T06-ELK Server and Client Setup Steps

Note that the client steps are presented up front so that the team can split tasking across its members and have an understanding of the dependencies. However, note that the client tasks cannot be completed fully until the ELK server setup is finalized and verified through the first two grading checks. The final grading check cannot be completed until at least one of each type of client is reporting in.

Client Setup

Note that the Winlogbeat and Filebeat shippers can be added and configured prior to or in tandem with the ELK server setup steps, but dashboards cannot be setup/loaded and logs cannot be shipped until the Elasticsearch/Kibana server steps are complete.

Configure Win10 clients with Winlogbeat

1. Create a folder in C:\Program Files (x86)\ named 'ELK'
2. Extract/copy the Winlogbeat files from the attached CD/DVD to an 'ELK' folder.
3. Open the winlogbeat.yml file for editing and make the following changes:

- Under the 'output.elasticsearch' section, change the hosts entry to match the public URL of this server
- Under the 'setup.kibana' section, change the host to match the public URL of this server

STOP HERE if you have not completed the server setup steps

4. In powershell, run '.\winlogbeat setup' to load the dashboard to Kibana. This command will verify your config changes and set up the dashboards. You should see a "Loaded dashboards" message once complete. This step also creates the winlogbeat index on the server towards passing Grading Check #3.
5. In powershell run '.\winlogbeat -e' to start shipping data

Leave this process running in the background.

Install and configure Ubuntu clients with Filebeat

1. Copy the Filebeat package from the attached CD/DVD to a directory of your choosing (it does not matter where)
2. Install Filebeat using 'sudo dpkg -i filebeat...'
3. Edit the config file located at /etc/filebeat/filebeat.yml and make the following changes:

- Set the enabled status of the 'filebeats.inputs' section to "true"

You may leave the default path of "/var/log/*log" but could add other paths for other types of information

- Modify the host entry to match the ELK server's settings under the Kibana section
- Modify the elasticsearch host field to match the ELK server's settings under the Elasticsearch Output section

4. Run 'sudo filebeat modules enable system' from /usr/bin to add the modules

STOP HERE if you have not completed the server setup steps

5. Run 'sudo filebeat setup' from /usr/bin to configure the dashboards. This may take a few minutes. You will see a similar "Loaded dashboards/Ingest pipelines" message to verify this task is complete. This step also creates the filebeat index on the server towards passing Grading Check #3.
6. Lastly, run 'sudo filebeat -e' from /usr/bin to start shipping data.

****Leave this process running in the background.****

Note that the shipping of logs can take a few minutes and you may not see all data immediately in Kibana.

ELK Server Setup

Step 1: Install Elasticsearch as a service

1. Install Elasticsearch from the MSI installer accepting all defaults except:

- Add a network host of "0.0.0.0"
- Check the box that this is the first master in a new cluster
- Add a discovery seed host of "[]"
- If you do not change these three settings here and now, you will need to edit the elasticsearch.yml file in C:\ProgramData\Elastic\Elasticsearch\config instead.

2. Confirm that Elasticsearch is running properly and accepts web connections over port 9200 on its publicly facing interface at 10.5.5.100, not just by browsing to localhost.

Barring any mistakes or misconfigurations, you should pass grading check #1 at this point and earn 15% of the total score for this task.

Step 2: Copy Kibana, configure, and run

1. Create a folder in C:\Program Files (x86)\ named 'ELK'
2. Copy/extract the Kibana files from the attached CD/DVD to this new folder
3. Open the config\kibana.yml file for editing and make the following changes:

- Uncomment the 'server.port' line, but leave the port as '5601'
- Uncomment the 'server.host' line and change the value to "0.0.0.0" (include the quotes)
- Uncomment the 'elasticsearch.hosts' line and make sure there are two entries of `http://localhost:9200` and "`http://10.5.5.100:9200` separated by a comma (include the quotes on each)

4. Using powershell (as the administrator), run the kibana.bat process in Kibana's bin directory.

If Kibana starts correctly, you should see "http server running at `http://0.0.0.0:5601`" near the end of the output. If Kibana gets stuck you might try restarting the Elasticsearch service and re-running kibana.bat.

Leave this process running in the background.

Confirm that Kibana is running properly and accepts web connections over port 5601 on its publicly facing interface on 10.5.5.100, not just by browsing to localhost.

Barring any mistakes or misconfigurations, you should pass grading check #2 at this point and earn 15% of the total score for this task

Note that you will need to set up Winlogbeat/Filebeat and begin shipping logs on at least one of the two Windows and Ubuntu clients first before moving on.

Step 3: Verify Winlogbeat data is loaded into Kibana

1. In the Kibana web GUI, click on the options (hamburger) button on the lefthand side near the "elastic" logo.
2. Select Discover under Analytics
3. Verify that the predefined 'winlogbeat-*' index is present in the dropdown list and that data appears from your two Win10 hosts when viewing it. This should occur naturally once one of the two systems begins shipping logs.

STEP 4: Verify that the Filebeat data is loaded into Kibana

Similar to the above step, you may need to add the Filebeat data index to Elasticsearch/Kibana.

1. In the Kibana web GUI, click on the options (hamburger) button on the lefthand side near the "elastic" logo.
2. Select Discover under Analytics
3. Verify that the predefined 'filebeat-*' index is present in the dropdown list and that data appears from your two Ubuntu hosts when viewing it. This should occur naturally once one of the two Ubuntu systems begins shipping logs.

If you do not see any data, remember to check that the time filter range is set properly, or that the winlogbeat/filebeat setup steps did not fail on the local clients.

You could also add these data indices manually in Kibana prior to this.

Barring any mistakes or misconfigurations, you should pass grading check #3 at this point and earn 20% of the total score for this task