

Using Elastic Stack to monitor your File Director cluster performance

Introduction

File Director already provides a syslog stream which can be configured to point to third party applications such as [Splunk](#) or [Graylog](#) which can then be indexed and reported upon in order to monitor the health of the File Director cluster. However, for customers who do not have expertise with these products or have licenses for them, we have produced an example set of dashboards along with the appropriate configurations for the Elastic Stack which can be provided as-is as a starting basis using open source tools.

Note: These instructions have been tested against Server 2016 and with a File Director 2019.3 cluster and are provided as-is. The scripts require PowerShell 5.0 or later. The version 5.1 of PowerShell can be obtained here <https://docs.microsoft.com/en-us/powershell/wmf/5.1/install-configure>.

Version History

FD Dash_2019.1.SP1 – July 2019

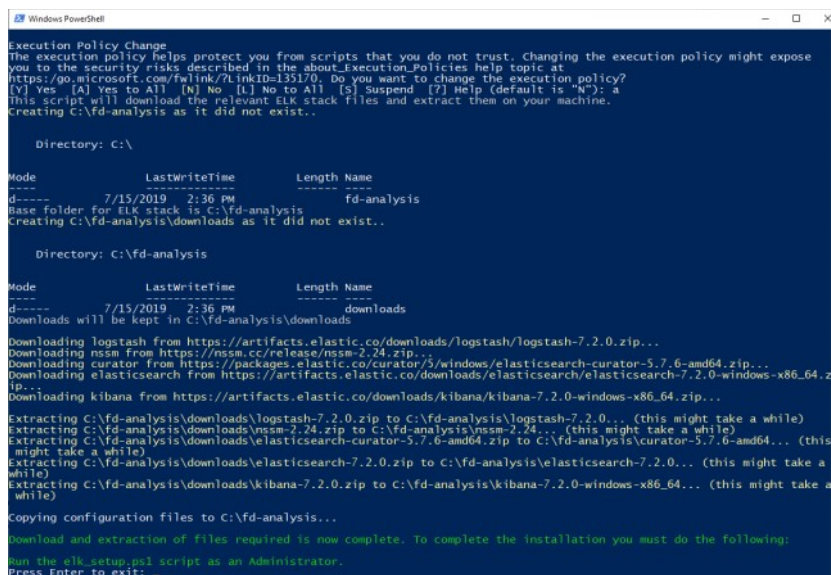
FD Dash_2019.3 – November 2019

Upgrades

If upgrading from a previous version of the dashboards you must first execute the ‘cleanup.ps1’ script found within the FD Dash_.zip folder of your currently installed version.

Setup Elastic Stack Instructions

1. Download and unzip the attached file that contains scripts and configurations
2. Open a PowerShell Window
3. Run the download.ps1 PowerShell script which will download the Elastic Stack to c:\fd-analysis



```
Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
([Y] Yes, [A] Yes to All, [N] No, [L] No to All, [S] Suspend, [?] Help (default is "N")): a
This script will download the relevant ELK stack files and extract them on your machine.
Creating C:\fd-analysis as it did not exist..

Directory: C:\
Mode                LastWriteTime         Length Name
----                -
d-----          7/15/2019   2:36 PM             fd-analysis
Base folder for ELK stack is C:\fd-analysis
Creating C:\fd-analysis\downloads as it did not exist..

Directory: C:\fd-analysis
Mode                LastWriteTime         Length Name
----                -
d-----          7/15/2019   2:36 PM             downloads
Downloads will be kept in C:\fd-analysis\downloads

Downloading logstash from https://artifacts.elastic.co/downloads/logstash/logstash-7.2.0.zip...
Downloading nssm from https://nssm.cc/release/nssm-2.24.zip...
Downloading curator from https://packages.elastic.co/curator/5/windows/elasticsearch-curator-5.7.6-amd64.zip...
Downloading elasticsearch from https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.2.0-windows-x86_64.zip...
Downloading kibana from https://artifacts.elastic.co/downloads/kibana/kibana-7.2.0-windows-x86_64.zip...

Extracting C:\fd-analysis\downloads\logstash-7.2.0.zip to C:\fd-analysis\logstash-7.2.0... (this might take a while)
Extracting C:\fd-analysis\downloads\nssm-2.24.zip to C:\fd-analysis\nssm-2.24... (this might take a while)
Extracting C:\fd-analysis\downloads\elasticsearch-curator-5.7.6-amd64.zip to C:\fd-analysis\curator-5.7.6-amd64... (this
might take a while)
Extracting C:\fd-analysis\downloads\elasticsearch-7.2.0.zip to C:\fd-analysis\elasticsearch-7.2.0... (this might take a
while)
Extracting C:\fd-analysis\downloads\kibana-7.2.0.zip to C:\fd-analysis\kibana-7.2.0-windows-x86_64... (this might take a
while)

Copying configuration files to C:\fd-analysis...
Download and extraction of files required is now complete. To complete the installation you must do the following:
Run the elk_setup.ps1 script as an Administrator.
Press Enter to exit:
```

