Cloudpath

Cloudpath
Enrollment System

How to Configure Cloudpath to Send Data to an ELK Server

Software Release 5.0

December 2016

Summary: This document describes the Elasticsearch, Logstash, Kibana (ELK) server configuration and how to set up Cloudpath to send data to an existing ELK server.
Document Type: Configuration
Audience: Network Administrator

Cloudpath

How To Configure Cloudpath to Send Data to an ELK Server

Overview

The Cloudpath Enrollment System (ES) provides information about secure wireless traffic in the form of enrollment, user, and certificate records, as well as scheduled reports, and the Cloudpath ES provides the ability to export this data into a spreadsheet or CSV file.

Starting with Cloudpath ES version 4.x, you can configure the Cloudpath ES to send data to an existing Elasticsearch, Logstash, Kibana (ELK) server.

> **Note >>**
>
> This feature is currently in the beta state, as we continue to develop and improve the integration. We encourage customers with an existing ELK system, and early adopters, to test this new functionality. Please submit questions and feedback on this feature by contacting our support desk at support@cloudpath.net.

This feature is available on Cloudpath version 4.1.x, and later.

Prerequisites

This set of instructions assumes you are using CentOS and Apache (httpd), but this configuration should work with other systems.

Setting Up the System

ELK Server Configuration

1. Download and install Elasticsearch, Logstash, and Kibana as outlined on the *https://www.elastic.co/products* website.
2. Edit the **/etc/elasticsearch/elasticsearch.yml** file.
3. Give the **cluster.name** a unique name.
4. Enter the **service elasticsearch start** command.
5. Configure services to run on boot using these commands:
   - **chkconfig --add elasticsearch** (adds it as a service)
   - **chkconfig --add logstash** (adds it as a service)

- • **chkconfig elasticsearch** on (tells the service to auto-run at boot level 3, 5, and 6)
- • **on** (tells the service to auto-run at boot level 3, 5, and 6)

6. Enter the s**ervice logstash start** command.

7. Enter the **service httpd restart** command.

8. Enter the **iptables -A INPUT -p tcp -m tcp --dport 9200 -j ACCEPT** command.

9. Download the *Schema Script* from the Cloudpath ES Admin UI (*Administration > System > System Services > Reporting Server* component).

10. Install the downloaded schema script on the ELK server.

Cloudpath ES Configuration

Configure the Cloudpath ES to communicate with the ELK server.

1. Enter the *Hostname* and *Port* of the reporting server. By default, the port number is 9200.

2. Select the *Frequency* of data uploads from the Cloudpath ES to the ELK server.

3. Create a new workflow snapshot on the *Configuration > Deploy* page.

Viewing the Cloudpath ES Data

To view the Cloudpath ES data on your ELK server, open a browser to **http://<ELK server hostname>:5901**.

> **Note >>**
> The *Use Index* contains time-based events. We recommend using '*' for the *index*, and then select *enrollmentStart* in the *Time-field name* drop-down box.