Juniper Secure Analytics Release Notes

2013.2
September 2015

Juniper Networks is pleased to introduce STRM/JSA 2013.2.

Security Threat Response Manager (STRM)/Juniper Secure Analytics (JSA) 2013.2 Release Notes provides new features, known issues and limitations, and fixes to known issues.

Contents

New and Updated Functionality

STRM/JSA 2013.2 introduces the following new and updated features.

- **Reference data collections:** Extends the Reference Set function to include complex and structured data into correlation, analysis, and reports. This capability allows you to include extended user identity groups, attributes, and asset information into STRM/JSA, and integrate of STRM/JSA with other Juniper Networks and Juniper Networks Business Partner solutions. For more information on reference data collections, see the Reference Data Collections Technical Note.
- **Read-only role permissions:** Adds STRM/JSA user role permissions that grant read-only privileges to STRM/JSA data. This feature is suitable for auditors who perform audit-related activities. For more information on new role permissions, see the STRM/JSA Administration Guide.
- **VMWare ESX 5.0 support for Virtual Appliances:** Adds support for VMware ESX 5.0 and maintains support for VMware ESX 4.x.
- **Accumulator enhancement:** Improves historical sampling and trend analysis functions to allow for more granular and precise time ranges. For more information on new data accumulation options on the event and flow search pages, see the STRM/JSA User Guide.
- **Notification enhancement:** Improves the system notification functions to provide a convenient and effective display of critical system messages. For more information on new Messages feature, see the STRM/JSA Administration Guide.
- **DSM reload:** Removes the need to restart certain event processing pipeline functions after installation or upgrade of a DSM.
- **Hard disk monitoring:** Adds a tool to monitor the appliance hard drive and generate system notifications in the event of hard drive failures or error conditions. This tool is enabled by default on Juniper Networks appliances.

Related Documentation

- Installing 2013.2.R11 on page 2
- Resolved Issues on page 3
- Known Issues and Limitations on page 6

Installing 2013.2.R11

To install STRM 2013.2.R11:

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

Related Documentation

- Known Issues and Limitations on page 6

Resolved Issues

The following issues are resolved in STRM/JSA 2013.2:

- **During the recovery partition, JSA2013.2.R4 will not mount /store.**

  You need to manually mount /store.

- **Re-installation might fail on STRM/JSA 2013.2.r2 patch system**

  An issue might occur on STRM/JSA 2013.2.r2 patch system where a re-installation from recovery partition could fail.

- **Event and flow search dashboard items do not display time series data after enabling data capture**

  On the **Dashboard** tab, if you start accumulation by clicking the **Capture Time Series Data** check box on event search or flow search dashboard items, the time series data might not load for an extended period of time.

- **Chart legends in generated reports no longer display truncated legend labels**

  On the **Reports** tab, generated reports might include charts that have truncated legend labels.

- **Duplicate report group database entries**

  A report group database table entry is created for every generated STRM/JSA report. This entry is duplicated for each user that received the generated content, which is multiplied by the number of groups that are associated with the report templates. Since these duplicated table entries are never removed, it causes unnecessary bloating. This bloating causes reports to take several minutes to load.

- **Accumulator rolls up unique counts incorrectly**

  The accumulator component does not roll up unique counts correctly after the first 1-minute interval.

- **My Offenses page of the Offenses tab might filter on the wrong username**

  An issue might occur where the My Offenses page of the Offenses tab might filter on the wrong username.

- **Moncton time zone not supported**

  The IBM JRE does not properly recognize the Moncton time zone region.

- **Restarting Tomcat causes reports to display incorrect time**

  Restarting the Tomcat process causes reports to display the date and time when Tomcat restarted instead of the date and time that the report generated.

- **Quick filter syntax error occurs**

  On the **Log Activity** and **Network Activity** tabs, if you enter a search string that includes the NOT operator, the filter might not return correct results.

- **"Contains" and "Contains Any Of" filter operators does not return expected results**

  On the **Log Activity** and **Network Activity** tabs, if you use the **contains** or **contains any** of filter operators for a filter, the filter results only include events or flows that exactly match your search string. The filter results do not include events or flows that partially match your search string, as implied by the operator name.

- **STRM/JSA Virtual Console do not send flows to a replaced console appliance while the temporary license is applied**

  If you replace a console appliance in a deployment that includes STRM/JSA Virtual console, these QFlow Collectors do not send flows to the new console. The 30-day temporary license does not get decrypted on the STRM/JSA Virtual console because the console appliance has a different serial number than the original console appliance.

- **Offense rules no longer fail to log syslog events locally**

  On the Rule Response page of the Rules Wizard, you can configure a rule to send an event or flow to the local syslog file. Offense rules might fail to log syslog events locally.

- **Benign error message displays when failover occurs on HA cluster configured with a shared offboard storage solution**

  During a failover on an HA cluster configured with a shared fibre channel or ISCSI storage solution, the following benign error message is displayed: **Failed to add static route to secondary**.

- **Improves response limiter values in default rules**

  This release improves the response limiter default value for some default rules.

- **Offense summary list for a renamed network does not open**

  On the By Network page, when you select a network to open the offense summary list, an error occurs. This happens when a network name changes and the user is not reassigned to the new network name.

- **No error message is displayed if the User Password field is empty in the IF-MAP Client/Server Settings pane on the System Settings window**

  The **User Password** field in the IF-MAP Client/Server Settings pane on the System Settings window does not display an error message if you do not type a password in the field. If you save your system settings without configuring a password, the console connection to the IF-MAP server fails.

- **Encrypted QFlow Collectors unable to connect to non-encrypted Event Collectors**

  When an encrypted QFlow Collector is configured to connect to non-encrypted Event Collector using Port 22, communication fails between the two managed hosts.

- **STRM/JSA appliances do not support USB flash-drive installations**

  STRM/JSA appliances do not currently support STRM/JSA software installation using a bootable USB flash-drive.

- **After changing the Backup Repository Path parameter, the existing backups list does not retain previous backup archive files**

After you edit the **Backup Repository Path** parameter on the **Backup Recovery Configuration** window, the Existing Backups pane no longer lists the backup archives that are stored in the previous backup repository.

- **AQL Event and Flow Query CLI searches return no results when searching custom property names with spaces**

  An error occurs in the AQL Event and Flow Query CLI where no results are returned when you search for custom properties that include spaces in the property name.

- **Report templates that are configured to include only closed offenses does not display results in the generated reports**

  When you create a report to generate closed offenses using the **Report Wizard > Container Details - Top Offenses** window, if you select only the **Closed Offenses** option in the Include pane and ensure the other check boxes are clear, the report generates no results.

- **Unable to delete user roles and security profiles**

  When you use the Mozilla Firefox 16.0.2 web browser to view the user interface, the following issues occur when you manage users on the **Admin** tab:

  - When you delete a user role, a list of users that are assigned that role are displayed. You are prompted to select another user role for the users from a list box. This list box is disabled; therefore, you are unable to complete the procedure to delete the user role.
  - When you delete a security profile, a list of users that are assigned that security profile are displayed. You are prompted to select another security profile for the users from a list box. This list box is disabled; therefore, you are unable to complete the procedure to delete the security profile.

- **Error occurs when you click the Admin tab more than once**

  If you click the **Admin** tab more than once to reload the page, a System Error window opens.

- **Common Interface File System (CIFS) plug-in restored**

  This maintenance release restores the CIFS file system.

- **Custom email notification does not generate if configured to include USB device IDs**

  If you configure the alert-config.xml file to include USB device IDs, the expected email notification does not generate.

- **Event Name filter for specific log source type does not function correctly**

  On the **Log Activity** tab, if you add the **Event Name** filter for a specific log source type, the search does not complete.

Related Documentation

- Installing 2013.2.R11 on page 2
- Known Issues and Limitations on page 6

Known Issues and Limitations

This section describes the known issues and limitations for the following areas:

General

- **JSA7500 event processor performance optimization**

  When log source sends around 20,000 events per second to the JSA7500 event processor, the event starts dropping.

  Workaround: None.

- **Deploying a JSA appliance with image 2013.2.r3.607582 requires reimaging to the common image**

  When deploying a JSA appliance with image 2013.2.r3.607582, you must reimage the appliance to the common image 2013.2.r3.615469.

  Workaround: For reimaging the JSA appliance from 2013.2.r3.607582 to 2013.2.r3.615469, see Installing JSA Using a Bootable USB Flash-Drive Technical Note.

- **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 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.

