Integrating the ELK Stack v5.0 with the Barracuda Web Application Firewall

https://campus.barracuda.com/doc/70584459/

The Elasticsearch, Logstash, and Kibana (ELK) stack is a robust log management platform. The ELK/Elastic stack is a combination of three (3) open-source tools: Elasticsearch, Logstash, and Kibana from Elastic. Elasticsearch is used for search and data analytics, Logstash for centralized logging and parsing, Kibana for data visualizations. You can install each tool either in a different server or all three tools in one server, and integrate with your existing applications. For more information on how to install and deploy the ELK Stack, refer to the Elastic website.

Ensure you download the ELK zip file and keep all scripts on your system before proceeding with ELK Stack configuration.

If you already have the ELK Stack installed on your instance/system, skip Step 1: Installing and Configuring ELK Stack. Also, note that the scripts provided in this article are supported only on Ubuntu systems. If you want to install and configure the ELK Stack on other systems, change the scripts accordingly.

Step 1: Install the ELK Stack on a Single System

- Run setup.bash on your system to install ELK Version 5 (v5).

Step 2: Configuring the ELK Stack

You can configure the ELK Stack on a system that has all the three (3) tools (Elasticsearch, Logstash, and Kibana) installed, or when each tool is installed on different systems.

Configure the ELK Stack on a System that Has All ELK Tools Installed

1. Edit elk_config.txt and provide the required attributes for configuring the ELK Stack.
2. Run initialize_elk.sh to configure the ELK Stack to integrate with the Barracuda Web Application Firewall.

Configure the ELK Stack When ELK Tools Are Installed on Different Systems

1. Edit elk_config.txt and provide the required attributes for configuring the ELK Stack.

2. To configure Logstash, run logstash_conf.sh on the system where Logstash is installed.
3. To configure Elasticsearch and Kibana, run elasticsearch_templates.sh and kibana_config.bash on the system where Elasticsearch is installed.

- The elk_config.txt file should be edited on the system(s) that has Logstash and Elasticsearch installed for the systems to work properly.
- To view the Kibana dashboard and other objects through the Kibana web interface, upload "kibana.json" in the Kibana web interface. Skip this if "kibana_config.bash" is executed in the system where Elasticsearch is installed.

Configure the ELK Stack Manually

1. Copy the "filter" and "output" logic from the 'waf.conf' file and paste it in the Logstash 'conf' file.
2. Run 'elasticsearch_templates.sh' to configure Elasticsearch index templates on the system where the Elasticsearch is installed. Also, ensure that the 'elk_config.txt' file exists and contains required attributes.
3. To view the Kibana dashboard and other objects through the Kibana web interface, perform any of the following:
    1. Run 'kibana_config.bash' on the system that has Elasticsearch installed to directly configure the Kibana index in Elasticsearch. Ensure that elk_config.txt exists and contains the required attributes.
    2. Upload "kibana.json" in the Kibana web interface.

It is highly recommended to complete the ELK Stack configuration first, and then proceed with the Barracuda Web Application Firewall configuration to send logs to Logstash.

For more information on how to install and deploy the ELK Stack, refer to the Elastic website.

Step 3: Configure the Barracuda Web Application Firewall to Send Logs to Logstash

1. Log into the Barracuda Web Application Firewall web interface.
2. Go to the **ADVANCED > Export Logs** page.
3. In the **Export Logs** section, click **Add Export Log Server**.
4. In the **Add Export Log Server** page, specify values for the following:
    - **Name** – Enter a name for the export log server.
    - **Log Server Type** – Select *Syslog NG*.
    - **IP Address or Hostname** – Enter the IP address or the hostname of the Logstash or ELK server.
    - **Port** – Enter the port number associated with the IP address of the Logstash or ELK server. By default, Logstash listens on port 1514 over UDP.

- Specify values for other parameters as required and click **Add**.

