Juniper Secure Analytics

Troubleshooting Guide

Release
2014.2

Published: 2014-07-15

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Secure Analytics Troubleshooting Guide

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 http://www.juniper.net/support/eula.html. 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 http://www.juniper.net/techpubs/.

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 http://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 at the Juniper Networks Technical Documentation site at http://www.juniper.net/techpubs/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/cgi-bin/docbugreport/.

- 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 JNASC 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 http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://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: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

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 http://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 http://www.juniper.net/support/requesting-support.html.

PART 1

Troubleshooting System Notifications

CHAPTER 1

Troubleshooting JSA System Notifications

Overview of Troubleshooting JSA System Notifications

Use the system notifications that are generated by Juniper Secure Analytics (JSA) to monitor the status and heath of your system. Software and hardware tools and processes continually monitor the JSA appliances and deliver information, warning, and error messages to users and administrators.

Related concepts:

Chapter 2 ,"Error Notifications for JSA Appliances" on page 5. Error notifications in JSA appliances require a response by the user or the administrator.

Chapter 3 ,"Information Notifications for JSA Appliance" on page 19. JSA provides information messages about the status or result of a process or action.

Chapter 4, "Warning Notifications for JSA Appliances" on page 23. JSA system health notifications are proactive messages of actual or impending software or hardware failures.

Related Documentation

- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6

CHAPTER 2

Error Notifications for JSA Appliances

Error notifications in Juniper Secure Analytics (JSA) appliances require a response by the user or the administrator.

Accumulator cannot Read the View Definition for Aggregate Data

Problem **Description: Accumulator: Cannot read the aggregated data view definition in order to prevent an out of sync problem. Aggregated data views can no longer be created or loaded. Time series graphs will no longer work as well as reporting.**

A synchronization issue occurred. The aggregate data view configuration that is in memory wrote erroneous data to the database.

To prevent data corruption, the system disables aggregate data views. When aggregate data views are disabled, time series graphs, saved searches, and scheduled reports display empty graphs.

Resolution

User Response

Contact Juniper Customer Support.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Automatic Update Error on page 6
- Auto Update Installed with Errors on page 6

Automatic Update Error

Problem

Description: Automatic updates could not complete installation. See the Auto Update Log for details.

The update process encountered an error or cannot connect to an update server. The system is not updated.

Resolution

User Response

Select one of the following options:

- Verify the automatic update history to determine the cause of the installation error.

  In the Admin tab, click the **Auto Update** icon and select **View Log**.

- Verify that your console can connect to the update server.

  In the Updates window, select **Change Settings**, then click the Advanced tab to view your automatic update configuration. Verify the address in the Web Server field to ensure that the automatic update server is accessible.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Auto Update Installed with Errors on page 6
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6

Auto Update Installed with Errors

Problem

Description: Automatic updates installed with errors. See the Auto Update Log for details.

The most common reason for automatic update errors is a missing software dependency for a DSM, protocol, or scanner update.

Resolution

User Response

Select one of the following options:

- In the Admin tab, click the Auto Update icon and select **View Update History** to determine the cause of the installation error. You can view, select, and then reinstall a failed RPM.
- If an auto update is unable to reinstall through the user interface, manually download and install the missing dependency on your console. The console replicates the installed file to all managed hosts.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6
- Backup Unable to Complete a Request on page 7

Backup Unable to Complete a Request

Problem

Description: Backup: Unable to Execute Backup Request.

A backup might fail for the following reasons:

- The system is unable to clean the backup replication synchronization table.
- The system is unable to delete a request.
- The system is unable to synchronize the backup by using the files on the disk.
- The NFS mounted backup directory is not available or has incorrect NFS export options (**no_root_squash**).
- Cannot initialize on-demand backup.
- Cannot retrieve configuration for the type of backup selected.
- Unable to initialize a scheduled backup.

Resolution

User Response

Manually start a backup to determine whether the failure reoccurs.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Automatic Update Error on page 6
- Auto Update Installed with Errors on page 6
- CRE Failed to Read Rules on page 8

CRE Failed to Read Rules

Problem

Description: The last attempt to read in rules (usually due to a rule change) has failed. Please see the message details and error log for information on how to resolve this.

The custom rules engine (CRE) on an Event Processor is unable to read a rule to correlate an incoming event. The notification might contain one of the following messages:

- If the CRE was unable to read a single rule, in most cases, a recent rule change is the cause. The payload of the notification message displays the rule or rule of the rule chain that is responsible.
- In rare circumstances, data corruption can cause a complete failure of the rule set. An application error is displayed and the rule editor interface might become unresponsive or generate more errors.

Resolution

User Response

For a single rule read error, review the following options:

- To locate the rule that is causing the notification, temporarily disable the rule.
- Edit the rule to revert any recent changes.
- Delete and re-create the rule that is causing the error.

NOTE: For application errors where the CRE failed to read rules, contact Juniper Customer Support.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6
- Auto Update Installed with Errors on page 6
- Backup Unable to Complete a Request on page 7

Disk Storage Unavailable

Problem

Description: Disk Sentry has detected that one or more storage partitions are not accessible.

The disk sentry did not receive a response within 30 seconds. A storage partition issue might exist, or the system might be under heavy load and not able to respond within the 30-second threshold.

