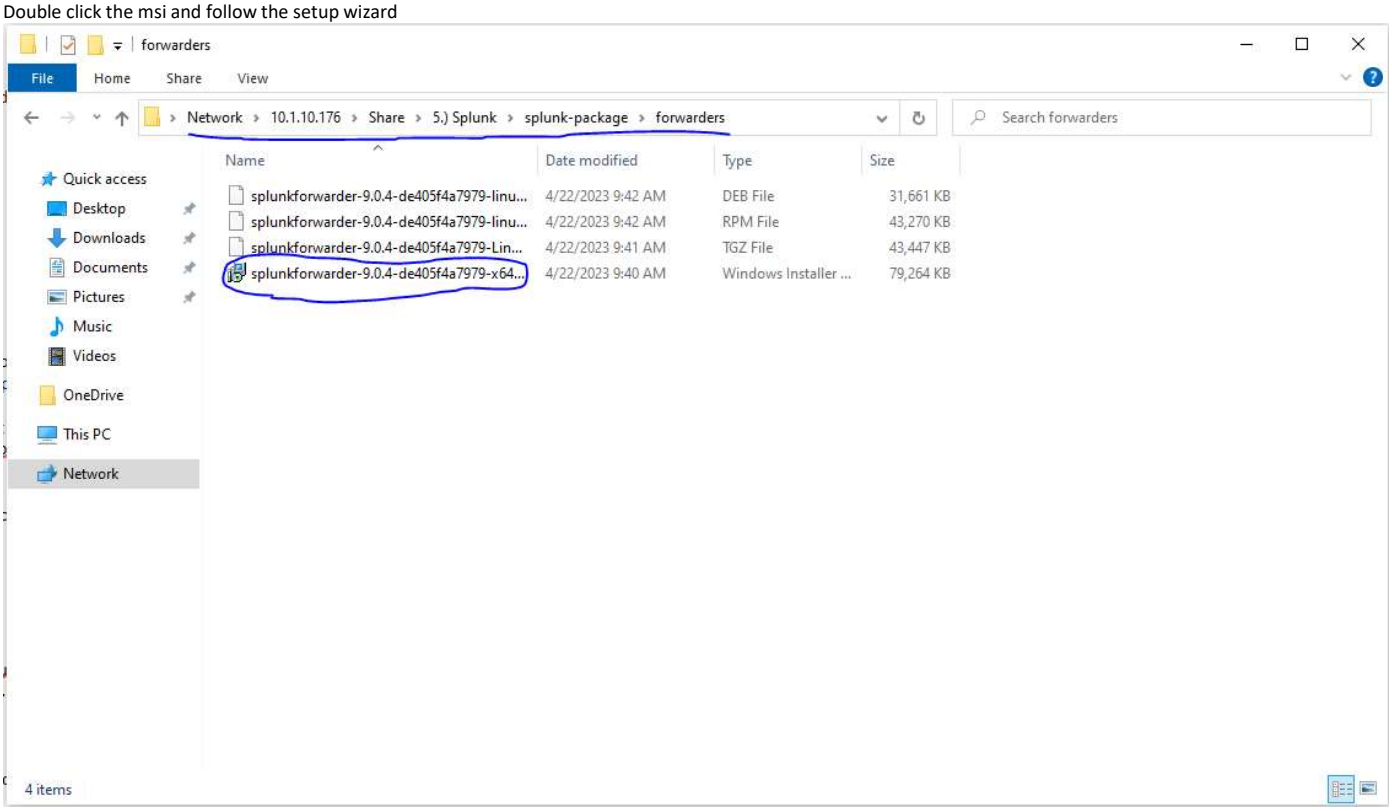
Splunk Forwarder (WINDOWS)

Thursday, March 28, 2024 12:18 PM

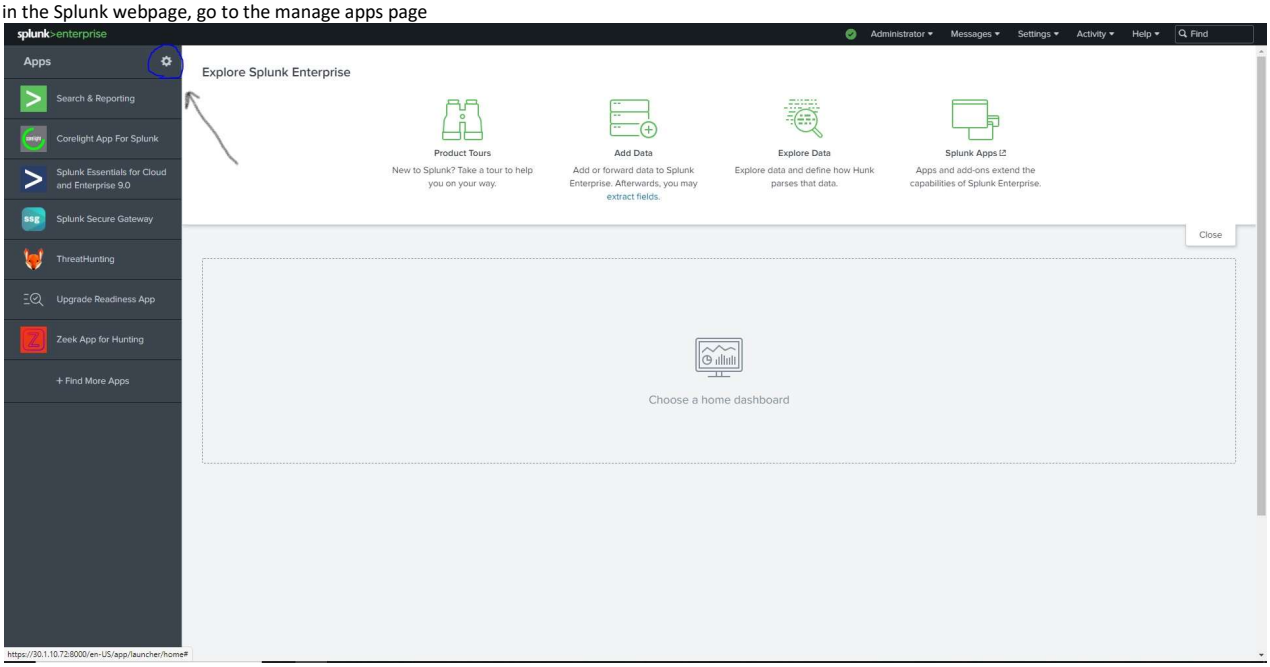
On the windows machine:

1) Install the forwarder onto the host
    a. Double click the msi and follow the setup wizard

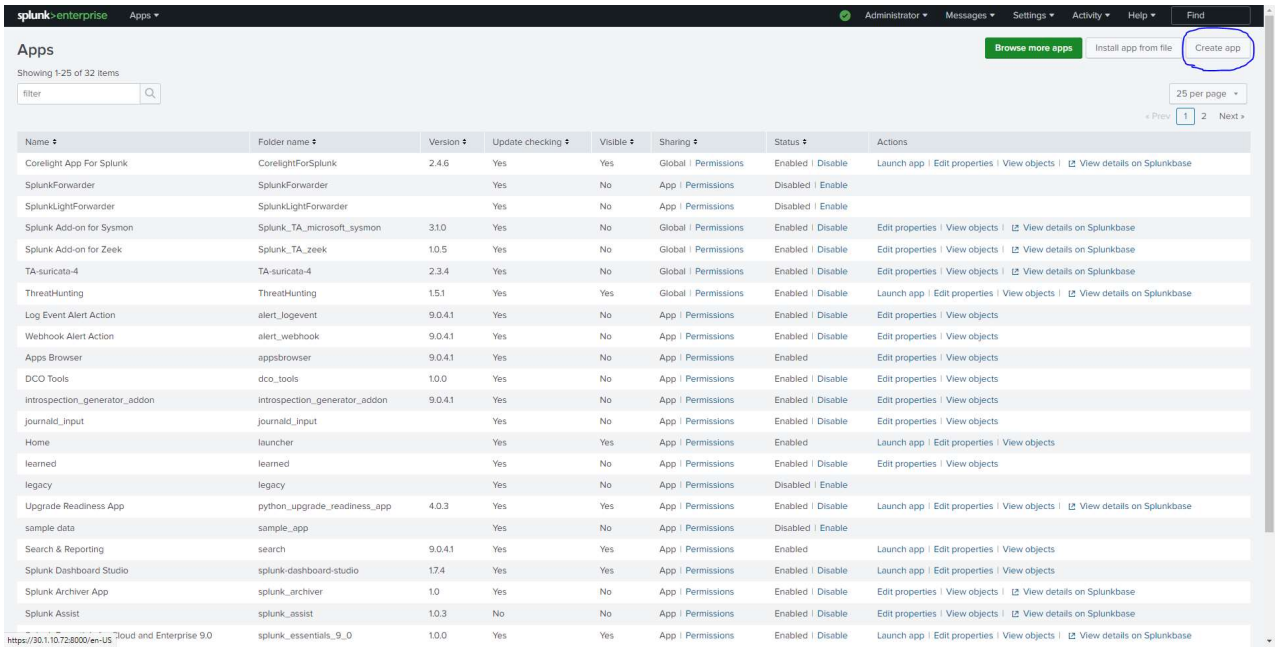


        1) It will need to script out

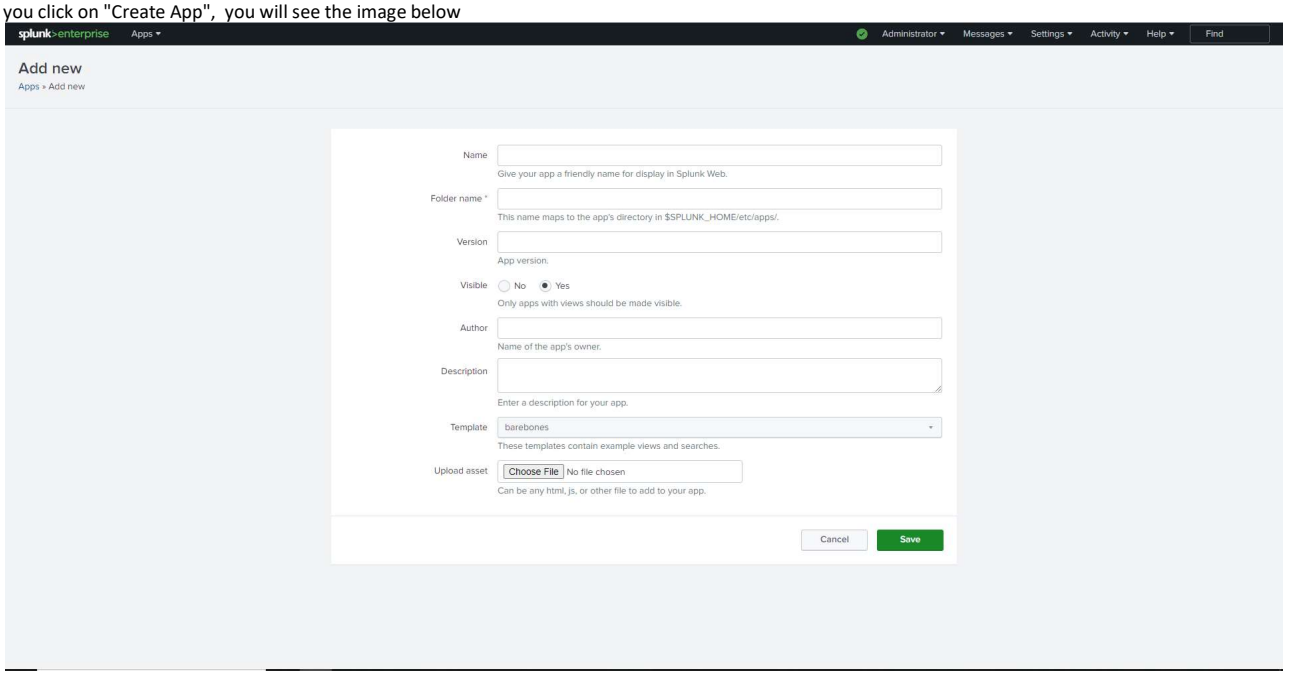
2) On the Splunk webpage
    a. Create an app
        i. Once in the Splunk webpage, go to the manage apps page



        ii. Once in the Manage Apps Page, you will click on "Create App"

