Configuring Windows Elastic Stack for DMARC Analysis

# Required Software

* Elasticsearch
* Logstash
* Kibana
* Java 8u152
* Non-Sucking Service Manager (NSSM)
* PowerShell version 5+
* Notepad++ (Optional)

# Pre-requisites

Prior to installing the Elastic Stack, the following modifications are required.

**Disable Windows Page File (Swap Disk)**Failure to disable the Page File can have a significant impact on the performance and reliability of the Elastic Stack.

* Open the **System Properties** window located in the control panel.
* Select **Advanced System Settings**
* On the **Advanced** tab, select **Settings…** under the Performance section.
* Select the **Advanced** tab on the following window and then **Change…**
* Uncheck **Automatically manage paging file size for all drives**, select the **No paging file** button, and click **Set**.
* Reboot computer.

**Install Java JDK and Set Environment Variable**The Elastic Stack relies on Java. Ensure that you install the JDK, not JRE. Versions verified with this configuration are Java 8u152 and 8u162. Java 9.0.4 is not compatible at the time of this writing. After installation of the JDK, you must configure an OS environment variable pointing to the JDK root folder.

* Open the **System** **Properties** window located in the control panel.
* Select **Advanced System Settings**
* On the **Advanced** tab, select **Environment Variables…**
* In the window that appears, in the **System Variables** section, select **New…**
  + Variable Name: JAVA\_HOME
  + Variable Value: JAVAROOTFOLDER (E.G. C:\Program Files\Java\jdk1.8.0\_162)

# Miscellaneous Considerations

**Hardware Requirements**  
For the purposes of this implementation; one CPU and 6 GB of RAM should be sufficient. If you intend to ingest more data, such as with Beats agents, you may need to allocate more resources.

**Path Referencing in This Guide**For the sake of simplicity and consistency, when referencing the installation location of an application, **root** shall imply drive letter and path to the application. For example, D:\Elastic Stack\Elasticsearch\bin will be root\bin.

**Example Configurations**I have included prebuilt example configuration files for each Elastic Stack application. These files require minimal modifications and are intended to get you up and running on a basic Elastic Stack implementation.

**Time Stamping**  
When creating an Index, you have three options for the Time Filter field. The decision on which field to use is dependent on your organization’s desires. Be aware, once you’ve selected a field, you cannot change it without first recreating the index and then removing all previously indexed data.

* @timestamp – This will tag each event with the date and time that it was processed by Logstash.
* Report.start – This is the starting time for the reporting period as reported by the aggregate generator (remote MTA server).
* Report.end – This is the ending time for the reporting period as reported by the aggregate generator (remote MTA server).

**Disk Buffer**  
As of this writing, there is an issue with using disk-based buffering (persisted queue) with this configuration on Elastic Stack 6.1.1 – 6.2.2. Previous versions may also be affected, please do not use disk-based buffering until further notice. If you have a pre-existing Elastic Stack and are using persisted queue, using the multipipeline configuration (as configured in this implementation), will allow you to specify per pipeline queueing settings.

**Elastic Stack Applications**The Elastic Stack applications do not have an installation process or executable. Wherever you decompress the archives effectively becomes the installation location. Ensure that you place the files in the proper location prior to configuration.

**Recommended Editor**  
It is highly recommended that you use a text editor like Notepad++ to maintain proper encoding of the configuration files. It also generally just makes for a friendlier method of working with configuration files.

