Extreme Networks SIEM Troubleshooting Guide

Release 7.1.0 (MR2)

Published July 2015
9034875

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys 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 about Extreme Networks trademarks, go to: www.extremenetworks.com/company/legal/trademarks/

Support

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

Contact

Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 95134
Tel: +1 408-579-2800
Toll-free: +1 888-257-3000

Table of Contents

1 Introduction to Extreme Security Troubleshooting

This information is intended for use with *Extreme Networks Security Analytics* and provides diagnostic and resolution information for common system notifications and errors that can be displayed when using Extreme SIEM.

Intended audience

System administrators responsible for troubleshooting must have administrative access to Extreme Security Analytics and your network devices and firewalls. The system administrator must have knowledge of your corporate network and networking technologies.

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 comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. EXTREME 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.

2 Extreme SIEM System Notifications

System notifications are displayed on the Extreme SIEM dashboard or in the notification window when unexpected system behavior occurs. You can troubleshoot the most common Extreme SIEM notifications.

Error messages can occur for a variety of reasons. After consulting this guide, if you are unable to resolve a Extreme SIEM error or system notification message, gather diagnostic information and contact Customer Support.

Performance degradation of disk storage

Each host in your Extreme SIEM deployment monitors the availability of partitions using hostcontext. Disk availability is tested every minute by opening, writing to, and deleting a file.

If this process takes longer than the default time period of five seconds, then the hostcontext process reports an error in the Extreme SIEM logs.

The error might resemble the following output:

```
Jun 24 07:22:41 127.0.0.1  [hostcontext.hostcontext] [5b3acf9a-aa8a-
437a-b059-01da87333f43/SequentialEventDispatcher]
com.q1labs.hostcontext.ds.DiskSpaceSentinel: [ERROR]
[NOT:0150062100][172.16.77.116/- -] [-/- -]The storage partition(s) /
store/backup on qradarfc (172.16.77.116) are not currently accessible.
Manual intervention may be required to restore normal operation.
```

NOTE

If your system is experiencing high loading and large volumes of data are being written, searched, purged, or copied to another system, an error might be displayed when your file system is still operational.

You must identify the frequency of the error message, by choosing one of the following options:

- If the message is displayed repeatedly, then verify the problem, see Verifying the problem on page 3.
- If the message is only displayed during peak times, then increase your partition test timeout period, see Increasing the partition test timeout period on page 3.

Verifying the problem

You can verify a partition storage problem by creating a temporary file on your Extreme SIEM Console or Managed Host.

About this task

Partition storage problems can occur on the Console or any Managed Host in your Extreme SIEM deployment.

Procedure

1 Using SSH, log in to the Extreme SIEM Console or Managed Host as the root user:

Username: **root**

Password: **<password>**

2 Type the following commands:

```
touch /store/backup/testfile
ls -la /store/backup/testfile
```

3 If either of the following messages are displayed, then go to step 4.

```
touch: cannot touch `/store/backup/testfile': Read-only file system
nfs server time out
```

4 Choose from one of the following options:

- If you are using a network file system, such as iSCSI, Fibre Channel or NFS, then contact your storage administrator to verify that the file servers are accessible and operational.
- If you are using a local file system on your Extreme SIEM appliance, you might have a file system issue or your disk might have failed. Contact Customer Support.
- If you are unable to identify the cause of your problem, contact Customer Support.

Increasing the partition test timeout period

You can modify the partition test timeout period.

About this task

The partition test timeout period must be increased to a level at which Extreme SIEM does not generate false positives, but remains operational. Do not increase the timeout period to a level that is excessive.

Procedure

1 Click the Admin tab.

2 On the navigation menu, click System Configuration.

3 Click the System Settings icon.

4 In the Partition Tester Timeout (seconds) list box, select or type 20 seconds.

5 Click Save.

Application error after protocol update

You might receive an error message when you attempt to edit a log source if you recently upgraded Extreme SIEM or updated Device Service Module (DSM), Protocol, or Vulnerability Information Services (VIS) components.

The message indicates that the web server might not have started after Extreme SIEM was updated. The web server might be storing old files in memory. To remove these files you must purge your Extreme SIEM files. See Purging Extreme SIEM files on page 4.

```
An error has occurred. Refresh your browser (press F5) and attempt
the action again. If the problem persists, please contact customer
support for assistance.
```

Purging Extreme SIEM files

You can clear Extreme SIEM files from your browser cache.

Before you begin

Ensure that you only have one instance of your web browser open, otherwise the cache cannot be cleared. If you are using Mozilla Firefox, you must clear the cache in Internet Explorer and Mozilla Firefox.

