# EclecticIQ Platform requirements

## Hardware and software requirements for system administrators

Last generated: March 08, 2017

Last generated on Mar 8, 2017

# Table of contents

# Before you start

**Summary:** Review these system requirements before proceeding to install the platform from an RPM package.

At times throughout this document, you may need to enter commands in the terminal, in the console, or in the command line. The commands we ask you to enter are prefixed by the `$` sign, and they look like this:

```
$ run this command
```

Code and configuration examples for reference look like this:

```
{
  "this" : [
  "some awesome code",
  "or nifty configuration parameters"
  ]
}
```

# About EclecticIQ Platform

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards. It enables consolidating, analyzing, integrating, and collaborating on intel from multiple sources.

| **EclecticIQ Platform** | **key features** |
|---|---|
| **Feed management** | Manage multiple cyber threat intelligence feeds from any source. |
| **Enrichment** | Enrich intel with external data sources, and refine it with de-duplication and pattern recognition. |
| **Sharing** | Identify threats together with partners as part of an information ecosystem. |
| **Collaboration** | Analyze and create intelligence in collaboration with other departments. |
| **Insights** | Generate insight with a high-fidelity normalized view into your intelligence. |
| **Integration** | Understand how cyber intelligence relates to your internal environment. |

# Hardware requirements

Hardware requirements for EclecticIQ Platform can vary depending on the target environment you plan to install the platform to. Therefore, the requirements outlined in this section are general guidelines that work in most cases, but they are not tailored to any specific situation.

## Single box

Hardware requirement guidelines for EclecticIQ Platform and related dependencies installation on one target machine.

| HW area | Minimum | Recommended | Notes |
|---|---|---|---|
| **Environment** | - | Physical machine/*rpm* install | |
| | - | VM/virtual appliance | |
| **CPUs** | 4 | 8 | Core count includes HT |
| **CPU speed** | 2.5 GHz | 2.5 GHz or faster | |
| **Memory** | 16 GB | at least 32 GB | 16 GB is unsuitable for production. A production environment should feature at least 32 GB memory. Consider expanding it to 64 GB when dealing with, for example, large data corpora ingestion or data-intensive graph visualizations. Monitor system memory usage to determine if your system may need more memory to operate smoothly. |
| **Storage** | SATA, 100 IOPS | SSD, 200 IOPS | Local attached storage is preferable to SAN or NAS; platform operations are write-intensive. Recommended IOPS range: 200-500 |
| **Drives** | 5 | 10 | 10 drives to set up 5 sets of mirrored drives (RAID 1) |
| **Drive sizes (GB)** | 10, 10, 25, 50, 200 | 20, 20, 50, 75, 300 | Each platform database should be allocated to a dedicated drive for data storage |

| **HW area** | **Minimum** | **Recommended** | **Notes** |
|---|---|---|---|
| **Drive allocation (GB)** | 10 | 20 | Root (EclecticIQ Platform + Redis) |
| | 10 | 20 | Log data storage |
| | 25 | 50 | Neo4j, graph database |
| | 50 | 75 | Elasticsearch, searching and indexing |
| | 200 | 300 | PostgreSQL, main data storage |
| **Network** | 2 network interfaces | 2 network interfaces | 1 interface for production, the other for system management |
| **Install size** | ~240 GB | ~240 GB | Full install, based on VM image size |

## Scaling out

The easiest approach to scaling out is allocating dedicated machines to the databases. In this scenario, you install each of the following components on a separate machine:

- EclecticIQ Platform
- PostgreSQL
- Redis
- Elasticsearch
- Neo4j

To optimize read-write operations and to ensure that the storage drives are fast, set up dedicated drives per partition.

# Software requirements

To correctly configure the system after installing the required products, ensure you have the following information available:

- DNS name of the host you are going to use to access the platform. Example: `platform.host`
- SSL certificate and key for the web server.
- EclecticIQ Platform login credentials.

| **EclecticIQ Platform default login credentials** | |
|---|---|
| user | `admin` |
| password | `EclecticIQ2015#` |

## Operating systems

Supported operating systems:

- **CentOS Linux 7 (1511)** `(https://lists.centos.org/pipermail/centos-announce/2015-december/021518.html)`
- **Red Hat Enterprise Linux 7** `(https://www.redhat.com/)`

**SELinux** `(http://selinuxproject.org/)` is supported as per release 0.13.

## Repositories

- Add the following repositories to the system as root:

```
$ sudo wget https://dl.fedoraproject.org/pub/epel/7/x86_64/e/epel-release-7-9.noarch.rpm && rpm -ivh epel-release-7-9.noarch.rpm

$ sudo wget https://centos7.iuscommunity.org/ius-release.rpm && rpm -ivh ius-release.rpm

$ sudo wget https://download.postgresql.org/pub/repos/yum/9.5/redhat/rhel-7-x86_64/pgdg-centos95-9.5-3.noarch.rpm && rpm -ivh pgdg-centos95-9.5-3.noarch.rpm
```

## Third-party products

Install the following software on the target system:

| Third-party product | Version | Reference |
|---|---|---|
| Oracle Java JDK | 1.8.0_71 | **Oracle Java download page** `(http://www.oracle.com/technetwork/java/javase/downloads/index.htm` |
| Nginx | 1.8 | **Nginx web site** `(http://nginx.org/en/download.html)` |
| PostgreSQL | 9.5.3 | **PostgreSQL web site** `(https://yum.postgresql.org/repopackages.php)` |
| Redis | 2.8.19-2.el7 | **Redis web site** `(http://redis.io/download)` |
| Neo4j | 2.3.1 Community | **Neo4j web site** `(http://neo4j.com/download/)` |
| unzip | - | **Install with `yum install` on CentOS/RHEL** `(https://linuxmoz.com/centos-install-unzip/)` |
| Node.js | 6.x | **Node.js for CentOS and RHEL** `(https://nodejs.org/en/download/package manager/#enterprise-linux-and-fedora)` |
| Elasticsearch | 2.3.3 | **Elastic web site** `(https://www.elastic.co/guide/en/elasticsearch/reference/2.3/setup repositories.html#_yum_dnf)` |
| delete-by-query | | **Elasticsearch plugin details** `(https://www.elastic.co/guide/en/elasticsearch/plugins/2.3/plugins delete-by-query.html)` |
| elasticdump | 2.4.2 | **Install globally as a Node js module** `(https://www.npmjs.com/package/elasticdump)` |
| Logstash | 2.0 or higher | **Logstash install instructions** `(https://www.elastic.co/guide/en/logstash/current/installing-logstash.html#_yum)` |
| Kibana | 4.5.1 | **Kibana 4.5.1 download page** `(https://www.elastic.co/downloads/past-releases/kibana-4-5-1)` |

- As per *elasticdump* version 2.4.0, we recommended installing *elasticdump* as a **global Node js module** `(https://www.npmjs.com/package/elasticdump#installing).`
- When carrying out maintenance and system administration activities on any of the required third-party platform components, first graciously shut down the platform, and then proceed with the other tasks.