EclecticIQ Intelligence at the core

Intelligence Hunting Response

EclecticIQ Endpoint Response Community Edition Deployment Guide

Version 3.5.1

May 2022

Table of contents

Getting started

The EclecticIQ Endpoint Response platform leverages the osquery tool, along with the EclecticIQ Extension to provide endpoint visibility and monitoring. It focuses on osquery-based agent management and offers the following features:

- Visibility into endpoint activities
- Query configuration management
- Live query interface
- Alerting capabilities based on security critical events

About this document

This document describes how to deploy the community edition of the EclecticIQ Endpoint Response platform.

Build and deploy the server

This section describes how to build and deploy the EclecticIQ Endpoint Response server for the community edition.

About the server

EclecticIQ Endpoint Response server is a collection of multiple micro services.

Service	***Description***
plgx-esp_nginx	Service that manages the web server for the EclecticIQ Endpoint Response server.
plgx-esp_plgx-esp-ui	Service that takes actions, such as modify properties of an endpoint.
plgx-esp_celery	Asynchronous task processor for the plgx-esp_plgx-esp micro service.
plgx-esp_plgx-esp	Service that processes requests coming from the EclecticIQ Endpoint Response clients.
plgx-esp_rsysylogf	Service that helps you stream query results and other logs from the clients to backend systems, such as Splunk, ELK, and GrayLog.
postgres:11.14	Service that manages the data store for the EclecticIQ Endpoint Response server.
rabbitmq:3.9.11-management-alpine	Service that controls messaging for the EclecticIQ Endpoint Response server.

Prerequisites

Before you deploy the EclecticIQ Endpoint Response server, ensure you have the following:

- Git client software
- Internet connectivity
- Availability of ports 5000 and 9000 (available and accessible through firewall)
- Docker (20.10 or later) and Docker Compose (1.21.1 or later)
- Node (10.3 or later) and Npm (6.1 or later)

Install Docker and Docker Compose

Before installing the EclecticIQ Endpoint Response server, download and install Docker and Docker compose.

Docker	20.10 or later	Docker is an open platform that helps you develop and ship applications. It allows you to deliver software quickly by detaching applications from the infrastructure. To get started with Docker, review the information on their website and follow instructions to install Docker on Ubuntu.
Docker Compose	1.21.1 or later	Docker Compose is a tool used to create and run multi-container Docker applications. You can define the application services using a YAML file and then create the services based on the configuration. To install Docker Compose, complete the prerequisites and then perform installation.

Install the server

After you install Docker and Docker Compose, you can install the EclecticIQ Endpoint Response server.

Complete these steps to install the EclecticIQ Endpoint Response community edition server.

1. Ensure you have root or administrative privileges.
2. Clone this repository.

```
~/Downloads$ git clone https://github.com/EclecticIQ/eiq-er-ce.git
Cloning into 'eiq-er-ce'...
```

3. Switch to the folder where the repository is cloned.

```
~/Downloads\$ cd eiq-er-ce/
```

4. Enter the certificate-generate.sh script to generate certificates for osquery.

```
~/Downloads/eiq-er-ce$ sh ./certificate-generate.sh <IP address>
Generating a 2048 bit RSA private key
.....................................................................
...................+++
```

```
.........................+++
writing new private key to 'nginx/private.key'
```

In the syntax, <IP address> is the IP address of the system which will host the EclecticIQ Endpoint Response server. This generates the certificate for osquery (used for provisioning clients) and places the certificate in the eiq-er-ce/nginx folder.

5. Edit the following configuration parameters in the .env file and save the file.

   In the syntax, replace the values in angle brackets with required values.

Parameter	***Description***
ENROLL_SECRET	Specifies the enrolment shared secret used for authentication.
POLYLOGYX_USER	Refers to the user login name for the EclecticIQ Endpoint Response server.
POLYLOGYX_PASSWORD	Indicates to the password for the EclecticIQ Endpoint Response server user.
RSYSLOG_FORWARDING	Set to true to enable forwarding of osquery and EclecticIQ Endpoint Response logs to the syslog receiver by using RSYSLOG. Alternatively, set to false.
VT_API_KEY	Represents the VirusTotal API key.
IBMxForceKey	Represents the IBMxForce key.
IBMxForcePass	Specifies the IBMxForce pass.
ALIENVAULT_OTX_KEY	Represents the AlienVault key.
PURGE_DATA_DURATION	Specifies the frequency (in number of days) for purging the data.
THREAT_INTEL_ LOOKUP_FREQUENCY	Specifies the frequency (in minutes) for fetching threat intelligence data.