5. In the **Logs Format** section, specify values for the following:
   - **Syslog Header**– Select **ArcSight Log Header**.
   - **Web Firewall Logs Format**– Select **Custom Format** and add the log format given below:

     %header LogType=%lt ServiceIP=%ai ServicePort=%ap Action=%at AttackDetails=%adl AuthenticatedUser=%au ClientIP=%ci ClientPort=%cp Method=%m Protocol=%p Referer=%r StartTime=%ta DeviceReceiptTime=%tarc URL=%u UserAgent=%ua UnitName=%un EventID=%uid ProxyPort=%pp RuleID=%ri FollowUpAction=%fa RuleType=%rt AttackGroup=%ag ProxyIP=%px SessionID=%sid

   - **Access Logs Format** – Select **Custom Format** and add the log format given below:

     %header ServiceIP=%ai AuthenticatedUser=%au BytesReceived=%br BytesSent=%bs CertificateUser=%cu ClientIP=%ci ClientPort=%cp Cookie=%c WAF_Host=%h HTTPStatus=%s LoginID=%id LogType=%lt Method=%m Protocol=%p QueryString=%q Referer=%r ServerIP=%si ServerPort=%sp DeviceReceiptTime=%tarc StartTime=%ta URL=%u UserAgent=%ua UnitName=%un EventID=%uid ClientType=%ct Protected=%pf ProxyIP=%px ProfileMatched=%pmf WFMatched=%wmf ServicePort=%ap CacheHit=%ch ProxyPort=%pp ServerTime=%st TimeTaken=%tt ProtocolVersion=%v CustomHeader1=%cs1 CustomHeader2=%cs2 CustomHeader3=%cs3 ResponseType=%rtf SessionID=%sid

   - **Audit Logs Format**– Select **Custom Format** and add the log format given below:

     %header LogType=%lt ObjectName=%on ObjectType=%ot AdminName=%an ClientType=%ct CommandName=%cn LoginIP=%li LoginPort=%lp DeviceReceiptTime=%tarc EventMessage=%add ChangeType=%cht UnitName=%un StartTime=%ta TransactionID=%tri NewValue=%nv OldValue=%ov Variable=%var EventID=%uid AdminRole=%ar

   - **Network Firewall Logs Format** – Select **Custom Format** and add the log format given below:

     %header LogType=%lt SourceIP=%srci SourcePort=%srcp DestinationIP=%di DestinationPort=%dp ActionID=%act StartTime=%ta UnitName=%un Protocol=%p DeviceReceiptTime=%tarc Details=%dsc EventID=%uid

   - **System Logs Format** – Select **Custom Format** and add the log format given below:

     %header LogType=%lt DeviceReceiptTime=%tarc EventID=%uid EventMessage=%ms UnitName=%un StartTime=%ta

6. Click **Save**.

Step 4: Access the Kibana Web Interface to View the Logs

1. Kibana can be accessed at *https://localhost:5601/app/kibana* or *https://<IP address used for*

KIBANA Installation>:5601/app/kibana.

2. The **Discover** tab displays the logs in detail. Navigate to the **Visualize** and the **Dashboard** tabs to view the following nine (9) saved visualizations:
    - **Attack_Origins**: Displays the geographical location from where the attacks originated.
    - **Attacks**: Displays the attack type and the total count for the attack type in the selected time frame.
    - **Attacks_Last_Day**: Displays all attack types and the count for all attacks in the last day.
    - **Attacks_Last_Hour**: Displays all attack types and the count for all attacks in the last hour.
    - **Attacks_Total**: Displays all attack types and the total count for all attacks.
    - **Response_Time_Graph**: Displays the average response time taken by each service.
    - **Top_Attacked_Domains**: Displays the count of top attacked domains based on the number of times each service has been attacked.
    - **Top_Attacked_URLs**: Displays the count of top attacked URLs based on the number of times each URL has been attacked.
    - **User_Agents_Per_Service**: Displays the count of user agents.

- By default, **Elasticsearch** and **Kibana** are configured to listen on localhost, which should be configured in '*elasticsearch.yml*' and '*kibana.yml*' as per your requirements.
- By default, **Elasticsearch** listens on port 9200 with tcp6 protocol for IPv6. In case of IPv4, add the following line in the **/etc/elasticsearch/jvm.options** file and restart Elasticsearch:
    - *-Djava.net.preferIPv4Stack=true*