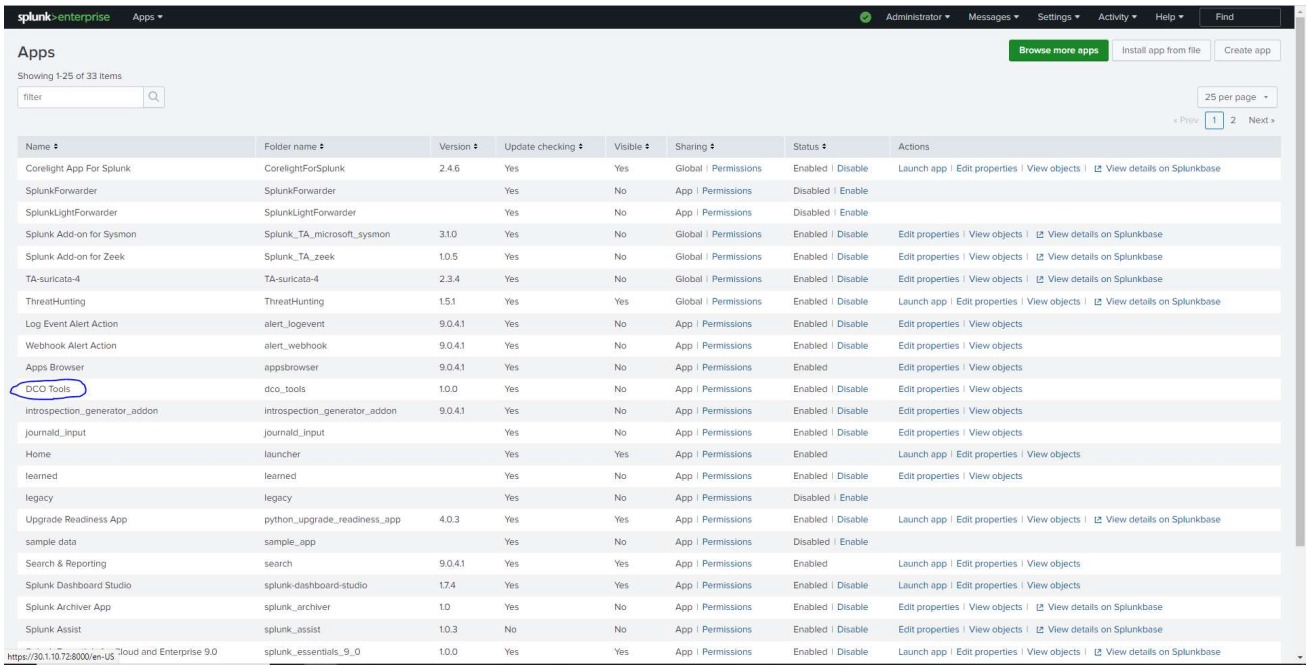


iii. Once you click on "Create App", you will see the image below



1) The following is what you will fill in, unless told otherwise
   a) Name = DCO Tools
   b) Foldername = dco_tools
   c) Version = 1.0.0
   d) Visible = no

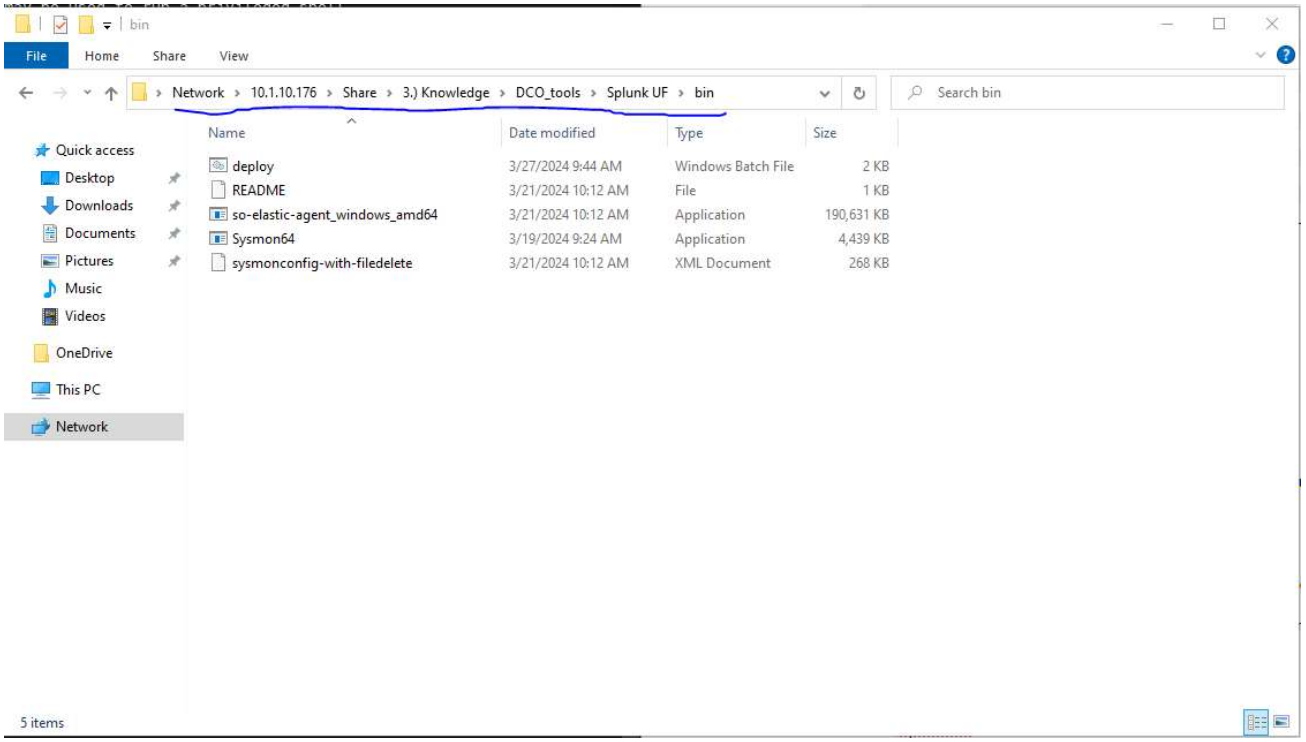
iv. Then double check the manage apps page to verify that the app was created



