Extreme Networks Security Troubleshooting System Notifications Guide

9034867

Published July 2015

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks/

Support

For product support, including documentation, visit: www.extremenetworks.com/documentation/

For information, contact:
Extreme Networks, Inc.
145 Rio Robles
San Jose, California 95134
USA

Table of Contents

Introduction to system notifications

Extreme Networks Security Troubleshooting System Notifications Guide provides information on how to troubleshoot and resolve system notifications that display on the Extreme Security Analytics® Console. System notifications that display on the Console can apply to any appliance or Extreme Security product in your deployment.

Unless otherwise noted, all references to Extreme Security Analytics can refer to the following products:

- Extreme SIEM
- Extreme Networks Security Log Manager
- Extreme Networks Security Network Anomaly Detection

Intended audience

Network administrators who are responsible for installing and configuring Extreme Security systems must be familiar with network security concepts and the Linux™ operating system.

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. Extreme Networks® systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. EXTREME NETWORKS 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.

Note

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. Extreme Networks Security Analytics may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of Extreme Networks Security Analytics.

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
👉	Tip	Helpful tips for using the product.
📝	Note	Important features or instructions.
⚡	Caution	Risk of personal injury, system damage, or loss of data.
⚠	Warning	Risk of severe personal injury.
New	New	This command or section is new for this release.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words enter and type	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as [Return] or [Esc]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del]
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Platform-Dependent Conventions

Unless otherwise noted, all information applies to all platforms supported by ExtremeXOS software, which are the following:

- BlackDiamond® X series switch
- BlackDiamond 8800 series switches
- Cell Site Routers (E4G-200 and E4G-400)
- Summit® family switches
- SummitStack™

When a feature or feature implementation applies to specific platforms, the specific platform is noted in the heading for the section describing that implementation in the ExtremeXOS command documentation. In many cases, although the command is available on all platforms, each platform uses specific keywords. These keywords specific to each platform are shown in the Syntax Description and discussed in the Usage Guidelines.

Terminology

When features, functionality, or operation is specific to a switch family, the family name is used. Explanations about features and operations that are the same across all product families simply refer to the product as the "switch."

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at InternalInfoDev@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks Global Technical Assistance Center using one of the following methods:

Web	www.extremenetworks.com/support
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-603-952-5000 For the Extreme Networks support phone number in your country: www.extremenetworks.com/support/contact
Email	support@extremenetworks.com To expedite your message, enter the product name or model number in the subject line.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of all involved Extreme Networks products in the network
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load and frame size at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

Related Publications

The Extreme Security product documentation listed below can be downloaded from http://documentation.extremenetworks.com.

Extreme Security Analytics Threat Protection

- *Extreme Networks Security API Reference Guide*
- *Extreme Networks Security Application Configuration Guide*
- *Extreme Networks Security Ariel Query Language Guide*
- *Extreme Networks Security DSM Configuration Guide*
- *Extreme Security DSM Configuration Guide Addendum*
- *Extreme Networks Security Hardware Guide*
- *Extreme Networks Security Installation Guide*
- *Extreme Networks Security Juniper NSM Plug-in User Guide*
- *Extreme Networks Security Log Manager Administration Guide*
- *Extreme Networks Security Log Sources User Guide*
- *Extreme Networks Security Managing Log Sources Guide*
- *Extreme Networks Security Offboard Storage Guide*
- *Extreme Security Release Notes*
- *Extreme Networks Security Risk Manager Adapter Configuration Guide*
- *Extreme Networks Security Risk Manager Getting Started Guide*
- *Extreme Networks Security Risk Manager Installation Guide*
- *Extreme Networks Security Risk Manager Migration Guide*
- *Extreme Networks Security Risk Manager User Guide*
- *Extreme Networks Security Troubleshooting System Notifications Guide*
- *Extreme Networks Security Upgrade Guide*
- *Extreme Networks Security Vulnerability Manager Release Notes*
- *Extreme Networks Security Vulnerability Manager User Guide*
- *Extreme Networks Security WinCollect User Guide*
- *Extreme Networks SIEM Administration Guide*
- *Extreme Networks SIEM Getting Started Guide*
- *Extreme Networks SIEM High Availability Guide*
- *Extreme Networks SIEM Troubleshooting Guide*
- *Extreme Networks SIEM Tuning Guide*
- *Extreme Networks SIEM Users Guide*
- *Migrating Extreme Security Log Manager to Extreme SIEM*

Extreme Security Threat Protection

- *Extreme Security Intrusion Prevention System Hardware Replacement Guide*
- *Extreme Security Threat Protection Release Notes*

1 Troubleshooting Extreme Security system notifications

Use the system notifications that are generated by Extreme Networks Security Analytics to monitor the status and health of your system. Software and hardware tools and processes continually monitor the Extreme Security appliances and deliver information, warning, and error messages to users and administrators.

