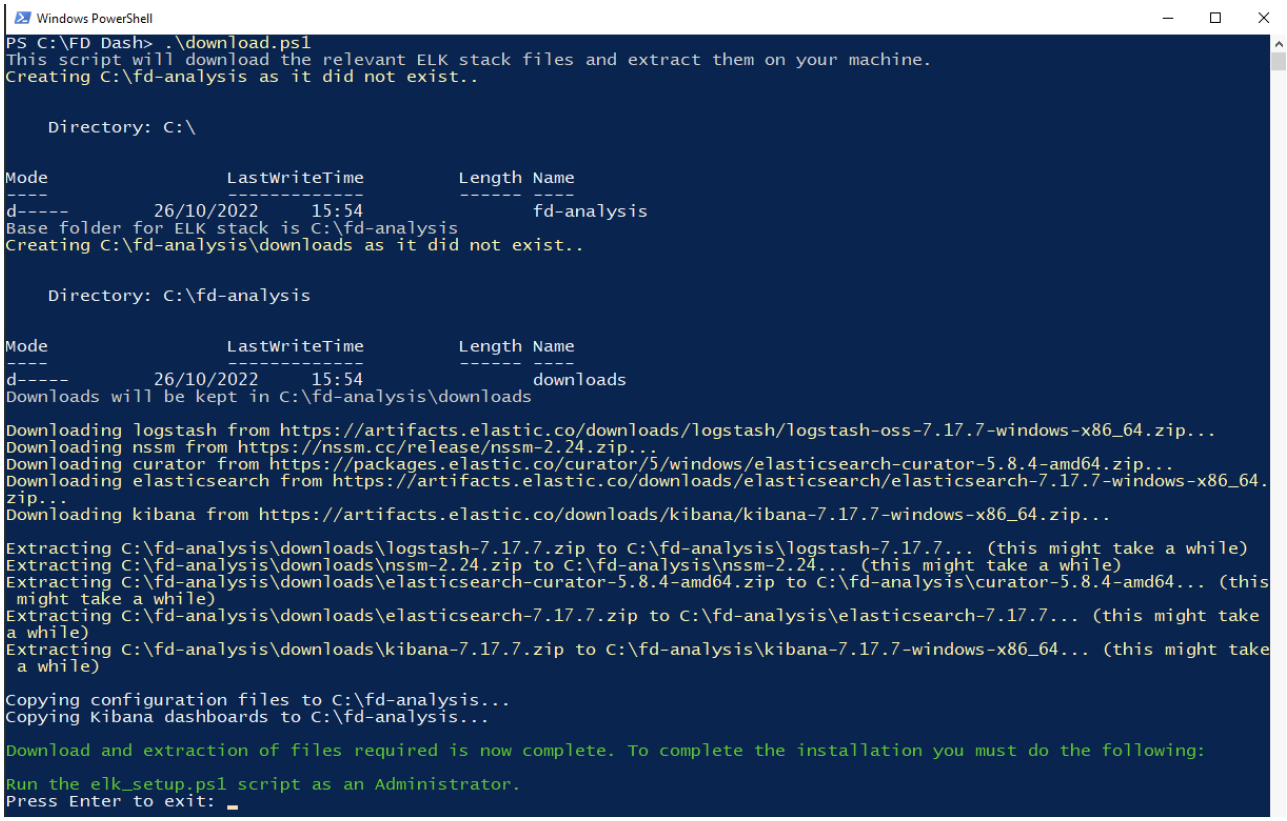
File Director dashboards using Elastic Stack

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 2019 and Server 2022 and with a File Director 2022.1 cluster and are provided as-is. The scripts require PowerShell 5.1 or later.

