GNU/Linux Administration - Support #416

Installing Logstash on Debian

07/11/2014 11:00 AM - Daniel Curtis

Status:	Suspended	**Start date:**	07/11/2014
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	40%
Category:	Logging Server	**Estimated time:**	3.00 hours
Target version:	Debian	**Spent time:**	2.00 hours

Description

This is a guide for install Logstash with kibana, elasticsearch, and nginx on Debian 8

Prepare the Environment

- Make sure the system is up to date;

```
sudo apt-get update && sudo apt-get upgrade
```

- Install openjdk:

```
sudo apt-get install openjdk-7-jdk
```

- Run the following command to import the Elasticsearch public GPG key into apt:

```
wget -O - http://packages.elasticsearch.org/GPG-KEY-elasticsearch | sudo apt-key add -
```

Install Elasticsearch

- Create the Elasticsearch source list:

```
echo "deb http://packages.elastic.co/elasticsearch/2.x/debian stable main" | sudo tee -a /etc/apt/sources.list.d/elasticsearch-2.x.list
```

- Update your apt package database:

```
sudo apt-get update
```

- Install Elasticsearch:

```
sudo apt-get install elasticsearch
```

- Elasticsearch is now installed. Let's edit the configuration:

```
sudo vi /etc/elasticsearch/elasticsearch.yml
```

  - Add the following line somewhere in the file, to disable dynamic scripts:

```
script.disable_dynamic: true
```

- You will also want to restrict outside access to your Elasticsearch instance (port 9200), so outsiders can't read your data or shutdown your Elasticseach cluster through the HTTP API. Find the line that specifies network.bind_host and uncomment it so it looks like this:

```
network.bind_host: localhost
```

- Now start Elasticsearch:

```
sudo service elasticsearch restart
```

- Then run the following command to start Elasticsearch on boot up:

```
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service
```

Install Logstash

- The Logstash package is available from the same repository as Elasticsearch, and we already installed that public key, so let's create the Logstash source list:

```
echo "deb http://packages.elastic.co/logstash/2.0/debian stable main" | sudo tee -a /etc/apt/sources.list.d/logstash-2.0.list
```

- Update your apt package database:

```
sudo apt-get update
```

- Install Logstash:

```
sudo apt-get install logstash
```

Configure Logstash

- Now let's create a configuration file called 10-syslog.conf, where we will add a filter for syslog messages:

```
sudo vi /etc/logstash/conf.d/10-syslog.conf
```

1. Insert the following syslog filter configuration:

```
filter {
  if [type] == "syslog" {
    grok {
      match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp} %{SYSLOGHOST:syslog_hostname} %{DATA:syslog_program}(?:\[%{POSINT:syslog_pid}\])?: %{GREEDYDATA:syslog_message}" }
      add_field => [ "received_at", "%{@timestamp}" ]
      add_field => [ "received_from", "%{host}" ]
    }
    syslog_pri { }
    date {
      match => [ "syslog_timestamp", "MMM  d HH:mm:ss", "MMM dd HH:mm:ss" ]
    }
  }
}
```

Save and quit. This filter looks for logs that are labeled as "syslog" type (by a Logstash Forwarder), and it will try to use "grok" to parse incoming syslog logs to make it structured and query-able.

- Restart Logstash to put our configuration changes into effect:

```
sudo service logstash restart
```

Install Kibana

- Download Kibana to your home directory with the following command:

```
cd ~; wget http://download.elasticsearch.org/kibana/kibana/kibana-latest.zip
```

- Install unzip so you can extract the kibana archive:

```
sudo apt-get install unzip
```

- Extract Kibana archive with unzip:

```
unzip kibana-latest.zip
```

- Open the Kibana configuration file for editing:

```
sudo vi ~/kibana-latest/config.js
```

  - In the Kibana configuration file, find the line that specifies the elasticsearch, and replace the port number (9200 by default) with 80:

    ```
    elasticsearch: "http://"+window.location.hostname+":80",
    ```

This is necessary because we are planning on accessing Kibana on port 80.

