Juniper Networks | Engineering Simplicity

Juniper Secure Analytics Getting Started Guide

Published
2022-05-13

RELEASE
7.5.0

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

Juniper Secure Analytics Getting Started Guide
7.5.0

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About This Guide

Use this guide to understand how to perform basic JSA configuration, begin collecting event and flow data, and generate custom or default reports.

1
CHAPTER

JSA Overview

JSA Overview

JSA is a network security management platform that provides situational awareness and compliance support. JSA uses a combination of flow-based network knowledge, security event correlation, and asset-based vulnerability assessment.

Log Activity

In JSA, you can monitor and display network events in real time or perform advanced searches.

The **Log Activity** tab displays event information as records from a log source, such as a firewall or router device. Use the **Log Activity** tab to do the following tasks:

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

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

RELATED DOCUMENTATION

Network Activity | 2

Assets | 3

Offenses | 4

Network Activity

In JSA, you can investigate the communication sessions between two hosts.

If the content capture option is enabled, the **Network Activity** tab displays information about how network traffic is communicated and what was communicated. Using the **Network Activity** tab, you can do the following tasks:

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

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

RELATED DOCUMENTATION

Assets | 3
Offenses | 4
Reports | 4

Assets

JSA automatically creates asset profiles by using passive flow data and vulnerability data to discover your network servers and hosts.

Asset profiles provide information about each known asset in your network, including the services that are running. Asset profile information is used for correlation purposes, which helps to reduce false positives.

Use the **Assets** tab to do the following tasks:

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

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

RELATED DOCUMENTATION

Offenses

In JSA, you can investigate offenses to determine the root cause of a network issue.

Use the **Offenses** tab to view all the offenses that occur on your network and complete the following tasks:

- 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.

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

RELATED DOCUMENTATION

Reports

In JSA, you can create custom reports or use default reports.

JSA provides default report templates that you can customize, rebrand, and distribute to JSA users.

Report templates are grouped into report types, such as compliance, device, executive, and network reports. Use the **Reports** tab to complete the following tasks:

- 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. Branding is beneficial for distributing reports to different audiences.
- Set a schedule for generating both custom and default reports.
- Publish reports in various formats.

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

RELATED DOCUMENTATION

Data Collection

IN THIS SECTION

JSA accepts information in various formats and from a wide range of devices, including security events, network traffic, and scan results.

Collected data is categorized into three major sections: events, flows, and vulnerability assessment (VA) information.

Event Data Collection

Events are generated by log sources such as firewalls, routers, servers, and intrusion detection systems (IDS) or intrusion prevention systems (IPS).

Most log sources send information to JSA by using the syslog protocol. JSA also supports the following protocols:

- Simple Network Management Protocol (SNMP)
- Java database Connectivity (JDBC)
- Security Device Event Exchange (SDEE)

By default, JSA automatically detects log sources after a specific number of identifiable logs are received within a certain time frame. After the log sources are successfully detected, JSA adds the appropriate device support module (DSM) to the **Log Sources** window in the **Admin** tab.

Although most DSMs include native log sending capability, several DSMs require extra configuration, or an agent, or both to send logs. Configuration varies between DSM types. You must ensure the DSMs are configured to send logs in a format that JSA supports. For more information, see *Adding a Log Source*. For more information about configuring DSMs, see the *Configuring DSMs Guide*.

Certain log source types, such as routers and switches, do not send enough logs for JSA to quickly detect and add them to the Log Source list. You can manually add these log sources. For more information, see *Adding a DSM*. For more information about manually adding log sources, see the *Configuring DSMs Guide*.

Collected data is categorized into three major sections: events, flows, and vulnerability assessment (VA) information.

Flow Data Collection

Flows provide information about network traffic and can be sent to JSA in various formats, including Flowlog files, NetFlow, J-Flow, sFlow, and Packeteer.

By accepting multiple flow formats simultaneously, JSA can detect threats and activities that would otherwise be missed by relying strictly on events for information.

JSA Flow Processor provide full application detection of network traffic regardless of the port on which the application is operating. For example, if the Internet Relay Chat (IRC) protocol is communicating on port 7500/TCP, a JSA flow processor identifies the traffic as IRC and provides a packet capture of the beginning of the conversation. NetFlow and J-Flow notify you only that port 7500/TCP has traffic without providing any context for what protocol is being used.

Common mirror port locations include core, DMZ, server, and application switches, with NetFlow providing supplemental information from border routers and switches.

JSA Flow Processor are enabled by default and require a mirror, span, or tap to be connected to an available interface on the JSA appliance. Flow analysis automatically begins when the mirror port is connected to one of the network interfaces on the JSA appliance. By default, JSA monitors on the management interface for NetFlow traffic on port 2055/UDP. You can assign extra NetFlow ports, if required.

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

Vulnerability Assessment (VA) Information

JSA can import VA information from various third-party scanners.

VA information helps JSA Risk Manager identify active hosts, open ports, and potential vulnerabilities.

JSA Risk Manager uses VA information to rank the magnitude of offenses on your network.

Depending on the VA scanner type, JSA Risk Manager can import scan results from the scanner server or can remotely start a scan.

For more information, see "Importing Vulnerability Assessment Information" on page 22.

RELATED DOCUMENTATION

JSA Rules | 7

Supported Web Browsers | 8

Reports | 4

JSA Rules

Rules perform tests on events, flows, or offenses. If all the conditions of a test are met, the rule generates a response.

JSA includes rules that detect a wide range of activities, including excessive firewall denies, multiple failed login attempts, and potential botnet activity. For more information about rules, see the *Juniper Secure Analytics Administration Guide*.

NOTE: A user with non-administrative access can create rules for areas of the network that they can access. You must have the appropriate role permissions to manage rules. For more information about user role permissions, see the *Juniper Secure Analytics Administration Guide*.

RELATED DOCUMENTATION

Supported Web Browsers | 8

Reports | 4

Data Collection | 5

Supported Web Browsers

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

When you access the JSA system, you are prompted for a user name and a password. The user name and password must be configured in advance by the administrator.

The following table lists the supported versions of web browsers.

Table 1: Supported Web Browsers for JSA Products

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

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

Security Exceptions and Certificates

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

Navigate the Web-Based Application

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

RELATED DOCUMENTATION

Apps Overview

JSA apps are created by developers. After a developer creates an app, Juniper certifies and publishes it in the IBM Security App Exchange. JSA administrators can then browse and download the apps and then install the apps into JSA to address specific security requirements.

