IBM Security QRadar
Version 7.2.0

Troubleshooting System Notifications Guide

Note: Before using this information and the product that it supports, read the information in “Notices and Trademarks” on page 57.

CONTENTS

A NOTICES AND TRADEMARKS

ABOUT THIS GUIDE

The *IBM Security QRadar Troubleshooting System Notifications Guide* provides information on how to troubleshoot and resolve system notifications that display on the QRadar Console. System notifications that display on the Console can apply to any appliance or QRadar product in your deployment.

Unless otherwise noted, all references to QRadar can refer to the following products:

- IBM Security QRadar SIEM
- IBM Security QRadar Log Manager
- IBM Security QRadar Network Anomaly Detection

Intended audience

This guide is intended to assist users or administrator on how to troubleshoot error, warning, health, or informational system notifications generated by QRadar systems. This includes QRadar Consoles, QRadar Risk Manager, QRadar Vulnerability Manager, and managed hosts in your QRadar deployment.

Conventions

The following conventions are used throughout this guide:

Note: Indicates that the information provided is supplemental to the associated feature or instruction.

CAUTION: *Indicates that the information is critical. A caution alerts you to potential loss of data or potential damage to an application, system, device, or network.*

WARNING: *Indicates that the information is critical. A warning alerts you to potential dangers, threats, or potential personal injury. Read any and all warnings carefully before proceeding.*

Technical documentation	For information on how to access more technical documentation, technical notes, and release notes, see the ***Accessing IBM Security QRadar Documentation Technical Note***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)
Contacting customer support	For information on contacting customer support, see the ***Support and Download Technical Note***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)
Statement of good security practices	IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

1 SYSTEM NOTIFICATIONS

IBM Security QRadar provides notifications for a variety of events that occur in your QRadar deployment or on your QRadar system. This document is intended to explain and assist with resolving notifications displayed to QRadar users.

Note: For more information on system notifications, see the support website, located at *https://ibm.com/support*.

Error notifications

The following notifications are categorized as system errors.

Out of Memory

This notification occurs when a QRadar application or service runs out of memory.

Error Message

```
Application ran out of memory.
```

Explanation

QRadar monitors the status of the applications and services. When QRadar detects that no additional memory or swap space can be allocated to an application or service, then the application or service can stop functioning. Out of memory issues can be caused by software, or user defined queries and operations that exhaust the available memory.

Behavior

The notification is generated and a detailed error message is written to /var/log/qradar.log to outline the cause of the memory issue.

Resolution

- Review /var/log/qradar.log to determine the cause of the notification. A service restart might be required to halt the offending application or service and redistribute resources.
- Review your system to determine if the notification occurs during large vulnerability scans or while importing large volumes of data in QRadar.

  For example, importing a large number of records from a log source using JDBC or the log file protocol can consume large amounts of system resources. If multiple large data imports occur simultaneously, then you can stagger the start time intervals for data imports.

- If out of memory notifications are a reoccurring issue, you can contact customer support.

Accumulator cannot read global view definition

This notification occurs due to a synchronization issue where the global view configuration in memory has written erroneous data to the database.

Error Message

```
Accumulator: Cannot read global view definition in order to
prevent an out of sync problem global views can no longer be
created or loaded. Time series graphs will no longer work as
well as reporting.
```

Explanation

The accumulator is a QRadar process that counts and prepares events and flows in data accumulations to assist with searches, displaying charts, and report performance. The accumulator process aggregates data in pre-defined time spans to create global views. A global view is the data set indexed to draw a Time Series graph or run scheduled reports. The process is available on appliances where event data is processed and stored.

Behavior

In order to prevent data corruption, QRadar disables global views. When global views are disabled, time series graphs, saved searches, and scheduled reports for hourly, daily, weekly, and monthly time frames display empty graphs in their data sets.

Resolution

Contact customer support for a resolution.

Auto update error encountered

This notification occurs when auto updates attempts to update your QRadar Console, but cannot continue.

Error Message

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

Explanation

Auto updates is a feature on the **Admin** tab of QRadar that allows you to check for QRadar updates, schedule updates for maintenance, view installed or failed updates, or examine logs for updates made to your QRadar system. If the update process encounters an error or cannot connect to an update server, then this notification is generated. The QRadar Console is responsible for migrating all updates to managed hosts in your deployment.

Behavior

The system behaves as normal; however, the auto update system encounters an error and cannot update QRadar.

Resolution

To resolve this issue, you can select one of the following options:

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

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

- Verify that your QRadar Console has connectivity and can access your update server.

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

- If the notification persists and you cannot resolve the issue, contact customer support.

CRE: Failed to read rules

This error occurs when the Custom Rules Engine (CRE) on an Event Processor is unable to read a rule to correlate an incoming event.

Error Message

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

Explanation

The Custom Rules Engine (CRE) is a process that allows QRadar to correlate incoming events against rule sets that have been defined by a user or the default rule set of QRadar. CRE is the process responsible for validating if an event matches a rule set and can trigger alerts, offenses, or notifications in QRadar. For example, a rule test that generates an offense after 5 failed login attempts within 10 minutes or matching regular expressions are rules evaluated by the CRE. The process is available on appliances where event data is processed and stored.

Behavior

- **Single rule read failure** - The notification message contains a single rule that the Custom Rule Engine was unable to read. In most cases, a recent rule change is the reason for the notification. The payload of the notification message displays the rule or rule of the rule chain responsible. The system should behave normally and the user interface of QRadar is available.
- **Complete rule set read failure** - In rare circumstances, data corruption can cause a complete failure of the rule set. An application error is displayed and the rule editor interface of QRadar might become unresponsive or generate additional errors.

Resolution

To resolve this issue, you can select one of the following options:

- **Single rule read failure** - In the case of a single rule read error you can review the following options:
  - Temporarily disable the rule to locate the rule that is causing the notification.
  - Edit the rule to revert any recent changes made by QRadar users.
  - Delete and recreate the rule in question that is causing the error.
- **Complete rule set read failure** - In the case of an application error and notifications that the CRE failed to read rules, you can contact support for a resolution.

Backup requires more disk space

This notification occurs when there is not enough free space to perform a backup.

Error Message

```
Backup: Not enough free disk space to perform backup.
```

Explanation

Disk Sentry is responsible for monitoring QRadar for disk and storage issues. Before a backup begins in QRadar, Disk Sentry checks the available disk space to determine if the backup can complete successfully. If you are above the threshold limit of 90% on the partition containing your backup data, then the backup is cancelled. By default, QRadar stores backups in /store/backup.

Behavior

This notification is generated when a backup is cancelled due to insufficient disk space.

Resolution

To resolve this issue, you can select one of the following options:

- Free up disk space on your QRadar appliance to allow for a backup to complete in /store/backup.
- Configure your existing backups to use to a partition with free disk space.
- Configure off-board storage for your appliance. For more information, see the *Configuring Offboard Storage Guide*.

Process monitor application failed to start multiple times

This notification occurs when the system is unable to start an application or process after multiple attempts.

Error Message

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

Explanation

QRadar uses this notification to warn you that the system is unable to start an application or process on your QRadar system.

Behavior

This notification is generated and QRadar attempts to start the failed application or process.

Resolution

To resolve this issue, you can select one of the following options:

- Review your flow sources to determine if a device has stopped sending flow data or determine if users have deleted a flow source from QRadar.

  Flow process issues are a common occurrence of this notification.The Deployment Editor expects flow data as the appliance contains a QFlow process that is enabled. To resolve this notification issue, you can either remove the QFlow process from the Deployment Editor or you can assign a flow source for your flow data on the **Admin** tab with the **Flow Sources** icon.
- If you have verified your flow sources and the notification still occurs, contact customer support.

Process monitor must lower disk usage

This notification occurs when the process monitor is unable to start processes due to a lack of system resources.

Error Message

```
Process Monitor: Disk usage must be lowered.
```

Explanation

Disk Sentry is responsible for monitoring QRadar for disk and storage issues. Before QRadar attempts to restart a process, the system validates the state of the disk to ensure that a process can start. This notification warns you that QRadar is unable to start a process on your system due to disk capacity. The storage partition on QRadar is likely 95% full or greater.

Behavior

This notification is generated and QRadar attempts to start an application or process, but cannot due to a shortage of disk space.

Resolution

To resolve this issue, you must free up disk space by manually deleting files or changing your event or flow data retention policies. QRadar can automatically restart system processes after you free up enough disk space to fall below a threshold of 92% capacity.

Event pipeline dropped events

This notification occurs when an event or flow is dropped from the QRadar event pipeline when processing data in QRadar.

Error Message

```
Events/Flows were dropped by the event pipeline.
```

Explanation

The QRadar event pipeline is responsible for receiving, processing, normalizing, and coalescing incoming event and flow data before it is stored to disk and prepared for display in QRadar. In the event pipeline, QFlow is responsible for collecting flow data and DSMs are responsible for collecting event data. If there is an issue with the event pipeline or you exceed your license limits, an event or flow can be dropped. QRadar attempts to mitigate pipeline issues or license-based dropped events and flows by queueing event and flow data. When the queue is full or exceeds the system rating, then the Event Collection System (ECS) in the event pipeline can drop an event or flow. Dropped events and flows cannot be recovered.

Details for this notification can include the following helpful licensing information:

- The EP (event processor) incoming event rate <EPS rate> is exceeding the event per second (EPS) rate of your appliance <license limit>.
- The average <flow source> rate on the wire in the last 60 seconds was <average flow rate> <peak flow rate>.
- The average event rate <log source> in the last 60 seconds was <average EPS> and within that time the license has exceeded <license limit> on the system <number of times exceeded>.