- Create a directory with the following command:

```
sudo mkdir -p /var/www/kibana
```

- Now copy the Kibana files into your newly-created directory:

```
sudo cp -R ~/kibana-latest/* /var/www/kibana/
```

Before we can use the Kibana web interface, we have to install Nginx.

Install Nginx

- Use apt to install Nginx:

```
sudo apt-get install nginx
```

- Download the sample Nginx configuration from Kibana's github repository to your home directory:

  ```
  cd ~; wget https://github.com/elasticsearch/kibana/raw/master/sample/nginx.conf
  ```

- Open the sample configuration file for editing:

  ```
  vi nginx.conf
  ```

  - Find and change the values of the server_name to your FQDN (or localhost if you aren't using a domain name) and root to where we installed Kibana, so they look like the following entries:

    ```
    server_name logstash.example.com;
    root /var/www/kibana;
    ```

- Save and exit. Now copy it over your Nginx default server block with the following command:

  ```
  sudo cp nginx.conf /etc/nginx/sites-available/default
  ```

- Now restart Nginx to put our changes into effect:

  ```
  sudo service nginx restart
  ```

Kibana is now accessible via your FQDN or the public IP address of your Logstash Server i.e. http://logstash.example.com/. If you go there in a web browser, you should see a Kibana welcome page which will allow you to view dashboards but there will be no logs to view because Logstash has not been set up yet. Let's do that now.

Generate SSL Certificates

Since we are going to use Logstash Forwarder to ship logs from our Servers to our Logstash Server, we need to create an SSL certificate and key pair. The certificate is used by the Logstash Forwarder to verify the identity of Logstash Server.

- Create the directories that will store the certificate and private key with the following commands:

  ```
  sudo mkdir -p /etc/pki/tls/certs
  sudo mkdir /etc/pki/tls/private
  ```

- Now generate the SSL certificate and private key, in the appropriate locations (/etc/pki/tls/...), with the following command:

  ```
  cd /etc/pki/tls; sudo openssl req -x509 -batch -nodes -newkey rsa:2048 -keyout private/logstash-forwarder.key -out certs/logstash-forwarder.crt
  ```

The logstash-forwarder.crt file will be copied to all of the servers that will send logs to Logstash but we will do that a little later. Let's complete our Logstash configuration.

Connect to Kibana

When you are finished setting up Logstash Forwarder on all of the servers that you want to gather logs for, let's look at Kibana, the web interface that we installed earlier.

In a web browser, go to the FQDN or public IP address of your Logstash Server. You should see a Kibana welcome page.

Click on Logstash Dashboard to go to the premade dashboard. You should see a histogram with log events, with log messages below (if you don't see any events or messages, one of your four Logstash components is not configured properly).

Here, you can search and browse through your logs. You can also customize your dashboard.

Try the following things:

- Search for "root" to see if anyone is trying to log into your servers as root
- Search for a particular hostname
- Change the time frame by selecting an area on the histogram or from the menu above
- Click on messages below the histogram to see how the data is being filtered

Kibana has many other features, such as graphing and filtering, so feel free to poke around!

Resources

- https://www.elastic.co/guide/en/kibana/current/setup.html
- https://www.elastic.co/guide/en/elasticsearch/reference/current/setup-repositories.html
- https://www.elastic.co/guide/en/logstash/current/package-repositories.html
- https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-ubuntu-14-04

History

#1 - 07/11/2014 11:59 AM - Daniel Curtis

- Description updated

#2 - 07/11/2014 05:11 PM - Daniel Curtis

- Description updated

#3 - 07/11/2014 06:05 PM - Daniel Curtis

- Description updated

#4 - 02/15/2015 09:07 PM - Daniel Curtis

- Project changed from 90 to GNU/Linux Administration

- Category set to Logging Server

#5 - 11/15/2015 07:52 PM - Daniel Curtis

- Description updated

#6 - 11/15/2015 08:14 PM - Daniel Curtis

- Description updated

- Status changed from New to In Progress

- Target version set to Debian

- % Done changed from 100 to 40

#7 - 06/04/2017 08:23 PM - Daniel Curtis

- Status changed from In Progress to Suspended