The IBM Security App Exchange is a community-based sharing hub, that you use to share apps across Juniper Security products. By participating in App Exchange, you can use the rapidly assembled, innovative workflows, visualizations, analytics, and use cases that are packaged into apps to address specific security requirements. Easy-to-use solutions are developed by partners, consultants, developers to address key security challenges. To detect and remediate threats, use these shared security components, from real-time correlation and behavioral modeling to custom responses and reference data.

NOTE: The combined memory requirements of all the apps that are installed on a JSA Console cannot exceed 10 per cent of the total available memory, or the apps won't work. If you exceed the 10 per cent memory allocation and want to run more apps, use a dedicated appliance for your apps (AppNode appliance for JSA 7.3.1 or the AppHost appliance for JSA 7.3.2 or later).

The QRadar Assistant app helps you to manage and update your app and content extension inventory, view app and content extension recommendations, follow the JSA Twitter feed, and get links to useful information. The app is automatically installed with JSA 7.3.2 or later.

FAQ

What is an app?

Apps create or add new functions in JSA by providing new tabs, API methods, dashboard items, menus, toolbar buttons, configuration pages, and more within the JSA user interface. You download apps from the IBM Security App Exchange. Apps that are created by using the GUI Application Framework Software Development Kit integrate with the JSA user interface to deliver new security intelligence capabilities or extend the current functions.

Every downloaded file from the IBM Security App Exchange is known as an extension. An extension can consist of an app or security product enhancement (content extension) that is packaged as an archive (.zip) file, which you can deploy on JSA by using the Extensions Management tool on the Admin tab.

Who can create an app?

You can use the GUI Application Framework Software Development Kit to create apps.

How do I share my app?

Only certified content is shared in the IBM Security App Exchange, a new platform for collaborating where you can respond quickly and address your security and platform enhancement requirements. In the IBM Security App Exchange, you can find available apps, discover their purpose, and what they look like, and learn what other users say about the apps.

How do I get an app that I downloaded into JSA?

A JSA administrator downloads an extension and imports it into JSA by using the **Extensions Management** tool, which is used to upload the downloaded extension from a local source.

Where do I get help for an app?

You can see information about an app in the overview section when you download the app from the IBM Security App Exchange. For apps developed solely by Juniper, you can find information in the Juniper Knowledge Center.

How much memory does an app need?

The combined memory requirements of all the apps that are installed on a JSA Console cannot exceed 10 per cent of the total available memory. If you install an app that causes the 10 per cent memory limit to be exceeded, the app does not work.

If your app requires a minimum memory allocation, you must specify this allocation as part of your app manifest. The default allocation is 200 MB.

What is the difference between an app, a content extension, and a content pack?

Extension

From within JSA, an extension is a term that is used for everything that you download from the IBM Security App Exchange. Sometimes that extension contains individual content items, such as custom AQL functions or custom actions, and sometimes the extension contains an app that is developed by

using the GUI App Framework Software Development Kit. You use the Extensions Management tool to install extensions.

App

An app is content that is created when you use the GUI App Framework Software Development Kit. The app extends or creates new functions in JSA.

Content extension

A content extension is typically used to update JSA security template information or add new content such as rules, reports, searches, logos, reference sets, custom properties. Content extensions are not created by using the GUI Application Framework Software Development Kit.

You download content packs from Juniper Customer Support in RPM format.

Typically, content extensions differ from content packs because you download content packs (RPM files) from Juniper Customer Support.

Apps that are Installed by Default with JSA

To improve workflow, some apps that were previously only available on the IBM Security App Exchange are now installed by default.

The following table describes the installed apps and their benefits.

App	Installed on JSA versions
QRadar Assistant Use the QRadar Assistant app to manage your app and content extension inventory, view app and content extension recommendations, and get links to other information. For more information, see *QRadar Assistant App Guide*.	• 7.3.3 Fix Pack 6 or later • 7.4.1 Fix Pack 2 or later • 7.4.2 GA or later

(Continued)

App	**Installed on JSA versions**
QRadar Pulse QRadar Pulse is a dashboard app that you can use to communicate insights and analysis about your network. Take the pulse of your SOC with dynamic real-time dashboards that provide meaningful insights into your security posture and threat landscape. Visualize offenses, network data, threats, and malicious user behavior from around the world in geographical maps, a built-in 3D threat globe, and auto updating charts. Import and export dashboards to share with colleagues. See offenses unfold near real time and track your security threats from around the globe. For more information, see *Pulse App Guide*.	7.4.0 or later
Log Source Management The Log Source Management app provides an easy-to-use workflow that helps you quickly find, create, edit, and delete log sources. Use the simplified workflow to change parameters for a number of log sources at the same time. To configure log sources in 7.4.0, you must use the Log Source Management app. For more information, see *Log Source Management App Guide*.	7.4.0 or later
Use Case Manager Use the guided tips in Use Case Manager to help you ensure that JSA is optimally configured to accurately detect threats throughout the attack chain. Use Case Manager includes a rule explorer that offers flexible reports that are related to your rules. Use Case Manager also exposes pre-defined mappings to system rules and to help you map your own custom rules to MITRE ATT&CK tactics and techniques. For more information, see *Use Case Manager Guide*.	7.4.1 or later

2

CHAPTER

Getting Started with JSA Deployment

Getting Started with JSA Deployment

Before you can evaluate JSA key capabilities, an administrator must deploy JSA.

To deploy JSA, administrators must do the following tasks:

- Install the JSA appliance.
- Configure your JSA installation.
- Collect event, flow, and vulnerability assessment (VA) data.
- Tune your JSA installation.

Installing the JSA Appliance

Before you install the JSA appliance, ensure that the following requirements are met:

- The required hardware is installed. For more information, see the *Juniper Secure Analytics Installation Guide*.
- A keyboard and monitor are connected by using the VGA connection.
- You are logged in as the root user.

Administrators must install the JSA appliance to enable access to the user interface.

1. Access the software and documentation.
   a. Review the release notes for the JSA component that you want to install.
   b. Follow the instructions in the download document.
2. Review the information about the front and back panel features for appliances to confirm proper connectivity and functionality. For more information on front and back panel features for appliances, see the *Juniper Secure Analytics Hardware Guide*.

   On the back panel of each appliance type, the serial connector and Ethernet connectors can be managed by using the Integrated Management Module.
3. Install the JSA appliance.
   a. Create the **/media/cdrom** directory by typing the following command:

      mkdir /media/cdrom
   b. Mount the JSA ISO image by typing the following command:

mount -o loop <path_to_the_qradar_ISO> /media/cdrom

c. To begin the installation, type the following command:

/media/cdrom/setup

d. Select **Appliance Install** for the appliance type.

e. Select the appliance type from the list.

f. For the type of setup, select **normal**.

g. Set up the date and time.

h. Select the IP address type.