Resolution

User Response

Select one of the following options:

- Verify the status of your /store partition by using the **touch** command.

  If the system responds to the **touch** command, the unavailability of the disk storage is likely due to system load.

- Determine whether the notification corresponds to dropped events.

  If events were dropped events and the disk storage is unavailable, event and flow queues might be full. Investigate the status of storage partitions.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6
- Auto Update Installed with Errors on page 6
- CRE Failed to Read Rules on page 8

Disk Failure

Problem

Description: Disk Failure: Hardware Monitoring has determined that a disk is in failed state.

On-board system tools detected that a disk failed. The notification message provides information about the failed disk and the slot or bay location of the failure.

Resolution

User Response

If the notification persists, contact Juniper Customer Support or replace parts.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6
- Disk Storage Unavailable on page 8
- CRE Failed to Read Rules on page 8

Event Pipeline Dropped Events

Problem

Description: Events/Flows were dropped by the event pipeline.

If there is an issue with the event pipeline or you exceed your license limits, an event or flow might be dropped.

NOTE: **Dropped events and flows cannot be recovered.**

Resolution

User response

Review the following options:

- Verify the incoming event and flow rates on your system. If the event pipeline is dropping events, expand your license to handle more data.
- Review the recent changes to rules or custom properties. Rule or custom property changes can cause changes to your event or flow rates and might affect system performance.
- Determine whether the issue is related to SAR notifications. SAR notifications might indicate queued events and flows are in the event pipeline. The system usually routes events to storage, instead of dropping the events.
- Tune the system to reduce the volume of events and flows that enter the event pipeline.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6
- Disk Storage Unavailable on page 8
- Disk Failure on page 9

Event Pipeline Dropped Connections

Problem

Description: Connections were dropped by the event pipeline.

A TCP-based protocol dropped an established connection to the system.

The number of connections that can be established by TCP-based protocols is limited to ensure that connections are established and events are forwarded. The event collection system (ECS) allows a maximum of 15,000 file handles and each TCP connection uses three file handles.

TCP protocols that provide drop connection notifications include the following protocols:

- TCP syslog protocol
- TLS syslog protocol
- TCP multiline protocol

Resolution

User Response

Review the following options:

- Distribute events to more appliances. Connections to other event and flow processors distribute the work load from the console.
- Configure low priority TCP log source events to use the UDP network protocol.
- Tune the system to reduce the volume of events and flows that enter the event pipeline.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6
- Disk Storage Unavailable on page 8
- Event Pipeline Dropped Events on page 9

External Scan Gateway Failure

Problem

Description: An invalid/unknown gateway IP address has been supplied to the external IBM hosted scanner, the scan has been stopped.

When an external scanner is added, a gateway IP address is required. If the address that is configured for the scanner in the deployment editor is incorrect, the scanner cannot access your external network.

Resolution

User Response

Select one of the following options:

- Review the configuration for any external scanners that are configured in the deployment editor to ensure that the gateway IP address is correct.
- Ensure that the external scanner can communicate through the configured IP address.
- Ensure that the firewall rules for your DMZ are not blocking communication between your appliance and the assets you want to scan.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6
- Disk Storage Unavailable on page 8
- Event Pipeline Dropped Connections on page 10

Failed to Install High Availability

Problem

Description: There was a problem installing High Availability on the cluster.

When you install a high availability appliance, the installation process links the primary and secondary appliances. The configuration and installation process contains a time interval to determine when an installation requires attention. The high availability installation exceeded the six-hour time limit.

NOTE: **No high availability protection is available until the issue is resolved.**

Resolution

User Response

Contact Juniper Customer Support.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6
- Disk Storage Unavailable on page 8
- External Scan Gateway Failure on page 11

Failed to Uninstall an High Availability Appliance

Problem

Description: There was a problem while removing High Availability on the cluster.

When you remove a high availability appliance, the installation process removes connections and data replication processes between the primary and secondary appliances. If the installation process cannot remove the high availability appliance from the cluster properly, the primary system continues to work normally.

Resolution

User Response

Try to remove the high availability appliance a second time.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6
- Disk Storage Unavailable on page 8
- Failed to Install High Availability on page 12

Filter Initialization Failed

Problem

Description: Traffic analysis filter failed to initialize.

If a configuration is not saved correctly, or if a configuration file is corrupted, the event collection service (ECS) might fail to initialize. If the traffic analysis process is not started, new log sources are not automatically discovered.

Resolution

User Response

Select one of the following options:

- Manually create log sources for any new appliances or event sources until traffic analysis process is working.

  All new event sources are classified as SIM Generic until they are mapped to a log source.

- If you get an automatic update error, review the automatic update log to determine whether an error occurred when a DSM or a protocol was installed.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6
- Disk Storage Unavailable on page 8
- Failed to Uninstall an High Availability Appliance on page 12

Insufficient Disk Space to Export Data

Problem

Description: Insufficient disk space to complete data export request.

If the export directory does not contain enough space, the export of event, flow, and offense data is canceled.

