IBM Security QRadar Log Manager
Version 7.2.0

Release Notes

Note: Before using this information and the product that it supports, read the information in “Notices and Trademarks” on page 31.

CONTENTS

1 IBM Security QRadar Log Manager Release Notes

IBM is pleased to introduce IBM Security QRadar Log Manager 7.2. This release provides you with new and updated functionality, and resolved issues.

Before you install the latest software version, you can view the Fix Central website to determine if any fix packs are available. Fix packs are cumulative updates that contain the necessary software to upgrade all QRadar products, including QRadar Risk Manager and QRadar Vulnerability Manager to the latest version.

Note: Third-party RPMs are not supported on QRadar Log Manager systems. Before you upgrade to QRadar Log Manager 7.2, pretest your systems to determine if your deployment includes any third-party RPMs. For more information, see the *IBM Security QRadar 7.2 Upgrade Guide*.

New and updated functionality

QRadar Log Manager 7.2 introduces the following new and updated features:

- **License management** - The System and License Management window now provides centralized license management. You can upload, allocate, and manage the licenses for your Console and all managed hosts in your deployment. This window also provides information about each license, such as the limits that the license enforces and the expiration date. For more information about license management, see the *IBM Security QRadar Log Manager Administration Guide*.
- **Multicultural support** - QRadar Log Manager 7.2 is an English-only release that includes multicultural support for the global marketplace. This release includes support for the following multicultural features:
  - Unicode support for the event pipeline. Unicode support includes:

    Event data that is converted from its local codepage to UTF-8.

    Payload and normalized data that is stored as UTF-8 in the database.

    The functions that are used to retrieve, display, and correlate Unicode data.
  - Multilingual reporting capabilities for report names, titles, and content.
  - Locale-specific calendars that are based on the locale setting of your web browser.
  - Locale-specific date and time format that is based on the locale setting of your web browser.

- Country and region flags that display according to your system setting.
- Unicode support for email content.
- Locale-sensitive searching and sorting is partially supported.

This release includes limitations for the following multicultural features:

- Support for bidirectional languages.
- Internationalized email addresses and domain names.
- Non-Gregorian calendars.
- Locale-sensitive number formatting.

- **Improved bar and pie charts on the Dashboard tab** - Previously, on the **Dashboard** tab, only the Time Series chart type used accumulated data. QRadar Log Manager 7.2 supports the use of accumulated data in bar and pie charts. The **Capture Time Series Data** and **Time Range** options are now provided on these chart types. For more information about dashboard chart configuration, see the *IBM Security QRadar Log Manager User Guide*.
- **Data obfuscation** - Data obfuscation encrypts specified event data parameters to prevent unauthorized access to sensitive information. For example, you can use data obfuscation to encrypt the **Username** field. After you configure data obfuscation using the command-line interface (CLI), the encrypted version of the data is displayed in the columns and parameters on the user interface. You can decrypt the obfuscated data using a command-line interface (CLI) utility.

  After you enable data obfuscation, the following fields might not display obfuscated data:

  - User names when the data is derived from log source extensions or after DSM parsing.
  - User names when extracted through the multiple regex format required for some log sources.

  For more information about data obfuscation, see the *IBM Security QRadar Log Manager Administration Guide*.
- **Identity and Access Management (IAM) integration** - You can configure QRadar Log Manager 7.2 to collect user and group information from the Identity and Access Management user registry. QRadar Log Manager can use the identity information and the log events from the IAM servers to monitor the activities of IAM privileged users. For more information about user information source management, see the *IBM Security QRadar Log Manager Administration Guide*.
- **Browser support** - QRadar Log Manager 7.2 introduces support for the Google Chrome web browser, updates the supports versions for Mozilla Firefox, and removes the Compatibility Mode requirement for the Microsoft Windows Internet Explorer web browser. For more information about the supported web browsers, see the *IBM Security QRadar Log Manager Administration Guide*.

- **Java 7 support** - The deployment editor window now supports Java™ 1.6 and 1.7.
- **New QRadar 2100 Light appliance** - This appliance is an all-in-one appliance that provides the abilities of the QRadar 2100 appliance, but supports 500 Events Per Second (EPS) instead of 1,000 EPS. You can upgrade this appliance to increase capacity and is available as a virtual appliance and software solution.

Patch installation instructions

This procedure applies if you want to install QRadar Log Manager 7.2 as a patch to your current system. If you want to install QRadar Log Manager 7.2 as a fresh installation, see the *IBM Security QRadar Log Manager Installation Guide*. If you are upgrading to QRadar Log Manager 7.2, see *IBM Security QRadar Upgrade Guide*.

Note: If you use Secure Shell (SSH) to patch your QRadar Log Manager system and your SSH session is disconnected while the patch installation is in progress, the patch continues to install on your system. When you reopen your SSH session and rerun the patch installer, the installation does not restart.