Behavior

This notification is generated and the event or flow that was dropped cannot be recovered by QRadar. The details of the notification message contain additional information on the events or flows dropped by the event pipeline.

Resolution

To resolve this issue, you can review the following options:

- Verify the incoming event and flow rates on your system. If the event pipeline is dropping events, you can expand your license to accommodate the additional data.
- Review recent changes to rules or custom properties on your system. Rule or custom property changes could be the cause of sudden changes to your event or flow rates and can possibly impact system performance.
- Determine if the issue corresponds with SAR sentinel notifications. SAR notifications can indicate performance issues and the performance issues can lead to unnecessarily queued events and flows in the event pipeline. QRadar attempts to mitigate performance issues by routing events to stored, instead of dropping an event.

- Tune the system to reduce the volume of events and flows entering the event pipeline.

Note: Altering your routing rules does not help a licensing issue as routing is part of the event pipeline and included in licensing limits.

Event pipeline dropped connections

This notification occurs when the event pipeline receives a notification message from a TCP-based protocol that the protocol dropped an established connection to QRadar.

Error Message

```
Connections were dropped by the event pipeline.
```

Explanation

The QRadar event pipeline is responsible for receiving, processing, normalizing, and coalescing incoming event and flow data before it is stored to disk and prepared for display in QRadar. In the event pipeline, a limit exists on the number of connections that can be established to QRadar by TCP-based protocols. This limit protects QRadar from reaching the maximum number of file handles allowed in the Event Collection System (ECS). ECS can allow a maximum of 15,000 file handles with each TCP connection consuming 3 file handles. This limit ensures that connections can be established and events can be forwarded to QRadar.

TCP protocols that provide drop connection notifications include:

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

Behavior

This notification is generated and the connection to QRadar has been dropped by the protocol.

Resolution

To resolve this issue, you can review the following options:

- Distribute events to additional appliances in your QRadar deployment. Connections can be made to other event and flow processors to off-load the connections and distribute the work load off of the QRadar Console.
- Transition low priority TCP log source events to use the UDP network protocol.
- Tune the system to reduce the volume of events and flows entering the event pipeline.

Auto update installed with errors

This error notification occurs when a scheduled auto update installs, but generates an error that requires review.

Error Message

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

Explanation

Auto updates is a feature on the **Admin** tab of QRadar that allows you to check for QRadar updates, schedule updates for maintenance hours, view installed or failed updates, or examine logs for updates made to your QRadar system. A QRadar update can successfully install, but generate an error that requires review by an administrator. The most common occurrence of auto update errors is a missing software dependency for a DSM, protocol, or scanner update.

Behavior

The auto update process completed the scheduled update, but one or more files installed with errors. The installation error was not catastrophic and QRadar continued to install updates. However, you should review recent auto updates to determine if you need to reinstall or download a missing software dependency.

Resolution

To resolve this issue, you can select one of the following options:

- In the **Admin** tab, click the **Auto Update** icon and select **View Update History** to determine the cause of the installation error. You can view, select, then attempt to reinstall a failed rpm through the auto updates interface.
- If an auto update is unable to reinstall with the auto updates interface, then you can manually download and install the missing dependency or rpm file on your QRadar Console. You must have SSH access to your QRadar Console to manually install an rpm. All files available through auto updates are also available on Fix Central.
- If the notification persists and you cannot resolve the issue, contact customer support.

Standby high availability (HA) system failure

This notification occurs when the standby (secondary) system in a high availability pair (HA) has failed or is unresponsive.

Error Message

```
Standby HA System Failure.
```

Explanation

QRadar uses a heart beat to communicate between HA pairs to determine that they can properly communicate and failover, when required. If the primary system cannot communicate to the standby system, then this notification is displayed. The status of the secondary appliance switches to FAILED. When the standby system is in a FAILED state, then QRadar has no HA protection.

Behavior

This notification is generated to alert you that the standby system is unresponsive or has failed. The notification message provides additional detail with the IP address of the failed system and the IP address of the primary system.

Resolution

To resolve this issue, you can review the following resolutions:

- You can attempt to restore the secondary from the QRadar user interface. Click the **Admin** tab, click the **System and License Management** icon and attempt to restore your appliance with the **Restore System** option.
- Inspect the secondary HA appliance to determine that it is not powered down or has experienced a hardware failure.
- Verify if you can communicate from the primary to the standby system using PING.
- Ensure that there have been no changes to the switch connecting the primary and secondary HA appliances that would prevent communication. You can also verify IPtables on the primary and secondary appliance.
- Review qradar.log on the standby appliance to determine the cause of the failure. The qradar.log file is located in /var/log/.
- Review the HA Guide for detailed information on resolving issues between your primary and secondary HA appliance.
- If you cannot resolve this issue, contact customer support for assistance.

Primary high availability (HA) system failure

This notification occurs when the secondary takes over as the primary and has failed or is unresponsive.

Error Message

```
Primary HA System Failure.
```

Explanation

QRadar uses a heart beat to communicate between HA pairs to determine that they can properly communicate and failover, when required. If the primary system cannot communicate to the standby system, then this notification is displayed to alert you of the condition of the primary system. The status of the primary appliance switches to OFFLINE. When the primary system is in an offline state, then QRadar attempts to failover to the standby (secondary) appliance.

Behavior

This notification is generated to alert you that the primary system is unresponsive or has failed. The secondary system takes over QRadar operations from the failed primary system. The notification message provides additional detail with the IP address of the failed system and the IP address of the secondary system.

Resolution

To resolve this issue, you can review the following resolutions:

- Inspect the primary HA appliance to determine that it is not powered down or has experienced a hardware failure.
- You can attempt to restore the primary from the QRadar user interface. Click the **Admin** tab, click the **System and License Management** icon and from the **High Availability** menu, attempt to restore your appliance with the **Restore System** option.
- Review qradar.log on the standby appliance to determine the cause of the failure. The qradar.log file is located in /var/log/.
- Verify if you can communicate from the secondary to the primary system with PING.
- Ensure that there have been no changes to the switch connecting the primary and secondary HA appliances that would prevent communication. You can also verify IPtables on the primary and secondary appliance.
- If you cannot resolve this issue, contact customer support for assistance.

Infrastructure component corrupted

This notification occurs when an infrastructure component responsible for host services on a managed host in the deployment did not start or is corrupted.

Error Message

```
Infrastructure component corrupted.
```

Explanation

QRadar managed hosts in the deployment use services that are responsible for communication (IMQ) and the PostgreSQL™ database on managed hosts. When the message service or database cannot be started or rebuilt on a managed host, then the system notifies users to an important infrastructure problem in your deployment.

Behavior

This notification is generated to caution you about an error condition on a managed host that prevents the managed host from operating properly and communicating data to the QRadar Console. The notification message provides additional detail with the corrupted host service and IP address of the managed host that requires immediate attention.

Resolution

To resolve this issue, you must contact customer support for assistance.

Data replication experiencing difficulty

This notification occurs when the QRadar Console experiences performance issues when it attempts to replicate database information from the QRadar Console to managed hosts in your deployment.

Error Message

```
Data replication experiencing difficulty.
```

Explanation

The QRadar Console is responsible for preparing select PostgreSQL™ database tables for managed hosts in your deployment to download from the QRadar Console. This process is called data replication. The purpose of data replication is to ensure that managed hosts can continue to operate and collect data in the event that the QRadar Console becomes unavailable or experiences a failure. If a managed host repeatedly falls behind on its replication data downloads, then the notification warns users of a possible performance problem or communication issue.

Behavior

This notification is generated to warn you that a managed host in your deployment is experiencing difficulty downloading replication data. The QRadar Console behaves normally.

Resolution

In most situations, a managed host attempts to resolve the replication issue on its own. However, if a managed host repeatedly generates this notification, you can contact customer support for assistance.

Failed to install high availability (HA)

This notification occurs when the default installation time limit is reached when you attempt to add a high availability appliance.

Error Message

```
There was a problem installing High Availability on the cluster.
```

Explanation

When you install an HA appliance, the installation process is responsible for linking the primary and secondary appliances. The configuration and installation process contains a time interval to determine when an installation requires attention. If the high availability installation exceeds a six hour time limit, then a notification communicates the issue to users.

Behavior

This notification is generated to warn you that QRadar experienced difficulty when installing HA. QRadar should behave normally, but no HA protection is available until the issue is resolved.

Resolution

To resolve this issue, you must contact customer support for assistance.

Failed to uninstall high availability (HA)

This notification occurs when QRadar attempts to remove a high availability appliance from a cluster, but is unable to complete the process.

Error Message

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

Explanation

When you remove an HA appliance, the installation process is responsible for removing connections and data replication processes between the primary and secondary appliances. If the installation process cannot remove the HA appliance from the cluster properly, then a notification communicates the issue to users.

Behavior

This notification is generated to warn you that QRadar experienced difficulty when attempting to remove a high availability appliance. The primary system should behave as normal.

Resolution

To resolve this issue, you can review the following resolutions:

- You can attempt to remove the high availability appliance a second time.
- If your QRadar system is unable to remove the secondary from the cluster after repeated attempts, you can contact customer support for assistance.

Scanner initialization error

This notification occurs when a scheduled vulnerability scan is unable to connect to the an external scanner to begin the scan import process.

Error Message

```
A scanner failed to initialize.
```

Explanation

QRadar imports vulnerability data from network security scanner appliances by adding scanners and creating a schedule in QRadar to import vulnerability data from APIs or downloading completed scan reports. If a scheduled scan cannot initialize to begin a scan, then the notification alerts the users to the issue. Scan initialization issues are typically caused by credential problems or connectivity issues to the remote scanner. Scanners that fail to initialize display detailed error messages in the hover text of a scheduled scan with a status of failed.