Resolution

User Response

Select one of the following options:

- Free some disk space in the **/store/exports** directory.
- Configure the Export Directory property in the System Settings window to use to a partition that has sufficient disk space.
- Configure an offboard storage device.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5

- Automatic Update Error on page 6
- Disk Storage Unavailable on page 8
- Filter Initialization Failed on page 13

Out of Memory Error

Problem

Description: Application ran out of memory.

When the system detects that no more memory or swap space is available, the application or service can stop working. Out of memory issues are caused by software, or user-defined queries and operations that exhaust the available memory.

Resolution

User Response

Review the error message that is written to the **/var/log/qradar.log** file. Restarting a service might stop the offending application or service and redistribute resources.

If you use Java Database Connectivity (JDBC) or the log file protocol to import many records from a log source, the system can use up resources. If multiple large data imports occur simultaneously, you can stagger the start time intervals.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6
- Disk Storage Unavailable on page 8
- Insufficient Disk Space to Export Data on page 13

Process Monitor Application Failed to Start Multiple Times

Problem

Description: Process Monitor: Application has failed to start up multiple times.

The system is unable to start an application or process on your system.

Resolution

User Response

Review your flow sources to determine whether a device stopped sending flow data or whether users deleted a flow source.

Either remove the flow process by using the deployment editor or assign a flow source to your flow data. On the Admin tab, click **Flow Sources**.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6

- Disk Storage Unavailable on page 8
- Out of Memory Error on page 14

Process Monitor Must Lower Disk Usage

Problem

Description: Process Monitor: Disk usage must be lowered.

The process monitor is unable to start processes because of a lack of system resources. The storage partition on the system is likely 95% full or greater.

Resolution

User Response

Free some disk space by manually deleting files or by changing your event or flow data retention policies. The system automatically restarts system processes when the used disk space falls below a threshold of 92% capacity.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6
- Disk Storage Unavailable on page 8
- Process Monitor Application Failed to Start Multiple Times on page 14

Primary High Availability System Failure

Problem

Description: Primary HA System Failure.

The primary system cannot communicate with the standby system because the primary system is unresponsive or failed. The secondary system takes over operations from the failed primary system.

Resolution

User Response

Review the following resolutions:

- Inspect the primary high availability appliance to determine whether it is powered down or experienced a hardware failure.
- Restore the primary system.

  Click the Admin tab and click **System and License Management**. From the High Availability menu, select **Restore System**.
- Review the **/var/log/qradar.log** file on the standby appliance to determine the cause of the failure.

- Use the ping command to check the communication between the primary and standby system.
- Check the switch that connects the primary and secondary high availability appliances. Verify the IPtables on the primary and secondary appliances.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6
- Disk Storage Unavailable on page 8
- Process Monitor Must Lower Disk Usage on page 15

Predictive Disk Failure

Problem

Description: Predictive Disk Failure: Hardware Monitoring has determined that a disk is in predictive failed state.

The system monitors the status of the hardware on an hourly basis to determine when hardware support is required on the appliance.

The on-board system tools detected that a disk is approaching failure or end of life. The slot or bay location of the failure is identified.

Resolution

User Response

Schedule maintenance for the disk that is in a predictive failed state.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6
- Disk Storage Unavailable on page 8
- Primary High Availability System Failure on page 15

Standby high availability System Failure

Problem

Description: Standby HA System Failure.

The status of the secondary appliance switches to failed and the system has no high availability protection.

Resolution

User Response

Review the following resolutions:

- Restore the secondary system.

  Click the Admin tab, click **System and License Management**, and then click **Restore System**.
- Inspect the secondary high availability appliance to determine whether it is powered down or experienced a hardware failure.
- Use the **ping** command to check the communication between the primary and standby system.
- Check the switch that connects the primary and secondary high availability appliances. Verify the IP tables on the primary and secondary appliances.
- Review the **/var/log/qradar.log** file on the standby appliance to determine the cause of the failure.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6
- Disk Storage Unavailable on page 8
- Predictive Disk Failure on page 16

Scanner Initialization Error

Problem

Description: A scanner failed to initialize.

A scheduled vulnerability scan is unable to connect to an external scanner to begin the scan import process.

Scan initialization issues are typically caused by credential problems or connectivity issues to the remote scanner. Scanners that fail to initialize display detailed error messages in the hover text of a scheduled scan with a status of failed.

Resolution

User Response

Follow these steps:

1. Click the Admin tab.
2. On the navigation menu, click **Data Sources**.
3. Click **Schedule VA Scanners** icon.
4. From the scanner list, hover the cursor in the Status column of any scanner to display a detailed success or failure message.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5

- Automatic Update Error on page 6
- Disk Storage Unavailable on page 8
- Standby high availability System Failure on page 16

Scan Tool Failure

Problem

Description: A scan has been stopped unexpectedly, in some cases this may cause the scan to be stopped.

The system cannot initialize a vulnerability scan and asset scan results cannot be imported from external scanners. If the scan tools stop unexpectedly, the system cannot communicate with an external scanner. The system tries the connection to the external scanner five times in 30-second intervals.

In rare cases, the discovery tools encounter an untested host or network configuration.