To install QRadar Log Manager 7.2:

Step 1 Download the 7s0_QRadar_patchupdate-7.s.0.<build_number>.sfs patch from the following website:

http://www.ibm.com/support

Step 2 Using SSH, log in to your system as the root user.

User name: **root**

Password: **<password>**

Step 3 Copy the patch file to the /tmp directory.

Note: If space in /tmp is limited, copy the patch file to another location with sufficient space.

Step 4 Create the /media/updates directory:

```
mkdir -p /media/updates
```

Step 5 Change to the directory where you copied the patch file:

```
cd <directory>
```

For example, `cd /tmp`

Step 6 Mount the patch file to the /media/updates directory:

```
mount -o loop -t squashfs
720_QRadar_patchupdate-7.2.0.<build_number>.sfs /media/updates/
```

Step 7 Run the patch installer:

```
/media/updates/installer
```

Note: The first time that you use the patch installer script, expect a delay before the first patch installer menu is displayed.

Step 8 Using the patch installer, install the patch on all systems in your deployment except secondary HA hosts. Install the patch on systems in your deployment in the following order:

1. Console
2. Event Processors
3. Event Collectors

Resolved issues

The following issues are resolved in QRadar Log Manager 7.2:

Bug 24251: Filtering on the Event Processor parameter no longer yields incorrect results

Previously, on the **Log Activity** tab, if you added the **Event Processor** column to your search results, and then right-clicked a value in the **Event Processor** column to apply the **is not equal** filter to exclude events from that Event Processor, the results only displayed events from the Event Processor you wanted to exclude.

Bug 26970: Saved Search Results No Longer Reference Deleted Saved Search Criteria

Previously, after you deleted saved search criteria, saved search results that were based on the deleted saved search criteria might still have displayed the name of saved search criteria that generated the results. The name of the saved search criteria was displayed in the **Using Search** field. This information was misleading, because the saved search criteria did not exist anymore.

Bug 29620: The BB: DeviceDefinition: IDS/IPS building block now includes the Sourcefire Defense Center Device

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

Bug 30129: Authentication icon on Admin tab no longer displays for users who do not have the Administrator Manager and Remote Networks and Services Configuration role permission

Previously, on the **Admin** tab, the **Authentication** icon was displayed in error for users who did not have the Administrator Manager or Remote Network and Services role permission. When the user clicked the icon, an empty window was displayed.

Bug 30206: Source Or Destination IP filter now works correctly when you use the Does not equal any of operator

Previously, on the Log Activity tab, if you added the **Source Or Destination IP filter**, selected **Does not equal any of** operator, and typed an IP address, the filtered results were incorrect.

Bug 33099: Error no longer occurs if 50 days have elapsed since Event Collection Service (ECS) was restarted

Previously, if 50 days had elapsed since the ECS service on your system had been restarted, rules that were configured to send Simple Network Management Protocol (SNMP) traps might have generated errors.

Bug 36181: Next refresh timer no longer fails to display after first interval

Previously, on the **Log Activity** tab, if you selected **Last Interval** from the **View** list box and any value other than default from the **Display** list box, the **Next Refresh** timer was not displayed after the search completed.

Bug 36263: The BB:DeviceDefinition:VPN building block now includes the Cisco Adaptive Security Appliance (ASA) VPN device

Previously, the BB:DeviceDefinition:VPN building block did not include the Cisco Adaptive Security Appliance (ASA) VPN device. As a result, your QRadar Log Manager system did not detect Cisco ASA VPN devices.

Bug 37515: Error no longer occurs when the system renders the XLS version of the report

When this error occurred, there was a date that is displayed in the **Generated Reports** list, but the XLS report did not generate. The results in the **Formats** column were empty.

Bug 37712: System notification no longer incorrectly specifies data is being dropped

Previously, when the accumulator could not process time intervals for event data quickly enough, the following system notification was displayed on the **Dashboard** tab: `Events were dropped by the accumulator`. This system notification incorrectly described the problem. No data was dropped.

Bug 38173: System notification now exists to indicate replication failure caused by a locked RPM database

Previously, when replication failed between a Console and the managed hosts because of a locked RPM database, no system notification was displayed on the **Dashboard** tab.

Bug 38409: Accumulator no longer generates errors after you delete a custom event property

Previously, after you deleted a custom event property, the accumulator generated errors that are associated with the deleted property. The following error message was displayed: `Custom property with ID <id) doesn't exist but it is referenced in a currently active search`.

Bug 38845: Pending and In Progress scans no longer cancel when you delete a completed scan

Previously, when you deleted a completed scan from the Scan Scheduling window, scans that had a status of **Pending** and **In Progress** might have been cancelled.

