Juniper Secure Analytics Release Notes

2014.3
November 2015

Juniper Secure Analytics (JSA) 2014.3 Release Notes provides new features, known issues and limitations, and fixes to known issues.

Contents

New and Updated Functionality

Table 1 on page 2 shows the new features of and enhancements to Juniper Secure Analytics (JSA) for the 2014.3 release.

Table 1: New Feature/Enhancement Descriptions

New Feature/Enhancement	Description
New JSA appliances	
JSA3800	The JSA3800 appliance is a 1-U, rack-mountable chassis with AC power supplies (or optional DC power supplies), six hot-swappable hard drives, 64 GB memory, and two 10 Gigabit and four Gigabit Ethernet interfaces.
JSA5800	The JSA5800 appliance is a 2-U, rack-mountable chassis with AC power supplies (or optional DC power supplies), eight hot-swappable hard drives, 128 GB memory, and two 10 Gigabit and four Gigabit Ethernet interfaces.
New and updated functionality for installers	
Installations in cloud environments	You can deploy the JSA console or managed hosts, or both, in JSA SoftLayer and Amazon AWS environments. You can establish secure communications between cloud and on-premises installations of JSA by configuring OpenVPN connections.
New and updated functionality for administrators	
Domain management for overlapping IP addresses in JSA Log Manager	Enhancements to the Content Management Tool make it easier to export user-created security and configuration content in a portable format. You can import the content into any JSA deployment. The Content Management Tool creates an XML representation of the content in the database tables and external files. All dependencies are also exported. The resulting XML and external files are archived and compressed.
Tuning assets	A new Asset Profiler Configuration tool shows information to administrators about assets that are discovered on the network from flows, events that have identity information, or scanner import data. For more information, see the online help and hover text in the tool.
Improvement to large deployments of managed hosts	Deployments in a large distributed environment are optimized and take minutes. Deployments of more than 200 managed hosts are supported.
User-created custom properties to improve queries about assets	Users can create custom properties for assets. Custom properties provide more query options.
Dynamic scanning	The vulnerability scanners that you deploy might not have access to all areas of your network. During a scan, each asset in the CIDR range that you want to scan is dynamically associated with the correct scanner.
Rebalance progress and feedback for Data Nodes	In the Deployment Editor, you can view the status of your data rebalancing to the Data Node appliance.
New and updated functionality for users	

Table 1: New Feature/Enhancement Descriptions *(continued)*

New Feature/Enhancement	Description
Log source reporting	You can now report on and export log source lists. You can generate reports that are limited to a specific set of log sources or log source groups or reports that are based on specific criteria.
Support date and time parsing for custom properties	JSA supports extracting date values in many formats, which then can be used in rules, searching, and reporting.
Search for information in JSA user interface by using AQL	To retrieve information about events, flows, assets, or reference sets, or to build complex queries, type Ariel Query Language (AQL) queries in the Advance Search text box. For more information about the AQL syntax enhancements and joining searches for reference tables and reference sets, see the *Ariel Query Language Guide*.
Custom colors based on risk score	You can configure different background colors based on the risk of a vulnerability. The colors are shown in asset details, vulnerability management, and vulnerability reports.

Related Documentation

- Installing JSA on page 3
- Known Issues and Limitations on page 5
- Resolved Issues on page 6

Installing JSA

To install JSA:

- *System Requirements*—For information about hardware and software compatibility, see the detailed system requirements in the *Juniper Security Analytics Installation Guide*.
- *Installing JSA*—For installation instructions, see the *Juniper Security Analytics Installation Guide*.

Related Documentation

- New and Updated Functionality on page 2
- Known Issues and Limitations on page 5
- Resolved Issues on page 6
- Installing CVE Scripts on page 3

Installing CVE Scripts

The release of CVE-2014-7169.sh.gz is cumulative and contains fixes for both CVE-2014-6271 and CVE-2014-7168. If you have:

- Not applied any fixes to your system for the Bash vulnerability, then you only need to download and install CVE-2014-7169.sh.gz on your STRM/JSA systems.

- Applied the fix for CVE-2014-6271 already to your STRM/JSA appliances, you must also install CVE-2014-7169.sh.

Installing CVE-2014-7169-fix. sh.gz Script on STRM/JSA

The installation procedure is applied to all appliances types.

NOTE: Administrators should start by patching the console appliance, then apply the patch to managed hosts in their networks. Administrators must install this update to both high availability pairs individually. This installation procedure requires the administrator to reboot systems.

Procedure

1. Download the CVE-2014-7169-fix.sh.gz script from Juniper Customer Support.

   This file contains the required software to patch any version of STRM 2012 and later versions of STRM/JSA for vulnerabilities.

2. Using SCP or WinSCP (for Windows systems), copy the script to the STRM/JSA appliance.

3. To extract the file, type the following command:

   gunzip CVE-2014-7169-fix.sh.gz

4. To set the correct permission on this file, type the following command:

   chmod +x CVE-2014-7169-fix.sh

5. On your high availability secondary system, type the following command to install the patch:

   ./CVE-2014-7169-fix.sh

   NOTE: If this system is an HA pair, install the update on the secondary first and reboot the secondary.

   The script updates bash version on STRM/JSA.

6. Type the following command:

   reboot

7. When the script has completed the update, the following message is displayed: **COMPLETE**.

   If you have an HA primary system, then continue with Step 8.

   NOTE: You must wait for the HA secondary to reboot before you set the primary system offline.

8. Log in to the STRM/JSA console.
9. Click the Admin tab and select **System and License Management** icon.
10. Select the high availability primary system.
11. From the toolbar, select **High Availability** > **Set System Offline**.

    This fails the primary system and the secondary will enter the active state.
12. From the command-line interface of the HA primary system, type the following command to install the patch:

    ./CVE-2014-7169-fix.sh

    The script updates the bash version on STRM/JSA.
13. When the script has completed the update, the following message is displayed: **COMPLETE**.
14. Type the following command:

    reboot

    NOTE: **You must wait for the HA primary to reboot before you set the primary system online.**
15. Click the Admin tab and select **System and License Management** icon.
16. Select the high availability primary system.
17. From the toolbar, select **High Availability** > **Set System Online**.

    This sets the primary system active and the secondary will enter the standby state.

Known Issues and Limitations

Table 2 on page 5 describes the known issues in JSA 2014.3.