3) SSH into splunk cli using MobaXterm
   a. Ip:30.1.10.72
   b. Username: dco_admin
   c. Password: Standard

4) **First step is you are going to copy dco_tools from /opt/splunk/etc/apps to /opt/splunk/etc/deployment-apps**
   a. Cd /opt/splunk/etc/apps
      i. You need to run this command before running the command below
   b. Sudo cp -r dco_tools/ /opt/splunk/etc/deployment-apps/
      i. This should copy the dco_tools app to the deployment-apps directory

5) You will then Switch to the dco_tools copy in the deployment apps directory
   a. Cd /opt/splunk/etc/deployment-apps/dco_tools
      i. If the command does not run, run the command "sudo su" and then run the cd command again
   b. When you use the "ls" command you should see 4 directories
      i. Bin, default, local, and metadata
   c. In the /opt/splunk/etc/deployment-apps/dco_tools/bin directory
      i. Mv the deploy.bat , sysmon.exe , sysmonconfig-with-filedelete.xml , so-elastic-agent-windows_amd64.exe into this directory
         1) Ensure you know the location of the files before running, if you need the files, they are in the share in the file location below
         2) Copy the files over to your desktop and then make note of where they are



3) The command to mv the files over to the splunk cli is "mv (filepath of the file)"
    a) Run this command individually for each file
        i) The commands below are examples as to how the command should look
        ii) Mv /home/dco_admin/deploy.bat .
        iii) Mv /home/dco_admin/sysmonconfig-with-filedelet.xml .
        iv) Mv /home/dco_admin/sysmon64.exe .
        v) Mv /home/dco_admin/so-elastic-agent_windows_amd64 .
    b) Modify the deploy.bat if need be

d. In the default directory
    i. Create file inputs.conf
        1) Sudo vim inputs.conf
            a) -copy the text below into inputs.conf
                i) [script://.\\bin\\deploy.bat]
                disabled = False
                interval = 3600

                [WinEventLog://Microsoft-Windows-Sysmon/Operational]
                index= sysmon
                sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
                disabled = false
                renderXml = true

                [WinEventLog://Security]
                disabled = false
                index = win_security
                sourcetype = wineventlog:Security
                renderXml = false

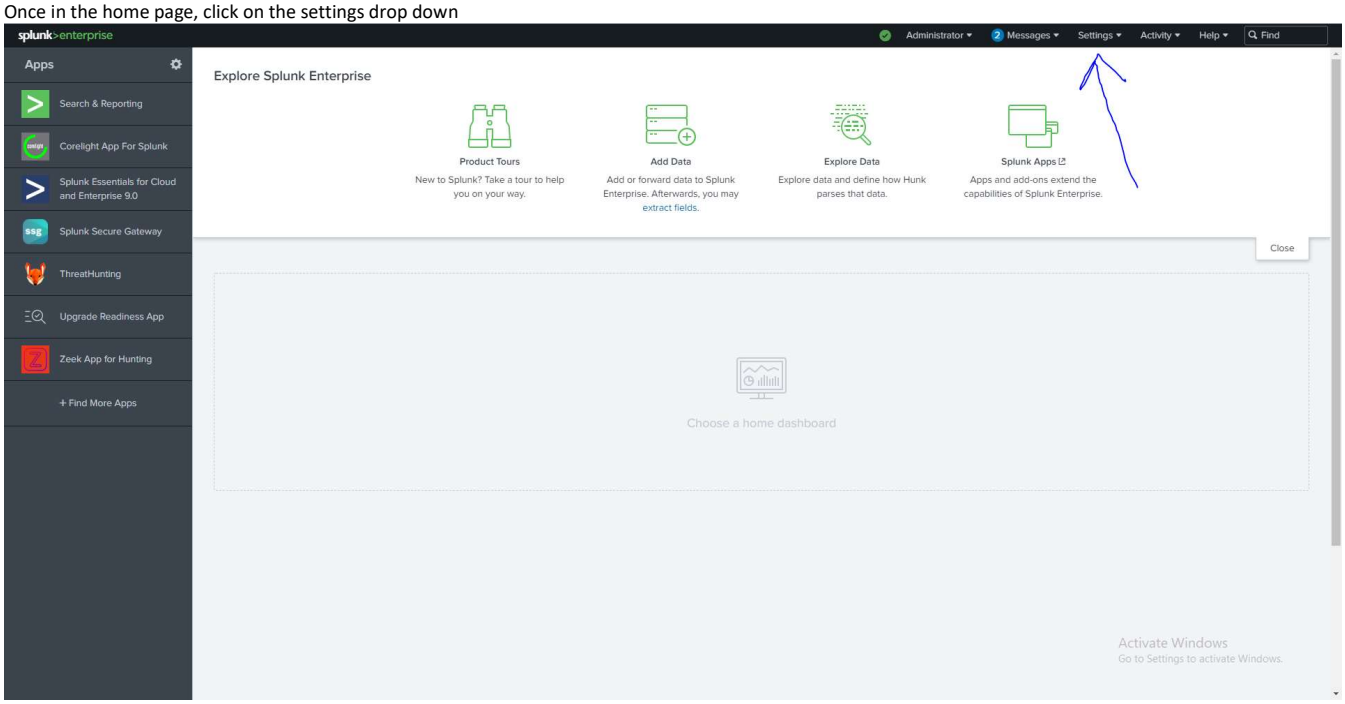
                [WinEventLog:System]
                disabled = false
                index = win_system
                sourcetype = wineventlog:System
                renderXml=false