Procedure

1 Using SSH, log in to the Extreme SIEM Console as the root user:

Username: **root**

Password: **<password>**

2 Stop tomcat by typing the following command:

```
service tomcat stop
```

3 Clear your browser's cache.

4 Restart tomcat by typing the following command:

```
service tomcat start
```

5 If the problem persists then contact Customer Support.

Disk usage system notifications

The Extreme SIEM disksentinel process monitors the /root, /store, and /store/tmp partitions in your deployment to determine if these partitions have reached a pre-defined usage threshold.

Depending on the disk usage of each monitored partition, the hostcontext process might display the following system notifications:

Table 1: Disk usage notifications

Notification	Description
`Disk Sentry: Disk Usage exceeded warning threshold.`	This message is displayed when disk usage reaches 90% on any of the monitored partitions. The operation of your Extreme SIEM system is not affected when the partition reaches this threshold. Continue to monitor your partition levels. For more information, see Verifying disk usage levels on page 6.
`Disk Sentry: Disk Usage exceeded max threshold.`	This message is displayed when disk usage reaches 95% on any of the monitored partitions. Extreme SIEM data collection (ecs) and search processes (ariel) are shut down in order to protect the file system from reaching 100%. For more information, see on page 6.
`Disk sentry: System disk usage back to normal levels.`	After disk usage has reached a threshold of 95%, disk usage must return to 92% before Extreme SIEM automatically restarts data collection and search processes. To lower the disk usage threshold, manually remove data from the affected partitions. For more information, see Resolving disk usage issues on page 6.

NOTE

The /var/log partition can continue to operate when disk usage reaches 100%. However, log data will not be written to disk and this can affect Extreme SIEM startup processes and components. For more information, see Resolving disk usage issues on page 6.

Verifying disk usage levels

You can verify the usage levels of the partitions on your Extreme SIEM Console or Managed Host.

Procedure

1 Using SSH, log in to the Extreme SIEM Console or Managed Host as the root user:

Username: `root`

Password: **<password>**

2 Type the following command:

```
df -h
```

3 Review the partitions to check their disk usage levels.

If any of the monitored partitions have reached 95%, review the recommended solutions to this problem. For more information, see Resolving disk usage issues on page 6.

Resolving disk usage issues

You can resolve disk usage issues.

About this task

Disk usage warnings might occur on the Console or any Managed Host in your Extreme SIEM deployment. Your file system partitions can reach 95% when your data retention period settings are too high or you have insufficient storage available for the rate at which Extreme SIEM receives data.

NOTE

If you reconfigure your retention bucket storage settings, this will have a global effect on the storage across your entire Extreme SIEM deployment.

Procedure

1 In the /root file system, identify and remove older debug or patch files.

2 Reduce disk usage on the /store file system. Choose one of the following options:

- Remove the oldest data from the /store/ariel/events file system. If you are not familiar with UNIX commands or performing large scale data removal, then contact Customer Support.
- Reduce your data retention period by adjusting the default retention bucket storage settings. For more information, see the *Extreme SIEM Administration Guide*.
- Identify which log sources you can retain for shorter periods and use the retention buckets feature to manage this. For more information, see the *Extreme SIEM Administration Guide.*
- Consider an offboard storage solution. For example, iSCSI or Fibre Channel. For more information, see the *Extreme Security Analytics Offboard Storage Guide*.

3 In the /store/tmp file system, if you identify that a large Log Activity or Network Activity export has occurred, contact Customer Support for assistance with removing data from your system.

4 If the /var/log file system reaches 100% capacity, Extreme SIEM will not shut down. However, there might be other issues which will cause your log files to grow faster than expected. Contact Customer Support.

User configurations that impact event processing

Depending on your Extreme SIEM configuration, the event processing pipeline can be severely impacted.

Administrators must review the following information to ensure that event processing is not affected:

DSM Extensions and Optimized Custom Properties

Extreme SIEM performance can be affected by the configuration of your DSM extensions and optimized custom properties.

DSM Extensions

Using a DSM extension, you can create custom parsing methods, based on regex pattern matching, to extract event data from unsupported log sources. As DSM extensions are used by the Extreme SIEM parsing engine, the regex patterns used in your extension can impact event processing. For more information see, Identifying DSM and optimized custom property issues on page 8.

Optimized Custom Properties

You can use regular expression patterns to extract data from events as they are parsed. If regular expressions are written inefficiently, they can degrade the performance of the Extreme SIEM parsing engine and impact event processing.

Issues with DSMs or optimized custom properties can cause the following system notification to be displayed. For more information see, Identifying DSM and optimized custom property issues on page 8.

```
Performance degradation has been detected in the event pipeline.
Events were routed directly to storage.
```

Identifying DSM and optimized custom property issues

You can identify issues with any recently installed a DSM extension or newly enabled custom property.