Table 2: Known Issues and Limitations

Issue	Description
The selected menu option is not highlighted using the up or down arrow keys when configuring the JSA appliance	In the JSA console during configuration, using up or down arrow keys to select a menu option does not highlight the selected option. For more information, see the KB article KB28225 at https://kb.juniper.net/KB28225. *Workaround:* Although your current position is not highlighted, use tab to navigate to the option and then use up or down arrow keys to select an option. Use left or right arrow keys to select **Next**. Choose any option from the time zone list and proceed with the configuration process. After the setup, you can change the time zone in the WebUI.

Table 2: Known Issues and Limitations *(continued)*

Issue	Description
JSA7500 event processor performance optimization	When log source sends around 30,000 events per second to the JSA7500 event processor, the event starts dropping with warning or error messages. NOTE: The Custom Rule Engine back up and store events without correlation is 30,000 events per second (0% coalescing). *Workaround*: None.

Related Documentation

- New and Updated Functionality on page 2
- Installing JSA on page 3
- Resolved Issues on page 6

Resolved Issues

Table 3 on page 6 describes the issues resolved in JSA 2014.3:

Table 3: Issues Resolved

Issue	Description
Backup unable to determine disk space on partitions with filesystem in the name	In JSA 2013.2 r2 backups will not be able to run when the backup location is mounted on a mount point that contains the case sensitive string **'Filesystem'** in the name. *Workaround*: Change the name of the mount point if possible. If changing the name is not possible contact Juniper Customer Support for a work around.
When running setup -t pretest before upgrading to JSA 2013.2 R2, It may set a logging directory to the incorrect version	When running setup -t before upgrading to JSA 2013.2.r2, it may change the log directory incorrectly.**This rule will be disabled**. This will result in all patch and upgrade logs going to **/var/log/setup-2013.2*** while still being at version 2010. *Workaround*: Complete the upgrade after running the setup -t pretest.
Active directory authentication delays occur when UDP communication is blocked	On networks where UDP communication between the JSA console and their Active Directory server is blocked, Active Directory authentication can take an extended period to log in. For example, it can take 3 minutes to log in. This delay occurs because the system attempts three time to log in using UDP before it automatically switches to TCP for a successful log in.

Table 3: Issues Resolved *(continued)*

Issue	Description
Offenses reports might display multiple (n) incorrectly	On a generated Offense report that includes the Username column, Multiple (n) is displayed incorrectly where the correct value should be N/A.
XSS vulnerability - get method	Reflected cross site scripting vulnerability: GET method of the Network Hierarchy user interface allows parameters **configarea** and **object** to contain CSS code.
Coalescing events option missing from system settings in JSA log manager	The Coalescing Events option under **Admin** --> **System Settings** is not seen in Log Manager 2013.2.r2 but is present in Log Manager 2010. *Workaround*: None.
Two character user names not allowed in JSA VM scan setup	Attempting to create a scan profile using two character Windows user name **HD,** JSA VM will not allow user name to be added to credentials under 'scan setup' and reports an error **Username must be greater than 2 characters.** This appears to be a defect in the original spec, which called for usernames to be > 2 characters. As a result it is not possible to complete credential scans on Windows machines.
Dashboard time series graphs might display incorrect data sets	The time series graphs on the Network Overview dashboard might display incorrect data sets for graphs generated from log events. *Workaround*: Refresh your Browser window.

Table 3: Issues Resolved *(continued)*

Issue	Description
The ECS service might display an error when a DNS lookup occurs on a host name that maps to more than 100 IP addresses	An unhandled exception might display in the user interface when the ECS service attempts to resolve host names that map to more than 100 IP addresses in a DNS lookup. The ECS error can coincide with the following message in **/var/log/qradar.log**: : Unhandled exception Type=Segmentation error vmState=0x00000000 J9Generic_Signal_Number=00000004 Signal_Number=0000000b Error_Value=00000000 Signal_Code=00000002 Handler1=00007FAC6F4835C0 Handler2=00007FAC6F1407F0 InaccessibleAddress=00007FAC46AE RDI=00007FAC46AE6320 RSI=00007FAC46B26798 RAX=00007FABB00510E0 RBX=00007FABB0051130 RCX=00000000000004D4 RDX=00007FABB0051130 R8=00000038E70CEF80 R9=0000000269641600 R10=0000000000000010 R11=0000000000200202 R12=00007FAC46AEF5F0 R13=000000000000019C R14=00007FABB0004A60 R15=00007FAC46B26888 RIP=00000038E7 GS=0000 FS=0000 RSP=00007FAC46AE6320 EFlags=0000000000210206 CS=0033 RBP=00007FAC46B26830 ERR=0000000000000006 TRAPNO=000000000000000E OLDMASK=0000000000000000 CR2=00007FAC46AE7000 xmm0 79c2520a00000002 (f: 2.000000, d: 3.247600e+278) xmm1 00ffffffffffffff (f: 4294967296.000000, d: 7.291122e-304) xmm2 0000000000000000 (f: 0.000000, d: 0.000000e+00) xmm3 0000000000000000 (f: 0.000000, d: 0.000000e+00) xmm4 4040404040404040 (f: 1077952512.000000, d: 3.250196e+01) xmm5 5b5b5b5b5b5b5b5b (f: 1532713856.000000, d: 1.213625e+132) xmm6 2020202020202020 (f: 538976256.000000, d: 6.013470e-154) xmm7 0000000000000000 (f: 0.000000, d: 0.000000e+00) xmm8 ffffff000000ff00 (f: 65280.000000, d: -nan) xmm9 0000000000000000 (f: 0.000000, d: 0.000000e+00) xmm10 ffffff000000ff00 (f: 65280.000000, d: -nan) xmm11 0000000000000000 (f: 0.000000, d: 0.000000e+00) xmm12 0000000000000000 (f: 0.000000, d: 0.000000e+00) xmm13 0000000000000000 (f: 0.000000, d: 0.000000e+00) xmm14 0000000000000000 (f: 0.000000, d: 0.000000e+00) xmm15 0000000000000000 (f: 0.000000, d: 0.000000e+00) Module=/lib64/libc.so.6 Module_base_address=00000038E7 Symbol=getaddrinfo Symbol_address=00000038E7 ----------- Stack Backtrace ----------- getaddrinfo+0x377 (0x00000038E7 [libc.so.6+0xd27e7]) Java_java_net_Inet6AddressImpl_lookupAllHostAddr (0x00007FAC5C770 [libnet.so+0x7950]) *Workaround*: For more information, contact Juniper Customer Support.

