Data Store Update Patch for Cisco Secure Network Analytics (formerly Stealthwatch) v7.4.2

This document provides the patch description and installation procedure for the Cisco Secure Network Analytics Data Store appliance v7.4.2.

> Make sure you read **Before You Begin** section before you get started.

Patch Name and Size

- **Name:** We changed the patch name so that it starts with "update" instead of "patch." The name for this rollup is **update-dnode-ROLLUP20240317-7.4.2-v2-01.swu**.
- **Size:** We increased the size of the patch SWU files. The files may take a longer time to download. Also, follow the instructions in the **Check the Available Disk Space** section to confirm you have enough available disk space with the new file sizes.

Patch Description

This patch, update-dnode-ROLLUP20240317-7.4.2-v2-01.swu, includes fixes for the following issues:

CDETS	Description
CSCwj00351	Syslog shows Null Pointer Exception on the non-Manager appliances when revocation check is enabled
CSCwi51110	SNMP crashes due to segfault error
CSCwj03302	IP addresses/interface configuration changes are incorrect in Central Management

> 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).

The following table lists the new patch file sizes:

Appliance	File Size
Manager	5.7 GB
Flow Collector NetFlow	2.6 GB
Flow Collector sFlow	2.4 GB
Flow Collector Database	1.9 GB
Flow Sensor	2.7 GB
UDP Director	1.7 GB
Data Store	1.8 GB

Download and Installation

Download

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

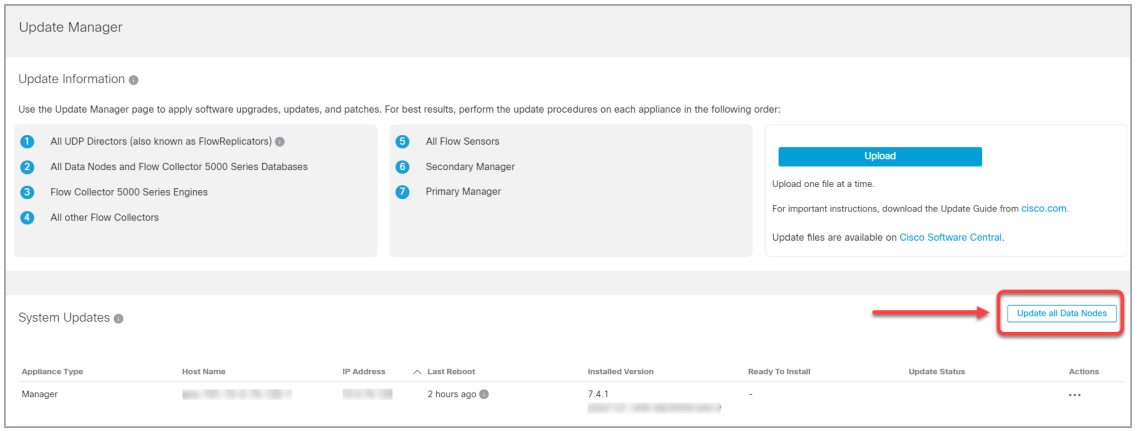
1. Log in to Cisco Software Central, https://software.cisco.com.
2. In the Download and Upgrade area, choose **Access downloads**.
3. Type **Secure Network Analytics** in the **Select a Product** search box.
4. Choose the appliance model from the drop-down list, then press **Enter**.
5. Under Select a Software Type, choose **Secure Network Analytics Patches**.
6. Choose **7.4.2** from the Latest Releases area to locate the patch.
7. Download the patch update file, update-dnode-ROLLUP20240317-7.4.2-v2-01.swu, and save it to your preferred location.

Installation

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

> Although you can update each Data Node individually, we recommend using the **Update all Data Nodes** button to update your Data Nodes at the same time.

1. Log in to the Manager.
2. From the main menu, choose **Configure** > **GLOBAL Central Management**.
3. Click the **Update Manager** tab.
4. On the Update Manager page, click **Upload**, and then open the saved patch update file, update-dnode-ROLLUP20240317-7.4.2-v2-01.swu.
5. Click **Update all Data Nodes** button.



Monitor Progress: To monitor the progress of the database services update on each Data Node, go to the **Data Store** > **Database Update Status** tab. Also, refresh each page to see the most recent status.

The patch stops the Vertica Database, then restarts the appliance.

Previous Fixes

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

Rollup 20240201	
CDETS	**Description**
CSCwi86232	Unable to upgrade the appliances after replacing the appliances identity certificates

Rollup 20240110	
CDETS	**Description**
CSCwi55301	Failover: the appliance status remains **Config Channel Down** on the promoted primary Manager
CSCwh56984	Manager does not support special characters in the users canonical name for LDAP authentication

Rollup 20231122	
CDETS	**Description**
CSCwi00243	Authentication issues caused by nginx reloading before client.crt is updated in the trust stores
CSCwh96737	Appliances that have not completed First Time Setup have upgrade errors

Rollup 20231018	
CDETS	**Description**
CSCwf39480	The **/etc/default/ssh** file goes back to its default configuration after rebooting the appliance.

Rollup 20230928	
CDETS	**Description**
CSCwf89883	The regenerating process for unexpired self-signed appliance identity certificates was simplified. For instructions, refer to the SSL/TLS Certificates Guide for Managed Appliances.

Rollup 20230823	
CDETS	**Description**
CSCwf79482	Fixed an issue where the CLI password was not restored when the Central Management and the appliance backup files were restored.
CSCwh17234	Fixed an issue where, after the Manager restarted, it failed to download Threat Feed updates.
CSCwh35228	Added SubjectKeyIdentifier and AuthorityKeyIdentifier extensions and clientAuth and serverAuth EKUs to Secure Network Analytics self-signed certificates.

Rollup 20230727	
CDETS	**Description**
CSCwe25794	Fixed an issue where Retention Management wasn't working properly withCisco Security Analytics and Logging (On Premises) enabled.
CSCwf80644	Fixed an issue where Manager was unable to handle more than 40 certificates in the Trust Store.

Rollup 20230727	
CDETS	**Description**
CSCwh08506	Fixed an issue where **/lancope/info/patch** wasn't containing the latest installed patch information for the v7.4.2 ROLLUP patches.

Rollup 001	
CDETS	**Description**
CSCwh57247	Added files to the Data Node diagnostic packs.

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: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Copyright Information