Installing CESA for Splunk on CentOS

October 2020

About this guide

This guide helps you install Splunk on Centos. Its meant for an all-in-one install of CESA for Splunk. You may use this guide to install on your favorite supported Linux but we recommend CentOS to keep it simple.

Note: I have had someone try same steps on Ubuntu and mainly the same.

This guide runs you through installation of Splunk on CentOS. To follow the rest of the install please visit
[Install and Configure AnyConnect NVM 4.7.x or Later and Related Splunk Enterprise Components for CESA]()

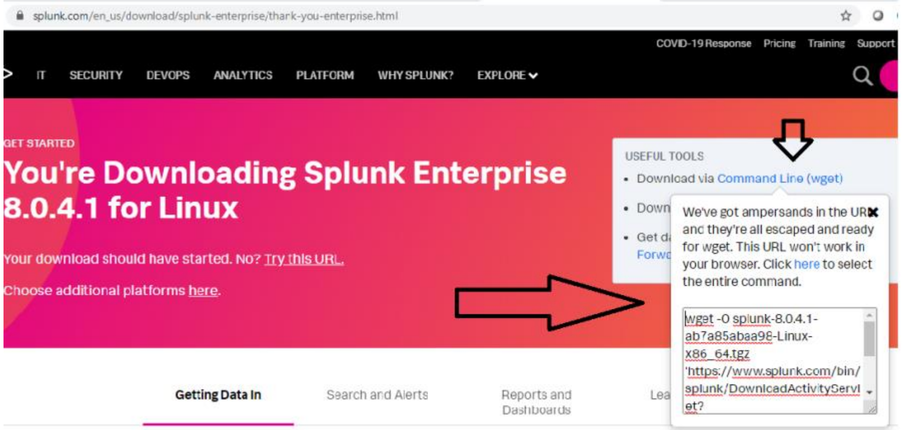
Download and install Splunk

1. Download the latest CentOS org download - https://www.centos.org/download/
2. Install splunk
   a. Choose Centos server install
   b. No dependencies on other packages

Update CentOS and install Splunk

1. As root, update Centos by doing run "yum update" before installing Splunk.
   a. Enter "Yes" in any prompt.
2. While waiting for that you can download Splunk

https://www.splunk.com/en_us/download/splunk-enterprise/thank-you-enterprise.html copy to the clipboard the .tgz command.



You're Downloading Splunk Enterprise 8.0.4.1 for Linux

Your download should have started. No? Try this URL.

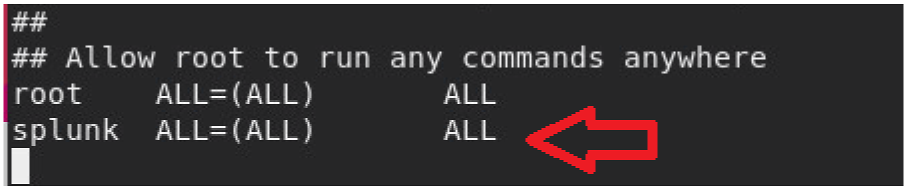
Choose additional platforms here.

We've got ampersands in the URL and they're all escaped and ready for wget. This URL won't work in your browser. Click here to select the entire command.

```
wget -O splunk-8.0.4.1-
ab7a85abaa98-Linux-
x86_64.tgz
'https://www.splunk.com/bin/
splunk/DownloadActivityServl
et?
```

3. Download by pasting the wget command in the cli and run it as root.
   a. Sudo (paste)
4. Create groups, users with correct permission
   Create splunk group, splunk user and add it to the sudoers file to install Splunk and run sudo commands.
   Run the following commands:
   - groupadd splunk

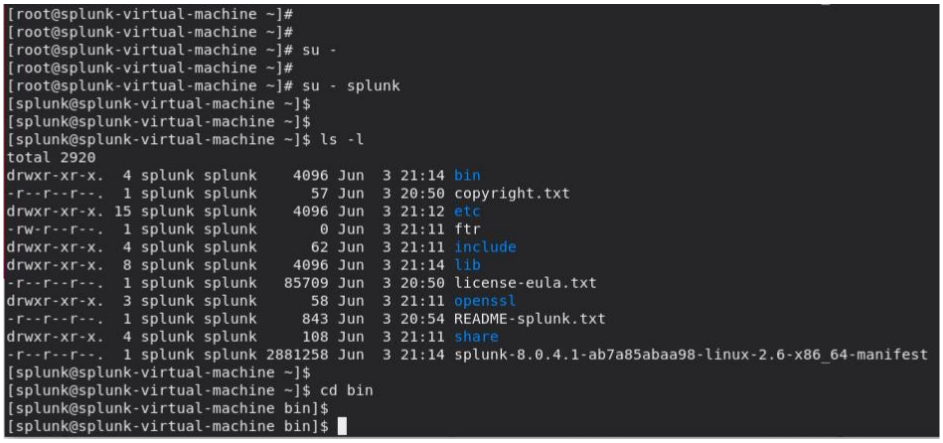
- useradd –d /opt/splunk –m –g splunk splunk
- passwd splunk (Add password and retype password.)
- sudo visudo (Add splunk user as follow by using vi text editor:)



```
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
splunk  ALL=(ALL)       ALL
```