Table 3: Issues Resolved *(continued)*

Issue	Description
'System Error' Popup message in JSA 2014.1 when opening vulnerability details panel	In JSA 2014.1 and later, you may encounter the following issue with the Web Interface: In the Asset Details panel (the window opened if an asset is selected in the Assets tab), a **System Error** popup error message will occur upon selecting an associated vulnerability record from the is opened from the 'Vulnerabilities' section of the panel. The error message will be similar to the following System Error: **There was a problem handling the response from the server while executing a remote method call (Details)** Upon selecting **Details** on the erro popup, the following detail will be provided: **Request Status: 200 Application: JSA Method: getAssetsForVulnerability Error: 'e' is null Code: undefined Name: TypeError File:** https://172.16.78.211/console/assetprofile/js/researchVulnerability/details.js?versi on=4... Line: 136 The method **getAssetsExceptionedForVulnerability** may also be seen. The Error, Code, Name, File, and Line values may vary. *Workaround*: None. After closing the error popup, the **Vulnerability Details** panel otherwise displays normally.
SNMP response in an offense rule might fail	An issue occurred where offense rules that are configured to generate an SNMP response might fail to trigger a response and the following error message might be displayed in the error log: **Attempt to query field "oa.annotationType.weight" from non-entity variable "oa". Perhaps you forgot to prefix the path in question with an identification variable from your FROM clause?**
Patching a 2014.1 high availability system might fail due to timing issue	If you patch a 2014.1 deployment that has multiple high availability managed hosts, the first patch on a managed host might fail because the secondary host is not in standby mode. *Workaround*: Re-run the patch.
Log source grouping removed when user is deleted	Log sources placed in log source groups by a specific user get disassociated from the group(s) when that user is deleted therefore Offense rules, searches or reports will no longer work after sources are disassociated from their group log sources should still be associated to the log source groups when the user is deleted. *Workaround*: If the user has not been deleted already then set their Role to **Disabled**.

Table 3: Issues Resolved *(continued)*

Issue	Description
"Accumulated data is not available" error in generated report only when using table view	Some reports based using table charts may display **Accumulated Data is not available** when it is actually available. Here is the associated error in qradar.log: **[report_runner] [main] com.q1labs.reporting.ReportServices: [WARN] [NOT:0000004000][132.208.246.161/--] [-/--]Error occurred creating Accumulated Result Set. Trying to fall back to raw query if possible. [report_runner] [main] java.lang.IllegalArgumentException: keyCreator should not be null [report_runner] [main] at com.q1labs.frameworks.nio.SortOrder.<(SortOrder.java:31) [report_runner] [main] at JSA Patch Release Notes Resolved Issues 29 com.q1labs.frameworks.nio.SortOrder.><(SortOrder.java:26) [report_runner] [main] at com.q1labs.ariel.QueryParams.setSortOrder(QueryParams.java:316) [report_runner] [main] at com.q1labs.reporting.charts.ArielChart.getData (ArielChart.java:1347) [report_runner] [main] at com.q1labs.reporting.Chart.getXML(Chart.java:212) [report_runner] [main] at com.q1labs.reporting.Report.createData(Report.java:238) [report_runner] [main] at com.q1labs.reporting.Report.process(Report.java:281) [report_runner] [main] at com.q1labs.reporting.ReportRunner.main(ReportRunner.java:176)>**
Routing rules interface might not display correctly when the rule contains a backslash (\\) character	In the Routing Rules interface on the Admin tab, the user interface might not display properly when the administrator attempts to edit a value. This issue is believed to be caused when the routing rule contains a backslash character (\\). The backslash is stored incorrectly in the database and causes the edit routing rule interface to display a blank page in the window. *Workaround*: For assistance with user interface issues, contact Juniper Customer Support.
Reports may fail to be e-mailed by the system if the size of the generated report exceeds 10 MB	JSA at version 2014 and above use Postfix as the mail transfer agent. The default configuration for Postfix limits e-mail to a maximum file size of 10 MB. When a report exceeds the default limit, the generated report is not e-mailed as intended. *Workaround*: Administrators who need to send reports over 10 MB in size can contact Juniper Customer Support to update the message size limit for the mail transfer agent.

Table 3: Issues Resolved *(continued)*

Issue	Description
High availability secondary systems in standby mode might accumulate log files and experience high disk usage	Secondary high availability appliances might experience an issue where disk space is limited due to log files accumulating over time. The disk usage issue on the high availability appliance might be due files not being cleaned up on the standby system over time in **/var/log/systemStabMon/**. The standby system should run disk maintenance to remove files in **/var/log/systemStabMon/** that are older than the systems default retention setting. *Workaround*: Administrators can verify the size of **/var/log/systemStabMon/** and safety delete any log files that are more than six months old.
The event details page is not showing the correct identity IP for the related asset	The Event Details page is not showing the correct identity IP for the related asset. 1. From the event viewer, click on an Event with Identity in the event search results grid. 2. Event details is displayed. 3. Scroll to the bottom of the details to see the event Identity Information. 4. Find the 'Identity IP' value. It has been intermittently observed that the value in this column is not an IP at all, but a seemingly random hostname. At other times the Identity IP address in this column is clearly not the identity IP specified in the payload. However, the Identity IP address column on the Search results grid for the same event shows the correct identity IP.
Reports that use the include link to report console check box might generate a certificate error	On the Reports tab, users that create a report and select the Include link to Report Console check box might receive an SSL error when the embedded URL is launched. This issue is due to the link containing the IP address when the SSL certificate for the console uses a hostname. Example 1: **destinationPort will return:** **com.q1labs.frameworks.nio.Port|53** Example 2: **destinationBytes will return:** **java.lang.Double|310.0** This can be recreated by running the following arielQuery commands: **/opt/qradar/bin/arielClient -x "select destinationPort from flows wheredestinationPort > 1024"** Results should only be returning the value.