Behavior

This notification is generated and a connection could not be made to the external scanner. The QRadar system behaves normally, but the failed scan requires investigation.

Resolution

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **Schedule VA Scanners** icon.

Step 4 From the scanner list, hover the cursor in the Status column of any scanner to display a detailed success or failure message.

The most common cause of scan failures are configuration issues. The detailed error message provides additional information on how to resolve the failed scan. If you cannot resolve or determine the context of the error message, you can contact customer support.

Filter initialization failed

This notification occurs when a Traffic Analysis does not start or initialize properly.

Error Message

```
Traffic analysis filter failed to initialize.
```

Explanation

The Event Collection Service (ECS) contains a process for automatically discovering and creating new log sources from events called Traffic Analysis. If a configuration does not save correctly or if a configuration file for Traffic Analysis is corrupted, then service can fail to initialize.

Behavior

The notification is generated and new log source that support automatic discover cannot be added automatically as Traffic Analysis is not started.

Resolution

To resolve this issue, you can select one of the following options:

- You must manually create log sources for any new appliances or event sources in your network until Traffic Analysis is functional, as auto discovery is not possible. All new event sources in QRadar can identify as SIM Generic, until mapped to a log source.
- If the initialization notification occurs with an auto update error notification, you can review the auto update log to determine if a DSM or protocol installed with an error.
- If the notification persists, you can contact customer support.

Disk storage unavailable

This warning notification occurs when one or more storage partitions are not accessible on the disk.

Error Message

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

Explanation

Disk Sentry is responsible for monitoring QRadar for disk and storage issues. The availability of a storage partition is determined with the touch command. If the Disk Sentry does not receive a response within a 30 second threshold, then this notification can display. This notification does not necessarily indicate a storage partition issue exists, as the system might be under heavy load and not respond within threshold.

However, if the storage unavailable notification is generated with notifications that QRadar has dropped events, then administrators should investigate that the storage partition is available.

Behavior

This notification is generated with details containing the host name and the partition that the Disk Sentry believes is unavailable.

Resolution

To resolve this issue, you can select one of the following options:

- Verify the status of your /store partition with the touch command.

  If the system responds to the touch command, then the disk storage unavailable notification is likely due to system load. In most cases, the notification does not indicate a disk issue when you also see SAR Sentinel notifications as the system load is typically the root cause.
- Determine if the notification corresponds with notification event pipeline dropped events.

  If QRadar indicates the system dropped events and disk storage is unavailable, then this can indicate that event and flow queues are full and the system is dropping events. Administrators should investigate the status of storage partitions for QRadar.
- If the notification persists, you can contact customer support for assistance.

Insufficient disk space for data export

This notification occurs when there is not enough free space to perform a data export.

Error Message

```
Insufficient disk space to complete data export request.
```

Explanation

QRadar allows you to export event, flow, and offense data to a directory for backup purposes. Before an export begins, the system monitors the amount of available disk space to determine if the export can complete successfully. If the partition does not contain enough space for your data export, then the export is cancelled.

Behavior

This notification is generated when an export is cancelled due to insufficient disk space. The system behaves as normal.

Resolution

To resolve this issue, you can select one of the following options:

- Free up disk space on your QRadar appliance to allow for a data export to complete in /store/exports.
- Configure the System Settings for QRadar to use to a partition with free disk space.
- Configure off-board storage for your data exports. For more information, see the *Configuring Offboard Storage Guide*.

Accumulator dropped records

This notification occurs when an event or flow accumulation is dropped from a data set.

Error Message

```
Flows/Events were dropped by the Accumulator.
```

Explanation

The accumulator is a QRadar process that counts and prepares events and flows in data accumulations to assist with searches, displaying charts, and report performance. The accumulator process aggregates data in pre-defined intervals to create a global view. A global view is the data set indexed to assist with Time Series graphs, searches, quickly generating scheduled reports. QRadar can drop an accumulation interval when the system attempts to process too much data for the global view or when the system load prevents the accumulation from completing within the defined threshold.

A dropped accumulation does not indicate that QRadar has lost any data. The original data for QRadar is maintained, as accumulations are data sets generated from stored data, but do not impact stored data when dropped. The notification provides additional detail on the dropped accumulation interval. The process is available on appliances where event data is processed and stored.

Behavior

The accumulator drops the interval containing the event or flow data for accumulation. The system should behave normally, however, the dropped interval is not displayed in the data set for your report, search, or chart.

Resolution

To resolve this issue, you can select one of the following options:

- Determine if the notification corresponds with SAR Sentinel notifications. If the dropped accumulation occurs with SAR Sentinel notifications, the issue is likely due to system load.
- Review recently added reports or time series searches for large numbers of unique values.
- Run the search, report, or chart display in QRadar and reduce the scope of the search data. A smaller data set is more easily processed and might resolve the issue.
- If the notification persists, you can contact customer support for assistance.

Scan tool failure This notification occurs when QRadar Vulnerability Manager stopped a failed scan.

Error Message

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

Explanation

QRadar Vulnerability Manager generates vulnerability data by detecting vulnerabilities within the applications, systems, or devices on your network. The scan engine requires information from the scan tools to discover and gather information from external scanners before a scan can begin. This notification is generated to inform you that the scan tools stopped unexpectedly. This notification is likely to occur when QRadar Vulnerability Manager cannot communicate properly to an external scanner configured in the Deployment Editor. QRadar Vulnerability Manager attempts to retry the connection to the external scanner five times in 30 second intervals.

In rare cases, the notification can be generated when the discovery tools for QRadar Vulnerability Manager encounter an untested host or network configuration.

Behavior

The notification is generated and QRadar Vulnerability Manager is unable to initialize a vulnerability scan to collect asset data from external scanners. Asset scan results cannot be imported from external scanners; however, the QRadar Console behaves as normal.

Resolution

To resolve this issue, you can select one of the following options:

- Review the configuration for any external scanners configured in the Deployment Editor to ensure the gateway IP address supplied is correct.
- Ensure that QRadar Vulnerability Manager can communicate through the supplied IP address and that firewall rules for your DMZ are not blocking communication between your appliance and the assets you expect to scan.
- If the notification persists, you can contact customer support.

External scan gateway failure

This notification occurs when QRadar Vulnerability Manager is configured with an external scanner and not supplied with a valid gateway IP address.

Error Message

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

Explanation

QRadar Vulnerability Manager can collect data about assets in your network by configuring an external scanner in the Deployment Editor. When an external scanner is added, the configuration requires a gateway IP address. If the address supplied in the Deployment Editor is incorrect or has changed, then this notification can display as QRadar Vulnerability Manager cannot access the DMZ. For more information about external scanners, see the *QRadar Vulnerability Manager Users Guide*.

Behavior

The notification is generated and QRadar Vulnerability Manager is unable to initialize an asset scan for your external scanner. Asset data cannot be collect from the external scanner as the scan is stopped. The QRadar Console behaves as normal.

Resolution

To resolve this issue, you can select one of the following options:

- Review the configuration for any external scanners configured in the Deployment Editor to ensure the gateway IP address supplied is correct.
- Ensure that QRadar Vulnerability Manager can communicate through the supplied IP address and that firewall rules for your DMZ are not blocking communication between your appliance and the assets you expect to scan.
- If the notification persists, you can contact customer support.

System health notifications

The following notifications are categorized as system health errors.

Disk Failure

This notification occurs when the hardware monitor on your QRadar appliance determines that a disk on the system has failed.

Error Message

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

Explanation

QRadar monitors the status of the hardware on an hourly basis to determine when hardware support is required on the appliance. Hardware monitoring leverages the hardware tools of your appliance to provide notifications through QRadar when intervention is required by system administrators. Disk failure notifications are available for both Dell and IBM xSeries appliances running QRadar.

Behavior

This notification is generated when the on-board system tools have noticed that a disk has failed. The notification identifies the failed disk and provides the slot or bay location of the failure.

Resolution

- If the notification persists, contact customer support.
- Open a customer support ticket to arrange for replacement parts.

Predictive disk Failure

This notification occurs when the hardware monitor on your QRadar appliance determines that a disk on the system is in a predictive failure state.

Error Message

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

Explanation

QRadar monitors the status of the hardware on an hourly basis to determine when hardware support is required on the appliance. Hardware monitoring leverages the hardware tools of your appliance to provide notifications through QRadar when intervention is required by system administrators. Predictive disk failure notifications are available for both Dell and IBM xSeries appliances running QRadar.

Behavior

This notification is generated when the on-board system tools have noticed that a disk is approaching failure or end of life. The notification identifies a predictive failed disk and provides the slot or bay location of the failure.

Resolution

Contact your server administrator to schedule maintenance for the disk in a predictive failed state. If the notification continues, you can open a customer support ticket to arrange for replacement parts.

Warning notifications

The following notifications are categorized as system warnings in QRadar.

Unable to determine associated log source

This notification occurs when Traffic Analysis is unable to automatically discover a log source for events provided to QRadar.

Error Message

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

Explanation

The Event Collection Service (ECS) contains a process for automatically discovering and creating new log sources from events called Traffic Analysis. Traffic Analysis identifies the log source from appliances that auto discover by analyzing the event payloads. At minimum, 25 events are required to identify a log source. If the log source cannot be identified by Traffic Analysis after 1,000 events, then QRadar abandons the auto discovery process. When a log source cannot be identified by the event payload and reaches the maximum threshold for Traffic Analysis, then the notification is generated.

Behavior

This notification is generated and the system behaves as normal. When Traffic Analysis exceeds the maximum threshold for auto discovery QRadar categorizes the log source as SIM Generic and labels the events as Unknown Event Log.