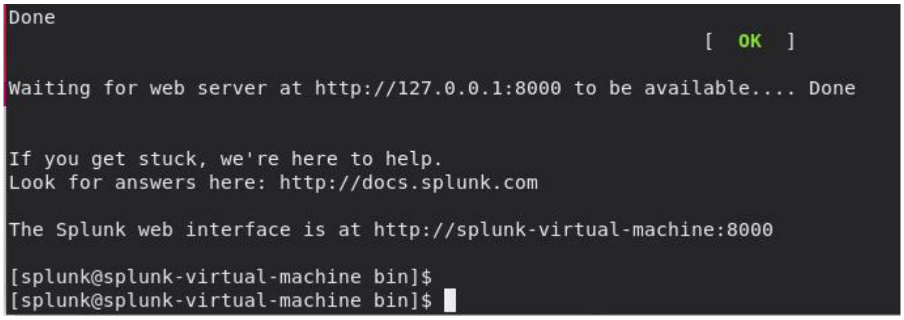
5. Install splunk
    a. Unzip the file .tgz by using the command “tar –xzvf splunk-file.tgz”
    b. Copy the files to the created folder by using the following command “cp –rp splunk/* /opt/splunk/”
    c. Run the following command to change the owner “chown –R splunk: /opt/splunk”

6. Start splunk
    a. Switch to splunk user by issuing the command “su – splunk”
    b. Change to the folder bin “cd bin”:



```
[root@splunk-virtual-machine ~]#
[root@splunk-virtual-machine ~]#
[root@splunk-virtual-machine ~]# su -
[root@splunk-virtual-machine ~]#
[root@splunk-virtual-machine ~]# su - splunk
[splunk@splunk-virtual-machine ~]$
[splunk@splunk-virtual-machine ~]$
[splunk@splunk-virtual-machine ~]$ ls -l
total 2920
drwxr-xr-x.  4 splunk splunk    4096 Jun  3 21:14 bin
-r--r--r--.  1 splunk splunk      57 Jun  3 20:50 copyright.txt
drwxr-xr-x. 15 splunk splunk    4096 Jun  3 21:12 etc
-rw-r--r--.  1 splunk splunk       0 Jun  3 21:11 ftr
drwxr-xr-x.  4 splunk splunk      62 Jun  3 21:11 include
drwxr-xr-x.  8 splunk splunk    4096 Jun  3 21:14 lib
-r--r--r--.  1 splunk splunk   85709 Jun  3 20:50 license-eula.txt
drwxr-xr-x.  3 splunk splunk      58 Jun  3 21:11 openssl
-r--r--r--.  1 splunk splunk     843 Jun  3 20:54 README-splunk.txt
drwxr-xr-x.  4 splunk splunk     108 Jun  3 21:11 share
-r--r--r--.  1 splunk splunk 2881258 Jun  3 21:14 splunk-8.0.4.1-ab7a85abaa98-linux-2.6-x86_64-manifest
[splunk@splunk-virtual-machine ~]$
[splunk@splunk-virtual-machine ~]$ cd bin
[splunk@splunk-virtual-machine bin]$
[splunk@splunk-virtual-machine bin]$
```

    c. Now let’s run Splunk with the command “./splunk start –-accept-license” (Notice the double dash.) Make sure to create an administrator username and password that will be used to log in to your Splunk GUI.
    d. Take note of the following details which will be used to access the Splunk server: port 8000

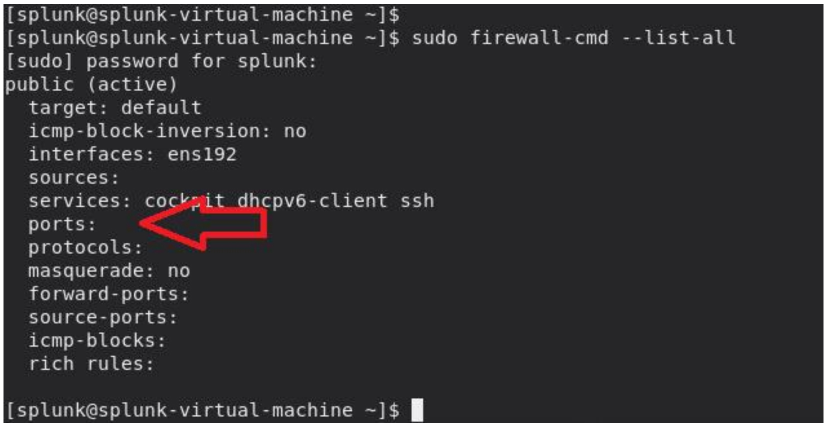


```
Done
                                                           [  OK  ]

Waiting for web server at http://127.0.0.1:8000 to be available.... Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://splunk-virtual-machine:8000

[splunk@splunk-virtual-machine bin]$
[splunk@splunk-virtual-machine bin]$
```