Related Links

Error notifications for Extreme Security appliances on page 10

Error notifications in Extreme Networks Security Analytics products require a response by the user or the administrator.

Warning notifications for Extreme Security appliances on page 21

Extreme Networks Security Analytics system health notifications are proactive messages of actual or impending software or hardware failures.

Information notifications for Extreme Security appliance on page 43

Extreme Networks Security Analytics provides information messages about the status or result of a process or action

2 Error notifications for Extreme Security appliances

Error notifications in Extreme Networks Security Analytics products require a response by the user or the administrator.

Out of memory error

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

Explanation

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

User response

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

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

Accumulator cannot read the view definition for aggregate data

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

Explanation

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

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

User response

Contact customer support.

Automatic update error

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

Explanation

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

User response

Select one of the following options:

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

  In the Admin tab, click the Auto Update icon and select View Log.
- Verify that your console can connect to the update server.

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

CRE failed to read rules

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

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

User response

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

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

For application errors where the CRE failed to read rules, contact customer support.

Process monitor application failed to start multiple times

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

Explanation

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

User response

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

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

Process monitor must lower disk usage

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

Explanation

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

User response

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

Event pipeline dropped events

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

Explanation

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

Dropped events and flows cannot be recovered.

User response

Review the following options:

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

Event pipeline dropped connections

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

Explanation

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

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

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

- TCP syslog protocol

- TLS syslog protocol
- TCP multiline protocol

User response

Review the following options:

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

Auto update installed with errors

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

Explanation

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

User response

Select one of the following options:

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

Standby HA system failure

```
Standby HA System Failure.
```

Explanation

The status of the secondary appliance switches to **`failed`** and the system has no HA protection.

User response

Review the following resolutions:

- Restore the secondary system.

  Click the Admin tab, click System and License Management, and then click Restore System.
- Inspect the secondary HA appliance to determine whether it is powered down or experienced a hardware failure.
- Use the `ping` command to check the communication between the primary and standby system.

- Check the switch that connects the primary and secondary HA appliances.

  Verify the IPtables on the primary and secondary appliances.
- Review the `/var/log/qradar.log` file on the standby appliance to determine the cause of the failure.

Active high availability (HA) system failure

```
Active HA System Failure.
```

Explanation

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

User response

Review the following resolutions:

- Inspect the active HA appliance to determine whether it is powered down or experienced a hardware failure.
- If the active system is the HA primary, restore the active system.

  Click the Admin tab and click System and License Management. From the High Availability menu, select the Restore System option.
- Review the `/var/log/qradar.log` file on the standby appliance to determine the cause of the failure.
- Use the `ping` command to check the communication between the active and standby system.
- Check the switch that connects the active and standby HA appliances.

  Verify the IPtables on the active and standby appliances.

Failed to install high availability

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

Explanation

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

No HA protection is available until the issue is resolved.

User response

Contact customer support.

Failed to uninstall an HA appliance

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

Explanation

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

User response

Try to remove the high-availability appliance a second time.

Scanner initialization error

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

Explanation

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

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

User response

Follow these steps:

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

Filter initialization failed

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

Explanation

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

User response

Select one of the following options:

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

  All new event sources are classified as SIM Generic until they are mapped to a log source.
- If you get an automatic update error, review the automatic update log to determine whether an error occurred when a DSM or a protocol was installed.

Disk storage unavailable

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

Explanation

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

User response

Select one of the following options:

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

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

- Determine whether the notification corresponds to dropped events.

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

Insufficient disk space to export data

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

Explanation

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

User response

Select one of the following options:

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

- Configure an offboard storage device.