4. Open a new Powershell window **as Admin**, and then run the elk_setup.ps1 PowerShell script will setup the Elastic Stack to run as a service and configure Logstash using the configuration in the attached file. This will also setup a cleanup task to run daily at 10pm which will cleanup the Elasticsearch database and remove and data older than 30 days

```
Administrator: Windows PowerShell
PS C:\temp\FD Dash> .\elk_setup.ps1
This script should be run as Administrator, it will setup the ELK stack services on your machine.

Configuring and setting up services...
Installing the Elasticsearch service...

Directory: C:\fd-analysis\elasticsearch-7.2.0

Mode                LastWriteTime         Length Name
-----
d-----       7/15/2019   4:51 PM            tmp

Installing service : "elasticsearch-service-x64"
Using JAVA_HOME (64-bit) : "C:\fd-analysis\elasticsearch-7.2.0\jdk"
-Xms1g;-Xmx1g;-XX:-UseConcMarkSweepGC;-XX:CMSInitiatingOccupancyFraction=75;-XX:+UseCMSInitiatingOccupancyOnly;-Des.networkaddr
ess.cache.ttl=60;-Des.networkaddress.cache.negative.ttl=10;-XX:+AlwaysPreTouch;-Xss1m;-Djava.awt.headless=true;-Dfile.encoding=
UTF-8;-Djna.nosys=true;-XX:-OmitStackTraceInFastThrow;-Dio.netty.noUnsafe=true;-Dio.netty.noKeySetOptimization=true;-Dio.netty
recycler.maxCapacityPerThread=0;-Dlog4j.shutdownHookEnabled=false;-Dlog4j2.disable.jmx=true;-Djava.io.tmpdir=C:\fd-analysis\el
asticsearch-7.2.0\temp;-XX:-HeapDumpOnOutOfMemoryError;-XX:HeapDumpPath=data;-XX:ErrorFile=logs\hs_err_pidNo.log;-Xlog:gc*:gc+age
+trace,safepoint:file=logs/gc.log:utime,pid,tags:filecount=32,filesize=64m;-Djava.locale.providers=COMPAT;-Dio.netty.allocation
r.type=unpooled;-XX:MaxDirectMemorySize=536870912
The service "elasticsearch-service-x64" has been installed.
Installing Kibana as a service...
Service "Kibana" installed successfully!
Set parameter "AppDirectory" for service "Kibana".
Set parameter "DependOnService" for service "Kibana".
Set parameter "AppStdout" for service "Kibana".
Set parameter "AppStderr" for service "Kibana".
Installing Logstash as a service...
Service "Logstash" installed successfully!
Set parameter "AppStdout" for service "Logstash".
Set parameter "AppStderr" for service "Logstash".
Set parameter "DependOnService" for service "Logstash".
Starting services...
The service "elasticsearch-service-x64" has been started
Kibana: START: The operation completed successfully.
Logstash: START: The operation completed successfully.
Setting up a daily cleanup of Elasticsearch at 10pm...

Actions
: (MSFT_TaskExecAction)
Author
:
Date
:
Description
: Daily cleanup of Elastic Search database
Documentation
:
Principal
: MSFT_TaskPrincipal2
SecurityDescriptor
:
Settings
: MSFT_TaskSettings3
Source
:
State
: Ready
TaskName
: ES_Cleanup
TaskPath
: \
Triggers
: (MSFT_TaskDailyTrigger)
URI
: \ES_Cleanup
Version
:
PSComputerName
:

The relevant services for the ELK stack should have now been started. Review the output above to confirm.
You will now need to configure auditing for your File Director cluster to this servers IP address and port 10514.
Once this is complete, you can navigate to Kibana @ http://localhost:5601, setup index patterns and import the dashboards provi
ded
Press Enter to exit:
```

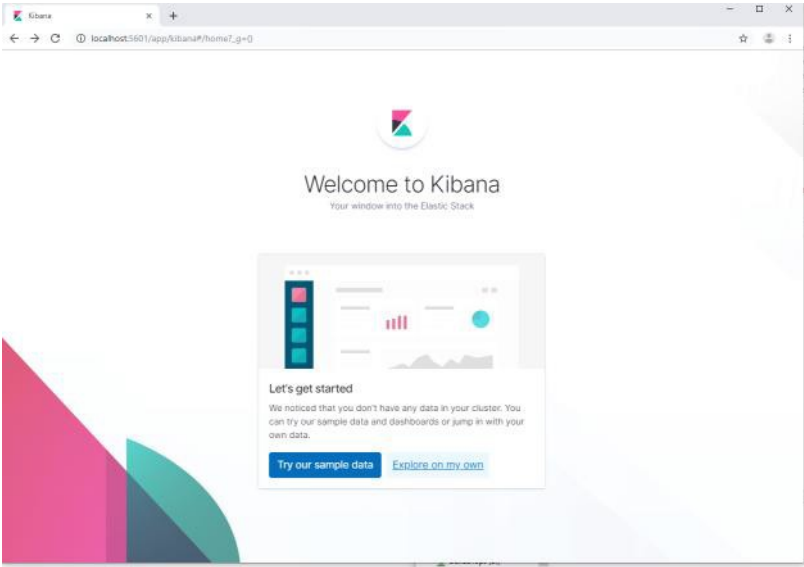
5. If the firewall is configured, configure it so that your FD appliances can connect to the server where the Elastic Stack is installed on TCP port 10514