                [WinEventLog://Application]
                disabled = false
                index = win_application
                sourcetype = wineventlog:Application
                renderXml=false
            b) Once put in, it should look like the image below

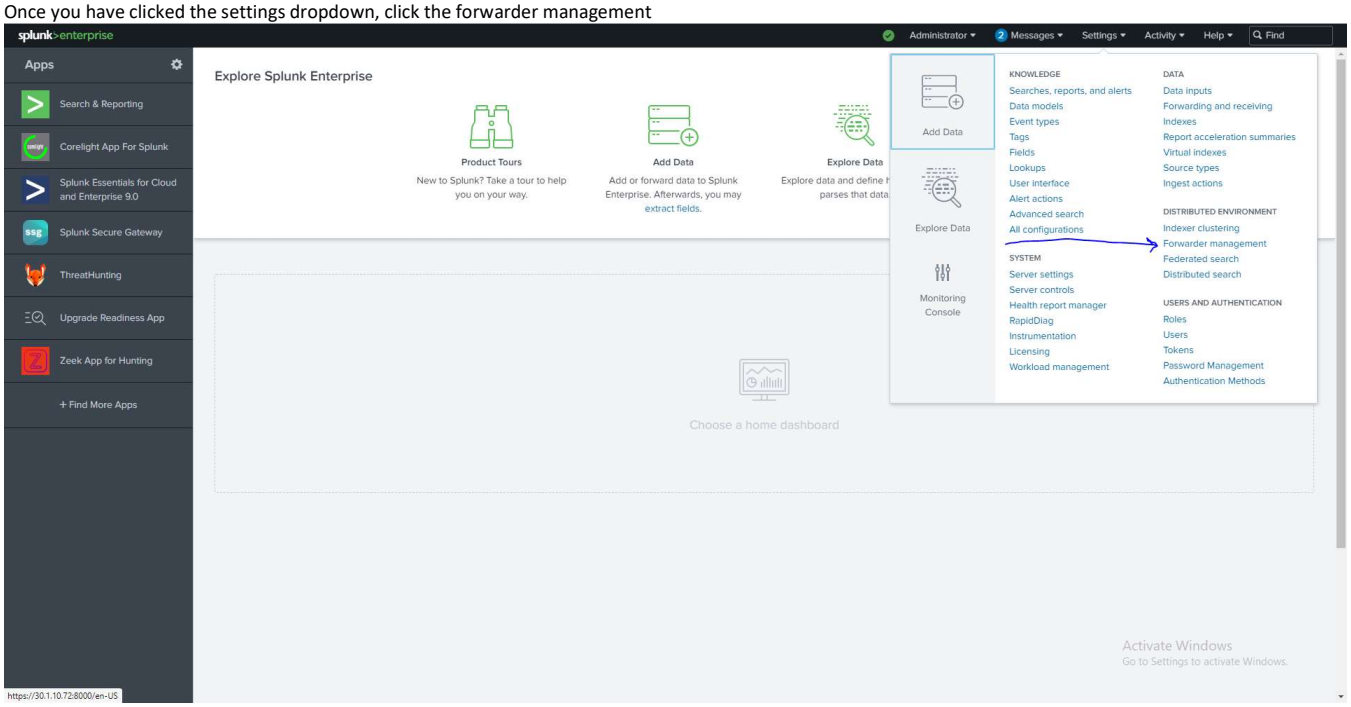
```
[script://.\\bin\\deploy.bat]
disabled = False
interval = 3600

[WinEventLog://Microsoft-Windows-Sysmon/Operational]
index= sysmon
sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
disabled = false
renderXml = true

[WinEventLog://Security]
disabled = false
index = win_security
sourcetype = wineventlog:Security
renderXml = false

[WinEventLog:System]
disabled = false
index = win_system
sourcetype = wineventlog:System
renderXml=false

[WinEventLog://Application]
disabled = false
index = win_application
sourcetype = wineventlog:Application
renderXml=false

~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"inputs.conf" 28L, 576B                                    1,1           All
```

ii. Reload the deployment server with the command below
    1) /opt/splunk/bin/splunk reload deploy-server