Resolution

User Response

Select one of the following options:

- Review the configuration for external scanners in the deployment editor to ensure that the gateway IP address is correct.
- Ensure that the external scanner can communicate through the configured IP address.
- Ensure that the firewall rules for your DMZ are not blocking communication between your appliance and the assets you want to scan.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Update Error on page 6
- Disk Storage Unavailable on page 8
- Scanner Initialization Error on page 17

CHAPTER 3

Information Notifications for JSA Appliance

Juniper Secure Analytics (JSA) provides information messages about the status or result of a process or action.

An Infrastructure Component was Repaired

Problem

Description: Corrupted infrastructure component repaired.

A corrupted component that is responsible for host services on a managed host was repaired.

Resolution

User Response

No action is required.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Automatic Updates Successfully Downloaded on page 20

Automatic Updates Successfully Downloaded

Problem

Description: Automatic updates successfully downloaded. See the Auto Updates log for details.

Software updates were automatically downloaded.

Resolution

User Response

Click the link in the notification to determine whether any downloaded updates require installation.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- An Infrastructure Component was Repaired on page 19

Automatic Update Successful

Problem

Description: Automatic updates completed successfully.

Automatic software updates were successfully downloaded and installed.

Resolution

User Response

No action is required.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- An Infrastructure Component was Repaired on page 19
- Automatic Updates Successfully Downloaded on page 20

Disk Storage Available

Problem

Description: One or more storage partitions that were previously inaccessible are now accessible.

The disk sentry detected that the storage partition is available.

Resolution

User Response

No action is required.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Automatic Updates Successfully Downloaded on page 20
- An Infrastructure Component was Repaired on page 19
- Automatic Update Successful on page 20

Disk Usage Returned to Normal

Problem **Description: Disk Sentry: System Disk Usage Back To Normal Levels.**
The disk sentry detected that the disk usage is below 90% of the overall capacity.

Resolution *User Response*

No action is required.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- An Infrastructure Component was Repaired on page 19
- Automatic Update Successful on page 20

License Near Expiration

Problem **Description: A license is nearing expiration. It will need to be replaced soon.**
The system detected that a license for an appliance is within 35 days of expiration.

Resolution *User Response*

No action is required.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- An Infrastructure Component was Repaired on page 19
- Disk Usage Returned to Normal on page 21

License Allocation Grace Period Limit

Problem **Description: An allocated license's grace period is almost over, and will be allocated in to place soon.**

The system detected that a license change for an appliance is within the license grace period.

An administrator can move unlocked licenses or apply unused event or flow licenses to other appliances in your deployment. When you allocate a license to a host, a grace period of 14 days for the license begins. After the grace period expires, the license cannot be moved.

Resolution

User Response

No action is required.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- An Infrastructure Component was Repaired on page 19
- License Near Expiration on page 21

SAR Sentinel Operation Restore

Problem

Description: SAR Sentinel: normal operation restored.

The system activity reporter (SAR) utility detected that your system load returned to acceptable levels.

Resolution

User Response

No action is required.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- An Infrastructure Component was Repaired on page 19
- License Allocation Grace Period Limit on page 21

CHAPTER 4

Warning Notifications for JSA Appliances

Juniper Secure Analytics (JSA) system health notifications are proactive messages of actual or impending software or hardware failures.

Asset Change Discarded

Problem

Description: Asset Changes Aborted.

An asset change exceeded the change threshold and the asset profile manager ignores the asset change request.

The asset profile manager includes a process, asset persistence, that updates the profile information for assets. The process collects new asset data and then queues the information before the asset model is updated. When a user attempts to add or edit an asset, the data is stored in temporary storage and added to the end of the change queue. If the change queue is large, the asset change can time out and the temporary storage is deleted.

Resolution

User Response

Select one of the following options:

- Add or edit the asset a second time.
- Adjust or stagger the start time for your vulnerability scans or reduce the size of your scans.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Persistence Queue Disk Full on page 24

Asset Persistence Queue Disk Full

Problem

Description: Asset Persistence Queue Disk Full.

The system detected the spillover disk space that is assigned to the asset persistence queue is full. Asset persistence updates are blocked until disk space is available. Information is not dropped.

Resolution

User Response

Reduce the size of your scan. A reduction in the size of your scan can prevent the asset persistence queues from overflowing.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24

Asset Update Resolver Queue Disk Full

Problem

Description: Asset Update Resolver Queue Disk Full.

The system detected that the spillover disk space that is assigned to the asset resolver queue is full.

The system continually writes the data to disk to prevent any data loss. However, if the system has no disk space, it drops scan data. The system cannot handle incoming asset scan data until disk space is available.

Resolution

User Response

Review the following options:

- Ensure that your system has free disk space. The notification can accompany SAR Sentinel notifications to notify you of potential disk space issues.
- Reduce the size of your scans.
- Decrease the scan frequency.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Asset Persistence Queue Disk Full on page 24

Custom Property Disabled

Problem

Description: A custom property has been disabled.

A custom property is disabled because of problems processing the custom property. Rules, reports, or searches that use the disabled custom property stop working properly.

Resolution

User Response

Select one of the following options:

- Review the disabled custom property to correct your regex patterns. Do not re-enable disabled custom properties without first reviewing and optimizing the regex pattern or calculation.
- If the custom property is used for custom rules or reports, ensure that the **Optimize parsing for rules, reports, and searches** check box is selected.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Asset Update Resolver Queue Disk Full on page 25

Cyclic Custom Rule Dependency Chain Detected

Problem

Description: Found custom rules cyclic dependency chain.

