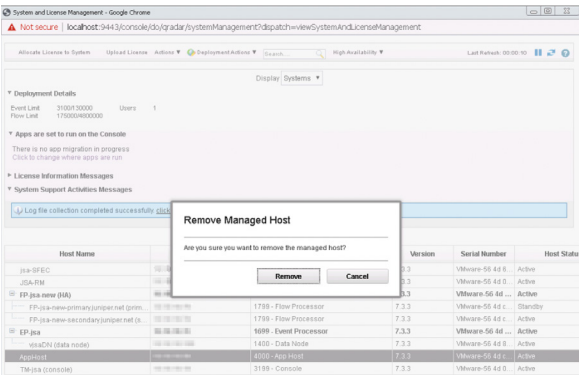
The System and License Management page appears (Figure 299). Select the managed host which is to be deleted from the deployment. On the navigation menu, select Deployment Actions > Remove Host.

Figure 299 Deployment Actions > Remove Host



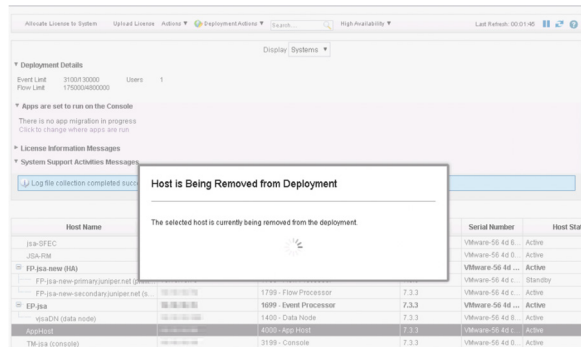
The Remove Management Host page appears asking for confirmation to remove the managed host, as shown in Figure 300. Click Remove.

Figure 300 Remove Managed Host



A pop-up appears displaying the status of the host being removed from the deployment, as shown in Figure 301.

Figure 301 Host is Being Removed from Deployment



At this point, the changes are not yet deployed. To deploy the changes, go to the Admin page (Figure 302). The changes that need to be deployed are shown on top of the page. Click View Details to see the changes.

Figure 302 Undeployed Changes

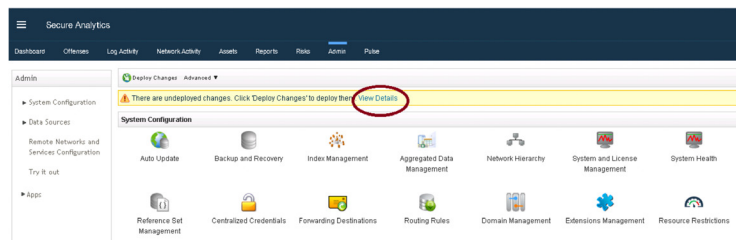
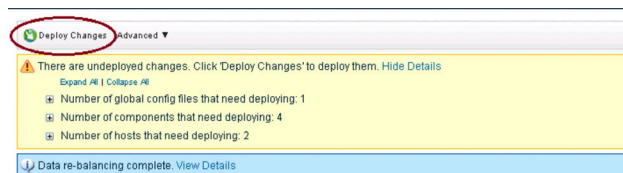
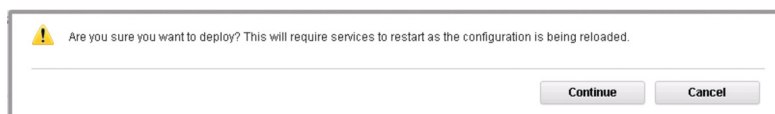


Figure 303 Changes to be Deployed



Click Deploy Changes. A confirmation page appears (Figure 304) asking for confirmation to deploy the changes. Click Continue to deploy the changes.

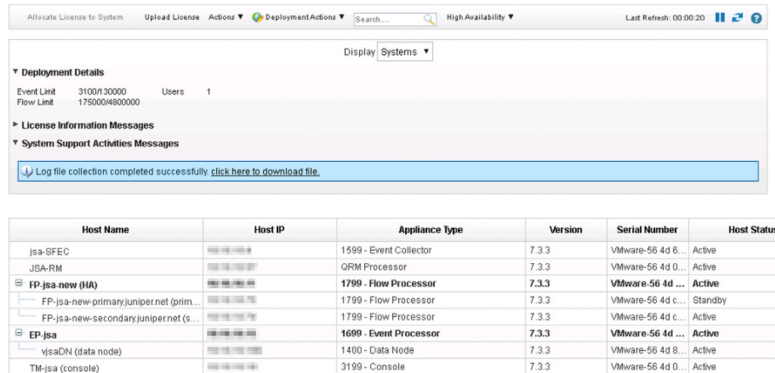
Figure 304 Deployment Confirmation



The deployment starts. This process typically takes several minutes. Although it might appear the system is not responding at times, wait for the deployment to complete.

After the deployment is complete, the selected managed host is removed from the deployment.

Figure 305 Managed Host Removed from Deployment



The screenshot shows the JSA Deployment Actions interface. At the top, there are tabs for 'Allocate License to System', 'Upload License', 'Actions', and 'Deployment Actions'. Below the tabs, there is a search bar and a 'High Availability' dropdown. The main content area is divided into sections: 'Deployment Details', 'License Information Messages', and 'System Support Activities Messages'. The 'Deployment Details' section shows 'Event Limit: 31000/30000' and 'Flow Limit: 175000/480000'. The 'System Support Activities Messages' section shows a message: 'Log file collection completed successfully click here to download file.' Below the messages, there is a table of managed hosts.

Host Name	Host ID	Appliance Type	Version	Serial Number	Host Status
jsa-SFEC	1599-Event Collector	1599 - Event Collector	7.3.3	Vmware-56 4d 6...	Active
JSA-RM	ORM Processor	ORM Processor	7.3.3	Vmware-56 4d 0...	Active
FP jsa-new (HA)	1799 - Flow Processor	1799 - Flow Processor	7.3.3	Vmware-56 4d ...	Active
FP jsa-new-primaryjuniper.net (prim...	1799 - Flow Processor	1799 - Flow Processor	7.3.3	Vmware-56 4d c...	Standby
FP jsa-new-secondaryjuniper.net (s...	1799 - Flow Processor	1799 - Flow Processor	7.3.3	Vmware-56 4d c...	Active
EP jsa	1699 - Event Processor	1699 - Event Processor	7.3.3	Vmware-56 4d ...	Active
vjsaDN (data node)	1400 - Data Node	1400 - Data Node	7.3.3	Vmware-56 4d 8...	Active
TM jsa (console)	3199 - Console	3199 - Console	7.3.3	Vmware-56 4d 0...	Active

Chapter 3

JSA Software Configuration and Troubleshooting Use Cases

Now that you are done with your JSA installations, here are some sample exercises for you to try with your JSA setup.

After reading this chapter you will be able to:

- Apply a license to JSA
- Understand how you can use the JSA web UI for some common scenarios
- Manage data backups
- Install and manage applications on JSA

Apply a License to JSA

When you install JSA, the default license key is temporary and gives you access to the system for 35 days from the installation date. The email that you received from Juniper Networks when you purchased JSA contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them before the default license expires.

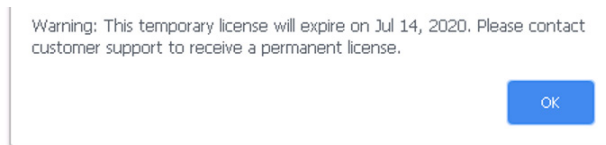
To apply a license key to the system, follow these steps:

- Obtain the license key (for new or updated license keys, contact your local sales representative)
- Upload a license key
- Allocate a license key to a host
- Deploy the changes

Scenario One: License Not Expired

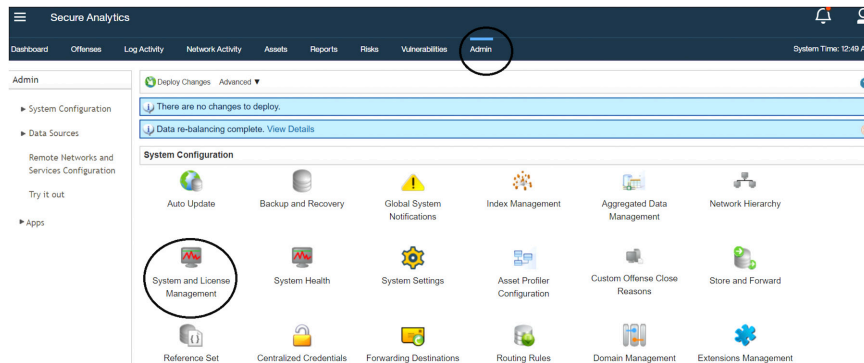
If you do not have a perpetual license and if the license is not expired when you log in to JSA Web UI, you will see a license warning message, as shown in Figure 306.

Figure 306 License Warning Message



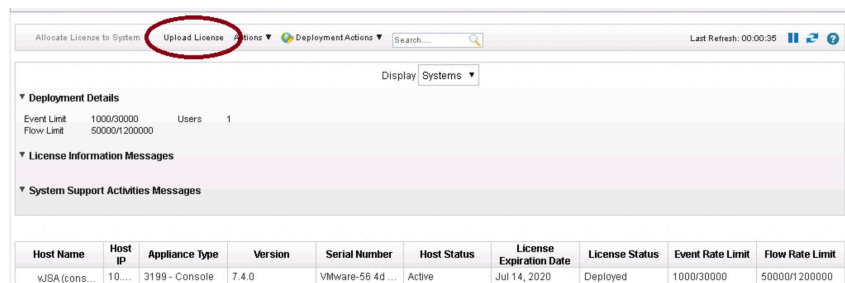
Click OK and follow these instructions. Click on Admin to open the Admin tab and in the System Configuration section click System and License Management, as shown in Figure 307.

Figure 307 System and License Management



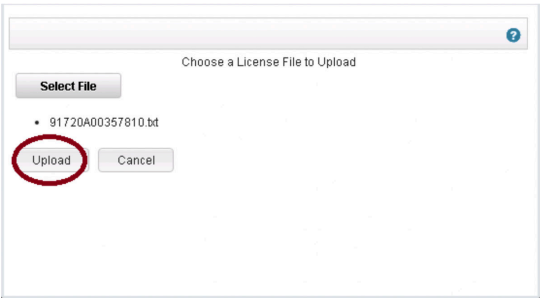
Select Upload License, as shown in Figure 308.

Figure 308 Upload License Option



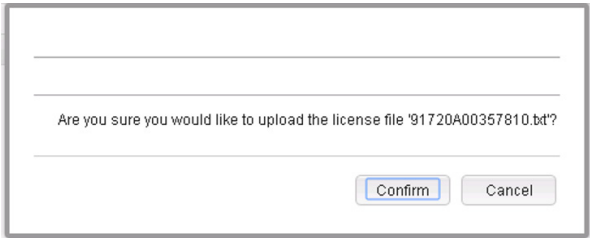
Select the license File and upload it, as shown in Figure 309.

Figure 309 Upload License File



Click confirm to confirm the upload, as shown in Figure 310.

Figure 310 Confirm Upload



The uploaded license is not yet allocated to the system. To allocate the license, go to the System and License Management page (Figure 311) and select Licenses in the Display drop-down.

Figure 311 Allocate License

Allocate License to System

Upload License

Actions

Deployment Actions

Search

Last Refresh: 00:00:15

Display

Systems

Systems

Licenses

Deployment Details

Event Limit: 1000/30000

Flow Limit: 50000/1200000

Users: 1

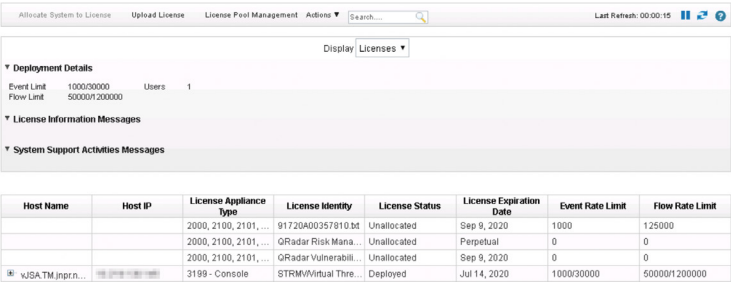
License Information Messages

System Support Activities Messages

Host Name	Host IP	Appliance Type	Version	Serial Number	Host Status	License Expiration Date	License Status	Event Rate Limit	Flow Rate Limit
xJSA(cons...	10...	3199 - Console	7.4.0	VMware-56 4d...	Active	Jul 14, 2020	Deployed	1000/30000	50000/1200000

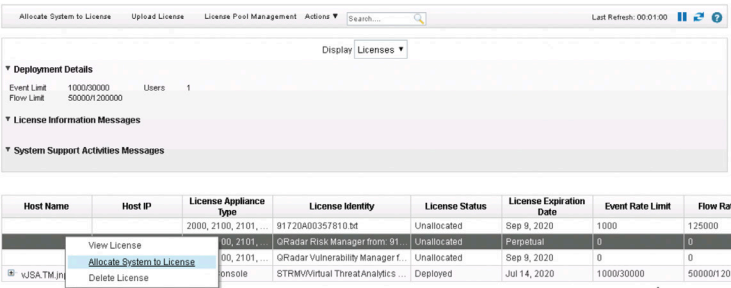
The page displays the license that you have uploaded (Figure 312).

Figure 312 License Display Page



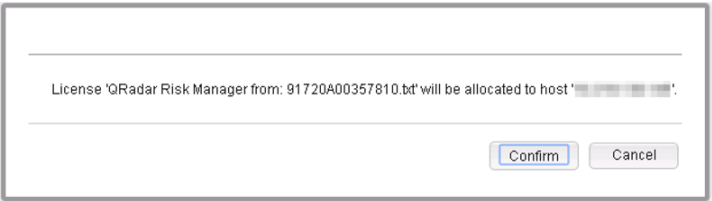
Right-click the license and click **Allocate System to License**, as shown in Figure 313.

Figure 313 Allocate System to License



A confirmation message appears asking you to confirm whether the license should be allocated to the system (Figure 314). Click **Confirm** to allocate the license file to the system.

Figure 314 Confirm Allocate System to License



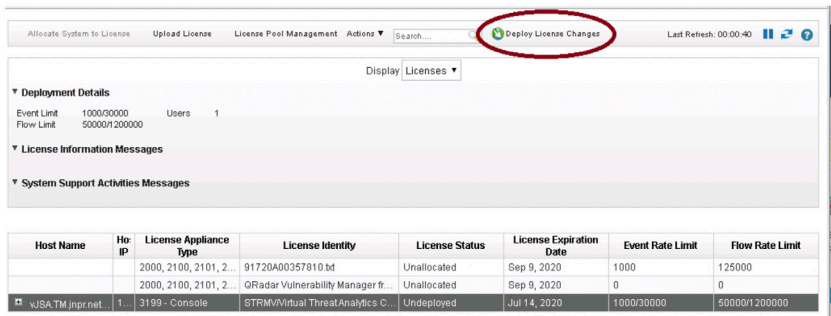
You can see the system was allocated to the system as shown in Figure 315.

Figure 315 System Allocated



Proceed with Deploy Changes as described in the next scenario.

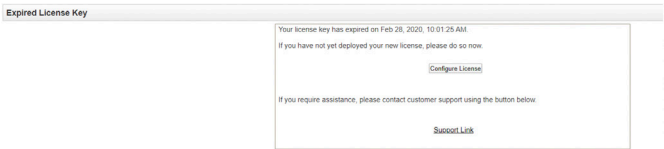
Figure 316 Deploy License Changes



Scenario Two: License has Expired

If the license has already expired, you will see a screen similar to Figure 317.

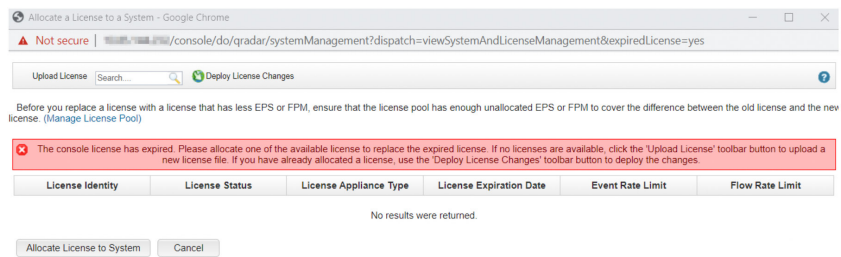
Figure 317 Expired License Key



Here's how to apply a license. First, make sure you have downloaded the license file to the system (for example, your desktop) from where you are accessing the JSA web UI.

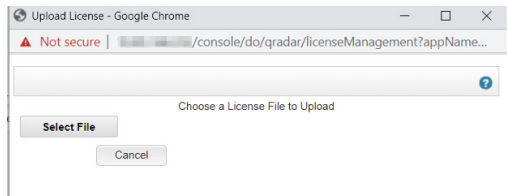
Then click on Configure License to apply a new license. Click on Upload License. The Upload License page appears (Figure 318).

Figure 318 Upload License Key



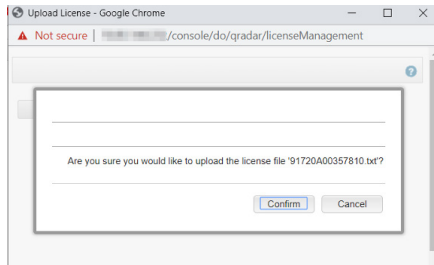
Select the license file that you have saved (Figure 319).

Figure 319 Select License Key



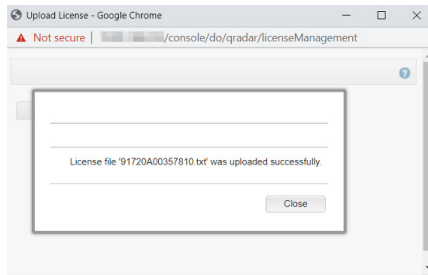
Click Confirm to upload the license file, as shown in Figure 320.

Figure 320 Upload License Key



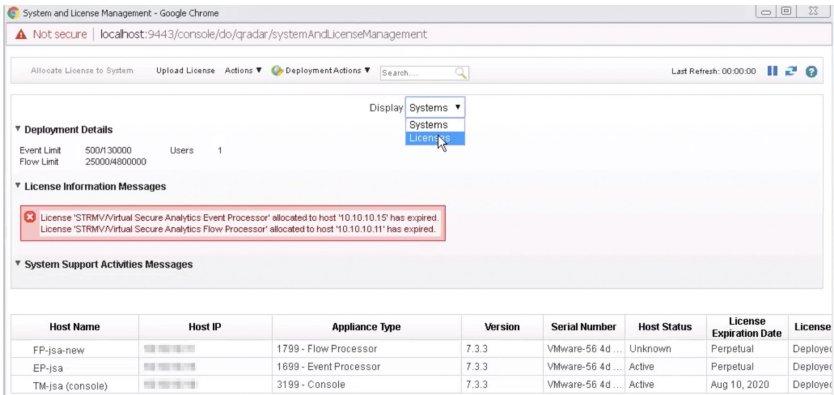
You will see a message that the license file is successfully uploaded, as shown in Figure 321.

Figure 321 License Key Upload Success



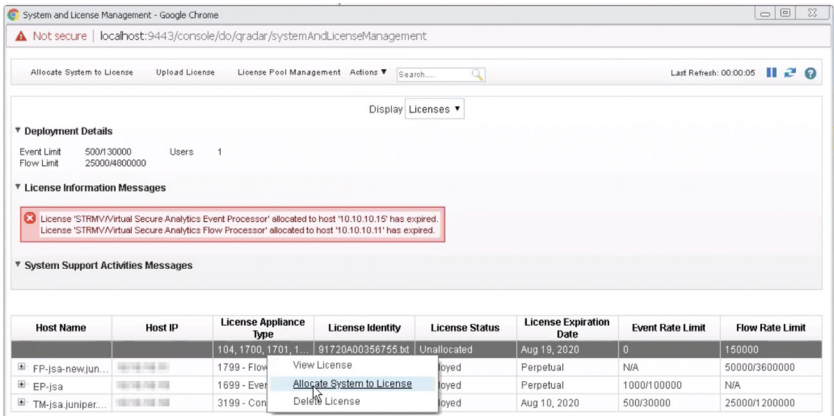
The uploaded license is not yet allocated to the system. To do so, go to the System and License Management page and select Licenses in the Display drop-down, as shown in Figure 322.

Figure 322 Go to Licenses Page



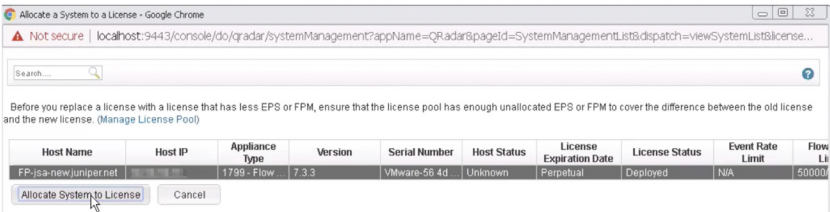
The page displays the license that you have uploaded. Right-click the license and click Allocate license to System, as shown in Figure 323.

Figure 323 Allocate License Key



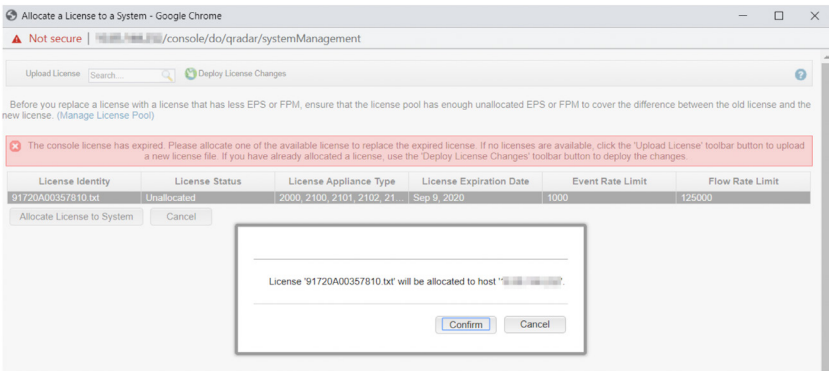
The Allocate a System to a License page appears (Figure 324). Select the license and click Allocate license to System.

Figure 324 *Allocate License Key*



A confirmation message appears asking you to confirm whether the license should be allocated to the system. Click Confirm to allocate the license file to the system, as shown in Figure 325.

Figure 325 *License Allocation Confirmation*



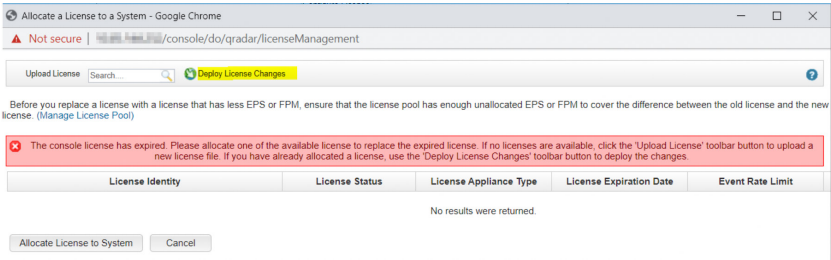
You will see a message confirming that the license has been allocated.

NOTE The procedure for applying a license is same irrespective of the appliance type. If you want to apply a license to a console, select console and allocate the license. If you want to apply license to an EP, select that specific EP and then allocate the license.

Changes that are made to the JSA deployment must be pushed from the staging area to the production area. Since you have uploaded and allocated a new license to JSA, you need to deploy this change. To do this. Click Deploy License Changes, as shown Figure 326.