7. Open the necessary ports for access to the splunk UI and for the ports necessary for the collector receive anyconnect NVM data

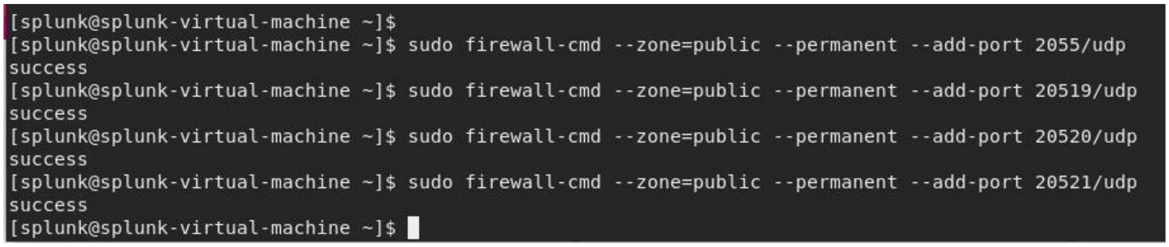
   We will run the following commands:

   a. Optional. Firewall-cmd –get-zones (To check the list of zones where the port might be opened.)
   b. Confirm that the port 8000 is not open as well as other ports in the server with the command “sudo firewall-cmd -–list-all” (Notice the double dash.):



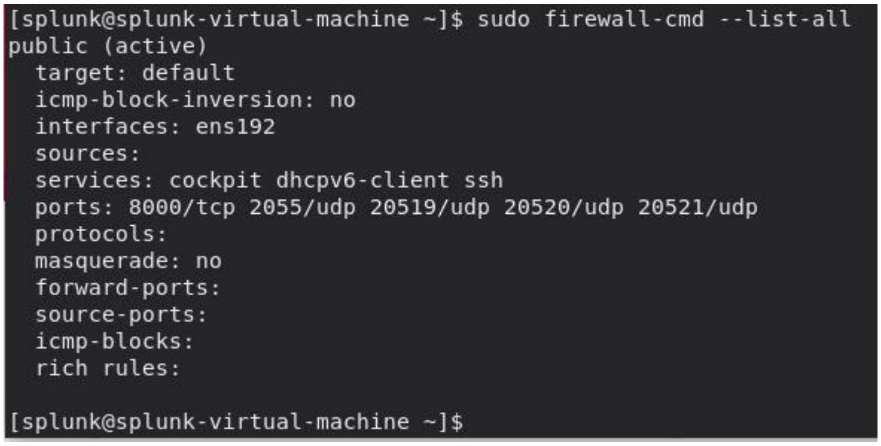
```
[splunk@splunk-virtual-machine ~]$
[splunk@splunk-virtual-machine ~]$ sudo firewall-cmd --list-all
[sudo] password for splunk:
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens192
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

[splunk@splunk-virtual-machine ~]$
```

- Add the ports 8000/tcp, 2055/udp, 20519/udp, 20520/udp and 20521/udp with command “sudo firewall-cmd -–zone=public –permanent –add-port 8000/tcp” and wait for the success output:



```
[splunk@splunk-virtual-machine ~]$
[splunk@splunk-virtual-machine ~]$ sudo firewall-cmd --zone=public --permanent --add-port 2055/udp
success
[splunk@splunk-virtual-machine ~]$ sudo firewall-cmd --zone=public --permanent --add-port 20519/udp
success
[splunk@splunk-virtual-machine ~]$ sudo firewall-cmd --zone=public --permanent --add-port 20520/udp
success
[splunk@splunk-virtual-machine ~]$ sudo firewall-cmd --zone=public --permanent --add-port 20521/udp
success
[splunk@splunk-virtual-machine ~]$
```

- Run “sudo firewall-cmd --reload” and “sudo firewall-cmd --list-all” confirm that the ports were added successfully.



```
[splunk@splunk-virtual-machine ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens192
  sources:
  services: cockpit dhcpv6-client ssh
  ports: 8000/tcp 2055/udp 20519/udp 20520/udp 20521/udp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

[splunk@splunk-virtual-machine ~]$
```