Table 3: Issues Resolved *(continued)*

Issue	Description
High availability secondary appliance with ISCSI might experience an issue where the secondary system goes offline after an hour	After a primary high availability appliance fails over to the secondary high availability appliance, an issue in the high availability manager can force the secondary offline after an hour. When a failover occurs, the system generates the following message when the secondary takes over in /var/log/qradar.log: **com.q1labs.ha.manager.HAManager: [INFO] [NOT:0000006000][IP Address/- -] [-/- -]Remote not found or not ACTIVE, going ACTIVE com.q1labs.ha.manager.ShellWorkerThread: [INFO] [NOT:0000006000][IP Address/- -] [-/- -]Executing shell task GoActive /opt/qradar/ha2/scripts/GoActive.sh com.q1labs.ha.manager.ipc.IPCWorkerThread: [INFO] [NOT:0000006000][IP Address/- -] [-/- -]IPC service "check" = "alive" com.q1labs.ha.manager.ipc.IPCWorkerThread: [INFO] [NOT:0000006000][IP Address/- -] [-/- -]IPC service "state" = "going_active"** After an hour, the administrator might notice that the secondary has gone offline and that the logs include the following error message: **com.q1labs.ha.manager.ShellWorkerThread: [INFO] [NOT:0000006000][IP Address/- -] [-/- -]Error reading ShellWorkerThread output stream: Interrupted system call com.q1labs.ha.manager.ShellWorkerThread: [INFO] [NOT:0000006000][IP Address/- -] [-/- -]Shell task GoActive /opt/qradar/ha2/scripts/GoActive.sh failed after 3600004 ms. [Exit Value: "-1",Was Interrupted: "true",Output Content: [],Error Content: [],Output Patterns: [null],Error Patterns: [null]]) com.q1labs.ha.manager.StateMachine: [ERROR] [NOT:0000003000][IP Address/- -] [-/- -]Failed to complete GoActive task, starting local RESTORE (host/4334) com.q1labs.ha.manager.ShellWorkerThread: [INFO] [NOT:0000006000][IP Address/- -] [-/- -]Executing shell task GoOffline /opt/qradar/ha2/scripts/GoOffline.sh com.q1labs.ha.manager.ipc.IPCWorkerThread: [INFO] [NOT:0000006000][IP Address/- -] [-/- -]IPC service "check" = "alive" com.q1labs.ha.manager.ipc.IPCWorkerThread: [INFO] [NOT:0000006000][IP Address/- -] [-/- -]IPC service "state" = "going_offline" [/etc/init.d/hostcontext] [WARN] Shutting down hostcontext service**

Table 3: Issues Resolved *(continued)*

Issue	Description
WinCollect - application error when adding new log sources from group	When adding a new WinCollect log source from a WinCollect group an F5 Aplication Error occurs when saving the new log source. Recreation Steps: 1. Add a new WinCollect Agent. 2. Create a new log source group for WinCollect log sources. 3. Open the Log Sources window and go to the WinCollect group. 4. Add a new WinCollect log source and once you hit save, the following error is displayed in the UI Window: **An error has occurred. Refresh your browser (press F5) and attempt the action again. If the problem persists, please contact Juniper Customer Support for assistance.**
Offense rule SNMP trap missing datasource_id and datasource_name	An Offense notification enabled via SNMP trap and e-mail in the SMTP trap case is missing the source IP (displayed as 'N/A'). Though Offense is generated correctly and contains source IP details (in Offense Detail record and in the notification e-mail), when it is sent via SNMP the source IP details are not sent. To Recreate: • Create an Offense Rule and configure the Offense to send to an SNMP server • In Rule Response, select send to SNMP • tcpdump will show the source IP as N/A • The 'source IP' should correspond to the DATASOURCE_NAME field in the SNMP trap
Vulnerability count for asset sometimes shows 0 even though the actual count is not 0	When using the DDI AVS scanner the "Vulnerabilities" count column in Assets -> Asset Profiles tab shows a count of 0 even though if the particular asset is opened up we can see that the vulnerability list is not empty. The numbers needs to be on the main asset pages so the customer can actually see the vulnerabilities and work with them instead of having to open each and every one of them. *Workaround*: To circumvent this issue, run the following command as root from an SSH session to the console: **psql -U qradar -c "update sql_query_definitions set xml_doc = replace(t2.xml_doc, 'JOIN asset.vulninstancestatistics', 'LEFT OUTER JOIN asset.vulninstancestatistics') from (select xml_doc from sql_query_definitions where name = 'assets.assetList') AS t2 where name = 'assets.assetList' and t2.xml_doc NOT LIKE '%LEFT OUTER JOIN asset.vulninstancestatistics%'"** This should return the result ' **UPDATE 1**'.

Table 3: Issues Resolved *(continued)*

Issue	Description
Special characters such as ampersand cannot be escaped in rule	When adding ampersand (&) character into a rule, just after saving, it is replaced by &. When trying to escape the "&" the result is: \&. Rule in use: When any of these properties match this regular expression.
Unable to sort on asset detail user list screen, columns cannot be sorted in ascending order or descending order	Unable to sort on asset detail user list screen, columns cannot be sorted in ascending or descending order. Replication steps: 1. At the log activity tab filter on Source IP. 2. Right-click. Select more options, then select information, then asset profile. 3. Click on **last user, all users link**. The order of the users in the list does not change when selecting to sort in ascending or descending order.
Update memory and disk space requirements documentation with correct 1299 memory requirements	When upgrading from 2013.2.r2 to 2014.1 the below error is received: **[PATCH_UPDATER] [INFO] Running 1 Patch Pretest(s) Running pretest 1/1: Minimum RAM Check This is an upgrade. Performing Minimum RAM Check. APPLIANCE ID = 1299 Resolved Issues 35 MINIMUM RAM = 6000 SYSTEM RAM = 2048 ERROR: Minimum memory requirements not met. This system has 2048MB and requires at least 6000MB. [PATCH_UPDATER] [ERROR] Patch pretest 'Minimum RAM Check' failed. (ramcheck.py)** The disk and space requirements documentation for the 1299 appliance need correcting. The current documented memory requirement is 6 GB but this is too high for non-JSA VM scanner installations. *Workaround*: None.
When customizing the right-click menu the user can still access options without the capabilities defined in the user role	When customizing the right-click menu a user with no administration capabilities in the User Role can still access menu options that are configured (through ip_context_menu.xml below) for user with Administration capabilities.

Table 3: Issues Resolved *(continued)*

Issue	Description
CRE 'Local Network' test should check both sides of a superflow	Offenses generated by flow rules when rule tests are based on network hierarchy do not produce the correct results. This appears to be due to an issue with SuperflowB flows not being expanded when this test executes in the custom rule engine. Desired Behavior: The flow rule test should properly evaluate for Superflows. *Workaround*: • Rule test to exclude most common destination IP's • Disable superflows
Offense "Reason for Closing" window is not displayed from pages includes OffenseCategoryList, OffenseRuleList, and, so on	If you close an Offense from any screen from pages including OffenseCategoryList, OffenseNetworkList, OffenseUserList, OffenseDeviceList, OffenseRuleList, and, so on, the Offense Reason for Closing window is not displayed. That window is displayed for other pages including OffenseSummary, OffenseAttackerList, and, so on. This is important not only to keep UI consistent but also ensure reason for closing is maintained. Steps to Recreate: 1. Double click on any offense. 2. Click **Display** and select any option - **category, user, rule**, and, so on. 3. Click **Actions** -> **Close**. The offense is closed with no option to specify a reason. Desired Behavior: Reason for Closing menu displayed on every screen when an offense is viewed and closed.
Offense search with source IP specified in search parameter does not return offenses that have multiple source IP	If you close an Offense from any screen from pages including OffenseCategoryList, OffenseNetworkList, OffenseUserList, OffenseDeviceList, OffenseRuleList, and, so on, the Offense Reason for Closing window is not displayed. Steps to Recreate: 1. Create a rule that will match to current weekday, fire offense and index by source IP. 2. Create another rule that will match to current weekday, fire offense and index by rule. 3. Play some events. 4. New offense search, specify source IP in search parameter, then click **search**. 5. You will find for some source IP, the offense created from step 2 is not returned in the result, but it should. Desired Behavior: Offense Search **by source IP** should return all source IPs.

