Table of Contents

ABSTRACT 2

Splunk Installation in CentOS and adding Agents 3

Splunk Adds on and running a query 18

Conclusion 42

Summary 43

Achievement 44

References 45

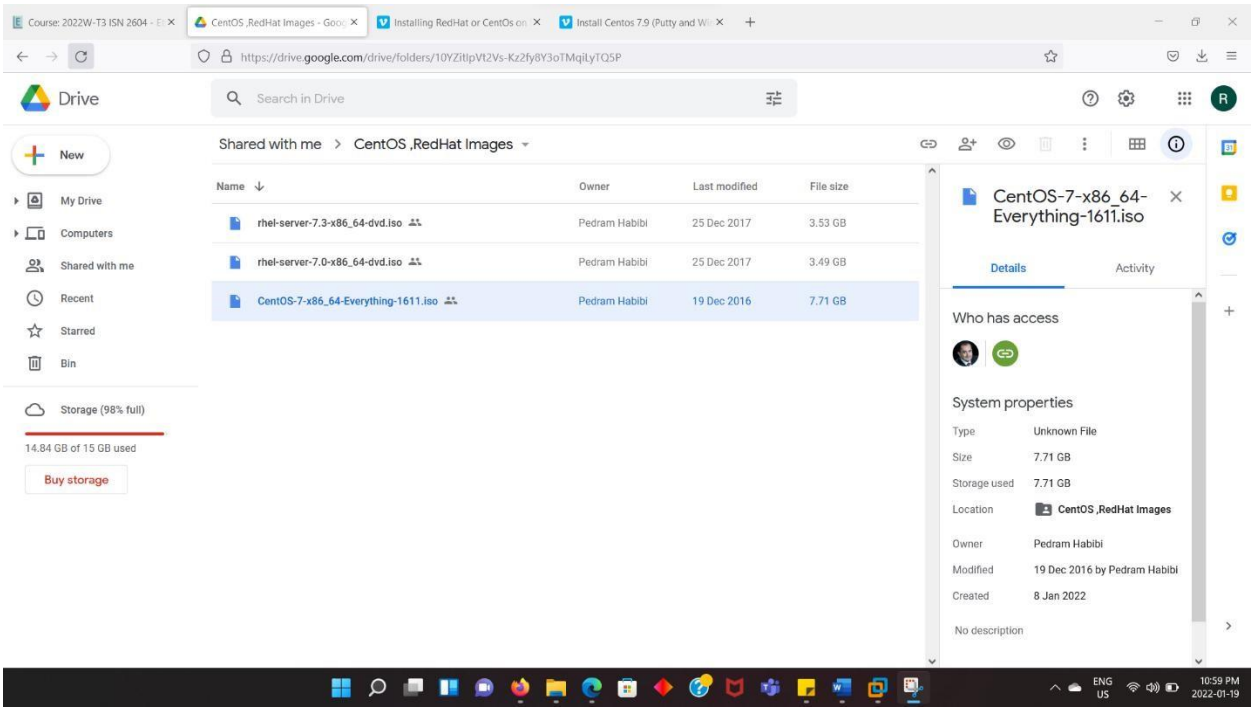
Abstract

In this report, we described how to install Splunk and how to benefit from its features. Splunk is a software platform that enables users to monitor, analyze, and visualize machine-generated data. From adding agents to using Splunk forwarder to get more intuitive reports/logs to maintain your network infrastructure. Here, we have used 3 agents to showcase Splunk added ability to monitor and report logs in a concise manner.