Install Node.js and Npm

Complete these steps to install Node.js and Npm on Ubuntu or Debian-based system

1. If curl is not installed, run the following command to install it.

   ```
   sudo apt-get install curl
   ```

2. Enable the nodesource repo.

   ```
   curl -sL https://deb.nodesource.com/setup_10.x | sudo -E bash -
   ```

   In this command, version 10.x of node.js is being installed. To install version 11, replace setup_10.x with setup_11.x.

3. Install Node.js and NPM on the Ubuntu machine.

```
sudo apt-get install -y nodejs
```

4. Verify the installed version.

```
node -version
npm -version
```

Generate the dist folder

Complete these steps to generate the dist folder.

1. Install angular packages using npm.

```
npm install -g @angular/cli@8.3.19
```

2. Switch to the angular folder.

```
cd plgx-angular-ui
```

3. Install the project packages.

```
sudo npm install
```

4. Install gzipper to generate the compressed files.

```
npm i gzipper@3.7.0 -g
```

5. Create the dist folder using gzipper.

```
ng build --prod --stats-json && sudo gzipper --verbose ../dist
```

Bringing up the server

Complete these steps to start the EclecticIQ Endpoint Response server.

1. Switch to the extracted folder.

```
cd ../
```

2. Run the following command to build the containers.

```
docker-compose -p 'eiq-er' up -d
```

Typically, this takes approximately 10-15 minutes. The following lines appear on the screen when Docker starts.

```
Starting plgx-esp_postgres_1 ... done
Starting plgx-esp_plgx-esp_1     ... done
Attaching to plgx-esp_rabbit1_1, plgx-esp_postgres_1, plgx-esp_plgx-esp_1
.
.
.
Server is up and running```
```

3. Access the server using the latest version of Chrome or Firefox.

```
https://<server IP>
```

In the syntax, <IP address> is the IP address of the system on which the EclecticIQ Endpoint Response server is hosted. This is the IP address you specified when generating certificates and osquery flags.

5. Ignore the SSL warning, if any.
6. Log on to the server using the credentials.

Provisioning the client

The EclecticIQ Endpoint Response client that is a part of the EclecticIQ ER platform, leverages osquery, a multi-platform operating system monitoring and instrumentation framework. Here are the features the EclecticIQ Endpoint Response client offers:

- Compliance (PCI, HIPAA)
- Digital forensics
- Asset and inventory use cases
- Vulnerability management
- Host intrusion detection
- Performance and operational troubleshooting

Typically, deploying osquery and running it across your fleet can be a daunting and complicated task, because of its large configuration surface and options. To simplify the deployment of EclecticIQ Endpoint Response osquery based agent, the platform is shipped with a Client Provisioning Tool (CPT) that offers the necessary configuration and simplifies the client provisioning.

Before you begin

Before you begin installation, ensure the endpoints meet the following system requirements.

- Support 32-bit and 64-bit architecture on Windows 7 and later, Linux, and macOS. For more information on the supported operating systems, review the *EclecticIQ Endpoint Response Community Edition 3.5.1 Release Notes*.
- Do not have these installed:
    - EclecticIQ Endpoint Response version older than 1.0.35.15 on Windows
    - Osquery agent on Linux/macOS
- Do not have host-based firewalls or other security tools that might interfere with a remote installation
- Allow outbound TCP traffic on port 9000

Download the Client Provisioning Tool (CPT)

To simplify the provisioning of the endpoints, EclecticIQ Endpoint Response provides the Client Provisioning Tool (CPT).

Complete these steps to download the latest client install files.

