Preparing to Install CCP

Date of publish: 2017-11-06

https://docs.cloudera.com/

Legal Notice

Contents

Cloudera Cybersecurity Platform Information Roadmap

This roadmap provides links to the information resources that are available for Cloudera Cybersecurity Package (CCP) powered by Apache Metron.

Information Type	Resources
Overview	• Apache Metron Website (Source: Apache wiki)
Installing	• Ambari Install Guide (Source: Hortonworks) • Ambari Upgrade Guide (Source: Hortonworks)
Administering	• Apache Metron Documentation (Source: Apache wiki)
Developing	• Community Resources (Source: Apache wiki)
Reference	• About Metron (Source: Apache wiki)
Resources for contributors	• How to Contribute (Source: Apache wiki)
Hortonworks Community Connection	• Hortonworks Community Connection for Metron (Source: Hortonworks)

Introduction to Cloudera Cybersecurity Platform

Cloudera Cybersecurity Platform (CCP) is a cybersecurity application framework that provides the ability to parse diverse security data feeds, enrich, triage, and store the data at scale, and detect cybersecurity anomalies.

CCP integrates a variety of open source big data technologies in order to offer a centralized tool for security monitoring and analysis. CCP provides capabilities for log aggregation, full packet capture indexing, storage, advanced behavioral analytics and data enrichment, while applying the most current threat intelligence information to security telemetry within a single platform.

Preparing to Install

Prior to installing CCP for the first time, you must ensure that you meet the minimum system requirements.

Operating System Requirements

Prior to installing CCP, ensure that you meet the operating system requirements for CCP.

CCP currently supports CentOS v7.x

Important:

If you are using CentOS 7.x, you must install the EPEL repo. Also make sure you are using python-requests version 2.6.1 or later.

Browser Requirements

The Ambari Install Wizard runs as a browser-based Web application. You must have a machine capable of running a graphical browser to use this tool.

The minimum required browser versions are:

- Windows (7, 8)
  - Firefox 18
  - Google Chrome 26
- Mac OS x (10.6 or later)
  - Firefox 18
  - Safari 5
  - Google Chrome 26
- Linux (CentOS)
  - Firefox 18
  - Google Chrome 26

On any platform, we recommend updating your browser to the latest, stable version.

Infrastructure Requirements

Prior to installing CCP, ensure that your physical nodes adhere to the specifications required by CCP.

CCP requires the following indicative specifications for your physical nodes:

Table 1: Physical Nodes

Role	Indicative Specifications
PCAP Collector Card	Ethernet—Adapter—X520—DA2 or DPDK compatible card 20 GB/Sec
PCAP Collector Server	• CPUs: 2 x 8 Core Processors • Memory: 128 GB RAM • Disk Storage: 10 x 2 TB SATA Drives • Network: 2 x 10 GB NIC
NiFi Server	• CPUs: 2 x 8 Core Processors • Memory: 128 GB RAM • Disk Storage: 10 x 2 TB SATA Drives • Network: 2 x 10 GB NIC
Apache Kafka / Storm Server	• CPUs: 2 x 8 Core Processors • Memory: 128 GB RAM • Disk Storage: 10 x 2 TB SATA Drives • Network: 2 through 10 GB NIC
Metron Master Nodes	• CPUs: 2 x 8 Core Processors • Memory: 128 GB RAM • Disk Storage: 10 x 2 TB SATA Drives • Network: 2 x 10 GB NIC
CCP Worker Nodes— Balanced	• CPUs: 2 x 8 Core Processors • Memory: 128 GB RAM • Disk Storage: 10—2 TB SATA Drives • Network: 2—10 GB NIC

Software Requirements

Prior to installing CCP, ensure that you meet the software specifications required by CCP.

The host where you will install Apache Metron services must have the following software tools installed:

- Hadoop (HDP 2.5 or HDP 2.6 recommended)

  The following are the required components for HDP 2.5.x and HDP 2.6.x:

  - Apache Hadoop
  - Apache Storm
  - Apache Kafka
  - Apache HBase
  - Apache ZooKeeper

  

  Note:

  Supervisor, Kafka Broker, and the HBase client must be installed on the host where you will install Apache Metron.
- To use the PCAP query user interface, you must perform the following:
  - Install Wireshark.

    For example, for CentOS, use the following command:

    ```
    yum -y install wireshark
    ```
  - Add a Metron user to the Wireshark group.

    For example, for CentOS, use the following command:

    ```
    -usermod -a -G wireshark metron
    ```
- MySQL
- Node.js repository installed on the Management UI host

  You can add the Node.js repository with the instructions from the Node.js Package Manager documentation.
- Installable during the Ambari installation of CCP

  The following software is required for CCP, but this software can be installed manually or during the CCP Ambari installation. Cloudera recommends that you wait to install this software until the Ambari installation of CCP. See the *CCP Release Notes* for supported version numbers.

  - Elasticsearch or Solr
  - Kibana

Memory Requirements

Prior to installing CCP, ensure that your meet the memory requirements for CCP.

For memory requirements, see the Memory Requirements provided in the *Apache Ambari Installation* guide.

Maximum Open File Descriptors

Prior to installing CCP, ensure that you meet the maximum number of open file descriptors required by CCP.

The recommended maximum number of open file descriptors is 50,000, or more. To check the current value set for the maximum number of open file descriptors, execute the following shell commands on each host:

```
ulimit -Sn
```

```
ulimit -Hn
```

If the output is not greater than 50,000, run the following command to set it to a suitable default:

```
ulimit -n 50000
```