Splunk Installation

Centos:

Create a Splunk User-

```
[root@server]# groupadd splunk
[root@server]# useradd -d /opt/splunk -m -g splunk splunk
[root@server]# passwd splunk
[root@server]# su - splunk
[splunk@server]$ id
uid=1001(splunk) gid=1001(splunk) groups=1001(splunk)
```

Confirm the server's architecture

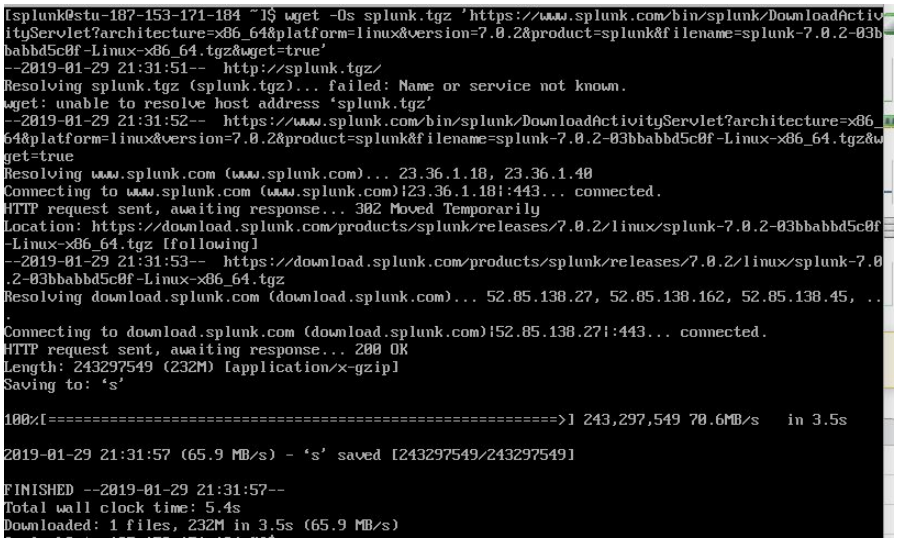
```
[splunk@server]$ getconf LONG_BIT
64
```

It is best to install this on a dedicated user and not root, create a user and add them to a group called 'Splunk', creating a folder to run Splunk is also ideal.

Download the package:

```
[splunk@server]$ wget -O splunk.tgz
'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&version=7.0.2&product=splunk&filename=splunk-7.0.2-03bbabbd5c0f-Linux-x86_64.tgz&wget=true'
```

Remember to type all of this as one line and check for typos



Name of file to edit

(line number) `Edit to make` Brief explanation of edit