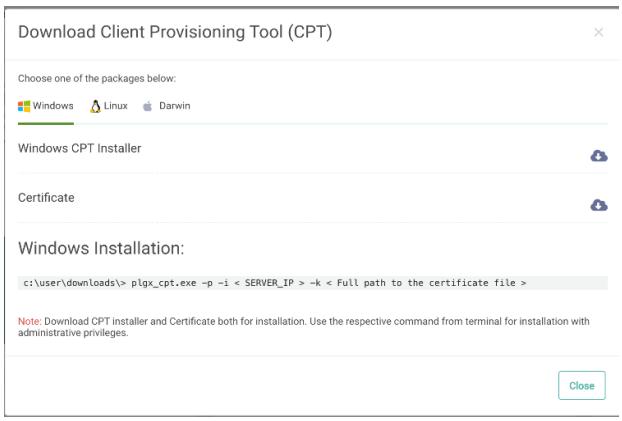
1. Ensure you have working knowledge of osquery.

   If not, please review osquery.

2. Navigate to the web interface of the EclecticIQ Endpoint Response server.

   `https://<server IP>`

3. Download the CPT file for the relevant operating system.



Here are the file names for the various operating systems.

Operating system	***File name***
Windows	plgx_cpt.exe
Linux	plgx_cpt
macOS	plgx_cpt.sh

4. Download the certificate (certificate.crt) file.

Deploy the Client on Windows

Use the EclecticIQ Endpoint Response Client Provisioning Tool (CPT) utility to deploy the EclecticIQ Endpoint Response client on endpoints.

Here is the syntax to execute the installation command.

plgx_cpt.exe -p -i <IP address> | -h <hostname> -k <server's public key file> [-o <download directory>] [-y <yara refresh interval>]

Here is the syntax description.

Parameter	***Description***
-p	Signifies the option for provisioning the client
-i or -h	Specify one of the following. This is a required parameter. -i represents the IP address of the EclecticIQ ER management server (x.x.x.x format). -h represents the fully qualified domain name to the management server in the format a.b.c. You don’t need to https.
-k	Indicates the full path to the server public key file. This is a required parameter.

Parameter	*Description*
-o	Indicates the location at which to download. The default value is C:\ %LOCALAPPDATA%\plgx-temp. This is an optional parameter.
-y	Indicates the yara refresh interval in seconds for downloading signature files from server.

The following output is displayed if the command is successful.

```
########### Installation operation started ###########
Downloading files...Done
Installing files...Done
Verifying EclecticIQ Endpoint Platform services are up and running....
EclecticIQ Endpoint Platform services initialized.
########### Installation operation completed successfully ###########
```

Deploy the client on Linux

Use the EclecticIQ Client Provisioning Tool (CPT) binary to deploy the EclecticIQ Endpoint Response client on the endpoints.

The following command can be invoked to deploy the client.

```
sudo ./plgx_cpt -p -i <server_IP> -k <path to certificate file >
```

Note: Execution permission is required before executing the above command.

Deploy the client on macOS

Use the EclecticIQ Client Provisioning Tool (CPT) shell script to deploy the EclecticIQ Endpoint Response client on the endpoints.

The following command can be invoked to deploy the client.

```
sudo bash plgx_cpt.sh -p -i <server_IP/hostname> -k certificate.crt
```

Verify the client installation

After you deploy the EclecticIQ Endpoint Response client, complete these steps to verify the installation. When the EclecticIQ Endpoint Response client is installed successfully, the following services and processes start.

Operating system	*EclecticIQ Endpoint Response Services*
Windows	• plgx_osqueryd service • vast service • vastnw service

	• plgx_win_extension.ext.exe process
Linux	• plgx_osqueryd service • plgx_linux_extension process
macOS	• osqueryd service

Installation is not successful if any of these services fail to start.

On Windows

Follow these steps to check if the required processes are running.

