GNU/Linux Administration - Support #415

Install an ElasticSearch, Logstash, Kibana (ELK) Stack on Arch Linux

07/10/2014 06:12 PM - Daniel Curtis

Status:	Closed	**Start date:**	07/10/2014
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Logging Server	**Estimated time:**	2.00 hours
Target version:	Arch Linux	**Spent time:**	3.00 hours

Description

This is a guide for installing an ElasticSearch, Logstash, and Kibana stack on Arch Linux.

Prepare the Environment

- Make sure the system is up to date:

```
sudo pacman -Syu
```

- Install yaourt

Install ElasticSearch

- Install ElasticSearch:

```
sudo pacman -S elasticsearch
```

- Enable cross origin access:

```
sudo echo 'http.cors.allow-origin: "/.*/"' >> /etc/elasticsearch/elasticsearch.yml
sudo echo 'http.cors.enabled: true' >> /etc/elasticsearch/elasticsearch.yml
```

- Start and enable ElasticSearch at boot:

```
sudo systemctl enable elasticsearch.service
sudo systemctl start elasticsearch.service
```

Install Logstash

- Install Logstash from the AUR:

```
yaourt logstash
```

- Now create a simple configuration file:

```
sudo vi /etc/logstash/conf.d/logstash-simple.conf
```

  - And add the following:

```
input {
```

```
  file {
    path => "/var/log/faillog"
    start_position => beginning
  }

  # network syslog input
  syslog {
    host => "0.0.0.0"
    port => 514
  }

}

output {
  elasticsearch { host => localhost }
}
```

- Start and enable the Logstash agent:

```
sudo systemctl enable logstash.service
sudo systemctl start logstash.service
```

- Start and enable the Logstash web interface:

```
sudo systemctl enable logstash-web.service
sudo systemctl start logstash-web.service
```

Install Kibana

- Install Kibana from the AUR:

```
yaourt kibana
```

- Start and enable kibana at boot:

```
sudo systemctl enable kibana.service
sudo systemctl start kibana.service
```

Install Nginx

- Install nginx:

```
sudo pacman -S nginx
```

- Install Apache Tools from the AUR:

```
yaourt apache-tools
```

  - **NOTE**: The AUR package was a little stale, I needed to edit the PKDBUILD and change the following:

```
pkgver=2.4.12
sha256sums=('ad6d39edfe4621d8cc9a2791f6f8d6876943a9da41ac8533d77407a2e630eae4'
'2dc48d34773b0c873d10e3542f77a4f7b50d5fb9bd8c52e3bb28b76ff9587f3f')
```

```
sha512sums=('f69db14b421f0e1e4861fe4d8b652688d50ca9eb41c622242d11ae55687eb6c2142a8505a8c3f
b6f2bd53167be535bc0a77ca1af97e0720930fc7f20f4c1f8e8'
'6e068e7820e852c788a521ad28c367af4c1c22fded51ede7ae3f840a8a04737cfbe4503c2f3f899c89461d984
007e84f80376b5a8a27c7eec8ec0fd78155c22b')
```

- Edit the nginx config:

```
sudo vi /etc/nginx/nginx.conf
```

  - And add the following server block:

```
# Nginx proxy for Elasticsearch + Kibana
#
server {
    listen                80;
    server_name           localhost;
    access_log            /var/log/nginx-logstash.log;

    auth_basic "Restricted Access";
    auth_basic_user_file /etc/webapps/kibana/htpasswd.users;

    location / {
        proxy_pass http://localhost:5601;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection 'upgrade';
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
    }
}
```

- Then generate a htpasswd file:

```
sudo htpasswd -c -b /etc/webapps/kibana/htpasswd.users username SuperSecretPassword
```

- Start and enable nginx at boot;

```
sudo systemctl enable nginx.service
sudo systemctl start nginx.service
```

History

#1 - 02/15/2015 09:07 PM - Daniel Curtis

- Project changed from 90 to GNU/Linux Administration

- Category set to Logging Server

#2 - 05/02/2015 12:53 PM - Daniel Curtis

- Subject changed from Installing Logstash on Arch Linux to Install an ElasticSearch, Logstash, Kibana (ELK) Stack on Arch Linux

- Description updated

- Target version set to Arch Linux

- % Done changed from 100 to 20

#3 - 05/02/2015 04:27 PM - Daniel Curtis

- Description updated

- % Done changed from 20 to 60

#4 - 05/02/2015 07:49 PM - Daniel Curtis

- Description updated

- % Done changed from 60 to 90

#5 - 06/09/2015 04:49 PM - Daniel Curtis

- Status changed from In Progress to Resolved

- % Done changed from 90 to 100

#6 - 06/12/2015 10:31 AM - Daniel Curtis

- Status changed from Resolved to Closed

#7 - 07/15/2016 07:48 PM - Daniel Curtis

- Description updated