Figure 326

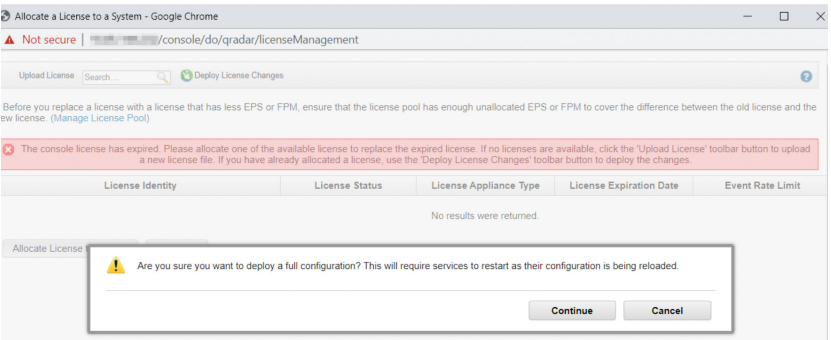
Deploy Changes



Click Continue to deploy the changes to the system, as shown in Figure 327.

Figure 327

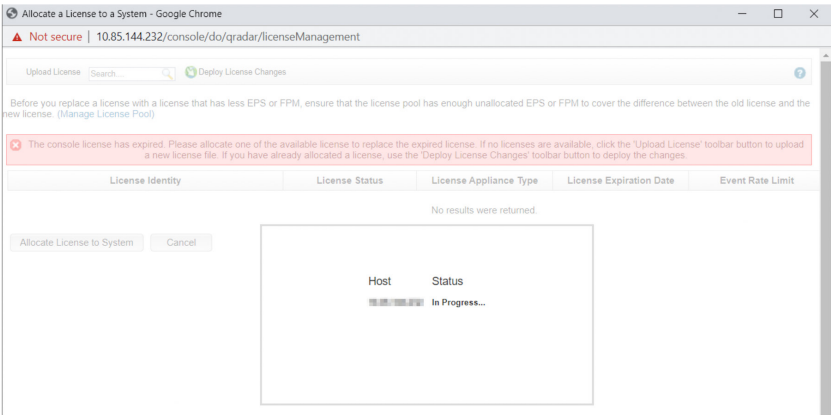
Deploy Changes Confirmation



The deployment process begins, as shown in Figure 328. It will take some time to complete.

Figure 328

Deploying Changes



Once the deployment is complete the license will be successfully applied to the system. You can now log in to the JSA web UI.

Manage the License Pool

After you apply the license keys to JSA, you can ensure that each of the managed hosts is allocated enough capacity to handle the average volume of network traffic and still have enough events per second (EPS) and flows per minute (FPM) available to efficiently handle a data spike.

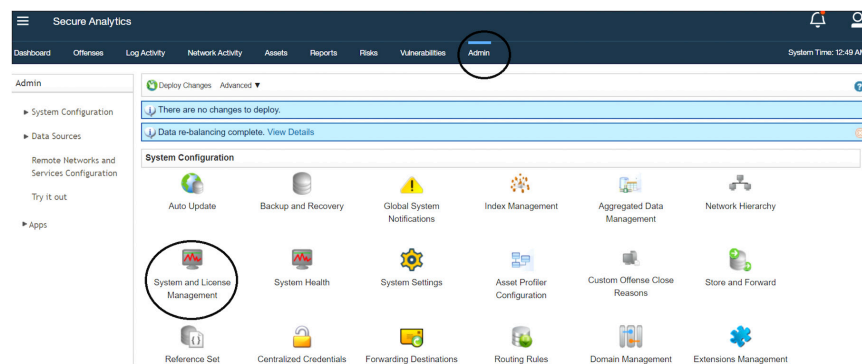
JSA allows license (EPS and FPM) values to be distributed to manage hosts the way you want. EPS and FPM values are not tied to any specific devices and you can increase or decrease the EPS/FPM values allocated to any managed hosts seamlessly. This is useful in situations where you see some sites' EP/FP requires more EPS/FPM compared to other sites where the EPS/FPM values may be under-utilized.

Flexible licensing means that the console manages all EPS. You can dynamically assign and control which EP gets how much EPS as needed. You can also move EPS/FPM from one EP/FP to another easily.

NOTE You do not need to deploy the changes after you redistribute the EPS and FPM capacity.

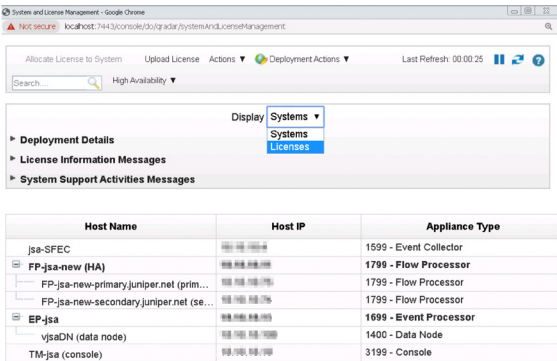
Here's how you can manage the license pool. Click Admin to open the Admin tab. In the System Configuration section, click System and License Management, as shown in Figure 329.

Figure 329 System and License Management



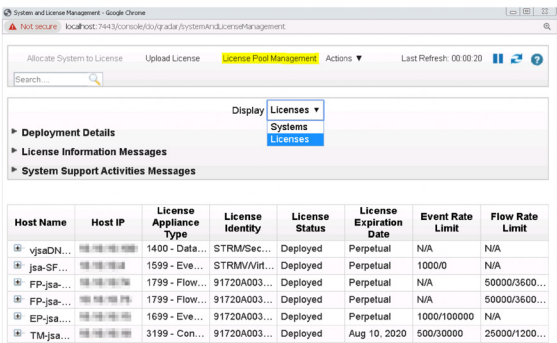
From the Display list (Figure 330), select Licenses.

Figure 330 Allocate License to System



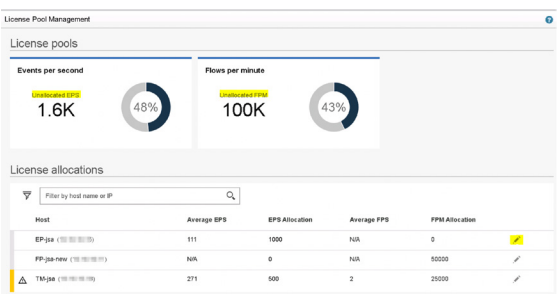
Click on License Pool Management (Figure 331).

Figure 331 License Pool Management



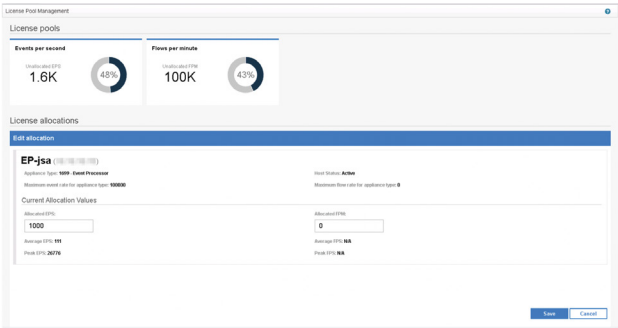
Edit and allocate EPS and FPM values to managed hosts from the total unallocated values as seen in Figure 332.

Figure 332 License Pools and Allocations



Click Save as shown in Figure 333.

Figure 333 License Pools and Allocations



The EPS and FPS values will be allocated to the managed hosts.

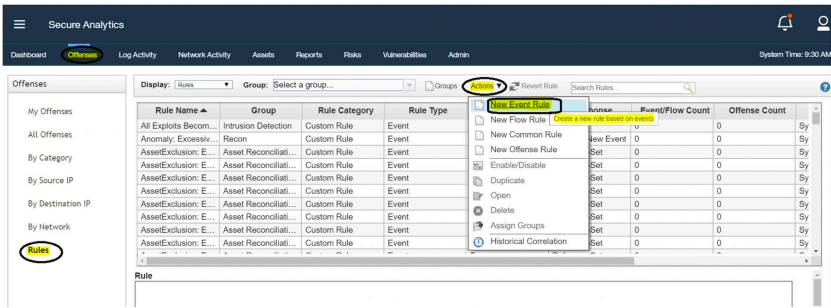
Create an Offense Rule

JSA comes with hundreds of default correlation rules. Rules can be event rules, flow rules, common (event + flow) rules, and offense rules. Though there are default rules, not all the rules are enabled. You can enable or disable the CRE rules per your requirements. Also, you can create and customize rules for your requirement.

Let’s suppose that you want to know if any user is using Telnet (unencrypted and hence, insecure) to access the servers. You can create an offense in JSA to track this activity and notify you if this event occurs.

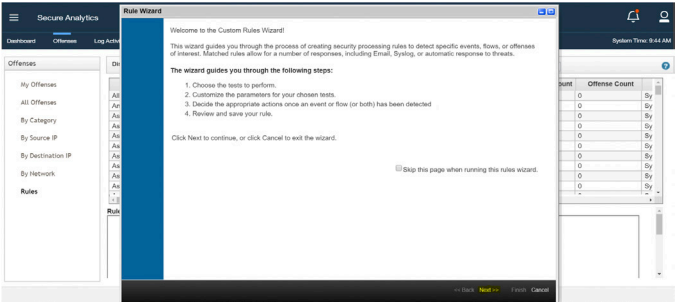
Here’s how to create that offense. Log in to JSA and select the Offense tab. Go to Rules and click the Actions menu. Select a New Event Rule as shown in Figure 334.

Figure 334 Create a New Event Rule



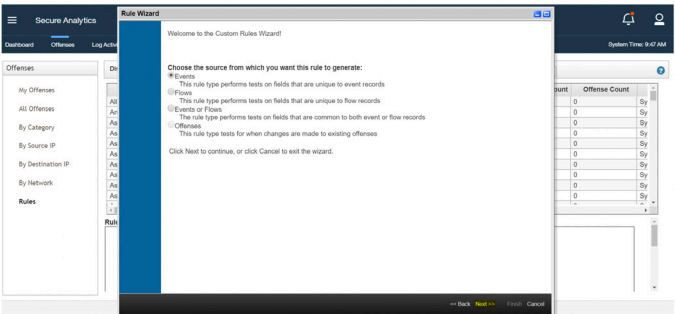
The Rules Wizard appears as shown in Figure 335. Click Next.

Figure 335 Rules Wizard



Select Events and click Next as in Figure 336.

Figure 336 Rule for Events



The Rule Test Stack Editor page appears. Enter a suitable name for the new rule, and then select the rule condition for which the offense needs to be triggered as shown in Figure 337 and Figure 338. In this example, you want an offense to be generated for events with destination port 23 (Telnet). Click Next.

Figure 337 Define a Rule – Port Information

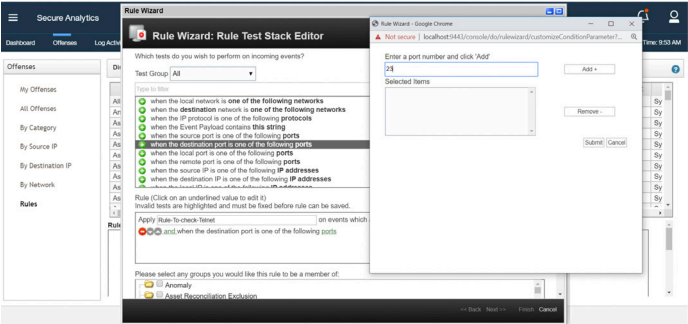
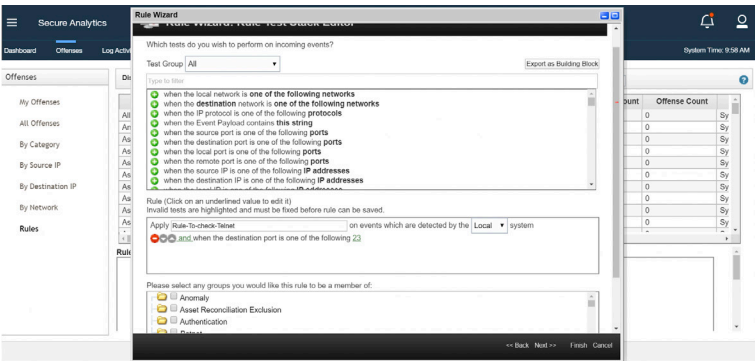
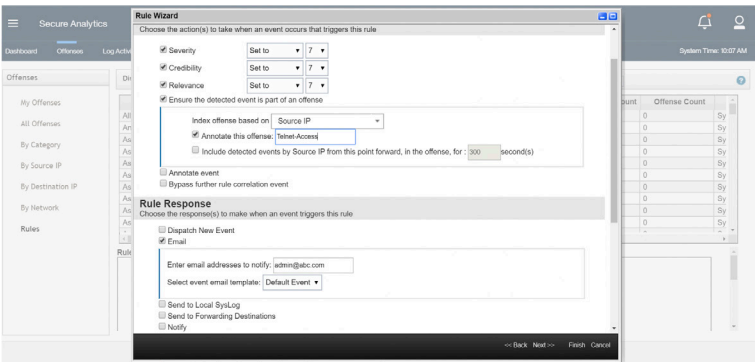


Figure 338 Define a Rule – Test Information



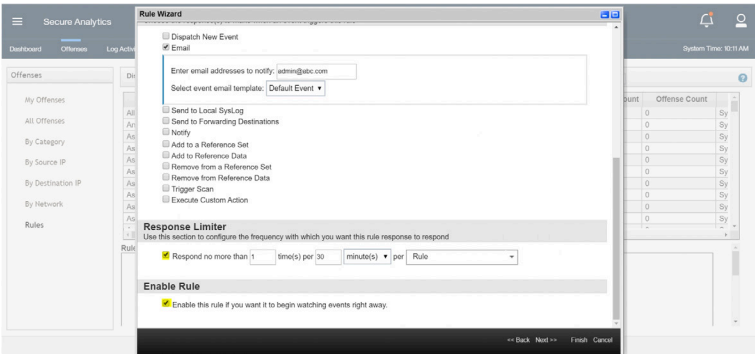
Now select the severity, credibility, and relevance of the rule shown in Figure 339. These values are used to calculate the magnitude of the offense.

Figure 339 Define Rule Severity, Credibility, and Relevance



Next, as shown in Figure 340, fill the response limiter with your requirements and enable the rule by selecting Enable this rule if you want to begin watching events right away. Click Finish.

Figure 340 Define Response Limiter and Enabling the Rule



The new offense is created and enabled. Whenever a user uses Telnet, an offense is created and allows you to track this activity.

NOTE Make sure that JSA is getting events from log sources indicating this activity (Telnet), for example, a firewall (log source) which has the firewall rule permitting or denying port 23, they should be logging this activity and sending these logs to JSA. Co-relation rules are applied on the data (events or flows) that JSA collects from log sources and flow sources.

Determine the Current Version of JSA Software

Run the `su` CLI command to find out the current version of JSA software, as shown in Figure 341.

Figure 341 The `su` Command

```
[root@TM-jsa ~]# su
This server has Secure Analytics 7.3.3 (Build 20191006204340) installed on Sat Nov 30 23:55:45 EST 2019.
```

For more details, run the `/opt/qradar/bin/myver -v` command, as shown in Figure 342.

Figure 342 JSA Software Version

```
[root@primary-primary ~]# /opt/qradar/bin/myver -v
Product is 'QRadar'
Appliance is '3199'
Core version is '7.3.1.20180327211425'
Patch '7.3.1.20181123182336'
Latest version is '7.3.1.20181123182336'
Branded version is ''
Branded latest version is ''
Release name is ''
Version installed with is '7.3.1.20180327211425'
Internal version is '7.3.1.8'
RPM version is '7.3.1.20181123182336'
QRM enabled: 'false'
QRM DB enabled: 'false'
QVM DB enabled: 'true'
QF DB enabled: 'false'
Graph DB enabled: 'false'
Console: 'true'
Console IP: '10.10.10.10'
IP address: '10.10.10.10'
Vendor: 'Juniper Networks'
Branded Product Name: 'Secure Analytics'
Product Description: 'Secure Analytics'
Kernel architecture: 'x86_64'
CPU supports 64bit: 'true'
Operating System: 'Red Hat Enterprise Linux Server release 7.5 (Maipo)'
HA identity: 'primary'
```

Collect Troubleshooting Logs from JSA

Following are the main log files:

`/var/log/qradar.log` – All logs including normal logs

`/var/log/qradar.error` – Errors and exceptions

Table 8 shows the other log files which will help you identify issues with specific modules.

Table 8 *List of JSA Log Files*

Log File	Description
<code>/var/log/qradar-sql.log</code>	SQL related logs
<code>/opt/tomcat6/logs/catalina.out</code>	Apache Tomcat related logs
<code>/var/log/qflow.debug</code>	Debug logs. You must first enable the debugging settings separately.
<code>/var/log/qradar-ha.log</code>	JSA High Availability related logs
<code>/var/log/qradar.old</code>	Old log files which are log rotated are zipped
<code>/var/log/qradar-iptables.log</code>	iptables related logs
<code>/var/log/autoupdates/</code>	Weekly auto updates related logs
<code>/var/log/dca/dca_info.log</code>	X-Force related logs

Collect Logs from the Command Line Interface

Use the `/opt/qradar/support/get_logs.sh` command to collect the following troubleshooting logs shown in Figure 343.

Figure 343 Using the `get_logs.sh` Command

```
[root@TM-jsa ~]# /opt/qradar/support/get_logs.sh

-----
get_logs.sh v5.6 - TM-jsa.juniper.net
-----

INFO: Gathering install information...
INFO: Collecting cliniq output...
INFO: Collecting DrQ output...
INFO: Collecting system files...
INFO: Collecting old files...
INFO: Collecting Cert metadata...
INFO: Collecting accumulator information with collectGvStats.sh v1.8...
INFO: Collecting deployment info with deployment_info.sh v0.6...
INFO: Collecting thread dumps from running java processes...
INFO: Collecting database information...
INFO: Collecting rpm version information...
INFO: Collecting QVM files...
INFO: running extractRules.py...
INFO: Gathering extract rules and adding to get_logs...
INFO: Compressing collected files...

The file /store/LOGS/logs_TM-jsa_20200322_2e8d9540.tar.gz (159M) has been created to send to support
```

To understand different options for the `get_logs.sh` command, use the help command, as shown in Figure 344.

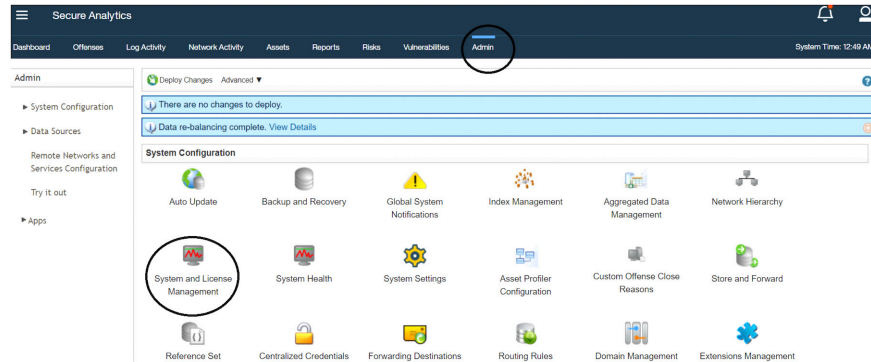
Figure 344 Understanding the `get_logs.sh` Command

```
[root@JSA-IM ~]# /opt/qradar/support/get_logs.sh --help
get_logs.sh v5.3
Usage:
  -o                :: Include /var/log/qradar.old/qradar.log.1.gz and qradar.error.1.gz (obsolete: this is now default behaviour)
  -g {# of days}   :: Include the last {# of days} of old files in /var/log/qradar.old/
  -s               :: Include /var/log/setup-(current version)/*
  -S              :: Include /var/log/setup-(all versions)/*
  -d               :: Include /var/log/qradar.java.debug (obsolete: will automatically grab qradar.java.debug if less than 30 days old)
  -D               :: Include logs from defect-inspector --long /var/log/qradar.error
  -a               :: Include app-framework logs and configuration (obsolete: this is now a default behaviour)
  -g {file}        :: Include git history of file in /opt/qradar/conf (runs: git log --stat -p <file>)
  -l               :: Generate only the log.qradar.info.txt file.
  -i {files}       :: Requires an argument of quoted and space separated files or directories to also include in the tarball
  -x {files}       :: Requires an argument of quoted and space separated files or directories to exclude from the tarball. Accepts regex patterns.
  -H {hosts}       :: Requires an argument of quoted and comma separated ips or hostnames. Will collect logs from these hosts and store them in ./GETLOGS 20200322. Always includes the console.
  -e               :: Encrypt the resulting tarball
  -v               :: Display revision information
  -t               :: Collect additional asset information and db tables
  -h,--help        :: Displays this dialog
```


Collect Logs from JSA Web UI

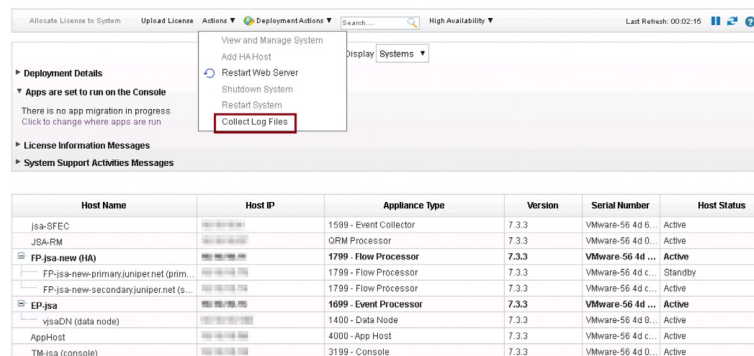
To collect the troubleshooting logs from the JSA web UI, log in to the JSA application and on the navigation menu, click Admin. The Admin page appears. In the Admin page, select System and License Management, as shown in Figure 345.

Figure 345 System and License Management



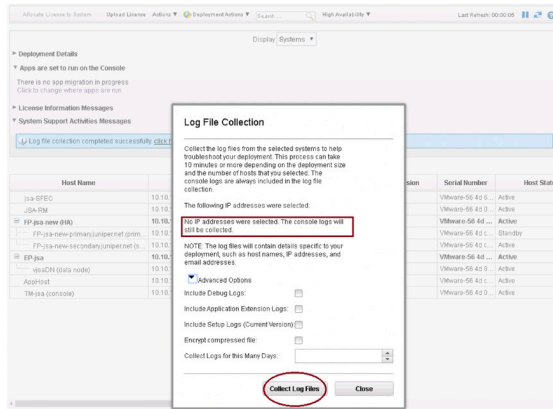
Now select Collect Log Files, as shown in Figure 346.

Figure 346 Collect Log Files



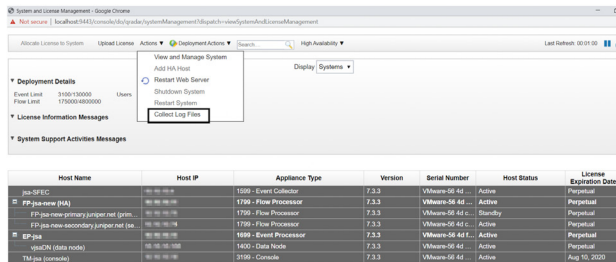
If no hosts are selected, by default, console logs will be collected (Figure 347).

Figure 347 Log File Collection



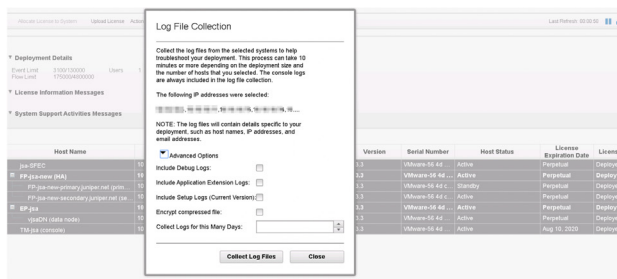
Select the host(s) you want to collect the troubleshooting logs from and then select **Collect Log Files**, as shown in Figure 348.