A single rule referred to itself directly or to itself through a series of other rules or building blocks. The error occurs when you deploy a full configuration. The rule set is not loaded.

Resolution

User Response

Edit the rules that created the cyclic dependency. The rule chain must be broken to prevent a recurring system notification. After the rule chain is corrected, a save automatically reloads the rules and resolves the issue.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Custom Property Disabled on page 25

Disk Usage Warning

Problem

Description: Disk Sentry: Disk Usage Exceeded warning Threshold.

The disk sentry detected that the disk usage on your system is greater than 90%.

When the disk space on your system reaches 90% full, the system begins to disable processes to prevent data corruption.

Resolution

User Response

You must free some disk space by deleting files or by changing your data retention policies. The system can automatically restart processes after the disk space usage falls below a threshold of 92% capacity.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Cyclic Custom Rule Dependency Chain Detected on page 26

Device Backup Failure

Problem

Description: Either a failure occurred while attempting to backup a device, or the backup was cancelled.

The error is commonly caused by configuration errors in Configuration Source Management (CSM) or if a backup is canceled by a user.

Resolution

User Response

Select one of the following options:

- Review the credentials and address sets in CSM to ensure that the appliance can log in.
- Verify the protocol that is configured to connect to your network device is valid.
- Ensure that your network device and version is supported.
- Verify that there is connectivity between your network device and the appliance.
- Verify that the most current adapters are installed.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Disk Usage Warning on page 26

Disk Replication Falling Behind

Problem

Description: DRBD Sentinel: Disk replication is falling behind. See log for details.

If the replication queue fills on the primary appliance, system load on the primary might increases. Replication issues are commonly caused by performance issues on the primary system, or storage issues on the secondary system, or bandwidth problems between the appliances.

Resolution

User Response

Select one of the following options:

- Review bandwidth activity by loading a saved search MGMT: Bandwidth Manager from the Log Activity tab. This search displays bandwidth usage between the console and hosts.
- If SAR sentinel notifications are reccurring on the primary appliance, distributed replicated block device (DRBD) queues might be full on the primary system.
- Use SSH and the **cat /proc/drbd** command to monitor the DRBD status of the primary or secondary hosts.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Device Backup Failure on page 27

Disk Full for the Asset Change Queue

Problem

Description: Asset Change Listener Queue Disk Full.

The asset profile manager includes a process, change listener, that calculates statistics to update the CVSS score of an asset. The system writes the data to disk, which prevents data loss of pending asset statistics. However, if the disk space is full, the system drops scan data.

The system cannot process incoming asset scan data until disk space is available.

Resolution

User Response

Select one of the following options:

- Ensure that your system has sufficient free disk space.
- Reduce the size of your scans.
- Decrease the scan frequency.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Disk Replication Falling Behind on page 28

Deployment of an Automatic Update

Problem

Description: Automatic updates installed successfully. In the Admin tab, click Deploy Changes.

An automatic update, such as an RPM update, was downloaded and requires that you deploy the change to finish the installation process.

Resolution

User Response

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

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Disk Full for the Asset Change Queue on page 28

Events Routed Directly to Storage

Problem

Description: Performance degradation has been detected in the event pipeline. Event(s) were routed directly to storage.

To prevent queues from filling, and to prevent the system from dropping events, the event collection system (ECS) routes data to storage. Incoming events and flows are not categorized. However, raw event and flow data is collected and searchable.

Resolution

User Response

Review the following options:

- Verify the incoming event and flow rates. If the event pipeline is queuing events, expand your license to hold more data.
- Review recent changes to rules or custom properties. Rule or custom property changes might cause sudden changes to your event or flow rates. Changes might affect performance or cause the system to route events to storage.
- DSM parsing issues can cause the event data to route to storage. Verify whether the log source is officially supported.

- SAR notifications might indicate that queued events and flows are in the event pipeline.
- Tune the system to reduce the volume of events and flows that enter the event pipeline.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Deployment of an Automatic Update on page 29

Event or Flow Data not Indexed

Problem

Description: Event/Flow data not indexed for interval.

If too many indexes are enabled or the system is overburdened, the system might drop the event or flow from the index portion.

Resolution

User Response

Select one of the following options:

- If the dropped index interval occurs with SAR sentinel notifications, the issue is likely due to system load or low disk space.
- To temporarily disable some indexes to reduce the system load, on the Admin tab, click the **Index Management** icon.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Events Routed Directly to Storage on page 29

Expensive Custom Rule Found

Problem

Description: Expensive Custom Rules Found in CRE: Performance degradation has been detected in the event pipeline. Found expensive custom rules in CRE.

The custom rules engine (CRE) is a process that validates if an event matches a rule set and then trigger alerts, offenses, or notifications.

When a user creates a custom rule that has a large scope or uses a regex pattern that is not optimized, the custom rule can affect performance.