The accumulator dropped records

```
The accumulator was unable to aggregate all events/flows for this
interval.
```

Explanation

The system might drop an accumulation interval from a data set if there is too much data to process for the aggregate data view. Dropped accumulation intervals also occur if the system load prevents the accumulation from completing within the defined threshold.

The data set for your report, search, or chart is not displayed. No data is lost because accumulations are data sets that are generated from stored data.

User response

To help diagnose the cause, review the following details:

- 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.
- Reduce the scope of the search data.

Scan tool failure

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

Explanation

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

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

User response

Select one of the following options:

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

External scan gateway failure

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

Explanation

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

User response

Select one of the following options:

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

Disk failure

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

Explanation

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

User response

If the notification persists, contact customer support or replace parts.

Predictive disk failure

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

Explanation

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

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

User response

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

3 Warning notifications for Extreme Security appliances

Extreme Networks Security Analytics system health notifications are proactive messages of actual or impending software or hardware failures.

Unable to determine associated log source

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

Explanation

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

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

User action

Review the following options:

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

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

Backup unable to complete a request

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

Explanation

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

Disk Sentry is responsible for monitoring system disk and storage issues. Before a backup begins, Disk Sentry checks the available disk space to determine whether the backup can complete successfully. If the disk space is above the threshold limit of 90% on the partition that contains your backup data, the backup is canceled. If the free disk space is less than two times the size of the last backup, the backup is canceled. By default, backups are stored in `/store/backup`.

User response

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

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

Backup unable to execute a request

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

Explanation

A backup cannot start or cannot complete for one of the following reasons:

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

User response

Manually start a backup to determine whether the failure recurs. If multiple backups fail to start, contact customer support.

Found an unmanaged process that is causing long transaction

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

Explanation

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

User response

Select one of the following options:

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

Time synchronization failed

```
Time synchronization to primary or Console has failed.
```

Explanation

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

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

User response

Contact customer support.

Restored system health by canceling hung transactions

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

Explanation

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

User response

No action is required.

Maximum active offenses reached

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

Explanation

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

User response

Select one of the following options:

- Change low security offenses from open (active) to closed, or to closed protected.
- Tune your system to reduce the number of events that generate offenses.

  To prevent a closed offense from being removed by your data retention policy, protect the closed offense.

Maximum total offenses reached

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

Explanation

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

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

User response

Select one of the following options:

- Tune your system to reduce the number of events that generate offenses.

- Adjust the offense retention policy to an interval at which data retention can remove inactive offenses.

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

Long running reports stopped

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

Explanation

The system cancels the report that exceeded the time limit. Reports that run longer than the following default time limits are canceled.

Table 3: Default time limits by report frequency

Report frequency	Default time limits (hours)
Hourly	2
Daily	12
Manual	12
Weekly	24
Monthly	24

User required

Select one of the following options:

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

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

Long transactions for a managed process

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

Explanation

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

A managed process is forced to restart.

User response

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

Protocol source configuration incorrect

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

Explanation

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

User response

To resolve protocol configuration issues:

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

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

MPC: Process not shutdown cleanly

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

Explanation

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

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

User response

The magistrate component is capable of self-repair. If the error continues, contact customer support.

Last backup exceeded the allowed time limit

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

Explanation

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

User response

Select one of the following options:

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

Log source license limit

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

Explanation

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

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

User response

Review the following options:

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

Log source created in a disabled state

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

Explanation

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

User response

Review the following options:

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

SAR sentinel threshold crossed

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

Explanation

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

User response

Review the following options:

- In most cases, no resolution is required.

  For example, when the CPU usage over 90%, the system automatically attempts to return to normal operation.
- If this notification is recurring, increase the default value of the SAR sentinel.

  Click the Admin tab, then click Global System Notifications. Increase the notification threshold.
- For system load notifications, reduce the number of processes that run simultaneously.

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

User does not exist or is undefined

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

Explanation

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

User response

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

Disk usage warning

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

Explanation

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

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

User response

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

Events routed directly to storage

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

Explanation

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

User response

Review the following options:

- Verify the incoming event and flow rates. If the event pipeline is queuing events, expand your license to hold more data.
- Review recent changes to rules or custom properties. Rule or custom property changes might cause sudden changes to your event or flow rates. Changes might affect performance or cause the system to route events to storage.
- DSM parsing issues can cause the event data to route to storage. Verify whether the log source is officially supported.
- SAR notifications might indicate that queued events and flows are in the event pipeline.
- Tune the system to reduce the volume of events and flows that enter the event pipeline.

