

IBM Security QRadar SIEM  
Version 7.1.0 (MR2)

*Troubleshooting Guide*



**Note:** Before using this information and the product that it supports, read the information in [Notices and Trademarks](#) on [page 13](#).

# CONTENTS

---

## ABOUT THIS GUIDE

Intended Audience . . . . .	1
Conventions . . . . .	1
Technical Documentation . . . . .	1
Contacting Customer Support . . . . .	1
Statement of good security practices . . . . .	2

---

## 1 QRADAR SIEM SYSTEM NOTIFICATIONS

Performance degradation of disk storage . . . . .	3
Verifying the problem . . . . .	4
Increasing the partition test timeout period . . . . .	4
Application error after protocol update . . . . .	5
Purging QRadar SIEM files . . . . .	5
Disk usage system notifications . . . . .	6
Verifying disk usage levels . . . . .	6
Resolving disk usage issues . . . . .	7
User configurations that impact event processing . . . . .	7
DSM Extensions and Optimized Custom Properties . . . . .	8
Identifying DSM and optimized custom property issues . . . . .	8
Non-optimized custom properties . . . . .	8
Rule tests that impact performance . . . . .	9
Global views . . . . .	9
Incomplete report results . . . . .	9
Resolving missing report data . . . . .	10
Limited disk space to perform backup . . . . .	10
Verifying the backup partition disk levels . . . . .	10
Resolving backup partition usage . . . . .	10

---

## A NOTICES AND TRADEMARKS

Notices . . . . .	13
Trademarks . . . . .	15



# ABOUT THIS GUIDE

The *IBM Security QRadar SIEM Troubleshooting Guide* provides diagnostic and resolution information for common system notifications and errors that can be displayed when using QRadar SIEM.

---

**Intended Audience** This guide is intended for all QRadar SIEM users responsible for investigating and managing network security. This guide assumes that you have QRadar SIEM access and a knowledge of your corporate network and networking technologies.

---

**Conventions** The following conventions are used throughout this guide:

- ▶ Indicates that the procedure contains a single instruction.

**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).  
(<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).  
(<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

## QRADAR SIEM SYSTEM NOTIFICATIONS

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

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

---

### Performance degradation of disk storage

Each host in your QRadar 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 QRadar 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](#).
- If the message is only displayed during peak times, then increase your partition test timeout period, see [Increasing the partition test timeout period](#).

**Verifying the problem** You can verify a partition storage problem by creating a temporary file on your QRadar SIEM Console or Managed Host.

**About this task**

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

**Procedure**

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

Username: `root`

Password: `<password>`

**Step 2** Type the following commands:

```
touch /store/backup/testfile
```

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

**Step 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
```

**Step 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 QRadar 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 QRadar SIEM does not generate false positives, but remains operational. Do not increase the timeout period to a level that is excessive.

**Procedure**

**Step 1** Click the **Admin** tab.

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

**Step 3** Click the **System Settings** icon.

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

**Step 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 QRadar 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 QRadar SIEM was updated. The web server might be storing old files in memory. To remove these files you must purge your QRadar SIEM files. See [Purging QRadar SIEM files](#).

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 QRadar SIEM files**

You can clear QRadar 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**

**Step 1** Using SSH, log in to the QRadar SIEM Console as the root user:

Username: `root`

Password: `<password>`

**Step 2** Stop tomcat by typing the following command:

```
service tomcat stop
```

**Step 3** Clear your browser's cache.

**Step 4** Restart tomcat by typing the following command:

```
service tomcat start
```

**Step 5** If the problem persists then contact Customer Support.

**Disk usage system notifications**

The QRadar 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 3-1** 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 QRadar SIEM system is not affected when the partition reaches this threshold. Continue to monitor your partition levels. For more information, see <a href="#">Verifying disk usage levels</a> .
Disk Sentry: Disk Usage exceeded max threshold.	This message is displayed when disk usage reaches 95% on any of the monitored partitions. QRadar 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 <a href="#">Resolving disk usage issues</a> .
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 QRadar 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 <a href="#">Resolving disk usage issues</a> .

**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 QRadar SIEM startup processes and components. For more information, see [Resolving disk usage issues](#).

**Verifying disk usage levels**

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

**Procedure**

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

Username: `root`

Password: `<password>`

**Step 2** Type the following command:

`df -h`

**Step 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](#).

**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 QRadar 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 QRadar SIEM receives data.

**Note:** If you reconfigure your retention bucket storage settings, this will have a global effect on the storage across your entire QRadar 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 *IBM Security QRadar 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 *IBM Security QRadar SIEM Administration Guide*.
  - Consider an offboard storage solution. For example, iSCSI or Fibre Channel. For more information, see the *IBM Security QRadar 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, QRadar 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 QRadar 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](#)
- [Non-optimized custom properties](#)
- [Rule tests that impact performance](#)
- [Global views](#)

### DSM Extensions and Optimized Custom Properties

QRadar 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 QRadar 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](#).

#### 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 QRadar 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](#).

```
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 QRadar 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 QRadar SIEM continues dropping events, there might be multiple DSM extensions or custom properties that are causing a problem with the event pipeline.
- 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 QRadar 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 *IBM Security QRadar SIEM Users Guide*.

If you experience performance impact, contact Customer Support.

**Rule tests that impact performance**

The rules and tests that you configure in QRadar 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 QRadar 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 QRadar SIEM performance because it compares passive and active ports with the events and flows received by QRadar 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 QRadar 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](#).

**Resolving missing report data**

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

**Procedure**

- 1 If QRadar 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 *IBM Security QRadar SIEM Users Guide*.

**Limited disk space to perform backup**

A system notification occurs if there is limited disk space on the destination file system. QRadar 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 *IBM Security QRadar SIEM Administration Guide*.

**Verifying the backup partition disk levels**

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

**About this task**

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

**Procedure**

- Step 1** Using SSH, log in to the QRadar SIEM Console or Managed Host as the root user:  
Username: `root`  
Password: `<password>`
- Step 2** Type the following command:  
`df -PTh /store/backup`
- Step 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](#).

**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 QRadar 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 *IBM Security QRadar 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 *IBM Security QRadar SIEM Administration Guide*.
  - Consider an offboard storage solution. For example, iSCSI or Fibre Channel. For more information, see the *IBM Security QRadar Offboard Storage Guide*.
- 2 If your QRadar 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 *IBM Security QRadar SIEM Administration Guide*.





# A

## NOTICES AND TRADEMARKS

What's in this appendix:

- [Notices](#)
- [Trademarks](#)

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](http://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 [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