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

j. In the **IP address** field, enter a static IP address, or use the DHCP-assigned IP address.

> **NOTE**: For information about setting IPv6 primary or secondary host, see the *Juniper Secure Analytics High Availability Guide*.

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

l. Enter a `root` password that meets the following criteria:

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

m. Follow the instructions in the installation wizard to complete the installation. The installation process might take several minutes.

4. Apply your license key.

a. Log in to JSA as the admin user: https://<*JSA_IP_address*>

b. Click the **Admin** tab.

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

d. Click **Upload License**, and upload your license key.

e. Select the license and click **Allocate System to License**.

f. From the list of licenses, select a license, and click **Allocate License to System**.

RELATED DOCUMENTATION

JSA Configuration

IN THIS SECTION

This topic includes:

JSA Configuration Procedure

By configuring JSA, you can review your network hierarchy and customize automatic updates.

1. Ensure that Java Runtime Environment (JRE) version 1.7 or IBM 64-bit Runtime Environment for Java V7.0 is installed on all desktop systems that you use to access the JSA product user interface.
2. Ensure that you are using a supported web browser.
3. Log in to the JSA user interface by typing the following URL with the IP address of the JSA console:

   https:// *IP Address*

Network Hierarchy

You can view different areas of your network that is organized by business function and prioritize threat and policy information according to business value risk.

JSA uses the network hierarchy to do the following tasks:

- Understand network traffic and view network activity.
- Monitor specific logical groups or services in your network, such as marketing, DMZ, or VoIP.
- Monitor traffic and profile the behavior of each group and host within the group.
- Determine and identify local and remote hosts.

When you develop your network hierarchy, consider the most effective method for viewing network activity. The network hierarchy does not need to resemble the physical deployment of your network. JSA supports any network hierarchy that can be defined by a range of IP addresses. You can base your network on many different variables, including geographical or business units.

The objects that are defined in your network hierarchy do not have to be physically in your environment. All logical network ranges belonging to your infrastructure must be defined as a network object.

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

Defining Your Network Hierarchy

A default network hierarchy that contains pre-defined network groups is included in JSA. You can edit the pre-defined network hierarchy objects, or you can create new network groups or objects.

Network objects are containers for Classless Inter-Domain Routing (CIDR) addresses. Any IP address that is defined in a CIDR range in the network hierarchy is considered to be a local address. Any IP address that is not defined in a CIDR range in the network hierarchy is considered to be a remote address. A CIDR can belong only to one network object, but subsets of a CIDR range can belong to another network object. Network traffic matches the most exact CIDR. A network object can have multiple CIDR ranges assigned to it.

Some of the default building blocks and rules in JSA use the default network hierarchy objects. Before you change a default network hierarchy object, search the rules and building blocks to understand how the object is used and which rules and building blocks might need adjustments after you modify the object. It is important to keep the network hierarchy, rules, and building blocks up-to-date to prevent false offenses.

1. On the navigation menu, click **Admin**.

2. In the **System Configuration** section, click **Network Hierarchy**.
3. From the menu tree on the **Network Views** window, select the area of the network in which you want to work.
4. To add network objects, click **Add** and complete the following fields:

Option	Description
Name	The unique name of the network object. **NOTE**: You can use periods in network object names to define network object hierarchies. For example, if you enter the object name D.E.F, you create a three-tier hierarchy with E as a subnode of D, and F as a subnode of E.
Group	The network group in which to add the network object. Select from the Group list, or click Add a New Group. **NOTE**: When you add a network group, you can use periods in network group names to define network group hierarchies. For example, if you enter the group name A.B.C, you create a three-tier hierarchy with B as a subnode of A, and C as a subnode of B.
IP/CIDR(s)	Type an IP address or CIDR range for the network object, and click Add. You can add multiple IP addresses and CIDR ranges.
Description	A description of the network object.
Country/Region	The country or region in which the network object is located.
Longitude and Latitude	The geographic location (longitude and latitude) of the network object. These fields are co-dependent.

Automatic Updates

Using JSA, you can either replace your existing configuration files or integrate the updated files with your existing files.

The JSA console must be connected to the Internet to receive updates. If your console is not connected to the Internet, you must configure an internal update server. For information about setting up an automatic update server, see the *Juniper Secure Analytics User Guide*.

Software update are available to download from the following website:https://support.juniper.net/support/downloads/.

Update files can include the following updates:

- Configuration updates, which include configuration file changes, vulnerability, QID map, and security threat information updates.
- DSM updates, which include corrections to parsing issues, scanner changes, and protocol updates.
- Major updates, which include items such as updated JAR files.
- Minor updates, which include items such as extra online help content or updated scripts.

Configuring Automatic Update Settings

You can customize the frequency of JSA updates, update types, server configuration, and backup settings.

You can select the **Auto Deploy** to automatically deploy updates. If **Auto Deploy** is not selected, then you must manually deploy changes, from the **Dashboard** tab, after updates are installed.

> **NOTE**: In high-availability (HA) environment, automatic updates aren't installed when a secondary host is active. The updates are installed only after the primary host become the active node.

You can select **Auto Restart Service** to allow automatic updates that require the user interface to restart. A user interface disruption occurs when the service restarts. Alternatively, you can manually install the updated from the **Check for Updates** window.

1. On the navigation menu, click **Admin**.
2. In the **System Configuration** section , click **Auto Update**.
3. Click **Change Settings**.
4. On the **Basic** tab, select the schedule for updates.
    a. 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**.

b. In the **DSM, Scanner, Protocol Updates** section, select an option to install updates.

c. In the **Major Updates** section, select an option for receiving major updates for new releases.

d. In the **Minor Updates** section, select an option for receiving patches for minor system issues.

e. If you want to deploy update changes automatically after updates are installed, select the **Auto Deploy** check box.

f. If you want to restart the user interface service automatically after updates are installed, select the **Auto Restart Service** check box.

5. Click the **Advanced** tab to configure the update server and backup settings.

a. In **Web Server** field, type the web server from which you want to obtain the updates.

b. In the **Directory field**, type the directory location on which the web server stores the updates.

The default directory is **autoupdates/**.

c. Optional: Configure the settings for 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.

d. 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. The minimum is one day and the maximum is 65535 years.

e. In the **Backup Location** field, type the location where you want to store backup files.

f. 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**.