Custom property disabled

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

Explanation

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

User response

Select one of the following options:

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

Device backup failure

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

Explanation

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

User response

Select one of the following options:

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

Event or flow data not indexed

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

Explanation

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

User response

Select one of the following options:

- If the dropped index interval occurs with SAR sentinel notifications, the issue is likely due to system load or low disk space.

- To temporarily disable some indexes to reduce the system load, on the Admin tab, click the Index Management icon.

Threshold reached for response actions

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

Explanation

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

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

User response

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

Disk replication falling behind

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

Explanation

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

User response

Select one of the following options:

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

Expensive custom rule found

```
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 validates if an event matches a rule set and then trigger alerts, offenses, or notifications.

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

User response

Review the following options:

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

Accumulation is disabled for the anomaly detection engine

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

Explanation

Aggregate data view is disabled or unavailable or a new rule requires data that is unavailable.

A dropped accumulation does not indicate lost anomaly data. The original anomaly data is maintained because accumulations are data sets generated from stored data. The notification provides more details about the dropped accumulation interval.

The anomaly detection engine cannot review that interval of the anomaly data for the accumulation.

User response

Update anomaly rules to use a smaller data set.

If the notification is a recurring SAR sentinel error, system performance might be the cause of the issue.

Process exceeds allowed run time

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

Explanation

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

User response

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

Asset persistence queue disk full

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

Explanation

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

User response

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

Blacklist notification

```
The Asset Reconciliation Exclusion rules added new asset data to the
asset blacklists.
```

Explanation

A piece of asset data, such as an IP address, host name, or MAC address, shows behavior that is consistent with asset growth deviations.

An *asset blacklist* is a collection of asset data that is considered untrustworthy by the Asset Reconciliation Exclusion CRE rules. The rules monitor asset data for consistency and integrity. If a piece of asset data shows suspicious behavior twice or more within 2 hours, that piece of data is added to the asset blacklists. Subsequent updates that contain blacklisted asset data are not applied to the asset database.

User response

- In the notification description, click Asset Reconciliation Exclusion rules to see the rules that are used to monitor asset data.
- In the notification description, click Asset deviations by log source to view the asset deviation reports that occurred in the last 24 hours.
- If your blacklists are populating too aggressively, you can tune the Asset Reconciliation Exclusion rules that populate them.
- If you want the asset data to be added to the asset database, remove the asset data from the blacklist and add it to the corresponding asset whitelist. Adding asset data to the whitelist prevents it from inadvertently reappearing on the blacklist.
- Review the asset reconciliation documentation.

Expensive custom properties found

```
Performance degradation was detected in the event pipeline. Expensive
custom properties were found.
```

Explanation

During normal processing, custom event and custom flow properties that are marked as optimized are extracted in the pipeline during processing. The values are immediately available to the custom rules engine (CRE) and are routed directly to storage.

Improperly formed regular expression (regex) statements can cause events to be incorrectly routed directly to storage.

User response

Select one of the following options:

- Review the payload of the notification. If possible, improve the regex statements that are associated with the custom property.
- Modify the custom property definition to narrow the scope of categories that the property tries to match.
- Specify a single event name in the custom property definition to prevent unnecessary attempts to parse the event.

Raid controller misconfiguration

```
Raid Controller misconfiguration: Hardware Monitoring determined that a
virtual drive is configured incorrectly.
```

Explanation

For maximum performance, raid controllers cache and battery backup unit (BBU) must be configured to use write-back cache policy. When write-through cache policy is used, storage performance degrades and might cause system instability.

User response

Review the health of the battery backup unit. If the battery backup unit is working correctly, change the cache policy to write-back.

An error occurred when the log files were collected

```
Collecting the required support logs failed with errors. See System and
License Manager.
```

Explanation

Errors were encountered while the log files were being collected. The log file collection failed.

User response

To view information about why the collection failed, follow these steps:

1. Click System and License Manager in the notification message.
2. Expand System Support Activities Messages.
3. View additional information about why the log file collection failed.

Expensive DSM extensions were found