Figure 348 Collect Log Files



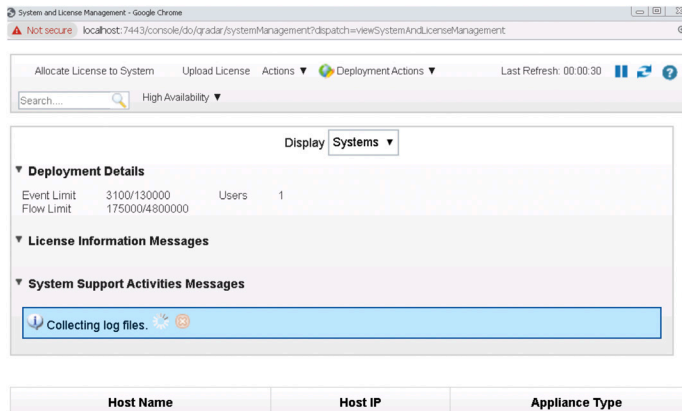
Now select the appropriate options (if required) and click **Collect Log Files**, as shown in Figure 349.

Figure 349 Collect Log Files Options



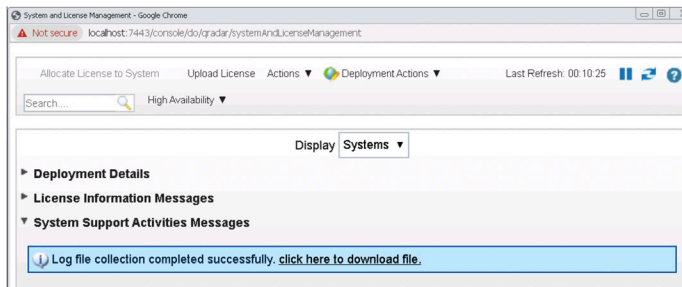
Log collection begins with status shown in Figure 350.

Figure 350 Collecting Log Files



Once the log collection is complete, a link is provided to download the log file, as shown in Figure 351. You can download the logs to your desktop.

Figure 351 Log Files Collection Confirmation



NOTE In the CLI, the troubleshooting logs generated by `get_logs.sh` are always downloaded into the `/store/LOGS` folder.

If you are having application or extension issues, use the `-a` option to collect the application logs with your console log information. If you have issues with a managed host, use the `get_logs.sh` utility as a backup when the JSA user interface is not available.

Configure Online Auto-updates

You can use online auto-updates to automatically or manually update your configuration files to ensure that your configuration files contain the latest network security information. Updated configuration files help eliminate false positives and protect your system from the latest malicious sites, botnets, and other suspicious Internet activity.

In order to receive the *online auto-updates*, your JSA console must be connected to the Internet. If your console is not connected to the Internet, you must configure an internal update server for your console to download the files from (*offline auto-update*) that is detailed in the next chapter section.

To maintain the integrity of your current configuration's information, you can either replace your existing configuration files or integrate the updated files with your existing files. After you install the updates on your console and deploy your changes, the console will update its managed hosts.

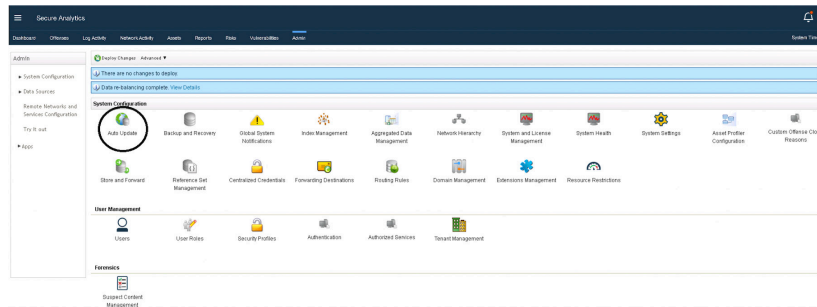
These files can include the following updates:

- Configuration updates that are based on content, including configuration file changes, vulnerabilities, QID maps, supportability scripts, and security threat information updates.
- DSM, scanner, and protocol updates that include corrections to parsing issues, scanner changes, and protocol updates.
- Major updates such as updated JAR files or large patches that require restarting the user interface service.
- Minor updates such as daily automatic update logs or QID map scripts that don't need restarting the user interface service.

Step-by-Step Procedure

Log in to the JSA application. Click Admin in the navigation menu. The Admin page appears (Figure 352).

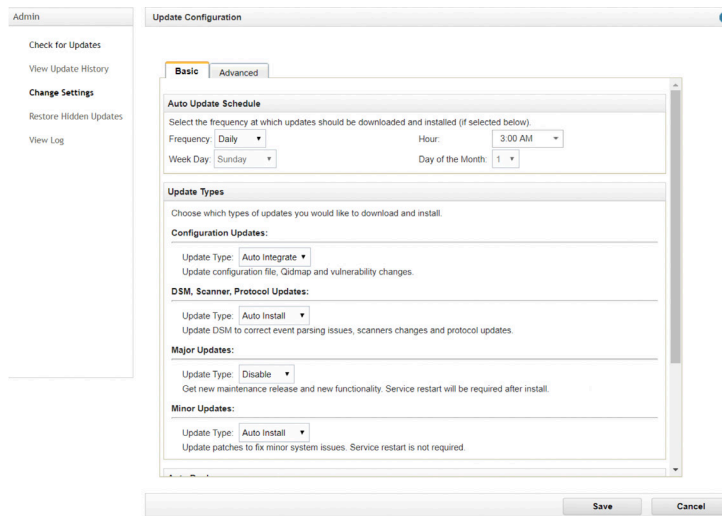
Figure 352 Admin Page



Click Auto Update.

The auto-update settings page appears (Figure 353).

Figure 353 Update Configuration



In the Basic tab, select the schedule for updates. In the Configuration Updates section, select the method that you want to use for updating your configuration files. To merge your existing configuration files with the server updates without affecting your custom signatures, custom entries, and remote network configurations, select Auto Integrate. To override your customizations with server settings, select Auto Update.

In the DSM, Scanner, Protocol Updates section, select an option to install updates.

In the Major Updates section, select an option for receiving major updates for new releases.

In the Minor Updates section, select an option for receiving patches for minor system issues.

If you want to deploy the updated changes automatically after the updates are installed, select the Auto Deploy check box. If you do not select Auto Deploy, you must manually deploy changes from the Dashboard tab.

NOTE In a high-availability (HA) environment, automatic updates are not installed when a secondary host is active. The updates are installed only after the primary host becomes the active node.

If you want to restart the user interface service automatically after updates are installed, select the Auto Restart Service check box. A user interface disruption occurs when the service restarts. Alternatively, you can manually install the update from the Check for Updates window.

Click the Advanced tab to configure the update server and backup settings. In the Web Server field, type the web server from which you want to obtain the updates. The default web server is <https://download.juniper.net/>.

In the Directory field, type the directory location on which the web server stores the updates. The default directory is `autoupdates/`.

Optional: Configure the Settings for a Proxy Server

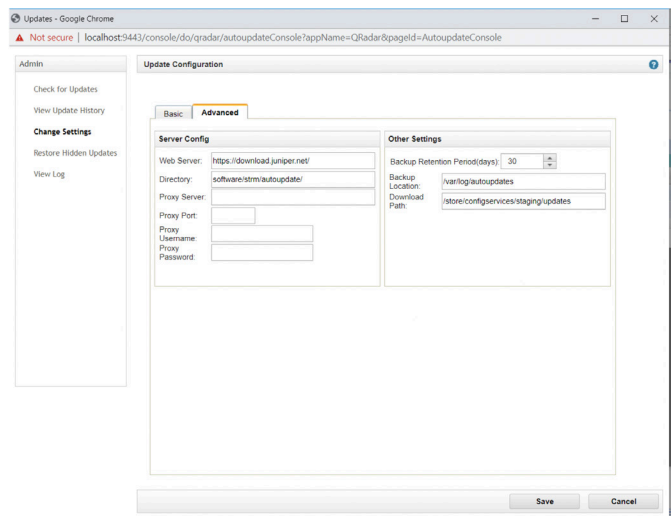
If the application server uses a proxy server to connect to the Internet, you must configure the proxy server. If you are using an authenticated proxy, you must provide the username and password for the proxy server.

In the Backup Retention Period list, type or select the number of days that you want to store files that are replaced during the update process. The files are stored in the location that is specified in the Backup Location.

In the Backup Location field, type the location where you want to store backup files. In the Download Path field, type the directory path location to which you want to store DSM, minor, and major updates. The default directory path is:

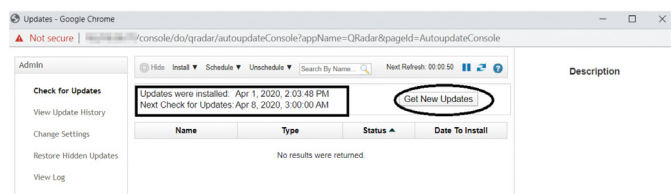
`/store/configservices/staging/updates`

Figure 354 Advanced Settings



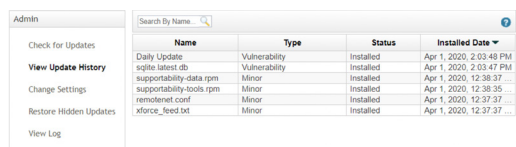
When complete, click Save. To see the latest auto-update details, click Check for Updates tab. To initiate an auto-update for the latest updates, click Get New Updates as shown in Figure 355.

Figure 355 Get New Updates



To see the details of the updates click View Update History, shown in Figure 356.

Figure 356 View Update History



You can view limited auto-update logs in /var/log/qradar.log using CLI commands.

Figure 357 View Auto-update Logs

```
[root@primary-primary ~]# less /var/log/qradar.log | grep -i autoupdate

Apr  7 03:37:14 primary-primary AUTOUPDATE[1769]: Version: 9.5
Apr  7 03:37:14 primary-primary AUTOUPDATE[1769]: Supplied Version: 9.5
Apr  7 03:37:14 primary-primary AUTOUPDATE[1769]: Manifest type is Patches
Apr  7 03:37:14 primary-primary AUTOUPDATE[1769]: Latest patches are already installed with serial 131315
9022 from 08/12/2011 at 19:53.
Apr  7 03:37:14 primary-primary AUTOUPDATE[1769]: Status: 3
Apr  7 03:37:14 primary-primary AUTOUPDATE[1769]: Auto updates has completed installing.
```

To view more detailed auto-update logs you must extract the AU-timestamp.gz file from the /var/log/autoupdates directory.

Figure 358 Detailed Auto-update Logs

```
[root@TM-jsa autoupdates]# less /var/log/qradar.log | grep -i autoupdate | more
Feb 27 03:25:01 TM-jsa AUTOUPDATE[17777]: Autoupdate 8.9 initialized.
Feb 27 03:25:01 TM-jsa AUTOUPDATE[17777]: Do we need to turn on SSL Cert
Feb 27 03:25:01 TM-jsa AUTOUPDATE[17777]: SSL cert is set correctly
Feb 27 03:25:16 :ffff:10.10.10.18 [qvmprocessor.qvmprocessor] [pool-3-thread-1] com.qllabs.qvm.workflow.event.handler.AutoUpdateStateChange
FO] (NOR:0000006000) [10.10.10.18/-] [/~ -]AutoUpdateStateChangedEventHandler >>> processing autoupdate changed event. state is (RUNNING)
Feb 27 03:25:25 TM-jsa AUTOUPDATE[17777]: Could not retrieve "manifest_list": 500 Can't connect to download.juniper.net:443
Feb 27 03:25:25 TM-jsa AUTOUPDATE[17777]: Could not download manifest list.
Feb 27 03:25:44 :ffff:10.10.10.18 [qvmprocessor.qvmprocessor] [pool-3-thread-3] com.qllabs.qvm.workflow.event.handler.AutoUpdateStateChange
FO] (NOR:0000006000) [10.10.10.18/-] [/~ -]AutoUpdateStateChangedEventHandler >>> processing autoupdate changed event. state is (STOPPED)
Feb 28 03:25:02 TM-jsa AUTOUPDATE[15557]: Autoupdate 8.9 initialized.
Feb 28 03:25:02 TM-jsa AUTOUPDATE[15557]: Do we need to turn on SSL Cert
Feb 28 03:25:02 TM-jsa AUTOUPDATE[15557]: SSL cert is set correctly
Feb 28 03:25:25 TM-jsa AUTOUPDATE[15557]: Could not retrieve "manifest_list": 500 Can't connect to download.juniper.net:443
Feb 28 03:25:25 TM-jsa AUTOUPDATE[15557]: Could not download manifest list.
Feb 29 03:25:01 TM-jsa AUTOUPDATE[23102]: Autoupdate 8.9 initialized.
Feb 29 03:25:01 TM-jsa AUTOUPDATE[23102]: Do we need to turn on SSL Cert
Feb 29 03:25:01 TM-jsa AUTOUPDATE[23102]: SSL cert is set correctly
Feb 29 03:25:09 :ffff:10.10.10.18 [qvmprocessor.qvmprocessor] [pool-3-thread-1] com.qllabs.qvm.workflow.event.handler.AutoUpdateStateChange
FO] (NOR:0000006000) [10.10.10.18/-] [/~ -]AutoUpdateStateChangedEventHandler >>> processing autoupdate changed event. state is (RUNNING)
Feb 29 03:25:24 TM-jsa AUTOUPDATE[23102]: Could not retrieve "manifest_list": 500 Can't connect to download.juniper.net:443
Feb 29 03:25:24 TM-jsa AUTOUPDATE[23102]: Could not download manifest list.
Feb 29 03:25:39 :ffff:10.10.10.18 [qvmprocessor.qvmprocessor] [pool-3-thread-1] com.qllabs.qvm.workflow.event.handler.AutoUpdateStateChange
FO] (NOR:0000006000) [10.10.10.18/-] [/~ -]AutoUpdateStateChangedEventHandler >>> processing autoupdate changed event. state is (STOPPED)
Mar  1 03:25:02 TM-jsa AUTOUPDATE[28205]: Autoupdate 8.9 initialized.
Mar  1 03:25:02 TM-jsa AUTOUPDATE[28205]: Do we need to turn on SSL Cert
Mar  1 03:25:02 TM-jsa AUTOUPDATE[28205]: SSL cert is set correctly
Mar  1 03:25:19 :ffff:10.10.10.18 [qvmprocessor.qvmprocessor] [pool-3-thread-2] com.qllabs.qvm.workflow.event.handler.AutoUpdateStateChange
FO] (NOR:0000006000) [10.10.10.18/-] [/~ -]AutoUpdateStateChangedEventHandler >>> processing autoupdate changed event. state is (RUNNING)
Mar  1 03:25:25 TM-jsa AUTOUPDATE[28205]: Could not retrieve "manifest_list": 500 Can't connect to download.juniper.net:443
Mar  1 03:25:25 TM-jsa AUTOUPDATE[28205]: Could not download manifest list.
Mar  1 03:25:49 :ffff:10.10.10.18 [qvmprocessor.qvmprocessor] [pool-3-thread-2] com.qllabs.qvm.workflow.event.handler.AutoUpdateStateChange
FO] (NOR:0000006000) [10.10.10.18/-] [/~ -]AutoUpdateStateChangedEventHandler >>> processing autoupdate changed event. state is (STOPPED)
```

root@TM-jsa:/var/log/autoupdates

```
-rw-r--r-- 1 root root 677 Mar 3 03:25 AU-1583223902.tgz
-rw-r--r-- 1 root root 676 Mar 4 03:25 AU-1583310301.tgz
-rw-r--r-- 1 root root 677 Mar 5 03:25 AU-1583396702.tgz
-rw-r--r-- 1 root root 679 Mar 6 03:25 AU-1583483101.tgz
-rw-r--r-- 1 root root 676 Mar 7 03:25 AU-1583569501.tgz
-rw-r--r-- 1 root root 677 Mar 8 03:25 AU-1583652302.tgz
-rw-r--r-- 1 root root 676 Mar 9 03:25 AU-1583738701.tgz
-rw-r--r-- 1 root root 678 Mar 10 03:25 AU-1583825102.tgz
-rw-r--r-- 1 root root 676 Mar 11 03:25 AU-1583911502.tgz
-rw-r--r-- 1 root root 680 Mar 12 03:25 AU-1583997902.tgz
-rw-r--r-- 1 root root 676 Mar 13 03:25 AU-1584084301.tgz
-rw-r--r-- 1 root root 1775 Mar 13 07:26 AU-1584098761.tgz
drwxr-xr-x 2 root root 53 Mar 13 07:27 AU-1584098823
[root@TM-jsa autoupdates]# pwd
/var/log/autoupdates
[root@TM-jsa autoupdates]# tail -f AU-1584098823/AU-1584098823.log
```


Configure Offline Auto-Updates

You can auto-update JSA when there is no connection available to the Juniper auto-update server. Often, due to security reasons, JSA is not allowed to access the Internet (hence there is no access to the Juniper auto-update site). But with JSA you can set up a local repository.

The auto-update bundle is an update of the latest RPMs for JSA. The auto update bundle from download.juniper.net contains the following content:

- Device support module (DSM) rpm files - New integrations and parsing/categorization updates for existing DSMs.
- Protocol rpm files - New protocols and updates are provided to listen for or retrieve events from remote sources.
- Scanner rpm files - New scanner module releases and updates.
- Vulnerability catalog updates - The vulnerability catalog update is a database file that includes CVE information, vulnerability descriptions, and signature information so that scan results have the latest vulnerability information to display in the Asset tab or Vulnerability tab for users with JSA Vulnerability Manager. Vulnerability catalog updates are typically delivered daily for Internet connected systems.

NOTE The auto-update file size is approximately 4.5 GB. Make sure you transfer the file to a partition/directory that has enough disk space available (for example /transient/autoupdate).

Step-by-Step Procedure

Download the autoupdate package from <https://support.juniper.net/support/downloads/>.

Log in to JSA as the root user. Create a directory in /transient (for example mkdir /transient/autoupdate). Now type the following command to create the auto-update directory and a soft-link to it.

NOTE By default the /opt directory has less disk space. So, copying the auto-update files into the /opt directory can cause disk space outage issues and may impact the services in JSA. Best practice is to create a soft link to the auto-update files:

```
cd /opt/qradar/www
mkdir -p software/strm/
cd /opt/qradar/www/software/strm
ln -s /transient/autoupdate autoupdate
```

By default, /opt/qradar/www/software/strm/autoupdate/ will not be present, you will need to create the directory.

Figure 359 Verify the Soft Link

```
[root@TM-jsa autoupdate]# cd /opt/qradar/www/software/strm/autoupdate/
[root@TM-jsa autoupdate]#
[root@TM-jsa autoupdate]# ls -la | grep -i autoupdate
lrwxrwxrwx 1 root root 21 Jun 28 04:55 autoupdate -> /transient/autoupdate
[root@TM-jsa autoupdate]#
```

Copy the autoupdate-XX.tgz file to the /transient/autoupdate directory. On your JSA console, type the following command to decompress the auto-update package.

```
tar -zxvf autoupdate[timestamp].tgz
```

Figure 360 Save Auto-update Package File in /transient Directory

```
[root@TM-jsa autoupdate]#
[root@TM-jsa autoupdate]# cd /transient/autoupdate
[root@TM-jsa autoupdate]# tar -zxvf autoupdate-02282020.tgz
dau/
dau/dau.manifest.xml.asc
dau/feeds/
```

Validate if all the files are present under /transient/autoupdate/.

```
cd /transient/autoupdate/
ls -la
```

Figure 361 Validate Files in /transient/autoupdate/

```
[root@TM-jsa autoupdate]# ls -la
total 3882444
drwxr-xr-x 6 root root      195 Jun 28 05:28 .
drwxrwxr-t 7 root siem     145 Jun 28 05:36 ..
-rwxr-xr-x 1 root root 3156403115 Mar 13 06:40 autoupdate-02282020.tgz
drwxr-sr-x 5 500 500       94 Feb 28 10:02 dau
-rw-rw-r-- 1 root root     263 Feb 28 00:55 manifest_list
-rwxr-xr-x 1 500 500     615 Feb 28 00:55 manifest_list_512
drwxr-sr-x 5 500 500     241 Feb 21 09:36 patches
drwxr-sr-x 2 500 500       94 Feb 21 09:36 scripts
-rwxr-xr-x 1 500 500     143 Feb 28 00:56 vendor_manifest_list
-rwxr-xr-x 1 500 500     319 Feb 28 00:56 vendor_manifest_list_512
drwxr-sr-x 4 500 500       93 Feb 21 09:36 wau
[root@TM-jsa autoupdate]#
```

Now, log into the JSA web UI and click Admin to open the Admin tab. In the System Configuration section, click Auto Update. Click Change Settings, and click the Advanced tab.

In the web server field, type: <https://localhost/> or <https://127.0.0.1/> and make sure you include forward slashes.

In the Directory field, type `software/strm/autoupdate/` and make sure you include forward slashes, as shown in Figure 362.

Figure 362 Update Configuration

The screenshot shows the 'Update Configuration' window with the 'Advanced' tab active. On the left is an 'Admin' sidebar with links: 'Check for Updates', 'View Update History', 'Change Settings', 'Restore Hidden Updates', and 'View Log'. The main area is divided into 'Server Config' and 'Other Settings'. Under 'Server Config', 'Web Server' is 'https://127.0.0.1/' and 'Directory' is 'software/strm/autoupdate/'. Under 'Other Settings', 'Backup Retention Period(days)' is 30, 'Backup Location' is '/var/log/autoupdates', and 'Download Path' is '/store/configservices/staging/updates'.

Click Save. You will receive a notification, which is normal.

Click Check for Updates from the left menu and click the Get New Updates button, as shown in Figure 363.

Figure 363 Get New Updates

The screenshot shows the 'Check for Updates' section. It includes a 'Get New Updates' button. Below the button, it states 'Updates were installed: Oct 14, 2019, 3:30:19 AM' and 'Next Check for Updates: Oct 15, 2019, 3:00:00 AM'. A table with columns 'Name', 'Type', 'Status', and 'Date To Install' is shown, with the message 'No results were returned.'

The auto-update process starts and will take several hours to complete.

Configuration and Data Backup in JSA

You can back up and recover JSA configuration information and data.

JSA configuration is stored in postgres DB. Events and flows collected by JSA are stored in the `/store/ariel` folder.

It is important that you back up the configuration and data so that you can restore this information on a replacement device if needed (such as RMA). For more information, see section *Restoring Data in the JSA Administration Guide*. (https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-administration-guide/information-products/pathway-pages/pathway-m-container-admin-siem.html).

By default, JSA creates a backup archive of your configuration information each midnight. The backup archive includes configuration information, data, or both from the previous day.

You can use two types of backups: configuration backups and data backups. The default installation only backs up the configuration. If you want to disable backups or enable data backups, navigate to Admin>Backup and Recovery> Configure. Configuration backups are a full backup whereas data backups are incremental.

NOTE Data backups contain only the previous day's data and not the entire data.

