TECHNICAL NOTE

ADAPTIVE LOG EXPORTER SERVICE UPDATE

MAY 2012

Adaptive Log Exporter installations can have issues where multiple Adaptive Log Exporter processes are started on a Windows host. When multiple Adaptive Log Exporter processes are started on a Windows host, your Adaptive Log Exporter installations can experience problems. The most common problem occurs when duplicate processes maintain socket connections to QRadar without forwarding event data. 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.

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.

This section includes the following topics:

CAUTION

This update is automatically included with new installations of the Adaptive Log Exporter. For existing installations, we recommend you 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

We recommend you 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.

To identify the issue:

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.

The Processes pane is displayed.

Step 4 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, we recommend that you 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 QRadar. You must have administrative privileges on the Windows host running the Adaptive Log Exporter to install or stop the updated Adaptive Log Exporter service.

This section includes the following topics:

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.

To stop the Adaptive Log Exporter service:

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.

The Services pane is displayed.

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

You are now ready to install the Adaptive Log Exporter service update.

Installing the Updated Service

To install the Adaptive Log Exporter service:

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 on Q1WindowsAgentSvc.exe and click **Properties**. The path is displayed in the **Location** field.

Step 3 Replace the Q1WindowsAgentSvc.exe when prompted.

The updated service is installed. You need to start the Adaptive Log Exporter service to complete this installation.

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

Step 5 Click the **Services** tab.

The Services pane is displayed.

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

The Adaptive Log Exporter service update is complete.

Q1 Labs Inc.
890 Winter Street
Suite 230
Waltham, MA 02451 USA