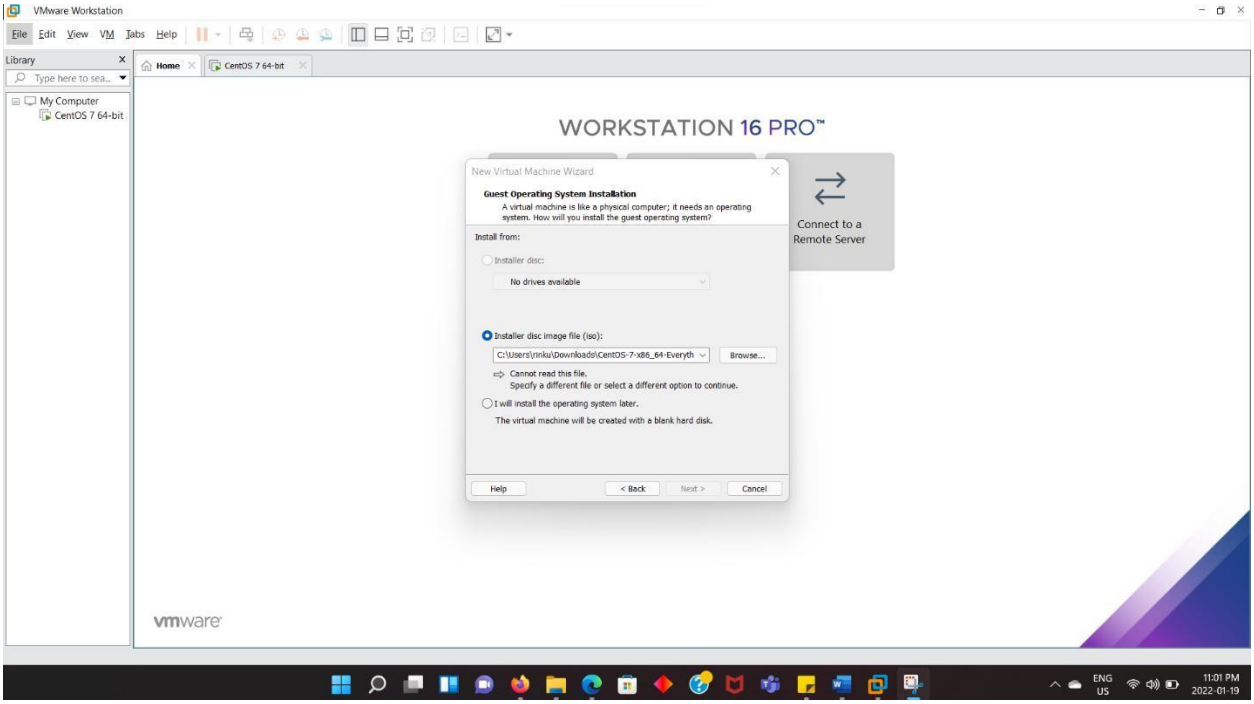
Part 1

Splunk Installation in CentOS and adding Agents

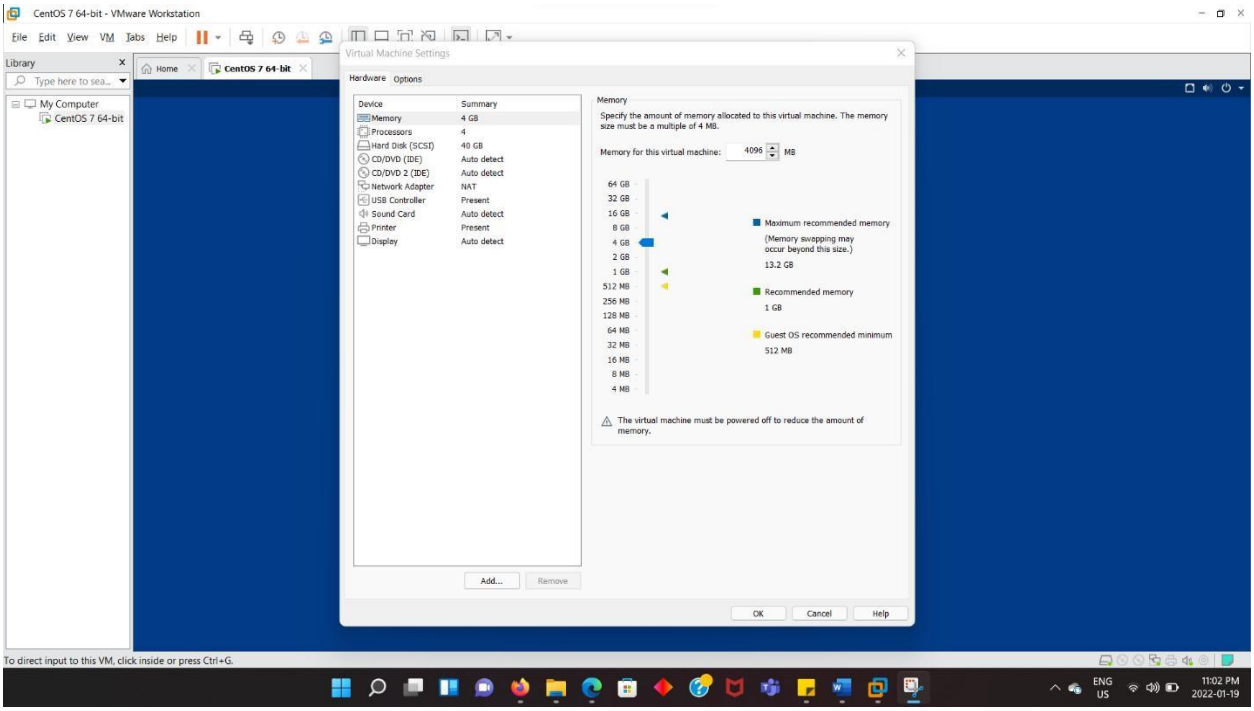