- **During an initial setup of a JSA appliance, the time zone page does not display the list of time zones**

  When configuring a JSA appliance, the appliance displays an error *0 Longyearbyen* instead of listing the time zones in the time zone screen.

  Workaround: When deploying a JSA appliance with image 2013.2.r3.607582, you need to reimage the appliance to the common image 2013.2.r3.615469. For reimaging the JSA appliance from 2013.2.r3.607582 to 2013.2.r3.615469, see *Installing JSA Using a Bootable USB Flash-Drive Technical Note.*

- **EP/FP combo in a distributed setup fails to complete upgrade to 2013.2r2**

  

  NOTE: This issue occurs only if you are upgrading STRM/JSA using the ISO file.

  During the upgrade of EP/FP combo in a distributed setup to 2013.2 R2 starting from 2009.2, the upgrade is not complete.

  Workaround: Run the /root/complete_upgrade.sh script to complete the upgrade.

- **Upgrading an STRM/JSA 5000 EP in a distributed setup fails**

  When an STRM/JSA 5000 EP which is installed with a base version of 2008 or 2009.2 is upgraded to 2013.2 R2 in a distributed setup, the upgrade process fails due to invalid appliance ID configuration.

  Workaround:

  

  NOTE: This workaround is applicable only for STRM/JSA 5000 EPs which are installed with the base version of 2008 or 2009.2. The minimum upgrade requirement for 2013.2 R2 is 2012.1. Before proceeding with the following workaround, ensure that the STRM/JSA 5000 EP setup is installed with 2012.1 ISO.

  Before you upgrade the STRM/JSA 5000 EP to 2013.2 R2:

  1. Log in to your system as the root user.
  2. Type the following command:**/opt/oem/branding/getkey**
  3. Select **1602 JN-LG-STRM-EP**. Select **Next** and press **Enter.**

     The system gets activated with the correct appliance ID and activation key for the STRM/JSA 5000 EP which is required for upgrading to 2013.2 R2.

- **Events without valid IPv4 addresses trigger rules incorrectly**

  Events that do not have a valid IPv4 address in the event payload for the source and destination parameters derive their IP address from the log source. This causes an issue when the log source resides in an IPv6 network. This incorrectly indicates that all

events from the log source shares the same IP address and this triggers the wrong rules, such as Excessive Firewall Anomaly rules.

- **Authentication icon on Admin tab displays for users who do not have the Administrator Manager and Remote Networks and Services Configuration role permission**

  On the **Admin** tab, the **Authentication** icon is displayed in error for users who do not have the Administrator Manager or Remote Network and Services role permission. When the user clicks the icon, an empty window is displayed.

- **Special characters in group names cause group name to display as a beta symbol**

  When creating a group, such as a Log Source group, if you include a symbol in the group name, the group name fails to display. Instead, a beta symbol is displayed as the group name. This error can occur for all group types in the **Log Activity, Network Activity, Offenses, Rules,** and **Reports** tabs.

  Workaround: Avoid using special characters in group names.

- **STRM/JSA virtual appliances are configured with a network interface flow source**

  The STRM/JSA virtual appliances have only one flow source configured for NetFlow, however eth0 network interface is configured with a second flow source. The second type of the flow source is **Network Interface.**

- **Menus display incorrectly after resizing your browser window**

  After resizing your browser window, if you click a menu item to display a list box, the list box displays near the center of your window, instead of under the menu as expected. This error occurs on all tabs of the user interface.

- **STRM/JSA Virtual Console virtual appliance limits are incorrect on the License window of the Admin tab**

  On the **License** window of the **Admin** tab for the STRM/JSA user interface, the Events Per Second (EPS) and Flows Per Interval (FPI) limits are incorrect. The default EPS is 1,000 and default FPI is 50,000.

- **ECS service might restart during periods of heavy processing load**

  If your system is experiencing heavy processing load, the Event Collection System (ECS) service might restart.

- **System notification incorrectly specifies data is being dropped**

  When the accumulator cannot process time intervals for flow or event data quickly enough, the following system notification is displayed on the **Dashboard** tab: **Flows/Events were dropped by the accumulator**. This system notification incorrectly described the problem. No data is being dropped.

- **Accumulator generates errors after deleting a custom event or flow property**

  After you delete a custom event or flow property, the accumulator generates errors associated with the deleted property. The following error message is displayed: **Custom property with ID Custom property with ID doesn't exist but it is referenced in a currently active search.**

- **Discrepancy in number of events specified in system notification and the list of events**

A discrepancy can occur between the number of events indicated in a system notification on the Messages window and the corresponding list of events. For example, if you click the **View All 23** link in a system notification, the List of Events window might display 25 events.

System Configuration

- **STRM/JSA objects associated to deleted users**

  After deleting a user, STRM/JSA objects, such as reports and saved searches, might remain associated to the deleted user. There is no option for re-assigning the objects to a current user.

  Workaround: Contact Juniper Customer Support.

- **Deployment editor times out when inactive for extended periods of time**

  If you leave the deployment editor open and inactive for an extended period of time, the deployment editor could timeout due to inactivity.

  Workaround: To close the deployment editor, access your operating system task manager and terminate the deployment editor process.

- **Upgrades fail if all flow sources are disabled**

  If you disable all flow sources for your QFlow Collector, the QFlow service might stop. If you subsequently upgrade STRM/JSA, the upgrade process detects that the QFlow service is not running and the upgrade fails.

  Workaround: Contact Juniper Customer Support.

- **Error occurs if 50 days have elapsed since Event Collection Service (ECS) was restarted**

  If 50 days have elapsed since the ECS service on your system has been restarted, rules that are configured to send Simple Network Management Protocol (SNMP) traps might generate errors.

  Workaround: Log in to your system as the root user and restart the ECS service.

- **LDAP authentication functions incorrectly if the server URL is a DNS or FQDN**

  LDAP authentication does not function if a Domain Name System (DNS) Fully Qualified Domain Names (FQDN) is configured in the **Server URL** parameter on the **Authentication Configuration** window.

- **Error message displays after you deploy configuration changes when your system experiences high process loads**

  After deploying your configuration changes on the **Admin** tab, the **$ is not defined** error message might be displayed if your system experiences high process loads.

  Workaround: Refresh your browser window.

- **Tomcat service threshold for the maximum number of clients can be reached when you add managed hosts**

  If the number of managed hosts in your deployment exceeds a certain threshold, the Tomcat service might indicate that you have reached the maximum number of clients.

- **AQL Event and Flow Query Command Line Interface (CLI) "Username != N/A" query does not function correctly**

  In the AQL Event and Flow Query CLI, data searches that use the **userName != N/A** query does not yield the correct results. The results include usernames that have a value of N/A.

- **Error occurs when you add a network hierarchy group with the same CIDR as another network hierarchy group**

  On the **Network Views** window, an error occurs if you attempt to add a group that has the same CIDR as an existing group.

- **Previously stored log source protocol file information is not included in a configuration backup archive**

  When you back up your configuration files, the list of log source protocol files and other log source state information is not backed up. After you restore your system, your protocols should still function, however, the protocols need to reload the information.

- **Installation sequence issues if you attempt to assign an IP address already in use**

  When you install STRM/JSA, if you attempt to assign an IP address that is already in use, a message is displayed to indicate that you must resolve this before you proceed. After you resolve the duplicate IP address issue and try to continue the installation procedure, the installation script does not complete correctly. A number of steps are skipped. Your console becomes unreachable after the installation is complete. When you restart the appliance, you are prompted to start the installation procedure from the start.

- **Patch installer repeats a prompt twice**

  When you use the patch installer to install a maintenance release patch, the **Do you want to turn on DSM auto-install and deploy through Auto Updates?** prompt can be displayed twice.

- **Heavy use of manual port scans causes excessive system load**

  If you start a large amount of port scans manually, your system experiences excessive system load.

  Workaround: Restart your system and avoid running excessive manual port scans.

- **Database exceptions occur after you update the Transaction Max Time Limit setting**

  On the **Admin** tab, if you select **System Settings** and update the **Transaction Max Time Limit** setting, database exceptions occur.

  Workaround: Do not change the **Transaction Max Time Limit** setting.

- **No installation progress is displayed for DSMs**

  DSM installation can take an extended period of time to complete. STRM/JSA does not display user feedback about the DSM installation progress. This can give the false impression that the installation process has failed.

- **No system notification exists to indicate replication failure caused by a locked RPM database**

When replication fails between a console and the managed hosts because of a locked RPM database, no system notification is displayed on the **Dashboard** tab.

