ThreatConnect™

ThreatConnect® Environment Server

Installation Guide

Software Version 2.0.1

October 11, 2019

30012-06 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

SYSTEM REQUIREMENTS

In order to install an On Premise Instance of the ThreatConnect Environment Server, the requirements in the following sections must be met.

Hardware

The ThreatConnect Environment Server platform requires a server, virtual or physical, that meets the following minimum specifications:

- 4 CPU/vCPU Cores (2 GHz)
- 4 GB of memory
- 10 GB of storage

As the number or frequency of jobs increases, the need to increase system resources will likely occur. The listing in Table 1 highlights typical TC Exchange™ apps and their specific system-resource needs.

Table 1

App Name	Frequency	CPU Used	Memory Used
ArcSight™ EMS Extract	Daily	1.44	75
Tanium™ Extract v2.0	Daily	< 1	< 50
QRadar® Extract v2.0	Daily	<1	< 50
Palo Alto PAN-OS® Block List	Daily	.10	2.5

Software

The ThreatConnect Environment Server and its supporting packages require the following software environment in order to run properly:

- **Operating System**: Red Hat® Linux® variant—either Red Hat Enterprise Linux® (RHEL) or CentOS™ 6 or 7
  - This guide assumes that the user for the installation of ThreatConnect is named **threatconnect**.

- **Java® Development Kit (JDK)**: Access to a local installation of Java 8 (JDK version 1.8)
- **Python®**: Installation of Python 3.6.x for Linux

SMTP Server

TC Exchange requires an available Simple Mail Transfer Protocol (SMTP) server to send email alerts and to correspond with users. This server must be routable from the server running the platform, and if SMTP authorization is required, the ThreatConnect Environment Server will need access to a username and password in order to generate these emails.

Preparing the Environment

Java JDK

The system needs access to the Java JDK as outlined in the "Software" section. In addition, the `JAVA_HOME` environment variable needs to be properly configured to point to that directory.

NOTE: Some CentOS/Red Hat versions come with a pre-installed, though unsupported, version of OpenJDK.

Linux

Users must execute the following commands to verify their current Linux `JAVA_HOME` environment variable:

```
# which java
# echo $JAVA_HOME
```

The first command should output the path to the user's Java installation. The second command should output the directory referenced by the `JAVA_HOME` environment variable. If `JAVA_HOME` does not reference the directory returned by `which java`, edit the bash profile:

```
# vi ~/.bashrc
```

Then add the following line:

```
export JAVA_HOME=<path to Java>
```

Then reload the bash profile:

```
# source ~/.bashrc
```

Enable Unlimited Java Cryptography Extension (JCE)

Set the **unlimited** policy in the **<jdk_home>/lib/security/java.securityfile** by searching for the line **#crypto.policy=unlimited** and removing the **#** character to uncomment it.

INSTALLATION

Getting Started

ThreatConnect clients can use this guide to configure and install their own Instance of the ThreatConnect Environment Server. This guide assumes a moderate level of systems-administration expertise and an operating environment that satisfies the requirements detailed previously. See *Playbook Environments* for more information about how to configure, administrate, and use Environments in ThreatConnect.

Downloading the Installer

The Environment Server installer **.zip** file is available for download from an Environment on the **Environments** tab of the **Playbooks** screen in ThreatConnect (Figure 1).