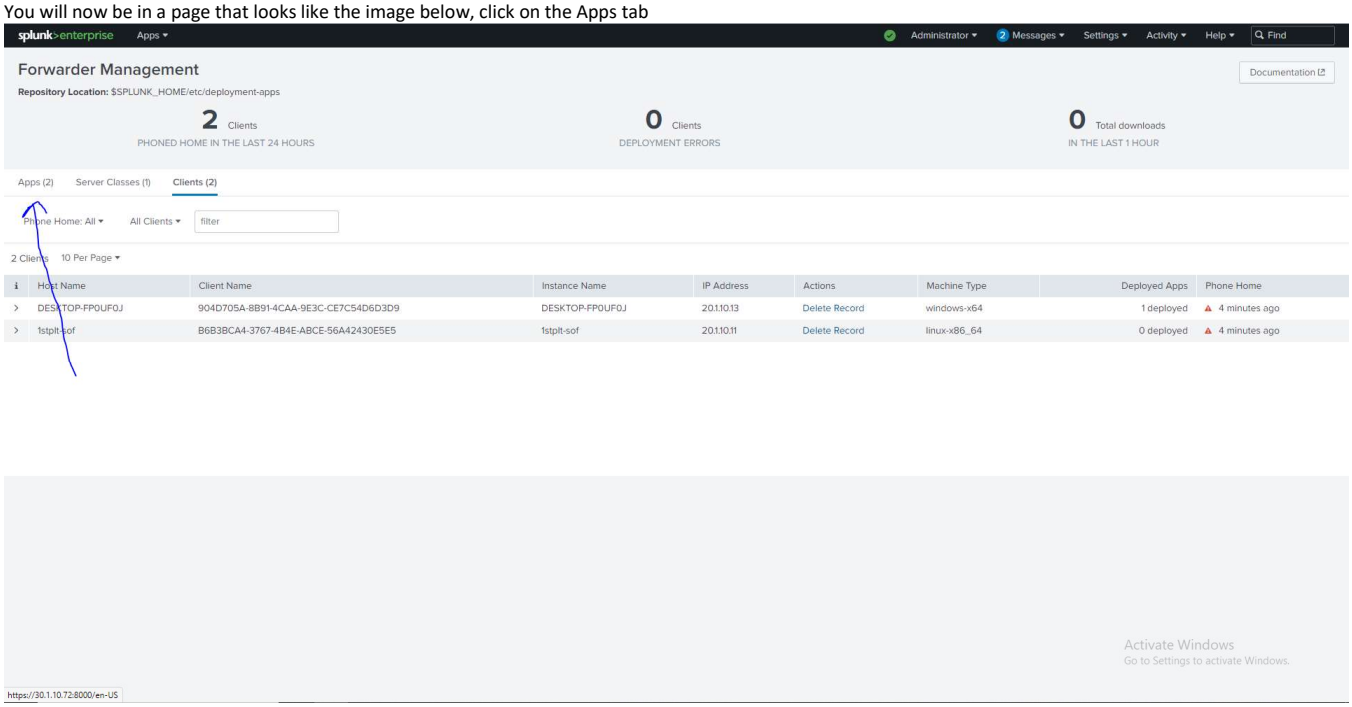
6) Once you the deployment server has been reloaded, go back to the Splunk webpage and verify the app is now up
    a. Once in the home page, click on the settings drop down



b. A
c. Once you have clicked the settings dropdown, click the forwarder management

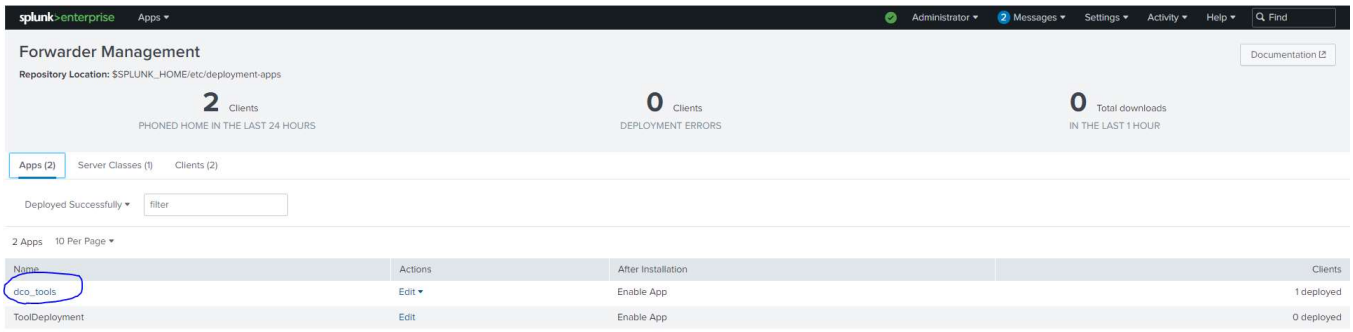


d. A
e. You will now be in a page that looks like the image below, click on the Apps tab



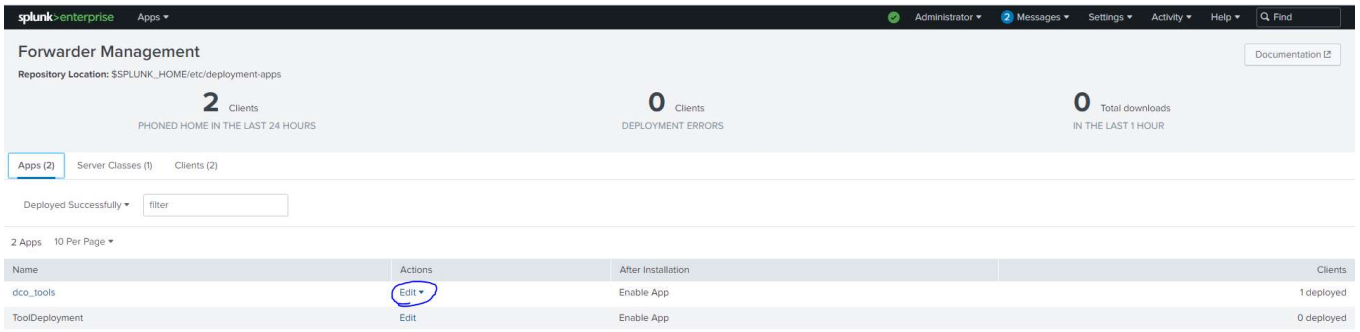
f.

g. A
h. Once you click on the apps tab you should now be able to see the app that you created



i.

