Juniper Secure Analytics Getting Started Guide

Release
7.3.1

Modified: 2018-07-31

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

Juniper Secure Analytics Getting Started Guide
7.3.1

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

Documentation Conventions

Table 1 on page viii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page viii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*

Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at https://www.juniper.net/documentation/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/documentation/feedback/.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: https://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at https://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://www.juniper.net/support/requesting-support.html.

CHAPTER 1

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.

To get started, configure a basic JSA installation, collect event and flow data, and generate reports.

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 event.
- Monitor log activity by using configurable time-series charts.
- Identify false positives to tune JSA.

Related Documentation

- Network Activity on page 14
- Assets on page 14
- Offenses on page 15

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.

Related Documentation

- Assets on page 14
- Offenses on page 15
- Reports on page 15

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.

Related Documentation

- Offenses on page 15
- Reports on page 15
- Data Collection on page 16

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.

Related Documentation

- Reports on page 15
- Data Collection on page 16
- JSA Rules on page 17

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.

Related Documentation

- Data Collection on page 16
- JSA Rules on page 17
- Supported Web Browsers on page 18

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.

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 about configuring DSMs, see the *Juniper Secure Analytics 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 about manually adding log sources, see the *Juniper Secure Analytics Log Sources User 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.

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.

Related Documentation

- JSA Rules on page 17
- Supported Web Browsers on page 18
- Reports on page 15

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 on page 18
- Reports on page 15
- Data Collection on page 16

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 3: Supported Web Browsers for JSA Products

Web browser	Supported versions
Mozilla Firefox	45.8 Extended Support Release
64-bit Microsoft Internet Explorer with Microsoft Edge mode enabled.	11.0, Edge 38.14393
Google Chrome	Latest

Related Documentation

- Reports on page 15
- Data Collection on page 16
- JSA Rules on page 17

CHAPTER 2

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

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

Before you install the JSA evaluation appliance, ensure that you have:

- Space for a two-unit appliance.
- Rack rails and shelving (mounted).
- Optional: a USB keyboard and standard VGA monitor for console access.

1. Connect the management network interface to the port labeled Ethernet 1.
2. Plug the dedicated power connections into the rear of the appliance.
3. If you need console access, connect the USB keyboard and standard VGA monitor.

4. If the appliance has a front panel, remove the panel by pushing in the tabs on either side and pulling the panel away from the appliance.

5. Power on the appliance.

Related Documentation

- The JSA Appliance on page 20
- JSA Configuration on page 20
- JSA Tuning on page 26

The JSA Appliance

The JSA evaluation appliance is a two-unit rack mount server. Rack rails or shelving are not provided with evaluation equipment.

The JSA appliance includes four network interfaces. For this evaluation, use the interface that is labeled Ethernet 1 as the management interface.

You can use the three remaining monitoring interfaces for flow collection. The JSA flow processor provides full network application analysis and can perform packet captures on the beginning of each conversation. Depending on the JSA appliance, flow analysis automatically begins when a span port or tap is connected to any interface other than Ethernet 1. Extra steps might be required to enable the JSA flow processor component within JSA.

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

NOTE: **The JSA evaluation appliance has a 50 Mbps limit for flow analysis. Ensure that the aggregate traffic on the monitoring interfaces for flow collection does not exceed 50 Mbps.**

Related Documentation

- JSA Configuration on page 20
- JSA Tuning on page 26
- Installing the JSA Appliance on page 19

JSA Configuration

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. If you use Internet Explorer, enable document mode and browser mode.
   a. In your Internet Explorer web browser, press F12 to open the **Developer Tools** window.
   b. Click **Browser Mode** and select the version of your web browser.
   c. Click **Document Mode** and select **Internet Explorer 7.0 Standards**.
4. 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.

For evaluation purposes, a default network hierarchy is included that contains predefined logical groups. Review the network hierarchy for accuracy and completeness. If your environment includes network ranges that are not displayed in the pre-configured network hierarchy, you must add them manually.

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.

NOTE: If your system does not include a completed network hierarchy, then use the **Admin** tab to create a hierarchy specific to your environment.

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

Reviewing Your Network Hierarchy

You can review your network hierarchy.

1. Click the **Admin** tab.
2. In the navigation pane, click **System Configuration**.
3. Click the **Network Hierarchy** icon.
4. In the **Name** column, expand **Regulatory_Compliance_Servers**.

   If your network hierarchy does not include a regulatory compliance server component, you can use your Mail component for the remainder of this procedure.
5. Click the nested **Regulatory_Compliance_Servers**.
6. Click the **Edit** icon.
7. To add compliance servers, follow these steps:
   a. In the **IP/CIDR(s)** field, type the IP address or CIDR range of your compliance servers.
   b. Click the **(+)** icon.
   c. Repeat for all compliance servers.
   d. Click **Save**.
   e. Repeat this process for any other networks that you want to edit.
8. On the **Admin** tab menu, click **Deploy Changes**.

   You can automatically or manually update your configuration files with the latest network security information. JSA uses system configuration files to provide useful characterizations of network data flows.

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://www.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.