Resolution

To resolve this issue, you can review the IP address provided in the notification to identify the log source that could not be identified by QRadar.

- Review any log sources that forward events at a very low rate. Log sources with low event rates are a common cause of this notification.
- Ensure auto update downloads the latest DSMs to properly parse events for your QRadar system.
- Review any log sources that provide events through a central log server. Log sources provided from central log servers or management consoles can require their log sources to be created manually.
- Review the **Log Activity** tab to determine the appliance type from the IP address in the notification message and manually create a log source in QRadar.

- Verify if the log source is officially supported by QRadar. Officially supported appliances and software versions are listed in the *DSM Configuration Guide.*
  - If your appliance is supported, you can manually create a log source for the events that Traffic Analysis could not auto discover.
  - If your appliance is not officially supported, you can create a Universal DSM to identify and categorize your events.
- If the notification persists, you can contact customer support for assistance.

Backup unable to execute request

This notification occurs when a backup cannot start or fails due to a number of possible reasons.

Error Message

```
Backup: Unable to Execute Backup Request.
```

Explanation

QRadar uses this notification to alert when a backup cannot start or cannot complete due to a failure. The following issues can generate this notification message:

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

Behavior

This notification is generated each time a backup is unable to start or fails during the backup process.

Resolution

To resolve this issue, you can manually start a backup to determine if the failure reoccurs. If multiple backups fail to start, contact Customer Support.

Disk sentry: Disk usage exceeded threshold

This notification occurs when disk capacity exceeds a set threshold.

Error Message

```
Disk Sentry: Disk Usage Exceeded Max Threshold.
```

Explanation

Disk Sentry is responsible for monitoring QRadar for disk and storage issues. QRadar uses this notification to warn you that at least one disk on your system is 95% full.

Behavior

This notification is generated and processes are to shut down to prevent data corruption on your system.

Resolution

To resolve this issue, you must free up disk space by manually deleting files or changing your event or flow data retention policies. QRadar can automatically restart system processes after you free up enough disk space to fall below a threshold of 92% capacity.

TX Sentry: Non system transaction

This notification occurs when the Transaction Sentry determines that an outside process or transaction is causing a database lock.

Error Message

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

Explanation

The Transaction Sentry is a process of Hostcontext that is designed to monitor and restart processes when a database transaction exceeds a default threshold. By default, this threshold is 10 minutes. If a process needs to be restarted, then the Transaction Sentry determines the process identifier (PID) that initiated the transaction and restarts the process to prevent a database lock. When an outside process, such as a database replication issue, maintenance script, auto update, or command line process exceeds the default transaction threshold, then the notification is displayed.

Behavior

This notification is generated as the Transaction Sentry cannot identify and restart the process that exceeded the transaction limit. This notification is intended to alert customers to transactions that can cause database locks or system instability, if not resolved.

Resolution

To resolve this issue, you can select one of the following options:

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

- If this notification persists, you can contact customer support.

TX Sentry: Restored system

This notification occurs when the Transaction Sentry restores QRadar to normal system health by cancelling suspended database transactions or removing database locks.

Error Message

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

Explanation

The Transaction Sentry is a process of Hostcontext that is designed to monitor and restart processes when a database transaction exceeds a default threshold. By default, this threshold is 10 minutes. When a process is restarted and the transaction causing system issues returns QRadar to normal health, this notification is displayed.

Behavior

This notification is generated and the system should behave as normal. This notification is intended to alert customers that a process was restarted and transactions that can cause database locks or system instability were resolved.

Resolution

There is no resolution to this issue as the Transaction Sentry handled the stability problem automatically.

If you want to determine the process that caused the error, you can review qradar.log for the word TxSentry. The qradar.log can help identify the cause of the transaction issue.

Maximum active offenses reached

This notification occurs when the Magistrate component of QRadar is unable to create a new offense as the number of active offenses is at the limit.

Error Message

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

Explanation

Your QRadar system includes a limit to the number of active offenses that can be open on your system. By default, the limit is 2500 active offenses. An active offense is any offense that continues to receive updated event counts. A notification is displayed to alert users to this issue.

Behavior

This notification is generated when the active offense limit is reached. The system is unable to create new offenses or transition a dormant offense to an active

offense. A dormant offense is an open offense that has not received a new offense in 5 days or less.

Resolution

To resolve this issue, you can select one of the following options:

- You can review offenses that are of low security concern and transition them from open (active) to closed or closed protected to free up space for more important active offenses.

  To prevent an offense you want to close from being removed by your data retention policy, you can protect the closed offense.
- You can tune your system to reduce the number of events that generate offenses.

Maximum total offenses reached

This notification occurs when the Magistrate component of QRadar is unable to process offenses as the overall number of active and dormant offenses has reached the limit.

Error Message

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

Explanation

Your QRadar system includes a limit to the number of active and dormant offenses for your system. By default, the limit is 2500 open (active) offenses and 100,000 overall offenses. If this limit is reached, QRadar cannot properly transition the active, dormant, and inactive offense states.

If an offense has not received an event update in 30 minutes, then an active offense transitions to dormant. A dormant offense can transition to active if an event update occurs. After 5 days, dormant offenses without any event updates transition to inactive. If the maximum number of offenses is reached, then offenses must be closed to allow your data retention policy to free up space for new offenses.

Behavior

This notification is generated and the system cannot generate new active offenses or transition dormant offenses to active until you reduce the offense count.

Resolution

To resolve this issue, you can select one of the following options:

- You can transition offenses from open (active) to closed (dormant) to free up space for more important active offenses.

  To prevent an offense you want to close from being removed by your data retention policy, you can protect the closed offense.

- You can tune your system to reduce the number of events that generate offenses.
- You can adjust the offense retention policy on your system to an interval at which data retention can clean inactive offenses from QRadar.

Terminating long running reports

This notification occurs when a report exceeds a time limit set for report generation.

Error Message

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

Explanation

Your QRadar system includes a time limit for report generation. A process in QRadar is responsible for monitoring reports and terminating reports that take longer to complete than is required. Reports that run longer than the default time limits are cancelled.

Report time thresholds:

- Hourly reports - 2 hour time limit
- Daily reports - 12 hour time limit
- Manual reports - 12 hour time limit
- Weekly reports - 24 hour time limit
- Monthly reports - 24 hour time limit

Behavior

This notification is generated and the system cancels the report that exceeded the time limit.

Resolution

To resolve this issue, you can select one of the following options:

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

  A manual report that consistently generates this notification might be relying on raw data and not have access to accumulated data. You can edit your manual report and transition the report to use an hourly, daily, monthly or weekly schedule, which can to speed up report creation.
- If this notification persists, you can contact customer support.

TX Sentry: No transactions for a managed process

This notification occurs when the Transaction Sentry determines that a managed process, such as Tomcat or Event Collection Service (ECS) is the cause of a database lock.

Error Message

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

Explanation

The Transaction Sentry is a process of Hostcontext that is designed to monitor and restart processes when a database transaction exceeds a default threshold. By default, this threshold is 10 minutes. This notification is intended to notify a user when a QRadar managed process is forced to restart.

Behavior

This notification is generated and the system should behave as normal. This notification is intended to alert customers that a QRadar process was restarted and transactions that can cause database locks or system instability were resolved.

Resolution

To resolve this issue, you can select one of the following options:

- If this is an ongoing issue with Transaction Sentry, contact customer support.
- If you want to determine the process that caused the error, you can review qradar.log for the word TxSentry. The qradar.log can help identify the cause of the transaction issue.

Protocol source configuration incorrect

This notification occurs when QRadar detects an incorrect protocol configuration for a log source.

Error Message

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

Explanation

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

Behavior

This notification is intended to alert administrators that a configuration issue prevents a log source in QRadar from retrieving events.

Resolution

To resolve protocol configuration issues:

- Review the log source to ensure that the protocol configuration is correct.

  This can include verifying authentication fields, file paths, database names for JDBC, and ensuring QRadar can communicate to remote servers. You can hover your mouse pointer over a log source to view additional error information. When you edit a log source, an attempt to reconnect is made after you save your changes.
- Review the /var/log/qradar.log file for more information on the protocol configuration error.

MPC: Process not shutdown cleanly

This notification occurs when the Magistrate process encounters an error.

Error Message

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

Explanation

The Magistrate component of your QRadar system did not shut down properly or closed unexpectedly. When this issue occurs, any active offense is closed, similar to performing a Soft Clean of the SIM data model in the **Admin** tab. Services are restarted and the database tables are verified and rebuilt, if required.

Behavior

This notification is generated and the system closes all active offenses to allow the system to synchronize and prevent data corruption. If the Magistrate component detects a corrupted state, then the database tables and files are rebuilt.

Resolution

The Magistrate component is capable of self-repair and the notification is intended as an alert to administrators. If this notification becomes a reoccurring issue, then you should contact customer support.

Last backup exceeded the allowed time limit

This notification occurs when a backup process exceeds the configured time limit.

Error Message

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

Explanation

Backups in QRadar are assigned a time limit for completion. The time limit is determined by the backup priority you assign when you configure a backup in QRadar.

Default backup time limits:

- **Configuration Backup** - A default time interval of 3 hours (180 minutes) is allocated to configuration backups.
- **Data Backup** - A default time interval of 17 hours (1020 minutes) is allocated to data backups.

Behavior

This notification is generated and the backup that exceeded the time limit is cancelled.

Resolution

To resolve this issue, you can select one of the following options:

- Edit the backup configuration to extend the time limit allowed to complete the backup. Do not extend over 24 hours.
- Edit the failed backup and change the priority level to a higher priority. Higher priority levels allow QRadar to allocate more system resources to completing the backup.
- If a backup repeatedly fails, you can contact customer support for assistance.