# Elasticsearch Installation

* Decompress Elasticsearch to your intended installation location.
* Download and Decompress ElasticMARC to a temporary location
* Copy the contents of ElasticMARC\elasticsearch to the Elasticsearch directory, overwriting any existing files.
* Open root\config\elasticsearch.yml and modify the following:
  + Node.name: HostnameOfComputer
  + Network.host: This is the IPv4 address of the host Elasticsearch will listen on, use 0.0.0.0 to listen on all available addresses.
  + http.port: This is the port number Elasticsearch will listen on, 9200 is used by default.
  + (Optional) path.data: Where Elasticsearch will store indexed data. By default, this is root\data.
  + (Optional) path.logs: Where Elasticsearch will store logs. By default, this is root\logs.
* Open root\config\jvm.options and modify the following, if necessary:
  + -Xms1g – This determines the initial amount of RAM consumed by the Elasticsearch JVM.
  + -Xmx1g - This determines the max amount of RAM consumed by the Elasticsearch JVM.
  + Xms and Xmx should be set to the same size. If they are not, you may experience performance issues.
  + These values represent the amount of RAM the Elasticsearch JVM will allocate. For the purposes of this guide, 1GB is sufficient.
* Open an administrative CMD window and enter the following commands:
  + Root\bin\elasticsearch-service.bat install
  + Root\bin\elasticsearch-service.bat manager
    - In the window that appears, modify the following:
      * Display Name: Optional, I personally remove the version information.
      * Startup Type: Automatic
    - Select apply, start the service, and close the service manager window.
* Elasticsearch installation is now complete.

# Kibana Installation

* Decompress Kibana to your intended installation location.
* Copy the contents of ElasticMARC\kibana to the Kibana directory, overwriting any existing files.
* Open root\config\kibana.yml and modify the following:
  + Server.port: This is the port the server will listen for requests on. Default is 5601
  + Server.host: Set to server’s hostname.
  + Server.name: Set to server’s hostname.
  + Elasticsearch.url: Set to server’s hostname with http:// at the beginning and the port elasticsearch is configured to listen on, 9200 is default.
  + Logging.dest: Filename and path for logging. Folder structure must already exist, file will be created. Preserve double quotes around value.
  + If you want to change the logging level, change the appropriate logging line value to true.
* Decompress NSSM to your intended installation location.
* Kibana does not have a service installer, we will utilize NSSM to create a service for Kibana. In the following steps, root refers to the location that NSSM has been extracted to.
* Open an administrative CMD prompt and enter the following command:

Root\win64\nssm.exe install Kibana

* On the Application tab, set the following:
  + Path: Root\bin\kibana.bat
  + Startup Directory: root\bin
* On the Details tab, set the following
  + Display Name: Kibana
  + (Optional) Description: Kibana VER (I.E. Kibana 6.2.2)
  + Startup Type: Automatic
* Select Install Service and click OK to finish.
* In the administrative CMD prompt enter the following to start the Kibana service.

Powershell -c Start-Service Kibana

* After a few moments, you can verify Kibana’s functionality by opening a browser and pointing it to http://hostname:port as configured in Kibana.yml’s server.host and server.port properties.

# Logstash Installation

* Decompress Logstash to your intended installation location.
* Copy the contents of ElasticMARC\logstashto the logstash directory, overwriting any existing files.
* Create a folder that will be the ingest point for the DMARC Aggregate reports.
* Open root\config\logastash.yml and modify the following:
  + Node.name: Set to hostname of server.
  + http.host: Set to IPv4 Address of Logstash server. This is for the REST API.
  + http.port: Set to port for REST API to listen on. Default is 9600.
  + (Optional) Log.level: Uncomment and set to desired level. Trace is most detailed but very chatty. Debug is usually sufficient for troubleshooting.
* Open root\config\jvm.options and modify the following:
  + -Xms1g – This determines the initial amount of RAM consumed by the Logstash JVM.
  + -Xmx1g - This determines the max amount of RAM consumed by the Logstash JVM.
  + Xms and Xmx should be set to the same size. If they are not, you may experience performance issues.
  + These values represent the amount of RAM the Logstash JVM will allocate. For the purposes of this guide, 1GB is sufficient.
* Open root\config\pipelines.yml and modify the following:
  + Path.config: Set this to the location of /root/config/pipelines/dmarcpipeline.yml. Do not use a drive letter, use forward slashes in path, and preserve double quotes around the path.
  + (Optional) If you’d like to implement Beats data ingesting, you can uncomment the second set of pipeline values that are preconfigured for this purpose.
* Open root\config\pipelines\dmarcpipeline.yml and modify the following:
  + Line 3 id => This is a cosmetic tag assigned to this portion of the ingest pipeline. I recommend setting it to the folder you will be ingesting the DMARC XML files. Preserve double quotes around value. This is visible in the Pipeline Monitor if you configure the X-Pack plugin
  + Line 4 path => This is the folder that Logstash will monitor for files to ingest. Use forward slashes in path, preserve double quotes around value, ensure you set to \*.xml after the folder path.
  + Line 95 hosts => This is the servername:port that Logstash will send the data to once it’s been processed. Preserve the brackets and double quotes around the value.
  + Line 98 template => This is the location of the Elasticsearch template that is used to configure the fields for each event. Use drive letter, use forward slashes in path, and preserve quotes around value.
* (Optional) If implementing Beats, open root\config\pipelines\beatspipeline.yml and modify the following:
  + Line 12 hosts => This is the servername:port that Logstash will send the data to once it’s been processed. Preserve the brackets and double quotes around the value.
* Logstash does not have a service installer, we will utilize NSSM to create a service for Logstash. In the following steps, root refers to the location that NSSM has been extracted to.
* Open an administrative CMD prompt and enter the following command:

Root\win64\nssm.exe install Logstash

* On the Application tab, enter the following:
  + Path: root\bin\logstash.bat
  + Startup Directory: root\bin
* On the Details tab, enter the following:
  + Logstash
  + (Optional) Description: Logstash VER (I.E. Logstash 6.2.2)
  + Startup Type: Automatic
* Select Install Service and click OK to finish.
* In the administrative CMD prompt enter the following to start the Logstash service.

Powershell -c Start-Service Logstash

* Logstash installation is now complete.

# Configuring Kibana

At this point, the Elastic Stack installation is complete and ready to start ingesting data. Before we start visualizing the reports, we need to ingest some sample data. This will allow us to create an index pattern and import the preconfigured visualizations and dashboards that are included. A sample report is included and exists alongside where this report was extracted to.

Basic Kibana Configuration  
URLs in Kibana can get large as you start manipulating data and especially when loading a dashboard with many visualizations. For this reason, I recommend changing Kibana to store the URL with the session.

* Open a browser and go to your Kibana instance
* Select Management from the menu on the left, then Advanced Settings.
* Set state:storeInSessionStorage to true
* I also recommend going through the remaining settings in this section but take caution, these settings can break your installation if improperly configured.

## Ingest Sample Data

* Open a Powershell window and execute the following:
* LogstashRoot\bin\dmarcscript.ps1
* Enter the folder path containing the sample report XML.
* Enter the folder path that Logstash is monitoring.
* Assuming all pre-requisites are met, PowerShell will modify the XML structure and save the modified file to the specified ingest folder. From here, Logstash will ingest, parse, and output the data to Elasticsearch.

## Index Pattern Creation

* Open a browser and navigate to your Kibana instance
  + Default is <http://servername:5601>
* Click Management on the left side, then Index Patterns.
* You will see a list of indexes that have been created. If this is a new install, there should be only one named dmarcxml-YYYY.MM.dd.
* Enter dmarcxml-\* for the index pattern and click Next Step
* Select a Time Filter field name
  + See Miscellaneous Considerations near the top of this guide for an explanation of these fields.
* Expand Show advanced options and enter dmarcxml-\* as a custom index pattern ID
* Click Create Index Pattern to finish index creation.

## Visualizations & Dashboard Import

Sample dashboards and visualizations have been created to assist in familiarization of the Kibana interface and get new users up and running quickly.

* Open a browser and navigate to your Kibana instance.
* Select Management on the left side, then Saved Objects.
* Click the Import button at the top right of this page.
* Navigate to the kibana\visuals folder and select dmarcvisuals.json
* If prompted, select Yes, to overwrite all saved objects.
* To view the preconfigured dashboards, select Dashboard on the left side of the page.
* To view individual visualizations, select Visualize on the left side of the page.

## Optional Field Formatting

Kibana provides the ability to format fields in a variety of ways. In particular, you can create links on fields utilizing the field value as part of the URL. Process to do this is outlined below.

* Open a browser and navigate to your Kibana instance.
* Select Management on the left side, then Index Patterns.
* Locate the authresult.spf\_domain field and click the pencil icon in the controls column.
* Use the following values:
* Format: URL
* Type: Link
* URL Template: https://dig.whois.com.au/whois/{{value}}
* Label Template: {{value}}

In addition, you can also use https://www.google.com/maps/place/{{value}} on many of the geographic fields, including the coordinates keyword field to link to Google Maps.