Bug 38963: No longer 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. Prevously, an issue might occur where the IPTables might have retained the previous IP address for the secondary host, therefore, HA could not be successfully re-added to the secondary HA host.

Bug 38984 and 38989: “Does not equal” and “Does not equal an” filter modifiers now function correctly

Previously, on the edit search page and the **Add Filter** dialog box, the **Does not equal** and **Does not equal any** filter modifiers did 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

Bug 39664: Now able to restore HA from the secondary HA host with /store mounted on an iSCSI offboard storage solution

Previously, if you mounted your /store partition on an iSCSI offboard storage solution on your HA cluster, you were unable to restore HA from the secondary HA host.

Bug 40168: OK and Cancel buttons now 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. Previously, the **Schedule the updates** dialog box did not display the **OK** and **Cancel** buttons in Microsoft Internet Explorer 8 web browser.

Bug 40621: Increased performance of event searches when five or more searches are running concurrently on your system

Previously, event searches were slow when five or more searches ran concurrently on your system.

Bug 40676 and 41757: Shared Reports Now Display Correct Accumulated Data

Previously, if another user shared an enabled report with you, your report may have not have displayed current accumulated data until you toggled the report off and then on again.

Bug 40757: Backup archives no longer fail on managed hosts with an underscore character in the host name.

Previously, on a managed host, the backup archival process ceased if the system's host name contained the underscore (_) character.

Bug 41496: Searches that include two Custom Rule filter no longer fail to return results

Previously, on the new search pages of the **Log Activity tab**, when you added more than one Custom Rule filter, the search did not return any results because the system treated the Custom Rule filter stack as an AND operation.

Bug 41512: Alphanumeric (Ignore Case) Reference Set elements are now handled correctly in rules

Previously, rules that were configured to generate a Reference Set rule response did not function correctly if the reference set type was alphanumeric (Ignore case). The rule did not generate responses for reference set elements with uppercase and lowercase equivalents, such as jdoe and JDoe.

Bug 41520: Custom Logos Now Scale Appropriately on Reports

Previously, if you added a custom logo to your reports, your logo may have been truncated because the system failed to scale the logo size.

Bug 41820: Now able to add a forwarding destination with a destination port of more than 32001

Previously, on the Forwarding Destination window, after you successfully added a forwarding destination with a destination port 32001 and higher, the following error message was displayed when the user interface restarted: `Failed to create forwarding destination`. The forwarding destination was no longer displayed in the user interface.

Bug 42110: Reports no longer fail to generate on systems that use Asia/Kokata time zone

Previously, if your system time zone was Asia/Kokata, an error could occur when you generate a report. The following message was logged in the error log: **`Failed to run using template`**.

Bug 42198: The Rule Wizard now opens to the correct page when you edit a rule from the Anomaly group

Previously, if you edited a rule from the Anomaly group, the Rule Wizard opened to the Rule Summary page instead of the Rule Test Stack Editor page.

Bug 42239 and 42673: Index Management window footer no longer displays in the center of the page

Previously, the footer of the Index Management window may have displayed in the center of the window.

Bug 42301: SSH access issues no longer occur for non-root users in the AQL CLI

Previously, if you tried to log into the AQL CLI as a non-root user using SSH, the ownership of /store/jheap was automatically changed and you were unable to log in successfully.

Bug 42356: Tomcat now restarts properly after automatic updates

Previously, a scheduled Tomcat service restart after an automatic update failed to restart properly.

Bug 42486: Security profiles that include the network permission of ALL now function correctly

Previously, if you selected the **All** option in the Networks pane when you created a security profile, users with that security profile may not have been granted access to data from all networks.

But 42498: Reports no longer fail when based on saved search criteria that is sorted on the column the search is grouped on

Previously, if you created a report that used saved search criteria that is sorted on the column that the search is grouped on, the report failed to generate and the following warning message was displayed: `Error occurred creating Accumulated Result Set. Trying to fall back to raw query if possible.`

Bug 43344: Error no longer occurs when you share generated report content with other users

Previously, if you created a report and shared the generated report content with other users, an error occurred.

Known issues and limitations

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

Globalization

Bug 36093, 36094, 36092, 36206: Non-English characters not accepted

Non-English characters are not accepted in some fields in the user interface. The following fields do not accept non-English characters:

- The **Web Server** field on the **Advanced** tab of the Auto Updates window
- The **Name** field on the Add Network Object page of the Network Views window

Additionally, when you create a bulk import file with non-English characters, an error message displays when you upload the bulk import file.

Bug 44068: The Payload field on the Custom Property Definition window does not retain globalization

After you create a custom property that uses non-English characters in the text fields and the payload field, when you open the Custom Property Definition window to edit the customer property, the payload is not globalized anymore.