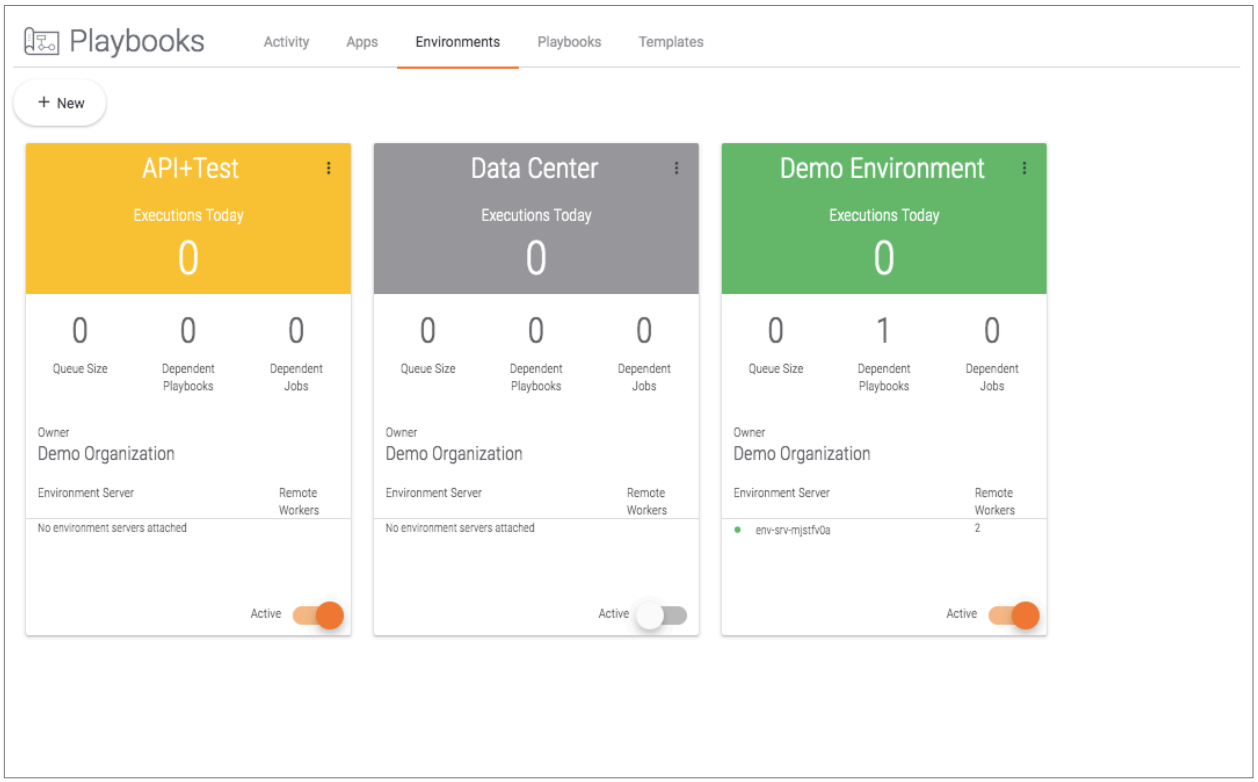

Figure 1

Click the vertical ellipsis ⋮ icon at the top right of the Environment and select the **Download** option. A window containing the download options for the Environment will appear (Figure 2).

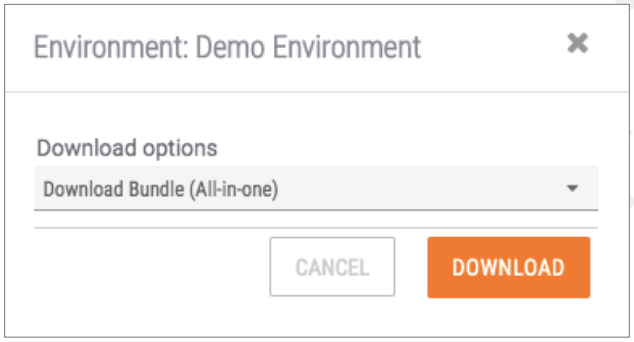

Figure 2

This window provides three options for download: **Download Bundle (All-in-one)**, **Environment Config Only**, and **Environment Server Only**. The **Download Bundle (All-in-one)** option includes both the Environment Config and the Environment Server as well as the KeyStore files required to make a secure connection to the host ThreatConnect instance. Select the **All-in-one Bundle**, and then click the **DOWNLOAD** button.

NOTE: Select** Environment Config Only **when an existing Environment Server needs to point to a new Environment. Select** Environment Server Only **when an existing Environment Server needs to be upgraded.