- **Upgrades and patches fail on systems that use a self-signed certification that includes a passphrase**

  If you use a self-signed certificate that includes a passphrase on your STRM/JSA system, patches and upgrades on your host fail when the services attempt to restart.

  Workaround: Before you upgrade, remove the passphrase requirement from your certificate:

  1. Log in to your system as the root user.
  2. Type the following command:
     openssl rsa -in private.key -out newprivate.key
  3. Install the new private key on your system. For more information, see the *Replacing the SSL Certificate* technical note.
  4. Proceed with your upgrade.
  5. After the upgrade is complete, replace the new private key with your self-signed certificate, if required.

- **Data Reduction Ratio parameter displays negative numeric values**

  On the **System Summary** dashboard item, the **Data Reduction Ratio** parameter displays negative numeric values when your system experiences high Event Per Second (EPS) rates.

- **RX packets might drop from network interfaces**

  An issue might occur where RX packets fail to transmit from your network interfaces, due to an inadequate ring buffer size. If this occurs, system notifications are displayed to indicate that RX packets are dropped.

  Workaround: Contact Juniper Customer Support for assistance. Juniper Customer Support can increase your ring buffer size.

- **Systems notifications might transmit on an unencrypted port in an encrypted deployment**

  On an encrypted deployment, where the console and managed hosts are encrypted, communication between hosts occurs on Port 22. An issue might occur where internal system notifications might transmit on Port 514, which is an unencrypted port.

- **Email server outage occurs if valid email addresses are not specified in the user interface**

  During STRM/JSA installation, you are required to configure an email server. After installation, if you do not configure feature-specific email address fields in the user interface, all system mail is sent to the email server specified during installation. This causes a large volume of unwanted email messages being delivered to the mail server, because the default emails addresses are not recognized as valid.

  Workaround: Configure a valid email address for each of the following fields:

- **Administrative Email Address** field in the System Settings window.
- **Alert Email From Address** in the System Settings window
- Notification Preferences page on the **Offenses** tab
- **Enter email addresses to notify** field on the Rules Response page of the Rules Wizard
- **Enter the report distribution email address(es)** field in the Reports Wizard

- **Java Logging does not function on systems that use IPv6 as the Internet Protocol**

  Java logging does not function on systems that use IPv6 as the internet protocol.

- **Unable to restore an IPv6 backup archive on an IPv4 system**

  If you create a backup archive on a system that uses IPv6 as the Internet Protocol and then restore the backup archive on system that uses IPv4, the system that uses IPv4 fails.

- **Pre-test fails on deployments that include pre-2012.1 off-site flow sources**

  On deployments that include off-site flow sources that use STRM/JSA 2009.2 or earlier, the upgrade to STRM/JSA 2013.2 fails the pre-test. This occurs because STRM/JSA 2013.2 does not support pre-2012.1 flow sources.

  Workaround: If your pre-test fails, log in to the STRM/JSA user interface and access Flow Sources window of the STRM/JSA user interface. Remove all pre-2012.1 off-site flow sources from the list. These flow sources display **Pre-2012.1 Offsite Flow Source** in the **Flow Source Type** column. After these flow sources are deleted, your upgrade should complete successfully. If you want to re-add the off-site flow sources after your upgrade is complete, you must install STRM/JSA 2013.2 on these hosts.

- **System failed to start after an uncontrolled shutdown**

  An issue occurred where the STRM/JSA system did not start properly after an uncontrolled shutdown while a deployment change was in process.

- **Time synchronization causes error on encrypted managed hosts**

  If you synchronize the time on an encrypted managed host, the time is synchronized to the local host instead of the console. This error prevents the managed host from updating the time settings when the console time changes.

- **Formatting error in exported data and reports for the Log Source Date and Log Source Time parameters**

  Reports, XML exports, and CSV exports display both the **Log Source Date** and **Log Source Time** parameters using the following format: yyyy-mm-dd hh:mm:ss. For example:
  <device Date> 2012-11-02 15:13:15 </deviceDate>
  <device Time> 2012-11-02 15:13:15 </deviceTime>

- **Error message indicates incorrect build number after upgrade failure**

  If your upgrade to STRM/JSA 2013.1 fails, the error message indicates the STRM/JSA build your system is currently using. This build number might be incorrect on a patched system. This issue does not affect your system performance.

- **Benign error message fills up log file and causes system errors**

  The qflow.debug file on your system might fill the /var/log with the following message: *Unsupported network layer protocol*. This error message is benign. When this occurs, the /var/log file is unable to rotate. When the /var/log file ceases to rotate, system notifications are displayed to indicate any system performance issues that occur as a result.

- **Application error occurs when you view a reference set that contains elements that include special characters**

  On the Reference Set Management window, an application error occurs when you select a reference set and click View if the reference set contains elements that include special characters.

- **Data deserialization causes time series chart to fail**

  After your system restarts, an issue with the data deserialization, which is required for time series charts, causes the chart display to fail and the following message to be displayed in the error log: *Could not deserialize Query Handle.*

- **Server Discovery fails to automatically discover DNS servers**

  An issue might occur where your system fails to automatically discover a DNS server sending bilateral traffic on Port 53 on your network.

- **TCP traffic on Port 1900 might incorrectly map as Misc.UPnP**

  The STRM/JSA application mapping process might incorrectly map TCP traffic on port 1900 as **Misc.UPnP.**

- **Summary line on Log Source window display incorrect item count**

  On the Log Source window, the summary line at the bottom of the page might show an incorrect log source count. For example, the line might say **Displaying 0 to 0 of 0 items** even though there are log sources listed on the page.

- **Backup archives fail on managed hosts with an underscore character in the host name.**

  On a managed host, the backup archival process ceases if the system's host name contains the underscore (_) character.

  Workaround: Rename your managed hosts to exclude the underscore character.

- **Backup restoration fails if you do not restore the deployment configuration**

  When you restore a backup archive, the restoration fails if you clear the **Deployment Configuration** check box on the Restore a Backup window.

- **Unable to add a QFlow Collector virtual appliance with failed Postfix service to your deployment**

  On the Deployment Editor window, an error occurs when you add a QFlow Collector virtual appliance to your deployment. This error occurs if the Postfix service failed on the virtual appliance.

  Workaround: If the **Could not add host to deployment, See log for details** error message is displayed when you add the virtual appliance, log in to the virtual appliance as the root user and restart the Postfix service.

- **Microsoft patch causes System Setup window to fail**

  The System Setup window might fail to open if the desktop system that you use to access the STRM/JSA user interface uses the Microsoft KB2661254 patch. This patch causes an issue with the RSA certificate on your system.

  Workaround: Log in to your system as the root user and type the following commands:
  cat /etc/httpd/conf/certs/cert.key > /etc/webmin/miniserv.pem
  cat /etc/httpd/conf/certs/cert.cert >> /etc/webmin/miniserv.pem
  service webmin restart

- **Unable to delete a security profile if it is the only security profile in a filtered list**

  On the Security Profile Management window, if you enter a value in the **Type to filter** field and only one security profile is displayed, you cannot delete that security profile. Your system must contain at least one security profile. When a filter only returns one result, the system incorrectly treats it as the last security profile and does not allow you to delete it.

- **Upgrade to STRM/JSA 2013.1 reverts your embedded SNMP daemon settings to the default settings**

  After you upgrade to STRM/JSA 2013.1, any customer setting you configured for the embedded SNMP daemon is reverted to the default settings.

- **Deleting a log source does not remove the log source from an administrative Security Profile**

  When you delete a log source from your system and the log source continues to send logs, the log source remains associated to Security Profiles for administrative users who were granted access to this log source.

- **STRM/JSA 2013.1 upgrade fails on QFlow Collector systems that use IPv4**

  An issue might occur when you upgrade a QFlow Collector to STRM/JSA 2013.1. The upgrade process detects that the system uses IPv6 and fail to proceed if the system actually uses IPv4.

- **Unable to add a forwarding destination with a destination port of more than 32001**

  On the Forwarding Destination window, after you successfully add a forwarding destination with a destination port 32001 and higher, the following error message is displayed when the user interface restarts: **Failed to create forwarding destination**. The forwarding destination is no longer displayed in the user interface

  Workaround: Do not configure a forwarding destination with a destination port of more than 32000.

- **The Add Flow Source Alias window does not prevent you from saving a flow source alias without an IP address**

  On the Add Flow Source Alias window, an error does not display if you save the flow source alias without specifying an IP address in the IP field. This issue causes the QFlow process to fail to restart after the changes are deployed.