Configuration and setup

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



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.

```
PS C:\FD Dash> .\elk_setup.ps1
Configuring and setting up Elastic Stack services..
Installing the ElasticSearch service...


    Directory: C:\fd-analysis\elasticsearch-7.17.7


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        26/10/2022     16:18                tmp
Installing service      :  "elasticsearch-service-x64"
Using ES_JAVA_HOME (64-bit):  "C:\fd-analysis\elasticsearch-7.17.7\jdk"
-Des.networkaddress.cache.ttl=60;-Des.networkaddress.cache.negative.ttl=10;-XX:+A
ion=true;-Dio.netty.recycler.maxCapacityPerThread=0;-Dio.netty.allocator.numDirec
;-XX:+UseG1GC;-Djava.io.tmpdir=C:\fd-analysis\elasticsearch-7.17.7\tmp;-XX:+HeapD
m;-Xmx2047m;-XX:MaxDirectMemorySize=1073741824;-XX:G1HeapRegionSize=4m;-XX:Initia
The service 'elasticsearch-service-x64' has been installed.
Updating the ElasticSearch configuration...
The service 'elasticsearch-service-x64' has been started
Waiting for the ElasticSearch service to be up...
Waiting for Elasticsearch to start...
Elasticsearch is running, status is green
Creating the ivanti user...

created : True

Updating the Kibana configuration...
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".
Set parameter "AppRotateFiles" for service "Kibana".
Set parameter "AppRotateOnline" for service "Kibana".
Set parameter "AppRotateBytes" for service "Kibana".
Updating the Logstash configuration...
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".
Set parameter "AppRotateFiles" for service "Kibana".
Set parameter "AppRotateOnline" for service "Kibana".
Set parameter "AppRotateBytes" for service "Kibana".
Starting Kibana and Logstash...
Kibana: START: The operation completed successfully.
Logstash: START: The operation completed successfully.
Updating the Curator configuration...
Setting up a daily cleanup of ElasticSearch at 10pm...
```

5. If the Windows Firewall is enabled, configure it so that your FD appliances can connect to the server where the Elastic Stack is installed by allowing incoming traffic on TCP port 10514. If you wish to access the dashboards from another computer you must also allow incoming traffic on TCP port 5601.

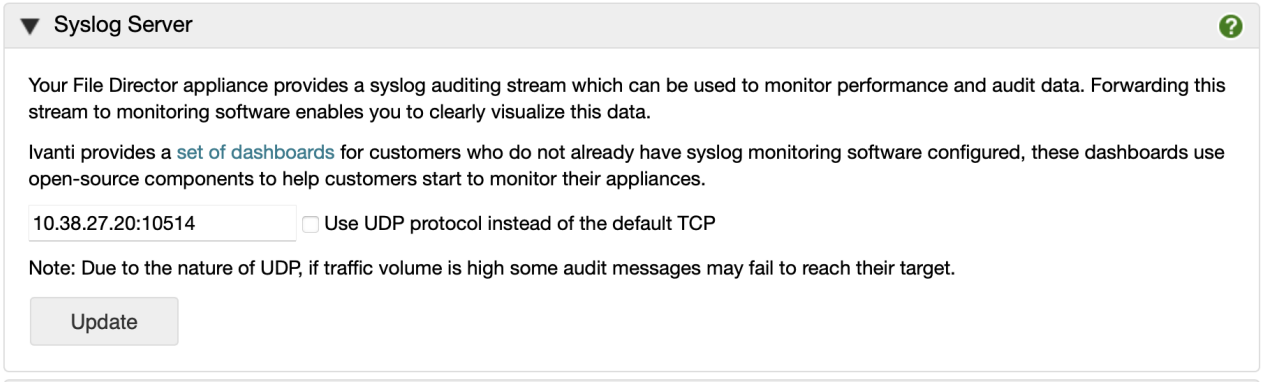
6. Make a note of the password for the `ivanti` username provided at the end of the script, this will be required to login to Kibana to access the audit data and view the dashboards.

```
Waiting for Kibana to start...
Kibana is not ready yet, waiting 30 seconds before retrying, 9 retries left.
Kibana is not ready yet, waiting 30 seconds before retrying, 8 retries left.
Kibana is not ready yet, waiting 30 seconds before retrying, 7 retries left.
Kibana is not ready yet, waiting 30 seconds before retrying, 6 retries left.
Kibana is not ready yet, waiting 30 seconds before retrying, 5 retries left.
Kibana is running, state is green

since    : 2022-10-26T15:22:52.782Z
state    : green
title    : Green
nickname : Looking good
icon     : success
uiColor  : secondary

Importing index patterns and dashboards...

successCount   : 45
success        : True
warnings       : {}
successResults : {@{type=index-pattern; id=d05e8810-d221-11e8-b069-d57f88345432; meta=}, @{type=visualization; id=afdd092
                 id=e6b08d80-2b6d-11e8-ae0e-cb387c146674; meta=}...}


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 to see the audit data and dashboards
Please use the username "ivanti" and password "Znn2N5csX^ShD_yb" to login when prompted by Kibana (ignoring the quotes)
```