General

Bug 28094: 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.

Bug 30537: 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**, **Rules**, and **Reports** tabs.

Workaround: Avoid using special characters in group names.

Bug 34041: 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.

Bug 34970: 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.

Bug 41219: 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

Bug 14978: QRadar Log Manager objects associated to deleted users

After deleting a user, QRadar Log Manager 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 Customer Support.

Bug 21210: 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.

Bug 33755: 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.

Bug 35404: 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.

Bug 34611: 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.

Bug 34872: 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 user names that have a value of N/A.

Bug 35079: 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.

Bug 35017: 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.

Bug 35125 and 35500: Installation sequence issues if you attempt to assign an IP address already in use

When you install QRadar Log Manager, 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.

Bug 37481: 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.

Bug 37527: 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.

Bug 37570: No installation progress is displayed for DSMs

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

Bug 38661: 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 QRadar Log Manager 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:

Step 1 Log in to your system as the root user.

Step 2 Type the following command:

```
openssl rsa -in private.key -out newprivate.key
```

Step 3 Install the new private key on your system. For more information, see the *Replacing the SSL Certificate* technical note.

Step 4 Proceed with your upgrade.

Step 5 After the upgrade is complete, replace the new private key with your self-signed certificate, if required.

Bug 38674: 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.

Bug 38689: 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 Customer Support for assistance. Customer Support can increase your ring buffer size.

Bug 38714: 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.

Bug 38841: Email server outage occurs if valid email addresses are not specified in the user interface

During QRadar Log Manager 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 to be delivered to the mail server, because the default email 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
- **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

Bug 38837: 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.

Bug 38883: 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.

Bug 39268: System failed to start after an uncontrolled shutdown

An issue occurred where the QRadar Log Manager system did not start properly after an uncontrolled shutdown while a deployment change was in process.

Bug 39485: 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.

Bug 39856: The Current License Details window does not display Internet Threat Information Center subscription

The Current License Details window does not display subscription information for the **Internet Threat Information Center** dashboard item.

Bug 39889: 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:

```
<deviceDate>2012-11-02 15:13:15</deviceDate>
<deviceTime>2012-11-02 15:13:15</deviceTime>
```

Bug 40004: Error message indicates incorrect build number after upgrade failure

If your upgrade to QRadar Log Manager 7.1 fails, the error message indicates the QRadar Log Manager build your system is currently using. This build number might be incorrect on a patched system. This issue does not affect your system performance.

Bug 40116 and 43464: 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.

Bug 40471: Server Discovery fails to automatically discover DNS servers

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

Bug 40569: TCP traffic on Port 1900 might incorrectly map as Misc.UPnP

The QRadar Log Manager application mapping process might incorrectly map TCP traffic on port 1900 as **Misc.UPnP**.

Bug 40711: 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 that are listed on the page.

Bug 40761: 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.

Bug 40807: Unable to add a QFlow 1290 virtual appliance with failed Postfix service to your deployment

On the Deployment Editor window, an error occurs when you add a QFlow 1290 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.