The configuration backup consists of:

- Application configuration
- Assets
- Custom logos
- Custom rules
- Device Support Modules (DSMs)
- Event categories
- Flow sources
- Flow and event searches
- Groups
- Index Management Information
- License key information
- Log sources
- Offenses
- Reference set elements
- Store and Forward schedules
- User and user roles information
- Custom Dashboards
- Vulnerability data
- Certificates

Data backups consists of:

- Audit log information
- Event data
- Flow data
- Report data
- Indexes

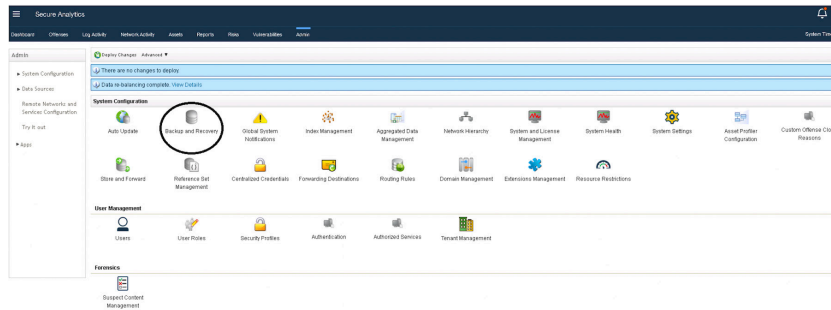
Step-by-Step Procedure

By default, the nightly backup process includes only your configuration files. You can customize your nightly backup process to include data from your JSA console and selected managed hosts. You can also customize your backup retention period, backup archive location, the time limit for a backup to process before timing out, and the backup priority in relation to other JSA processes.

NOTE When you enable data backup on managed hosts, the backup is placed locally on the managed hosts itself. If you require a one-time full back-up of JSA data, you must do this manually. All event and flow data is stored in the /store/ ariel/ directory and this is the directory structure that you need to back up to save event and flow data.

Data backups must be manually enabled. If you want to disable backups or enable data backups, log into the JSA web UI and click on Admin to open the Admin tab (Figure 364). In the System Configuration section, click Backup and Recovery.

Figure 364 Backup and Recovery



The Backup Archives page appears, as shown in Figure 366. On the toolbar click Configure. The Backup Recovery Configuration page appears (Figure 365).

Figure 365 Backup Recovery Configuration

 A screenshot of the 'Backup Recovery Configuration' page in a web browser. The page has a title bar 'Backup Recovery Configuration' and a toolbar with a 'Configure' button. The main content area is divided into sections: 'General Backup Configuration' with fields for 'Backup Repository Path' (set to '/store/backup') and 'Backup Retention Period (days)' (set to 7); 'Nightly Backup Schedule' with radio buttons for 'No Nightly Backups' and 'Configuration Backup Only' (selected); 'Configuration and Data Backups' with a radio button for 'Configuration Only Backup' (selected); 'Configuration Only Backup' with fields for 'Backup Time Limit (min)' (180) and 'Backup Priority' (HIGH, with a warning message: 'Medium and high priorities will have a greater impact on system performance'); 'Data Backup' with fields for 'Backup Time Limit (min)' (1,020) and 'Backup Priority' (LOW); and a red message at the bottom: 'For changes to take effect, click Deploy Changes in the Admin tab menu.' with 'Save' and 'Cancel' buttons.

On the Backup Recovery Configuration window, customize your nightly backup and click Save.

Figure 366 Backup Archives

⚠ Not secure | localhost:7443/console/do/gradar/maintainBackupSummary?dispatch=init

Backup Archives ☐ On Demand Backup Restore Delete Configure

Existing Backups

!	Host	Name	Type	Size	Time Initiated	Duration	Initialized By	Correct Version
	TM-isa_53	nightly	config	852.6MB	Apr 7, 2020, 12:00...	8m 6s	scheduled_initiator	true
	TM-isa_53	nightly	config	852.6MB	Apr 6, 2020, 12:00...	7m 48s	scheduled_initiator	true
	TM-isa_53	nightly	config	852.6MB	Apr 5, 2020, 12:00...	7m 40s	scheduled_initiator	true
	TM-isa_53	nightly	config	852.6MB	Apr 4, 2020, 12:00...	7m 56s	scheduled_initiator	true
	TM-isa_53	nightly	config	852.6MB	Apr 3, 2020, 12:00...	7m 49s	scheduled_initiator	true
	TM-isa_53	nightly	config	852.6MB	Apr 2, 2020, 12:00...	7m 41s	scheduled_initiator	true
	TM-isa_53	nightly	config	852.6MB	Apr 1, 2020, 12:00...	7m 48s	scheduled_initiator	true

Close the Backup Archives page.

On the Admin tab menu, click Deploy Changes. The automatic backup is now configured and will run per the configuration you have provided.

Configure On-Demand Backup

By default, JSA creates a backup archive of your configuration information each midnight. The backup archive includes your configuration information, data, or both from the previous day. You can customize this nightly backup and create an on-demand configuration backup, if required.

If you must back up your configuration files at a time other than your nightly scheduled backup, you can create an on-demand backup archive. On-demand backup archives include only configuration information.

NOTE Initiate an on-demand backup archive during a period when JSA has low processing load, such as after normal office hours because during the backup process system performance can be affected.

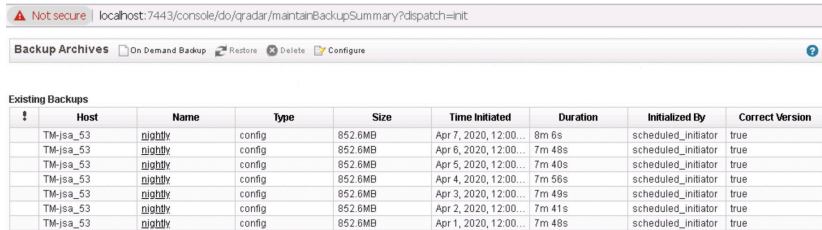
On-demand backup is possible only for configuration. For data this is not possible because of the huge data size.

To make an on-demand configuration back-up, log on to the JSA web UI. Click Admin to open the Admin tab. In the System Configuration section, click Backup and Recovery.

From the toolbar, click On Demand Backup, as shown in Figure 367.

Figure 367

On Demand Backup



Backup Archives | On Demand Backup | Restore | Delete | Configure

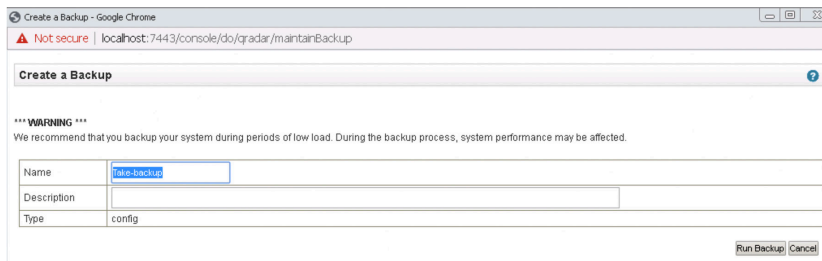
Existing Backups

!	Host	Name	Type	Size	Time Initiated	Duration	Initialized By	Correct Version
	TM-isa_53	nightly	config	852.6MB	Apr 7, 2020, 12:00...	8m 6s	scheduled_initiator	true
	TM-isa_53	nightly	config	852.6MB	Apr 6, 2020, 12:00...	7m 40s	scheduled_initiator	true
	TM-isa_53	nightly	config	852.6MB	Apr 5, 2020, 12:00...	7m 40s	scheduled_initiator	true
	TM-isa_53	nightly	config	852.6MB	Apr 4, 2020, 12:00...	7m 56s	scheduled_initiator	true
	TM-isa_53	nightly	config	852.6MB	Apr 3, 2020, 12:00...	7m 49s	scheduled_initiator	true
	TM-isa_53	nightly	config	852.6MB	Apr 2, 2020, 12:00...	7m 41s	scheduled_initiator	true
	TM-isa_53	nightly	config	852.6MB	Apr 1, 2020, 12:00...	7m 48s	scheduled_initiator	true

Now enter a Name and Description for the backup archive then click Run Backup (Figure 368).

Figure 368

Run Backup



Create a Backup - Google Chrome

Not secure | localhost:7443/console/do/gradar/maintainBackup

Create a Backup

*** WARNING ***
We recommend that you backup your system during periods of low load. During the backup process, system performance may be affected.

Name	tm-isa-backup
Description	
Type	config

Run Backup Cancel

You can start a new backup or restore processes only after the on-demand backup is complete. You can monitor the backup archive process in the Backup Archives window.

The backups are stored under the /store/backup folder on your appliance. Backup files are saved by using the following format:

backup.<name>.<hostname>_<hostID>.<targetdate>.<backup type>.<timestamp>.tgz

Where:

<name> is the name associated with the backup

<hostname> is the name of the system hosting the backup file

<host ID> is the identifier for the system

<target date> is the date that the backup file was created

<backup type> is the type of backup. The options are data or config

<timestamp> is the time that the backup file was created.

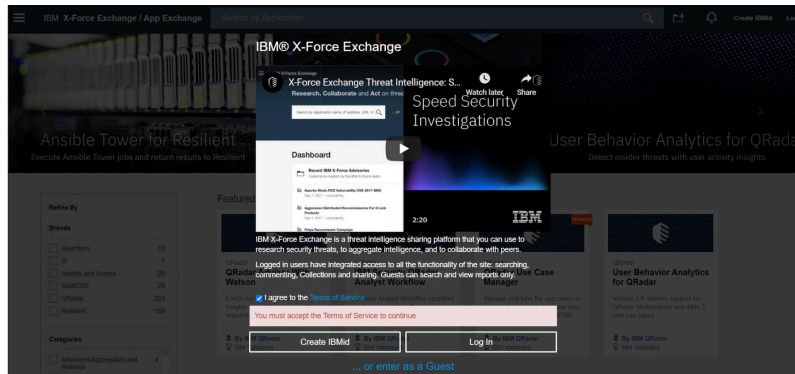
The backup needs to be copied to the remote server before re-imaging the appliance.

Install an Application on JSA

To install an application on JSA: log in to the IBM App Exchange Site to download the desired app, as shown in Figure 369.

Figure 369

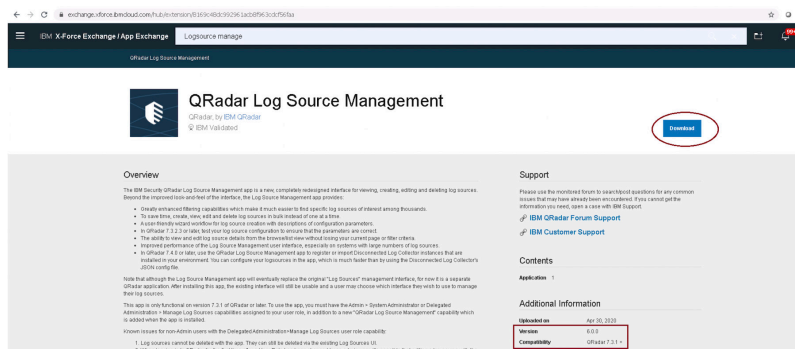
IBM App Exchange Login



Search for the desired application and download the application file to your local system, as shown in Figure 370.

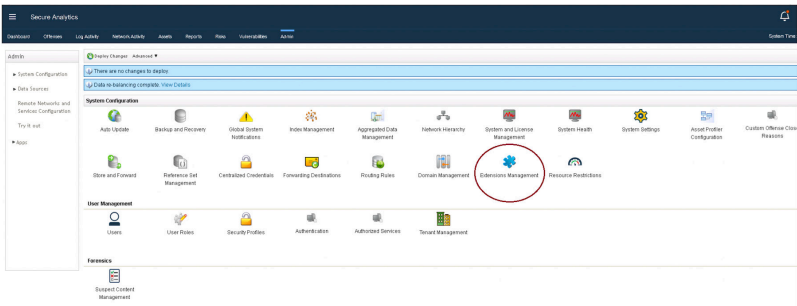
Figure 370

Application File Download Site



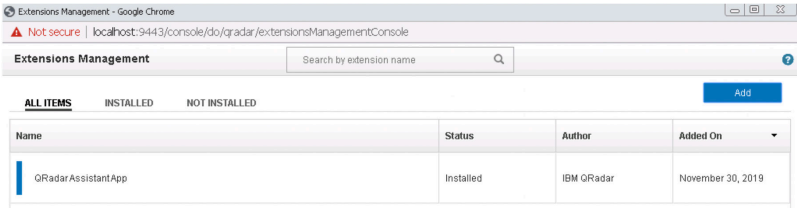
Ensure the application version is compatible with the JSA version. Now, log in to the JSA web UI and from the Admin Tab, click Extensions Management, as shown in Figure 371.

Figure 371 JSA Admin Tab



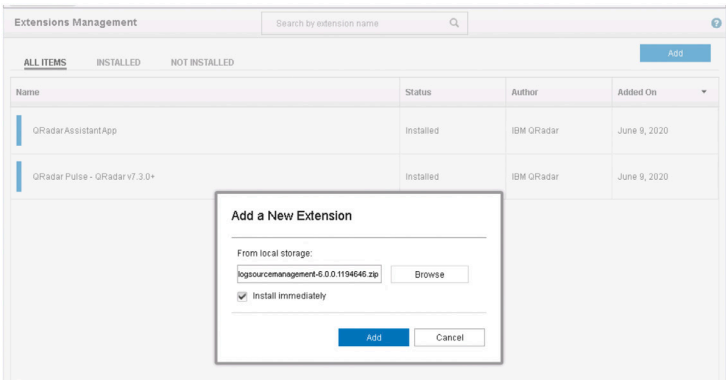
The Extension Management page appears. Click Add to select the application that you have downloaded earlier from the IBM App Exchange, as shown in Figure 372.

Figure 372 Extensions Management Page



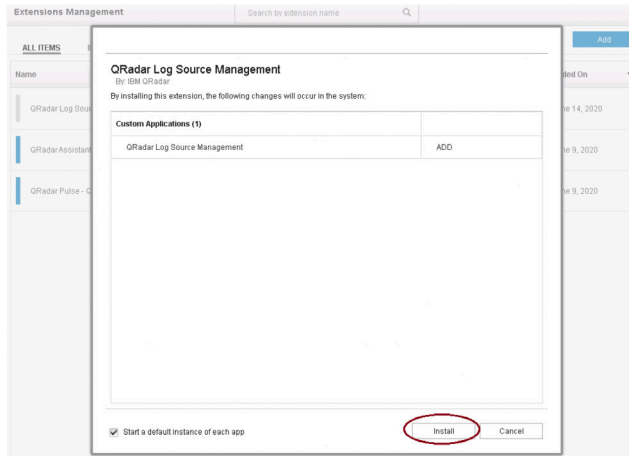
In the Add a New Extension page, click Browse to select the app file that you have downloaded and saved in your local system, as shown in Figure 373.

Figure 373 Add a New Extension Page



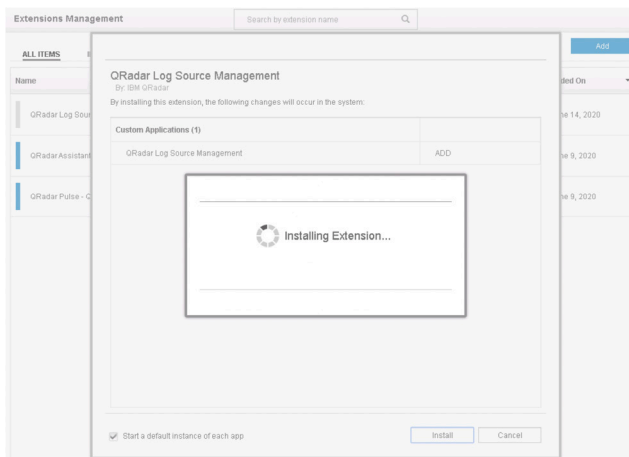
Click Add and the QRadar Log Source Management page appears (Figure 374).

Figure 374 *QRadar Log Source Management Page*



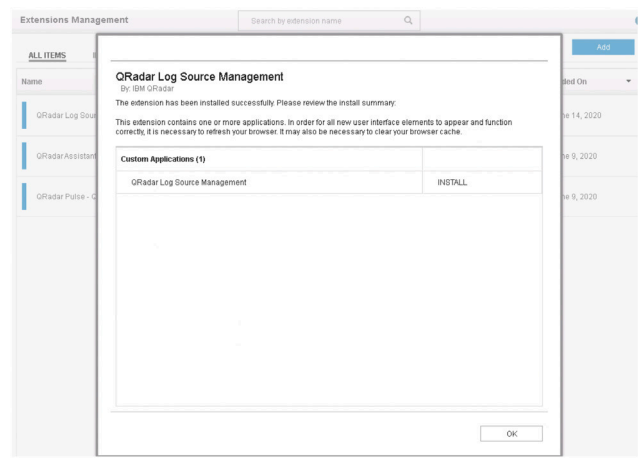
Click Install to install the application. The installation progress window appears, as shown in Figure 375.

Figure 375 *Installation Progress Message*



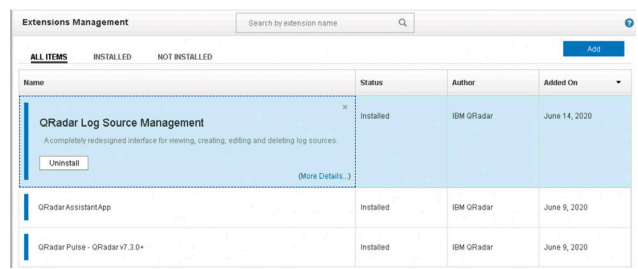
Once the application installation is complete, a confirmation message appears, as shown in Figure 376.

Figure 376 *Installation Complete Message*



Click OK and the installed application is now listed in the Extensions Management page, as shown in Figure 377.

Figure 377 *Installed Application in the Extensions Management Page*

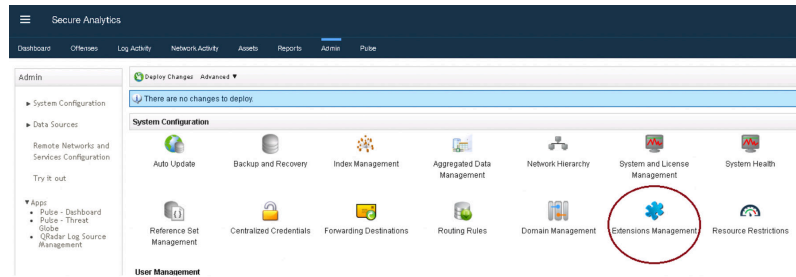


Upgrade an Existing Application on JSA

Before upgrading the application, you must first download the latest version of the application from the IBM App Exchange and save it to your local system.

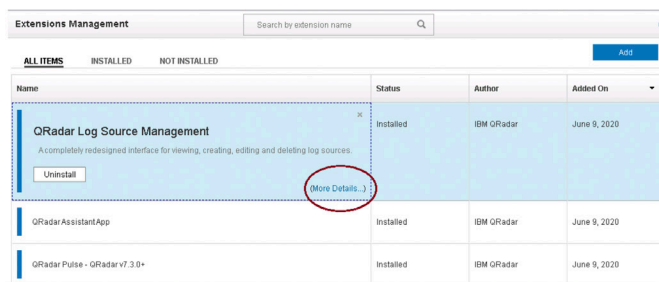
To upgrade an application on JSA, log in to the JSA web UI and from the Admin tab and select Extensions Management, as shown in Figure 378.

Figure 378 JSA Admin Tab



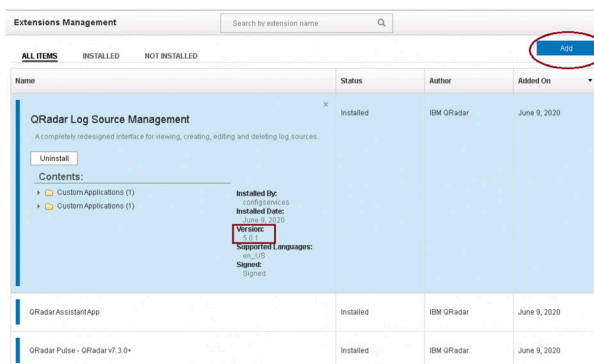
The Extensions Management page will open (Figure 379). Select the application that you want to upgrade and click More Details to verify the current version of the application.

Figure 379 Extensions Management Page



The More Details option provides version number and additional information, as shown in Figure 380.

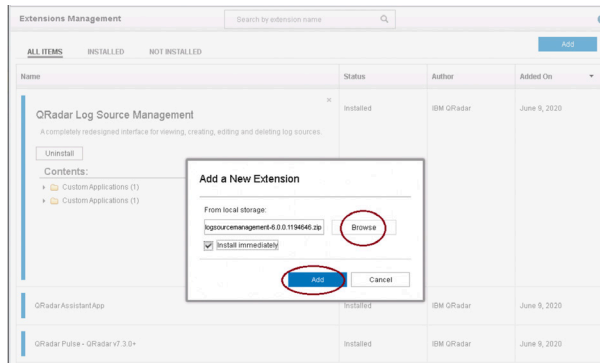
Figure 380 QRadar Log Source Management More Details



In this example, we are upgrading the QRadar Log Source Management application from the current 5.0.1 version to the latest 6.0.0 version.

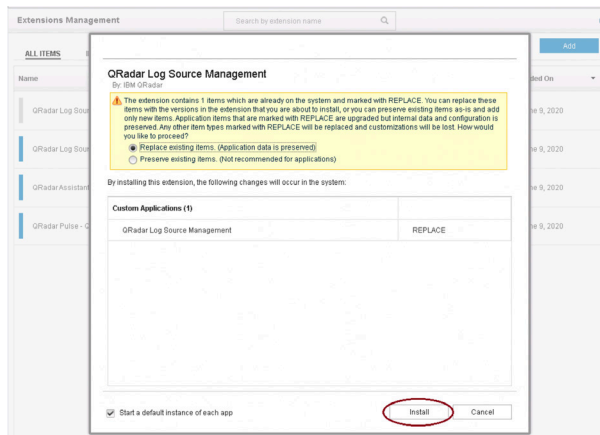
Click Add. The Add New Extension page appears. Click Browse and select the latest downloaded application version from the local system, as shown in Figure 381.

Figure 381 Add a New Extension Page



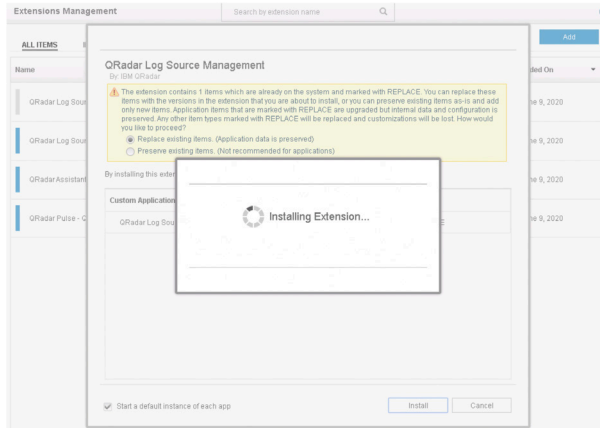
Click Add. The QRadar Log Source Management page appears, as shown in Figure 382.

Figure 382 QRadar Log Source Management Install Page



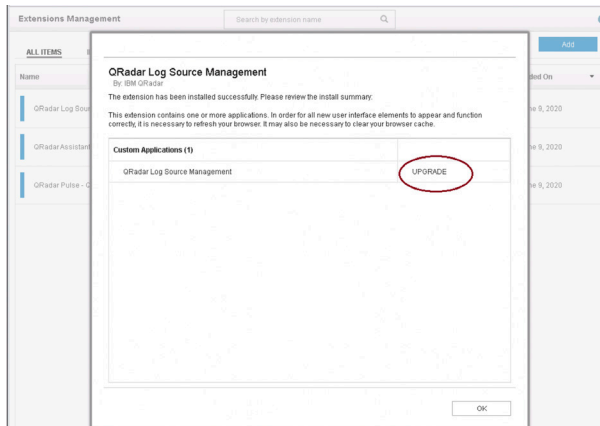
Click Install. The progress window appears, as shown in Figure 383.

Figure 383 Installation Progress Message



Once the upgrade is successful, a confirmation message appears, as shown in Figure 384.