  Workaround: Remove and recreate the flow source alias with a value in the IP address field.

- **Users might have ungranted access to network activity**

  If a user has a Security Profile that has the **Network OR Log Sources** permission precedence, users who are assigned this Security Profile might have access to flows from a network that is not on the **Assigned Networks** list.

- **Default quick searches does not display for new administrative users after the upgrade to STRM/JSA 2013.2**

  After you upgrade your system, default quick searches is not listed in the Quick Searches list box for administrative users that you create after the upgrade.

High Availability (HA) Issues

- **Primary of HA in AIO setup and as console in distributed setup fails to complete upgrade to 2013.2r2 while starting from 2009.2**

  

  NOTE: **This issue occurs only if you are upgrading STRM/JSA using the ISO file.**

  During the upgrade of primary of HA as console and AIO(5000) to 2013.2 R2 starting from 2009.2, whenever the fstab configuration does not match with the configuration defined in the ha.conf, the primary upgrade is not complete.

  Workaround: Run the /root/complete_upgrade.sh script to complete the primary upgrade

- **The About STRM/JSA page does not accurately indicate whether the primary or secondary system is active**

  In an HA deployment, the **About STRM/JSA page** might display **This is the primary system of an HA cluster**, when the secondary system is actually the active system.

- **HA clusters configured with Network File System (NFS) might not failover properly**

  If you configure an NFS off-board storage solution on an pre-configured HA cluster, HA failover fails to occur. This occurs because the appropriate mount commands do not get configured for the cluster virtual IP address.

  Workaround: Perform the following steps:

  1. Using SSH, log in to the cluster virtual IP address as the root user.
  2. Add the appropriate NFS mount command to the /opt/qradar/ha/fstab.back file.
  3. Type the following command:
     /opt/qradar/ha/bin/ha_setup.sh --restore

  For more information on configuring NFS, see the *STRM/JSA Offboard Storage Guide*.

- **Off-site event and flow forwarding might fail after you add a secondary HA console host to a primary console host**

  When you add a secondary HA console host to a primary console host, the SSH public key file might be overwritten. The HA cluster can communicate with each other, but if

both HA hosts in the pair are configured for off-site event and flow forwarding, off-site event and flow forwarding might fail.

- **Original Host IP addresses remain associated to HA cluster after you change the IP addresses**

  To change the IP addresses of hosts that are included in an HA cluster, you must first remove HA from the cluster. After you remove HA, change the IP addresses of the two hosts, and then re-add the HA cluster, the original host IP addresses remain associated to the cluster.

- **Unable to restore a backup archive a different HA host than the original HA host**

  When you restore a configuration backup archive on an HA host that was created on another HA host, the backup archive might fail to restore because of an issue with the routing routes.

- **Unable to re-add HA to a secondary host after you change network information**

  If you want to change the network settings of a secondary host in an HA cluster, you must first disconnect the HA cluster, stop IPTables, change the network settings using the qchange_netsetup utility, and then re-add the HA cluster. An issue might occur where the IPTables might retain the previous IP address for the secondary host, therefore, HA cannot be successfully re-added to the secondary HA host.

- **IPTable rules are not updated after you remove an encryption-enabled managed secondary HA host**

  After you remove a managed Secondary HA host that has encryption enabled from an HA cluster, IPTable rules are not updated.

- **Unable to restore HA from the secondary HA host with /store mounted on an iSCSI offboard storage solution**

  If you have your /store partition mounted on an iSCSI offboard storage solution on your HA cluster, you are unable to restore HA from the secondary HA host.

- **The Auto Restart Service check box is selectable even if the Auto Deploy check box is not**

  On the Change Settings page of the Updates window, you can select the **Auto Deploy** check box or the **Auto Restart Service** check box. The system allows you to select the **Auto Restart Service** check box without also selecting the **Auto Deploy** check box first. If you do not select the **Auto Deploy** check box, the automatic restart only restarts your user interface, but does not deploy your changes.

  Workaround: If you want to select the**Auto Restart Service** check box, you must also select the **Auto Deploy** check box.

- **Security profiles might become uneditable if you click the Delete icon twice**

  On the Security Profile Management window, if you select an administrative security profile and click the**Delete** icon twice while the deletion is in progress, an issue occurs where the security profile becomes uneditable.

  Workaround: Do not click the **Delete** icon a second time while the deletion is in progress.

- **Time synchronization might fail after a system restart**

Time synchronization on encrypted managed HA hosts might fail after a system restart. When this occurs, the following system notification is displayed: **failed to get listen pid of tunnel process tunnelrdate.**

Web Browser Issues

- **An error occurs when you resize your browser window when you view bar, pie, or table charts in the Log Activity and Network Activity tabs**

  If bar, pie, or table charts are displayed in the Log Activity or Network Activity tabs, resizing the Microsoft Internet® Explorer 8 web browser window causes the following error to occur: **Object doesn't support this property or method.**

- **Dashboard items cease to refresh after you click the title bar**

  On the **Dashboard** tab, after you click anywhere in the title bar of a time series dashboard item, the dashboard item pauses and is no longer refreshed. This error only occurs when you use the Microsoft Internet Explorer 8 or Mozilla Firefox 9.0.1 web browsers.

  Workaround: If you are using the Microsoft Internet Explorer 8 web browser, press **F5** to refresh your browser window or resize your browser window.

- **Error message displayed if your Results Per Page system setting is configured to a value greater than 40**

  Due to limitations in the Microsoft Internet Explorer 7 web browser Javascript engine, if your **Results Per Page** system setting is configured to a value greater than 40, error messages might be displayed on the **Log Activity** and **Network Activity** tabs indicating a problem handling the server response.

  Workaround: Configure the **Results Per Page** parameter to specify a value no greater than 40. To access the **Results Per Page** parameter, click **Admin > System Configuration > Console**.

- **System error occurs when a time series chart is displayed**

  On the **Log Activity** and **Network Activity** tabs, a system error might occur when a time series chart displays. This error only occurs when you use the Microsoft Internet Explorer 8.0 or Mozilla Firefox 11 web browsers.

- **Log Source hierarchy might display incorrectly on the Log Sources window**

  On the **Log Sources** window, the hierarchy might be displayed incorrectly as **Please select any groups you would like this log source to be a member of** pane. This issue only occurs in the Microsoft Internet Explorer 8 web browser.

- **System error might occur when you perform searches with a time range of 15 minutes**

  On the **Log Activity** and **Network Activity** tabs, a system error might occur when you perform a search that has a time range of 15 minutes. This issue only occurs in the Microsoft Internet Explorer 8 web browser.

- **Scroll bar disappears when you resize the Report Wizard**

  When you resize the Report Wizard, the scroll bar disappears. This error only occurs in the Microsoft Internet Explorer 8 web browser.

- **Qualys scanner proxy settings do not display correctly**

  On the Add Scanner window or Edit Scanner window, if you select the **Qualys Scanner** option from the Type list box and then select the **User Proxy** check box, the proxy parameters do not display. This issue only occurs in the Microsoft Internet Explorer 9 web browser.

- **List boxes in Column Definition pane do not display**

  On the edit search page of the **Log Activity** and **Network Activity** tabs, list boxes are displayed next to some columns in the Column Definition pane. These list boxes allow you to specify which aspect of the parameter you want to include in the grouped search results. For example, for the **Magnitude** parameter, you can select to display the minimum, average, or maximum magnitude for each group. An issue occurs when you view the user interface with the Mozilla Firefox 16.0.2 web browser where these list boxes are not displayed.

- **OK and Cancel buttons do not display on the Schedule the updates window**

  On the Check for Updates page of the Updates window, if you select an update and then select **Schedule > Selected Updates**, the Schedule the updates dialog box opens. The Schedule the updates dialog box does not display the **OK** and **Cancel** buttons in Microsoft Internet Explorer 8 web browser.

Dashboard Tab

- **Dashboard tab might display time series charts to non-administrative users who do not have permission**

  Non-administrative users that do not have permission to manage time series charts have access to flow-search based time series charts on the **Dashboard** tab.

- **Vertical scroll bar not displayed on Event Searches menu**

  On the **Dashboard** tab, the vertical scroll bar is not displayed on the **Event Searches** menu. If more searches are listed than are displayed, you are unable to scroll to them.

- **User accounts that have been updated to administrative roles might not have access to all dashboard saved searches**

  If a user with a non-administrative role is subsequently granted administrative privileges, that user can only access the Top Rules event search dashboard item in the **Log Activity > Event Searches** menu. The user should have access to all the event searches configured to be available on the **Dashboard** tab.

