ThreatConnect® Upgrade Guide

Software Version 7.0.1

Technical Guide

February 8, 2023

10021-10 EN Rev. A

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

Overview

This guide provides instructions for upgrading to the latest version of ThreatConnect. Please read all steps in their entirety before proceeding with the upgrade.

Important: These instructions assume that the application has been installed to the directory **/opt/threatconnect**. If the application has been installed to a different directory, please adjust the commands to reflect the location of the install directory.

Pre-Upgrade Steps

Upgrade OpenSearch 1.2.3 to 1.3.2

1. **Stop OpenSearch®.** Run either of the following commands to stop the OpenSearch service, depending on the user's environment:

   ```
   service opensearch stop
   ```

   ```
   systemctl stop opensearch
   ```

2. **Upgrade to OpenSearch 1.3.2.** Follow the steps from the beginning of the "OpenSearch Installation" section of *ThreatConnect Installation Guide_Linux Operating System* through installation of the plugin (in the "Plugin Installation and Starting OpenSearch" subsection).

3. **Migrate data.** Use one of the following two options to migrate existing data from OpenSearch 1.2.3:

   - The preferred method is to copy the data over via the following command, effectively backing up the data:

     ```
     $ mkdir /opt/opensearch-1.3.2
     $ cp -r /opt/opensearch-1.2.3/data /opt/opensearch-1.3.2
     ```

   - Update the path.data property in the /etc/opensearch/opensearch.yml file:

     ```
     path.data: /opt/opensearch-1.3.2/data
     ```

Next, change ownership of the Elasticsearch data folder to the OpenSearch user that was created in the "Downloading and Installing OpenSearch 1.3.2" section of *ThreatConnect Installation Guide_Linux Operating System*:

```
$ chown -R opensearch:opensearch /opt/opensearch-1.3.2
```

4. **Start OpenSearch**.

```
service opensearch start
```

Install Java 11

Java® 11 (OpenJDK or Oracle® version 11) is required for the latest version of ThreatConnect to function properly.

1. Back up the **cacerts** file under the current Java installation. Note that this procedure will vary between OpenJDK and Oracle installations.
2. Run the following command to install the Java **.rpm** file that is currently downloaded:

```
yum localinstall <downloaded-java-rpm-file>.rpm
```

3. Run the following command and select the Java 11 option (typically option **2**, but this option may vary depending on the version of Java that is currently installed). Press the **Enter** key to save:

```
sudo alternatives --config java #
```

4. Note the location of the Java 11 installation. Edit **bashrc** for the **threatconnect** user account, and update the existing location for **JAVA_HOME** to the new location for the Java 11 installation.

```
export JAVA_HOME= <location>
```

Important: These instructions use the delete method to remove the current installation of Java and then install the OpenJDK version of Java 11. Testing has not been performed for an upgrade of Java from 8 to 11.

Install Redis 6.2.6

1. Navigate to **/usr/local/bin**, which is the default install path for Redis®.
2. From command line interface (CLI), run the following command to use the Redis prompt:

```
./redis-cli
```

3. From the Redis prompt, run the following command to stop Redis:

```
Enter SHUTDOWN SAVE
```

4. Type **quit**.
5. From the Redis prompt, run the following command to back up Redis files to **/tmp/redis5**:

```
cp -P /usr/local/bin/redis-* /tmp/redis5
```

6. From the CLI, run the following command to search for the **dump.rdb** file:

```
find / -iname dump.rdb
```

7. Delete the **dump.rdb** file within the Redis directory, which is typically located at **/var/lib/redis**.
8. Download the source code:

```
wget http://download.redis.io/releases/redis-6.2.6.tar.gz
```

9. Run the following command within the folder containing the **redis-6.2.6.tar.gz** file:

```
tar -xvzf redis-6.2.6.tar.gz
```

10. Navigate to the location of the un-tarred Redis installation:

```
cd redis-6.2.6
```

11. Run the following command to copy Redis to **/usr/local/bin**:

```
cp redis-* /usr/local/bin
```

> **Note**: The default location for the Redis installation is **/usr/local/bin**. If a different location is to be used, adjust the file path accordingly in the command.

12. Select **y** to overwrite the files that are being prompted.
13. Run the following command to start the Redis service:

```
service redis_6379 start
```

14. Navigate to **/usr/local/bin** (or the location where the Redis installation is located), and execute **./redis-cli**.
15. Type **info**, and then scroll to the top of the information displayed and verify that the Redis version displayed is **6.2.6**.
16. Type **quit** to complete the installation of Redis.

Configure Open File Limits

Standalone 3 Server ThreatConnect Server Instance

The following changes will need to be performed on the ThreatConnect server:

1. Add the following lines at the end of the **/etc/security/limits.conf** file:

```
threatconnect - nofile 150000
tc-job - nofile 100000
redis - nofile 100000
```

2. Add the following line at the end of the **/etc/sysctl.conf** file:

```
fs.file-max = 150000
```

All-in-One ThreatConnect Server

For an All-in-One server instance running ThreatConnect, the database server, and the OpenSearch server, the following changes need to be performed on the All-in-One ThreatConnect server:

1. Add the following lines at the end of the **/etc/security/limits.conf** file:

```
threatconnect - nofile 150000
tc-job - nofile 100000
redis - nofile 100000
```

2. Add the following line at the end of the **/etc/sysctl.conf** file:

```
fs.file-max = 150000
```

Create Database Backups

Before upgrading to the latest version of ThreatConnect, it is recommended that a backup of the database be performed.