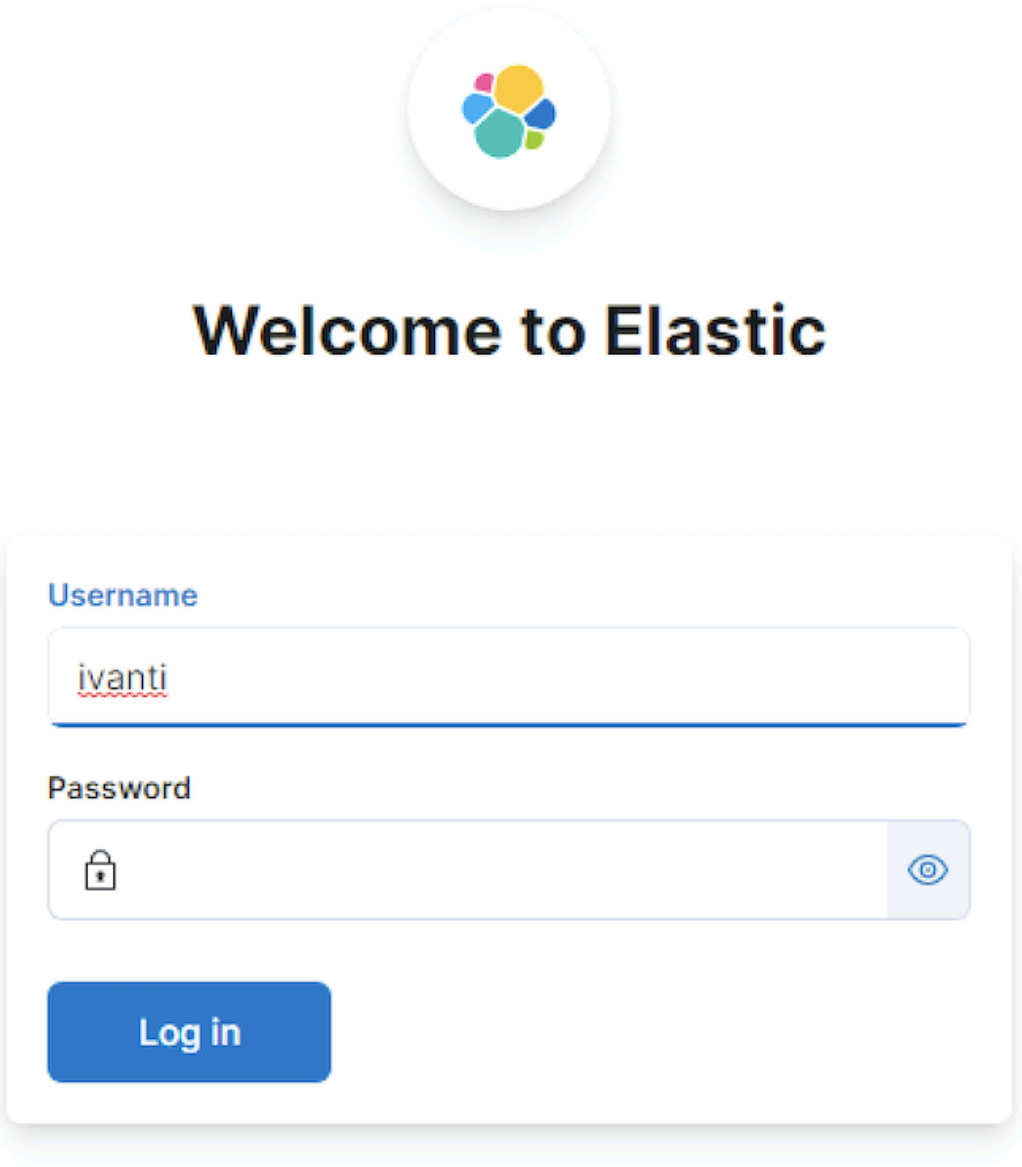
These steps have been tested with Windows Server 2019 and Elastic Stack 7.17 and are provided as-is.