1. Click the **Admin** tab.
2. In the navigation pane, click **System Configuration**.
3. Click the **Auto Update** icon.
4. In the navigation pane, click **Change Settings**.
5. Select the **Basic** tab.
6. In the **Auto Update Schedule** pane, accept the default parameters.
7. In the **Update Types** pane, configure the following parameters:
   a. In the **Configuration Updates** list box, select **Auto Update**.
   b. Accept the default values for the following parameters:
      - **DSM, Scanner, Protocol Updates**
      - **Major Updates**
      - **Minor Updates**
8. Clear the **Auto Deploy** check box.

By default, the check box is selected. If the check box is not selected, a system notification is displayed on the **Dashboard** tab to indicate that you must deploy changes after updates are installed.

9. Click the **Advanced** tab.
10. In the **Server Configuration** pane, accept the default parameters.
11. In the **Other Settings** pane, accept the default parameters.
12. Click **Save** and close the **Updates** window.
13. On the toolbar, click **Deploy Changes**.

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. 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*.
5. Close the **Log Sources** window.
6. On the **Admin** tab menu, click **Deploy Changes**.

Collecting Flows

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

For more information about how to enable flows on third-party network devices, such as switches and routers, see your vendor documentation.

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.
9. Click **Add**.
10. 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.
11. Click **Save**.

Related Documentation

- JSA Tuning on page 26
- Installing the JSA Appliance on page 19
- The JSA Appliance on page 20

JSA Tuning

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 Quick Filter** 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 about index management and statistics, 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 navigation pane, click **System Configuration**.
3. Click the **Index Management** icon.
4. In the **Quick Search** field, type the following:

   quick filter
5. Right-click the **Quick Filter** property that you want to index.
6. Click **Enable Index**.
7. Click **Save**.
8. Click **OK**.
9. 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 detailed information about the parameters that are displayed in the **Index Management** window, 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

You can automatically add servers to building blocks.

1. Click the **Assets** tab.
2. In the navigation pane, click **Server Discovery**.
3. In the **Server Type** list, select the server type that you want to discover.

   Keep the remaining parameters as default.
4. Click **Discover Servers**.

5. In the **Matching Servers** pane, select the check box of all servers you want to assign to the server role.

6. 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 after the phrase **and when either the source or destination IP is one of the following**.

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**.

9. Click **Submit**.

10. Click **Finish**.

11. Repeat Step 1 to 10 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 *Juniper Secure Analytics Administration Guide*
5. Close the Rules wizard.
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. Check the **Are you sure you want to reset the data model?** box.

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 on page 19
- The JSA Appliance on page 20
- JSA Configuration on page 20

CHAPTER 3

Getting Started in JSA

Feature Overview 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.

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**.
   b. In the second list, select **Equals**.
   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.
6. Click **Search**.

Related Documentation

- Saving Event Search Criteria on page 34
- Configuring a Time Series Chart on page 35
- Searching Flows on page 36

Saving Event Search Criteria

You can save specified event search criteria for future use.

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 35.

Related Documentation

- Configuring a Time Series Chart on page 35
- Searching Flows on page 36
- Saving Flow Search Criteria on page 37

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 on page 36
- Saving Flow Search Criteria on page 37
- Creating a Dashboard Item on page 37

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 on page 37
- Creating a Dashboard Item on page 37
- Searching Assets on page 38

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 37.

Related Documentation

- Creating a Dashboard Item on page 37
- Searching Assets on page 38
- Offense Investigations on page 39

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 on page 38
- Offense Investigations on page 39
- Example: Enabling the PCI Report Templates on page 40

Searching Assets

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.

Use the search feature to search host profiles, assets, and identity information. Identity information provides more details, such as DNS information, user logins, and MAC addresses on your network.

For example:

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, do 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, do 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 on page 39
- Example: Enabling the PCI Report Templates on page 40
- Example: Creating a Custom Report Based on a Saved Search on page 41

Offense Investigations

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

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.

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 on page 40
- Example: Creating a Custom Report Based on a Saved Search on page 41
- Searching Assets on page 38

Example: Enabling the PCI Report Templates

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

Enable 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:
   a. Click the first report on the list.
   b. Select all report templates by holding down the Shift key, while you click the last report on the list.
5. In the **Actions** list, select **Toggle Scheduling**.
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 on page 41
- Searching Assets on page 38
- Offense Investigations on page 39

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 34.

To create a custom report based on saved search:

1. Click the **Reports** tab.
2. In the **Actions** list, select **Create**.
3. Click **Next**.
4. Configure the report schedule.
   a. Select the **Daily** option.
   b. Select the **Monday, Tuesday, Wednesday, Thursday, and Friday** options.
   c. Using the lists, select **8:00** and **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 **Limit Events/Logs To Top** list, select **10**.
   d. In the **Graph Type** list, select **Stacked Bar**.
   e. Click **All data from the previous (24 hours)**.
   f. In the **Base this event report on** 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. In the **Limit Flows To Top** list, select **10**.
   d. In the **Graph Type** list, select **Stacked Bar**.
   e. Click **All data from the previous 24 hours**.
   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. Using the list box in the **Generated Reports** column, select the time stamp of your report.

Related Documentation

- Searching Assets on page 38
- Offense Investigations on page 39

- Example: Enabling the PCI Report Templates on page 40