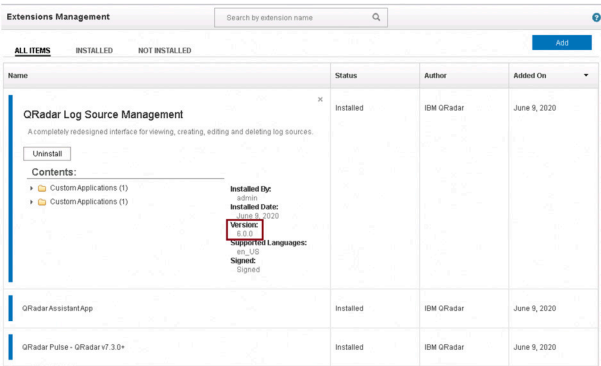
Figure 384 Application Upgrade Complete



Click Ok.

The application is successfully upgraded to 6.0.0 version. In the Extensions Management page, select the upgraded application, and click More Details. The Version field should show the upgraded version, as shown in Figure 385.

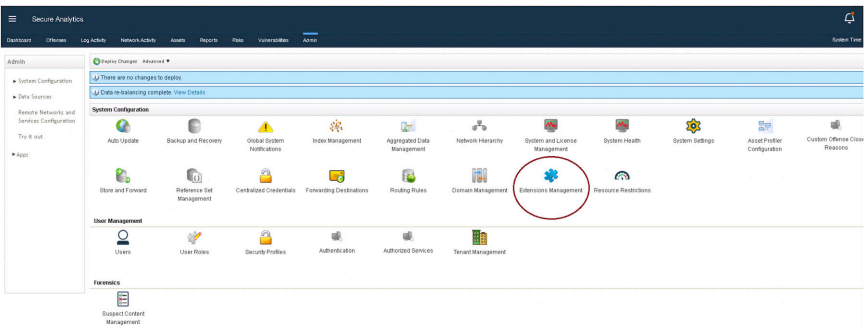
Figure 385 Extensions Management Page



Delete an Application from JSA

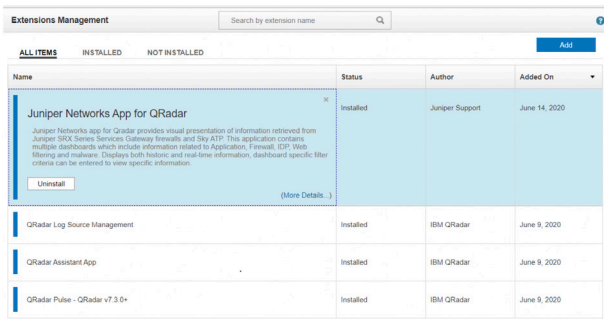
To delete an application from JSA, log in to the JSA web UI and from the Admin tab, select Extensions Management, as shown in Figure 386.

Figure 386 JSA Admin Tab



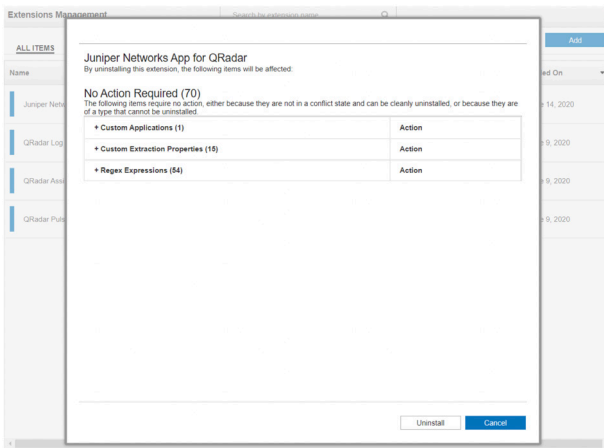
The Extensions Management page appears. Select the application that you want to delete, as shown in Figure 387.

Figure 387 Extensions Management Page



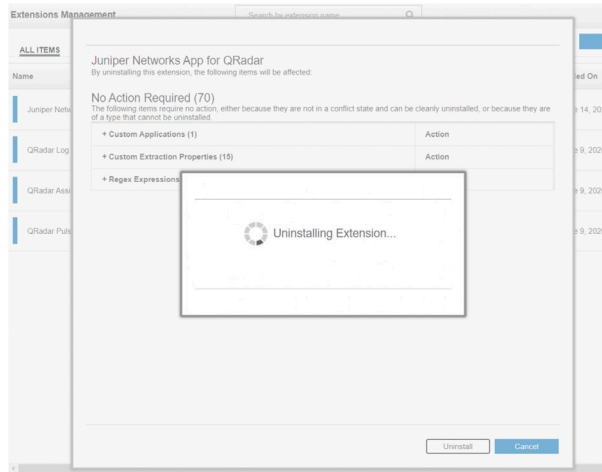
Click Uninstall. The Juniper Networks App for QRadar page appears listing all affected items, as shown in Figure 388.

Figure 388 Application Uninstall Page



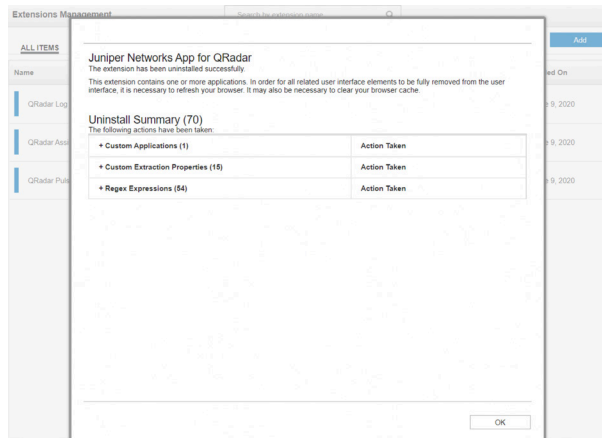
Click Uninstall. A progress message appears, as shown in Figure 389.

Figure 389 Application Uninstall Progress Page



Once the uninstall is complete, a summary page appears, as shown in Figure 390.

Figure 390 Application Uninstall Summary Page

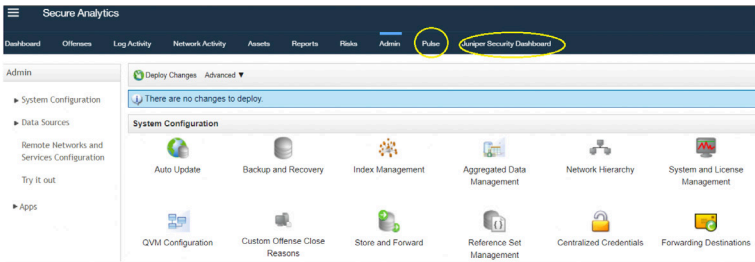


Click OK. The uninstalled application will not appear in the Extensions Management page any longer.

View Applications on JSA

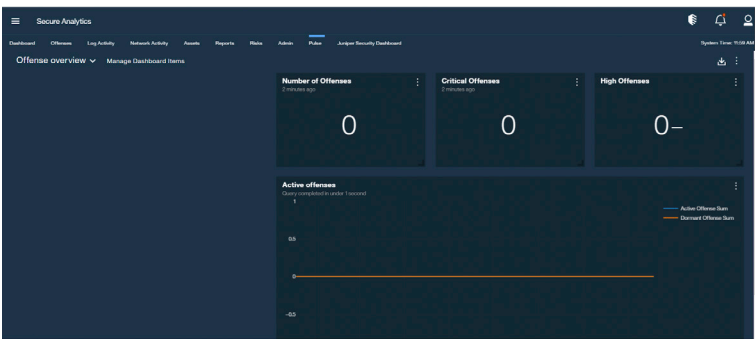
You can see the installed applications on JSA as tabs in the JSA web UI, as shown in Figure 391.

Figure 391 JSA Web UI



In this example, you can see the Pulse and Juniper Security Dashboard applications. You can click the application tab to see more information about the application, as shown in Figure 392.

Figure 392 Pulse Application Details



To view the list of all applications installed on JSA, go to Admin>Extensions Management. All applications are listed, as shown in Figure 393.

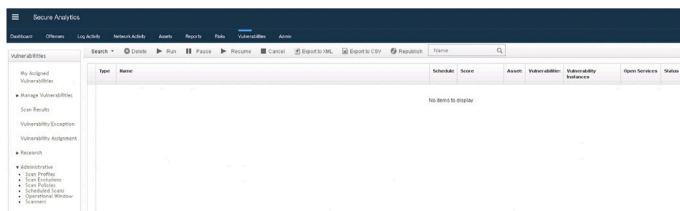
Figure 393 Extensions Management Page

Extensions Management				
Search by extension name				
ALL ITEMS INSTALLED NOT INSTALLED Add				
Name	Status	Author	Added On	
Juniper Networks App for QRadar	Installed	Juniper Support	June 14, 2020	
QRadar Log Source Management	Installed	IBM QRadar	June 9, 2020	
QRadar Assistant App	Installed	IBM QRadar	June 9, 2020	
QRadar Pulse - QRadar v7.3.0+	Installed	IBM QRadar	June 9, 2020	

Trigger a Vulnerability Scan

You must apply the Vulnerability Manager license to JSA to enable this feature. There can be only one vulnerability processor (VP) in a single deployment. This can either be the console or a dedicated VP hardware or a virtual appliance. There can be multiple vulnerability scanners (VS) in a single JSA deployment and any managed host or console itself can act as a VS. If required, you can have a dedicated VS hardware or a virtual appliance as well. To configure JSA to trigger a vulnerability scan, log in to the JSA web UI and select the Vulnerabilities tab, as shown in Figure 394.

Figure 394 JSA Vulnerability Tab



Select Scan Policies from the left pane to view the policy that you want to use, as shown in Figure 395.

Figure 395 Scan Policies Option

Name	Description	Enabled	Share With Everyone	Scan Type
Web Scan	Scans ports 20, 80, 443, 8080, and 8081 to detect web vulnerabilities and checks for cross-site scripting, file inclusion, weak crypto, and other web-related CVEs. The application scanning is performed on assets where a web application is installed.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Zero-credentialed
PD Scan	This scan performs a scan against the PD compliance. This scan performs a full scan against host IP ranges in the 10.0.0.0/8 and 172.16.0.0/12 ranges.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Full scan
Host Scan	Enables the ability to discover assets that perform a full scan and credentialed scan of the assets.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Partial scan
Full Scan	Discovers network assets using a full scan port range. Performs a scan credentialed and scan without credentialed scan.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Full scan
Discovery Scan	Discovers network assets that perform asset scan to identify live and down assets, including operating system, services, and ports that are provided by the asset. No vulnerability scanning is performed.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Discovery Scan
Database Scan	Scans ports 422, 1433, 1521, and 3306 to identify popular database services like MSSQL, Oracle, IBM DB2, and MySQL. Database operations are subject to the same user settings and email configurations. Vulnerability scanning is performed on assets where a database is installed.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Zero-credentialed

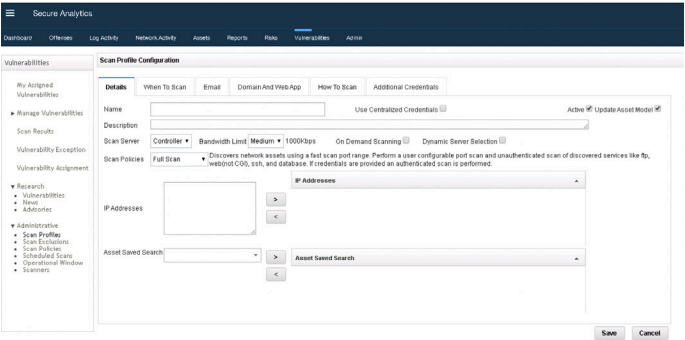
Select Scan Profiles from the left pane, as shown in Figure 396.

Figure 396 Scan Profiles Option

Type	Name	Scanner	Schedule	Status	Progress
<input checked="" type="checkbox"/>	CS Benchmark Profile - Weekly	Controller	Weekly	Not Started	0%
<input checked="" type="checkbox"/>	CS Benchmark Profile - RunOnce	Controller	RunOnce	Not Started	0%
<input checked="" type="checkbox"/>	CS Benchmark Profile - Monthly	Controller	Monthly	Not Started	0%
<input checked="" type="checkbox"/>	CS Benchmark Profile - Daily	Controller	Daily	Not Started	0%

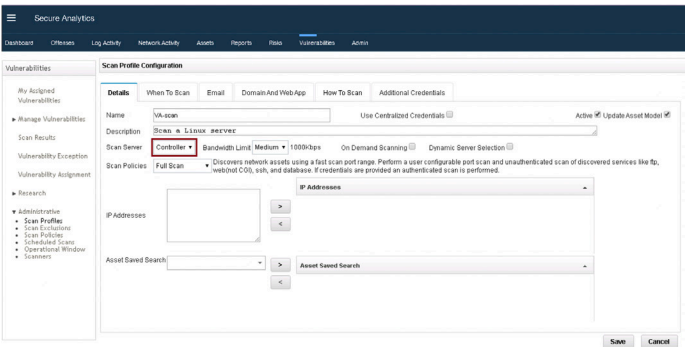
Click Add. The Scan Profile Configuration page appears, as shown in Figure 397.

Figure 397 Scan Profile Configuration Page



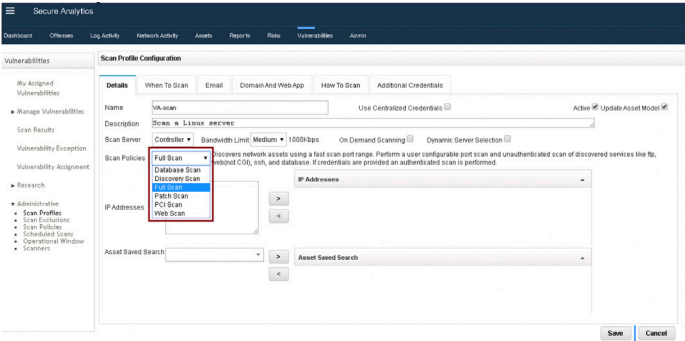
In the Name field, enter a name of the scan profile. In the description field, enter a description. In the Scan Server field, select the required scan server from the list. By default, the Controller/Console option is selected, as shown in Figure 398.

Figure 398 Scan Profile Configuration Page



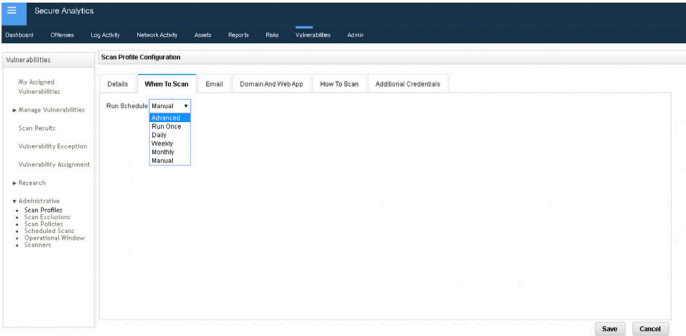
Select the type of scan from the Scan Policies drop-down list, shown in Figure 399.

Figure 399 Scan Profile Configuration Page



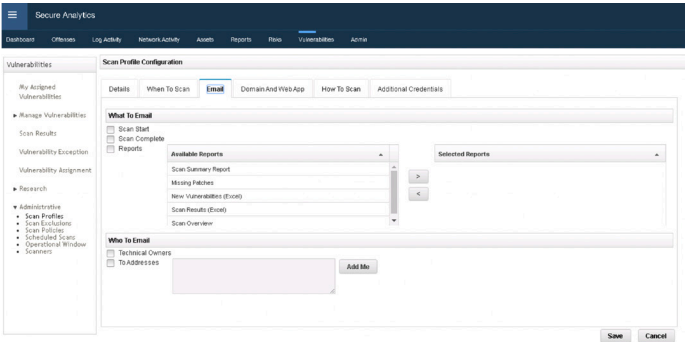
In the When to Scan tab, select the required scan interval from the Run Schedule drop-down list, as shown in Figure 400.

Figure 400 Scan Profile Configuration Page-When to Scan Tab



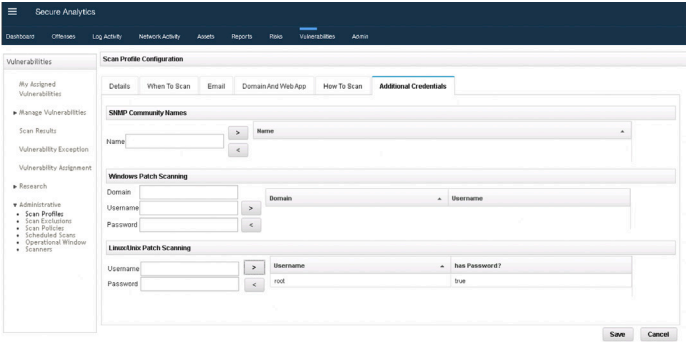
(Optional) in the Email tab, provide Email details, as shown in Figure 401. VA scan reports are emailed to given email ID once the scan is completed.

Figure 401 Scan Profile Configuration Page-Email Tab



In the Additional Credentials tab, provide credentials of the target server to be scanned, as shown in Figure 402.

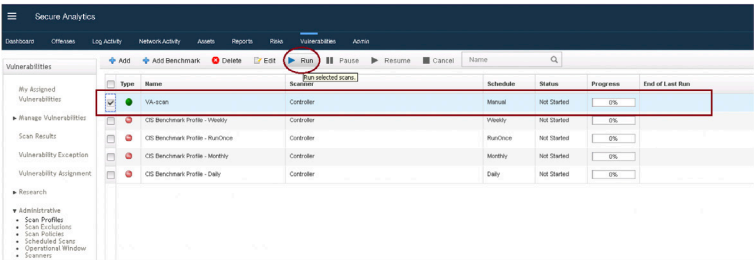
Figure 402 Scan Profile Configuration Page-Additional Credentials Tab



Click Save. The Scan Profile is listed in the Scan Profiles page, as shown in Figure 403.

Figure 403

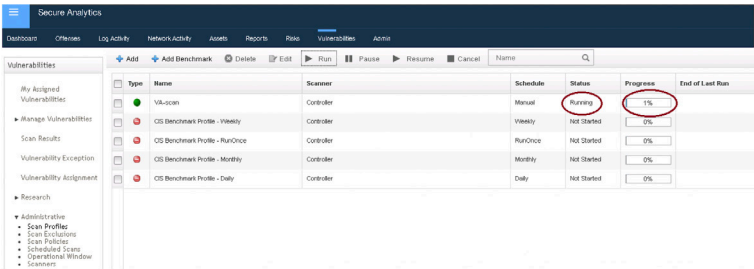
Scan Profiles Page



Select the scan profile and click Run. Verify the scan status and progress details, as shown in Figure 404.

Figure 404

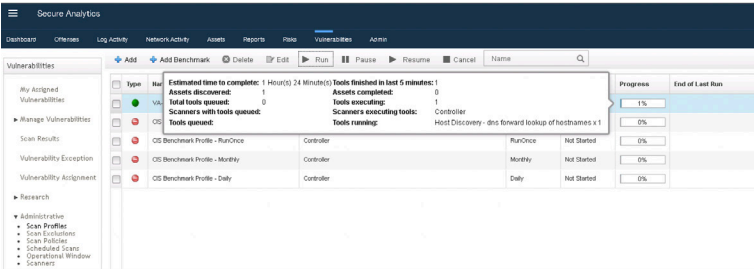
Scan Profile Running



Hover the mouse over the progress bar to see the real-time scan status and details, as shown in Figure 405.

Figure 405

Scan Profile Progress Details



Once the scan is complete, you can see the scan results, as shown in Figure 406.

Figure 406

Scan Results

The screenshot shows the 'Secure Analytics' dashboard. On the left, there's a sidebar with navigation options: 'My Assigned Vulnerabilities', 'Manage Vulnerabilities', 'Scan Results', 'Vulnerability Assignment', 'Research', and 'Administration'. The main area displays a table of scan results for an asset named 'VM-001'. The table has columns for 'Name', 'Status', 'Score', 'Assess', 'Vulnerability Instance', 'Open Services', 'Status', 'Progress', 'Start Date/Time', and 'End'. The 'Status' column shows a red circle around the word 'High', indicating a high-risk vulnerability.

Click on the Vulnerabilities field to see all the vulnerabilities, shown in Figure 407.

Figure 407

List of Vulnerabilities

The screenshot shows the 'Secure Analytics' dashboard with the 'Vulnerabilities' tab selected. It displays a table of vulnerabilities for the asset 'VM-001'. The table has columns for 'Risk', 'PCI Severity', 'Vulnerability', 'Assets', and 'Instances'. The 'Risk' column shows 'High' for all entries. The 'PCI Severity' column shows 'High' for all entries. The 'Vulnerability' column lists various CVEs and their descriptions. The 'Assets' column shows 'VM-001' for all entries. The 'Instances' column shows '1' for all entries.

All vulnerabilities are listed here. Click on any specific vulnerability to see details and the Scan Results page for the selected vulnerability appears (Figure 408).

Figure 408

Selected Vulnerability Details

The screenshot shows the 'Secure Analytics' dashboard with the 'Vulnerability Details' tab selected for the vulnerability 'CVE-2017-0226 - Sublinenap - Security Review Issue'. The table displays details for this vulnerability, including its name, assets, and instances. The 'Assets' column shows 'VM-001' and 'VM-002'. The 'Instances' column shows '1' for 'VM-001' and '2' for 'VM-002'. The table also includes a 'Vulnerability Details' section with fields for 'Vulnerability ID', 'Published Date', 'Name', 'Asset Name', 'IP Address', 'Domain', 'CVSS Base Score', 'CVSS Temporal Score', 'CVSS Base Metrics', 'CVSS Temporal Metrics', 'Vulnerability Impact', 'Description', 'Comments', and 'Status'.

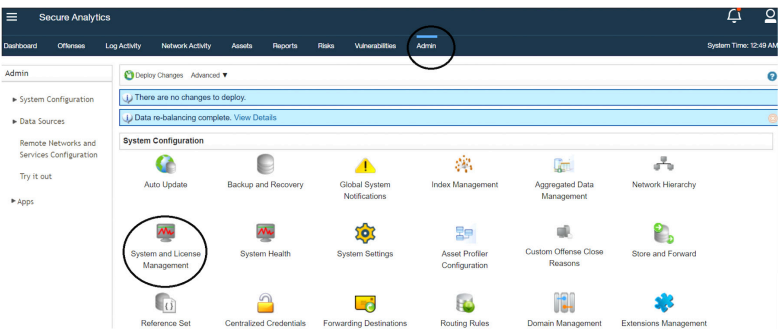
You can download or export this report in XML or CSV format. If you have configured your email ID, the report will be sent to your email ID.

Restart a Managed Host from JSA Web UI

At times, you might have to restart the managed host or console as a part of troubleshooting or planned maintenance.

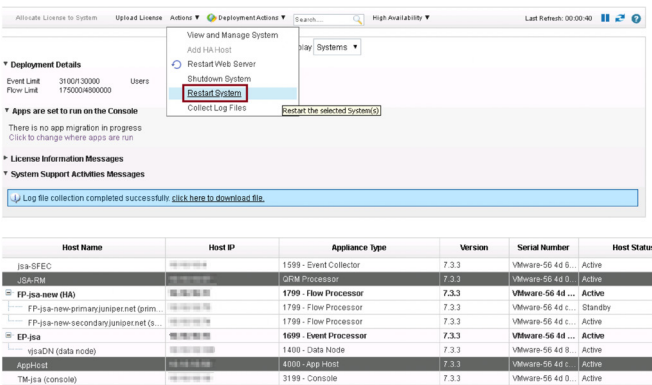
To initiate the managed host restart process from UI, log in to the JSA web UI and select Admin > System and License Management, as shown in Figure 409.