Table 3: Issues Resolved *(continued)*

Issue	Description
Application error in system and license management details panel	If the console has a private and public ip the wrong ip is being used in the URL. Under these circumstances you will get an application error when accessing the license details screen. The following error can be seen in qradar.log: com.q1labs.uiframeworks.action.ExceptionHandler: [ERROR] [NOT:0000003000][</--] [-/--]An exception occurred while processing the request: java.lang.NullPointerException at com.q1labs.qradar.ui.qradarservices.UISystemManagementServices.getSystem(UISystemManagementServices.java:1400) at com.q1labs.qradar.ui.action.SystemAndLicenseManagement.viewSystemDetails(SystemAndLicenseManagement.java:207) at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method) at sun.reflect.NativeMethodAccessorImpl.invoke>(NativeMethodAccessorImpl.java:76) *Workaround*: Change the URL to use the correct hostIP.
Eventthrottlefilterqueue on disk chunk size is too small resulting in ECS pipeline failure and shutdown	The EventThrottleFilterQueue on disk chunk size is too small causing ECS to stop processing events if an event > 10 MB enters the ECS pipeline. In order for this to happen two conditions have to occur: 1. EC has to back up in EventThrottleFilter enough for EventThrottleFilter to completely fill in-memory portion and start writing data out to its spillover queue, meaning there is likely a burst in traffic rate over the license/capabilities. 2. An event over 10 MB must present. NOTE: The EventThrottleFilter's spillover queue will fail due to the default the on-disk size is set to 10 MB.
Search criteria for inactive offenses does not function as documented from the offenses search screen	Steps to Reproduce: • Check all boxes except The Inactive Offenses under Exclude. • Click **Search**. The expectation was to see the list of all inactive offenses available but instead no results were returned.
JSA is using an older version of Webmin	Request for new version of Webmin to eliminate security issues.

Table 3: Issues Resolved *(continued)*

Issue	Description
System notifications can stress Tomcat in extreme cases	When a rule is created or modified to send an event to Notification it ends up in the Messages section of the UI, the System Notifications dashboard item and the Alert Popup message. This mechanism was designed to provide immediate UI alerts for critical issues. In conditions where the rule fires on events several thousand times a day the resulting flood of notifications can cause the UI to slow down and in some cases UI access will be lost intermittently. *Workaround*: Review rules that use notification as a response and either remove the notification response or use a response limiter. In addition, clear out the current notifications.
HTTP-only keywords not set in cookies	Application mis-configuration which leads to an exploit on the client side; Best Practices fix for the server side. It is possible to use client-side scripting to access a cookie via the document.cookie property. Attackers may be able to combine this vulnerability with cross-site scripting (XSS) or malicious AJAX (Asynchronous JavaScript and XML) code for cookie harvesting.
Event export for CSV or XML missing first column	The first column is missing when exporting events to CSV or XML from log activity. To recreate, in the Log Activity tab, make an export of the events as XML or CSV by selecting Visible Columns. The result is a file with the first column missing.

Table 3: Issues Resolved *(continued)*

Issue	Description
SQL exception in Offense tab	Certain pages of Offense tab may be inaccessible. The following exception is displayed in the logs: May 28 15:26:46 <IP Address 1> [tomcat] [admin@<IP Address 2> (2798) /console/do/sem/offensesearch] com.q1labs.uiframeworks.action.ExceptionHandler: [ERROR] [NOT:0000003000][<IP Address 1>/- -] [-/- -]An exception occurred while processing the request: May 28 15:26:46 <IP Address 1> [tomcat] [admin@<IP Address 2> (2798) /console/do/sem/offensesearch] openjpa-2.2.1-r422266:1396819 fatal general error org.apache.openjpa.persistence.PersistenceException: ERROR: missing FROM-clause entry for table "o" Position: 218 {prepstmnt -643663665 SELECT op.id FROM offense_properties op JOIN offense_view ov ON op.id=ov.id JOIN attacker_view av ON ov.attacker_id=av.id WHERE (INET(ip2address(av.network)) = INET('172.16.0.0/16')) AND op.dismissed_code 1 AND o.active_code 3} [code=0, state=42P01] May 28 15:26:46 <IP Address 1> [tomcat] [admin@<IP Address 2> (2798) /console/do/sem/offensesearch] at org.apache.openjpa.jdbc.sql.DBDictionary.narrow (DBDictionary.java:4958) ... 47 more lines ... May 28 15:26:46 <IP Address 1> [tomcat] [admin@<IP Address 2>(2798) /console/do/sem/offensesearch] Caused by: May 28 15:26:46 <IP Address 1> [tomcat] [admin@<IP Address 2>(2798) /console/do/sem/offensesearch] org.apache.openjpa.lib.jdbc.ReportingSQLException: ERROR: missing FROM-clause entry for table "o" Position: 218 {prepstmnt -643663665 SELECT op.id FROM offense_properties op JOIN offense_view ov ON op.id=ov.id JOIN attacker_view av ON ov.attacker_id=av.id WHERE (INET(ip2address(av.network)) = INET('172.16.0.0/16')) AND op.dismissed_code 1 AND o.active_code 3} [code=0, state=42P01] May 28 15:26:46 <IP Address 1> [tomcat] [admin@<IP Address 2>(2798) /console/do/sem/offensesearch] at