Bug 41020: 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 QRadar Log Manager 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
```

Bug 41089: Upgrade to QRadar Log Manager 7.1 (MR 1) reverts your embedded SNMP daemon settings to the default settings

After you upgrade to QRadar Log Manager 7.1 (MR1), any customer setting you configured for the embedded SNMP daemon is reverted to the default settings.

Bug 41178: 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.

Bug 41207: QRadar Log Manager 7.1 upgrade fails on QRadar QFlow Collector systems that use IPv4

An issue might occur when you upgrade a QRadar QFlow Collector to QRadar Log Manager 7.1. The upgrade process detects that the system uses IPv6 and fail to proceed if the system actually uses IPv4.

Bug 41600: Issues Occur in the TACACS fields on the Authentication Window

On the Authentication Configuration window, the TACACS Server field might accept an invalid IP address or DNS name and not display an error message. Therefore, you will be unaware that your configured TACACS authentication does not function. Also, the Authentication Type list box does not display the correct list. ARAP is missing on the list.

Bug 41641: Event Routing Rules window displays as a blank window after you create a routing rule that contains double quotation marks

The Event Routing Rules window displays as a blank window after you create a routing rule that has a double quotation mark (“) in the search filters.

Bug 41942: Default quick searches do not display for new administrative users after the upgrade to QRadar Log Manager 7.2

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.

Bug 42066: Exception occurs when you try to view reference set contents on a system that was migrated from QRadar Log Manager to QRadar Log Manager

After you migrate your system from QRadar Log Manager to QRadar Log Manager system, an exception is displayed on the Reference Set Management window when you double-click a reference set to view the contents.

Bug 42369: Re-installation might fail on a QRadar Log Manager 7.1 MR1 Patch 1 system

An issue might occur on a QRadar Log Manager 7.1 MR1 Patch 1 system where a re-installation from recovery partition could fail.

Workaround: Before you re-install a QRadar Log Manager 7.1 MR1 Patch 1 system, contact Customer Support for assistance.

Bug 42605: Benign request to deploy changes

After you shutdown your system and then start your system up again, a message is displayed on the **Admin** tab to indicate that there are undeployed changes. It also requests you to click **Deploy Changes**. This message is incorrect. You do not need to click **Deploy Changes**. You can ignore this message.

Bug 42468: On an encrypted managed host, data is not encrypted when it flows from the Console to the managed host

If you add enable encryption on a managed host, data that flows from the managed host to the Console is encrypted. Data that flows from the Console to the managed host is not encrypted.

Bug 43392: System might become unavailable after you remove a bonded interface

After you remove a bonded interface using the qchange_netsetup utility, your system might become inaccessible.

Workaround: If this issue occurs to you, stop the network service and then type the following command: **`rmmod bonding restart network service`**. This command restores your access.

Bug 43569: CRE Description custom event property is disabled during installation process

The **CRE Description** custom event property contains a regex statement that causes installations to run slow. Consequently, the installer disables this custom event property. If you want to use this custom event property after your upgrade or installation, you must manually re-enable it.

Bug 44056: No error is logged if you create multiple expressions with the same name when you configure data obfuscation

When you add expressions to the obfuscation_expressions.xml file, you must type a unique name for each expression. If you inadvertently add multiple expressions that use the same name, the first expression with the name is processed for obfuscation, and the remainder is ignored. No error message is logged to indicate that this issue exists in your obfuscation_expressions.xml file.

Bug 43904: Swap space error message is displayed after you install QRadar SIEM 7.2 software on your own hardware

After you install QRadar Log Manager 7.2 software on your own hardware, the following error might be displayed:

```
QRadar requires 4092M of swap space but was only able to find
0m, please increase swap space by at least 4092M. Without this
additional swap space, some components of QRadar will not
function properly (such as complex queries or reports). Please
contact Customer Support for further details and assistance in
resolving this issue.
```

This error displays when swap space was not enabled or attempted to mount on the wrong device.

Workaround: If you see this error message, type **`swapon <device_path>`** to enable swap on the correct device. For example: **`/dev/sda3`**.

High Availability (HA) issues

Bug 32576: The About QRadar Log Manager page does not accurately indicate whether the primary or secondary system is active

In an HA deployment, the **About QRadar Log Manager** page might display **This is the primary system of an HA cluster,** when the secondary system is actually the active system.

Bug 25600: HA clusters configured with Network File System (NFS) might not failover properly

If you configure an NFS offboard storage solution on a 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:

Step 1 Using SSH, log in to the cluster virtual IP address as the root user.

Step 2 Add the appropriate NFS mount command to the /opt/qradar/ha/fstab.back file.

Step 3 Type the following command:

```
/opt/qradar/ha/bin/ha_setup.sh --restore
```

For more information about configuring NFS, see the *IBM Security QRadar OffBoard Storage Guide*.

Bug 37391: Off-site event 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 forwarding, off-site event forwarding might fail.

Bug 38961: 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.

Bug 39087: 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.

Bug 39503: 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.

Bug 40187: 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.

Bug 40399: 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.

Bug 40673: 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`.

Bug 41980: Upgrade script automatically runs when you change network settings on a primary HA host that is disconnected from the secondary HA host

If you use the qchange_netsetup script to change network settings on a primary HA host after you removed the secondary HA host, the upgrade script automatically runs.

Bug 42660: Benign error message might be displayed in error log when you add an HA cluster

When you add an HA cluster, the following benign error message might be displayed in your error log file:

```
Could not update ha host status for 172.16.150.59
```

Bug 42703: Re-installation from the recovery partition might fail after you remove a secondary HA host

After you remove a secondary HA host from a cluster, if you re-install the host from the recovery partition, the re-installation might fail.

Workaround: Restart the host, use the **`/opt/qradar/bin/recovery.py -u`** command in an SSH session, and then perform the re-installation procedure again.

Web browser issues

Bug 30959: An error occurs when you resize your browser window when you view bar, pie, or table charts in the Log Activity tabs

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

Bug 32464: 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 the F5 key to refresh your browser window or resize your browser window.

Bug 34763: System error occurs when a time series chart is displayed

On the **Log Activity** tab, 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.

Bug 34808: Log Source hierarchy might display incorrectly on the Log Sources window

On the **Log Sources** window, the hierarchy might be displayed incorrectly on the **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.

Bug 35892: 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.

Bug 39472: 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.

Bug 40060: List boxes in Column Definition pane do not display

On the edit search page of the **Log Activity** tab, 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.

Bug 42020: The Quick Filter field does not support the & and) symbols when you use the Google Chrome web browser

When you use the Google Chrome web browser, you cannot type the & and) symbols in the **Quick Filter** field on the **Log Activity** tab.

Bug 42133: The Maximum option in Start Time list box is not selectable when you use the Mozilla Firefox web browser

If you add the **Start Time** column to a group search, you are unable to select the **Maximum** option from the **Start Time** list box in the Columns pane. This error occurs in the Column Definition page on the edit search page of the **Log Activity** tab.

Dashboard tab

Bug 26163: The Dashboard tab issue occurs after you minimize the browser window

If you minimize your browser window while the **Dashboard** tab in open, maximize the window after you navigate to another tab, and then return to the **Dashboard** tab, the dashboard items do not display correctly.

Workaround: Reload the user interface.

Bug 30929: 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.

Bug 31139: 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.

Bug 34366: Event charts might not display correctly when viewed from the Dashboard tab

On the **Dashboard** tab, if you click the **View in Log 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.

Bug 35851: 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.`

Bug 38141: 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.

Bug 38223: System summary dashboard item might fail to display

If your QRadar Log Manager deployment is configured with a large number of managed hosts, the **System Summary** dashboard item takes a extended period of time to load or might fail to display.

Bug 43242: Inconsistent unique counts might be seen between a dashboard charts and the corresponding view in the Log Activity tab

When unique counts are enabled for a parameter on a dashboard chart, when you click **View in Log Activity**, the value for that parameter might not match.

Bug 44291: No audit log entry for when you add a new dashboard

When you add a new dashboard to your **Dashboard** tab, the action is not logged in the audit log.

Rules page

Bug 24681: 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 events because the Custom Rule Engine (CRE) does not process generic log sources.

Bug 30412: QRadar Log Manager 7.2 custom rules do not test events from QRadar Log Manager 6.3.1

After you upgrade your system to QRadar Log Manager 7.2 from QRadar Log Manager 6.3.1, custom rules that are created in QRadar Log Manager 7.2 do not test events that were stored before you upgraded your system.

Bug 35046: “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 event.

Bug 35117: 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 that is associated with a QRadar Log Manager element, the associated element no longer functions.

Bug 36744: Custom rule might fire before the event count threshold is reached

The following rule might fire before the specified number of events has been reached:

```
when any of these <rules> with the same <field> more than <this
many> times across <more than|exactly> <this many> <field>
within <this many> <time period>
```

The following example includes values for the parameters:

`when any of these` **`BB: Firewall Deny with the same source IP`** `more than` **`300`** `times across` **`more than 10 destination IP`** `within` **`5 minutes`**

In this example, the rule might fire when the event count within 5 minutes is less than 300 if the total event count that matches the other parameters over a time period greater than 5 minutes exceeds 300.

Bug 39238: 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.

Bug 40631: The Results Per Page setting does not enforce a maximum value

On the Console Configuration window, you can configure the maximum number of results that are displayed on the **Log 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.

Bug 40648: Accumulator process failure

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

Bug 40917: 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.

Bug 41715: 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.

Bug 43568: Benign error message when you create an anomaly detection rule

When you create an anomaly detection rule, a benign error message is displayed when you click **Finish**. The error message indicates that you need to enter an event name and description.

Workaround: Click **Finish** again.

Bug 18548: Dates not displayed in consistent format on the Log Activity tab

On the **Log Activity** tab, dates are not consistently displayed in the same format.

Bug 25425: Filtering event lists on a custom property does not function properly

On the **Log Activity** tab, 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.

Bug 29366: 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** tab, 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.

Bug 31174: Reference set contents are unsearchable on the Log Activity tab

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

Bug 31369: Custom calculated property filters generate an error if the name includes quotations or parenthesis without a preceding space

On the **Log Activity** tab, 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.

Bug 33349: 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.

Bug 33469: Last Minute (Auto Refresh) view option might not function on grouped searches

When the **Log 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.

Bug 33667: 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 that are returned by the search, the graphs do not correctly display the maximum and minimum values for the time period you have searched.

Bug 33693 and 34551: 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** tab, a tooltip is displayed, providing information about 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.

Bug 33833 and 38503: 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.

Bug 34248: Regex-based numeric custom property columns do not sort properly

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

Bug 34298: Deleted custom properties are still displayed in saved searches

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

Bug 34321: Destination address and source address parameters do not display geographic flags

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

Bug 34299: Pie charts configured to graph deleted custom calculated properties might not display correctly

Pie charts on the **Log 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.

Bug 34412: Canceling a queued search might result in error

On the **Manage Search Results** page of the **Log Activity** tab, 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.

Bug 34772: Sorting on a search in progress generates fatal exception error

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

Bug 35319: Time series chart might fail to display in concurrent searches that group on the same custom property

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

Bug 35533: Benign error message displayed in error log when you change display options on Log Activity tab

When viewing data in real time (streaming) mode on the **Log Activity** tab, 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.

Bug 35600: Grouped search results are not sorted in the same order when exported to a CSV or XML file

On the **Log Activity** tab, 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.

Bug 35665: Save Criteria window might not retain check marks that indicate which group in which the Saved Search Criteria Belongs

When you save search criteria on the **Log Activity** tab, 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.

Bug 36027 and 36065: Canceling a queued search might result in the search displaying an error status

On the **Log Activity** tab, 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.**

Bug 38762: Out of Memory errors might occur when you sort 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 you sort search results by the **Payload** parameter.

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

Bug 37785 or 38301: 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.

Bug 39814: Error occurs when you search for events using the payload matches regular expression filter

An error occurs when you search events using the following search filter on the edit search page: **Payload Matches Regular Expression > Is ><regex>**. If you type a regular expression that starts with a square bracket ([), the following error message is displayed:

