Troubleshooting command for logstash

If you have installed Logstash on a RPM-based Linux distribution (such as CentOS, RHEL, or Fedora) using the RPM package, you can use the following troubleshooting commands:

Step-1 : Check Logstash service status: You can use the following command to check the status of the Logstash service to ensure it is running:

```
systemctl status logstash
```

Step-2 : Restart Logstash service: You can use the following command to restart the Logstash service:

```
systemctl restart logstash
```

Step-3 : View Logstash service logs: You can use the following command to view the logs of the Logstash service to identify any error messages or warnings:

```
journalctl -fu logstash
```

Step-4 : Verify Logstash configuration syntax: You can use the following command to check the syntax of your Logstash configuration file(s) for any errors or typos:

```
/usr/share/logstash -t -f /etc/logstash/logstash.conf
```

Step-5 : Enable Logstash debug mode: You can use the following command to enable Logstash debug mode, which provides more detailed logging for troubleshooting purposes:

```
/usr/share/logstash -f /etc/logstash/logstash.conf --debug
```

Step-6 : Check Logstash plugin version: You can use the following command to check the version of a specific Logstash plugin:

```
/usr/share/logstash/bin/logstash-plugin list --verbose | grep <plugin-name>
```

Step-7 : Check sometime logstash restart command will not work then follow below mentioned steps

Find the process ID (PID) of the Logstash process using a command such as "ps" or "pgrep". For example:

```
ps aux | grep logstash
```

Once you have the PID of the Logstash process, use the "kill" command with the PID and the desired signal. For example:

```
kill -15 <PID> or kill -9 <PID>
```

where <PID> is the PID of the Logstash process.

The SIGTERM signal (15) is a soft termination signal that allows Logstash to perform cleanup operations before exiting gracefully. If you need to forcefully kill Logstash without giving it a chance to perform cleanup, you can use the SIGKILL signal (9) instead. However, using SIGKILL should be avoided unless absolutely necessary, as it can result in data loss or other undesirable consequences.

Please note that forcefully killing the Logstash process using "kill" or similar tools should be done with caution and only in exceptional situations where other methods for stopping Logstash gracefully are not working or feasible. It's generally best to use the appropriate methods to stop Logstash gracefully to ensure safe and reliable operation.

Note: The paths mentioned in the commands above are based on the default installation paths for Logstash on RPM-based Linux distributions. If you have installed Logstash in a different location, please adjust the paths accordingly.