Table 3: Issues Resolved *(continued)*

Issue	Description
	org.apache.openjpa.lib.jdbc.LoggingConnectionDecorator.wrap(LoggingConnectionDecorator.java:219) May 28 15:26:46 <IP Address 1> [tomcat] [admin@<IP Address 2> (2798) /console/do/sem/offensesearch] at org.apache.openjpa.lib.jdbc.LoggingConnectionDecorator.access$700(LoggingConnectionDecorator.java:59) May 28 15:26:46 <IP Address 1> [tomcat] [admin@<IP Address 2> (2798) /console/do/sem/offensesearch] at org.apache.openjpa.lib.jdbc.LoggingConnectionDecorator.wrap(LoggingConnectionDecorator.java:203) May 28 15:26:46 <IP Address 1> [tomcat] [admin@<IP Address 2> (2798) /console/do/sem/offensesearch] at org.apache.openjpa.lib.jdbc.LoggingConnectionDecorator$LoggingConnection$LoggingPreparedStatement.executeQuery(LoggingConnection Decorator.java:1118) May 28 15:26:46 <IP Address 1> [tomcat] [admin@<IP Address 2> (2798) /console/do/sem/offensesearch] at org.apache.openjpa.lib.jdbc.DelegatingPreparedStatement.executeQuery(DelegatingPreparedStatement.java:265) May 28 15:26:46 <IP Address 1> [tomcat] [admin@<IP Address 2>(2798) /console/do/sem/offensesearch] at org.apache.openjpa.jdbc.sql.PostgresDictionary$PostgresPreparedStatement.executeQuery(PostgresDictionary.java:1019) May 28 15:26:46 <IP Address 1>[tomcat] [admin@<IP Address 2> (2798) /console/do/sem/offensesearch] at org.apache.openjpa.lib.jdbc.DelegatingPreparedStatement.executeQuery(DelegatingPreparedStatement.java:265) May 28 15:26:46 <IP Address 1> [tomcat] [admin@<IP Address 2> (2798) /console/do/sem/offensesearch] at org.apache.openjpa.jdbc.kernel.JDBCStoreManager$CancelPreparedStatement.executeQuery(JDBCStoreManager.java:1774) May 28 15:26:46 <IP Address 1> [tomcat] [admin@<IP Address 2 >(2798) /console/do/sem/offensesearch] at org.apache.openjpa.lib.jdbc.DelegatingPreparedStatement.executeQuery(DelegatingPreparedStatement.java:255) May 28 15:26:46 <IP Address 1> [tomcat] [admin@<IP Address 2 >(2798) /console/do/sem/offensesearch] at org.apache.openjpa.jdbc.kernel.SQLStoreQuery$SQLExecutor.executeQuery(SQLStoreQuery.java:318) May 28 15:26:46 <IP Address 1> [tomcat] [admin@<IP Address 2> (2798) /console/do/sem/offensesearch] at org.apache.openjpa.jdbc.kernel.SQLStoreQuery$SQLExecutor.executeQuery(SQLStoreQuery.java:221) May 28 15:26:46 <IP Address 1> [tomcat] [admin@IP Address 2 (2798) /console/do/sem/offensesearch] NestedThrowables: May 28 15:26:46 <IP Address 1> [tomcat] [admin@<IP Address 2> (2798) /console/do/sem/offensesearch] ... 42 more lines ... Steps to Recreate: • Do an offense search and check **Exclude Inactive Offenses** • Add a Source IP filter, IE: <IP Address 1> • An error has occurred, refresh your browser (press F5) and attempt the action again.

Table 3: Issues Resolved *(continued)*

Issue	Description
	Workaround: Do not use a Source IP filter search in junction with Exclude Inactive Offenses.
Rules that access reference set data may cause system performance degradation messages	After upgrading to JSA 2014.2 and later customers who use reference sets in rule tests may notice a sudden performance degradation leading to events being routed to storage around the CRE. This scenario is particularly bad when the reference sets are being compared against a large number of events in scenarios where the event property is not normally expected to be found in the reference set. The following entry may be seen in qradar.log: **com.q1labs.semsources.cre.CRE: [WARN] [NOT:0080004101][192.168.136.35/- -] [-/- -]Custom Rule Engine has sent a total of 400000000 event(s) directly to storage. 143638 event(s) were sent in the last 60 seconds. Queue is at 100 percent capacity.** *Workaround*: None.
Asset exports that take longer than 20 minutes will fail	In JSA 2014.1, exporting a list of assets will fail if the asset export takes longer
Event parsing order not properly respected by the event pipeline after parsing order is changed	If log source parsing order is changed for log sources with the same log source identifier, JSA does not reflect the change properly and that may cause event parsing issues.
"Last Seen Active" for assets with services remains blank after an initial va scan, but populates after a subsequent scan	After a newly created VA scan is run for the first time, any asset with Services will show the **Last Seen Active** field as blank until a subsequent scan is run.
Search failures due to /store/ariel/persistent_data partition becoming full	Searches fail when **/store/ariel/persistent_data** partition runs out of disk space and does not clear temporary files. This also then makes it impossible to run new searches until the temporary files are cleared out. This can be caused by having many failed searches and or long searches that have been terminated prior to completion or that fail. The temporary files will be located in **/store/ariel/persistent_data/ariel.ariel_proxy_server/data/** and will prefix with **Q1Tmp** and look similar to: Q1Tmp0fd58f2e-1b36-4181-89bd-2967e9828422 *Workaround*: Contact Juniper Customer Support for assistance in clearing the tmp files.

Table 3: Issues Resolved *(continued)*

Issue	Description
Search failures due to /store/sriel/persistent_data partition becoming full	Searches fail when **/store/ariel/persistent_data** partition runs out of disk space and does not clear temporary files. This also then makes it impossible to run new searches until the temporary files are cleared out. This can be caused by having many failed searches and or long searches that have been terminated prior to completion or that fail. The temporary files will be located in **/store/ariel/persistent_data/ariel.ariel_proxy_server/data/** and will prefix with "Q1Tmp..." and look similar to: **Q1Tmp0fd58f2e-1b36-4181-89bd-2967e9828422** *Workaround*: Contact Juniper Customer Support for assistance in clearing the tmp files.
Vulnerability RHSA-2014-0164	VULNERABILITY RHSA-2014-0164. Associated with following CVEs: • CVE-2013-5908 • CVE-2014-0001 • CVE-2014-0386 • CVE-2014-0393 • CVE-2014-0401 • CVE-2014-0402 • CVE-2014-0412 • CVE-2014-0437
Vulnerability 2014-7169	The script CVE-2014-7169.sh.gz patches the following vulnerability for JSA appliances: • CVE-2014-6271 • CVE-2014-7186 • CVE-2014-7187 • CVE-2014-6277 • CVE-2014-6278 For more information, see "Installing CVE Scripts" on page 3.
Forensics/PCAP IP tables line number error prevents rule updates	Iptables.post includes an error that is being injected by Forensics. The system attempts to open port 37 for time synchronization and this causes other protocols that update iptables to fail. *Workaround*: Open **opt/qradar/conf/iptables.post** in vi or vim, remove the ' 3', and save. Then run **/opt/qradar/bin/iptables_update.pl**.