6. Click **Save**.

Collecting Events

By collecting events, you can investigate the logs that are sent to JSA in real time.

To collect the events:

1. Click the **Admin** tab.
2. In the navigation pane, click **Data Sources >Events**.
3. Click the **Log Sources** icon.
4. In the JSA Log Source Management app, click **Log Sources**.
5. Review the list of log sources and make any necessary changes to the log source.

   For information about configuring log sources, see the *Juniper Secure Analytics Log Sources User Guide*.
6. Save your changes, and then close the app.

Collecting Flows

By collecting flows, you can investigate the network communication sessions between hosts.

To collect the flows:

1. Click the **Admin** tab.
2. In the navigation menu, click **Data Sources >Flows**.
3. Click the **Flow Sources** icon.
4. Review the list of flow sources and make any necessary changes to the flow sources.

   For more information about configuring flow sources, see the *Juniper Secure Analytics Administration Guide*.
5. Close the **Flow Sources** window.
6. On the **Admin** tab menu, click **Deploy Changes**.

Importing Vulnerability Assessment Information

By importing vulnerability assessment information, you identify active hosts, open ports, and potential vulnerabilities.

To import VA information:

1. Click the **Admin** tab.
2. In the navigation menu, click **Data Sources >Vulnerability**.
3. Click the **VA Scanners** icon.
4. On the toolbar, click **Add**.
5. Enter values for the parameters.

   The parameters depend on the scanner type that you want to add.

   > **NOTE**: The CIDR range specifies which networks JSA integrates into the scan results. For example, if you want to conduct a scan against the 192.168.0.0/16 network and specify 192.168.1.0/24 as the CIDR range, only results from the 192.168.1.0/24 range are integrated.

6. Click **Save**.
7. On the **Admin** tab menu, click **Deploy Changes**.
8. Click the **Schedule VA Scanners** icon, and then click **Add**.
9. Specify the criteria for how often you want the scan to occur.

   Depending on the scan type, the criteria includes how frequently JSA imports scan results or starts a new scan. You also must specify the ports to be included in the scan results.

10. Click **Save**.

RELATED DOCUMENTATION

JSA Tuning | 23

Installing the JSA Appliance | 14

JSA Tuning

IN THIS SECTION

This topic includes:

Configuring JSA Tuning

You can tune JSA to meet the needs of your environment.

Before you tune JSA, wait one day to enable JSA to detect servers on your network, store events and flows, and create offenses that are based on existing rules.

Administrators can perform the following tuning tasks:

- Optimize event and flow payload searches by enabling a payload index on the **Log Activity** and **Network Activity** property.
- Provide a faster initial deployment and easier tuning by automatically or manually adding servers to building blocks.
- Configure responses to event, flow, and offense conditions by creating or modifying custom rules.
- Ensure that each host in your network creates offenses that are based on the most current rules, discovered servers, and network hierarchy.

Payload Indexing

Use the **Quick Filter** function, which is available on the **Log Activity** and **Network Activity** tabs, to search event and flow payloads.

To optimize the **Quick Filter**, you can enable a payload index **Quick Filter** property.

Enabling payload indexing might decrease system performance. Monitor the index statistics after you enable payload indexing on the **Quick Filter** property.

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

Enabling Payload Indexing

You can optimize event and flow payload searches by enabling a payload index on the **Log Activity** and **Network Activity Quick Filter** property.

To enable the payload indexing:

1. Click the **Admin** tab.
2. In the **System Configuration section**, click **System Configuration**.
3. Click the **Index Management** icon.
4. In the **Quick Search** field, type **quick filter**:
5. Right-click the **Quick Filter** property that you want to index.
6. Click **Enable Index**.
7. Click **Save**, and then click **OK**.
8. Optional: To disable a payload index, choose one of the following options:
   - Click **Disable Index**.
   - Right-click a property and select **Disable Index** from the menu.

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

Servers and Building Blocks

JSA automatically discovers and classifies servers in your network, providing a faster initial deployment and easier tuning when network changes occur.

To ensure that the appropriate rules are applied to the server type, you can add individual devices or entire address ranges of devices. You can manually enter server types, that do not conform to unique protocols, into their respective Host Definition Building Block. For example, adding the following server types to building blocks reduces the need for further false positive tuning:

- Add network management servers to the **BB:HostDefinition: Network Management Servers** building block.
- Add proxy servers to the **BB:HostDefinition: Proxy Servers** building block.
- Add virus and Windows update servers to the **BB:HostDefinition: Virus Definition and Other Update Servers** building block.
- Add vulnerability assessment (VA) scanners to the **BB-HostDefinition: VA Scanner Source IP** building block.

The Server Discovery function uses the asset profile database to discover several types of servers on your network. The Server Discovery function lists automatically discovered servers and you can select which servers you want to include in building blocks.

For more information about discovering servers, see the *Juniper Secure Analytics Administration Guide*.

Using Building blocks, you can reuse specific rule tests in other rules. You can reduce the number of false positives by using building blocks to tune JSA and enable extra correlation rules.

Adding Servers to Building Blocks Automatically

The Server Discovery function uses the asset profile database to discover different server types that are based on port definitions. Then, you can select the servers to add to a server-type building block for rules.

1. Click **Assets** > **Server Discovery**.
2. In the **Server Type** list, select the server type that you want to discover.

   Keep the remaining parameters as default.
3. Click **Discover Servers**.
4. In the **Matching Servers** pane, select the checkbox of all servers you want to assign to the server role.

5. Click **Approve Selected Servers**.

> **NOTE**: You can right-click any IP address or host name to display DNS resolution information.

Adding Servers to Building Blocks Manually

If a server is not automatically detected, you can manually add the server to its corresponding Host Definition Building Block.

To add servers to building blocks manually:

1. Click the **Offenses** tab.
2. In the navigation pane, click **Rules**.
3. In the **Display** list, select **Building Blocks**.
4. In the **Group** list, select **Host Definitions**.

   The name of the building block corresponds with the server type. For example, **BB:HostDefinition: Proxy Servers** applies to all proxy servers in your environment.
5. To manually add a host or network, double-click the corresponding Host Definition Building Block appropriate to your environment.
6. In the **Building Block** field, click the underlined value for the source or destination IP address.
7. In the **Enter an IP address or CIDR** field, type the host names or IP address ranges that you want to assign to the building block.
8. Click **Add** > **Submit**.
9. Click **Finish**.
10. Repeat Step "1" on page 26 to "9" on page 26 for each server type that you want to add.

Configuring Rules

From the **Log Activity**, **Network Activity**, and **Offenses tab**, you can configure rules or building blocks.

