ThreatConnect® Environment Server System Requirements

Document Version 1.0

Technical Guide

October 12, 2022

10029-06 EN Rev. A

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

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

Table of Contents

Overview

Multi-environment orchestration allows ThreatConnect® users that have an Environment Server behind a firewall to use their instance to communicate with that server and run applications inside their firewall. This article provides the system requirements for installing an instance of the ThreatConnect Environment Server. See *Playbook Environments* for information about how to administrate an Environment and configure an Environment to an Environment Server.

Environment Server Architecture

Environment Servers are lightweight, deployable agents that sit behind a customer's firewall. This configuration allows for secure outbound traffic from the customer to ThreatConnect that enables ThreatConnect to interact with data and run automation based on the customer's security environment. Port 62000 and Port 443 are used for this communication, with Port 62000 utilizing a raw socket. Figure 1 illustrates where an Environment Server resides in a customer's ThreatConnect instance and how it communicates with ThreatConnect.

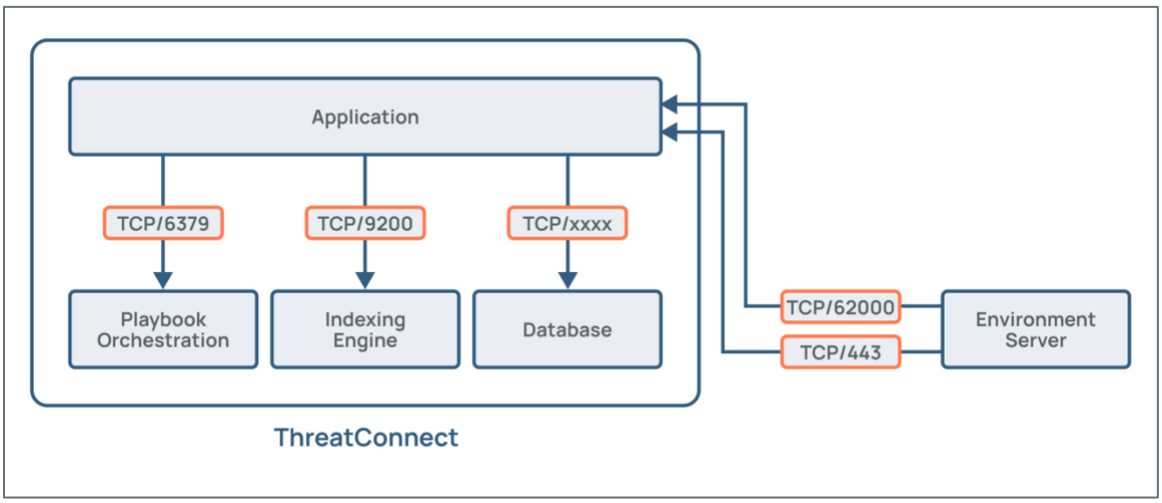

Figure 1

Environments are configured to house Environment Servers inside ThreatConnect. Doing so makes it possible to conduct health and performance monitoring to assess usage and collect statistics that are useful when administering Environment Servers.

System Requirements

In order to install an 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

Important: These requirements apply specifically to the Environment Server, not to the ThreatConnect server operating system in general. Minimum memory and storage requirements must be available to the Environment Server. Operating system requirements may vary.

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 (Cores)	Memory Used (MB)
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) 6, 7, or 8 or Community Enterprise Operating System (CentOS™) 6 or 7
- **Java® Development Kit (JDK)**: Access to a local installation of Java 11 (OpenJDK version 1.11)
- **Python®**: Installation of Python 3.6.x for Linux

End-User Web Browser

It is recommended that secure WebSockets be allowed from the ThreatConnect user's browser out to the cloud instance so that the Environment Server metrics can be monitored from the user interface. The specific traffic that needs to be allowed is wss://FQDN-of-cloud-instance:62000.

Important: Port 62000 must be allowed on the local firewall (firewalld/iptable), SELinux (if using the "Enforcing" mode), the external firewall, or the proxy server if they are used.

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.