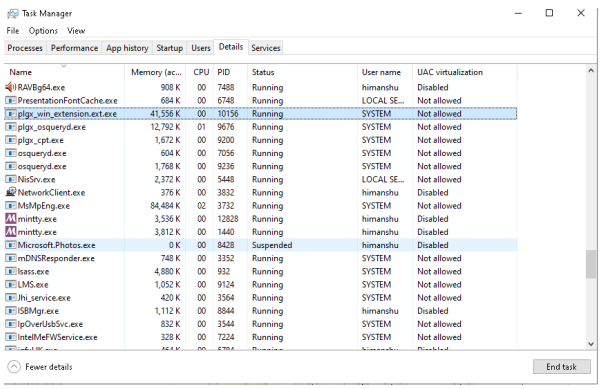
1. Open a command window with administrative privileges.
2. Switch to C:\Program Files\plgx_osquery folder on the command prompt.
3. Run the following command to check the state of software stack, including osquery, EclecticIQ Endpoint Response Extension and associated services.

```
plgx_agent.exe –c
```

The command output lists the current state of the osqueryd, vast, and vastnw services.

```
Service vastnw up and running.
Service plgx_osqueryd up and running.
============== Query Execution Output ==============
name : plgx_win_extension
path : \\.\pipe\plgx_osquery.em.10020
sdk_version : 0.0.0
type : extension
uuid : 10020
version : 1.0.40
============== Query Execution Finished ==============
Service plgx_agent up and running.
```

4. Review the output to verify if the required services are running.
5. Check if the plgx_win_extension.exe process is running.
6. Open Task Manager.
7. Switch to the Details tab.
8. Locate the entry for the plgx_win_extension.exe process.
9. Verify that process status is set to Running.



On Linux

Follow these steps to verify EclecticIQ Endpoint Response client installation.

1. Open a command window with administrative privileges.
2. Switch to directory where the installer files are downloaded.
3. Run the following command.

   ```
   sudo ./plgx_cpt -c
   ```

   Review the output to verify the status of EclecticIQ Endpoint Response.

   ```
   ##### EclecticIQ Osquery Client Provisioning Tool v3.5.1.0#####
   EclecticIQ Endpoint Platform services running successfully.
   ```

On macOS

Follow these steps to verify EclecticIQ Endpoint Response client installation.

1. Open a command window with administrative privileges.
2. Switch to directory where the installer files are downloaded.
3. Run the following command.

   ```
   ps -ef|grep osquery
   ```

   Review the output.

```
  0    702   1  0   3:25PM    ??    0:00.09     /usr/local/bin/osqueryd -
flagfile=/private/var/osquery//osquery.flags
  0    705   02  0  3:25PM    ??    0:01.16     /usr/local/bin/osqueryd
  501  712  639 0   3:26PM    ttys  0000:00.00  grep osquery
```

Uninstalling the server

To uninstall the EclecticIQ Endpoint Response server, run the following command to cleanup existing Docker images and containers.

```
~/Downloads\$ sh ./docker-cleanup.sh
```

Note: This will clean **all** the images and containers.

Uninstalling the client

Complete these steps to uninstall the EclecticIQ ER client.

1. Open a command window with administrative privileges.
2. Close any open instances of the osqueryd, vast, and vastnw services.
3. Close installation directory "C:\Program Files\plgx_osquery" if opened in Explorer view or command prompt.
4. Close Event Viewer.
5. Using the command prompt, navigate to the directory where the CPT tool was downloaded.

   This is not the installation directory.

6. Run the uninstall command.

   Here is the syntax to execute the command.

   ```
   plgx_cpt -u <d / s>
   ```

The -u parameter is used to uninstall the agent and cannot be combined with any other options. With the –u option, you must use one of these options:

Option	***Description***
s	Used with the –u parameter for shallow uninstall. This option only uninstalls the software and does not delete associated data files.
d	Used with the –u parameter for deep uninstall. This option removes all traces of the agent, including data files.

Here are command examples.

Command	***Output***

`plgx_cpt.exe -u d`	The following output displays if the command is successful.
	
	`########## Deep uninstall started ##########`
	`Stopping EclecticIQ Endpoint Platform services...Done`
	`Deleting Install directory...Done`
	`Deleting other files...Done`
	`########## Deep uninstall completed successfully ##########`

`plgx_cpt.exe -u s`	The following output displays if the command is successful.
	
	`########## Shallow uninstall started ##########`
	`Stopping EclecticIQ Endpoint Platform services...Done`
	`Cleaning installed files...Done`
	`Deleting other files...Done`
	`########## Shallow uninstall completed successfully ##########`

Note: If for any reasons the uninstall does not work, you can perform a forced clean on the Windows systems by using the *agent_cleanup.bat* file included in this repository. Download the batch file on the target system and invoke it from an administrator privileged command prompt.