Log source license limit

This notification occurs when a QRadar reaches the maximum number of log sources for the license on the appliance.

Error Message

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

Explanation

Every QRadar appliance is sold with a license that allows you to collect events from a specific number of log sources. If you approach or exceed your license limit, then QRadar notifies you of the condition. The notification provides detail on your current number of log sources and the maximum number of log sources allowed by your license.

Behavior

The notification is generated and any additional log sources added to QRadar are disabled by default. Events are not collected for disabled log sources.

Resolution

To resolve this issue, you can review the following options:

- On the **Admin** tab, click the **Log Sources** icon and disable or delete any log sources you consider a low priority or inactive event source. Disabled log sources do not count against your log source license. However, the event data collected by disabled log sources is still available and searchable.
- Ensure that log sources you deleted do not automatically rediscover in QRadar. If the log source rediscovers, you can disable the log source in QRadar. Disabling a log source prevents automatic discovery by Traffic Analysis.
- Ensure that you do not exceed your license limit when you bulk add log sources.
- If the notification persists or require additional log sources, you can contact your sales representative.

Log source created in a disabled state

This notification occurs when QRadar automatically adds a log source in the disabled state.

Error Message

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

Explanation

The Event Collection Service (ECS) contains a process to automatically discover and create new log sources from events called Traffic Analysis. If you are at your current log source license limit, then Traffic Analysis can create the log source in the disabled state. Disabled log sources do not count against your log source limit and do not collect events.

Behavior

The notification is generated and any additional log sources added to QRadar are disabled by default. Events are not collected for disabled log sources.

Resolution

To resolve this issue, you can review the following options:

- On the **Admin** tab, click the **Log Sources** icon and disable or delete any log sources you consider a low priority or inactive event source. Disabled log sources do not count against your log source license.
- Ensure that log sources you delete do not automatically rediscover in QRadar. If the log source rediscovers, you can disable the log source in QRadar. Disabling a log source prevents automatic discovery by Traffic Analysis.

- Ensure that you do not exceed your license limit when you bulk add log sources.
- If you require an expanded license to include additional log sources, you can contact your sales representative.

SAR Sentinel threshold crossed

This notification occurs when the System Activity Reporter (SAR) utility detects that your QRadar system load is above average.

Error Message

```
SAR Sentinel: threshold crossed.
```

Explanation

The SAR Sentinel utility monitors QRadar for a broad number of functions, such as running processes, CPU usage, and hardware functions. The function of the SAR Sentinel is to monitor the system and provide notifications when the system load exceeds a set threshold.

Behavior

This notification is generated and your QRadar system can experience reduced system performance.

Resolution

To resolve this issue, you can review the following options:

- In most cases there is no resolution is required. When the system notices that a threshold is crossed, a notification is provided. For example, CPU usage over 90%. The system automatically attempts to return to normal operation.
- If this notification is reoccurring, you can increase the default value of the SAR Sentinel. Click the **Admin** tab, then click the **Global System Notifications** icon and raise the notification threshold.
- For system load notifications, you can reduce the number of processes that run simultaneously.

  To reduce the number of simultaneous processes, you can stagger the start time for reports, vulnerability scans, or data imports for your log sources. You can also schedule backups and system processes to start at different times to lessen the system load.
- If your QRadar system is continually receiving SAR Sentinel threshold notifications, you can contact customer support for assistance.

User nonexistent or undefined

This notification occurs when QRadar attempts to perform a task when a user account or user role for the task does not exist.

Error Message

```
User either does not exist or has an undefined role.
```

Explanation

QRadar attempted to update a user account with additional permissions, but the user account or user role does not exist. This notification typically occurs when creating a new user or updating user roles on your QRadar system.

Behavior

This notification is generated and the system behaves as normal.

Resolution

To resolve this issue, you can review the following options:

- On the **Admin** tab, click **Deploy Changes**.

  Any update to user accounts or roles requires a deploy to update user account permissions. This notification often occurs when you perform a task without deploying, such as creating a user and attempting to update Security Profiles or User Roles. This notification can also occur when a user attempts a permissions update before the deploy in process completes.
- If multiple attempts to deploy changes are completed or a deploy never completes on your QRadar system, you can contact Customer Support for assistance.

Disk Sentry: disk usage warning

This notification occurs when the Disk Sentry utility detects that the disk usage on your QRadar system is greater than 90%.

Error Message

```
Disk Sentry: Disk Usage Exceeded warning Threshold.
```

Explanation

Disk Sentry is the process responsible for monitoring QRadar for disk and storage issues. Disk Sentry generates this notification to warn you that the disk space on your QRadar system is 90% full.

Behavior

This notification is generated to alert you that processes on QRadar can shut down when the disk space on your system reaches 90% full. At 95% full, QRadar begins to disable processes to prevent data corruption due to disk capacity.

Resolution

To resolve this issue, you must free up disk space by manually deleting files or changing your event or flow data retention policies. QRadar can automatically

restart system processes after you free up enough disk space to fall below a threshold of 92% capacity.

Events routed directly to storage

This notification occurs when the event pipeline cannot categorize events and flows, so the events are routed directly to storage.

Error Message

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

Explanation

The QRadar event pipeline is responsible for receiving, processing, normalizing, and coalescing incoming event and flow data before it is stored to disk and prepared for display in QRadar. If there is a performance problem in the event pipeline or you exceed your license limits, an event or flow can be routed directly to storage. Routing an event or flow to storage is preferable to dropping the event or flow data, as raw data is stored and searchable in QRadar, but not categorized or processed. QRadar attempts to mitigate event pipeline issues and license-based dropped events and flows by queueing event and flow data. The Event Collection System (ECS) in the event pipeline can route data to storage to prevent queues from filling up. QRadar cannot return and re-categorize events in storage after the issue is resolved.

Details for this notification can include the following helpful information:

- Flow Support Filter has sent a total of <value> flows directly to storage. <value> flows have been sent in the last <time> seconds. Queue is at <value> percent capacity.
- The current incoming raw flow rate: <value> fps is currently exceeding the <total> fps license set on the system.
- Event Forwarded Filter has sent a total of <value> events directly to storage. <value> events have been sent in the last <time> seconds. Queue is at <value> percent capacity.
- The current incoming raw event rate: <value> eps is currently exceeding the <total> eps license set on the system.

Behavior

This notification is generated and any incoming events or flows to the system are not categorized and sent directly to storage. Raw event and flow data is still collected and searchable, but the issue requires review to prevent queues from potentially dropping events.

Resolution

To resolve this issue, you can review the following options:

- Verify the incoming event and flow rates on your system. If the event pipeline is queuing events, you can expand your license to accommodate the additional data.
- Review recent changes to rules or custom properties on your system. Rule or custom property changes could be the cause of sudden changes to your event or flow rates and can possibly impact system performance or cause events to route to stored.
- A DSM parsing issues can cause the event data to route to storage. Verify if the log source is officially supported by QRadar. Officially supported appliances and software versions are listed in the *DSM Configuration Guide.*
- Determine if the issue corresponds with SAR sentinel notifications. SAR notifications can indicate performance issues and the performance issues can lead to unnecessarily queued events and flows in the event pipeline. QRadar attempts to mitigate performance issues by routing events to stored, instead of dropping an event.
- Tune the system to reduce the volume of events and flows entering the event pipeline.

Scan failure error This notification occurs when a scheduled vulnerability scan fails to import vulnerability data.

Error Message

```
A scanner has failed.
```

Explanation

QRadar imports vulnerability data from network security scanner appliances by adding scanners and creating a schedule in QRadar to import vulnerability data from APIs or downloading completed scan reports. If a scheduled scan cannot complete the import, then the notification alerts the users to the issue. Scan failures are typically configuration issues or performance issues due to the volume of the data import. Scan failures can also occur when a scan report downloaded by QRadar is in an unreadable format. Failed scans display detailed error messages to the cause of the failed scan in the hover text of a scheduled scan with a status of failed.

Behavior

This notification is generated and vulnerability data from the external scanner could not be retrieved. The QRadar system behaves normally, but the failed data import from the scanner requires investigation.

Resolution

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **Schedule VA Scanners** icon.

Step 4 From the scanner list, hover the cursor in the Status column of any scanner to display a detailed success or failure message.

The most common issue around scan failures are configuration issues. The detailed error message provides additional information on how to resolve the failed scan. If you cannot resolve or determine the context of the error message, you can contact Customer Support.

Custom property disabled

This notification occurs when a custom property is disabled due to performance problems.

Error Message

```
A custom property has been disabled.
```

Explanation

Custom properties allow you to search, view, and report on information within logs using regular expressions for data that QRadar does not typically normalize and display in the user interface. This notification indicates that a custom property is disabled due to problems processing the custom property. Rules, reports, or searches that use the disabled custom property cease to function properly. Before you re-enable a disabled custom event or flow property, you must review and refine the regular expression to reduce the performance impact. The notification contains additional information on the regex, custom property name, identifier, and payload for the event or flow custom property that was cancelled.

Behavior

This notification is generated and the system should behave normally after the resource intensive custom event property is disabled.

Resolution

To resolve this issue, you can select one of the following options:

- Review the disabled custom property to correct your regex patterns to resolve this issue. You should not re-enable disabled custom properties without reviewing and optimizing the regex pattern or calculation.
- Ensure the **Optimize parsing for rules, reports, and searches** check box is selected if the custom property is used for custom rules or reports.
- If the notification persists, you can contact customer support for assistance.