j. You will then click on the edit button under the actions column



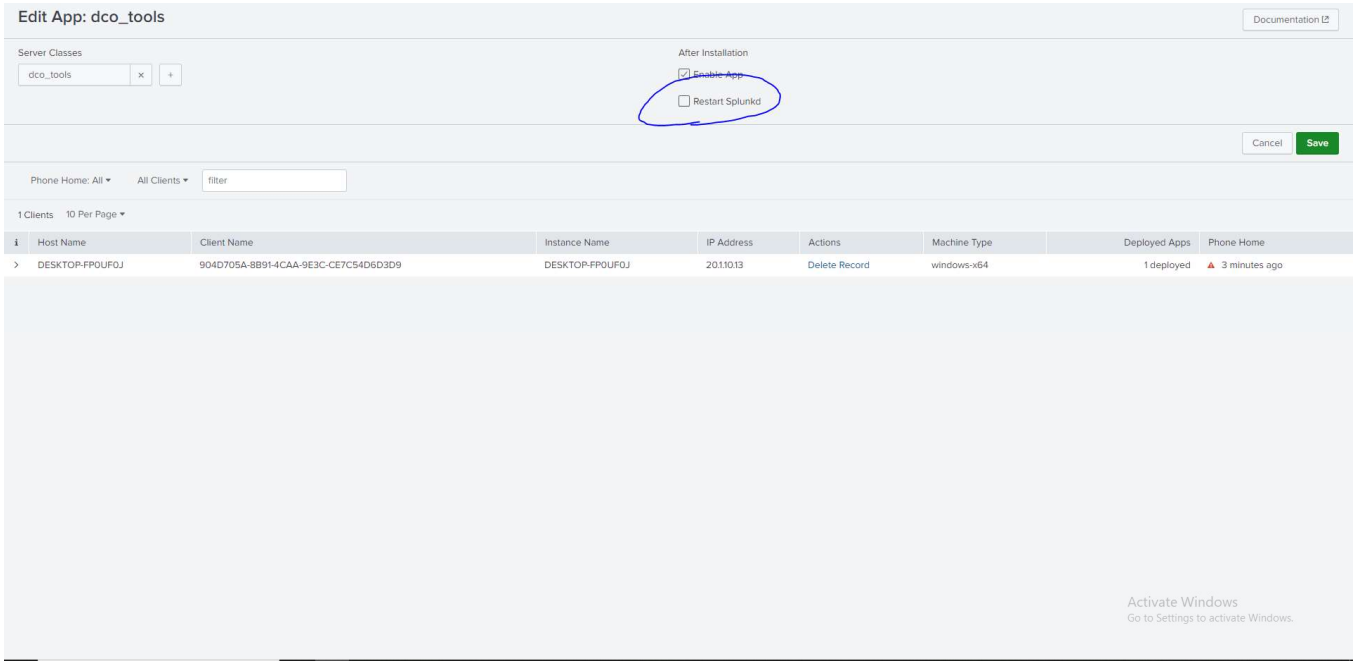
k.

https://30.1.10.72:8000/en-US

l. A

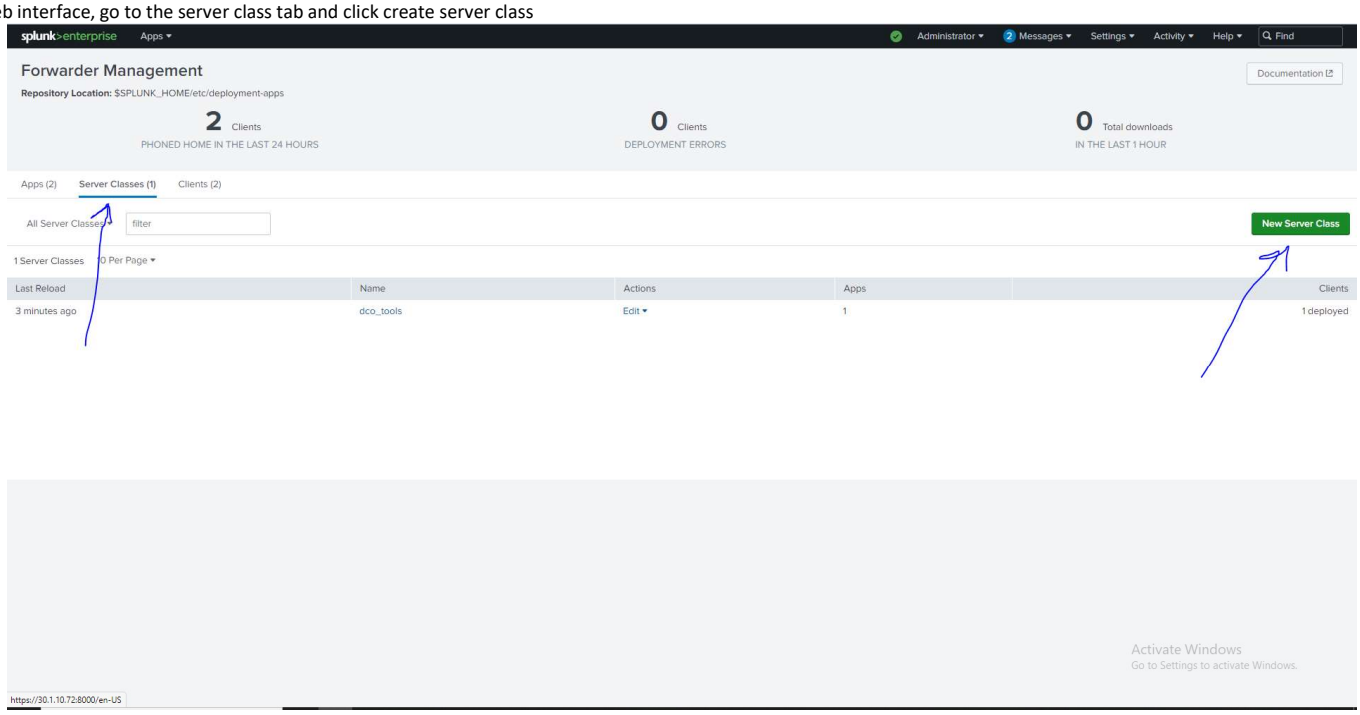
m. Once you click on the edit button, you should be on a page that looks like the image below, you will then click the check box to enable "Restart Splunkd" and click save

n.