Resolution

User Response

Review the following options:

- On the Offenses tab, click **Rules** and use the search window to find and either edit or disable the expensive rule.
- If SAR sentinel notifications are recurring with the expensive rule notification, investigate the rule.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Event or Flow Data not Indexed on page 30

External Scan of an Unauthorized IP Address or Range

Problem

Description: An external scan execution tried to scan an unauthorized IP address or address range.

When a scan profile includes a CIDR range or IP address outside of the defined asset list, the scan continues. However, any CIDR ranges or IP addresses for assets that are not within your external scanner list are ignored.

Resolution

User Response

Update the list of authorized CIDR ranges or IP address for assets that are scanned by your external scanner. Review your scan profiles to ensure that the scan is configured for assets that are included in the external network list.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Expensive Custom Rule Found on page 30

Found an Unmanaged Process that is Causing Long Transaction

Problem

Description: Transaction Sentry: Found an unmanaged process causing unusually long transaction that negatively effects system stability.

The transaction sentry determines that an outside process, such as a database replication issue, maintenance script, auto update, or command line process, or a transaction is causing a database lock.

Resolution

User Response

Select one of the following options:

- Review the **/var/log/qradar.log** file for the word TxSentry to determine the process identifier that is causing your transaction issues.
- Wait to see whether the process completes the transaction and releases the database lock.
- Manually release the database lock.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- External Scan of an Unauthorized IP Address or Range on page 31

Flow Collector cannot Establish Initial Time Synchronization

Problem

Description: Flow collector could not establish initial time synchronization.

The QFlow process contains an advanced function for configuring a server IP address for time synchronization. In most cases, do not configure a value. If configured, the QFlow process attempts to synchronize the time every hour with the IP address time server.

Resolution

User Response

In the deployment editor, select the QFlow process. Click **Actions** > **Configure** and click **Advanced**. In the Time Synchronization Server IP Address field, clear the value and click **Save**.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Found an Unmanaged Process that is Causing Long Transaction on page 31

Infrastructure Component is Corrupted or did not Start

Problem

Description: Infrastructure component corrupted.

When the message service (IMQ) or PostgreSQL database cannot start or rebuild, the managed host cannot operate properly or communicate with the console.

Resolution

User Response

Contact Juniper Customer Support.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Flow Collector cannot Establish Initial Time Synchronization on page 32

Last Backup Exceeded the Allowed Time Limit

Problem

Description: Backup: The last scheduled backup exceeded execution threshold.

The time limit is determined by the backup priority that you assign during configuration.

Resolution

User Response

Select one of the following options:

- Edit the backup configuration to extend the time limit that is configured to complete the backup. Do not extend over 24 hours.
- Edit the failed backup and change the priority level to a higher priority. Higher priority levels allocate more system resources to completing the backup.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Infrastructure Component is Corrupted or did not Start on page 32

Long Running Reports Stopped

Problem

Description: Terminating a report which was found executing for longer than the configured maximum threshold.

The system cancels the report that exceeded the time limit. Table 3 on page 33 describes the reports that run longer than the default time limits are canceled.

Table 3: Default Time Limits by Report Frequency

Report frequency	Default time limits (hours)
Hourly	2

Table 3: Default Time Limits by Report Frequency *(continued)*

Report frequency	Default time limits (hours)
Daily	12
Manual	12
Weekly	24
Monthly	24

Resolution

User Required

Select one of the following options:

- Reduce the time period for your report, but schedule the report to run more frequently.
- Edit manual reports to generate on a schedule.

  A manual report might rely on raw data but not have access to accumulated data. Edit your manual report and change the report to use an hourly, daily, monthly, or weekly schedule.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Last Backup Exceeded the Allowed Time Limit on page 33

Long Transactions for a Managed Process

Problem

Description: Transaction Sentry: Found managed process causing unusually long transaction that negatively effects system stability.

The transaction sentry determines that a managed process, such as Tomcat or event collection service (ECS) is the cause of a database lock.

A managed process is forced to restart.

Resolution

User Response

To determine the process that caused the error, review the **qradar.log** for the word TxSentry.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3

- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Long Running Reports Stopped on page 33

Log Source License Limit

Problem

Description: The number of configured Log Sources is approaching or has reached the licensed limit.

Every appliance is sold with a license that collects events from a specific number of log sources. You approached or exceeded the license limit.

Any more log sources that added are disabled by default. Events are not collected for disabled log sources.

Resolution

User Response

Review the following options:

- On the Admin tab, click the **Log Sources** icon and disable or delete any log sources that are a low priority or have an inactive event source. Disabled log sources do not count towards your log source license. However, the event data that is collected by disabled log sources is still available and searchable.
- Ensure that log sources you deleted do not automatically rediscover. If the log source rediscovers, you can disable the log source. Disabling a log source prevents automatic discovery.
- Ensure that you do not exceed your license limit when you add log sources in bulk.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Long Transactions for a Managed Process on page 34

Log Source Created in a Disabled State

Problem

Description: A Log Source has been created in the disabled state due to license limits.

Traffic analysis is a process that automatically discovers and creates log sources from events. If you are at your current log source license limit, the traffic analysis process might create the log source in the disabled state. Disabled log sources do not collect events and do not count in your log source limit.

