Mandiant

LOGRHYTHM ELASTICSEARCH

> This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview** (https://docs.mandiant.com/home/msv-integrations-overview).

This integration is remote capable.

Update LogRhythm Elasticsearch

Prerequisites

1. Ensure network connectivity between the DX and the Security Validation Director.
2. Identify the IP address used to access Elasticsearch. This could be direct access to an Elasticsearch node, Primary node, or something such as an nginx reverse proxy.

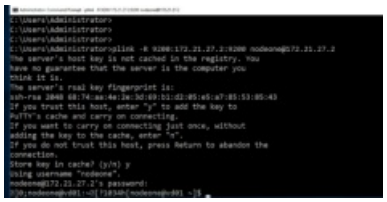
Configuration

Complete the following steps on the LogRhythm Server (if single-tiered deployment) or DX (administrative access not required).

On the LogRhythm Server

SSH from the LogRhythm DX to the Validation Platform Director.

- On a Microsoft(R) Windows(R) host, plink.exe can be used as follows:
  `plink -R 9200:localhost:9200 nodeone@DIRECTORIP`
- If linux DX, use normal ssh instead of plink:
  `ssh -N -R 9200:localhost:9200 nodeone@DIRECTORIP`



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12ecc9cba0017c2f7ea1/n/lge-step1.png)

SSH from LogRhythm to the Validation Platform Director

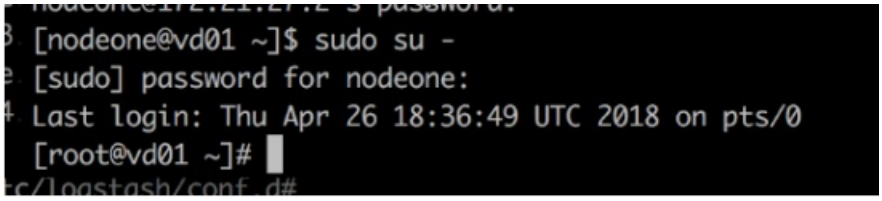
On the Validation Platform Director (CLI)

1. SSH to the Security Validation Director using the "nodeone" password.
   a. `ssh nodeone@DIRECTOR_IP`

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12eac9cba0017c2f7e93/n/lge-step2.png)

SSH to the Validation Platform Director using nodeone password

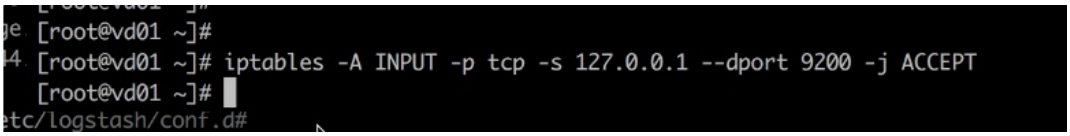
2. Assume root access.
    a. `sudo su -`



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12ebc9cba0017c2f7e98/n/lge-step3.png)

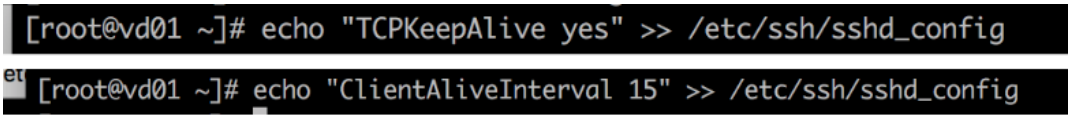
Assume root access

3. Add the following custom iptables rule to allow communication to Elastic over the SSH tunnel:
    a. `iptables -A INPUT -p tcp -s 127.0.0.1 --dport 9200 -j ACCEPT`



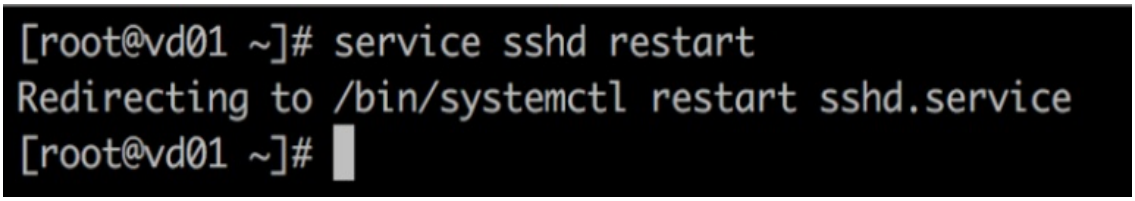
Add iptables Rules

4. Add the following configuration lines to `/etc/ssh/sshd_config`.
    a. `TCPKeepAlive yes`
    b. `ClientAliveInterval 15`



Configure Keepalive

5. Restart the SSH service.
    `service sshd restart`



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12efc9cba0017c2f7ec7/n/lge-step6.png)