CentOS .iso file download



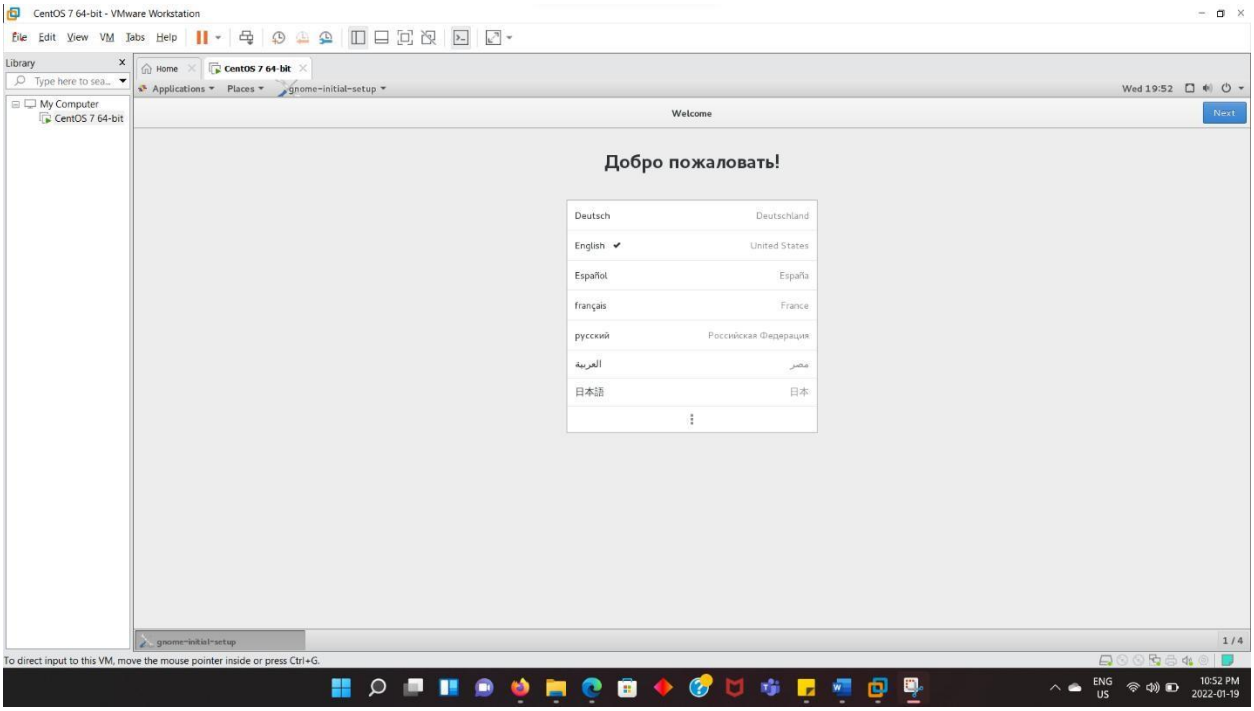
Configuring the iso file



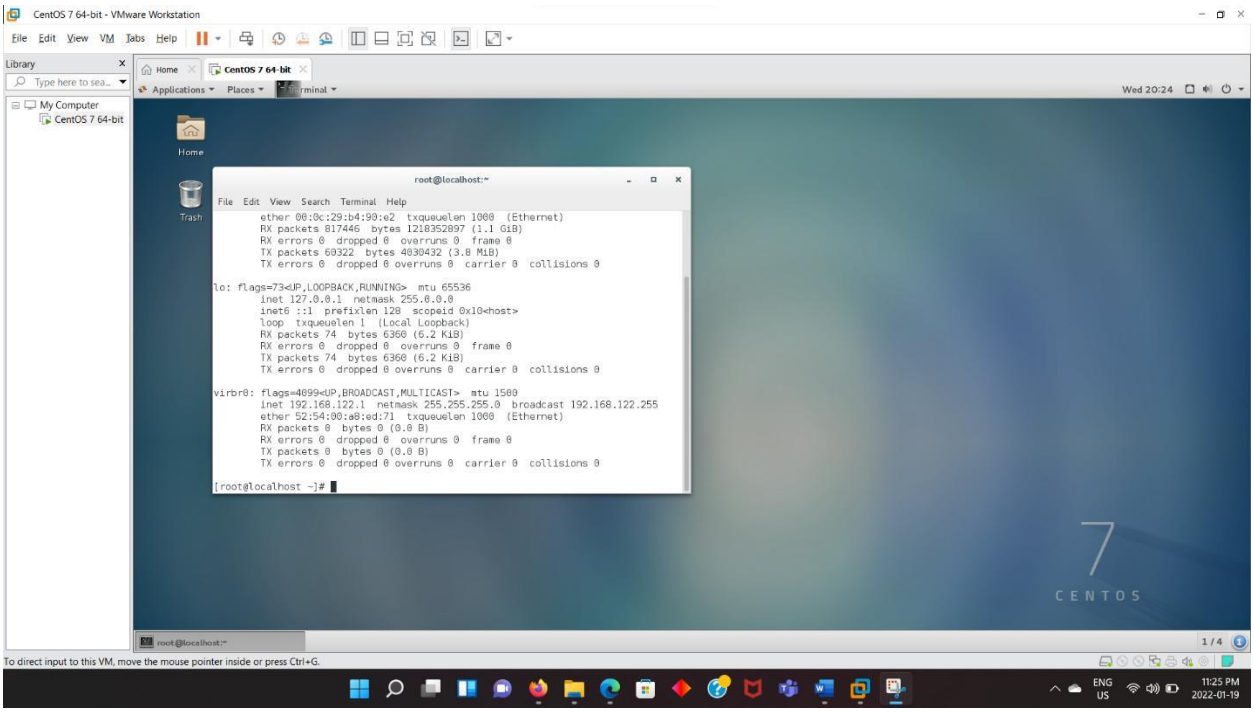
