IBM Security QRadar
Version 7.2.1

Payload Indexing for Quick Filtering

Note: Before using this information and the product that it supports, read the information in Notices and Trademarks on page 5.

CONTENTS

1 QRADAR PAYLOAD INDEXING

A NOTICES AND TRADEMARKS

1 QRADAR PAYLOAD INDEXING

You can use the IBM® Security QRadar® Quick Filter to search event and flow payloads. This option is accessible from the **Log Activity** and **Network Activity** tabs.

You can enable a payload index on a quick filter property to optimize a search that uses a quick filter. This is helpful for searches that take extended time.

Enabling payload indexing increases disk storage requirements and could decrease system performance. Only enable payload indexing if the event and flow processors in your deployment are at no greater than:

- 70% disk utilization.
- 70% of the maximum Events Per Second (EPS) or Flows Per Interface (FPI) rating.

Unless otherwise noted, all references to QRadar refer to IBM Security QRadar SIEM, IBM Security QRadar Log Manager, and IBM Security QRadar Network Anomaly Detection. References to flows do not apply to QRadar Log Manager.

Enabling payload indexing

Enable payload indexing on the Quick Filter property to optimize event and flow search times.

Procedure

Step 1 Log in to QRadar.

Step 2 Click the **Admin** tab.

Step 3 On the navigation menu, click **System Configuration**.

Step 4 Click the **Index Management** icon.

Step 5 In the **Quick Search** field, type **Quick Filter**.

Step 6 Select the **Quick Filter** property you want to index.

You can identify the event and flow Quick Filter properties using the value in the **Database** column.

Step 7 On the toolbar, click **Enable Index**.

A green dot indicates that the payload index is enabled.

Step 8 Click **Save**.

Step 9 Click **OK**.

Results

The selected Quick Filter properties are indexed. If a list includes event or flow properties, indexed property names are appended with the following text: `[Indexed]`.

Configuring the payload index retention period

You can configure the time period to store Quick Filter payload indexes.

About this task

By default, payload indexes are retained for one week. The minimum retention period is one day and the maximum is two years.

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 Database Settings pane, select a retention time period from the **Payload Index Retention** list box.

Step 5 Click **Save**.

Step 6 Close the System Settings window.

Step 7 On the **Admin** tab menu, click **Deploy Changes**.

Troubleshoot payload indexing

When you enable payload indexing, a warning about performance degradation might be displayed.

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 is for planning purposes only. The information herein is subject to change before the products described become available.

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