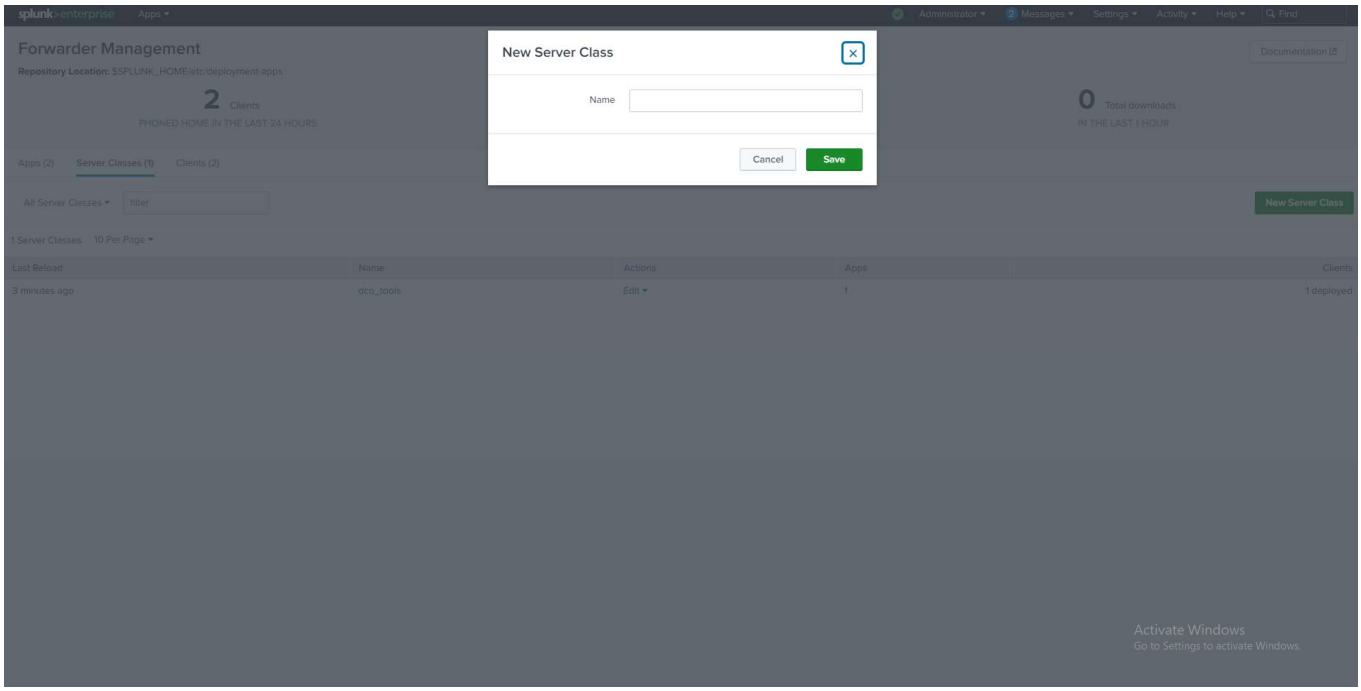
7) In web interface, go to the server class tab and click create server class

a.



8) Once you click to create a new server class, you will give it a name

a.

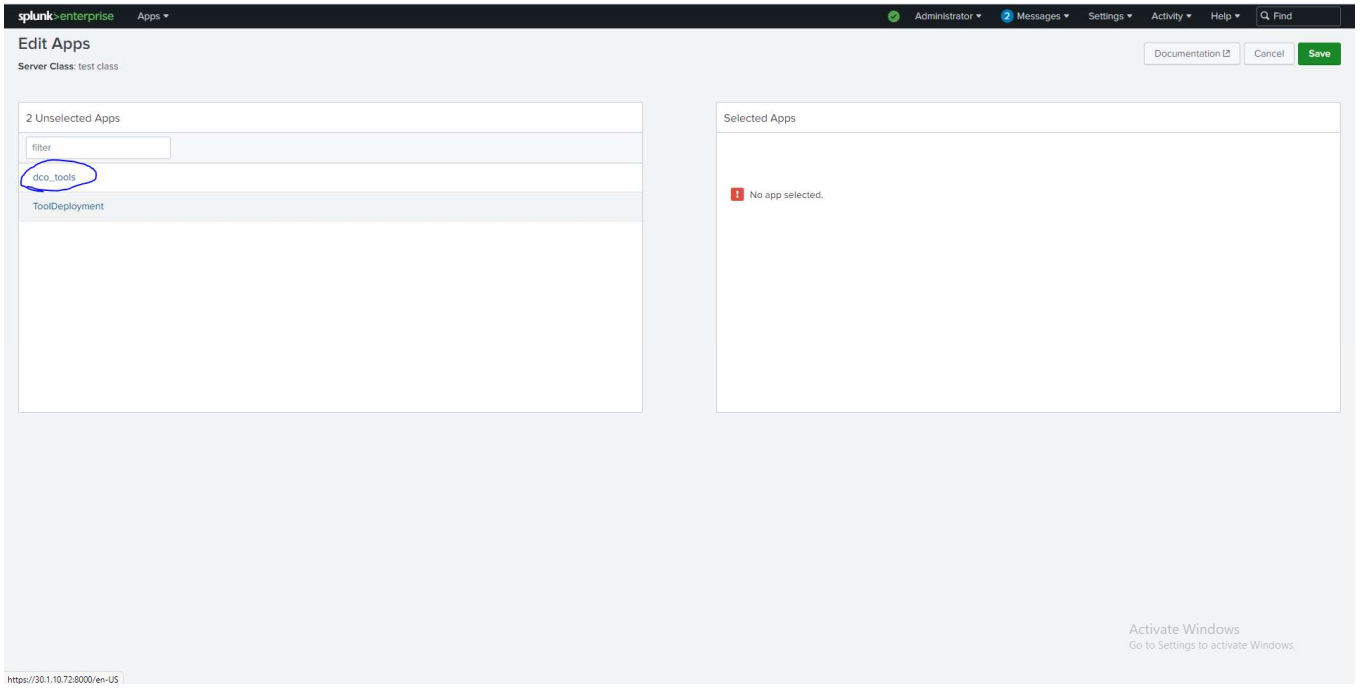


9) Once you have created a name, you should be in a page like the image below

a.

10) Once you do click to add apps, you will click the app you created and save, you save, you will click "Go back to Forwarder Management" so you can verify the creation of the server class

a.



Edit server class and include "*"