Opening the Installer

Unzipping the File

The ThreatConnect Environment Server **.zip** file serves as an archive of all the necessary files and folders needed to install the application. There are two ways to unzip this file:

1. Copy the **.zip** file to the desired directory on which the ThreatConnect Environment Server will be installed. By default, this directory is **/opt**, which will result in an installation directory of **/opt/threatconnect-envsvr**.
2. Unzip the file from the command-line interface with the following command: **unzip environment-server-bundle.zip**.
3. Configure permissions within the operating system to ensure that the **threatconnect** user can access the ThreatConnect Environment Server files. In the following command, the default values of **threatconnect** and **/opt/threatconnect-envsvr**, respectively, are being used:

```
# chown -R threatconnect:threatconnect /opt/threatconnect-envsvr
```

Installation Directory Structure

After the archive has been extracted, the new folder will contain the following directory structure:

```
threatconnect-envsvr/
    .tcenvsvr
    README.txt
    configure.sh
    run.sh
    shutdown.sh
    threatconnect-envsvr.init.sh
    threatconnect-envsvr.jar
```

- The **.tcenvsvr** directory contains the default keystore and broker connection settings.
- The **README.txt** file contains instructions on how to install the Environment Server.
- The **configure.sh** file is used to configure the Environment Server settings using a command-line interface.
- The **run.sh** file is used to run the Environment Server directly from the command line (not as a service).
- The **shutdown.sh** file is used to shut down the current Environment Server.
- The **threatconnect-envsvr.init.sh** file is the **init.d** service script.
- The **threatconnect-envsvr.jar** file is the file for the Environment Server only (i.e., it does not contain the configuration file).

NOTE: Users patching their ThreatConnect Environment Server Instance to a newer version should select the** Environment Server Only **option from an Environment instead of the** All-in-one Bundle**. (See the "Downloading the Installer" section for more information.) This download extracts to a** threatconnect-envsvr.jar **file. Replace the existing** .jar **file and restart to complete the upgrade.

The ThreatConnect Environment Server Setup

Creating **tc-job** User

NOTE: The information covered in this section is an optional security enhancement.

To provide additional security, it is recommended that a separate user on Linux systems be created to run TC Exchange jobs. It is also recommended that **read** and **write** groups be created to control the permissions to these files. Use the following code to perform these tasks:

```
useradd tc-job
echo "tc-job-pass123" | passwd tc-job --stdin
groupadd tc-job-read
usermod -a -G tc-job-read tc-job
chgrp -R tc-job-read /opt/threatconnect-envsvr/.tcenvsvr/exchange/programs
chmod -R 755 /opt/threatconnect-envsvr/.tcenvsvr/exchange/programs
groupadd tc-job-write
usermod -a -G tc-job-write tc-job
chgrp -R tc-job-write /opt/threatconnect-envsvr/.tcenvsvr/exchange/jobs
chmod -R 777 /opt/threatconnect-envsvr/.tcenvsvr/exchange/jobs
chmod +t /opt/threatconnect-envsvr/.tcenvsvr/exchange/jobs
```

User Privilege Configuration

Add the following lines to `/etc/pam.d/su` after the first `auth` command:

```
auth    [success=ignore default=1] pam_succeed_if.so user = tc-job
auth    sufficient pam_succeed_if.so use_uid user = threatconnect
```

Configuring **sudoers**

Create `/etc/sudoers.d/threatconnect` using the following command:

```
visudo -f /etc/sudoers.d/threatconnect
```

Then add the following lines:

```
Defaults:threatconnect !requiretty
threatconnect ALL=(tc-job) NOPASSWD: ALL
```

This configuration allows the `threatconnect` user to run the jobs as the `tc-job` user.

STARTING THE THREATCONNECT ENVIRONMENT SERVER

After completing the installation and configuration procedures, it is time to start the ThreatConnect Environment Server.

Starting as a Linux Service

The options in the previous sections allow a user to run the ThreatConnect Environment Server in a single session. This approach presents a number of limitations: The platform will need to be started manually after each reboot, or a terminal window or Secure Shell (SSH) session may have to be left open. To address this problem, this section details the file configuration to run the ThreatConnect Environment Server as a service in Linux.

