ThreatConnect® Upgrade Guide: Containerized Deployment

Software Version 7.6

Technical Guide

July 2, 2024

10033-04 EN Rev. B

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | F: 703.229.4489
www.ThreatConnect.com

Table of Contents

Important: This guide describes how to upgrade ThreatConnect on a ThreatConnect instance that is running in a containerized solution using Docker®. To upgrade ThreatConnect and keep it running directly on an OS, see *ThreatConnect Upgrade Guide: Operating System Deployment*. Note that the containerization deployment was tested on AlmaLinux OS™ and is the preferred deployment method for all production and non-production systems starting with ThreatConnect version 7.5.

Overview

This guide describes how to upgrade ThreatConnect on a ThreatConnect instance that has been deployed to a containerized environment. As of ThreatConnect version 7.5, you will no longer be required to install Java®, Python®, OpenSearch®, and Redis® during the ThreatConnect upgrade process. Instead, these software, along with ThreatConnect, are now packaged together in a containerized solution using Docker. The only thing that is not included in the Docker environment is the database, which will not be touched during the upgrade process.

Upgrading ThreatConnect

Follow all steps outlined in the following subsections to upgrade ThreatConnect.

Step 1: Stop and Remove Containers

Run the following command to stop and remove the service containers:

```
docker-compose rm -fs tc-mon tc-app tc-job
```

Step 2: Update TC_VERSION in the .env File

Restore the `.env` file and update the `TC_VERSION` variable's value to the latest ThreatConnect version (replace the `<version>` placeholder value with the ThreatConnect version number):

```
TC_VERSION=v<version>
```

For example, to upgrade to ThreatConnect 7.6.0, update the value of `TC_VERSION` to `v7.6.0` (i.e., `TC_VERSION=v7.6.0`).

Step 3: Start ThreatConnect

Start each of the following services in the order outlined in the accompanying steps. After starting each service, run `docker-compose logs --tail=10 --follow` to verify that the service started successfully before moving on to the next. Once a service is started, press **Ctrl-C**.

1. Start **tc-mon**:

   ```
   docker-compose up -d nginx redis tc-mon
   ```

2. Start **tc-app**:

   ```
   docker-compose up -d nginx tc-app
   ```

3. Start **tc-job**:

   ```
   docker-compose up -d tc-job
   ```

Step 4: Re-Create the OpenSearch Index on ThreatConnect

Important: If upgrading **from ThreatConnect 7.6.0 to ThreatConnect 7.6.1 or newer**, you do not need to re-create the OpenSearch index during the upgrade process if you did so when you upgraded to ThreatConnect 7.6.0. If upgrading **from ThreatConnect 7.5.2 or earlier to ThreatConnect 7.6.1 or newer**, you must re-create the OpenSearch index during the upgrade process.

1. Log into ThreatConnect with a System Administrator account.
2. Hover over **Settings** on the top navigation bar and select **System Settings**.
3. Click **CREATE SEARCH INDEX** at the top right of the **Settings** tab.
4. On the **Setup** tab of the **Search Index Configuration** window, select the **Perform search indexing on database source** and **Load file contents into search index** checkboxes, and then click **INITIALIZE**.

   Note: The **Perform search indexing on database source** checkbox determines whether to index objects that exist in the ThreatConnect database, and the **Load file contents into search index** checkbox determines whether to index objects that exist in document storage.

5. (Optional) To view the health and status of the OpenSearch nodes, index, and cluster, select the **Health** tab.

   Warning: Only *advanced users* should access the **Repair** and **Wipe** tabs, as the utilities on these tabs will delete existing data.

6. The indexing status will be logged in the log file specified for ThreatConnect. Review the log on the **Logs** tab of the **System Settings** screen.