Flow Collector NetFlow Update Patch for Cisco Secure Network Analytics (formerly Stealthwatch) v7.4.1

This document provides the patch description and installation procedure for the Cisco Secure Network Analytics Flow Collector NetFlow appliance v7.4.1. Make sure to review the **Before You Begin** section before you get started.

> ⓘ There are no prerequisites for this patch.

Patch Description

This patch, patch-fcnf-ROLLUP003-7.4.1-v2-02.swu, includes the following fixes:

Defect	Description
SWD-16633/ SWD-17957	Fixed an issue where the Flow Collector 5210 engine had a Capture performance degradation issue.
SWD-17799	Added support to the Flow Collector engine for IPFIX AVC/ART fields supported in version 9.
SWD-17849	Fixed an issue where the Flow Collector 5000 series had sizing/scaling issues when it was installed in a Data Store deployment.
SWD-17888	Fixed an issue which allows any valid MTU range that the operating system kernel permits.
SWD-18072/ SWD-17991	Fixed an issue where the Flow Collector engine showed UDP InErrors during the average traffic.
SWD-18124	Fixed an issue where webproxy traffic processing stopped after the Flow Collector reload.
SWD-18145/ SWONE-23440	Added **enable_user_sessions_from_flow** to Advanced Settings and set it to "0" to stop generating user sessions.
SWONE-22896	Fixed an issue where the Flow Collector engine **ingest_enable_compression** setting was changed to the default setting during software updates.

Defect	Description
SWONE-22943/ SWONE-23817	Fixed an issue where the reported serial number was changed to use the full hardware serial number.

ⓘ Previous fixes included in this patch are described in **Previous Fixes**.

Before You Begin

⚠ Make sure you have enough available space on the Manager for all appliance SWU files that you upload to Update Manager. Also, confirm you have enough available space on each individual appliance.

Check the Available Disk Space

Use these instructions to confirm you have enough available disk space:

1. Log in to the Appliance Admin interface.
2. Click **Home**.
3. Locate the **Disk Usage** section.
4. Review the **Available (byte)** column and confirm that you have the required disk space available on the **/lancope/var/** partition.
    - **Requirement:** On each managed appliance, you need at least four times the size of the individual software update file (SWU) available. On the Manager, you need at least four times the size of all appliance SWU files that you upload to Update Manager.
    - **Managed Appliances:** For example, if the Flow Collector SWU file is 6 GB, you need at least 24 GB available on the Flow Collector (/lancope/var) partition (1 SWU file x 6 GB x 4 = 24 GB available).
    - **Manager:** For example, if you upload four SWU files to the Manager that are each 6 GB, you need at least 96 GB available on the /lancope/var partition (4 SWU files x 6 GB x 4 = 96 GB available).

Download and Installation

Download

To download the patch update file, complete the following steps:

1. Log in to Cisco Software Central, https://software.cisco.com.
2. In the Download and Upgrade area, choose **Access downloads**.
3. Type **Secure Network Analytics** in the **Select a Product** search box.

4. Choose the appliance model from the drop-down list, then press **Enter**.
5. Under Select a Software Type, choose **Secure Network Analytics Patches**.
6. Choose **7.4.1** from the Latest Releases area to locate the patch.
7. Download the patch update file, patch-fcnf-ROLLUP003-7.4.1-v2-02.swu, and save it to your preferred location.

Installation

To install the patch update file, complete the following steps:

1. Log in to the Manager.
2. Click the ⚙ (**Global Settings**) icon, then choose **Central Management**.
3. Click **Update Manager**.
4. On the Update Manager page, click **Upload**, and then open the saved patch update file, patch-fcnf-ROLLUP003-7.4.1-v2-02.swu.
5. Choose the **Actions** menu for the appliance, then choose **Install Update**.

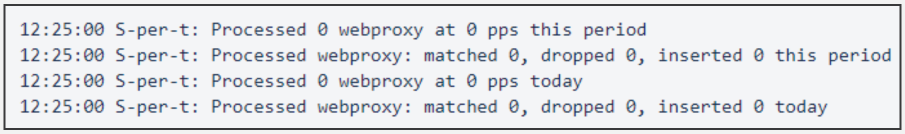
> ⓘ The patch stops the Flow Collector engine, then restarts the appliance.

Previous Fixes

The following items are previous defect fixes included in this patch:

Defect	Description
SWD-17309	Fixed an issue where th SGT, SGT ID, and Username field were missing from active user sessions after rebooting the Flow Collector.
SWD-17405	Reduced the wait time for restarting the svc_fc_engine after a shutdown.
SWD-17628	Fixed an issue where the group index in the baseline file being equal to the number of host groups generated a SIGABRT problem.
SWD-17663	Fixed an issue where false values were displaying in the flow_stats table.
SWD-17668	Fixed an issue where under Interfaces, Top Application Traffic did not show any data.

Defect	Description
SWD-17711/ SWD-17718	Increased the advanced setting configuration value for insane_average_packet_size from 16 to 32 bits.
SWD-17734	Fixed an issue where there were duplicate Avro files.
SWD-17745	Fixed an issue where UEFI mode enabled on VMware prevented users from accessing the Appliance Setup Tool (AST).
SWD-17762/ SWD-17743	Enhanced the Flow Collector engine to ensure it's processing all telemetry (including NVM) in all interfaces (eth0 and eth1).
SWD-17788/SWD-17791	Enhanced the Flow Collector engine to ensure that it would accept the templates 272 and 273, which are exported by AnyConnect version 4.10.0407 (or newer).
SWD-17832	Fixed an issue where the system-stats folder was missing from v7.4.1 diag packs.

SWD-17873	Reviewed an issue where the Flow Collector engine didn't restart automatically after installing a patch, which caused webproxy traffic processing to stop.
	Additional Instructions: If you notice the Flow Collector has stopped collecting proxy data for flow searches, check the `/lancope/var/sw/today/logs/sw.log`:
	
	`12:25:00 S-per-t: Processed 0 webproxy at 0 pps this period`
	`12:25:00 S-per-t: Processed webproxy: matched 0, dropped 0, inserted 0 this period`
	`12:25:00 S-per-t: Processed 0 webproxy at 0 pps today`
	`12:25:00 S-per-t: Processed webproxy: matched 0, dropped 0, inserted 0 today`
	If the numbers are all zero when webproxy data is expected, then restart the Flow Collector engine:
	1. Log in to the appliance console as root.
	2. Type the following command: `systemctl restart engine`
	3. Press Enter.

SWD-17973	Reviewed an issue where the appliance was unable to install patches due to a lack of disk space.

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
  - To open a case by web: http://www.cisco.com/c/en/us/support/index.html
  - To open a case by email: tac@cisco.com
  - For phone support: 1-800-553-2447 (U.S.)
  - For worldwide support numbers: www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html

Copyright Information