To configure rules:

1. Click the **Offenses** tab.
2. Double-click the offense that you want to investigate.
3. Click **Display >Rules**.
4. Double-click a rule.

   You can further tune the rules. For more information about tuning rules, see the *Use Case Manager Guide*
5. Close the Rules wizard.

   The **Creation Date** property changes to the date and time when you last updated a rule.
6. In the **Rules** page, click **Actions**.
7. Optional: If you want to prevent the offense from being removed from the database after the offense retention period is elapsed, select **Protect Offense**.
8. Optional: If you want to assign the offense to a JSA user, select **Assign**.

Cleaning the SIM Data Model

Clean the SIM data model to ensure that each host creates offenses that are based on the most current rules, discovered servers, and network hierarchy.

To clean the SIM model

1. Click the **Admin** tab.
2. On the toolbar, select **Advanced >Clean SIM Model**.
3. Select an option:
   - **Soft Clean** to set the offenses to inactive.
   - **Soft Clean** with the optional **Deactivate all offenses** check box to close all offenses.
   - **Hard Clean** to erase all entries.
4. Select the **Are you sure you want to reset the data model** checkbox.
5. Click **Proceed**.
6. After the SIM reset process is complete, refresh your browser.

When you clean the SIM model, all existing offenses are closed. Cleaning the SIM model does not affect existing events and flows.

RELATED DOCUMENTATION

Installing the JSA Appliance | 14

JSA Configuration | 16

3
CHAPTER

Getting Started in JSA

Getting Started in JSA

To get started in JSA, learn about investigating offenses, creating reports, and searching events, flows, and assets.

For example, you can search information by using default saved searches in the **Log Activity** and **Network Activity** tabs. You can also create and save your own custom searches.

Administrators can perform the following tasks:

- Search event data by using specific criteria and display events that match the search criteria in a results list. Select, organize, and group the columns of event data.
- Visually monitor and investigate flow data in real time, or perform advanced searches to filter the displayed flows. View flow information to determine how and what network traffic is communicated.
- View all the learned assets or search for specific assets in your environment.
- Investigate offenses, source and destination IP addresses, and network behaviors.
- Edit, create, schedule, and distribute default or custom reports.

Getting Started for Administrators

If you're an administrator, the following topics are a good place to get started to learn how to use JSA in your everyday workflow.

Administration

Do you know how the Network Hierarchy impacts the JSA deployment?

- **Network hierarchy**

  You can view different areas of your network that is organized by business function and prioritize threat and policy information according to business value risk.

- **Defining your network hierarchy**

  A default network hierarchy that contains pre-defined network groups is included in JSA. You can edit the pre-defined network hierarchy objects, or you can create new network groups or objects.

Do you know how to create integrations with IBM solutions such as Guardium and AppScan?

- **IBM Guardium integration**

IBM Guardium is a database activity and audit tracking tool for system administrators to retrieve detailed auditing events across database platforms.

- **AppScan Enterprise integration**

  JSA retrieves HCL AppScan Enterprise reports with the Representational State Transfer (REST) web service to import vulnerability data and generate offenses for your security team.

Do you know how to configure multiple log source groups for filtering, rules, and reporting?

- **Adding multiple log sources at the same time**

  Use the JSA Log Source Management app to add multiple log sources to JSA at the same time. You can add as many log sources as you want.

- **Editing multiple log sources at the same time**

  In the JSA Log Source Management app, view and edit a number of log sources at the same time. You can edit the settings of up to 1000 log sources at one time. Edit multiple log sources at the same time when the log sources have similar settings that you want to change, instead of editing each log source individually.

Do you know how to quantify and prioritize data sources in your environment to ensure adequate data collection?

- **Data collection**

  JSA accepts information in various formats and from a wide range of devices, including security events, network traffic, and scan results. Collected data is categorized into three major sections: events, flows, and vulnerability assessment (VA) information.

- **Adding a managed host**

  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.

APIs

Do you know how to create an authorization token for services to be used for remote access?

- **Managing authorized services**

  You can configure authorized services to authenticate an API call for your JSA deployment. The JSA RESTful API uses authorized services to authenticate API calls to the JSA Console. You can add or revoke an authorized service at any time.

- **Creating an authentication token for WinCollect agents**

Third-party or external applications that interact with JSA require an authentication token. Before you install managed WinCollect agents in your network, you must create an authentication token.

Backup and restore

Do you know how the backup and recovery functions are configured?

- **Backup and recovery**

  You can use the backup and recovery feature to back up your event and flow data; however, you must restore event and flow data manually.

- **Backup configurations and data**

  By default, JSA creates a backup archive of your configuration information daily at 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, as required.

High Availability/Disaster Recovery

Do you know how to create an HA cluster, and how to implement HA nodes in JSA, including moving online/offline?

- **HA overview**

  If your hardware or network fails, JSA can continue to collect, store, and process event and flow data by using high-availability (HA) appliances.

- **Creating an HA cluster**

  Pairing a primary host, secondary high-availability (HA) host, and a virtual IP address creates an HA cluster.

- **Setting an HA host online**

  You can set the primary or secondary HA host to Online.

- **Setting an HA host offline**

  You can set the primary or secondary high-availability (HA) host to **Offline** from the **Active** or **Standby** state.

License management

Do you know how to measure license allocation vs. usage and ensure adequate coverage?

- **License management**

License keys entitle you to specific JSA products, and control the event and flow capacity for your JSA deployment. You can add licenses to your deployment to activate other JSA products, such as JSA Vulnerability Manager.

- **Burst handling**

  JSA uses burst handling to ensure that no data is lost when the system exceeds the allocated events per second (EPS) or flows per minute (FPM) license limits.

- **Distributing event and flow capacity**

  Use the License Pool Management window to ensure that the events per second (EPS) and flows per minute (FPM) that you are entitled to is fully used. Also, ensure that JSA is configured to handle periodic bursts of data without dropping events or flows, or having excessive unused EPS and FPM.

Log sources

Do you know how to create a new log source?

- **Adding log sources manually**

  You can manually add log sources that JSA does not detect automatically.

- **Adding a log source**

  Use the JSA Log Source Management app to add new log sources to receive events from your network devices or appliances.

Do you know how to add Log Sources by using non-Syslog protocols, such as OpSec LEA?

- **Configuring an OPSEC/LEA log source**

  To integrate Check Point OPSEC/LEA with JSA, you must create two Secure Internal Communication (SIC) files and enter the information in to JSA as a Check Point log source.

