ThreatConnect® Upgrade Guide

Software Version 6.3

September 13, 2021

10021-02 EN Rev. A

ThreatConnect, Inc.

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

P: 1.800.965.2708 | F: 1.703.229.4489

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.

NOTE: 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

Install Elasticsearch 7.7.1

1. Download the Elasticsearch® 7.7.1 rpm and ingest-attachment rpm files.
2. Run either of the following commands to stop the Elasticsearch service, depending on the user's environment:

```
service elasticsearch stop –
```

```
systemctl stop elasticsearch
```

3. Run the following command to install Elasticsearch 7.7.1:

```
rpm -Uvh elasticsearch-7.7.1-x86_64.rpm
```

4. Follow the prompts to ensure the Elasticsearch installation completes.
5. Run the following commands to reinstall the new **ingest-attachment.rpm** file:

```
cd /usr/share/elasticsearch/bin/
./elasticsearch-plugin remove ingest-attachment
./elasticsearch-plugin install file:/<path-to-ingest-file>.zip
```

6. Add the following line to the **elasticsearch.yml** file, which can be found in **/etc/elasticsearch/**:

```
discovery.type: single-node
```

7. Run the following command to start the Elasticsearch service:

```
systemctl start elasticsearch
```

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>
```

NOTE: 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 5.0.9

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/redis4**:

```
cp -P /usr/local/bin/redis-* /tmp/redis4
```

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 Redis 5.0.9.
9. Run the following command within the folder containing the **redis-5.0.9.tar.gz** file:

```
tar -xvzf redis-5.0.9.tar.gz
```

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

```
cd redis-5.0.9
```

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

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

NOTE:** /usr/local/bin **is the default location for the Redis installation. 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 **5.0.9**.
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 Elasticsearch 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
```

Update Database Schemas

MySQL

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

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

```
mysqldump -u threatconnect user -p <database-name> > /<save-
location>/TC_pre620.sql
```

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

MySQL requires particular schema upgrades, depending on the current version of ThreatConnect. These files are located within an organization's ThreatConnect folder (**/app/scripts/mysql/upgrade/...script.sql**).

At times, multiple scripts will need to be ingested incrementally into the MySQL server environment to ensure that the schemas are upgraded properly for a user's environment. A ThreatConnect Deployment Engineer can help with this process to ensure that the proper SQL scripts are ingested in the correct order. The following example demonstrates the proper syntax for executing script ingestions into the MySQL environment:

NOTE: There are several .sql scripts that need to be ingested to fully upgrade the schema for the latest version of ThreatConnect. Please verify the current version of ThreatConnect beforehand, as the SQL schema will need to be sequentially upgraded from the current version to the latest version.

```
mysql -u username -p <database-name> <username>
/opt/threatconnect/app/scripts/mysql/upgrade/ThreatConnect-<version>.sql
```

NOTE: It is recommended that MySQL script upgrades be performed with a MySQL user account that has SUPERUSER permissions . If the user account setup for ThreatConnect does not have SUPERUSER permissions, use the MySQL root account.

PostgreSQL

PostgreSQL® requires particular schema upgrades, depending on the current version of ThreatConnect. These files are located within an organization's ThreatConnect folder (**/app/scripts/postgres/upgrade/...script.sql**).

NOTE: At times, multiple scripts will need to be ingested incrementally into the PostgreSQL server environment to ensure that the schemas are properly upgraded for a user's environment. A ThreatConnect Deployment Engineer can help with this process to ensure that the proper SQL scripts are ingested in the correct order. To contact a ThreatConnect Deployment Engineer, please email support@threatconnect.com.

NOTE: Please reference the following example, which demonstrates the proper syntax for executing script ingestions into the PostgreSQL environment.

```
su - postgres
psql -U tcuser -d <database-name> <
/opt/threatconnect/app/scripts/postgres/ThreatConnect-<version>.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 commands 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. 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.

4. 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
```

   NOTE: Please change the origin and destination directories according to the organization's current configuration as the preceding command is just an example.

5. 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/
```

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

```
su  threatconnect
```

7. Navigate to the ThreatConnect installation folder that contains the **app** folder, which is typically **/opt/threatconnect/app**.
8. Execute the **setup.sh** script as the **threatconnect** user account.
9. Select option **6** to apply the upgrade.

   NOTE: The option number listed in Step 8 does change at times with ThreatConnect releases.

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

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

11. Start the ThreatConnect service using either of the following commands, depending on the user's environment:

```
service threatconnect start
```

```
systemctl start threatconnect
```

12. ThreatConnect should now be upgraded to the latest version.