MySQL

To perform a backup on the MySQL® server, run the following command:

```
mysqldump -u threatconnect user -p <database-name> > /<save-location>/TC_pre700.sql
```

Note: If a different MySQL socket is configured, execute the preceding command while specifying that particular socket.

PostgreSQL

To perform a backup on the PostgreSQL® server, run the following command:

```
cd /tmp
sudo -u postgres pg_dumpall -p 5432 > TC_pre700.sql
```

Upgrade Steps

1. Stop the ThreatConnect service from running by using either of the following commands:

```
service threatconnect stop
```

```
systemctl stop threatconnect
```

2. Run the following command to back up the **threatconnect.xml** file, which is typically located at **/opt/threatconnect/config**:

```
cp /opt/threatconnect/config/threatconnect.xml
/opt/threatconnect/config/threatconnect.xml.bak
```

> **Note**: If an installation location other than **/opt/threatconnect/config** is set up within the organization's ThreatConnect installation, then this file will be located within the **/config/** folder for the organization.

3. Run the following command to copy the new **version.txt** file, which is typically located at **/opt/threatconnect/config**:

```
cp /tmp/threatconnect/config/version.txt /opt/threatconnect/config/version.txt
```

> **Note**: If an installation location other than **/opt/threatconnect/config** is set up within the organization's ThreatConnect installation, then this file will be located within the **/config/** folder for the organization.

4. Download and extract all upgrade files to a directory that is separate from the one used for the existing ThreatConnect installation.

> **Note**: A link will be supplied ahead of time for the latest ThreatConnect installer **.zip** file.

5. Rename the existing **app** directory in the current ThreatConnect installation, and then replace it with the **app** directory from the downloaded **.zip** file. The proper way to do this is to create a recursive copy of the new **app** folder and place it in the current installation directory, as demonstrated in the following example:

```
cp -R /tmp/threatconnect/app /opt/threatconnect
```

Important: Change the origin and destination directories according to the organization's current configuration, as the preceding command is just an example.

6. Confirm that the **threatconnect** user has the appropriate permissions for the newly copied **app** folder. Permission changes can be accomplished by running the following command:

```
chown -R threatconnect:threatconnect /opt/threatconnect/app
```

7. Run the following commands to install dependencies for the ThreatConnect reporting feature:

```
yum install fontconfig libXrender libXext -y
curl -L https://dl.google.com/linux/direct/google-chrome-
stable_current_x86_64.rpm -o google-chrome.rpm && \
yum install ./google-chrome.rpm -y && \
rm -f google-chrome.rpm
echo "export CHROME_BIN=/usr/bin/google-chrome" >> /home/threatconnect/.bashrc
```

8. Run the following command to apply secure permissions for App integrations:

```
# get rid of old group permissions
chgrp -R threatconnect /opt/threatconnect/exchange/

# get rid of old groups
groupdel tc-job-read
groupdel tc-job-write

# correct octal permissions
find /opt/threatconnect/exchange/ -type f -exec chmod 644 -- {} +
find /opt/threatconnect/exchange/ -type d -exec chmod 755 -- {} +

# set exiting ACLs
setfacl -Rm u:tc-job:rx /opt/threatconnect/exchange/programs/
setfacl -Rm u:tc-job:rwx /opt/threatconnect/exchange/jobs/

# set new default ACLs
setfacl -Rdm u:tc-job:rx /opt/threatconnect/exchange/programs/
setfacl -Rdm u:tc-job:rwx /opt/threatconnect/exchange/jobs/
```

9. Run the following command to change to the **threatconnect** user account within the organization:

```
su - threatconnect
```

10. Navigate to the ThreatConnect installation folder that contains the **app** folder, which is typically **/opt/threatconnect/app**.

11. Execute the **setup.sh** script as the **threatconnect** user account.

12. Select option **6** to apply the upgrade.

> **Note**: The option number listed in this step does change at times with ThreatConnect releases.

13. After selecting option **6**, the ThreatConnect installer will prompt you for super user credentials. You must provide a super user account that can execute Database Definition Language (DDL) SQL statements such as CREATE TABLE and ALTER TABLE, as well as grant privileges on the ThreatConnect database. After entering the super user credentials, the ThreatConnect installer will upgrade the ThreatConnect database to the latest schema.

> **Warning**: Before completing this section, verify that the ThreatConnect database schema has been upgraded to 6.6.2.

14. Once the upgrade has been applied, select option **0** to exit the **setup.sh** script.

> **Warning**: Running **setup.sh** as the root user may inadvertently break permissions to some of the necessary configuration files.

> **Important**: If you are using Java version 11.0.11 or above, you will need to modify the **threatconnect.xml** file afterwards and make the following changes to each **"jdbc"** database connection entry:

a. Search for "**jdbc**" in the **threatconnect.xml** file within your ThreatConnect installation folder/configuration.

b. In the two **jdbc** entries, add the following string to each jdbc property, at the end of each string:

```
&amp;useSSL=false
```

c. Save the changes, and quit your file editor. Then proceed with the remaining steps in this section.

15. Start the ThreatConnect service using either of the following commands, depending on your environment:

```
service threatconnect start
```

```
systemctl start threatconnect
```

ThreatConnect should now be upgraded to the latest version.