Resolution

User Response

Review the following options:

- On the Admin tab, click the **Log Sources** icon and disable or delete low priority log sources. Disabled log sources do not count towards your log source license.
- Ensure that deleted log sources do not automatically rediscover. You can disable the log source to prevent automatic discovery.
- Ensure that you do not exceed your license limit when you add log sources in bulk.
- If you require an expanded license to include more log sources, contact your sales representative.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Log Source License Limit on page 35

License Expired

Problem

Description: An allocated license has expired and is no longer valid.

When a license expires on the console, a new license must be applied. When a license expires on a managed host, the host context is disabled on the managed host. When the host context is disabled, the appliance with the expired license cannot process event or flow data.

Resolution

User Response

To determine the appliance with the expired license, click the Admin tab, click **System** and **License Management**. A system that has an expired license displays an invalid status in the License Status column.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Log Source Created in a Disabled State on page 35

License Expired

Problem

Description: An allocated license has expired and is no longer valid.

When a license expires on the console, a new license must be applied. When a license expires on a managed host, the host context is disabled on the managed host. When the host context is disabled, the appliance with the expired license cannot process event or flow data.

Resolution

User Response

To determine the appliance with the expired license, click the Admin tab, click **System** and **License Management**. A system that has an expired license displays an invalid status in the License Status column.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- License Expired on page 36

Maximum Active Offenses Reached

Problem

Description: MPC: Unable to create new offense. The maximum number of active offenses has been reached.

The system is unable to create offenses or change a dormant offense to an active offense. The default number of active offenses that can be open on your system is limited to 2500. An active offense is any offense that continues to receive updated event counts in the past five days or less.

Resolution

User Response

Select one of the following options:

- Change low security offenses from open (active) to closed, or to closed protected.
- Tune your system to reduce the number of events that generate offenses. To prevent a closed offense from being removed by your data retention policy, protect the closed offense.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- License Expired on page 36

Maximum Total Offenses Reached

Problem

Description: MPC: Unable to process offense. The maximum number of offenses has been reached.

By default, the process limit is 2500 active offenses and 100,000 overall offenses.

If an active offense does not receive an event update within 30 minutes, the offense status changes to dormant. If an event update occurs, a dormant offense can change to active. After five days, dormant offenses that do not have event updates change to inactive.

Resolution

User Response

Select one of the following options:

- Tune your system to reduce the number of events that generate offenses.
- Adjust the offense retention policy to an interval at which data retention can remove inactive offenses.

  To prevent a closed offense from being removed by your data retention policy, protect the closed offense.
- To free disk space for important active offenses, change offenses from active to dormant.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Maximum Active Offenses Reached on page 37

MPC: Process not Shutdown Cleanly

Problem

Description: MPC: Server was not shutdown cleanly. Offenses are being closed in order to re-synchronize and ensure system stability.

The magistrate process encountered an error. Active offenses are closed, services are restarted, and if required, the database tables are verified and rebuilt.

The system synchronizes to prevent data corruption. If the magistrate component detects a corrupted state, then the database tables and files are rebuilt.

Resolution

User Response

The magistrate component is capable of self-repair. If the error continues, contact Juniper Customer Support.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Maximum Total Offenses Reached on page 38

Maximum Sensor Devices Monitored

Problem

Description: Traffic analysis is already monitoring the maximum number of log sources.

The system contains a limit to the number of log sources that can be queued for automatic discovery by traffic analysis. If the maximum number of log sources in the queue is reached, then new log sources cannot be added.

Events for the log source are categorized as SIM Generic and labeled as Unknown Event Log.

Resolution

User Response

Select one of the following options:

- Review SIM Generic log sources on the Log Activity tab to determine the appliance type from the event payload.
- Ensure that automatic updates can download the latest DSM updates to properly identify and parse log source events.
- Verify whether the log source is officially supported.

  If your appliance is supported, manually create a log source for the events that were not automatically discovered.
- If your appliance is not officially supported, create a universal DSM to identify and categorize your events.
- Wait for the device to provide 1,000 events.

  If the system cannot auto discover the log source after 1,000 events, it is removed from the traffic analysis queue. Space becomes available for another log source to be automatically discovered.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- MPC: Process not Shutdown Cleanly on page 38

Maximum Events Reached

Problem

Description: Events per interval threshold was exceeded in past hour.

Each appliance has a license that processes a specific volume of event and flow data.

If the license limit continues to be exceeded, the system might queue events and flows, or possibly drop the data when the backup queue fills.

Resolution

User Response

Tune the system to reduce the volume of events and flows that enter the event pipeline.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Maximum Sensor Devices Monitored on page 39

Out of Memory Error and Erroneous Application Restarted

Problem

Description: Out of Memory: system restored, erroneous application has been restarted.

An application or service ran out of memory and was restarted. Out of memory issues are commonly caused by software issues or user-defined queries.

Resolution

User Response

Review the **/var/log/qradar.log** file to determine whether a service restart is required.

Determine whether large vulnerability scans or the importing of large volumes of data is responsible for the error. For example, compare when the system imports events or vulnerability data on your system with the notification timestamp. If necessary, stagger the time intervals for the data imports.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Maximum Events Reached on page 40

Protocol Source Configuration Incorrect

Problem

Description: A protocol source configuration may be stopping events from being collected.