Restart SSH service

Update the Validation Platform

Prerequisites

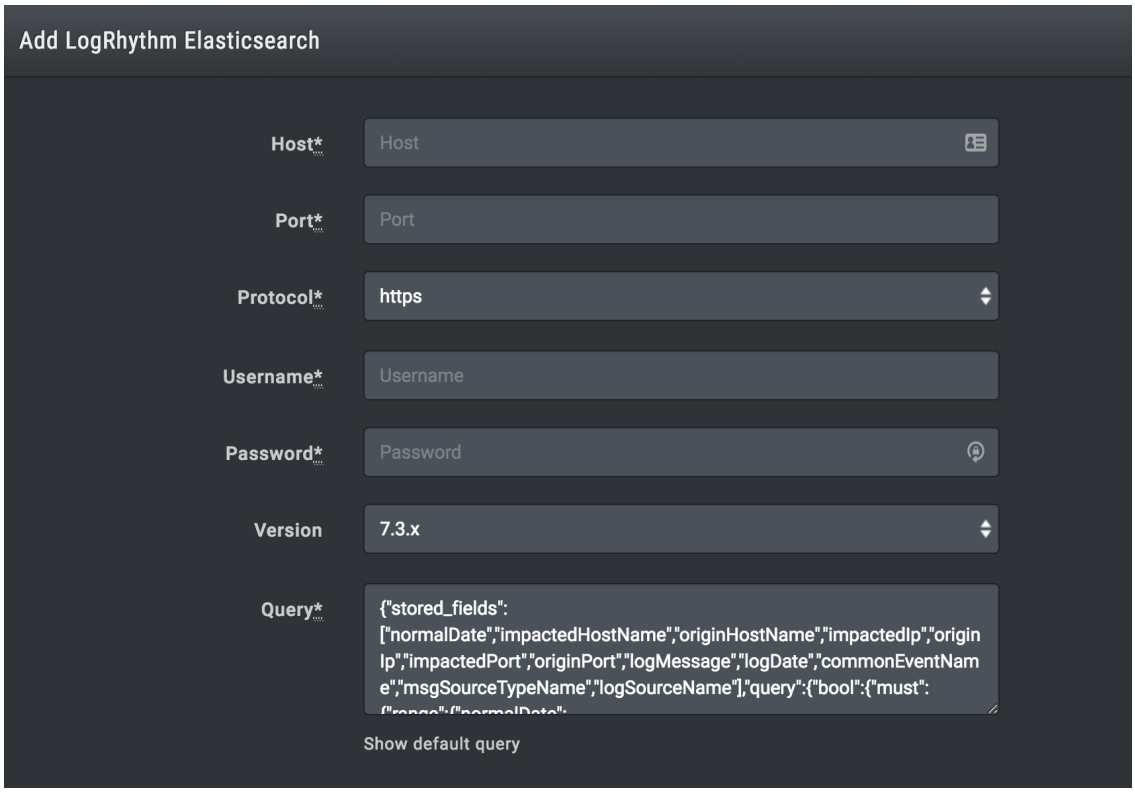
Information to gather before you start:

1. Identify the port for Elasticsearch communication (default is 9200).
2. Identify whether the protocol is HTTP or HTTPS for connections to the Elasticsearch port.
3. Identify the field name mappings for the following (there could be multiple of each, depending on log sources and configuration):
    - Source IP
    - Destination IP
    - Source Port
    - Destination Port
    - Event Start Time (timestamp)
    - Event Unique ID
    - Event Signature ID
    - Event Description
    - Event Source Host

Configuration

TO ADD THE LOGRHYTHM ELASTICSEARCH INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **LogRhythm Elasticsearch**.



LogRhythm Elasticsearch Integration

3. Enter the **Host**.

   This will almost always be either "localhost" or "127.0.0.1".

4. Enter the **Port**, **Protocol**, and if using, the **Username** and **Password**.
5. Select the appropriate version.

   This may adjust the default query and field name mapping section.

6. Review and update the **Query**, if necessary.
7. Expand **Advanced options**.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12dec9cba0017c2f7e24/n/logrhythm-elasticsearch-advanced.png)

LogRhythm Elasticsearch Integration (Advanced Options)

8. (Optional) Update **Query time** and **Delay time**.

   The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

   If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

9. (Optional) Enable the special query for Host CLI Actions and review the **Query**.

   If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

10. (Optional) Select **Discover network devices automatically**.
11. Review and update the field name mapping section.
    a. Inputs are enclosed by square brackets `[ ]`.
    b. Inputs point to the path location (`["_id"]`).
    c. Nested locations should be enclosed in one set of brackets, encompassed in quotes, and separated by commas (`["_source","src_ip"]`).
12. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
13. (Optional) Assign a **Name**.

14. (Optional) Choose **Yes** to save suspicious events.
15. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO LOGRHYTHM ELASTICSEARCH

Click **Test** to verify that:

- The Director can communicate with the Elasticsearch host IP address on the port specified.
- The Elasticsearch credentials can perform queries on the index or indexes with relevant data.

Updating the Integration

If you update LogRhythm, you will need to update the integration within the Validation Platform. Modifying the version may adjust the default query and the field name mapping section.

Any changes you made previously to the query and field mapping will be retained. Review the default query and the field name mapping sections to verify that no additional changes are required.