- **Event or flow charts might not display correctly when viewed from the Dashboard tab**

  On the **Dashboard** tab, if you click the **View in Log Activity** or **View in Network Activity** link on a time series chart that is configured to graph a parameter that is not based on accumulated data, the window might not display charts correctly and might filter on the wrong time range. The expected graphs are a time series chart with an error message and a bar chart that displays a message that requests you to click **Update Details** to view the chart. Instead, the bar chart displays with incorrect data due to the time range being incorrect.

- **Dashboard time series charts might not display when your disk usage is over 90%**

  When disk usage is over 90% on your system, time series chart might not display on the **Dashboard** tab. The following error message is displayed: **There was an issue with generating time series**.

- **Dashboards might fail to display**

  On the **Dashboard** tab, an error might occur where the dashboards fail to display and there are no options in the **Show Dashboard** list box.

- **System summary dashboard item might fail to display**

  If your STRM/JSA deployment is configured with a large number of managed hosts, the **System Summary** dashboard item take a extended period of time to load or might fail to display.

Offenses Tab

- **"Exploit: Chained Exploit Followed by Suspicious Events" rule might not generate expected responses**

  Source and destination IP addresses can be chained, meaning that a destination IP address of one offense can become the source IP address for other offenses. STRM/JSA 2010 introduced a new method of indexing offenses based on offense type. The **Exploit: Chained Exploit Followed by Suspicious Events** rule relies on the offense type, therefore, it stops adding events to an offense after the destination IP address becomes a source IP address; instead, a new offense is created. The rule is not effectively reporting events in the chained offenses.

- **Offense count discrepancies**

  On the **Offenses** tab, discrepancies might occur for the **Offense Count** parameter between the Offense Search page and the various panes on the Offense Summary page. For example, if you double click an offense, the Offense Source Summary pane displays the number of offenses for the Source IP offense type. If you click the **Offense** link on the Offense Source Summary pane, the number of offenses displayed on the Offense Search page does not match the offense count on the Offense Source Summary pane.

- **Selected offense exports result in all offenses exported to CSV or XML**

  If you export a selection of offenses to CSV or XML, the exported file might contain all offenses in your system, not only the offenses you chose to export.

- **Application error occurs when you click the Source link in an annotation for a chained offense**

  In Annotation panel on the **Offenses** tab, if you click the **source** link in an annotation for a chained offense, an application error occurs.

- **Columns on the By Network page of the offenses tab are not sortable**

  On **By Network** page of the **Offenses** tab, the following columns are not sortable: Magnitude, Source IPs, Destination IPs, Offenses Targeted, Offenses Launched. On all other pages of the **Offenses** tab, these columns are sortable.

- **Offense icon on the Flow List window does not display offenses**

  When investigating an offense summary, if you click the **Flows** icon to view the **Flow List** window, and then click the **Offenses** icon in the flow list table, the following message is displayed: **The offense associated with this event has not yet been created, has been purged from the database, or you have reached your maximum number of offenses**. This message is incorrect because the flow that you are investigate is associated with the offense summary you launched the **Flow List** window from.

- **Application error occurs when you search offenses on the By Network page**

  On the By Network page of the Offenses tab, an application error occurs if you create a search that includes the following search parameters:

  - For the **Magnitude** search parameter, select **Less than** from the first list box and type a number in the text box.
  - From the **Order By** list box, select **Magnitude**.

  Magnitude column in the Top 10 Events pane does not sort correctly On the **Offenses** tab, the **Magnitude** column in the Top 10 Events pane does not sort correctly.

- **Special characters in the Regular Expression (Regex) statement for rule test cause rules to fail**

  On the Rules page of the **Offenses** tab, when you create a new rule with the following **when the username matches the following regex** test and include special characters in the regular expression, the rule fails to generate offenses.

- **Recent offense searches provide incorrect results**

  On the **Offenses** tab, no results are displayed if you create a new search using the **Recent** option with Event/flows received in the last 5 minutes.

  Workaround: Click **Refresh**.

- **Flag column icon tooltips do not display correctly when you magnify your browser window (zoom in)**

  On the **Offenses** tab, if you magnify your browser window (zoom in) when you view the All Offenses page, and then move your mouse pointer over the icons that are displayed in the **Flag** column, the tooltip text on the **Follow Up, Assigned User**, and **Note Count** icons are not displayed correctly.

- **The Rule Group list box might detach from New Offense Search page when scrolling**

  On the new offense search page, if you open the **Rule Group** list box in the **Contributing Rule** pane, and then use the scroll bar to move the page up or down, the list box detaches from the page.

- **Offenses exported from the By Source IP page do not include notes**

  On the By Source IP page of the **Offenses** tab, if you add a note to an offense and then export the offense in either CSV or XML format, the notes that you added to the offense are not displayed in the exported file.

- **Navigation issue exists on the By Network page**

On the **Network** page of the **Offenses** tab, if you open and close an offense before you perform an action, you are incorrectly returned to the list of networks instead of the Network page you were investigating.

- **Offense type does not export correctly**

  Using the **Offenses** tab, if you export a list of offenses in either CSV or XML format, the **Offense Type** in the output is incorrectly displayed as **Offense** for every type of offense.

- **Saved searches for all offenses ignore filters**

  When you create and save an offense search, some of the filters that you set are ignored when you run the saved search. For example, you create a saved search based on Event Names and a specific QID. When you load the saved search, the search results display the searches that are indexed for event name instead of the searches indexed for event name and the specific QID. This can impact reports that are based on this search.

- **Notes field on the Close Offense window is truncated in the payload of custom properties extracted from the audit log**

  You can create a custom property to extract the audit log file data from **Notes** field on the Close Offense window. The note text is truncated in the custom property payload, therefore, the notes are not displayed correctly in any reports that include that custom property.

- **Benign error message might display after you delete a saved search**

  When you click the **Edit Search** icon after you delete a saved offense search, the following error message might be displayed: **Error retrieving Offense Search**. This error message is benign.

  Workaround: Refresh your browser display.

- **Magnitude column on the By Source page does not sort correctly**

  On the By Source page of the **Offense** tab, the **Magnitude** column does not sort correctly.

- **Offenses might include events that do not match the associated rule**

  An offense might include an event that does not match the rule that generated the offense if the following check boxes are selected on the Rules Response page of the Rules Wizard:

  - Ensure the dispatched event is part of an offense
  - Include detected events by Source IP from this point forward, for <n> seconds, in the offense

- **Application error occurs when you close listed offenses**

  On the **Offenses** tab, an application error might occur if you close a large number of offenses using the **Close List** icon.

- **The Assign to User list box on the Offense Search page does not retain your selection if the username includes an underscore.**

On the Offense Search page, if you select a username that includes an underscore from the **Assign to User** list box and save the search criteria, the selection for the Assign to User list box changes back to the default option.

- **Offense creation ceases after you remove a network that has an associated offense note**

  Offense creation might cease to generate after a network is removed from your network hierarchy if that network has an associated offense note.

Rules Page

- **The "these log sources" rule test does not function if the "generic log source" option is selected**

  In the Rule Wizard, the **these log sources test** provides a **generic log source** option. If you select generic log source, the rule does not function properly. The rule does not generate offenses because the Custom Rule Engine (CRE) does not process generic log sources.

- **"Anomaly: Potential Honeypot Access" rule description references functionality that no longer exists in STRM/JSA 2013.2**

  The description for the **Anomaly: Potential Honeypot Access** rule is not accurate, however, the rule functions properly. The description references **Network Surveillance** tab functionality, which no longer exists in STRM/JSA 2013.2.

- **The BB: DeviceDefinition: IDS/IPS building block does not include the Sourcefire Defense Center Device**

  On the Rules page, the BB: DeviceDefinition: IDS/IPS building block does not include the Sourcefire Defense Center device. This omission might lead rules that include this building block to fail to generate offenses based on Sourcefire Defense Center events.

- **STRM/JSA 2013.2 custom rules do not test events from STRM/JSA 2009.2**

  After upgrading your system to STRM/JSA 2013.2 from STRM/JSA 2009.2, custom rules created in STRM/JSA 2013.2 do not test events that were stored before you upgraded your system.

- **A system rule generates offenses based on the flow source test that specifies the overflow buffer as a flow source**

  On the **Rules** page, the **Flow Source** test in the **System: Flow Source Stopped Sending Flows** rule is detecting the overflow buffer as a flow source. When the overflow buffer sends flows and then ceases to send flows, the **System: Flow Source Stopped Sending Flows** rule generates offenses. The overflow buffer should not be considered to be a flow source.

