
Logging in to AWS instance

```
--- 34.194.227.66 ping statistics ---
6 packets transmitted, 0 packets received, 100.0% packet loss
[Toms-iMac:~ tommarler$ ssh ubuntu@34.194.227.66 -i ~/.ssh/dictatorship-in-a-box.pem
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-1038-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

16 packages can be updated.
0 updates are security updates.

*** System restart required ***
Last login: Tue Nov 14 19:33:30 2017 from 128.206.251.39
ubuntu@ip-10-0-0-42:~$
```

ServerContainer

- Navigate to /ServerContainer and run
 - build -t server/securityonion
 - [Network-Research/EvilBox/Images/SecurityOnionServices.pn](#)

```
$PREFIX/etc/node.cfg -- configure network interface to monitor
$PREFIX/etc/networks.cfg -- configure local networks
$PREFIX/etc/broctl.cfg -- change MailTo address and the log rotation
```

BRO INSTALL

- Now lets get started on the Bro IDS Installation under Ubuntu 16.04

Grab the required packages using apt.

```
apt install cmake make gcc g++ flex bison libpcap-dev libssl-dev python-dev swig zlib1g-dev libgeoip-dev
```

As you can see we have included the `libgeoip-dev` package as we are going to configure our installation with GeoIP support.

```
wget http://geolite.maxmind.com/download/geoip/database/GeoLiteCity.dat.gz
wget http://geolite.maxmind.com/download/geoip/database/GeoLiteCityv6-beta/GeoLiteCityv6.dat.gz
gzip -d GeoLiteCity.dat.gz
gzip -d GeoLiteCityv6.dat.gz
```

Now move the GeoIP files over to the default location `/usr/share/GeoIP/`, we need to rename them to match the location that Bro is expecting.

```
mv GeoLiteCity.dat /usr/share/GeoIP/GeoIPCity.dat
mv GeoLiteCityv6.dat /usr/share/GeoIP/GeoIPCityv6.dat
```

Install Bro on Ubuntu from package

```
sh -c "echo 'deb http://download.opensuse.org/repositories/network:/bro/xUbuntu_16.04/ '/' > /etc/apt/sources
.list.d/bro.list"
apt update
apt install bro
```

Install Bro on Ubuntu from source

Install Bro on Ubuntu from source

Download the source, extract and use the standard **configure, make, make install**.

```
wget https://www.bro.org/downloads/bro-2.5.1.tar.gz

tar zxvf bro-2.5.1.tar.gz
cd bro-2.5.1
./configure
make
make install
```

No errors? Good now add bro to your PATH.

```
export PATH=/usr/local/bro/bin:$PATH
```

You can also add `PATH=/usr/local/bro/bin:$PATH` to your `~/.profile` file in your home directory to make the change permanent.

Bro is a powerful tool, to get started quickly we will follow the [guide on the project page](#).

Edit the following files before starting:

```
$PREFIX/etc/node.cfg -- configure network interface to monitor
$PREFIX/etc/networks.cfg -- configure local networks
$PREFIX/etc/broctl.cfg -- change MailTo address and the log rotation
```

To start the program simply enter `broctl` at a shell.

=====| Bro Build Summary |=====

Build type: RelWithDebInfo
Build dir: /root/bro/build
Install prefix: /usr/local/bro
Bro Script Path: /usr/local/bro/share/bro
Debug mode: false

CC: /usr/bin/cc
CFLAGS: -Wall -Wno-unused -O2 -g -DNDEBUG
CXX: /usr/bin/c++
CXXFLAGS: -Wall -Wno-unused -std=c++11 -O2 -g -DNDEBUG
CPP: /usr/bin/c++

Broker: false
Broker Python: false
Broccoli: true
Broctl: true
Aux. Tools: true

GeoIP: true
gperftools found: false
 tcmalloc: false
 debugging: false
jemalloc: false