Table 3: Issues Resolved *(continued)*

Issue	Description
Paired console high availability primary and secondary appliances may experience high disk load	If the console pair is in high availability and **/store/ariel/persistent_data** is mounted on its own partition the console may experience periods of high disk I/O due to an error which leads to all search results being replicated to the primary. The expected result is that only search results that have been protected should be synced to the secondary. *Workaround*: Contact Juniper Customer Support for a possible solution that may work in some instances.
The JSA UI session may not require login re-authentication in some session timeout instances	In JSA if you close all browser sessions the users session should timeout after the Persistent Setting Timeout setting elapses (10 minutes by default). There are some scenarios where this does not occur and the user remains authenticated past the timeout session.
If a reference set is not found when called by a rule, any subsequent reference sets will not be called	If a rule looks for a reference set that it cannot find, any subsequent reference sets in the rule test will not be called upon either.
Empty reference sets from earlier JSA revisions that are migrated during a patch cannot be used/referenced	When patching to JSA 2014.2 and later from a previous version a migration of reference sets occurs. Any reference sets that were empty prior to 2014.2 will not work after the patch is complete. *Workaround* :Do not use any reference sets that were empty prior to patching, create new reference sets instead.
An error message appears when trying to open the Manage Search Results screen	When navigating to the Manage Search Results screen, an error message appears similar to: **An error has occurred. Refresh your browser (press F5) and attempt the action again.** If the problem persists, please contact Juniper Customer Support for assistance. The following error will be seen in the logs: **Caused by: java.lang.NullPointerException at com.q1labs.ariel.ui.UIArielServices.getFullArielQueryList (UIArielServices.java:1024) at com.q1labs.ariel.ui.UIArielServices.getArielQueryListCount (UIArielServices.java:1220) ... 35 more**
Last Seen Active for assets with services remains blank after an initial VA scan, but populates after a subsequent scan	After a newly created VA scan is run for the first time, any asset with Services will show the **Last Seen Active** field as blank until a subsequent scan is run.

Table 3: Issues Resolved *(continued)*

Issue	Description
Configuration restore can fail on a system migrated from 2010- broken triggers left hanging around	Backup Configuration restore can fail with the following errors present in qradar.log: Feb 5 18:38:22 [hostcontext.hostcontext] [BackupServices_restore] org.postgresql.util.PSQLException: ERROR: null value in column "schemaname" violates not-null constraint Detail: Failing row contains (ariel_property, null). Where: SQL statement "INSERT INTO rep.replicate_truncate VALUES ('ariel_property')" PL/pgSQL function replicate_track_truncate_ariel_property()line 4 at SQL statement Steps to Recreate: Patch your box in the following order: [user1@oc7184128236 67080]$ egrep 'Installed.*QRadar|Upgraded.*QRadar|patch' var/log/install.log Mon Jan 9 17:02:25 GMT 2012: Installed QRadar version 7.0.0.219547. Tue Jan 10 11:56:50 EST 2012: Applied 7.0.0.226721-700_patchupdate-7.0.0.226721 to 7.0.0.219547 Tue Jan 10 12:03:44 EST 2012: Applied 7.0.0.236444-700_patchupdate-7.0.0.236444 to 7.0.0.219547 Tue Jan 10 12:03:45 EST 2012: Applied 7.0.0.238823-700_patchupdate-7.0.0.238823 to 7.0.0.219547 Tue Jan 10 12:03:49 EST 2012: Applied 7.0.0.241982-700_patchupdate-7.0.0.241982 to 7.0.0.219547 Tue Jan 10 12:04:06 EST 2012: Applied 7.0.0.247969-700_patchupdate-7.0.0.247969 to 7.0.0.219547 Tue Mar 13 21:53:49 GMT 2012: Applied 7.0.0.260907-700_patchupdate-7.0.0.260907 to 7.0.0.219547 Tue Mar 13 21:58:31 GMT 2012: Applied 7.0.0.263204-700_patchupdate-7.0.0.263204 to 7.0.0.219547 Tue Mar 13 22:01:54 GMT 2012: Applied 7.0.0.267307-700_patchupdate-7.0.0.267307 to 7.0.0.219547 Fri Jul 13 14:55:14 GMT 2012: Applied 7.0.0.276729-700_patchupdate-7.0.0.276729 to 7.0.0.219547 Fri Jul 13 14:57:24 GMT 2012: Applied 7.0.0.288468-700_patchupdate-7.0.0.288468 to 7.0.0.219547 Fri Jul 13 14:57:38 GMT 2012: Applied 7.0.0.301503-700_patchupdate-7.0.0.301503 to 7.0.0.219547 Fri Jul 13 14:57:41 GMT 2012: Applied 7.0.0.322258-700_patchupdate-7.0.0.322258 to 7.0.0.219547 Fri Jul 13 15:01:02 GMT 2012: Applied 7.0.0.325222-700_patchupdate-7.0.0.325222 to 7.0.0.219547 Fri Aug 3 13:30:54 GMT 2012: Applied 7.0.0.342942-700_patchupdate-7.0.0.342942 to 7.0.0.219547 Wed Nov 14 11:16:06 EST 2012: Upgraded QRadar Log Manager to version 7.1.0.414913 Wed Nov 14 11:17:51 EST 2012: Installed QRadar version 7.1.0.414913. Wed Nov 14 11:29:04 EST 2012: Upgraded QRadar from version 7.0.0.342942 to version 7.1.0.414913 Thu Jan 17 16:29:04 EST 2013: Applied 7.1.0.431888-