Device backup failure

This QRadar Risk Manager notification occurs when a device backup has failed in Configuration Source Management (CSM).

This notification only applies to deployments that include QRadar Risk Manager appliances.

Error Message

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

Explanation

QRadar Risk Manager uses Configuration Source Management to retrieve configuration information about devices in your network. The information downloaded from your network devices is used to populate topology maps on the **Risks** tab. The most common cause of this notification is configuration issues. Configuration Source Management attempts to log in to the device remotely. If the credentials or configuration is incorrect, the backup is likely to fail and the notification is generated.

Behavior

This notification is generated each time Configuration Source Management fails to backup a device or can occur when a backup is cancelled by the user.

Resolution

To resolve this issue, you can select one of the following options:

- The error message in CSM.
- Review the credentials and address sets in Configuration Source Management to ensure QRadar Risk Manager can log in to backup your devices and firewalls.
- Review the Configuration Source Management settings to verify the protocol configured to connect to your network device is valid. For a list device protocols, see the *QRadar Risk Manager Adapter Configuration Guide*.
- Ensure your network device and version is compatible with QRadar Risk Manager. For a list of compatible devices, see the *QRadar Risk Manager Adapter Configuration Guide*.
- Verify the device is available and that there is not a connectivity issue between your network device and QRadar Risk Manager.
- Verify that you have the latest adapters installed for QRadar Risk Manager.
- If the notification persists, you can contact customer support for assistance.

Event or flow data not indexed

This notification occurs when event or flow data is not indexed from the Ariel database.

Error Message

```
Event/Flow data not indexed for interval.
```

Explanation

QRadar contains a feature called Index Management that allows users to index the Ariel database for specific event and flow properties to optimize search results. Incoming data is indexed on specific intervals for your search term. If too many indexes are enabled or the system is overburdened, then QRadar can drop the event or flow from the index. The notification provides additional detail on the interval name if the interval was for the event or flow database.

Behavior

The interval for the event or flow index was dropped and that interval is not included in the search optimization. The system should behave as normal.

Resolution

To resolve this issue, you can select one of the following options:

- Determine if the notification corresponds with SAR Sentinel notifications. If the dropped index interval occurs with SAR Sentinel notifications, the issue is likely due to system load or low disk space.
- On the **Admin** tab, click the **Index Management** icon and temporarily disable some indexes to reduce the system load.
- If the notification persists, you can contact customer support for assistance.

Response action: threshold reached

This notification occurs when the Custom Rules Engine (CRE) attempts to respond to a rule in the system, but is unable to because the response threshold is full.

Error Message

```
Response Action: Threshold reached.
```

Explanation

The Custom Rules Engine (CRE) is a process that allows QRadar to validate incoming data against rules that have been defined by a user or the default rule set of QRadar. CRE determines if an event or flow matches a rule set. When the rule is triggered, the system can apply a response to the triggered rule called a response action.

Generic rules or a QRadar system that has not been tuned can generate a large number of response actions, especially systems with IF-MAP enabled. Response actions are queued in the system, so they can be processed by QRadar. If the queue exceeds 2000 response actions in the Event Collection System (ECS) or 1000 response actions in Tomcat, then response actions can be dropped. The notification provides additional detail on the responses that were dropped.

Behavior

The notification is displayed and the system should behave as normal. There is a possibility that QRadar is generating a large number of events if the notification persists. This notification is likely to display in systems that are not tuned, systems with generic rules that are too broad in scope, or systems with IF-MAP enabled, but incorrectly configured.

Resolution

- If IF-MAP is enabled on QRadar, verify that the connection to the IF-MAP server exists or that a bandwidth problem is not causing rule response queue to back up in Tomcat.
- You can tune your system to reduce the number of rules triggering to reduce the number of rule responses in the system.
- If the notification persists, you can contact customer support for assistance.

DRBD Sentinel: disk replication falling behind

This notification occurs when the Distributed Replicated Block Device (DRBD) Sentinel falls behind when it replicates data between a high availability (HA) primary and secondary appliance.

Error Message

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

Explanation

The DRBD Sentinel monitors data replication to ensure that data collected by the primary appliance is replicated immediately to the secondary. This notification alerts users that data replication between the primary and secondary HA system is falling behind on replication intervals. DRBD mitigates potential performance problems by queueing replication intervals and ensuring that the secondary acknowledges the data between appliances is correct. If the replication queue fills on the primary, it can increase the increase system load on the primary and create performance issues. The most common reasons for replication issues is the performance on the primary system, mount or storage issues on the secondary, or bandwidth issues between appliances.

Behavior

This notification alerts you that a high availability cluster is experiencing issues when replicating data from the primary to secondary. This notification can indicate potential performance issues on the primary, but in most cases the system behaves normally.

Resolution

To resolve this issue, you can select one of the following options:

- You can review bandwidth activity for your deployment by loading a saved search MGMT: Bandwidth Manager from the **Log Activity** tab. This search displays bandwidth usage between the Console and hosts in your deployment.

- Determine if the notification corresponds with SAR Sentinel notifications for your primary appliance. If SAR Sentinel notifications are reoccurring on the primary, this can indicate DRBD queues filling on the primary system and can lead to additional performance issues.
- Using SSH, you can verify the DRBD state of the primary to the secondary with the cat /proc/drbd command.
- If the DRBD notifications persists, you can contact customer support for assistance.

Expensive custom rule found

This notification occurs when the Custom Rules Engine (CRE) on an Event Processor identifies a custom rule that can cause performance issues.

Error Message

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

Explanation

The Custom Rules Engine (CRE) is a process that allows QRadar to correlate incoming events against rule sets that have been defined by a user or the default rule set of QRadar. CRE is the process responsible for validating if an event matches a rule set and can trigger alerts, offenses, or notifications in QRadar. For example, a rule test that generates an offense after 5 failed login attempts within 10 minutes or matching regular expressions are rules evaluated by the CRE.

When a user creates a custom rule, the custom rule can impact performance if the scope of the rule is too large or uses a regex pattern that is not optimized. The notification message displays the name of the rule or rule chain that the system believes is an expensive rule.

Behavior

This notification is generated and the system can start to experience performance issues when processing events and flows.

Resolution

- On the **Offenses** tab, click **Rules** and use the search window to locate and edit or disable the expensive rule.
- Determine if the notification corresponds with SAR Sentinel notifications. If SAR Sentinel notifications are reoccurring with the expensive rule notification, then you should investigate the rule to ensure it does not impact overall system performance.
- If the notifications persists, you can contact customer support for assistance.

Anomaly Detection Engine accumulation disabled

This notification occurs when an accumulation is disabled for an anomaly rule used by the Anomaly Detection Engine (ADE).

Error Message

```
Accumulation disabled for the Anomaly Detection Engine.
```

Explanation

QRadar continuously monitors incoming data to detect anomalies. The Anomaly Detection Engine is responsible for evaluating data and detecting patterns in a given data set that do not conform to an established normal behavior. The accumulator prepares anomaly data to create global views, which assist with searches, displaying data, and preparing data for discovering anomalies. If a global view is disabled or unavailable, or if a new rule requires data that is unavailable, then this notification can display. The ADE process works with the Custom Rules Engine (CRE) and is available on appliances where event data is processed and stored.

A dropped accumulation does not indicate that QRadar has lost any anomaly data. The original anomaly data for QRadar is maintained, as accumulations are data sets generated from stored data, but do not impact stored data when dropped. The notification provides additional detail on the dropped accumulation interval.

Behavior

QRadar responds as normal, but ADE is unable to review that interval of anomaly data for the accumulation as the global view is not present to pass anomalies to the CRE.

Resolution

To resolve this issue, you can select one of the following options:

- Review any new anomaly rules or recent changes to your anomaly rules. An update to an anomaly rule to use a smaller data set can resolve the notification.
- Determine if the notification corresponds with SAR Sentinel notifications. If SAR Sentinel notifications are reoccurring, then the issue can be due to system performance.
- If the notification persists, you can contact customer support for assistance.

Process exceeds allowed run time

This notification is informational and occurs when a QRadar process exceeds a default time limit without completion.

Error Message

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

Explanation

Your QRadar system includes a default time limit of one hour for an individual process to complete a task. A process in QRadar is responsible for monitoring

reports and reporting processes that take longer to complete than is typically required. The notification provides the name of the process that exceeded the default timeout.

Behavior

This notification is generated and the system continues to run the process. In most cases, notification can be considered a prompt for administrators to ensure a process completes as the issue can be caused by system load.

Resolution

To resolve this issue, you can select one of the following options:

- Administrators can review the running process to determine if the task is a process that can continue to run or if the process should be stopped.
- If the notification persists, you can contact customer support.

Asset persistence queue memory full

This notification occurs when QRadar Vulnerability Manager detects the memory assigned to the asset persistence queue is completely allocated.

Error Message

```
Asset Persistence Queue Memory Full.
```

Explanation

The Asset Profile Manager includes a process called asset persistence that allows QRadar to update the profile information for assets, such as IP addresses, MAC addresses, or DNS names. As new asset data is available, asset persistence collects asset data in data sets and queues the information to be processed to update the asset model. When the persistence queue for pending asset changes is consumed, this notification is generated and asset updates are written to disk to ensure they are not lost.

Behavior

The notification is generated and pending asset updates are written to disk. The system behaves as normal.

Resolution

This notification is informational and no further action is required.

Asset persistence queue disk full

This notification occurs when QRadar Vulnerability Manager detects the spillover disk space assigned to the asset persistence queue is completely allocated.