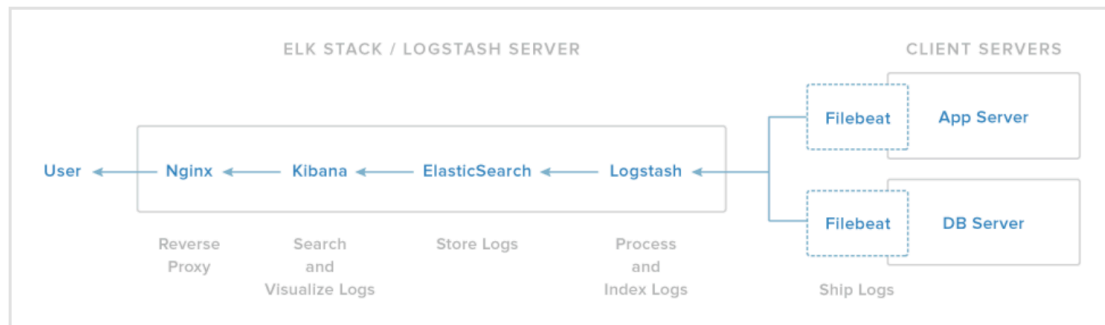
=====

-- Configuring done
-- Generating done
-- Build files have been written to: /root/bro/build
root@d8909c5d3e43:~/bro# █

ELKStack

Our ELK stack setup has four main components:

- **Logstash:** The server component of Logstash that processes incoming logs
- **Elasticsearch:** Stores all of the logs
- **Kibana:** Web interface for searching and visualizing logs, which will be proxied through Nginx
- **Filebeat:** Installed on client servers that will send their logs to Logstash, Filebeat serves as a log shipping agent that utilizes the *lumberjack* networking protocol to communicate with Logstash



Java 8 Install

I am trying to download java8 it is a dependency that the Elkstack relies on

- Elkstack includes - Kibana, Logstash and elastic search
 - 1. Build Dockerfile for elkstack install
 - update and upgrade system and app ppa

```
## Elk Stack
FROM ubuntu:16.04

CMD "This is from the Metric Container debian:latest with ELK Stack"

# Update the System
RUN apt-get -y update && apt-get -y upgrade \
    software-properties-common \
    nano

# Install Java
RUN add-apt-repository -y ppa:webupd8team/java
RUN apt-get update
RUN apt-get -y install oracle-java8-installer
```

- 2. Run `docker build -t metric/elkstack .` received an error and try to manually installed Java8 by `/bin/bash`

- For some reason Oracle needs the user to type yes and I guess -y command does not work for this.

```

Configuring oracle-java8-installer
-----
Oracle Binary Code License Agreement for the Java SE Platform Products and JavaFX

You MUST agree to the license available in http://java.com/license if you want to use Oracle JDK.

In order to install this package, you must accept the license terms, the "Oracle Binary Code License Agreement for the Java SE Platform Products and JavaFX ". Not accepting will cancel the installation.

Do you accept the Oracle Binary Code license terms? [yes/no] y

debconf: falling back to frontend: Teletype
Configuring oracle-java8-installer
-----
Oracle Binary Code License Agreement for the Java SE Platform Products and
JavaFX

You MUST agree to the license available in http://java.com/license if you want
to use Oracle JDK.

In order to install this package, you must accept the license terms, the
"Oracle Binary Code License Agreement for the Java SE Platform Products and
JavaFX ". Not accepting will cancel the installation.

Do you accept the Oracle Binary Code license terms? [yes/no]
Use of uninitialized value $_[1] in join or string at /usr/share/perl5/Debconf/DbDriver/Stack.pm line 111.
Declined "Oracle Binary Code License for Java"

If you do not agree to the license terms you cannot install this software.

The installation of this package will be canceled.

user did not accept the oracle-license-v1-1 license
Use of uninitialized value $val in substitution (s///) at /usr/share/perl5/Debconf/Format/822.pm line 83, <GEN6> line 9.
Use of uninitialized value $val in concatenation (.) or string at /usr/share/perl5/Debconf/Format/822.pm line 84, <GEN6> line 9.
dpkg: error processing archive /var/cache/apt/archives/oracle-java8-installer_8u151-1-webupd8-0_all.deb (--unpack):
 subprocess new pre-installation script returned error exit status 1
Errors were encountered while processing:
 /var/cache/apt/archives/oracle-java8-installer_8u151-1-webupd8-0_all.deb
E: Sub-process /usr/bin/dpkg returned an error code (1)
The command '/bin/sh -c apt-get --yes install oracle-java8-installer' returned a non-zero code: 100
Toms-iMac:Elkstack tommarler$

