LogStash - Installation

Created by Florian Dambrine, last modified just a moment ago

Table of contents

Create new EC2 instance

Create a new EC2 instance (c3.large) on AWS **using the baseline** and affect the following security groups:

SG Name	Description
sshonly	SSH port
logstashSG	Access to the Redis ElastiCache and ElasticSearch cluster

LogStash Installation

- Create a file named **/etc/profile.d/aws.sh** with the following content:

> **Check if the file does not exist before erasing it!**

```
sudo su
touch /etc/profile.d/aws.sh && \
```

```
echo -e "export AWS_DEFAULT_REGION=us-east-1\nexport AWS_ACCESS_KEY_ID=...\nexport AW
chmod +x /etc/profile.d/aws.sh
exit
```

- Install the **aws client**

```
wget https://s3.amazonaws.com/aws-cli/awscli-bundle.zip
unzip awscli-bundle.zip
sudo ./awscli-bundle/install -i /usr/local/aws -b /usr/local/bin/aws
rm -rf awscli-bundle*
```

- Install the **runurl** program

```
sudo add-apt-repository ppa:alestic/ppa &&
sudo apt-get update &&
sudo apt-get install -y runurl
```

- Download LogStash from the **gumgum-distributions** S3 bucket
  - The first command allows you to load the AWS credentials in your environnement

```
source /etc/profile.d/aws.sh
aws s3 cp s3://gumgum-cookbooks/latest/logstash-bundle.tar.gz .
```

- Extract the LogStash archive

```
sudo su
mv /home/ubuntu/logstash-bundle.tar.gz /usr/local/ && cd /usr/local/ && tar -xzf logs
exit
```

- Update the code

```
cd -P /usr/local/logstash/servers-configuration && git checkout master && git pull &&
```

<u>Setup the LogStash Client</u>

- Set the script as a Unix service

```
cd /etc/init.d/ && ln -s /usr/local/logstash/servers-configuration/logstash/sh/logsta
```

- Update rc.d in order to start the LogStash Client when an instance starts

```
update-rc.d logstash-client defaults
```

Setup the LogStash Server

- Set the script as a Unix service

```
cd /etc/init.d/ && ln -s /usr/local/logstash/servers-configuration/logstash/sh/logsta
```

- Update rc.d in order to start the LogStash Server when an instance starts

```
update-rc.d logstash-cluster defaults
```

Like Be the first to like this   No labels

Powered by Atlassian | Terms of Use | Answers | Maintenance Schedule