  Workaround: Edit the **System: Flow Source Stopped Sending Flows** rule to exclude qflow:overflow as a flow source.

- **New offenses not generated after you update rule settings**

  Rules do not generate offenses correctly if you update the **Offense Type** and **Name** settings. The rule should generate a new offense, however, the rule contributes to the

offense that was generated using the previous offense type using the previous offense name.

- **"Anomaly: Single IP with Multiple MAC Addresses" rule might not function**

  The **Anomaly: Single IP with Multiple MAC Addresses** rule might not detect Media Access Control (MAC) address changes and does not generate an offense.

- **Offense naming options might not function for anomaly detection rules**

  On the Rule Response page of the Rule Wizard, you can select from three options in the **Offense Naming** list:

  - This information should contribute to the name of the associated offense(s)
  - This information should set or replace the name of the associated offense(s)
  - This information should not contribute to the naming of the associated offense(s)

  If you create an anomaly detection rule and select one of these options, your selection might not work. Offenses and notifications generated as a result of your rule might be named according to the **Event Name** parameter on the Rule Response page, regardless of your **Offense Naming** selection.

- **BB:FalsePositive: DNS Server False Positive Categories" building block is not defined correctly**

  The BB:FalsePositive: DNS Server False Positive Categories building block includes the following building block tests:

  - when a flow or an event matches any of the following BB:HostDefinition: DNS Servers
  - when a flow or an event matches any of the following BB:CategoryDefinition: Recon Events, BB:CategoryDefinition: Suspicious Events, BB:CategoryDefinition: DDoS Attack Events

  The second test only tests events, not flows.

- **Rules that reference the network hierarchy objects does not update properly when the network hierarchy is updated**

  Rules and building blocks are typically associated with objects in your network hierarchy. If you update your network hierarchy to remove an object associated with a STRM/JSA element, the associated element no longer functions.

- **The BB:DeviceDefinition:VPN building block does not include the Cisco Adaptive Security Appliance (ASA) VPN device**

  The BB:DeviceDefinition:VPN building block does not include the Cisco Adaptive Security Appliance (ASA) VPN device. As a result your STRM/JSA system does not detect Cisco ASA VPN devices.

- **Rules that contain specific rule test does not generate rules on a system with superflows enabled**

  Using the Rules page, if you create a custom rule with the following test: **when any of these rules with the same source IP more than this many times, across more than|exactly this many destination IP within this many minutes**, the test does not generate an event

if all the conditions are met. This error occurs when superflows are enabled on your system

Workaround: Reduce the number of IP addresses required by the test criteria and increase the value which verifies **the same source IP**.

- **Rule group selection is cleared when you edit the "And" operator in a rule test**

  When you edit a rule test in the Rules Wizard, the rule group selection is cleared if you click the **and** operator to change it to **and not**, and then click it again to change it back to **and**.

  Workaround: Select the rule group that the rule originally belonged to.

- **Duplicated rule might not display on the Rules page**

  Using the **Custom Rule Wizard**, if you duplicate a rule in an existing building block, by selecting **Actions > Duplicate**, and then attempt to add the rule to another building block, the rule you have duplicated is not displayed.

  Workaround: To ensure the duplicate rule is displayed, you must restart the Tomcat service.

- **Application error occurs when you edit the "when the destination side of the flow has payload data" rule test**

  In the Rules Wizard, an application error occurs and you cannot close the Rule Wizard if you attempt to edit the **when the destination side of the flow has payload data** rule test on a rule that you previously edited to change the rule type from **Flow** to **Common**.

- **Rule test might generate error**

  An issue might occur when you configure the following rule test:

  when at least this many of these rules, in|in any order, with the same source IP followed by at least this many of these rules in|in any order to|from the same destination IP from the previous sequence, within this many minutes

  When you click Save, the following error message is displayed:
  There are parameters in the test stack which have not been specified. You are not able to save the rule test.

- **Send to Forwarding Destinations rule response displayed in error for offense and flow rules**

  On the Rule Response page of the Report Wizard, the **Send to Forwarding Destinations** rule response is displayed for offense and flow rules. This response is not supported for offense or flow rules.

  Workaround: Do not select the **Send to Forwarding Destinations** rule response.

- **Building block might generate error**

  On the Rule Text Stack editor page of the Rule Wizard, the following building block (BB) might generate an error message:
  Apply BB:PortDefinition: Network Management Client Ports on events or flows which are detected by the Local system and when the source or destination port is any of 52311

- **Event and flow searches are slow when five or more searches are running concurrently on your system**

  Event and flow searches are slow when five or more searches are running concurrently on your system.

- **The Results Per Page setting does not enforce a maximum value**

  On the console Configuration window, you can configure the maximum number of results displayed on the **Offenses, Log Activity, Assets, Network Activity**, and **Reports** tabs. The system does not limit the **Results Per Page** setting to a maximum number. If you configure this setting to more than 100 results per page, your user interface might malfunction.

  Workaround: Do not type a value of more than 100 in the **Results Per Page** field.

- **Accumulator process failure**

  The accumulator process might fail when more than 20 users perform event or flow searches concurrently. When this issue occurs, the following message is displayed in the error log: **Could not launch Cron Component Process**.

- **Rule text counters might reset when the rule test reloads**

  An issue might occur where the rules automatically reload in your system and cause rule tests that use counters to reset. Rules might reload each time a rule is manually or automatically updated.

- **AlphaNumeric (Ignore Case) Reference Set elements not handled correctly in rules**

  Rules that are configured to generate a Reference Set rule response do not function correctly if the reference set type is AlphaNumeric (Ignore case). The rule does not generate responses for reference set elements with uppercase and lower case equivalents, such as jdoe and JDoe.

- **Line of system code might be displayed in building block list of IP address**

  In the Report Wizard, when you paste a large list of IP addresses (for example, more than 650) into a building block, an error might occur where a line of system code could be displayed in the list.

Common Event and Flow Functionality

- **Dates not displayed in consistent format on the Log Activity tab**

  On the **Log Activity** and **Network Activity** tabs, dates are not consistently displayed in the same format.

- **Filtering event and flow lists on a custom property does not function properly**

  On the **Log Activity** and **Network Activity** tabs, if you click **Add Filter** to create a filter based on a custom property and the filter uses the **contains** or **does not contain**option, the results are not filtered and the **Current Filter** section displays the filter option as **is**or **is not**. Also, custom property filters that use a value of N/A do not filter properly.

- **Deleting a saved search removes the search from the database, but the saved search is still displayed in the Manage Search Results window**

On the **Log Activity** and **Network Activity** tabs, if a non-administrative user deletes a saved search, the saved search is still displayed on the **Manage Search Results** window in an error state, even though the search is removed from the database.

Workaround: Double-click the saved search to view the results. You are then prompted to run the search again or remove the saved search result.

- **Reference set contents are unsearchable on the Log Activity and Network Activity tabs**

  On the **Log Activity** and **Network Activity** tabs, there are no filters to allow you to search the contents of a reference set.

- **Custom calculated property filters generate an error if the name includes quotations or parenthesis without a preceding space**

  On the **Log Activity** and **Network Activity** tabs, filtering on a custom calculated property might generate an error if the property contains the following characters in the name:

  - Quotations
    For example: cc"SC"
  - Parenthesis without a preceding space
    For example, cc(cc1*cc2

  The following error is displayed: **Filter <property_name> is not a known property or predicate**. This error occurs when you add the filter using the right-click menu options or the **Add Filter** window.

- **OK and Cancel buttons repeated on error message on the Manage Search Results page**

  On the **Manage Search Results** page, when you click the **ERROR** link in the **Status** column, an error message is displayed to indicate that the search contains an error and asks to you click **OK** to re-execute the search or **Cancel** to remove the invalid entry. The **OK** and **Cancel** buttons on the error message window might be repeated two or three times.

- **Last Minute (Auto Refresh) view option might not function on grouped searches**

  When the **Log Activity** or **Network Activity** tab is configured to display grouped search results and the **Last Interval (Auto Refresh)** option is selected from the **View** list box, the data and charts are only refreshed once, not every 60 seconds as expected.

- **Searches that include a custom property might display minimum and maximum values on time series charts incorrectly**

  When you perform a search that includes a new custom property and display time series graphs for both the maximum and minimum values returned by the search, the graphs do not correctly display the maximum and minimum values for the time period you have searched.