Table 3: Issues Resolved *(continued)*

Issue	Description
	710_patchupdate-7.1.0.431888 to 7.1.0.414913 Thu Jan 17 16:29:09 EST 2013: Applied 7.1.0.445128-710_patchupdate-7.1.0.445128 to 7.1.0.414913 Thu Jan 17 16:34:20 EST 2013: Applied 7.1.0.449508-710_patchupdate-7.1.0.449508 to 7.1.0.414913 Thu Jul 11 14:02:30 EDT 2013: Applied 7.1.0.457882-710_patchupdate-7.1.0.457882 to 7.1.0.414913 Thu Jul 11 14:03:49 EDT 2013: Applied 7.1.0.495292-710_patchupdate-7.1.0.495292 to 7.1.0.414913 Thu Jul 11 14:10:06 EDT 2013: Applied 7.1.0.501605-710_patchupdate-7.1.0.501605 to 7.1.0.414913 Thu Jul 11 14:10:45 EDT 2013: Applied 7.1.0.519185-710_patchupdate-7.1.0.519185 to 7.1.0.414913 Thu Jul 11 14:16:56 EDT 2013: Applied 7.1.0.581477-710_patchupdate-7.1.0.581477 to 7.1.0.414913 Fri Aug 30 09:33:22 EDT 2013: Running "/media/updates/installer --exec" from /media/updates using Patch /var/tmp/720_QRadar_patchupdate-7.2.0.614901.sfs Fri Aug 30 09:59:12 EDT 2013: Upgraded QRadar to version 7.2.0.599863 from version 7.1.0.581477 Fri Aug 30 10:12:00 EDT 2013: Upgraded QRadar to version 7.2.0.614901 from version 7.2.0.599863 Fri Aug 30 10:56:02 EDT 2013: Running "/media/updates/installer --exec" from /media/updates using Patch /var/tmp/720_QRadar_patchupdate-7.2.0.614901.sfs Tue Oct 8 10:00:53 EDT 2013: Running "/media/updates/installer --exec" from /media/updates using Patch /tmp/720_QRadar_patchupdate-7.2.0.666700.sfs Tue Oct 8 10:03:08 EDT 2013: Upgraded QRadar to version 7.2.0.636622 from version 7.2.0.614901 Tue Oct 8 10:11:26 EDT 2013: Upgraded QRadar to version 7.2.0.666700 from version 7.2.0.636622 After your box is patched or upgraded run a config backup and restore. *Workaround*: Please contact Juniper Customer Support for assistance in restoring the backup.

Table 3: Issues Resolved *(continued)*

Issue	Description
Orderby table alias incorrectly defined in SNMP event.createeventfromoffense	The OffenceCRE may generate the following error and exception, which will cause the SNMP event notification to fail to be generated. **Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] com.q1labs.core.dao.sem.views.OffenseView: [ERROR] [NOT:0000003000][x.x.x.x/- -] [-/- -]An error occurred while parsing the query filter Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at org.apache.openjpa.kernel.exps.AbstractExpressionBuilder.parseException(AbstractExpressionBuilder.java:119) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at org.apache.openjpa.kernel.jpql.JPQLExpressionBuilder.getPath(JPQLExpressionBuilder.java:1958) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at org.apache.openjpa.kernel.jpql.JPQLExpressionBuilder.getPathOrConstant(JPQLExpressionBuilder.java:1891) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at org.apache.openjpa.kernel.jpql.JPQLExpressionBuilder.eval(JPQLExpressionBuilder.java:1189) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at org.apache.openjpa.kernel.jpql.JPQLExpressionBuilder.getValue(JPQLExpressionBuilder.java:2084) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at org.apache.openjpa.kernel.jpql.JPQLExpressionBuilder.getValue(JPQLExpressionBuilder.java:2070) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at org.apache.openjpa.kernel.jpql.JPQLExpressionBuilder.evalOrderingClauses(JPQLExpressionBuilder.java:532) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at org.apache.openjpa.kernel.jpql.JPQLExpressionBuilder.getQueryExpressions(JPQLExpressionBuilder.java:306) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at org.apache.openjpa.kernel.jpql.JPQLParser.eval(JPQLParser.java:67) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at org.apache.openjpa.kernel.ExpressionStoreQuery$DataStoreExecutor.<(ExpressionStoreQuery.java:763) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at org.apache.openjpa.kernel.ExpressionStoreQuery.newDataStoreExecutor(ExpressionStoreQuery.java:179) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at**

Table 3: Issues Resolved *(continued)*

Issue	Description
	org.apache.openjpa.kernel.QueryImpl.createExecutor (QueryImpl.java:749) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at org.apache.openjpa.kernel.QueryImpl.compileForDataStore (QueryImpl.java:707) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at org.apache.openjpa.kernel.QueryImpl.compileForExecutor (QueryImpl.java:689) > Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at org.apache.openjpa.kernel.QueryImpl.compile(QueryImpl.java:589) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at org.apache.openjpa.persistence.EntityManagerImpl.createQuery(EntityManagerImpl.java:997) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at org.apache.openjpa.persistence.EntityManagerImpl.createQuery(EntityManagerImpl.java:979) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at org.apache.openjpa.persistence.EntityManagerImpl.createQuery(EntityManagerImpl.java:102) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] atcom.q1labs.frameworks.session.JPASessionDelegate.createQuery(JPASessionDelegate.java:229) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at com.q1labs.frameworks.session.JPASessionDelegate.queryForList(JPASessionDelegate.java:606) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at com.q1labs.core.dao.sem.views.OffenseView.getAnnotationsForDisplay(OffenseView.java:1617) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at com.q1labs.sem.types.snmp.SNMPEvent.createEventFromOffense (SNMPEvent.java:974) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at com.q1labs.sem.magi.cre.responses.SNMPResponse.apply (SNMPResponse.java:38) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at com.q1labs.sem.magi.cre.responses.ResponseLoggingDecorator.apply (ResponseLoggingDecorator.java:37) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at com.q1labs.sem.magi.cre.Rule.createResponseEvents (Rule.java:498) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at com.q1labs.sem.magi.cre.CRE.process(CRE.java:340) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at com.q1labs.sem.magi.cre.CRE.run(CRE.java:271) Feb 17 10:36:46 x.x.x.x [ecs] [Offense CRE] at java.lang.Thread.run(Thread.java:780)

Related Documentation

- New and Updated Functionality on page 2
- Installing JSA on page 3
- Known Issues and Limitations on page 5

Documentation Updates

This section lists the errata or changes in Juniper Secure Analytics (JSA) documentation.

- Documentation Updates for JSA Hardware Documentation on page 27

Documentation Updates for JSA Hardware Documentation

- **How to Set Up Your JSA3800 Appliance**—In the Physical Specifications section, the weight of the JSA3800 is wrongly documented as 37 lb. The actual weight of JSA3800 is 27.9 lb.
- **How to Set Up Your JSA5800 Appliance**—In the Physical Specifications section, the weight of the JSA5800 is wrongly documented as 50 lb. The actual weight of JSA5800 is 41.9 lb.

Related Documentation

- New and Updated Functionality on page 2
- Installing JSA on page 3
- Known Issues and Limitations on page 5
- Resolved Issues on page 6