```
Performance degradation was detected in the event pipeline. Expensive DSM
extensions were found.
```

Explanation

A log source extension is an XML file that includes all of the regular expression patterns that are required to identify and categorize events from the event payload. Log source extensions might be referred to as *device extensions* in error logs and some system notifications.

During normal processing, log source extensions are executed in the event pipeline. The values are immediately available to the custom rules engine (CRE) and are stored on disk.

Improperly formed regular expressions (regex) can cause events to be routed directly to storage.

User response

Select one of the following options:

- Review the payload of the notification. If possible, improve the regex statements that are associated with the device extension.
- Ensure that the log source extension is applied only to the correct log sources.

  On the Admin tab, click System Configuration > Data Sources > Log Sources. Select each log source and click Edit to verify the log source details.
- If you are working with batch log sources, modify the event throttle to ensure that the events do not buffer to disk. The event throttle settings are part of the protocol configuration for the log source.

Asset growth deviations detected

```
The system detected asset profiles that exceed the normal size threshold.
```

Explanation

The system detected one or more asset profiles in the asset database that show deviating or abnormal growth. Deviating growth occurs when a single asset accumulates more IP addresses, DNS host names, NetBIOS names, or MAC addresses than the system thresholds allow. When growth deviations are detected, the system suspends all subsequent incoming updates to these asset profiles.

User response

Determine the cause of the asset growth deviations:

- Hover your mouse over the notification description to review the notification payload. The payload shows a list of the top five most frequently deviating assets. It also provides information about why the system marked each asset as a growth deviation and the number of times that the asset attempted to grow beyond the asset size threshold.
- In the notification description, click **Review a report of these assets** to see a complete report of asset growth deviations over the last 24 hours.
- Review the documentation about asset growth deviations.

Asset update resolver queue disk full

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

Explanation

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

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

User response

Review the following options:

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

Disk full for the asset change queue

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

Explanation

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

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

User response

Select one of the following options:

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

Asset change discarded

```
Asset Changes Aborted.
```

Explanation

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

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

User response

Select one of the following options:

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

Cyclic custom rule dependency chain detected

```
Found custom rules cyclic dependency chain.
```

Explanation

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

User response

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

Maximum sensor devices monitored

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

Explanation

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

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

User response

Select one of the following options:

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

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

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

Flow collector cannot establish initial time synchronization

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

Explanation

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

User response

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

License expired

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

Explanation

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

User response

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

Maximum events reached

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

Explanation

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

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

User response

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

Process monitor license expired or invalid

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

Explanation

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

User response

Contact your sales representative to renew your license.

Out of memory error and erroneous application restarted

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

Explanation

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

User response

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

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

Deployment of an automatic update

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

Explanation

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

User response

In the Admin tab, click Deploy Changes.

License expired

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

Explanation

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

User response

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

External scan of an unauthorized IP address or range

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

Explanation

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

User response

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

Infrastructure component is corrupted or did not start

```
Infrastructure component corrupted.
```

Explanation

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

User response

Contact customer support.

4 Information notifications for Extreme Security appliance

Extreme Networks Security Analytics provides information messages about the status or result of a process or action

Automatic updates successfully downloaded

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

Explanation

Software updates were automatically downloaded.

User response

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

Automatic update successful

```
Automatic updates completed successfully.
```

Explanation

Automatic software updates were successfully downloaded and installed.

User response

No action is required.

SAR sentinel operation restore

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

Explanation

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

User response

No action is required.

Disk usage returned to normal

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

Explanation

The disk sentry detected that the disk usage is below 90% of the overall capacity.

User response

No action is required.

An infrastructure component was repaired

```
Corrupted infrastructure component repaired.
```

Explanation

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

User response

No action is required.

Disk storage available

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

Explanation

The disk sentry detected that the storage partition is available

User response

No action is required.

License near expiration

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

Explanation

The system detected that a license for an appliance is within 35 days of expiration.

User response

No action is required.

License allocation grace period limit

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

Explanation

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

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

User response

No action is required.

Log files were successfully collected

```
The required support logs have been successfully collected. See System
and License Manager.
```

Explanation

The log files were successfully collected.

User response

To download the log file collection, follow these steps:

1. Click System and License Manager in the notification message.
2. Expand System Support Activities Messages.

3 Click Click here to download file.

Index