- **Quick filter tooltip might remain on user interface after closing the Quick Filter window**

  When you click the **Quick Filter** text field on **Add Filter** window in the **Log Activity** or **Network Activity** tabs, a tooltip is displayed, providing information on the appropriate syntax to use for search criteria. If you click the tooltip to expand it, and then click the **Close** icon to minimize it, the tooltip might remain displayed on the tab after you close the **Quick Filter** window.

Workaround: Click any other tab in the user interface to remove the tooltip.

- **No legend to indicate the time segment for each data point in a time series chart**

  On a time series chart, if you zoom in or out of your chart, it might appear that the data point values change incorrectly. The value changes because the time segment represented by each data point changes as you zoom in or out. For example, the time segment might change from 30 second intervals to 1 minute intervals when you zoom in, therefore, the number of matched records must change. This chart function is working as designed, however, there is no legend to indicate that the time segment has changed.

- **Regex-based numeric custom property columns do not sort properly**

  On the **Log Activity** and **Network Activity** tabs, regex-based numeric custom property columns do not sort properly.

- **Deleted custom properties are still displayed in saved searches**

  If you delete a custom event or flow property that is included in saved search criteria, when you load the saved search criteria, the deleted custom property is still displayed.

- **Destination address and source address parameters do not display geographic flags**

  On the **Log Activity** and **Network Activity** tabs, the **Destination Address** and **Source Address** parameters do not display geographic flags.

- **Pie charts configured to graph deleted custom calculated properties might not display correctly**

  Pie charts on the **Log Activity, Network Activity**, and **Dashboard** tabs do not display properly if the chart is grouped on the Source or Destination IP parameter and configured to graph a custom calculated column that has been deleted.

- **Cancelling a queued search might result in error**

  On the **Manage Search Results** page of the **Log Activity** and **Network Activity** tabs, if you cancel a search that has a status of **Queued** in the **Status** column, the status changes to **Error**. If you double-click the **Error** status, a message is displayed to request you to click **OK** to run the search again or **Cancel** to remove the search. If you click **OK**, the search is not run again; it is removed.

- **Sorting on a search in progress generates fatal exception error**

  On the **Log Activity** and **Network Activity** tabs, if you click a column header to sort a search while it is in progress, a fatal exception error occurs.

- **Time series chart might fail to display in concurrent searches grouping on the same custom property**

  When you view search results for multiple concurrent searches on the **Log Activity** and **Network Activity** tabs, time series charts might fail to display if the search is configured to group the results on the same custom event property.

- **Benign error message displayed in error log when you change display options on Log Activity and Network Activity tabs**

When viewing data in real time (streaming) mode on the **Log Activity** and **Network Activity** tabs, if you select a time frame from the View list box. the following error might be displayed in the error log:**Failed to find stream consumer to get contents for id: 22a55564-99ed-4f13-8297-3c0f1d45cee4-STREAMING**. This error message is benign.

- **Benign message displayed when you view associated rules from an Offense page launched from the Log Activity or Network Activity tab**

  On the **Log Activity** and **Network Activity** tabs, a benign error message is displayed when you try to view the associated rules for an offense you accessed from event or flow search results that include the **Associated with Offense** column and the time range is **Last 5 Minutes** time range. The following message is displayed: **Connection to the console has been lost**.

- **Grouped search results are not sorted in the same order when exported to a CSV or XML file**

  On the **Log Activity** and **Network Activity** tabs, if you export grouped search results that are sorted on the **Event Name** parameter to an CSV or XML file, the search results are not sorted in the export file in the same order as they are sorted on the user interface.

- **Save Criteria window might not retain check marks that indicate which group in which the Saved Search Criteria Belongs**

  When saving search criteria on the **Log Activity** and **Network Activity** tabs, you can assign the saved search criteria to a group. On the Save Criteria window, if you select a check box for a group in the Assign Search to Group(s) pane, a check mark is displayed. If you close the Save Criteria window and then click **Save Criteria** again, the Save Criteria window does not retain the check mark. This issue only affects the appearance of the check mark; the saved search criteria is still assigned to the group and therefore can be searched within the group.

- **Cancelling a queued search might result in the search displaying an error status**

  On the **Log Activity** and **Network Activity** tabs, if you run multiple searches, the status of several searches on the Manage Search Results page might be listed as **Queued**. If you cancel one of these queued searches, the status of the search is incorrectly set to **Error**.

- **Next refresh timer fails to display after first interval**

  On the **Log Activity** and **Network Activity** tabs, if you select **Last Interval** from the **View** list box and any value other than default from the **Display** list box, the **Next Refresh** timer is not displayed after the search completes.

- **Out of Memory errors might occur when sorting on the Payload parameter**

  An Out of Memory error might occur when you perform a search that is sorted on the **Payload** parameter or when sorting search results by the **Payload** parameter.

  Workaround: Do not sort search results by the **Payload** parameter.

- **Errors might occur when you perform a search grouped or sorted on a custom property**

  Out of Memory errors might occur when you perform a search that is grouped or sorted on a custom property.

- **Add filter dialog box displays filter incorrectly for category filters**

  On the **Log Activity** and **Network Activity** tabs, if you create a Category filter, select any option from the **High Level Category** list box and select **Any** from the **Low Level Category** list box on the **Add Filter** dialog box, the displayed filter displays incorrectly. For example, if you select **Malware** as the high level category and **Any** as the low level category, the filter displays the following: **Low Level Category is Malware**.

- **"Does not equal" and "Does not equal an" filter modifiers do not function for certain parameters**

  On the edit search page and the Add Filter dialog box, the **Does not equal** and **Does not equal any** filter modifiers do not function as expected for the following parameters:

  - Source or Destination ASN
  - Source or Destination MAC Address
  - Source or Destination Network
  - Source or Destination Port

- **Search results might fail to display on the Dashboard tab**

  An issue might occur where the time range selection changes to **Last Interval** and search results fail to display on the **Dashboard** tab for a saved search that includes the following search parameters on the edit search page:

  - **Time Range > Recent > Last 6 Hours**
  - **Search Parameters > Custom Rule Matched**
  - **Column Definition > Grouped By > Source IP**

- **Error occurs when you search for events or flows using the payload matches regular expression filter**

  An error occurs when you search events or flows using the following search filter on the edit search page: **Payload Matches Regular Expression > Is > <regrex>**. If you type a regular expression that starts with a square bracket ([), the following error message is displayed:
  regex used: [<regrex statement>]
  This is not a valid regular expression:
  Unclosed character class near index 10

  Workaround: Add a space before the opening square bracket in the regular expression.

- **No search results returned for Reference Set filter if the reference set elements contain a dollar symbol**

  If you search events or flows using the Reference Set filter, and there is a dollar symbol ($) in any reference set elements, the search does not return any results.

- **Searches that include two Custom Rule filters fail to return results**

  On the new search pages of the **Log Activity** and **Network Activity** tabs, when you add more than one Custom Rule filter, the search does not return any results because the system treats the Custom Rule filter stack as an AND operation.

- **Special characters processed as wildcard characters in the Quick Filter text field**

  The Quick Filter text field might process special characters as wildcard characters.

- **System error displays when you click the Save icon on the Save Criteria dialog box before the Search Group pane loads.**

  On the Save Criteria dialog box, if you click the Save icon before the Search Group pane completely loads, a system error is displayed.

Log Activity Tab

- **Event searches grouped by the Log Source Group parameter takes an extended period of time to complete**

  If your deployment includes a large number of log sources, an event search that filters on the **Log Source Group** parameter might take an extended period of time to complete.

- **Filtering on the Event Processor parameter yields incorrect results**

  On the **Log Activity** tab, if you add the **Event Processor** column to your search results, and then right-click a value in the **Event Processor** column to apply the is **not equal** filter to exclude events from that Event Processor, the results only display events from the Event Processor you wanted to exclude.

- **EventID (Custom) filter might not filter correctly**

  On the **Log Activity** tab, the **EventID (Custom)** filter does not filter correctly. The filter should search for an Event ID that directly matches your filter criteria, however, it looks for all Event IDs that contain your filter criteria. For example, when searching for an Event ID of 624, the filter results could include 4624.

- **Searches for events that match a numeric QID do not return any results**

  On the **Log Activity** tab, an event search might not return any results if the search criteria includes a filter for event names that match a numeric QID.

  Workaround: Place double quotes (“) around the numeric QID.

- **Events received at the end of a minute time interval might display an incorrect time stamp**

  If STRM/JSA receives an event at the end of a minute interval, such as 11:23:59, the event can receive a time stamp for the next minute interval, such as 11:24:59. When this occurs, the **Storage Time** parameter does not display an accurate time stamp. STRM/JSA objects that use this parameter, such as time series charts and pending offense searches, might provide misleading time information.

