General

The following is a basic example of how one could use an [ELK stack](https://www.elastic.co/elk-stack) running in [Docker](https://www.docker.com/) containers to pull Umbrella logs from S3 and build reports/visualisations for this data.

\*\*\* **Important** \*\*\*

This guide is intended as an example only. For convenience, we are demonstrating this example with a stack built by [deviantony](https://github.com/deviantony). You should consider putting together your own deployment which will most likely need to include other elements, be appropriately scaled and take into account things like:

* The needed storage.
* The amount of data and how you should deploy/scale the stack elements.
* Bandwidth considerations.
* Security considerations.
* Other environmental considerations.

Preparations and Prerequisites

* You'll need to be able to run [Docker](https://www.docker.com/) containers.
* You'll need to setup [S3 logging in Umbrella](https://support.umbrella.com/hc/en-us/articles/231248448-Cisco-Umbrella-Log-Management-in-Amazon-S3) and have the key/secret/bucket name available.
* Make sure that you have traffic in your environment and that this traffic is reaching your bucket:

|  |
| --- |
| aws s3 ls s3://<*YourBucketName*>/ --recursive |

Getting Started

* Clone the following repo <https://github.com/deviantony/docker-elk>:

|  |
| --- |
| git clone <https://github.com/deviantony/docker-elk> |

* Replace ../logstash/pipeline/logstash.conf with:  <https://github.com/CiscoDevNet/cloud-security/blob/master/Umbrella/Reporting/logstash.conf>
* Edit ../logstash/pipeline/logstash.conf and enter your AWS details under the **S3** section (do not change the other settings):

|  |
| --- |
| s3 {       access\_key\_id => "XXX"       secret\_access\_key => "XXX"       bucket => "XXX"       prefix => "dnslogs/XXX"       additional\_settings => {         force\_path\_style => true         follow\_redirects => false       } |

* Make sure that you are in the root folder: ../docker-elk and then run:

|  |
| --- |
| docker-compose up -d (or to keep up: docker-compose up) |

* Kibana will be available at [http://localhost:5601](http://localhost:5601/)
* Goto Management -> Index Patterns and enter: log\* -> select 'timestamp'
* Import the [dashboard json file](https://github.com/CiscoDevNet/cloud-security/blob/master/Umbrella/Reporting/VisConfig.json).