Reference data and building blocks

Do you know how to adjust building block and reference set content to effectively tune JSA rules?

- **Review building blocks**

  Building blocks are a reusable set of rule tests that can be used within rules when required. Host definition building blocks (BB:HostDefinition) categorize assets and server types into CIDR/IP ranges. By populating host definition building blocks, JSA can identify the type of appliance that belongs to an address or address range. These building blocks can then be used in rules to exclude or include entire asset categories in rule tests.

Rules

Do you know how to run correlation rules in "test mode" to avoid excessive offense generation?

- **Configuring an event or flow as false positive**

  You might have legitimate network traffic that triggers false positive flows and events that make it difficult to identify true security incidents. You can prevent events and flows from correlating into offenses by configuring them as false positives.

- **Creating a custom rule**

  JSA includes rules that detect a wide range of activities, including excessive firewall denies, multiple failed login attempts, and potential botnet activity. You can also create your own rules to detect unusual activity.

Threat intelligence

Do you know how to use native X-Force threat feed data to enhance corporate security and visibility?

- **Enabling X-Force Threat Intelligence in JSA**

  By enabling X-Force Threat Intelligence in JSA, you can receive feeds of the X-Force Threat Intelligence information to your console.

Troubleshooting

Do you know how to collect logs from the JSA deployment to help support troubleshoot issues?

- **Collecting log files**

  JSA log files contain detailed information about your deployment, such as hostnames, IP addresses, and email addresses. If you need help with troubleshooting, you can collect the log files and send them to Juniper Customer Support.

Getting Started for Architects

If you're an architect, the following topics are a good place to get started to learn how to use JSA in your everyday workflow.

Architecture

Do you understand the distributed architecture and the roles of various components of JSA?

- **JSA architecture overview**

  JSA is a modular architecture that provides real-time visibility of your IT infrastructure, which you can use for threat detection and prioritization. You can scale JSA to meet your log and flow collection, and analysis needs. You can add integrated modules to your JSA platform, such as JSA Risk Manager, and JSA Vulnerability Manager.

- **JSA components**

  Use JSA components to scale a deployment, and to manage data collection and processing in distributed networks.

- **JSA events and flows**

  The core functions of JSA are managing network security by monitoring flows and events. A significant difference between event and flow data is that an event, which typically is a log of a specific action such as a user login, or a VPN connection, occurs at a specific time and the event is logged then. A flow is a record of network activity that can last for seconds, minutes, hours, or days, depending on the activity within the session.

Do you know how to scope an environment for architectural requirements, data rates, and retention policies to optimally build a JSA deployment?

- **Data retention**

  Retention buckets define how long event and flow data is retained in JSA. As JSA receives events and flows, each one is compared against the retention bucket filter criteria. When an event or flow matches a retention bucket filter, it is stored in that retention bucket until the deletion policy time period is reached. The default retention period is 30 days; then, the data is immediately deleted.

- **Distributing event and flow capacity**

  Use the License Pool Management window to ensure that the events per second (EPS) and flows per minute (FPM) that you are entitled to is fully used. Also, ensure that JSA is configured to handle periodic bursts of data without dropping events or flows, or having excessive unused EPS and FPM.

Flow sources

Do you know how to determine which network segments are reporting to JSA?

- **Guidelines for defining your network hierarchy**

  Building a network hierarchy in JSA is an essential first step in configuring your deployment. Without a configured network hierarchy, JSA cannot determine flow directions, build a reliable asset database, or benefit from useful building blocks in rules.

- **Defining your network hierarchy**

  A default network hierarchy that contains pre-defined network groups is included in JSA. You can edit the pre-defined network hierarchy objects, or you can create new network groups or objects.

Getting Started for Security Analysts

If you're a security analyst, the following topics are a good place to get started to learn how to use JSA in your everyday workflow.

Offense Workflow

Do you understand offense elements such as magnitude, hosts, users, involved?

- **Offense prioritization**

  The magnitude rating of an offense is a measure of the importance of the offense in your environment. JSA uses the magnitude rating to prioritize offenses and help you to determine which offenses to investigate first.

- **Managed hosts**

  For greater flexibility over data collection and event and flow processing, build a distributed JSA deployment by adding non-console managed hosts, such as collectors, processors, and data nodes.

- **Assigning offenses to users**

  By default, all new offenses are unassigned. You can assign an offense to a JSA user for investigation.

Do you know how to investigate an offense, including viewing related events and flows?

- **Offense investigations**

  JSA uses rules to monitor the events and flows in your network to detect security threats. When the events and flows meet the test criteria that is defined in the rules, an offense is created to show that a security attack or policy breach is suspected.

- **Network activity monitoring**

  Visually monitor and investigate flow data in real time, or conduct advanced searches to filter the displayed flows. A flow is a communication session between two hosts.

- **Log activity monitoring**

  JSA displays events in streaming mode so that you to view events in real time.

Searching and filtering

Do you know how to use columns (such as **Event Name, Username**) to show events grouped by one of those properties?

- **Creating a customized search**

You can search for data that matches your criteria by using more specific search options. For example, you can specify columns for your search, which you can group and reorder to more efficiently browse your search results.

Do you know how to use the Quick Filter to search the events for keywords?

- **Quick filter search options**

  Search event and flow payloads by typing a text search string that uses simple words or phrases.

- **Enabling quick filtering**

  You can enable the **Quick Filter** property to optimize event and flow search times. You can use the **Quick Filter** option to search event and flow payloads by typing free text search criteria.

Do you know how to save search criteria for future use, scheduling, or dashboarding?

- **Saving search criteria**

  You can save configured search criteria so that you can reuse the criteria and use the saved search criteria in other components, such as reports. Saved search criteria does not expire.

Do you know how to specify content requirements for searches?

- **Creating a customized search**

  You can search for data that matches your criteria by using more specific search options. For example, you can specify columns for your search, which you can group and reorder to more efficiently browse your search results.

Do you know how to create time series charts?

- **Creating a time series chart in JSA Pulse dashboard app**

  Time series charts in the JSA Pulse dashboard app illustrate data points at successive intervals of time. You use a time series chart to show trending or comparisons.

- **Configuring a time series chart in JSA**

  You can display interactive time series charts that represent the records that are matched by a specific time interval search.

Reporting and dashboards

Do you know how to generate a JSA published report with preexisting content?

- **Manually generating a report**

  A report can be configured to generate automatically; however, you can manually generate a report at any time.

- **Creating custom reports**

  Use the Report wizard to create and customize a new report. The Report wizard provides a step-by-step guide on how to design, schedule, and generate reports.

