IBM Security QRadar
Version 7.1.0 (MR1)

Adaptive Log Exporter Service Update Technical Note

Note: Before using this information and the product that it supports, read the information in Notices and Trademarks on page 7

CONTENTS

1 ADAPTIVE LOG EXPORTER SERVICE UPDATE

This service update addresses the startup and shutdown issues in the Adaptive Log Exporter service. To resolve this issue, you must update your Adaptive Log Exporter service with a new Q1WindowsAgentSvc file.

When multiple Adaptive Log Exporter processes are started on a Windows host, your Adaptive Log Exporter installations can experience problems.

About the Adaptive Log Exporter service update

This update is automatically included with new installations of the Adaptive Log Exporter. For existing installations, update the Adaptive Log Exporter service on Windows hosts that have limited resources or hosts that are extremely active. You do not need to reconfigure any settings when you update your Adaptive Log Exporter service.

Identifying the issue

A issue occurs when duplicate processes maintain socket connections to QRadar without forwarding event data.

About this task

The Adaptive Log Exporter duplicates can occur on the Windows host when the available resources are consumed or the CPU usage on Windows host reaches 100% for an extended period.

Before you begin

Review your Adaptive Log Exporter installations on Windows hosts with high event processing rates and Windows hosts that display high CPU usage. These hosts can display duplicate Adaptive Log Exporter processes, which require the service update.

Procedure

Step 1 Log in to the Windows host using the Adaptive Log Exporter.

Step 2 Press the Ctrl + Shift + Esc keys to start the Windows Task Manager.

Step 3 Click the **Processes** tab.

Step 4 On the processes pane, select the **Show processes from all users** check box.

Step 5 The following Adaptive Log Exporter processes are displayed:

- Q1WindowsAgent.exe *32
- Q1WindowsAgentSvc.exe *32

Step 6 If the **Processes** tab displays multiple versions of these files, update your Adaptive Log Exporter service.

Updating your Adaptive Log Exporter service

The Adaptive Log Exporter service is responsible for reading and forwarding events to IBM Security QRadar SIEM. You must have administrative privileges on the Windows host running the Adaptive Log Exporter to install or stop the updated Adaptive Log Exporter service.

Stopping the Adaptive Log Exporter service

Before you can install the Adaptive Log Exporter service update, you need to stop any Adaptive Log Exporter services that are running.

Procedure

Step 1 Log in to the Windows host using the Adaptive Log Exporter.

Step 2 Close all instances of the Adaptive Log Exporter.

Step 3 Press the Ctrl + Shift + Esc keys to start the Windows Task Manager.

Step 4 Click the **Services** tab.

Step 5 In the **Name** column, on the **Services** pane, right-click the **AdaptiveLogExporterService** and select **Stop Service**.

Installing the updated service

You can install the Adaptive Log Exporter service.

Procedure

Step 1 Download the Q1WindowsAgentSvc.exe file from the Qmmunity website to your Windows host.

https://qmmunity.q1labs.com/node/546

Step 2 Copy the Q1WindowsAgentSvc.exe file to the following directory:

`<Adaptive Log Exporter>/bin/`

Where **`<Adaptive Log Exporter>`** is the installation directory for the Adaptive Log Exporter on the Windows host.

Note: You can view the exact path for the Q1WindowsAgentSvc.exe file using the **Processes** tab. Right-click Q1WindowsAgentSvc.exe and select **Properties**. The path is displayed in the **Location** field.

Step 3 Replace the Q1WindowsAgentSvc.exe when prompted.

Step 4 Press the Ctrl + Shift + Esc keys to start the Windows Task Manager.

Step 5 Click the **Services** tab.

Step 6 In the Name column on the **Services** tab, right-click on the **AdaptiveLogExporterService**, and click **Start Service**.

A NOTICES AND TRADEMARKS

What's in this appendix:

This section describes some important notices, trademarks, and compliance information.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the

capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices sho8wn are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at *http:\\www.ibm.com/legal/copytrade.shtml*.

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

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.