View File Director events in Elastic Stack

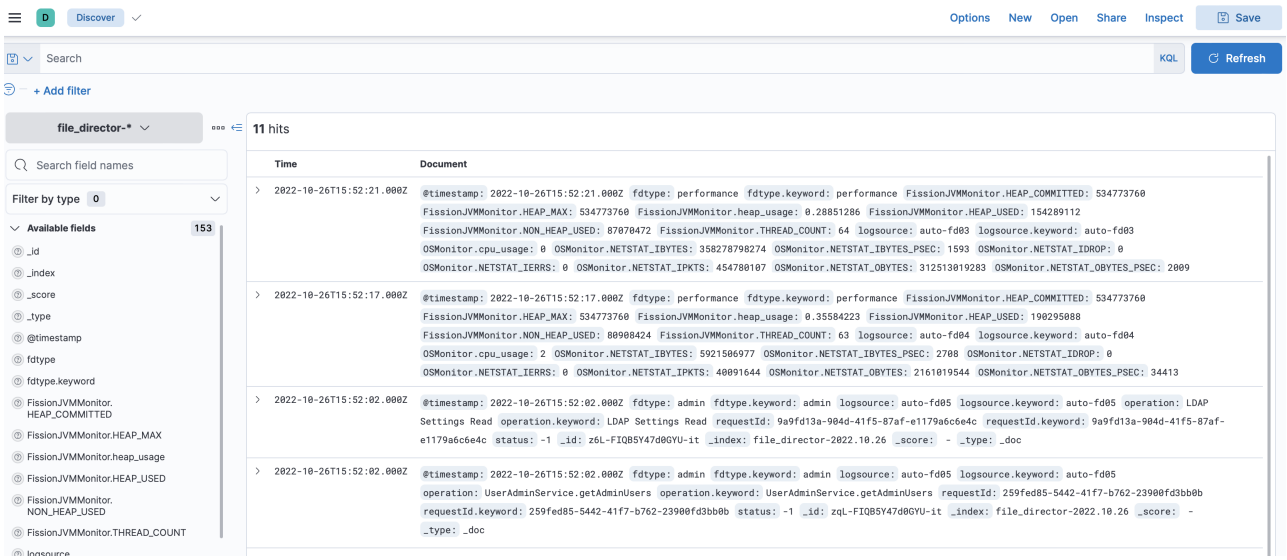
1. Login to the File Director Admin Console
2. Navigate to the Configuration -> Advanced section, and under the syslog field enter the IP address of the server that is running the Elastic Stack and set the port to 10514 as per the example screenshot below



