ThreatConnect® System Requirements

Software Version 7.4

Technical Guide

January 17, 2024

10006-16 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-Premises Instance of ThreatConnect, the **minimum** requirements in the following sections must be met.

Hardware

ThreatConnect requires a server, virtual or physical, that meets the **minimum** specifications listed in Tables 1–5.

Important: If performing an installation with high-utilization requirements, further separating the application-server functions onto more than one host is recommended. Refer to the "Appendix" section for specifications. These types of installations are for advanced users only, who should consult with ThreatConnect to determine the correct sizing that will meet their needs.

Table 1

	Playbooks	Memory (GB)[1,2]	CPU Cores (2GHz)[2]	Estimated Storage (GB)[3,4]
Application Server	No	16	8	50
	Yes	48	8	150

[1] Allocated to TC; OS needs extra. Large single sources (a source with 2+ million Indicators) may require more memory for bulk processing.

[2] Plus cores and memory indicated by installed apps. (This memory is not allocated to TC in the configuration, because apps run in their own OS process and require their own memory.)

[3] High IOPS, ideally SSDs, are preferred.

[4] ThreatConnect must be installed on an ext4 or XFS partition when running Playbooks.

Table 2

	Indicators (Millions)	Memory (GB)[1]	CPU Cores (2GHz)	Estimated Storage (GB)
Database Server	0–2	12	6	20
	2–5	16	8	40
	5–10	32	12	60

[1] Allocated to the database; OS needs extra.

Table 3

	Indicators (Millions)	Memory Min (GB)	Min CPU Cores/ vCPUS (2GHz)	Estimated Storage (GB)
OpenSearch® Server	0–2	12	6	20
	2–5	16	8	40
	5–10	32	12	60

Table 4

	Highly Available Document Storage (usually network-mounted storage)
Document Storage	Equal to the desired capacity of documents stored

Table 5

	Memory Minimum (GB)	Memory Recommended (GB)
Swap Space	4	8

Note: As the number of users increases, or as the frequency or complexity of automated analysis increases, the need to increase system resources will likely occur.

Software

ThreatConnect and its supporting packages require the following software environment in order to run correctly:

- **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
- **Oracle® Java® Development Kit (JDK)**: Access to a local installation of Oracle Java 11 or OpenJDK (JDK version 11)
- **OpenSearch**: OpenSearch Server 2.6.0
- **Python®**: Installation of Python 3.6.*x* and Python 3.11.*x* is required

  > **Important**: This requirement refers to CPython. No other type of Python is permitted.

- **Python SDK**: TcEx CLI 1.*x*

  > **Important**: Starting with ThreatConnect version 7.2, a specific version of TcEx should no longer be installed. Instead, install the TcEx CLI package, which provides the necessary functionality for App Builder.

- **Redis®**: Installation of Redis 6.2.6
- Database (select from the following):
  - **MySQL®**: Installation of MySQL 8.0.*x* Community or Enterprise Edition.
  - **SAP HANA®**: Installation of SAP HANA 2.0 SPS 02
  - **PostgreSQL®**: Installation of PostgreSQL v14

  > **Important**: Install only one as the working database.

Database

ThreatConnect requires an available instance of the MySQL 8.0 database, SAP HANA 2.0 SPS 02 database, or PostgreSQL v14 database. For MySQL and PostgreSQL, a client connection requires permissions to create users, databases, and tables within this instance during the installation process. Also, while it is acceptable to run one instance of the database on the same server as ThreatConnect, clients are advised to instantiate another machine for the replicated database. It is recommended that these machines conform to the hardware specifications provided in this document.

SMTP Server

ThreatConnect 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, ThreatConnect will need access to a username and password in order to generate these emails.

Web Browsers

The ThreatConnect platform supports up to two versions behind the current stable release of the following Web browsers:

- Google Chrome™
- Mozilla Firefox®

Whitelist Requirements

Whitelist **api.threatconnect.com:443**, **broker.threatconnect.com:443**, and **feeds.threatconnect.com:443** to ensure the ThreatConnect application will be able to communicate properly with the primary ThreatConnect domain.

Network Traffic Port Requirements

The ports and protocols listed in Table 6 must be opened when deploying the ThreatConnect Application server inside a network. Appropriate firewall rules must be enabled for these ports from the machine running the Application server in order to allow connectivity to a ThreatConnect Dedicated Cloud instance.

Table 6

Network Port	Protocol	Traffic Direction	Description
443	HTTPS/TCP	Inbound/Outbound	This port connects users to the ThreatConnect Application server. The connection is bidirectional from the client to the server for API access and from the server to the client for the UI. At a minimum, this port must be opened between the Application server and the network from which users will connect.
62000	TCP	Inbound/Outbound	This port is defined within the system settings for ThreatConnect. It enables the UI to connect securely with the ThreatConnect message broker to receive real-time commands in order to provide command-and-control capabilities. Traffic is lightweight and used primarily in a request/response model to show the status of Playbook activities and Services.

Appendix

Multi-Server Specifications

Important: The minimum requirements listed in the Tables 7–9 exemplify what is needed for typical initial deployments. Large deployments or advanced-use cases will require additional resources.

Table 7

	Playbooks	Memory Min (GB)	Min CPU Cores/ vCPUs (2GHz)	Estimated Storage (GB)[1,2]
Web/API Server	N/A	8	4	50

[1] High IOPS, ideally SSDs, are preferred.

[2] ThreatConnect is to be installed on an extra ext4 or XFS partition.

Table 8

	Playbooks	Memory Min (GB)	Min CPU Cores/ vCPUs (2GHz)	Estimated Storage (GB)[1,2]
Job Server	N/A	32	8	150

[1] High IOPS, ideally SSDs, are preferred.

[2] ThreatConnect is to be installed on an extra ext4 or XFS partition.

Table 9

	Playbooks	Memory Min (GB)	Min CPU Cores/ vCPUs (2GHz)	Estimated Storage (GB)[1,2]
Messaging Server	N/A	16	8	150

[1] High IOPS, ideally SSDs, are preferred.

[2] ThreatConnect is to be installed on an extra ext4 or XFS partition.