Figure 409 JSA Admin Tab



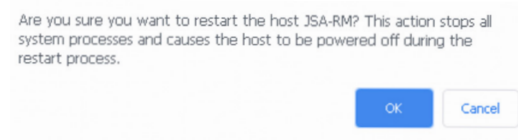
Select the host that you want to restart. You can select a single host or multiple hosts for restart. From the Actions menu, select Restart System, as shown in Figure 410.

Figure 410 Restart System Option



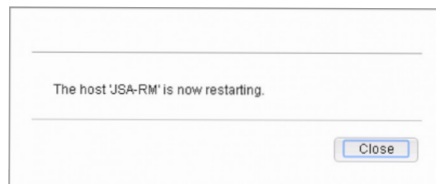
A confirmation message to restart the selected host is shown in Figure 411.

Figure 411 Restart Confirm Message



Click OK. The restart process begins, as shown in Figure 412.

Figure 412 Restart Progress Message



Click Close. The Host Status shows as Restarting, as shown in Figure 413.

Figure 413 Host Restarting Status

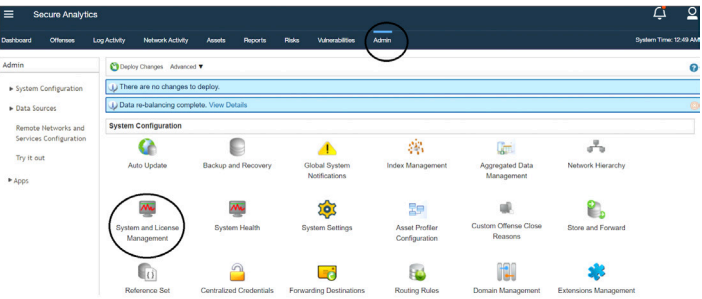
Allocate License to System Upload License Actions Deployment Actions Search... High Availability Last Refresh: 00:00:05 [Refresh] [Help]					
Display Systems					
Deployment Details Event Limit: 3100/30000 Users: 1 Flow Limit: 175000/4800000					
License Information Messages System Support Activities Messages Log file collection completed successfully click here to download file.					
Host Name	Host IP	Appliance Type	Version	Serial Number	Host Status
JSA-VS	192.168.1.101	610 - QVM Scanner	7.3.3	VMware-56 4d c...	Active
JSA-VP	192.168.1.102	600 - QVM Processor	7.3.3	VMware-56 4d 5...	Active
JSA-SFEC	192.168.1.103	1599 - Event Collector	7.3.3	VMware-56 4d 6...	Active
JSA-RM	192.168.1.104	QRM Processor	7.3.3	VMware-56 4d 0...	Restarting
FP-JSA-new (HA)	192.168.1.105	1799 - Flow Processor	7.3.3	VMware-56 4d ...	Active
[Filter] [Refresh] [Export] [Import] [Help]					

Restart a Web Server from JSA Web UI

At times, you might have to restart the web servers (tomcat and httpd service) as a part of troubleshooting or planned maintenance during a maintenance window.

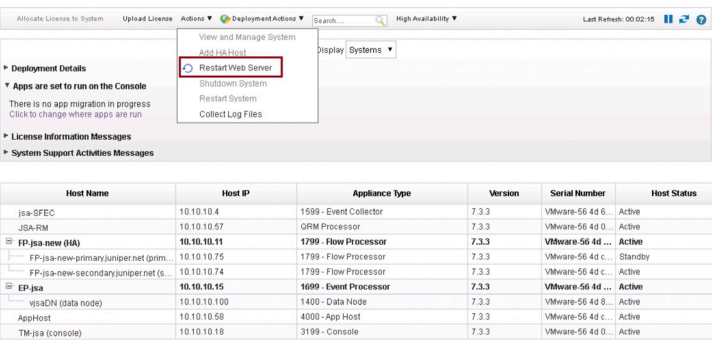
To initiate the restart process of web servers from UI, log in to the JSA web UI and select Admin > System and License Management, as shown in Figure 414.

Figure 414 JSA Admin Tab



From the Actions menu, select Restart Web Server, as shown in Figure 415.

Figure 415 Restart Web Server Option



A confirmation message appears to restart the selected host, as shown in Figure 416.

Figure 416 Web Server Restart Confirmation Message

Are you sure you want to restart the web server? This will cause an interruption of the user interface. During the restart, data collection will continue. When the web server has restarted you will see a "The connection with the Console has restored" message.

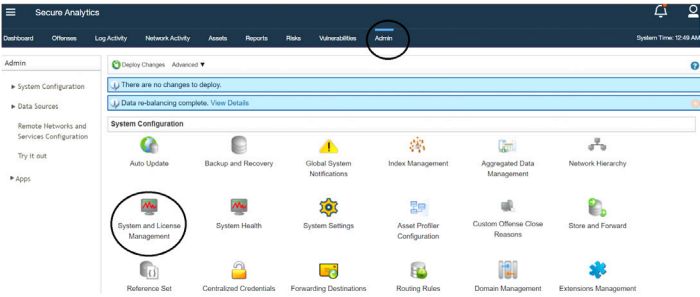


Click OK to proceed with the restart.

Configure or Change the SMTP Server on JSA

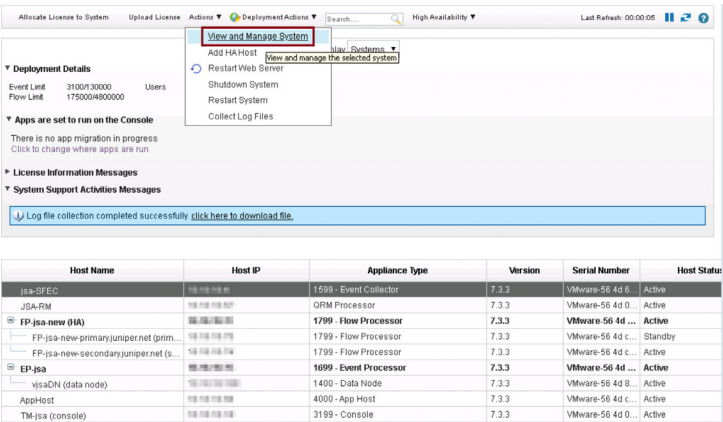
To configure or change the SMTP server on JSA, log in to the JSA web UI and select Admin > System and License Management, as shown in Figure 417.

Figure 417 JSA Admin Tab



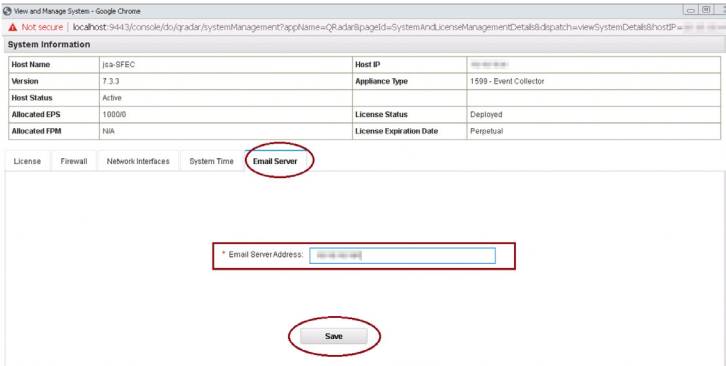
Select the host on which you want to configure the SMTP server and select Actions > View and Manage System, as shown in Figure 418.

Figure 418 View and Manage System Option



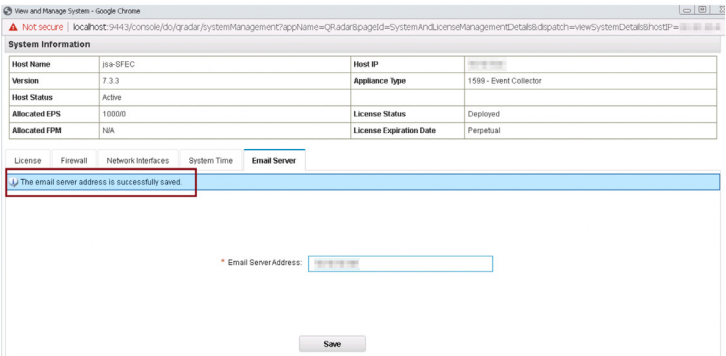
In the View and Manage System page, click the Email Server tab and Enter the email server address, as shown in Figure 419.

Figure 419 Email Server Tab



Click Save.
The email server address is successfully configured, as shown in Figure 420.

Figure 420 Email Server Configured Successfully

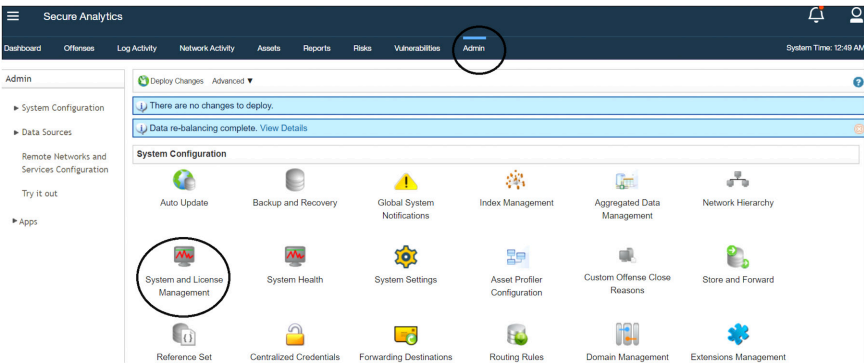


Configure or Change an NTP Server

You can configure NTP server only in the Threat Analytics (TA) or Log Analytics (LA) console.

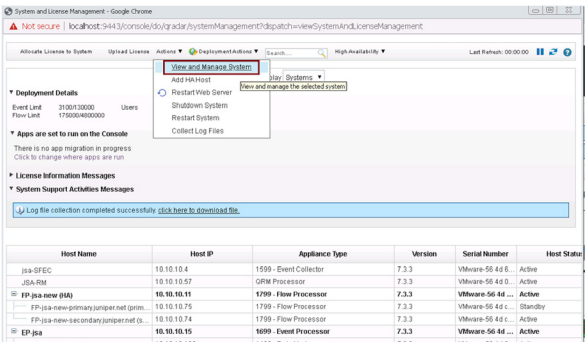
To configure or change the NTP server in JSA, log in to the JSA web UI and select Admin > System and License Management, as shown in Figure 421.

Figure 421 JSA Admin Tab



Select the host where you need to configure the NTP server and select Actions > View and Manage System, as shown in Figure 422.

Figure 422 View and Manage System Option



In the View and Manage System page, click the System Time tab to specify the NTP server details, as shown in Figure 423.

Figure 423 System Time Tab

View and Manage System - Google Chrome

Not secure | localhost:9443/console/50/qg/adar/systemManagement?appName=Q&adarPageId=SystemAndLicenseManagementDetails&dispatch=viewSystem

System Information

Host Name	TM-isa (console)	Host IP	10.10.10.10
Version	7.3.3	Appliance Type	3199 - Console
Host Status	Active		
Allocated EPS	500/20000	License Status	Deployed
Allocated FPM	25000/120000	License Expiration Date	Aug 10, 2020

Security Data Distribution

License

Firewall

Network Interfaces

System Time

Email Server

Time Zone:

UTC-04:00:America/New York

Set time manually:

Date: 6/7/2020

Time: 8:23 AM

Specify NTP servers:

Add four or more NTP servers to get the most accurate time.

ip: Add NTP...

Save

Select the Specify NTP servers option and provide the server details, as shown in Figure 424.

Figure 424 NTP Server Details

View and Manage System - Google Chrome

Not secure | localhost:9443/console/50/qg/adar/systemManagement?appName=Q&adarPageId=SystemAndLicenseManagementDetails&dispatch=viewSystem

System Information

Host Name	TM-isa (console)	Host IP	10.10.10.10
Version	7.3.3	Appliance Type	3199 - Console
Host Status	Active		
Allocated EPS	500/20000	License Status	Deployed
Allocated FPM	25000/120000	License Expiration Date	Aug 10, 2020

Security Data Distribution

License

Firewall

Network Interfaces

System Time

Email Server

Time Zone:

UTC-04:00:America/New York

Set time manually:

Date: 6/7/2020

Time: 8:23 AM

Specify NTP servers:

Add four or more NTP servers to get the most accurate time.

Server 1 Address: 10.10.10.10

ip: Add NTP...

Save

Click Save. Services are restarted as a part of NTP server confirmation. Click OK to proceed, as shown in Figure 425.

Figure 425 NTP Server Change Confirmation Message

System Information

Host Name	TM-isa (console)	Host IP	10.10.10.10
Version	7.3.3	Appliance Type	3199 - Console
Host Status	Active		
Allocated EPS	500/20000	License Status	Deployed
Allocated FPM	25000/120000	License Expiration Date	Aug 10, 2020

Security Data Distribution

License

Firewall

Network Interfaces

System Time

Email Server

Time Zone:

UTC-04:00:America/New York

Services are restarted when you change the time setting, which interrupts data collection and causes the user interface to be unavailable for several minutes. Are you sure that you want to change the system time?

OK

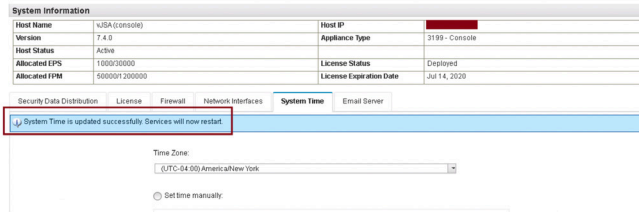
Cancel

Specify NTP servers:

Add four or more NTP servers to get the most accurate time.

The system time gets updated successfully, as shown in Figure 426.

Figure 426 System Time Updated Successfully

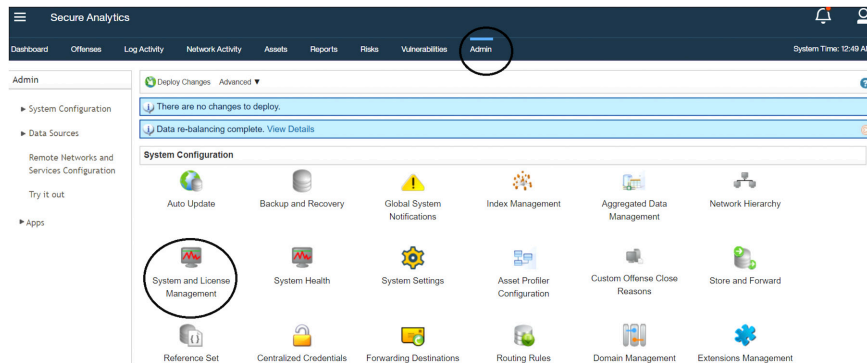


Configure or Change Time Zone

You can configure or change the time zone only on Threat Analytics (TA) or Log Analytics (LA) console and as well as on the managed hosts.

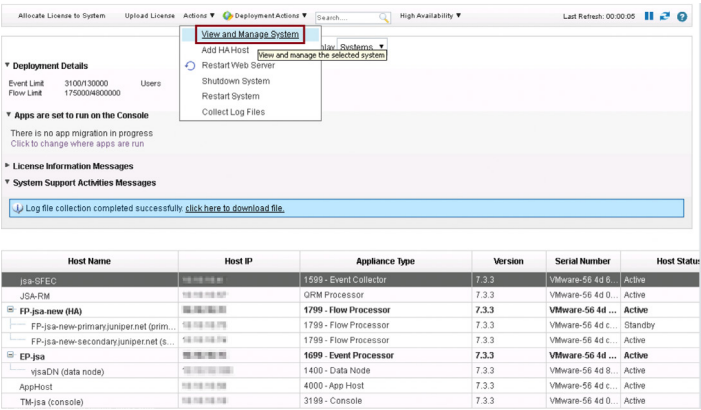
To configure the time zone, login to the JSA web UI and select Admin > System and License Management, as shown in Figure 427.

Figure 427 JSA Admin Tab



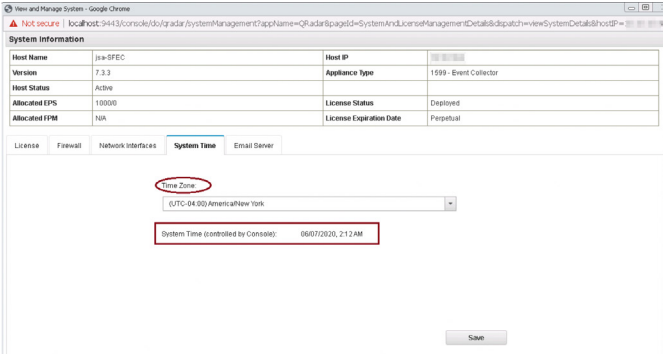
Select the host on which you want to configure the time zone and select Actions > View and Manage System, as shown in Figure 428.

Figure 428 View and Manage System Option



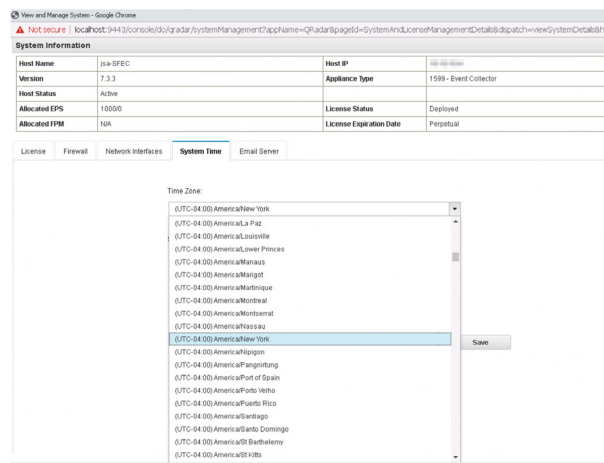
In the View and Manage System page, click the System Time tab to specify the time zone details, as shown in Figure 429.

Figure 429 System Time Tab



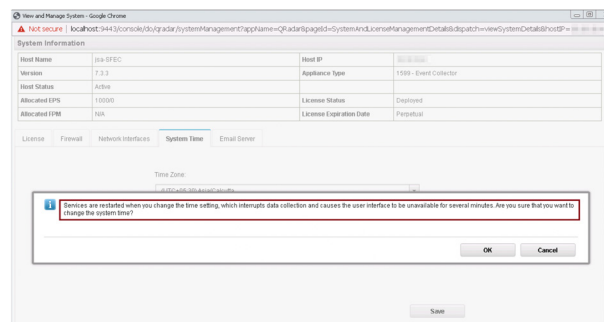
Select the required time zone and click Save, as shown in Figure 430.

Figure 430 Time Zone List



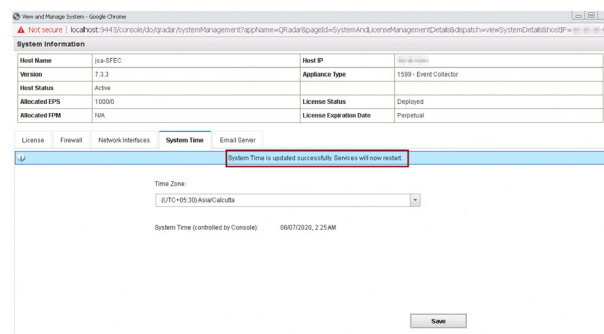
Services are restarted as a part of the time zone change. Click OK to proceed, as shown in Figure 431.

Figure 431 Time Zone Modification Confirmation



The time zone is successfully configured, as shown in Figure 432.

Figure 432 Time Zone Modified Successfully



Add a Log Source to Collect Events from an SRX Series Device

You can configure a log source to send events to JSA. Log sources are devices from which events are sent to (or pulled by) JSA. Events can be periodically pulled from devices, or devices can be configured to send events to JSA. Once the logs are sent to JSA, the logs are parsed and then stored in JSA. Based on your predefined correlation rules, appropriate actions are taken when specific events happen.

For example, you can configure JSA to send an email alert when an event is seen with the source or destination IP address as a BotNet IP. The example here provides the high-level steps that you can use to configure event collection from an SRX Series device.

NOTE For SRX specific configuration, see Juniper Networks KB 16224 and KB 29539).

You configure an SRX Series device to send syslog events to JSA by adding appropriate commands in the SRX CLI. First check if JSA is receiving events from log sources:

- You can use the `tcpdump` utility to verify this on JSA interfaces.
- If your deployment is all-in-one TM or LM, run `tcpdump` on the console.
- If the deployment is distributed across various event processors or collectors, run `tcpdump` on event processors or collectors where events are being sent by SRX.
- Make sure that the ECS service is running on the JSA host which is collecting the SRX events.

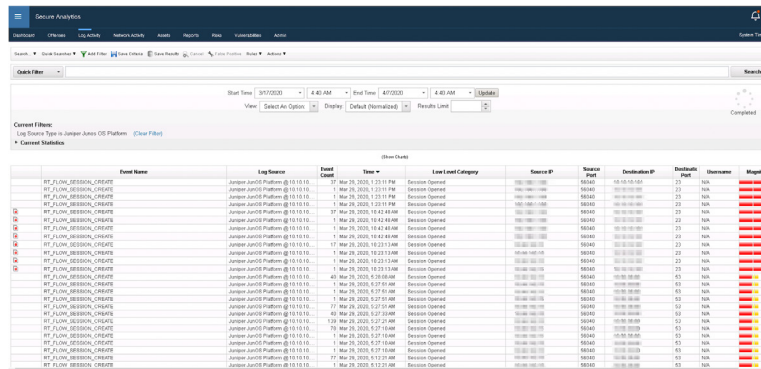
Figure 433 shows how you can verify SRX events reaching the JSA interface using `tcpdump`.