```

Tire

--force-yes

Force yes. This is a dangerous option that will cause **apt-get** to continue without prompting if it is doing something potentially harmful. It should not be used except in very special situations. Using **force-yes** can potentially destroy your system!

Configuration Item: *APT::Get::force-yes.*

-y, --yes, --assume-yes

Automatic yes to prompts. Assume "yes" as answer to all prompts and run non-interactively. If an undesired situation, such as changing a held package or removing an essential package, occurs then **apt-get** will abort.

Configuration Item: *APT::Get::Assume-Yes.*

Solution

<https://askubuntu.com/questions/190582/installing-java-automatically-with-silent-option>

If OpenJDK/OpenJRE works fine for you, I recommend using that package instead as suggested by @SAM. However, some software really requires Oracle's JDK/JRE. This answer is how to silence the license question with the Oracle package from the PPA.

First, let's recognize the question asked is a *feature* of the package, created by the developer.

```
oracle-java7-installer (7u7-0~webupd8~4) maverick; urgency=medium

* removed cookie file use or else the PPA stays disabled
* request the user to accept the Oracle license before installation
-- Alin Andrei <webupd8@gmail.com>   Tue, 04 Sep 2012 14:18:29 +0200
```

As @Nate indicated in his answer, there should be a silent option. And there is. Do this before installing it:

```
$ echo debconf shared/accepted-oracle-license-v1-1 select true | \
  sudo debconf-set-selections
$ echo debconf shared/accepted-oracle-license-v1-1 seen true | \
  sudo debconf-set-selections
```

This sets the value of the debconf key to true, but also marks it as seen by the user. Now this question should not appear!

How did I find this?

In the source of the package, I tracked this down in the `oracle-java7-installer.preinst` file:

```
license=oracle-license-v1-1

# snip

db_get shared/accepted-$license
if [ "$RET" = "true" ]; then
    echo "$license license has already been accepted" >&2
    exit 0
fi
```

Apparently, it uses debconf's value for the key `shared/accepted-oracle-license-v1-1` to check whether the user has already accepted the license. If it is, the script will exit gracefully and allow the installation to continue without asking you the question. We should now just tell debconf you already accept the Oracle Licence 1.1.

Please refer to the manpage of `debconf-set-selections` on more details, but this is the example for your issue and works similar for other packages. What other keys do you have on your system in debconf's database? Install `debconf-utils` and do

```
$ sudo debconf-get-selections
```

Then grep for more keys you need to set in your automated installation. This is way more flexible than using `-y` with `apt-get` as it gives you the opportunity to set other than default settings on installation times.

Java Installed

- docker build -t metric/elkstack
- docker run -itd metric/elkstack /bin/bash
- docker attach metric/elkstack
- java -version

```
root@92f9d4f12acb:/#  
[root@92f9d4f12acb:/# java -version  
java version "1.8.0_151"  
Java(TM) SE Runtime Environment (build 1.8.0_151-b12)  
Java HotSpot(TM) 64-Bit Server VM (build 25.151-b12, mixed mode)  
root@92f9d4f12acb:/#
```

```
# Elasticsearch repo added  
## Get elasticsearch signed key  
### Update and upgrade  
RUN echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main" | tee -a /etc/apt/sources.list.d/elasticsearch-5.x.list  
RUN wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add - \&& apt-get update && apt-get upgrade  
  
RUN apt-get -y install elasticsearch \&& service elasticsearch start \&& service elasticsearch status
```

```
Failed to connect to bus: No such file or directory  
Processing triggers for systemd (229-4ubuntu21) ...  
* Starting Elasticsearch Server  
sysctl: setting key "vm.max_map_count": Read-only file system  
...done.  
* elasticsearch is running  
---> effcf316edf4  
Removing intermediate container 5954e695689f  
Successfully built effcf316edf4  
Successfully tagged metric/elkstack:latest  
Toms-iMac:Elkstack tommarler$
```