Network Activity Tab

- **Time series charts based on Total Bytes (AVG) calculate results incorrectly**

  On the **Network Activity** tab, any time series chart that displays Total Bytes (AVG) provides inaccurate results. The results are calculated as a sum and not an average.

- **Web-related flow data on Port 80 not mapped to application correctly**

On the **Network Activity** tab, when web-related flow data is received on port 80, the **Application** column might incorrectly indicate the source as **Other**.

- **Application based flows with destination port 80 display an incorrect event description**

  On the **Network Activity** tab, flows that were detected by application signature and have a destination port of 80 display the following event description: **Application detected with port based lookup**. This event description is incorrect.

- **The Link Utilization - Last 6 Hours quick search fails to complete**

  On the **Network Activity** tab, if you select **Link Utilization - Last 6 Hours** from the **Quick Searches** list box, the search does not complete and the charts display the following message: **No Time Series Data Available**.

- **Application filter does not allow you to filter for "Other"**

  In a recent release, the **Misc.Unknown_TCP and Misc.Unknown_UDP** applications were changed to **Other**; however, you are unable to filter for flows associated with the Other application. The **Application** filter on the **Network Activity** tab and Rules Wizard does not include **Other** as an option in the list box.

- **Source IF Index and Destination IF Index parameters might not sort properly in the search results**

  If you select **Source IF Index** or **Destination IF Index** from the **Order By** list box on the new search page of the **Network Activity** tab, the **Source IF Index** or **Destination IF Index** parameters do not sort properly in the search results.

- **Quick filter for a CIDR value on Source or Destination IPv6 parameters fails**

  An error occurs if you create a flow search that includes a Quick Filter for a CIDR value on the **IPv6 Source** or **IPv6 Destination** parameters.

- **Invalid characters might display on chart legends**

  On **Network Activity** tab chart legends, invalid characters display for custom flow properties that parse payloads that include special characters.

Assets Tab

- **Asset searches on same server type result in error**

  On the **Server Discovery** page of the **Assets** tab, if you perform a search on the same server type (for example, FTP servers), the search does not complete and the following error message is displayed in the log files: **Cyclic rule dependency chain detected**.

- **Exported asset data might not include open ports**

  Exported asset data might not include open ports for the assets, even when open ports were detected and displayed in the Ports and Vulnerabilities pane of the **Asset Profile** page on the **Assets** tab. The exported data displays a value of null for the **Ports** parameter.

- **Adding an asset with a non-unique IP address creates issues**

On the **Add Asset Profile** window of the **Assets** tab, if you type an IP address in the IP field and the IP address is already associated with an automatically discovered asset, you can save the asset profile successfully. No warning or error message is displayed. However, the asset information you added modifies the existing asset with the same IP address and does not add a new asset profile.

- **Values for asset searches do not stay set as Override Forever**

  On the **Assets** tab, when you view an asset, you can select the **Override Forever** parameter to specify that you want to manually enter operating system information and disable the scanner from updating the information. The following situation is known to occur. Even though you selected the **Override Forever** option to modify an asset, when you run a new VA scan and view the same modified asset, you might find that the operating system information was not overridden. Instead, the value reverted to the original value that was detected by the VA scanner.

- **Spaces in asset profile search cause application errors**

  On the Asset Profile Search page, if there are spaces in the specified search parameters in **Asset Extended Properties** or **Vulnerability Attributes** panes, an application error occurs.

  Workaround: Do not use spaces when you type search parameters in the **Asset Extended Properties** and **Vulnerability Attributes** panes on the Asset Profile Search page.

- **Asset Profile window might display incorrectly**

  The Asset Profile window might display the status bar in the middle of the page, instead of at the bottom. If this occurs, the Ports and Vulnerabilities pane becomes inaccessible. This issue only occurs when you access the Asset Profile window from the right-click menu option on an IP address.

  Workaround: To restore the Asset Profile window, click the **Save Changes** icon.

Vulnerability Assessment

- **The Next Start Time column on VA scan page does not sort correctly**

  On VA Scan page of the **Assets** tab, if the **Next Start Time** column contains numbers and text, the data cannot be correctly sorted when you click the column heading.

- **Vulnerability scans scheduled from managed hosts can fail or import the scan data multiple times**

  If you assign a scan to a managed host, the scan results might be imported multiple times or cause the scan result import to fail. This is due to an issue between the scan scheduler and the managed host that attempts to start the scan.

  Workaround: Delete any scanners that are assigned to a managed host and assign the scanners to the STRM/JSA console.

- **STRM/JSA might fail to start scans on vulnerability scanners**

  STRM/JSA might fail to start scans if the scan name has an ampersand (&) in the scan name.

- **Pending and In Progress scans might cancel when you delete a completed scan**

When you delete a completed scan from the Scan Scheduling window, scans that have a status of Pending and scans that are in progress might be cancelled.

Workaround: Launch a new scan.

- **Unable to disable the Max Report Age option on the Add a Scanner page**

  On the Add Scanner window, you can configure the **Max Report Age** option. To disable this option, you type a zero (0). This function is not working as designed, therefore, you are unable to disable the **Max Report Age** option.

Reports Tab

- **Reports display Start Date and Start Time parameters in different format than the corresponding search results**

  Reports that are based on an event or flow search that includes the **Start Date** and **Start Time** parameters does not display the date and time in the same format that display in the corresponding search results on the **Log Activity** and **Network Activity** tab. The report shows the date and time for both parameters, whereas the search results show only the date for the **Start Date** parameter and the time for the **Start Time** parameter.

- **Report subtitles might truncate**

  On a generated report, a lengthy report subtitle might truncate depending on the size of the chart the subtitle is associated with.

- **Reports legend might not display correctly**

  Reports might not display legends correctly if the report template is configured with the following parameters:

  - Schedule = Daily
  - Chart Type = Flows
  - Graph Type = Line
  - Graph Content = Any grouped search
  - Horizontal Axis = Time
  - Timeline Interval = 1 Hour

  The legend does not display labels for all hours on the timeline.

- **Line chart types for reports based on flows are broken**

  When you use the Report Wizard to create a line chart, the resulting line chart does not display a line on the graph.

- **Distributing Reports Via Email role permission results in no reports listed on the Reports tab**

  Your **Report** tab might contain no reports if your user account is only assigned the **Distribute Reports Via Email** role permission.

- **Error occurs when the system renders the XLS version of the report**

When this error occurs, there is a date displayed in the **Generated Reports** list, but the XLS report does not generate. This results in the **Formats** column being empty.

- **Top Offense report does not return results when configured to report on only inactive offenses**

  An error occurs when you create a **Top Offenses** report that is configured to include only inactive offenses. If you select only the **Inactive Offenses** check box in the Includes pane, the generated report does not display any results. This error also occurs on the **Offenses** tab when you perform a search for only inactive offenses.

- **Application error might occur when you create or edit a schedule report associated with a saved flow search**

  When you create or edit a scheduled report that is associated with a saved flow search, an application error might occur when you click **Finish** on the last page of the Report Wizard. This error occurs when the saved flow search includes the **Remote Networks** parameter in the column definition.

  Workaround: Edit the saved flow search to remove the **Remote Networks** parameter from the column definition, and then restart your Tomcat service.

- **Out of Memory occurs on reports that use a saved search with more than 50,000 results**

  An Out of Memory error occurs if you create a report that uses a saved event search that returns more than 50,000 events even if the report is configured to display no more than 50,000 events.

WinCollect

- **Error occurs when WinCollect Agent accesses the registry from multiple threads**

  In the WinCollect agent error log, the following errors might be generated: **Invalid Handle** or **Overlapped I/O Operation** is in Progress. These errors occur when two individual processes in the WinCollect agent compete for the same registry key. The errors in the WinCollect agent error log are forwarded to STRM/JSA as log source events. The events for Invalid Handle or Overlapping I/O process can be ignored.

- **WinCollect log sources display N/A in the Log Source Status column**

  In the Log Sources window, the **Status** column for events forwarded by WinCollect agents display not available (N/A). The **Status** column always displays N/A, even when events are properly received by STRM/JSA.

- **Benign application error occurs when you save a new WinCollect log source**

  When you add a new WinCollect log source from a WinCollect group, a benign application error might occur when you save the new log source.

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).

Revision History

September 2015—Revision 1, for JSA Release 2013.2