Figure 433 Example SRX Device

```
[root@primary-primary ~]# tcpdump -i eth0 host 10.10.10.10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

After you verify that events are reaching the JSA interface using `tcpdump`, you can use the JSA web UI to check the SRX logs (Figure 434).

Figure 434 SRX Logs



To parse the events correctly, use the latest DSM / RPMs for the log source. DSM has the necessary logic for JSA to understand the events in the syslog collected from the log sources. DSMs are delivered manually or through auto-updates. For an SRX Series device, use Junos DSM. Use the following command to verify whether you have the latest DSM.

Figure 435 Verify DSM Version

```
[root@jsa-testx /]# rpm -qa | grep -i junos |grep -i dsm
DSM-JuniperJunos-7.3-20180110134923.noarch
[root@jsa-testx /]#
```

You don't have to create a log source manually from the JSA web UI. Log source auto-discovery creates a log source automatically. JSA inspects the first few events and identifies the event type or the device type and creates a log source. You can disable this feature if you want to manually control the creation of log sources.

Install and Upgrade DSM/Protocols

You can install and update DSM/PROTOCOLS using the following commands:

```
rpm -ivh <DSM RPM>
```

```
rpm -Uvh <DSM RPM>
```

NOTE DSMs / PROTOCOLs can be installed or upgraded only on consoles, not on managed hosts. In cases of a high availability installation, you must install DSM/PROTOCOL on the active servers. After installing or upgrading the DSM/PROTOCOL, you must deploy the changes so that the resulting .jar files are pushed to the managed hosts.

NOTE Download and copy the DSM/PROTOCOL locally before installing or upgrading RPM.

To upgrade a DSM/PROTOCOL, check the current version of DSM / PROTOCOL installed on the console using the `rpm -qa` command.

Figure 436 Check DSM Version

```
[root@TM-jsa ~]#
[root@TM-jsa ~]# rpm -qa | grep -i DSM-JuniperJunOS
DSM-JuniperJunOS-7.3-20170622121822.noarch
[root@TM-jsa ~]#
```

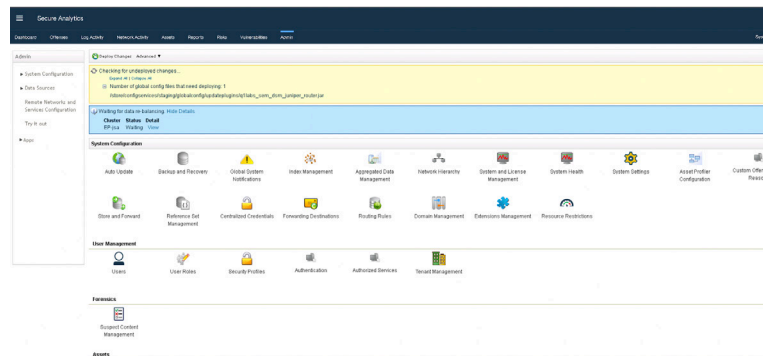
Use the `rpm -Uvh <DSM RPM>` to upgrade the DSM.

Figure 437 Upgrade DSM

```
[root@TM-jsa ~]# rpm -Uvh DSM-JuniperJunOS-7.3-20180515163707.noarch.rpm
Preparing... ##### [100%]
Installing 'DSM-JuniperJunOS-7.3.20180515163707'.
Updating / installing:
  1:DSM-JuniperJunOS-7.3-201805151637##### [ 50%]
Found 6 QIDMAP data files to apply. (one '#' per file)
Currently importing /store/tmp/73/JuniperJunOS/1327508559471.qidmap-import.xml (
Currently importing /store/tmp/73/JuniperJunOS/1484056493004.qidmap-import.xml (
Currently importing /store/tmp/73/JuniperJunOS/1484064061357.qidmap-import.xml (
Currently importing /store/tmp/73/JuniperJunOS/1522350994008.qidmap-import.xml (
Currently importing /store/tmp/73/JuniperJunOS/1522353482297.qidmap-import.xml (
Currently importing /store/tmp/73/JuniperJunOS/1526320606265.qidmap-import.xml (
file 6 of 6 to import)
All 6 import file(s) successfully imported.
Compressing QidMap file /store/tmp/73/JuniperJunOS/1327508559471.qidmap-import.xml...
Compressing QidMap file /store/tmp/73/JuniperJunOS/1484056493004.qidmap-import.xml...
Compressing QidMap file /store/tmp/73/JuniperJunOS/1484064061357.qidmap-import.xml...
Compressing QidMap file /store/tmp/73/JuniperJunOS/1522350994008.qidmap-import.xml...
Compressing QidMap file /store/tmp/73/JuniperJunOS/1522353482297.qidmap-import.xml...
Compressing QidMap file /store/tmp/73/JuniperJunOS/1526320606265.qidmap-import.xml...
Installed rpm DSM-JuniperJunOS-7.3.20180515163707
You must Deploy Changes to complete the DSM installation. After installation has completed
, navigate to the Admin tab in the user interface and click Deploy Changes
```

After you have installed or upgraded the DSM/PROTOCOL, to deploy the changes go to the JSA web UI. You will see the .jar file that needs to be deployed displayed on the screen. To deploy this file to the managed hosts, click Deploy Changes (Figure 438).

Figure 438 Deploy Changes



Chapter 4

JSA Hardware Use Cases

Before you use JSA hardware appliances, you should have a thorough understanding of the hardware specifications. This section explains how to determine all the important details about your JSA hardware modules, such as RAM, CPU, monitoring HDD/RAID health, and serial number.

Let’s start off with a summary of RAM, CPUs, HDDs, Storage Space, and RAID information for the JSA hardware models in Table 9.

Table 9 JSA Hardware Information

JSA Model	RAM	CPU	Storage Space	No of HDDs	No of HDDs	Maximum Events per sec (EPS)	Flows per minute (FPM)
JSA3800	64 GB	12	2.57 TB	6	RAID 10	5000	100,000
JSA5800	128 GB	40	3.27 TB	8	RAID 10	20,000	600,000
JSA7500	128 GB	32	11.44 TB	28	RAID 10	30,000	1.2 million
JSA7800	128 GB	40	25.46 TB	16	RAID 6	40,000	1.2 million

Monitor Health for JSA 3800

The Juniper Secure Analytics 3800 (JSA3800) is an enterprise-class appliance that provides a scalable network security management solution for medium-sized companies up to large global organizations.

Figure 439 JSA 3800 Front and Rear Views



The JSA3800 appliance is a 1-U, rack-mountable chassis with AC power supplies (or optional DC power supplies), six hot-swappable hard drives, 64 GB memory, and two 10 Gigabit and four Gigabit Ethernet interfaces.

Figure 440 JSA3800 RAM Details

```
[root@jtac-JSA3800-BSE-r002 ~]# free -m
```

	total	used	free	shared	buff/cache	available
Mem:	64233	3628	51675	2158	8929	57816
Swap:	24575	0	24575			

Figure 441 JSA3800 CPU Details

```
[root@jtac-JSA3800-BSE-r002 ~]# lscpu | more
```

```
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                12
On-line CPU(s) list:   0-11
Thread(s) per core:    2
Core(s) per socket:    6
Socket(s):             1
NUMA node(s):         1
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 62
Model name:            Intel(R) Xeon(R) CPU E5-2630 v2 @ 2.60GHz
Stepping:              4
CPU MHz:               2939.828
BogoMIPS:              5199.60
Virtualization:        VT-x
L1d cache:             32K
L1i cache:            32K
L2 cache:              256K
L3 cache:             15360K
NUMA node0 CPU(s):    0-11
```

The JSA3800 appliance ships with hot-swappable hard disks to offer component redundancy. The JSA3800 appliance uses the RAID10 configuration. In RAID10, drives are duplicated for fault tolerance. Monitor the JSA3800 RAID array with the following series of commands. To obtain the volume status, run `sas2ircu 0 status`, as shown in Figure 442.

Figure 442 JSA3800 Obtain Volume Status

```
[root@jtac-JSA3800-BSE-r002 ~]# sas2ircu 0 status
LSI Corporation SAS2 IR Configuration Utility.
Version 16.00.00.00 (2013.03.01)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

Background command progress status for controller 0...
IR Volume 1
  Volume ID           : 286
  Current operation    : None
  Volume status        : Enabled
  Volume state         : Optimal
  Volume wwid          : 0f830175d49f0389
  Physical disk I/Os   : Not quiesced
SAS2IRCU: Command STATUS Completed Successfully.
SAS2IRCU: Utility Completed Successfully.
```

The Volume state is shown as Optimal which indicates that RAID is healthy. If there are any faulty HDDs, the Volume state is displayed as Degraded.

To find out the faulty HDD, use the `sas2ircu 0 display` command. To obtain the device status, run `sas2ircu 0 display`, as shown in Figures 443 and 444.

Figure 443 JSA3800 Obtain Device Status

```
[root@jtac-JSA3800-BSE-r002 ~]# sas2ircu 0 display | more
LSI Corporation SAS2 IR Configuration Utility.
Version 16.00.00.00 (2013.03.01)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

Read configuration has been initiated for controller 0

-----
Controller information
-----
Controller type       : SAS2308 1
BIOS version          : 7.39.02.00
Firmware version      : 20.00.07.00
Channel description   : 1 Serial Attached SCSI
Initiator ID          : 0
Maximum physical devices : 255
Concurrent commands supported : 3072
Slot                  : 3
Segment               : 0
Bus                   : 5
Device                : 0
Function              : 0
RAID Support           : Yes
-----
```

Figure 444 JSA3800 Device Status Information

```
IR volume 1
  Volume ID           : 286
  Status of volume     : Okay (OKY)
  Volume wwid          : 0f830175d49f0389
  RAID level           : RAID10
  Size (in MB)         : 2572059
  Physical hard disks   :
  PHY[0] Enclosure#/Slot# : 1:0
  PHY[1] Enclosure#/Slot# : 1:1
  PHY[2] Enclosure#/Slot# : 1:2
  PHY[3] Enclosure#/Slot# : 1:3
  PHY[4] Enclosure#/Slot# : 1:4
  PHY[5] Enclosure#/Slot# : 1:5
-----
```

From the output, you can see that the JSA 3800 provides a total storage space of 2.5 TB and has a total of six physical HDDs.

Use the same `sas2ircu 0 display` command with different filters to see more HDD details, as shown in Figures 445 and 446, where if the State is Optimal it indicates that the physical HDDs are healthy.

Figure 445 JSA3800 Obtain HDD Details

```
[root@jtac-JSA3800-BSE-r002 ~]# sas2ircu 0 display | grep State
State      : Optimal (OPT)
State      : Optimal (OPT)
State      : Optimal (OPT)
State      : Optimal (OPT)
State      : Optimal (OPT)
State      : Optimal (OPT)
```

Figure 446 JSA3800 Obtain HDD Details

```
[root@jtac-JSA3800-BSE-r002 ~]# sas2ircu 0 display | grep "in sectors"
Size (in MB)/(in sectors) : 858483/1758174767
Size (in MB)/(in sectors) : 858483/1758174767
Size (in MB)/(in sectors) : 858483/1758174767
Size (in MB)/(in sectors) : 858483/1758174767
Size (in MB)/(in sectors) : 858483/1758174767
Size (in MB)/(in sectors) : 858483/1758174767
```

Monitor Health for JSA 5800

The Juniper Secure Analytics 5800 (JSA5800) is an enterprise and carrier-class appliance that provides a scalable network security management solution for medium-sized companies up to large global organizations.

Figure 447 JSA 5800



The JSA5800 appliance is a 2-U, rack-mountable chassis with AC power supplies (or optional DC power supplies), eight hot-swappable hard drives, 128 GB memory, and two 10 Gigabit and four Gigabit Ethernet interfaces.

Figure 448 JSA5800 RAM Details

```
[root@jsaEP-FP ~]# free -m
```

	total	used	free	shared	buff/cache	available
Mem:	128734	2283	118867	241	7584	125694
Swap:	24575	0	24575			

Figure 449 JSA5800 CPU Details

```
[root@jsaEP-FP ~]# lscpu | more
Architecture: x86_64
CPU op-mode(s): 32-bit, 64-bit
Byte Order: Little Endian
CPU(s): 40
On-line CPU(s) list: 0-39
Thread(s) per core: 2
Core(s) per socket: 10
Socket(s): 2
NUMA node(s): 2
Vendor ID: GenuineIntel
CPU family: 6
Model: 62
Model name: Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz
Stepping: 4
CPU MHz: 1251.489
CPU max MHz: 3600.0000
CPU min MHz: 1200.0000
```

JSA5800 appliance uses the RAID10 configuration. In RAID10, the drives are duplicated for fault tolerance. To monitor the JSA5800 RAID array, run the following commands.

To obtain the RAID status, run `/opt/MegaRAID/MegaCli/MegaCli64 -LDinfo -Lall -a 0`, as shown in Figure 450.

Figure 450 JSA5800 Obtain RAID Status

```
[root@jsaEP-FP ~]# /opt/MegaRAID/MegaCli/MegaCli64 -LDinfo -Lall -a 0

Adapter 0 -- Virtual Drive Information:
Virtual Drive: 0 (Target Id: 0)
Name:
RAID Level: Primary-1, Secondary-0, RAID Level Qualifier-0
Size: 3.270 TB
Sector Size: 512
Is VD emulated: No
Mirror Data: 3.270 TB
State: Optimal
Strip Size: 64 KB
Number Of Drives per span: 2
Span Depth: 4
Default Cache Policy: WriteBack, ReadAhead, Cached, No Write Cache if Bad BBU
Current Cache Policy: WriteBack, ReadAhead, Cached, No Write Cache if Bad BBU
Default Access Policy: Read/Write
Current Access Policy: Read/Write
Disk Cache Policy: Enabled
Encryption Type: None
Bad Blocks Exist: No
PI type: No PI
```

From the output, you can see that the JSA 5800 provides a total storage space of 3.2 TB and has a total of eight physical HDDs (4 drives per 2 spans). The Logical Disk (LD) state is Optimal which indicates that RAID is healthy. If there are any faulty HDDs, LD state is displayed as Degraded. To find out which HDD is faulty, use the PDLIST command. To obtain the driver status, run `/opt/MegaRAID/MegaCli/MegaCli64 -PDList -a 0` lmore, as shown in Figure 451.

Figure 451 JSA5800 Obtain Driver Status

```
[root@jsaEP-FP ~]# /opt/MegaRAID/MegaCli/MegaCli64 -PDList -a 0 | grep "Firmware state"
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
```

Use the same `/opt/MegaRAID/MegaCli/MegaCli64 -PDList -a 0` command with different filters to see the HDD Serial Number, HDD model, and Raw size details, as shown in Figure 452.

Figure 452 JSA5800 Obtain HDD Details

```
[root@jsaEP-FP ~]# /opt/MegaRAID/MegaCli/MegaCli64 -PDList -a 0 | grep -i "Seagate"
Inquiry Data: SEAGATE ST900MM0026 0003S0N33JHD
Inquiry Data: SEAGATE ST900MM0026 0003S0N2P6RK
Inquiry Data: SEAGATE ST900MM0026 0003S0N33GZF
Inquiry Data: SEAGATE ST900MM0026 0003S0N34QQR
Inquiry Data: SEAGATE ST900MM0026 0003S0N33WXR
Inquiry Data: SEAGATE ST900MM0026 0003S0N34JA9
Inquiry Data: SEAGATE ST900MM0026 0003S0N32W6K
Inquiry Data: SEAGATE ST900MM0026 0003S0N33WYX
[root@jsaEP-FP ~]# /opt/MegaRAID/MegaCli/MegaCli64 -PDList -a 0 | grep "Raw Size"
Raw Size: 838.362 GB [0x68cb9e30 Sectors]
Raw Size: 838.362 GB [0x68cb9e30 Sectors]
Raw Size: 838.362 GB [0x68cb9e30 Sectors]
Raw Size: 838.362 GB [0x68cb9e30 Sectors]
Raw Size: 838.362 GB [0x68cb9e30 Sectors]
Raw Size: 838.362 GB [0x68cb9e30 Sectors]
Raw Size: 838.362 GB [0x68cb9e30 Sectors]
Raw Size: 838.362 GB [0x68cb9e30 Sectors]
```

Monitor Health for JSA7500

The Juniper Secure Analytics 7500 (JSA7500) is an enterprise and carrier-class appliance that provides a scalable network security management solution for medium-sized companies up to large global organizations.

Figure 453 JSA 7500 Front and Rear Views



Figure 454 JSA7500 RAM Details

```
[root@jttac-JSA7500-r004 ~]# free -m
```

	total	used	free	shared	buff/cache	available
Mem:	128669	24755	96638	4326	7275	98316
Swap:	24575	0	24575			

Figure 455 JSA7500 CPU Details

```
[root@jttac-JSA7500-r004 ~]# lscpu
```

```
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                32
On-line CPU(s) list:   0-31
Thread(s) per core:    2
Core(s) per socket:    8
Socket(s):             2
NUMA node(s):         2
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 45
Model name:            Intel(R) Xeon(R) CPU E5-2648L 0 @ 1.80GHz
Stepping:              7
CPU MHz:               1800.000
BogoMIPS:              3596.28
Virtualization:        VT-x
L1d cache:             32K
L1i cache:             32K
L2 cache:              256K
L3 cache:              20480K
NUMA node0 CPU(s):    0-7,16-23
NUMA node1 CPU(s):    8-15,24-31
```

JSA7500 uses RAID10. In RAID10, drives are duplicated for fault tolerance. To monitor the JSA7500 RAID array, run the following commands. To obtain the RAID status, run `/opt/MegaRAID/MegaCli/MegaCli64 -LDInfo -LAll -a 0`, as shown in Figure 456.

Figure 456 JSA7500 Obtain RAID Status

```
root@j1tac-JSA7500-r003 ~]# /opt/MegaRAID/MegaCli/MegaCli164 -LDInfo -Lall -a 0

Adapter 0 -- Virtual Drive Information:
Virtual Drive: 0 (Target Id: 0)
Name                : RAID-10
RAID Level           : Primary-1, Secondary-0, RAID Level Qualifier-0
Size                : 11.446 TB
Sector Size          : 512
Is VD emulated       : No
Mirror Data          : 11.446 TB
State                : Optimal
Strip Size           : 512 KB
Number Of Drives per span:4
Span Depth           : 7
Default Cache Policy : WriteBack, ReadAdaptive, Direct, Write Cache OK if Bad BBU
Current Cache Policy : WriteBack, ReadAdaptive, Direct, Write Cache OK if Bad BBU
Default Access Policy: Read/Write
Current Access Policy: Read/Write
Disk Cache Policy    : Disk's Default
Encryption Type      : None
PI type: No PI
```

From the output, you can see that JSA7500 provides a total storage space of 11.4 TB and has a total of twenty-eight physical HDDs (7 drives per 4 spans). The Logical Disk (LD) state is Optimal which indicates that RAID is healthy. If there are any faulty HDDs, LD state is displayed as Degraded. To find out which HDD is faulty, use the `/opt/MegaRAID/MegaCli/MegaCli64 -PDlist -a 0` command.

To obtain the driver status, run `/opt/MegaRAID/MegaCli/MegaCli64 -PDlist -a 0`, as shown in Figure 457.

Figure 457 JSA7500 Obtain Driver Status

```
root@tarc-JUA7500-0003 ~# /opt/megaraid/Megacli/Megacli64 -Pdlist -a 0 | grep "Firmware state"
```

The state of the Firmware State as Online indicates that the physical HDDs are working fine. Use the same `/opt/MegaRAID/MegaCli/MegaCli64 -PDlist -a 0` command with different filters to see the HDD Serial Number, HDD model, and Raw size details, as shown in Figures 458 and 459.

Figure 458 JSA7500 Obtain HDD Details

```
[root@jtc-JSA7500-r003 ~]# /opt/MegaRAID/MegaCli/MegaCli64 -PDlist -a 0 | grep "Firmware state" | wc -l
28
```

Figure 459 JSA7500 Obtain HDD Details

```
[root@jtc-JSA7500-r003 ~]# /opt/MegaRAID/MegaCli/MegaCli64 -PDlist -a 0 | grep "Inquiry Data"
Inquiry Data: SEAGATE ST900MM0026 0001S0N0TFH7
Inquiry Data: SEAGATE ST900MM0026 0001S0N0WFP8E
Inquiry Data: SEAGATE ST900MM0026 0001S0N0WFP2E
Inquiry Data: SEAGATE ST900MM0026 0001S0N0WNH5E
Inquiry Data: SEAGATE ST900MM0026 0001S0N0V0V0V
Inquiry Data: SEAGATE ST900MM0026 0001S0N0WNKXW
Inquiry Data: SEAGATE ST900MM0026 0001S0N0VWZD0
Inquiry Data: SEAGATE ST900MM0026 0001S0N0VNM6M
Inquiry Data: SEAGATE ST900MM0026 0001S0N0K1L1E
Inquiry Data: SEAGATE ST900MM0026 0001S0N0VQMG5
Inquiry Data: SEAGATE ST900MM0026 0001S0N0VG944
Inquiry Data: SEAGATE ST900MM0026 0001S0N0VFPF1
Inquiry Data: SEAGATE ST900MM0026 0001S0N0WRF00
Inquiry Data: SEAGATE ST900MM0026 0001S0N0KDG6M
Inquiry Data: SEAGATE ST900MM0026 0001S0N0VSZ59
Inquiry Data: SEAGATE ST900MM0026 0001S0N0PK000
Inquiry Data: SEAGATE ST900MM0026 0001S0N0WTF7X
Inquiry Data: SEAGATE ST900MM0026 0001S0N0JYX00
Inquiry Data: SEAGATE ST900MM0026 0001S0N0JYER8
Inquiry Data: SEAGATE ST900MM0026 0001S0N0TFP44
Inquiry Data: SEAGATE ST900MM0026 0001S0N0WCKW3
Inquiry Data: SEAGATE ST900MM0026 0001S0N0WGTW6
Inquiry Data: SEAGATE ST900MM0026 0001S0N0VMD07
Inquiry Data: SEAGATE ST900MM0026 0001S0N0VQB37
Inquiry Data: SEAGATE ST900MM0026 0001S0N0WFP2C
Inquiry Data: SEAGATE ST900MM0026 0001S0N0WNC62
Inquiry Data: SEAGATE ST900MM0026 0001S0N0WNK77
Inquiry Data: SEAGATE ST900MM0026 0001S0N0WNFD0
```

In the unlikely scenario that you find a faulty HDD, create a support ticket with Juniper Support Team for RMA.

Monitor Health for JSA7800

The Juniper Secure Analytics 7800 (JSA7800) is an enterprise and carrier-class appliance that provides a scalable network security management solution for medium-sized companies up to large global organizations.

Figure 460 JSA7800 Front and Rear Views



The JSA7800 appliance is a 2-rack-unit (2-U) rack mountable. It supports hot-swappable dual-AC (or optional dual-DC) power supplies with redundant configuration, sixteen hot-swappable hard drives that support RAID, 128-GB memory, and two 10-Gigabit SFP+ interfaces and four 1-Gigabit Ethernet interfaces.

Figure 461 JSA7800 RAM Details

```
[root@jtac-JSA7800-BSE-r001 ~]# free -m
```

	total	used	free	shared	buff/cache	available
Mem:	128734	1895	126290	17	549	126256
Swap:	24575	0	24575			

Figure 462 JSA7800 CPU Details

```
[root@jtac-JSA7800-BSE-r001 ~]# lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                 40
On-line CPU(s) list:   0-39
Thread(s) per core:    2
Core(s) per socket:    10
Socket(s):              2
NUMA node(s):          2
Vendor ID:              GenuineIntel
CPU family:             6
Model:                  62
Model name:             Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz
Stepping:               4
CPU MHz:                1660.791
CPU max MHz:            3600.0000
CPU min MHz:            1200.0000
BogoMIPS:               5600.31
Virtualization:         VT-x
L1d cache:              32K
L1i cache:              32K
L2 cache:               256K
L3 cache:               25600K
```

The JSA7800 appliance uses the RAID6 configuration. In RAID6, drives are duplicated for fault tolerance. To monitor the JSA7800 RAID array, run the following commands.

To obtain the RAID status, run `/opt/MegaRAID/MegaCli/MegaCli64 -LDinfo -Lall -a 0`, as shown in Figure 463.

Figure 463 JSA7800 Obtain RAID Status

```
[root@jttac-JSA7800-BSE-r001 ~]# /opt/MegaRAID/MegaCli/MegaCli64 -LDinfo -Lall -a 0

Adapter 0 -- Virtual Drive Information:
Virtual Drive: 0 (Target Id: 0)
Name                :
RAID Level           : Primary-6, Secondary-0, RAID Level Qualifier-3
Size                 : 25.463 TB
Sector Size          : 512
Is VD emulated       : No
Parity Size          : 3.637 TB
State                : Optimal
Strip Size           : 256 KB
Number Of Drives     : 16
Span Depth           : 1
Default Cache Policy: WriteBack, ReadAhead, Direct, No Write Cache if Bad BBU
Current Cache Policy: WriteBack, ReadAhead, Direct, No Write Cache if Bad BBU
Default Access Policy: Read/Write
Current Access Policy: Read/Write
Disk Cache Policy    : Disk's Default
Encryption Type      : None
Bad Blocks Exist: No
PI type: No PI
```

From the output, you can see that the JSA7800 provides a total storage space of 25.4 TB and has a total of sixteen physical HDDs. The Logical Disk (LD) state is Optimal, which indicates that RAID is healthy.

If there are any faulty HDDs, LD state is displayed as Degraded. To find out which HDD is faulty, use the `/opt/MegaRAID/MegaCli/MegaCli64 -PDlist -a 0` command.

To obtain the driver status, run `/opt/MegaRAID/MegaCli/MegaCli64 -PDList -a 0 |more`, as shown in Figure 464.

Figure 464 JSA7800 Obtain Driver Status