Error Message

```
Asset Persistence Queue Disk Full.
```

Explanation

The Asset Profile Manager includes a process called asset persistence that allows QRadar to update the profile information for assets, such as IP addresses, MAC addresses, or DNS names. As new asset data is available, asset persistence collects asset data in data sets and queues the information to be processed to update the asset model. When the persistence queue and the disk queue fills with pending asset changes, this notification is generated. Asset persistence updates are blocked until disk space is available.

Behavior

The notification is generated and new asset changes are blocked from updating, but the information is not dropped. The system behaves as normal.

Resolution

To resolve this issue, you can review the following options:

- Review the size of your scans in QRadar Vulnerability Manager.

  If a disk full notification is triggered by each scan to alert you that the spillover disk space assigned to the asset persistence queue is full, then you should consider a reduction in the size of your scan. A reduction in the size of your scan can prevent the asset persistence queues from overflowing.
- If the notification persists, you can contact customer support for assistance.

Asset update resolver queue memory full

This notification occurs when QRadar Vulnerability Manager detects the memory assigned to the asset resolver queue is completely allocated.

Error Message

```
Asset Update Resolver Queue Memory Full.
```

Explanation

The Asset Profile Manager includes a process called asset resolver that allows QRadar to understand the incoming raw scan data and normalize the scan information for QRadar. As new asset data is available, the asset resolver processes the raw asset data in data sets and queues the information for the asset persistence process to update the asset model. When the resolver memory queue for processing incoming asset data is consumed, this notification is generated and asset data is written to disk to ensure it is not lost.

Behavior

The notification is generated and new asset information is written to disk. The system behaves as normal.

Resolution

This notification is informational and no further action is required.

Asset update resolver queue disk full

This notification occurs when QRadar Vulnerability Manager detects the spillover disk space assigned to the asset resolver queue is completely allocated.

Error Message

```
Asset Update Resolver Queue Disk Full.
```

Explanation

The Asset Profile Manager includes a process called asset resolver that allows QRadar to understand the incoming raw scan data and normalize the scan information for QRadar. As new asset data is available, the asset resolver processes the raw asset data in data sets and queues the information for the asset persistence process to update the asset model. When the resolver queue and the disk queue fills with pending asset changes, this notification is generated. The system continually writes the data to disk to prevent any data loss. However, if the system has exhausted disk space, then the notification indicates that the system has dropped scan data.

Behavior

The notification is generated and new asset data is written to disk, until all disk space is consumed. If disk space is unavailable, then the scan information is dropped. The system cannot handle incoming asset scan data until disk space is available.

Resolution

To resolve this issue, you can review the following options:

- Ensure that your QRadar system has free disk space. The notification can accompany SAR Sentinel notifications to notify you of potential disk space issues. You should take the proper steps to ensure that new scan data can be written to disk and not dropped.
- Review the size of your scans in QRadar Vulnerability Manager.

  If a disk full notification is triggered by each scan to alert you that the spillover disk space assigned to the asset resolver queue is full, then you should consider a reduction in the size of your scan or decreasing the scan frequency. A reduction in the scope or frequency of your scan can prevent asset resolver queues from overflowing.
- If the notification persists, you can contact customer support for assistance.

Asset change listener queue memory full

This notification occurs when QRadar Vulnerability Manager detects the memory assigned to the asset change listener queue is completely allocated.

Error Message

```
Asset Change Listener Queue Memory Full.
```

Explanation

The Asset Profile Manager includes a process called asset change listener that allows QRadar to understand asset changes and calculate statistics to update an assets CVSS score in QRadar. When the change listener memory queue for processing asset change statistics is consumed, this notification is generated and data is written to disk to ensure it is not lost.

Behavior

The notification is generated and asset change information is written to disk, until it can be processed. The system behaves as normal.

Resolution

This notification is informational and no further action is required.

Asset change listener queue disk full

This notification occurs when the QRadar Vulnerability Manager system detects the spillover disk space assigned to the asset change listener queue is completely allocated.

Error Message

```
Asset Change Listener Queue Disk Full.
```

Explanation

The Asset Profile Manager includes a process called asset change listener that allows QRadar to understand asset changes and calculate statistics to update an assets CVSS score in QRadar. When the change listener memory queue and the disk queue fills, this notification is generated. The system continually writes the data to disk to prevent any data loss to pending asset statistics. However, if the system has exhausted disk space, then the notification indicates that the system has dropped scan data.

Behavior

The notification is generated and new asset change listener data is written to disk, until disk space is consumed. If disk space is unavailable, then the change listener information is dropped. The system cannot handle incoming asset scan data until disk space is available.

Resolution

To resolve this issue, you can review the following options:

- Ensure that your QRadar system has free disk space. The notification can accompany SAR Sentinel notifications to notify you of potential disk space issues. You should take the proper steps to ensure that new scan data can be written to disk and not dropped.
- Review the size of your scans in QRadar Vulnerability Manager.

  If a disk full notification is triggered by each scan to alert you that the spillover disk space assigned to the asset change listener queue is full, then you should consider a reduction in the size of your scan or decreasing the scan frequency. A reduction in the scope or frequency of your scan can prevent asset resolver queues from overflowing.
- If the notification persists, you can contact customer support for assistance.

Asset change discarded

This notification occurs when the Asset Profile Manager determines that an asset change exceeded the change threshold and discards an asset change.

Error Message

```
Asset Changes Aborted.
```

Explanation

The Asset Profile Manager includes a process called asset persistence that allows QRadar to update the profile information for assets, such as IP addresses, MAC addresses, or DNS names. As new asset data is available, asset persistence collects asset data in data sets and queues the information to be processed to update the asset model. When a user attempts to add a new asset or edit an asset, the data is placed in temporary storage and added to the end of the change queue. If a large amount of data is in front of the user change, then the asset change can time out and the temporary storage with the change is deleted. This notification indicates that the system has discarded an asset change due to the size of pending asset updates present in the system. The notification detail outlines the asset and the information that was discarded.

Behavior

The notification is generated and a change made to an asset by a user is discarded due to the timeout threshold. The system should behave normally, however, the system is attempting to process a large number of asset changes.

Resolution

To resolve this issue, you can review the following options:

- Wait and attempt to add or edit the asset a second time.
- Stagger the start time for your vulnerability scans or reduce the size of your scans in QRadar Vulnerability Manager.

If this notification is reoccurring, then you should consider a reduction in the scan size or change in start time to prevent a user change from timing out in the asset queue.

- If the notification persists, you can contact customer support for assistance.

Information notifications

The following notifications are categorized as informational.

Maximum sensor devices monitored

This notification occurs when QRadar reaches the maximum number of log sources that the Traffic Analysis process is capable of monitoring.

Error Message

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

Explanation

The Event Collection Service (ECS) contains a process for automatically discovering and creating new log sources from events called Traffic Analysis. Your QRadar system contains a limit to the number of log sources that can be queued for automatic discovery by Traffic Analysis. If the maximum number of log sources in the queue is reached, then new log sources cannot be added to QRadar.

Behavior

The notification is generated and events for the log source are categorized as SIM Generic and labeled as Unknown Event Log.

Resolution

To resolve this issue, you can select one of the following options:

- Review any log sources classified as a SIM Generic log source on the **Log Activity** tab to determine the appliance type from the event payload.
- Ensure auto updates can download the latest DSM updates to properly identify and parse log source events for your QRadar system. The latest DSM updates can assist when automatically discovering log sources.
- Verify if the log source is officially supported by QRadar. Officially supported appliances and software versions are listed in the *DSM Configuration Guide.*
  - If your appliance is supported, you can manually create a log source for the events that Traffic Analysis could not auto discover.
  - If your appliance is not officially supported, you can create a Universal DSM to identify and categorize your events.
- Wait for the device to provide 1,000 events to QRadar.

  If QRadar cannot auto discover the log source after 1,000 events, then it is removed from the Traffic Analysis queue. When a log source is removed from

the Traffic Analysis queue, then space is available for another log source to be automatically discovered.

Store and forward schedule did not forward events

This notification occurs when a store and forward schedule completes while events are still on the disk in queue.

Error Message

```
A store and forward schedule finished while events were left on
disk. These events will be stored on the local event collector
until the next forwarding sessions begins.
```

Explanation

Store and forward is a feature of QRadar that allows you to assign schedules to Event Collector appliances in your deployment and create schedules when events are forwarded. Store and forward can provide events from an Event Collector appliance to any systems with a QRadar event processors component. If the schedule contains a short start and end time or a large number of events to forward, the Event Collector appliance might not have the time complete the transfer of the queued events. When this occurs, then the notification is generated and the events are stored until the next opportunity to forward events.

Behavior

This notification is generated and the system continues to behave normally. When the next store and forward interval occurs, the events are forwarded to the QRadar event processor.

Resolution

To resolve this issue, you can select one of the following options:

- If the QRadar Console displays a reoccurring notifications, you can increase the event forwarding rate from your Event Collector appliance or increase the time interval allowed for forwarding events.
- If the notification persists, you can contact customer support.

Infrastructure component repaired

This notification occurs when an infrastructure component responsible for host services on a managed host in the deployment is repaired by QRadar.

Error Message

```
Corrupted infrastructure component repaired.
```

Explanation

QRadar successfully started the message service, started the PostgreSQL™ database, or repaired a database on a managed host. The system notifies the user that the corrupted component on the managed host is repaired.

Behavior

This notification is generated to the managed host is returned to normal operating conditions. The notification message provides additional detail with the repaired service and IP address of the managed host.

Resolution

This notification is informational and no further action is required.

Disk storage available

This notification occurs when one or more previously unavailable storage partitions are now accessible to QRadar.