View File Director events in Elastic Stack

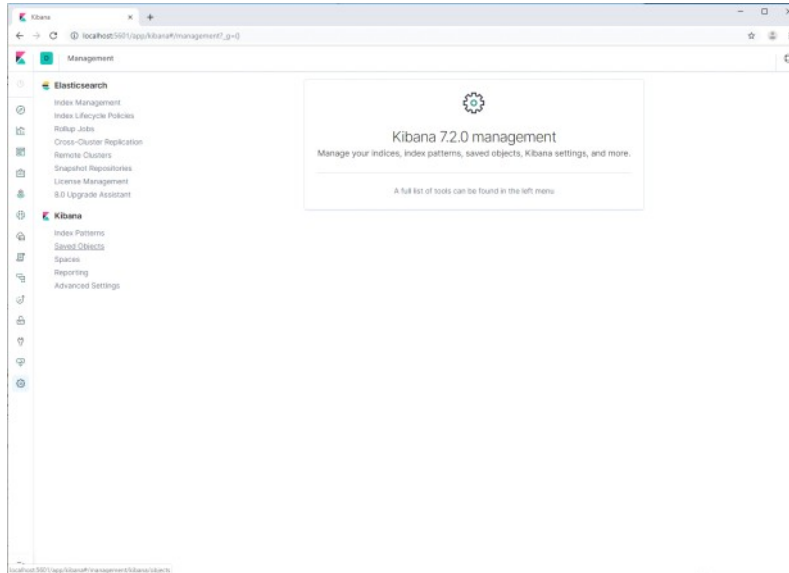
- 1. Login to the File Director Admin Console
- 2. Navigate to the Configuration -> Advanced section, and under the syslog field enter the IP address of the server that is running the Elastic Stack and set the port to 10514 as per the example screenshot below



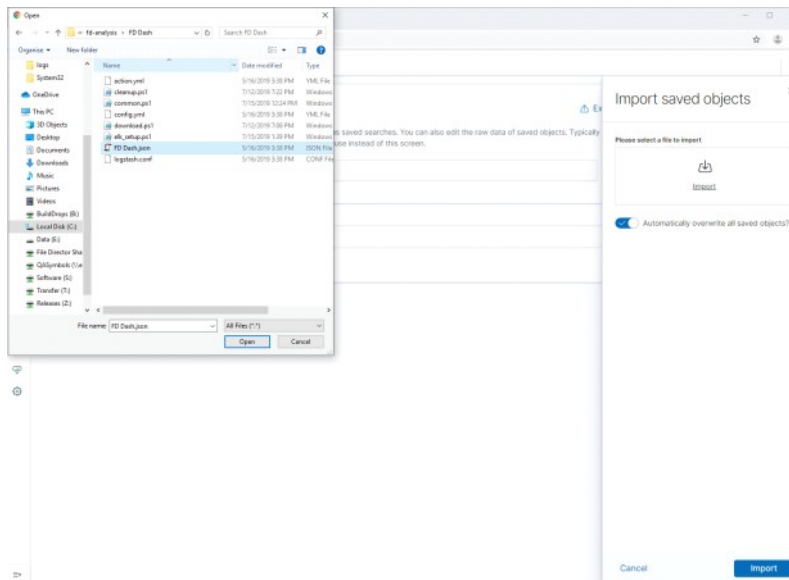
- 3. Click Update so that the nodes in the File Director cluster will start sending their syslog stream to the server
- 4. Go back to the server where the Elastic Stack was installed in the previous steps and navigate to <http://localhost:5601> (as per the instructions on [Download Kibana Free • Get Started Now | Elastic](#))



5. Click explore on my own, then navigate to Settings (the cog icon) and click on Saved Objects under Kibana



6. Click on the import button and select the FD Dash.json file included with this bundle, this will import the index patterns and dashboards that are provided for your use



7. You will now be able to go to the Dashboards tab (third icon) and view either the Performance or Overview dashboards which will show data from the last 24 hours by default. Screenshot below shows an example from the Performance dashboard.



8. If you wish to query or explore the data that is being sent to Elastic Stack, you can do so by going to the Discover tab (first icon) in Kibana and you should see some performance data appearing from the File Director nodes