Do you know how to modify a dashboard's properties to what you want to visualize?

- **Creating Pulse dashboard items from an AQL data source**

  You can use Ariel Query Language (AQL) statements to create dashboard items. AQL is a structured query language that you use to extract, filter, and manipulate event and flow data that you extract from the Ariel database in JSA.

Do you know how to use saved search criteria to create custom dashboard items?

- **Creating a custom dashboard**

  You can create a custom dashboard to view a group of dashboard items that meet a particular requirement.

Rules

Do you know how to determine which rules are associated with a specific log or flow record?

- **Investigating threats in JSA**

  JSA uses rules to monitor the events and flows in your network to detect security threats. When the events and flows meet the test criteria that is defined in the rules, an offense is created to show that a security attack or policy breach is suspected. But knowing that an offense occurred is only the first step; identifying how it happened, where it happened, and who did it, requires some investigation.

- **Investigating rules with the JSA Use Case Manager app**

  Tune your rules by filtering different properties to ensure that the rules are defined and working as intended, including log source coverage. Determine which rules you might need to edit in JSA or investigate further in JSA Use Case Manager.

DSMs and uDSMs

Do you know how to view raw log data versus normalized metadata in logs and flow records?

- **Viewing raw events**

  An event is a record from a log source, such as a firewall or router device, that describes an action on a network or host. You can view raw event data, which is the unparsed event data from the log source.

- **Viewing normalized events**

Events are collected in raw format, and then normalized for display. Normalization involves parsing raw event data and preparing the data to display readable information about the tab. When events are normalized, the system normalizes the names as well.

Searching Events

You can search for all authentication events that JSA received in the last 6 hours.

To search an event:

1. Click the **Log Activity** tab.
2. On the toolbar, select **Search >New Search**.
3. In the **Time Range** pane, define the time range for the event search:
   a. Click **Recent**.
   b. In the **Recent** list, select **Last 6 Hours**.
4. In the **Search Parameters** pane, define the search parameters:
   a. In the first list, select **Category [Indexed]**.
   b. In the second list, select **Equals to**.
   c. In the **High Level Category** list, select **Authentication**.
   d. In the **Low Level Category** list, accept the default value of **Any**.
   e. Click **Add Filter**.
5. In the **Column Definition** pane, select **Event Name** in the **Display** list and drag it to the **Columns** list.
6. Click **Search**.

RELATED DOCUMENTATION

Saving Event Search Criteria | 40

Configuring a Time Series Chart | 40

Searching Flows | 41

Saving Event Search Criteria

You can save configured search criteria so that you can reuse the criteria and use the saved search criteria in other components, such as reports. Saved search criteria does not expire.

To save the event search criteria:

1. Click the **Log Activity** tab.
2. On the toolbar, click **Save Criteria**.
3. In the **Search Name** field, type **Example Search 1**.
4. In the **Timespan options** pane, click **Recent**.
5. In the **Recent** list, select **Last 6 Hours**.
6. Click **Include in my Quick Searches**.
7. Click **Include in my Dashboard**.

   If **Include in my Dashboard** is not displayed, click **Search >Edit Search** to verify that you selected **Event Name** in the **Column Definition** pane.
8. Click **OK**.

Configure a time series chart. For more information, see "Configuring a Time Series Chart" on page 40.

RELATED DOCUMENTATION

Configuring a Time Series Chart

You can display interactive time series charts that represent the records that are matched by a specific time interval search.

To configure the time series chart:

1. In the chart title bar, click the **Configure** icon.
2. In the **Value to Graph** list, select **Destination IP (Unique Count)**.
3. In the **Chart Type** list, select **Time Series**.

4. Click **Capture Time Series Data**.
5. Click **Save**.
6. Click **Update Details**.
7. Filter your search results:
   a. Right-click the event that you want to filter.
   b. Click **Filter on Event Name is <Event Name>**.
8. To display the event list that is grouped by the user name, select **Username** from the **Display** list.
9. Verify that your search is visible on the **Dashboard** tab:
   a. Click the **Dashboard** tab.
   b. Click the **New Dashboard** icon.
   c. In the **Name** field, type **Example Custom Dashboard**.
   d. Click **OK**.
   e. In the **Add Item** list, select **Log Activity >Event Searches >Example Search 1**.

The results from your saved event search display in the Dashboard.

RELATED DOCUMENTATION

Searching Flows | 41
Saving Flow Search Criteria | 42
Creating a Dashboard Item | 43

Searching Flows

You can search, monitor, and investigate flow data in real time. You can also run advanced searches to filter the displayed flows. View flow information to determine how and what network traffic is communicated.

To search flows:

1. Click the **Network Activity** tab.
2. On the toolbar, click **Search >New Search**.
3. In the **Time Range** pane, define the flow search time range:
   a. Click **Recent**.

   b. In the **Recent** list, select **Last 30 Minutes**.
4. In the **Search Parameters** pane, define your search criteria.
   a. In the first list, select **Flow Direction**.
   b. In the second list, select **Equals**.
   c. In the third list, select **R2L**.
   d. Click **Add Filter**.
5. In the **Display** list in the **Column Definition** pane, select **Application**.
6. Click **Search**.

All flows with a flow direction of remote to local (R2L) in the last 30 minutes are displayed, grouped, and sorted by the **Application** field.

RELATED DOCUMENTATION

Saving Flow Search Criteria | 42
Creating a Dashboard Item | 43
Searching Assets | 43

Saving Flow Search Criteria

You can save specified flow search criteria for future use.

To save the flow search criteria:

1. On the **Network Activity** tab toolbar, click **Save Criteria**.
2. In the **Search Name** field, type the name **Example Search 2**.
3. In the **Recent** list, select **Last 6 Hours**.
4. Click **Include in my Dashboard** and **Include in my Quick Searches**.
5. Click **OK**.

Create a dashboard item. For more information, see "Creating a Dashboard Item" on page 43.

RELATED DOCUMENTATION

Creating a Dashboard Item | 43

Creating a Dashboard Item

You can create a dashboard item by using saved flow search criteria.

To create a dashboard item:

1. On the **Network Activity** toolbar, select **Quick Searches >Example Search 2**.
2. Verify that your search is included in the Dashboard:
   a. Click the **Dashboard** tab.
   b. In the **Show Dashboard** list, select **Example Custom Dashboard**.
   c. In the **Add Item** list, select **Flow Searches >Example Search 2**.
3. Configure your dashboard chart:
   a. Click the **Settings** icon.
   b. Using the configuration options, change the value that is graphed, how many objects are displayed, the chart type, or the time range that is displayed in the chart.
4. To investigate flows that are currently displayed in the chart, click **View in Network Activity**.