Problem: Service elastic search start in docker file is not running with container starts, even though pictures above tells different story

Quick Fix: docker run -itd elkstack /bin/bash -> docker attach elkstack

- manually start elastic search with -> service elastic search start
- curl localhost:9200 to issue elasticsearch is working properly

```

root@1fc66f4bd213:/# service --status-all
[ - ] bootmisc.sh
[ - ] checkfs.sh
[ - ] checkroot-bootclean.sh
[ - ] checkroot.sh
[ - ] cron
[ - ] dbus
[ - ] elasticsearch
[ - ] hostname.sh
[ ? ] hwclock.sh
[ - ] killprocs
[ - ] mountall-bootclean.sh
[ - ] mountall.sh
[ - ] mountdevsubfs.sh
[ - ] mountkernfs.sh
[ - ] mountnfs-bootclean.sh
[ - ] mountnfs.sh
[ ? ] ondemand
[ - ] procs
[ - ] rc.local
[ - ] sendsigs
[ - ] umountfs
[ - ] umountnfs.sh
[ - ] umountroot
[ - ] unattended-upgrades
[ - ] urandom
[ - ] x11-common
root@1fc66f4bd213:/# service elasticsearch start
* Starting Elasticsearch Server
sysctl: setting key "vm.max_map_count": Read-only file system
root@1fc66f4bd213:/# wget http://localhost:9200
--2017-11-21 16:24:49-- http://localhost:9200/
Resolving localhost (localhost)... 127.0.0.1, ::1
Connecting to localhost (localhost)|127.0.0.1|:9200... connected.
HTTP request sent, awaiting response... 200 OK
Length: 327 [application/json]
Saving to: 'index.html'

index.html                               100%[=====>] 327  --.-KB/s  in 0s

2017-11-21 16:24:49 (36.4 MB/s) - 'index.html' saved [327/327]

```

```

[ root@1fc66f4bd213:/# cat index.html
{
  "name" : "ukfu_gu",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "Aga9kTCJSi6mewKMNOaKtw",
  "version" : {
    "number" : "5.6.4",
    "build_hash" : "8bbedf5",
    "build_date" : "2017-10-31T18:55:38.105Z",
    "build_snapshot" : false,
    "lucene_version" : "6.6.1"
  },
  "tagline" : "You Know, for Search"
}
root@1fc66f4bd213:/# █

```

Install Kibana

- sudo apt-get install kibana
- runs on port 5600

- `wget http://localhost:5600 -> cat index.html`

```
[ - ] x11-common
[root@2c29f7aa2b26:/# service elasticsearch start
 * Starting Elasticsearch Server
 sysctl: setting key "vm.max_map_count": Read-only file system

[root@2c29f7aa2b26:/# service kibana start
 kibana started
[root@2c29f7aa2b26:/# wget http://localhost:5601
--2017-11-21 16:37:28-- http://localhost:5601/
Resolving localhost (localhost)... 127.0.0.1, ::1
Connecting to localhost (localhost)|127.0.0.1|:5601... connected.
HTTP request sent, awaiting response... 200 OK
Length: 217 [text/html]
Saving to: 'index.html'

index.html                               100%[=====]

2017-11-21 16:37:28 (9.06 MB/s) - 'index.html' saved [217/217]

[root@2c29f7aa2b26:/# cat index.html
<script>var hashRoute = '/app/kibana';
var defaultRoute = '/app/kibana';

var hash = window.location.hash;
if (hash.length) {
  window.location = hashRoute + hash;
} else {
  window.location = defaultRoute;
}</script>root@2c29f7aa2b26:/#
```