```
[root@jttac-JSA7800-BSE-r001 ~]# /opt/MegaRAID/MegaCli/MegaCli64 -PDList -a 0 | grep "Firmware state"
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
```

The state of the Firmware State as Online indicates that the physical HDDs are working fine. Use the same `/opt/MegaRAID/MegaCli/MegaCli64 -PDList -a 0` command with different filters to see the HDD Serial Number, HDD model, and Raw size details, as shown in Figures 465.

Figure 465 JSA7800 Obtain HDD Details

```
[root@jtac-JSA7800-BSE-r001 ~]# /opt/MegaRAID/MegaCli/MegaCli64 -PDList -a 0 | grep "Raw Size"
Raw Size: 1.819 TB [0xe8e088b0 Sectors]
Raw Size: 1.819 TB [0xe8e088b0 Sectors]
Raw Size: 1.819 TB [0xe8e088b0 Sectors]
Raw Size: 1.819 TB [0xe8e088b0 Sectors]
Raw Size: 1.819 TB [0xe8e088b0 Sectors]
Raw Size: 1.819 TB [0xe8e088b0 Sectors]
Raw Size: 1.819 TB [0xe8e088b0 Sectors]
Raw Size: 1.819 TB [0xe8e088b0 Sectors]
Raw Size: 1.819 TB [0xe8e088b0 Sectors]
Raw Size: 1.819 TB [0xe8e088b0 Sectors]
Raw Size: 1.819 TB [0xe8e088b0 Sectors]
Raw Size: 1.819 TB [0xe8e088b0 Sectors]
Raw Size: 1.819 TB [0xe8e088b0 Sectors]
Raw Size: 1.819 TB [0xe8e088b0 Sectors]
Raw Size: 1.819 TB [0xe8e088b0 Sectors]
Raw Size: 1.819 TB [0xe8e088b0 Sectors]
```

Figure 466 JSA7800 Obtain HDD Details

```
[root@jtac-JSA7800-BSE-r001 ~]# /opt/MegaRAID/MegaCli/MegaCli64 -PDList -a 0 | grep "Inquiry Data"
Inquiry Data: SEAGATE ST2000NX0433 N005W462FV8A
Inquiry Data: SEAGATE ST2000NX0433 N005W462CW8R
Inquiry Data: SEAGATE ST2000NX0433 N005W462EWFS
Inquiry Data: SEAGATE ST2000NX0433 N005W462CK3H
Inquiry Data: SEAGATE ST2000NX0433 N005W462EX3N
Inquiry Data: SEAGATE ST2000NX0433 N005W462FVJV
Inquiry Data: SEAGATE ST2000NX0433 N005W462EWFT
Inquiry Data: SEAGATE ST2000NX0433 N005W462EXT9
Inquiry Data: SEAGATE ST2000NX0433 N005W462CVV0
Inquiry Data: SEAGATE ST2000NX0433 N005W462G8RW
Inquiry Data: SEAGATE ST2000NX0433 N005W462G85D
Inquiry Data: SEAGATE ST2000NX0433 N005W462GH1T
Inquiry Data: SEAGATE ST2000NX0433 N005W462FV9Z
Inquiry Data: SEAGATE ST2000NX0433 N005W462G8G0
Inquiry Data: SEAGATE ST2000NX0433 N005W462CW2M
Inquiry Data: SEAGATE ST2000NX0433 N005W462EXDY
```

In the unlikely scenario that you find a faulty HDD, create a support ticket with Juniper Support Team for RMA.

Determine Model Details and Serial Number of JSA Appliances

To determine the serial number of JSA appliances, use the `dmidecode | grep -i serial | more` command.

To determine the model details of JSA appliances, use the `dmidecode | grep -i product` command.

JSA3800 Sample Output

Run `dmidecode | grep -i product` to verify the appliance model.

Figure 467 Verify Appliance Model (JSA3800)

```
[root@jtac-JSA3800-BSE-r002 ~]# dmidecode | grep -i product
Product Name: JSA3800
Product Name: JSA3800
```


Run `dmidecode | grep -i serial` to verify the serial number.

Figure 468

Verify Serial Number (JSA3800)

```
[root@jttac-JSA3800-BSE-r002 ~]# dmidecode | grep -i serial
Serial services are supported (int 14h)
Serial Number: CS3115AM0003
Serial Number: ZM157S006719
Serial Number: C1130LD50N40172
Serial Number: Not Specified
Port Type: Serial Port 16550A Compatible
Serial Number: 4019EC49
Serial Number: Dimm1_SerNum
Serial Number: 4019EC30
Serial Number: Dimm3_SerNum
Serial Number: 4019EC42
Serial Number: Dimm5_SerNum
Serial Number: 4019EC45
Serial Number: Dimm7_SerNum
Serial Number:
Serial Number: P7041CE37ST0365
Serial Number: P7041CE35ST0213
```

JSA5800 Sample Output

Run `dmidecode | grep -i product` to verify the appliance model.

Figure 469

Verify Appliance Model (JSA5800)

```
[root@jsaEP-FP ~]# dmidecode | grep -i product
Product Name: JSA5800
Product Name: JSA5800
```

Run `dmidecode | grep -i serial` to verify the serial number.

Figure 470

Verify Serial Number (JSA5800)

```
[root@jsaEP-FP ~]# dmidecode | grep -i serial
Serial services are supported (int 14h)
Serial Number: CT1315AM0023
Serial Number: VM14CS019758
Serial Number: C2130LC50MA0359
Serial Number: Not Specified
Serial Number: Not Specified
Port Type: Serial Port 16550A Compatible
```

JSA7500 Sample Output

Run `dmidecode | grep -i product` to verify the appliance model.

Figure 471

Verify Appliance Model (JSA7500)

```
[root@jttac-JSA7500-r004 ~]# dmidecode | grep -i product
Product Name: JSA7500
Product Name: S2600CO
```

Run `dmidecode | grep -i serial` to verify the serial number.

Figure 472 Verify Serial Number (JSA7500)

```
[root@jttac-JSA7500-r004 ~]# dmidecode | grep -i serial
Serial services are supported (int 14h)
Serial Number: 0329122013000009
Serial Number: QSC032600438
Serial Number: .....
Serial Number:
Serial Number:
```

JSA7800 Sample Output

Run `dmidecode | grep -i product` to verify the appliance model.

Figure 473 Verify Appliance Model (JSA7800)

```
[root@jttac-JSA7800-BSE-r001 ~]# dmidecode | grep -i product
Product Name: JSA7800
Product Name: JSA7800
```

Run `dmidecode | grep -i serial` to verify the serial number.

Figure 474 Verify Serial Number (JSA7800)

```
[root@jttac-JSA7800-BSE-r001 ~]# dmidecode | grep -i serial
Serial services are supported (int 14h)
Serial Number: CU0520AM0002
Serial Number: VM199S022251
Serial Number: C2160LI37NA0055
Serial Number: Not Specified
Serial Number: Not Specified
Port Type: Serial Port 16550A Compatible
```

Appendices

Appendix A: Memory Requirements for Virtual Appliances

Table A.1 lists the minimum memory requirements for JSA virtual appliances.

Table A.1 *Advanced Options for the HA Host*

JSA Virtual Appliance	Minimum memory requirement	Suggested memory requirement
QFlow Virtual	6 GB	6 GB
Data Node Virtual 1400	24 GB	48 GB
Event Collector Virtual 1599	12 GB	16 GB
Event Processor Virtual 1699 up to 20,000 EPS	12 GB	48 GB
Event Processor Virtual 1699 20,000 EPS or higher	128 GB	128 GB
Flow Processor Virtual 1799 up to 1,200,000 FPM	12 GB	48 GB
Flow Processor Virtual 1799 1,200,000 FPM or higher	128 GB	128 GB
All-in-One Virtual 3199 5,000 EPS or less 200,000 FPM or less	32 GB	48 GB

All-in-One Virtual 3199 30,000 EPS or less 1,000,000 FPM or less	64 GB	128 GB
Log Analytics Virtual 8099	24 GB	48 GB
Risk Manager	24 GB	48 GB
Vulnerability Manager Processor	32 GB	32 GB
Vulnerability Manager Scanner	16 GB	16 GB
App Host	12 GB	64 GB or more for a medium sized App Host 128 GB or more for a large sized App Host

Appendix B: CPU Requirements for Virtual Appliances

Table B.1 lists the CPU requirements for virtual appliances.

Table B.1 CPU Requirements for JSA Virtual Appliances

JSA Virtual Appliance	Threshold	Minimum Number of CPU Cores	Suggested Number of CPU Cores
QFlow Virtual 1299	10,000 FPM or less	4	4
Event Collector Virtual 1599	2,500 EPS or less	4	16
	5,000 EPS or less	8	16
	20,000 EPS or less	16	16
Event Processor Virtual 1699	2,500 EPS or less	4	24
	5,000 EPS or less	8	24
	20,000 EPS or less	16	24
	40,000 EPS or less	40	40
	80,000 EPS or less	56	56

Flow Processor Virtual 1799	150,000 FPM or less	4	24
	300,000 FPM or less	8	24
	1,200,000 FPM or less	16	24
	2,400,000 FPM or less	48	48
	3,600,000 FPM or less	56	56
Event and Flow Processor Virtual 1899	200,000 FPM or less 5,000 EPS or less	16	24
	300,000 FPM or less 15,000 EPS or less	48	48
	1,200,000 FPM or less 30,000 EPS or less	56	56
All-in-One Virtual Appliance 3199	25,000 FPM or less 500 EPS or less	4	24
	50,000 FPM or less 1,000 EPS or less	8	24
	100,000 FPM or less 1,000 EPS or less	12	24
	200,000 FPM or less 5,000 EPS or less	16	24
	300,000 FPM or less 15,000 EPS or less	48	48
	1,200,000 FPM or less 30,000 EPS or less	56	56
Log Analytics Virtual 8099	2,500 EPS or less	4	16
	5,000 EPS or less	8	16
Vulnerability Manager Processor		4	4
Vulnerability Manager Scanner		4	4
Risk Manager		8	8
Data Node Virtual 1400 appliance		4	16
App Host		4	12 or more for a medium sized App Host

Appendix C: Common Ports Used by JSA

Table C.1 lists 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 C.1: 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.
37	rdate (time)	UDP/ TCP	All systems to the JSA console. JSA console to the NTP or rdate server.	Time synchronization between the JSA console and managed hosts.
111	Port mapper	TCP/ UDP	Managed hosts that communicate with the JSA console. Users that connect to the JSA console.	Remote Procedure Calls (RPC) for required services, such as Network File System (NFS).
123	Network Time Protocol (NTP)	TCP/ UDP	JSA Console to the NTP server. HA primary to secondary, and vice versa.	Time synchronization between JSA HA pairs, and between the JSA Console and the NTP server.

135 and dynamically allocated ports above 1024 for RPC calls.	DCOM	TCP	<p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.</p> <p>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.</p>	<p>This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.</p> <p>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.</p>
137	Windows NetBIOS name service	UDP	<p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.</p> <p>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.</p>	<p>This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.</p>
138	Windows NetBIOS datagram service	UDP	<p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.</p> <p>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.</p>	<p>This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.</p>

139	Windows NetBIOS session service	TCP	<p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.</p> <p>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.</p>	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
162	NetSNMP	UDP	<p>JSA managed hosts that connect to the JSA console.</p> <p>External log sources to JSA Event Collectors.</p>	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	<p>JSA managed hosts that connect to the JSA console.</p> <p>External log sources to JSA Event Collectors.</p>	TCP port for the NetSNMP daemon that listens for communications (v1, v2c, and v3) from external log sources. The port is open only when the SNMP agent is enabled.
443	Apache/HTTPS	TCP	<p>Bidirectional traffic for secure communications from all products to the JSA console.</p>	<p>Configuration downloads to managed hosts from the JSA console.</p> <p>JSA managed hosts that connect to the JSA console.</p> <p>Users must have login access to JSA.</p> <p>JSA console that manages and provides configuration updates for WinCollect agents.</p>
445	Microsoft Directory Service	TCP	<p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.</p> <p>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.</p> <p>Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.</p>	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.

514	Syslog	UDP/ TCP	<p>External network appliances that provide TCP syslog events use bidirectional traffic.</p> <p>External network appliances that provide UDP syslog events use uni-directional traffic.</p> <p>Internal syslog traffic from JSA hosts to the JSA console.</p>	<p>External log sources to send event data to JSA components.</p> <p>Syslog traffic includes WinCollect agents, event collectors, and Adaptive Log Exporter agents capable of sending either UDP or TCP events to JSA.</p>
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.
2375	Docker command port	TCP	Internal communications. This port is not available externally.	Used to manage JSA application framework resources.
4333	Redirect port	TCP		This port is assigned as a redirect port for Address Resolution Protocol (ARP) requests in JSA offense resolution.

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.
6543	High-availability heartbeat	TCP/UDP	Bidirectional between the secondary host and primary host in an HA cluster.	Heartbeat ping from a secondary host to a primary host in an HA cluster to detect hardware or network failure.
7676, 7677, and four randomly bound ports above 32000.	Messaging connections (IMQ)	TCP	Message queue communications between components on a managed host.	<p>Message queue broker for communications between components on a managed host.</p> <p>NOTE You must permit access to these ports from the JSA console to unencrypted hosts.</p> <p>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 section Viewing IMQ port associations.</p>

7777, 7778, 7779, 7780, 7781, 7782, 7783, 7788, 7790, 7791, 7792, 7793, 7795, 7799, and 8989.	JMX server ports	TCP	Internal communications. These ports are not available externally.	JMX server (Java Management Beans) monitoring for all internal JSA processes to expose supportability metrics. These ports are used by JSA support.
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	Apache Tomcat	TCP	From the Event Collector to the JSA console.	Anomaly detection engine port.
7804	QRM 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.

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	UDP	External SNMP systems that request SNMP trap information from the JSA console.	UDP listening port for external SNMP data requests.
8005	Apache Tomcat	TCP	Internal communications. Not available externally.	Open to control tomcat. This port is bound and only accepts connections from the local host.
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.
8413	WinCollect agents	TCP	Bidirectional traffic between WinCollect agent and JSA console.	This traffic is generated by the WinCollect agent and communication is encrypted. It is required to provide configuration updates to the WinCollect agent and to use WinCollect in connected mode.

8844	Apache Tomcat	TCP	Unidirectional from the JSA console to the appliance that is running the JSA Vulnerability Manager processor.	Used by Apache Tomcat to read RSS feeds from the host that is running the JSA Vulnerability Manager processor.
9090	XForce IP Reputation database and server	TCP	Internal communications. Not available externally.	Communications between JSA processes and the XForce Reputation IP database.
9913 plus one dynamically assigned port	Web application container	TCP	Bidirectional Java Remote Method Invocation (RMI) communication between Java Virtual Machines	When the web application is registered, one additional port is dynamically assigned.
9995	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the JSA flow processor.	NetFlow datagram from components, such as routers.
9999	JSA Vulnerability Manager processor	TCP	Unidirectional from the scanner to the appliance running the JSA Vulnerability Manager processor	Used for JSA Vulnerability Manager command information. The JSA console connects to this port on the host that is running the JSA Vulnerability Manager processor. This port is only used when JSA Vulnerability Manager is enabled.

10000	JSA web-based, system administration interface	TCP/UDP	User desktop systems to all JSA hosts.	In JSA 2014.5 and earlier, this port is used for server changes, such as the hosts root password and firewall access. Port 10000 is disabled in 2014.6.
10101, 10102	Heartbeat command	TCP	Bidirectional traffic between the primary and secondary HA nodes.	Required to ensure that the HA nodes are still active.
15433	Postgres	TCP	Communication for the managed host that is used to access the local database instance.	Used for JSA Vulnerability Manager configuration and storage. This port is only used when JSA Vulnerability Manager is enabled.
20000-23000	SSH Tunnel	TCP	Bidirectional from the JSA Console to all other encrypted managed hosts.	Local listening point for SSH tunnels used for Java Message Service (JMS) communication with encrypted managed hosts. Used to perform long-running asynchronous tasks, such as updating networking configuration via System and License Management.
23111	SOAP web server	TCP		SOAP web server port for the Event Collection Service (ECS).

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

32000-33999	Data flow (flows, events, flow context)	TCP	Bidirectional between JSA components.	Data flows, such as events, flows, flow context, and event search queries.
40799	PCAP data	UDP	From Juniper Networks SRX Series appliances to JSA.	Collecting incoming packet capture (PCAP) data from Juniper Networks SRX Series appliances. NOTE The packet capture on your device can use a different port. For more information about configuring packet capture, see your Juniper Networks SRX Series appliance documentation.

Appendix D: Important services running on JSA

While there are numerous services running on JSA, let us briefly look into the important ones, listed in Table D.1.

Note that in an all-in-one deployment, all these are running on a single system. In a distributed deployment, the services are running on different managed hosts.

Table D.1: Listening Ports That Are Used by JSA Services and Components

Service Name	Description	Runs On	Impact if the Service is Down
tomcat	Responsible for rendering the web UI.	Console	Web UI will not be available to users.
ariel_proxy_server	Queries data from managed hosts. Proxys search requests from different processes to the various ariel query servers.	Console	Affects searching of events and flows from JSA web UI.

accumulator	Responsible for scheduled reports, saved searches, and time-series graphs. To speed-up searches and reports, the accumulator service accumulates the required data on a by-minute, by-hour and by-day fashion.	Console	Scheduled reports, timeseries graphs and saved searches will get affected if this service is down.
hostcontext	<p>Runs the <i>ProcessManager</i> component that is responsible for starting, stopping, and verifying status for each component within the deployment.</p> <p>Manages database replication bundles between console and managed hosts.</p> <p>Requests for updated configuration files, downloads and unpacks them, and notifies other components within an appliance.</p> <p>Monitors postgresql transactions and restarts any processes that have exceeded the predetermined time limit.</p> <p>Runs disk maintenance routines for disk cleanup.</p> <p>Starts tunnels, ecs, accumulator, ariel_proxy, ariel_query, qflow, reporting, and asset_profiler services.</p>	Console and all managed hosts	Hostcontext manages all the other services except tomcat, hostservices and ecs-ec-ingress. All services controlled by hostcontext are inactive until they are restarted.
hostservices	Responsible for imq and postgresql services.	Console and all managed hosts	Affects all JSA services on the device where the hostservices service is down, and that specific device will not function properly.
ariel_query_server	Reads the ariel database on the managed hosts, and sends the data matching the request back to the console's proxy server for further processing.	Managed hosts (except SFEC, App Host, VP, and VS)	You cannot search for events and flows from that specific managed host on the JSA web UI.
asset_profiler	Builds the Asset database on the console with identity details.	Console	Assets are not added, updated, or deleted.
ecs-ec-ingress (Event Correlation Service -Event Collector-ingress)	Collects events in a buffer while ecs-ec and ecs-ep are being restarted. Then it spools the data back to ecs-ec and ecs-ep	Console and managed hosts (except DN, VP, VS, App Host, and RM)	Events are not collected in a buffer and spooled to the other ecs services.

ecs-ec (Event Correlation Service -Event Collector)	Parses, normalizes and coalesces events.	Console and managed hosts (except DN, VP, VS, App Host, and RM)	Impacts event and flow collection.
ecs-ep (Event Correlation Service -Event Processor)	Correlates events, stores events in the Ariel database, and forwards events matching the rules within CRE to the Magistrate component.	Console and managed hosts (except DN, VP, VS, App Host, and RM)	Impacts event and flow collection and their storage.
vis (Vulnerability Import Service)	Drives third-party scanner modules.	Console and managed hosts (except RM, App Host, and DN)	Vulnerability import and scans are affected.
imq	Responsible for communication between various internal components.	Console and all managed hosts	Affects all JSA services on the device where the imq service is down, and that specific device will not function properly.
postgresql	Responsible for postgres database. JSA configuration is stored in the postgres database.	Console and all managed hosts	Affects all JSA services on the device where the postgres service is down, and that specific device will not function properly.
reporting_executor	Runs the scheduler for reporting.	Console	You cannot generate new reports.
qflow	Responsible for flow collection.	Console and flow processors (FP/FC)	Affects flow collection.
qvmprocessor	Responsible for vulnerability processing.	Console and vulnerability processor	VA scans are affected.
qvmscanner	Responsible for VA scans.	Console, vulnerability scanner, and managed hosts which act as scanners.	VA scans are affected.
ha_manager	Runs when HA is configured. Responsible for managing high-availability.	On primary and secondary HA hosts	Affects HA functionality.
drbd	Runs when HA is configured. Responsible for disk synchronization between high-availability hosts.	On primary and secondary HA hosts	Affects HA functionality.
dataNode	Responsible for data node functions.	Data nodes	Affects data rebalancing.
docker	Responsible for Apps (Apps run as containers).	Console and App Hosts	Affects JSA Apps only.

Appendix E: Most Popular JSA Incidents and Checks

Table E.1 JSA Incidents and Checks

Issue	Check Points
Deployment times out	<p>Check for the following:</p> <p>The required ports (see Appendix C) are open between the console and the managed hosts.</p> <p>There are no connectivity issues between the console and managed host.</p> <p>Services are up on both console and managed hosts.</p> <p>See qradar.log for more details.</p>
JSA services down	<p>Check to see if there is enough disk space available on the console and managed hosts.</p> <p>Whenever the disk utilization goes beyond a certain threshold, services will be shutdown to avoid data loss. See qradar.log for more details.</p>
Unable to search events/flows from JSA web UI	<p>Make sure that the /transient partition has enough disk space available.</p> <p>Doing a full deploy may resolve temporary search issues because this action restarts ariel service. Ensure that the services are UP on console and managed hosts. See qradar.log for more details.</p>
Unable to see events in Log Activity tab	<p>Check for the following:</p> <p>Make sure that the log sources are configured to send events, and the required ports are open between the log sources and the JSA console or event collectors.</p> <p>Use tcpdump to verify if events are reaching the JSA console or collector interfaces.</p> <p>Check to see if services are running fine on the JSA console or collector.</p> <p>Use latest DSMs and PROTOCOLS.</p> <p>See qradar.log for more details.</p>
Unable to see flows in Network Activity tab	<p>Check for the following:</p> <p>Ensure that the flow sources are configured to send flows and the required ports are open between the flow sources and the JSA console or flow collector.</p> <p>Use tcpdump to verify if the flows are reaching JSA console or collector interfaces.</p> <p>Make sure services are running fine on console or flow collector.</p> <p>See qradar.log for more details.</p>
Unable to access JSA web UI	<p>Ensure that the tomcat service is up on console. See qradar.log for more details.</p>
Unable to get email alerts for offenses	<p>Verify the following:</p> <p>SMTP access is configured for the console, event collectors, and flow collectors.</p> <p>Port 25 is open between the SMTP server and JSA console or collectors. See qradar.log for more details.</p>

Issues while adding managed hosts	<p>Check for the following:</p> <p>The required ports (see Appendix C) are open between the console and the managed hosts.</p> <p>There are no connectivity issues between the console and the managed hosts.</p> <p>Services are up on both console and managed hosts.</p> <p>See qradar.log for more details.</p>
Issues while configuring high-availability	<p>Ensure that all the required ports are open (see Appendix C) and there are no connectivity issues between the primary and secondary hosts.</p> <p>The /store partition on the secondary host must be equal or more than primary device's /store partition.</p> <p>See qradar.log and qradar-ha.log for more details.</p>
Issues with X-Force updates	<p>Ensure that JSA has access to update.xforce-security.com and license.xforce-security.com and that you can download updated files.</p> <p>See /opt/qradar/dca/logs/sca_server.log for more details.</p>
Issues with auto-updates	<p>Ensure that JSA has access to download.juniper.net on port 443 and that you can download auto-update files.</p> <p>See qradar.log for more details.</p>
Events shown as Unknown	<p>Update the DSM to the latest available version.</p>