

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.

```
[root@stu-187-153-171-184 caitlin]# useradd -d/opt/splunk -m -g splunk splunk
[root@stu-187-153-171-184 caitlin]# su - splunk
[splunk@stu-187-153-171-184 ~]$ id
uid=1001(splunk) gid=1001(splunk) groups=1001(splunk) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[splunk@stu-187-153-171-184 ~]$ getconf LONG_BIT
64
```

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

```
[splunk@stu-187-153-171-184 ~]$ wget -O splunk.tgz 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&version=7.0.2&product=splunk&filename=splunk-7.0.2-03bbabd5c8f-Linux-x86_64.tgz&wget=true'
--2019-01-29 21:31:51-- http://splunk.tgz/
Resolving splunk.tgz (splunk.tgz)... failed: Name or service not known.
wget: unable to resolve host address 'splunk.tgz'
--2019-01-29 21:31:52-- https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&version=7.0.2&product=splunk&filename=splunk-7.0.2-03bbabd5c8f-Linux-x86_64.tgz&wget=true
Resolving www.splunk.com (www.splunk.com)... 23.36.1.18, 23.36.1.40
Connecting to www.splunk.com (www.splunk.com)|23.36.1.18|:443... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: https://download.splunk.com/products/splunk/releases/7.0.2/linux/splunk-7.0.2-03bbabd5c8f-Linux-x86_64.tgz [following]
--2019-01-29 21:31:53-- https://download.splunk.com/products/splunk/releases/7.0.2/linux/splunk-7.0.2-03bbabd5c8f-Linux-x86_64.tgz
Resolving download.splunk.com (download.splunk.com)... 52.85.138.27, 52.85.138.162, 52.85.138.45, ...
Connecting to download.splunk.com (download.splunk.com)|52.85.138.27|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 243297549 (232M) [application/x-gzip]
Saving to: 's'

100%[=====>] 243,297,549 70.6MB/s in 3.5s

2019-01-29 21:31:57 (65.9 MB/s) - 's' saved [243297549/243297549]

FINISHED --2019-01-29 21:31:57--
Total wall clock time: 5.4s
Downloaded: 1 files, 232M in 3.5s (65.9 MB/s)
```

Name of file to edit

(line number) Edit to make Brief explanation of edit