## Logjam: Installation Guide

## OS Requirements

Throughout this document, we will be assuming you are using a Debain-based UNIX system. Logjam has not been fully tested on OSX or Windows, so there is no guarantee of correct functionality on these systems.

## Docker

Logjam is containerized using Docker and uses a modified ELK image. To use our tool, you’ll need to download Docker and install the image, as well as make a few modifications within the image.

### Installation

To install Docker on a Debian-based machine, please refer to the official documentation, which can be found at https://docs.docker.com/install/linux/docker-ce/ubuntu/.

### Image

Once Docker is installed, you’ll need to create our custom Logjam image. Provided in our GitHub repository is a file called “dockerfile.” You can run either sudo docker build -t logjam\_image . or using our wrapper script, ./logjam.sh -b. This will create the Logjam image. Note: our image is based off of the elk-docker image, which can be found at http://elk-docker.readthedocs.io/.

To create a container using our Logjam image, you can run:

sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name logjam logjam\_image

A container using the “Logjam” image should have now been created. The container will be named ‘logjam’. You can see the status of the container (and all other containers) by running the following:

sudo docker ps -a

## Ingest.py

Since Logjam uses a Python script to manage support cases, you will need to download the latest version of Python 2.X (found at: https://www.python.org/downloads/) and follow the installation guide. This script has only been tested on Python 2.7.13/14, so we can only guarantee it will function correctly on this version.

Ingest.py uses numerous packages not included with the base installation. See the Package Setup section (below) for configuration instructions.

### Package Setup

The script has several packages that need to be imported. The following commands need to be run to fully setup the script:

1. pip install conan (Used for unzipping files)

2. pip install gzip (Also used for unzipping, specifically gzip files)

3. pip install pycurl (Used for sending data to Logstash)

4. pip install pyunpack (Used for unpacking zipped directories)

5. pip install patool (Used for additional unpacking methods)

6. pip install python-magic (Determines extensionless files)

Before running ingest.py, setup.py needs to be run first to initialize a database with a proper table. (This is used for eliminating duplicates being sent to Logstash, and is an important step to not skip.) Open the terminal, cd into the directory you’ve saved duplicates.py in, and run the command python setup.py to initialize the database. Currently, to run the ingest.py script, setup.py needs to be in a directory above ingest.py. Ingest.py takes two arguments: the path to the directory to ingest, and an optional -v verbose argument. For example, python ingest.py ../dirToIngest -v is a valid command, given that duplicates.py was run in a folder above it.

## Other Packages

The following are apt packages used for Logjam and should be installed on the instance hosting the Docker containers.

* build-essential
* checkinstall
* libreadline-gplv2-dev
* libncursesw5-dev
* libssl-dev
* libsqlite3-dev
* tk-dev
* libgdbm-dev
* libc6-dev
* libbz2-dev

## Troubleshooting

If you are running this on an AWS instance, you may run into a lack of memory due to AWS default configurations. To remedy this, you can run:

sysctl -w vm.max\_map\_count=262144

## Verification Plan

Per each step of the installation, Docker, ELK, and pip installs will all notify you if it has been installed correctly.

## Kibana

By default, Kibana does not come pre-loaded with our dashboard. For each new instance of Kibana, you will need to perform the following process. After initially loading Kibana, navigate to “Management” on the left-side menu. Select “Saved Objects”, then “Import”. A file selector window will prompt you to load in a JSON file. From the logjam project directory, select “kibana”, “logjam\_default.json”. You can confirm that the dashboard has been properly installed by ensuring “Common Failure/Error Concentrations” appears in the list of available dashboards.