

Logstash Cheatsheet

Installation and Setup

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -  
Add Elastic GPG key  
  
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list  
Add Elastic repository  
  
sudo apt-get update && sudo apt-get install logstash  
Install Logstash  
  
sudo systemctl enable logstash.service  
Enable Logstash service to start at boot
```

Service Management

```
sudo systemctl start logstash  
Start Logstash service  
  
sudo systemctl stop logstash  
Stop Logstash service  
  
sudo systemctl restart logstash  
Restart Logstash service  
  
sudo systemctl status logstash  
Check Logstash service status
```

Configuration

```
vi /etc/logstash/logstash.yml  
Edit main configuration file  
  
vi /etc/logstash/pipelines.yml  
Edit pipeline configuration  
  
vi /etc/logstash/conf.d/*.conf  
Edit pipeline configuration files  
  
sudo -u logstash /usr/share/logstash/bin/logstash --path.settings /etc/logstash -t  
Test configuration validity
```

Pipeline Creation

```
input { ... }  
Define input sources (e.g., file, beats, jdbc)  
  
filter { ... }  
Define filters (e.g., grok, mutate, date)  
  
output { ... }  
Define outputs (e.g., elasticsearch, stdout, file)
```

Running Directly

```
/usr/share/logstash/bin/logstash -e 'input { stdin { } } output { stdout { } }'  
Run simple pipeline from command line  
  
/usr/share/logstash/bin/logstash -f /path/to/config.conf  
Run Logstash with specific config file  
  
/usr/share/logstash/bin/logstash --config.reload.automatic  
Enable automatic config reloading
```

Monitoring

```
curl -XGET 'localhost:9600/_node/stats'  
Get Logstash stats  
  
curl -XGET 'localhost:9600/_node/hot_threads'  
Get information about hot threads  
  
curl -XGET 'localhost:9600/?pretty'  
Get basic node info
```

Plugin Management

```
/usr/share/logstash/bin/logstash-plugin list  
List installed plugins  
  
/usr/share/logstash/bin/logstash-plugin install logstash-input-http  
Install a plugin  
  
/usr/share/logstash/bin/logstash-plugin update logstash-input-http  
Update a plugin  
  
/usr/share/logstash/bin/logstash-plugin remove logstash-input-http  
Remove a plugin
```

Debugging

```
/usr/share/logstash/bin/logstash --debug  
Run with debug output  
  
/usr/share/logstash/bin/logstash --verbose  
Run with verbose output  
  
/usr/share/logstash/bin/logstash --log.level=debug  
Set log level to debug  
  
tail -f /var/log/logstash/logstash-plain.log  
View Logstash logs
```