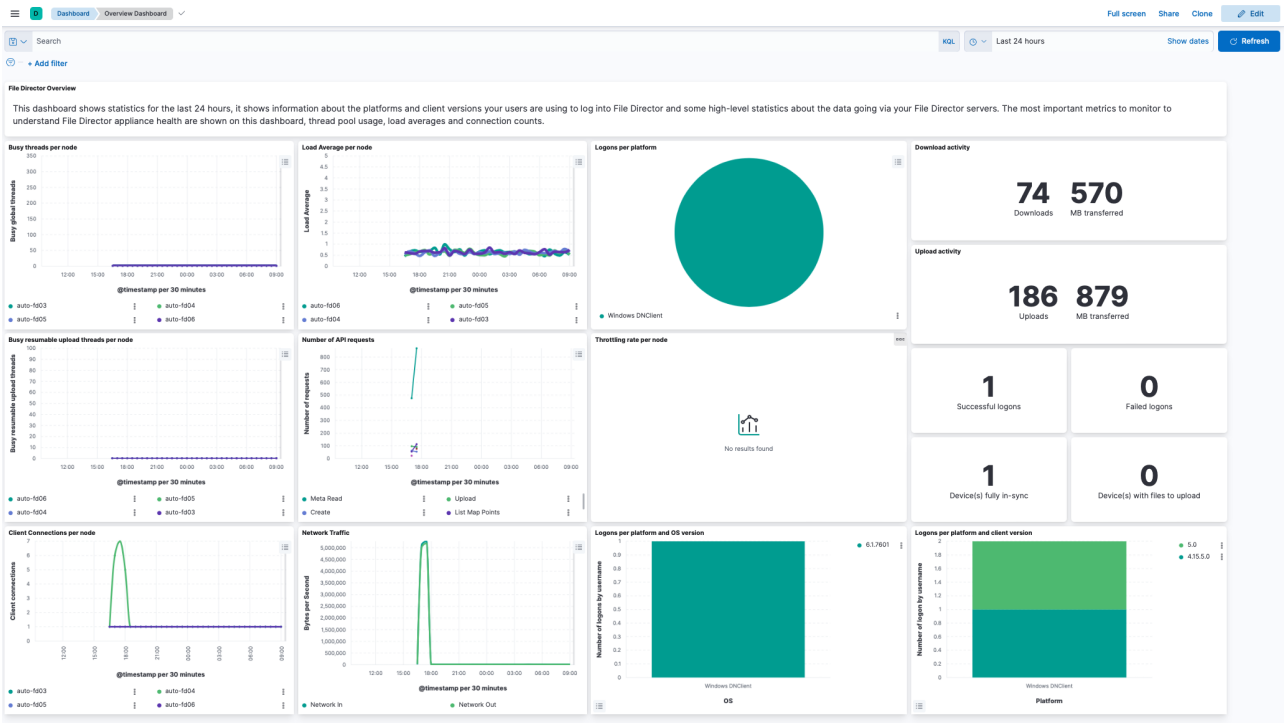
3. Click Update so that the nodes in the File Director cluster will start sending their syslog stream to the server
4. Go back to the server where the Elastic Stack was installed in the previous steps and navigate to http://localhost:5601 (or use the servers IP address or hostname if you have allowed access via the Windows Firewall)
5. Login to Kibana using the `ivanti` user credentials provided by the `elk_setup.ps1` script run in the previous section



6. You will be shown the Discover tab after you have logged in, where you should see some audit information from your File Director nodes.



7. If you wish to view the dashboards, use the navigation menu (at the top on the left hand side, click the three lines) to go to the Dashboards section. The list of dashboards available and a brief description is listed below.



Dashboards

The following dashboards are available out of the box:

- **Overview** - shows information about the platforms and client versions your users are using to log into File Director and some high-level statistics about the data going via your File Director servers. The most important metrics to monitor to understand File Director appliance health are shown on this dashboard, thread pool usage, load averages and connection counts.
- **Performance** - shows information about the performance of your File Director estate to allow you to monitor the application health. The most important metrics to monitor to understand File Director appliance health are shown on this dashboard, thread pool usage, load averages and connection counts. Additionally, there are graphs showing you how the cloud connectors are performing as well as the number of any throttling messages you are receiving.
- **User Data** - shows information about the user data that is being managed by File Director. If you are looking to perform a migration of storage or devices, you can check here to see if your companies user data is fully in-sync. There are also additional statistics shown on this dashboard which can give you a better understanding of how much user data users in your company typically has.
- **File Discovery** - shows information about the files discovered outside of the profile within your environment in the last 24 hours. From 2020.3 onwards, the outside of the profile scan can be enabled on the client and allows you to see the number of files and size of files outside the profile per user. If enabled, detailed reporting show file extensions and paths of these discovered files to allow you to better understand where and what type of files your users are storing outside of the profile.