Open a terminal window and browse to the app directory within the ThreatConnect Environment Server directory. Run the **run.sh** file as follows:

```
# su - threatconnect -c ./opt/threatconnect-envsvr/run.sh
```

The Service Script

Within the ThreatConnect Environment Server installation, there is a script used for running the ThreatConnect Environment Server as an initialized service:

```
# /opt/threatconnect-envsvr/threatconnect-envsvr.init.sh
```

This script must be copied into the **/etc/init.d** directory for it to be recognized as a system service. Note that users may require privileges to copy to this directory:

```
# cp /opt/threatconnect-envsvr/threatconnect-
envsvr.init.sh/etc/init.d/threatconnect-envsvr
```

Configuring Services

The service script requires proper permissions and paths to be set.

1. Specify the **TCENVSVR_HOME** variable within the script to point to the path where the ThreatConnect Environment Server installation exists. By default, this path is **/opt/threatconnect-envsvr**.
2. Specify the **USER** variable within the script to identify which user owns the files for the ThreatConnect Environment Server application. It is advisable, for security reasons, that the root user not be employed. By default, the username is assumed to be **threatconnect**.

Starting the ThreatConnect Environment Server as a Service

Once the services have been configured, the ThreatConnect Environment Server can be started as a service. To do so, enter one of the following commands while logged in as the root user:

```
# service threatconnect-envsvr start
# /etc/init.d/threatconnect-envsvr start
```

To stop the service, use either one of the following commands:

```
threatconnect-envsvr stop
```

or

```
/etc/init.d/threatconnect-envsvr stop
```

To have the ThreatConnect Environment Server start on system startup, issue the following commands after the script is configured in the **/etc/init.d** directory:

```
# chkconfig --add threatconnect-envsvr
# chkconfig threatconnect-envsvr on
```

THE FIRST LOGIN

Setting Master Key for Keychain

The Keychain feature is required for the ThreatConnect Environment Server. When prompted, enter a Master Password. The Master Password is used to encrypt sensitive values and is required on every server restart.

System Settings Checklist

Users should review their Instance settings to ensure that they are configured according to their needs. Table 2 provides a description of each system configuration value.

Table 2

System Configuration Value	Description
apiURL	This setting should point to the URL for the API at port 8443 (e.g., https://api.threatconnect.com:8443).
appDeliveryToken	This setting is the token that is used to authenticate with the App Catalog Server.
appsJavaHome	This setting holds the path to the Java binary.
appsNumberofJobExecutors	This setting is the number of Job Executors that can run concurrently. It is a factor of the number of CPUs and the available memory on the server. It should not exceed available resources.
appsPythonHome	This setting holds the path to the Python® binary.
appsSandboxUser	This setting represents the user account used to execute Jobs. It is pertinent only in Linux® installs.

appsSessionDaystoKeep	This setting is placed at 5 in Cloud. It indicates the number of days that logs will be kept in the Jobs log directory: **%threatconnect%/exchange/jobs**.
brokerHost	This setting is the remote host name of the messaging server to which the Environment Server will connect.
brokerToken	This setting is the secure key used to authenticate a connection to the remote message broker.
proxyExternal	This setting is set to true when all external connections for apps should be routed through a proxy server.
proxyHost	This setting is the proxy host to use if a proxy server is required. Acceptable values are a valid IP address or host name for a proxy accessible by the ThreatConnect instance.
proxyPassword	This setting is the proxy password to use if a proxy server requires authentication.
proxyPort	This setting is the proxy port to use if a proxy server is required. Enter a valid proxy port number.
proxyTC	This setting is set to true when all connections to the ThreatConnect host server should be routed through a proxy server.
proxyUsername	This setting is the proxy username to use if a proxy server requires authentication.
relaySystemInfoPublishSeconds	The frequency at which to notify the remote ThreatConnect instance of the status of the Environment Server.

serverName	The name of the Environment Server to display on the ThreatConnect **Environments** screen and administration page.
serverXid	This setting is a static number that uniquely identifies the given Environment Server. Its value should not be changed.