```
regex used: [<regex 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.

Bug 40448: No search results returned for Reference Set filter if the reference set elements contain a dollar symbol

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

Bug 41511: Special characters are processed as wildcard characters in the Quick Filter text field

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

Bug 41966: 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.

Bug 42522: Deleted custom properties are not removed from the user interface

An issue might occur where the user interface may display a deleted custom property. When you delete a custom property, an error message displays if there are saved searches that use that custom property. You are directed to delete the specified saved searches. After you delete the saved searches, and then delete the custom property without error messages, the custom property might still be displayed in property lists on the user interface.

Bug 42653: Benign error message might display on the Save Criteria dialog box

On the **Log Activity** tab, an error message might be displayed if you click **OK** on the **Save Criteria** dialog box before the list of group is displayed. This error message is benign.

Bug 44380: MAC address filter does not validate character length

In event searches, the MAC Address filter does not indicate when you inadvertently typed an extra character. For example, 11-22-4f-5e-66-888 instead of 11-22-4f-5e-66-88. As a result, your MAC Address filter fails to return results.

Log Activity tab

Bug 18548: Dates not displayed in consistent format on the Log Activity tab

On the **Log Activity** tab, dates are not consistently displayed in the same format.

Bug 25425: Filtering event lists on a custom property does not function properly

On the **Log Activity** tab, 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.

Bug 29366: 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** tab, 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.

Bug 31174: Reference set contents are unsearchable on the Log Activity tab

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

Bug 31369: Custom calculated property filters generate an error if the name includes quotations or parenthesis without a preceding space

On the **Log Activity** tab, 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.

Bug 33349: 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.

Bug 33469: Last Minute (Auto Refresh) view option might not function on grouped searches

When the **Log 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.

Bug 33667: 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 that are returned by the search, the graphs do not correctly display the maximum and minimum values for the time period you have searched.

Bug 33693 and 34551: 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** tab, a tooltip is displayed, providing information about 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.

Bug 33833 and 38503: 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.

Bug 34248: Regex-based numeric custom property columns do not sort properly

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

Bug 34298: Deleted custom properties are still displayed in saved searches

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

Bug 34321: Destination address and source address parameters do not display geographic flags

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

Bug 34299: Pie charts configured to graph deleted custom calculated properties might not display correctly

Pie charts on the **Log 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.

Bug 34412: Canceling a queued search might result in error

On the **Manage Search Results** page of the **Log Activity** tab, 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.

Bug 34772: Sorting on a search in progress generates fatal exception error

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

Bug 35319: Time series chart might fail to display in concurrent searches that group on the same custom property

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

Bug 35533: Benign error message displayed in error log when you change display options on Log Activity tab

When viewing data in real time (streaming) mode on the **Log Activity** tab, 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.

Bug 35600: Grouped search results are not sorted in the same order when exported to a CSV or XML file

On the **Log Activity** tab, 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.

Bug 35665: Save Criteria window might not retain check marks that indicate which group in which the Saved Search Criteria Belongs

When you save search criteria on the **Log Activity** tab, 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.

Bug 36027 and 36065: Canceling a queued search might result in the search displaying an error status

On the **Log Activity** tab, 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.**

Bug 38762: Out of Memory errors might occur when you sort 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 you sort search results by the **Payload** parameter.

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

Bug 37785 or 38301: 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.