The system detected an incorrect protocol configuration for a log source. Log sources that use protocols to retrieve events from remote sources can generate an initialization error when a configuration problem in the protocol is detected.

Resolution

User Response

To resolve protocol configuration issues:

- Review the log source to ensure that the protocol configuration is correct. Verify authentication fields, file paths, database names for JDBC, and ensure that the system can communicate with remote servers. Hover your mouse pointer over a log source to view more error information.
- Review the **/var/log/qradar.log** file for more information about the protocol configuration error.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Out of Memory Error and Erroneous Application Restarted on page 40

Process Exceeds Allowed Run Time

Problem

Description: Process takes too long to execute. The maximum default time is 3600 seconds.

The default time limit of 1 hour for an individual process to complete a task is exceeded.

Resolution

User Response

Review the running process to determine whether the task is a process that can continue to run or must be stopped.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Protocol Source Configuration Incorrect on page 40

Process Monitor License Expired or Invalid

Problem

Description: Process Monitor: Unable to start process: license expired or invalid.

The license is expired for a managed host. All data collection processes stop on the appliance.

Resolution

User Response

Contact your sales representative to renew your license.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Process Exceeds Allowed Run Time on page 41

Restored System Health by Canceling Hung Transactions

Problem

Description: Transaction Sentry: Restored system health by canceling hung transactions or deadlocks.

The transaction sentry restored the system to normal system health by canceling suspended database transactions or removing database locks. To determine the process that caused the error, review the **qradar.log** file for the word TxSentry.

Resolution

User Response

No action is required.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Process Monitor License Expired or Invalid on page 41

SAR Sentinel Threshold Crossed

Problem

Description: SAR Sentinel: threshold crossed.

The system activity reporter (SAR) utility detected that your system load is above the threshold. Your system can experience reduced performance.

Resolution

User Response

Review the following options:

- In most cases, no resolution is required.

  For example, when the CPU usage over 90%, the system automatically attempts to return to normal operation.

- If this notification is recurring, increase the default value of the SAR sentinel.

  Click the Admin tab, then click **Global System Notifications**. Increase the notification threshold.

- For system load notifications, reduce the number of processes that run simultaneously.

  Stagger the start time for reports, vulnerability scans, or data imports for your log sources. Schedule backups and system processes to start at different times to lessen the system load.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Restored System Health by Canceling Hung Transactions on page 42

Time Synchronization Failed

Problem

Description: Time synchronization to primary or Console has failed.

The managed host cannot synchronize with the console or the secondary high availability appliance cannot synchronize with the primary appliance.

Administrators must allow rdate communication on port 37. When time synchronization is incorrect, data might not be reported correctly to the console. The longer the systems go without synchronization, the higher the risk that a search for data, report, or offense might return an incorrect result. Time synchronization is critical to successful requests from managed host and appliances.

Resolution

User Response

Contact Juniper Customer Support.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- SAR Sentinel Threshold Crossed on page 42

Threshold Reached for Response Actions

Problem

Description: Response Action: Threshold reached.

The custom rules engine (CRE) cannot respond to a rule because the response threshold is full.

Generic rules or a system that is tuned can generate a many response actions, especially systems with the IF-MAP option enabled. Response actions are queued. Response actions might be dropped if the queue exceeds 2000 in the event collection system (ECS) or 1000 response actions in Tomcat.

Resolution

User Response

- If the IF-MAP option is enabled, verify that the connection to the IF-MAP server exists and that a bandwidth problem is not causing rule response to queue in Tomcat.
- Tune your system to reduce the number of rules that are triggering.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Time Synchronization Failed on page 43

Unable to Determine Associated Log Source

Problem

Description: Unable to automatically detect the associated log source for IP address <IP address>.

At minimum, 25 events are required to identify a log source. If the log source is not identified after 1,000 events, the system abandons the automatic discovery process.

When the traffic analysis process exceeds the maximum threshold for automatic discovery, the system categorizes the log source as SIM Generic and labels the events as Unknown Event Log.

Resolution

User Action

Review the following options:

- Review the IP address to identify the log source.
- Review any log sources that forward events at a low rate. Log sources that have low event rates commonly cause this notification.
- To properly parse events for your system, ensure that automatic update downloads the latest DSMs.
- Review any log sources that provide events through a central log server. Log sources that are provided from central log servers or management consoles might require that you manually create their log sources.
- Review the Log Activity tab to determine the appliance type from the IP address in the notification message and then manually create a log source.

- Verify whether the log source is officially supported. If your appliance is supported, manually create a log source for the events.
- If your appliance is not officially supported, create a universal DSM to identify and categorize your events.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Threshold Reached for Response Actions on page 43

User does not Exist or is Undefined

Problem

Description: User either does not exist or has an undefined role.

The system attempted to update a user account with more permissions, but the user account or user role does not exist.

Resolution

User Response

On the Admin tab, click **Deploy Changes**. Updates to user accounts or roles require that you deploy the change.

Related Documentation

- Overview of Troubleshooting JSA System Notifications on page 3
- Accumulator cannot Read the View Definition for Aggregate Data on page 5
- Disk Storage Unavailable on page 8
- Asset Change Discarded on page 24
- Unable to Determine Associated Log Source on page 44

PART 2

Index

Index

T