The **Network Activity** page displays results that match the parameters of your time series chart. For more information on time series charts, see *JSA User Guide*.

RELATED DOCUMENTATION

Searching Assets

You can search host profiles, assets, and identity information. Identity information provides more details, such as DNS information, user logins, and MAC addresses on your network.

When you access the **Assets** tab, the **Asset** page is displayed populated with all discovered assets in your network. To refine this list, you can configure search parameters to display only the asset profiles you want to investigate.

To search the assets:

1. Click the **Assets** tab.
2. In the navigation pane, click **Asset Profiles**.
3. On the toolbar, click **Search >New Search**.
4. If you want to load a saved search, complete the following steps:
   a. In the **Group** list, select the asset search group that you want to display in the **Available Saved Searches** list.
   b. Choose one of the following options:
      - In the **Type Saved Search or Select from List** field, type the name of the search you want to load.
      - In the **Available Saved Searches** list, select the saved search that you want to load.
   c. Click **Load**.
5. In the **Search Parameters** pane, define your search criteria:
   a. In the first list, select the asset parameter that you want to search for.

      For example, **Hostname**, **Vulnerability Risk Classification**, or **Technical Owner**.
   b. In the second list, select the modifier that you want to use for the search.
   c. In the **Entry** field, type specific information that is related to your search parameter.
   d. Click **Add Filter**.
   e. Repeat these steps for each filter that you want to add to the search criteria.
6. Click **Search**.

You receive a notification that CVE ID: CVE-2010-000 is being actively exploited. To determine whether any hosts in your deployment are vulnerable to this exploit, complete the following steps:

1. From the list of search parameters, select **Vulnerability External Reference**.
2. Select **CVE**.
3. To view a list of all hosts that are vulnerable to that specific CVE ID, type the following command:

   2010-000

For more information, see the Open Source Vulnerability Database and the National Vulnerability Database.

RELATED DOCUMENTATION

Offense Investigations

IN THIS SECTION

JSA can correlate events and flows with destination IP addresses located across multiple networks in the same offense and the same network incident. You can effectively investigate each offense in your network.

Using the **Offenses** tab, you can investigate offenses, source and destination IP addresses, network behaviors, and anomalies on your network.

Viewing Offenses

You can investigate offenses, source and destination IP addresses, and network behaviors.

1. Click the **Offenses** tab.
2. Double-click the offense that you want to investigate.
3. On the toolbar, select **Display >Destinations**.

   You can investigate each destination to determine whether the destination is compromised or exhibiting suspicious behavior.

4. On the toolbar, click **Events**.

The **List of Events** window displays all events that are associated with the offense. You can search, sort, and filter events.

RELATED DOCUMENTATION

Example: Enabling the PCI Report Templates | 46

Example: Creating a Custom Report Based on a Saved Search | 47

Searching Assets | 43

Example: Enabling the PCI Report Templates

Using the **Reports** tab, you can enable, disable, and edit report templates.

Enable the Payment Card Industry (PCI) report templates.

To enable the PCI report templates:

1. Click the **Reports** tab.
2. Clear the **Hide Inactive Reports** check box.
3. In the **Group** list, select **Compliance >PCI**.
4. Select all report templates on the list:
5. In the **Actions** list, select **Run Report**.
6. Access generated reports:
   a. From the list in the **Generated Reports** column, select the time stamp of the report that you want to view.
   b. In the **Format** column, click the icon for report format that you want to view.

RELATED DOCUMENTATION

Example: Creating a Custom Report Based on a Saved Search | 47

Searching Assets | 43

Offense Investigations | 45

Example: Creating a Custom Report Based on a Saved Search

You can create reports by importing a search or creating custom criteria.

Create a report that is based on the event and flow searches you created in "Searching Events" on page 39.

To create a custom report based on saved search:

1. Click the **Reports** tab.
2. In the **Actions** list, select **Create**.
3. In the report wizard, click **Next**.
4. Configure the report schedule.
   a. Select the **Daily** option.
   b. Select the **Monday, Tuesday, Wednesday, Thursday, and Friday** options.
   c. Select **8:00 AM**.
   d. Make sure that the **Yes - Manually generate report** option is selected.
   e. Click **Next**.
5. Configure the report layout:
   a. In the **Orientation** list, select **Landscape**.
   b. Select the layout with two chart containers.
   c. Click **Next**.
6. In the **Report Title** field, type **Sample Report**.
7. Configure the top chart container:
   a. In the **Chart Type** list, select **Events/Logs**.
   b. In the **Chart Title** field, type **Sample Event Search**.
   c. In the **Daily Scheduling** section, select **All data from the previous (24 hours)**.
   d. In the **Graph Type** list, select **Stacked Bar**.
   e. In the **Limit Events/Logs To Top** list, select **10**.
   f. In the **Available Saved Searches** list, select **Example Search 1**.

The remaining parameters automatically populate by using the settings from the **Example Search 1** saved search.

g. Click **Save Container Details**.

8. Configure the bottom chart container:
   a. In the **Chart Type** list, select **Flows**.
   b. In the **Chart Title** field, type **Sample Flow Search**.
   c. Click **All data from previous 24 hours**.
   d. In the **Graph Type** list, select **Stacked Bar**.
   e. In the **Limit Flows To Top** list, select **10**.
   f. In the **Available Saved Searches** list, select **Example Search 2**.

      The remaining parameters are automatically populated by using the settings from the **Example Search 2** saved search.

   g. Click **Save Container Details**.
9. Click **Next**.
10. Click **Next**.
11. Choose the report format:
    a. Click the **PDF and HTML** check boxes.
    b. Click **Next**.
12. Choose the report distribution channels:
    a. Click **Report Console**.
    b. Click **Email**.
    c. In the **Enter the report destination email address(es)** field, type your email address.
    d. Click **Include Report as attachment**.
    e. Click **Next**.
13. Complete the final Report wizard details:
    a. In the **Report Description** field, type a description of the template.
    b. Click **Yes - Run this report when the wizard is complete**.
    c. Click **Finish**.
14. Click **Sample Report** in the **Report Name** column, and click **Actions** > **Run Report**.
15. Using the list box in the **Generated Reports** column, select the time stamp of your report.

16. In the **Format** column, click the icon for the report format that you want to view.

RELATED DOCUMENTATION

Searching Assets | 43

Offense Investigations | 45

Example: Enabling the PCI Report Templates | 46