Error Message

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

Explanation

Disk Sentry is responsible for monitoring QRadar for disk and storage issues. The availability of a storage partition is determined with the touch command. If the Disk Sentry does not receive a response within a 30 second threshold, then a notification can display that the storage partition is unavailable. When the touch command succeeds on the next attempt, the Disk Sentry generates the notification to alert you that the storage partition is available.

Behavior

This notification is generated with details containing the host name and the partition that is available.

Resolution

This notification is informational and no further action is required.

QRadar Risk Manager license expired

This notification occurs when the license is expired for your QRadar Risk Manager appliance.

Error Message

```
License expired for QRadar Risk Manager.
```

Explanation

The QRadar Console manages licenses for the managed hosts in the deployment. When a license expires for QRadar Risk Manager a notification is generated.

Behavior

This notification is generated and the **Risks** tab is unusable.

Resolution

To resolve this issue, contact your sales representative to renew your QRadar Risk Manager license.

Maximum events reached

This notification occurs when an event or flow threshold for your QRadar licenses is exceeded in the past hour.

Error Message

```
Events per interval threshold was exceeded in past hour.
```

Explanation

Every QRadar appliance is sold with a license that allows you to process a specific volume of event and flow data. If you exceed your license limits, then QRadar notifies you that you exceeded the license limit. The notification provides detail that you exceeded your flow or event limit and includes the percentage of time in the last hour you were over the license limit. The purposes of this notification is to identify if you need to tune your system or if you need to expand your license limits to deal with the additional event and flow data.

Behavior

This notification is generated and the system behaves as normal. If you continue to exceed your license limit, QRadar can queue events and flows or possibly drop the data when the backup queue fills.

Resolution

To resolve this issue, you can review the following options:

- Tune the system to reduce the volume of events and flows entering the event pipeline.
- Contact your sales representative to purchase an updated license for your QRadar appliance.

Time synchronization

This notification occurs when a QFlow process in the Deployment Editor on a QRadar appliance cannot establish time synchronization.

Error Message

```
Flow collector could not establish initial time synchronization.
```

Explanation

The QFlow process in the Deployment Editor contains an advanced function for configuring a time server IP address for time synchronization. In most cases, you should not configure a value and leave the field blank, which allows the QFlow process to automatically synchronize with the QRadar Console. However, if you configure a time synchronization server and the server is unreachable, then this notification can display. The QFlow process attempts to synchronize the time every hour with the IP address time server.

Behavior

This notification is generated and the QRadar QFlow Collector behaves as normal, even though time synchronization did not complete. An attempt is made every

hour to synchronize time for the QRadar QFlow Collector and if unsuccessful, the notification is generated.

Resolution

To resolve this issue, you can review the following options:

- In the Deployment Editor. select the QFlow process, then select **Actions > Configure** and click **Advanced**. In the **Time Synchronization Server IP Address** field, clear the value and click **Save**.
- If the notification persists or you are unable to clear the time synchronization value, you can contact customer support.

Process monitor license expired or invalid

This notification occurs when the license is expired for a managed host in the deployment.

Error Message

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

Explanation

The QRadar Console manages licenses for the managed hosts in the deployment. When a license expires for a managed host, all data collection processes stop on the appliance and the notification is generated.

Behavior

This notification is generated and the appliance with the expired license cannot provide data to the QRadar Console.

Resolution

To resolve this issue, you can contact your sales representative to renew your license.

Out of memory erroneous application restarted

This notification occurs when an application or service runs out of memory and must be restarted on your QRadar system.

Error Message

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

Explanation

QRadar monitors the status of all applications and services. When QRadar detects that no additional memory can be allocated to an application or service, then QRadar can restart the application or service. Out of memory issues can be caused by software issues or user defined queries and operations that exhaust the available memory.

Behavior

The notification is generated and an application or service was restarted by the system and the appliance should behave as normal. A detailed error message is written to /var/log/qradar.log to outline the cause of the memory issue.

Resolution

To resolve this issue, you can review the following options:

- Review /var/log/qradar.log to determine the cause of the notification. A service restart might be required to halt the offending application or service and redistribute resources.
- The notification can generate during large vulnerability scans or while importing large volumes of data. For example, importing a large number of records from a log source using JDBC or the log file protocol. You can review when QRadar imports events or vulnerability data on your system and compare the notification timestamp and stagger the time intervals for data imports.
- If the notification persists, you can contact customer support.

Auto update successful download

This notification occurs when auto update downloads one or more updates to your QRadar system.

Error Message

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

Explanation

Auto Update is a feature on the **Admin** tab of QRadar to automatically download software updates. The notification informs you that auto update downloaded software updates, such as QRadar updates, DSMs, scanners, or protocols that can be installed.

Behavior

The notification is generated and the system behaves as normal. The notification provides a link to review the downloaded updates.

Resolution

This notification is informational and typically no further action is required. You can view the updates downloaded to QRadar with the link provided in the notification to determine if any downloaded content requires installation.

Auto update deploy required

This notification occurs when an auto update is downloaded for QRadar that requires a Deploy Changes to complete the installation process.

Error Message

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

Explanation

Auto Update is a feature on the **Admin** tab of QRadar to automatically download and install software updates, DSMs, scanners, or protocols. If an RPM update downloaded using auto updates requires a Deploy Changes to complete the installations, then system generates a notification.

Behavior

The notification is generated and the system behaves as normal. If a DSM, scanner, or protocol update requires a Deploy Changes, then updates might not apply parsing, scanner, or protocol changes until the deploy process completes.

Resolution

To resolve this issue, you can review the following options:

- In the **Admin** tab, click **Deploy Changes** to resolve this notification.
- If your system does not deploy or the deploy cannot complete, you can contact customer support.

Auto update successful

This notification occurs when an auto update is completed successfully to notify you that your QRadar system is updated.

Error Message

```
Automatic updates completed successfully.
```

Explanation

Auto Update is a feature on the **Admin** tab of QRadar to automatically download and install software updates, DSMs, scanners, or protocols. When an update is successful, the system generates a notification.

Behavior

The notification is generated and the system behaves as normal.

Resolution

This notification is informational and no further action is required.

SAR Sentinel recovered

This notification occurs when the System Activity Reporter (SAR) utility detects that your QRadar system load returned to acceptable levels.

Error Message

```
SAR Sentinel: normal operation restored.
```

Explanation

The SAR Sentinel utility monitors QRadar for a broad number of functions, such as running processes, CPU usage, and hardware functions. The function of the SAR Sentinel is to monitor the system and provide notifications when the system load exceeds a set threshold or returns to normal operating conditions.

Behavior

This notification is generated and your system behaves as normal.

Resolution

This notification is informational and no further action is required.

Disk Sentry: disk usage returned to normal

This notification occurs when the Disk Sentry utility detects that the disk usage is below 90% of the overall capacity.

Error Message

```
Disk Sentry: System Disk Usage Back To Normal Levels.
```

Explanation

Disk Sentry is the process responsible for monitoring QRadar for disk and storage issues. Disk Sentry generates this notification to alert you that your QRadar system has returned to normal operating conditions, as disk space is at an acceptable level.

Behavior

This notification is generated to inform you that disk usage on your QRadar system has returned to normal. The system behaves as normal.

Resolution

This notification is informational and no further action is required.

License expired

This notification occurs when the QRadar Console detects that a license is expired.

Error Message

```
An allocated license has expired and is no longer valid.
```

Explanation

The QRadar Console manages licenses for the managed hosts in the deployment. When a license expires a notification is generated on the QRadar Console to inform administrators. When a license expires on the QRadar Console, then a new license must be applied to use the Console. When a license expires on a managed host in your deployment, host context is disabled on the managed host. When host context is disabled, the appliance with the expired license is unable to process event or flow data.

Behavior

This notification is generated and the appliance with the expired license does not operate normally. Event and flow data can stop from managed hosts with expired licenses or the QRadar Console interface can become unusable.

Resolution

To resolve this issue, you can review the following options:

- To determine the appliance with the expired license, click the **Admin** tab, click the **System and License Management** icon. A system with an expired license displays invalid statement in the License Status column.
- Contact your sales representative to renew your QRadar license.

License near expiration

This notification occurs when the QRadar Console detects that a license for an appliance in your deployment is nearing expiration.

Error Message

```
A license is nearing expiration. It will need to be replaced
soon.
```

Explanation

The QRadar Console manages licenses for the managed hosts in the deployment. A license near expiration notification is generated on the QRadar Console to inform administrators that a license is within 35 days of expiration. The notification is generated daily to ensure that administrators realize that a license is nearing expiration.

Behavior

This notification is generated to inform you that a license is nearing expiration; however, the system behaves as normal.

Resolution

This notification is informational and no further action is required. To determine the appliance with the license nearing expiration, click the **Admin** tab, then click the **System and License Management** icon. If you have questions about your license, you can contact your sales representative for more information.

License near lock

This notification occurs when the QRadar Console detects that a license change for an appliance is within the license grace period.

Error Message

```
An allocated license's grace period is almost over, and will be
locked into place soon.
```

Explanation

QRadar licenses now allow you move any unlocked licenses or apply unused event or flow licenses to other appliances in your deployment. This provides customers the ability to adjust their license requirements and increase their event or flow capabilities. When you allocate a license to a host, then a grace period for the license begins and the notification is generated. The license grace period allows an administrator 10 days to move the license or cancel a license assigned to a host before the license locks to the appliance. After the grace period expires,

the license cannot be moved. The notification then repeats daily as a reminder that you have an appliance in your network that is approaching the license lock threshold.

Behavior

This notification is generated and the system behaves as normal.

Resolution

This notification is informational and no further action is required. However, system administrators should review licenses in the deployment that are within the grace period to determine if they want to reassign a license or allow the license change to become permanent.

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.