Procedure

1 Disable any recently installed DSM extension or custom property.

2 If Extreme SIEM stops dropping events, but you continue to receive a system notification, then review your DSM extensions or custom properties to identify inefficient regex patterns.

3 If Extreme SIEM continues dropping events, there might be multiple DSM extensions or custom properties that are causing a problem with the event pipepline.

4 If the issue persists after you have disabled all DSM extensions and custom properties, contact Customer Support.

Non-optimized custom properties

Custom properties that are regularly used by Extreme SIEM rules, or for searching and filtering, must be marked as Optimized.

In cases where they are not optimized, the data is parsed by the UI engine (tomcat). This can affect search speeds and UI load times. For more information on optimizing custom properties, see the *Extreme Networks SIEM Users Guide*.

If you experience performance impact, contact Customer Support.

Rule tests that impact performance

The rules and tests that you configure in Extreme SIEM can affect performance.

Regular expressions tests

Rules that test if the event payload contains or matches a regular expression, perform a search of the entire payload and have a greater impact on Extreme SIEM performance.

Before you add a payload test to a rule, include filters in the rule that reduce the number of events. For example, to search for a specific message that is only contained in the Active Directory Logs, first apply the following filters to the rule:

- Log source type
- Log source group or specific log source filter
- Optional. Source IP

Host with port open tests

The host with port open test can impact Extreme SIEM performance because it compares passive and active ports with the events and flows received by Extreme SIEM. Before using this test, perform a bidirectional check to ensure that the host responds to the communication request.

Global views

Creating a saved search that is grouped by multiple fields can generate a global view with a large number of unique entries. As the volume of data increases, disk usage, processing times, and search performance can be impacted.

To prevent this, only aggregate searches on fields that are necessary. You could also reduce the impact on the accumulator by adding a filter to your search criteria.

Incomplete report results

Depending on how you configure and run Extreme SIEM reports, the results you generate might appear to be different from what you expect. It is common to assume that a report is not displaying all the data that you require.

Data accumulation for a search only starts when the search is added to a scheduled report. Therefore, a report that is created on Wednesday, but is scheduled to run weekly on a Monday, will not display a full week of data.

NOTE

The next time the report runs it will contain a full week of data.

Using the Network Activity or Log Activity tabs, run the search again and make a comparison with the generated report.

If the results are different, see Resolving missing report data on page 9.

Resolving missing report data

Extreme SIEM 7.0 MR5 implements the resolutions for report data issues.

Procedure

1. If Extreme SIEM detects that your data is incomplete, a notification message is displayed on the Reports tab.
2. To ensure you capture all the report data, you have the option to run your report against raw data during the initial time period. For more information on how to configure this option, see the *Extreme SIEM Users Guide*.

Limited disk space to perform backup

A system notification occurs if there is limited disk space on the destination file system. Extreme SIEM cannot complete a backup if there is insufficient disk space.

You might receive the following system notification:

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

System notifications about limited disk space are displayed when the partition used for the backup is at greater than 90% capacity. This can be caused by the volume of data and your backup retention period settings. For more information, see the *Extreme SIEM Administration Guide*.

Verifying the backup partition disk levels

You can verify the disk levels of your Extreme SIEM backup partition.

About this task

Disk usage warnings can occur on the Console or any Managed Host in your Extreme SIEM deployment. To check disk usage levels, review the monitored partitions on your Extreme SIEM Console or Managed Hosts.

Procedure

1 Using SSH, log in to the Extreme SIEM Console or Managed Host as the root user:
Username: `root`
Password: **<password>**

2 Type the following command:

```
df -PTh /store/backup
```

3 Review the backup partition to check the disk utilization levels.

If the backup partition is at greater than 90% capacity, see Resolving backup partition usage on page 11.

Resolving backup partition usage

You can reduce your backup disk usage levels.

About this task

Configuring the retention bucket storage settings has a global impact on the storage across your Extreme SIEM deployment.

Procedure

1 Reduce disk utilization on the /store file system. Choose from the following options:
   - Remove the oldest data from the /store/ariel/events/ file system. If you are not familiar with Unix file systems or performing large scale data removal, then contact Customer Support.
   - Reduce your data retention period by adjusting the default retention bucket storage settings. For more information, see the *Extreme SIEM Administration Guide*.
   - Identify which log sources that you can retain for shorter periods and use the retention buckets feature to manage this. For more information, see the *Extreme SIEM Administration Guide.*
   - Consider an offboard storage solution. For example, iSCSI or Fibre Channel. For more information, see the *Extreme Security Analytics Offboard Storage Guide*.

2 If your Extreme SIEM backup partition is mounted on an NFS share, the retention period for the backup can be too high. By default, the backup retention period is two days. For more information on configuring backup retention periods, see the *Extreme SIEM Administration Guide*.