Bug 39814: Error occurs when you search for events using the payload matches regular expression filter

An error occurs when you search events using the following search filter on the edit search page: **Payload Matches Regular Expression > Is >`<regex>`**. If you

type a regular expression that starts with a square bracket ([), the following error message is displayed:

```
regex used: [<regex 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.

Bug 40448: No search results returned for Reference Set filter if the reference set elements contain a dollar symbol

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

Bug 41511: Special characters are processed as wildcard characters in the Quick Filter text field

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

Bug 41966: 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.

Bug 42522: Deleted custom properties are not removed from the user interface

An issue might occur where the user interface may display a deleted custom property. When you delete a custom property, an error message displays if there are saved searches that use that custom property. You are directed to delete the specified saved searches. After you delete the saved searches, and then delete the custom property without error messages, the custom property might still be displayed in property lists on the user interface.

Bug 42653: Benign error message might display on the Save Criteria dialog box

On the **Log Activity** tab, an error message might be displayed if you click **OK** on the **Save Criteria** dialog box before the list of group is displayed. This error message is benign.

Bug 44380: MAC address filter does not validate character length

In event searches, the MAC Address filter does not indicate when you inadvertently typed an extra character. For example, 11-22-4f-5e-66-888 instead of 11-22-4f-5e-66-88. As a result, your MAC Address filter fails to return results.**Bug 18091: Event searches grouped by the Log Source Group parameter takes an extended period of time to complete**

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

Bug 30053: 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 you search for an Event ID of 624, the filter results could include 4624.

Bug 39357: 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 quotation marks (“) around the numeric QID.

Bug 42692: Text on the Payload parameter tooltip is truncated

When you move your mouse over the **Payload** parameter on **Log Activity** tab search results, the text in the tooltip is truncated.

Bug 44333: Event Processor Equals Console filter does not function when you view events in Last Interval mode

When you view events in **Last Interval** mode on the **Log Activity** tab and then add the **Event Processor Equals Console** filter, the correct results do not display. The results display events from the managed hosts.

Bug 44334: Log Source list might not populate correctly on the Add Filter dialog box

The **Log Source** list for the **Log Source** filter on the **Add Filter** dialog box might not include all manually added log sources. This might occur if you had added two log sources that used the same log source name, and then edited the log source name of one of them.

Workaround: The **Log Source** list populates correctly on the new or edit search page. If this error occurs to you, you can add your Log Source filter on the new search page.

Reports tab

Bug 25516: Reports display Start Date and Start Time parameters in different format than the corresponding search results

Reports that are based on an event 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** 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.

Bug 31737: 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.

Bug 36789: 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.

Bug 41948 and 40086: 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.

Bug 41911: Report charts cannot display multiple parameters on the X-axis

Report charts that are based on search results that are grouped on multiple parameters do not display all grouped parameters on the X-axis.

Bug 44466: Reports tab is not automatically refreshed after you create a new report

The list of reports on the **Reports** tab is not automatically refreshed after you create a new report.

WinCollect

Bug 38602: 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 QRadar Log Manager as log source events. The events for Invalid Handle or Overlapping I/O process can be ignored.

Bug 38655: 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 QRadar Log Manager.

Bug 40729: 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 addendum

This release notes included the documentation amendments. The updates that are listed in this addendum are included in the PDF documentation, but are not included in the Online Help.

System and License Management Updates

This maintenance release includes the following amendments to the System and License Management chapter of the *IBM Security QRadar Log Manager Administration Guide*:

- The Unlocked license status description is updated to increase the default grace period to 14 days.:

  Unlocked - Indicates that this license has been unlocked. You can unlock a license if it has been deployed within the last 14 days. This is the default grace period to reallocate a license. After the grace period is passed, the license is locked to the system. If you need to unlock a license after that period, contact Customer Support.

- All content related to the **Actions > Export System** menu item is removed.
- The **Allocating a system to a license** task is updated to include a missing step:

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System and License Management** icon.

Step 4 From the **Display** list box, select **Licenses**.

Step 5 Select an unallocated license.

Step 6 Click **Allocate System to License**.

Step 7 Optional. To filter the list of licenses, type a keyword in the Upload License search box.

Step 8 From the list of licenses, select a license.

Step 9 Select a system.

Step 10 Click **Allocate License to System**.

Configuring browser and document mode for Microsoft Internet Explorer

You must configure browser mode and document mode if you use Microsoft Internet Explorer to access IBM Security QRadar.

Procedure

Step 1 In your Microsoft Internet Explorer browser, press F12 to open the Developer Tools window.

Step 2 To configure browser mode, from the **Browser Mode** list box, select the version of your web browser.

Step 3 To configure document mode, from the **Document Mode** list box, select the version of your web browser.

Step 4 For example, Internet Explorer 9 users can select **Browser Mode: IE9** and **Document Mode: IE 9 Standards**.

A NOTICES AND TRADEMARKS

What's in this appendix:

This section describes some important notices, trademarks, and compliance information.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the

capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at *http://www.ibm.com/legal/copytrade.shtml*.

The following terms are trademarks or registered trademarks of other companies:

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.