Selecting the memory size, processor, and network adapter



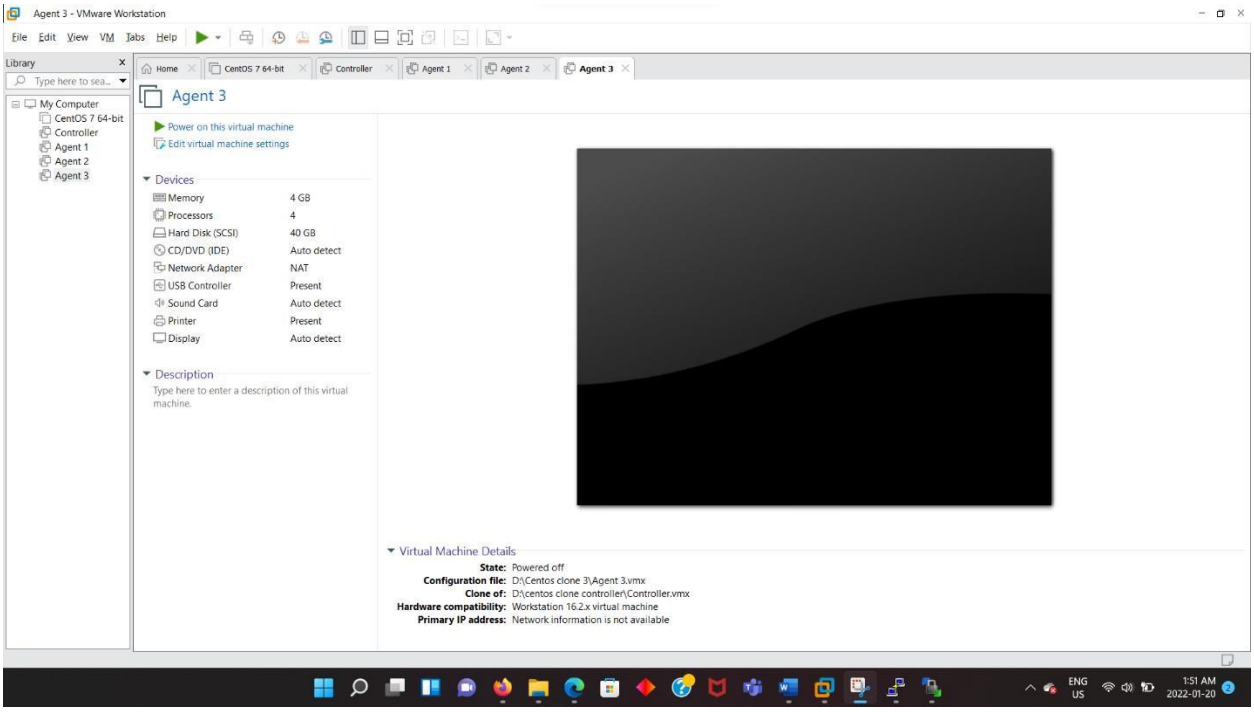
Configuration after restart



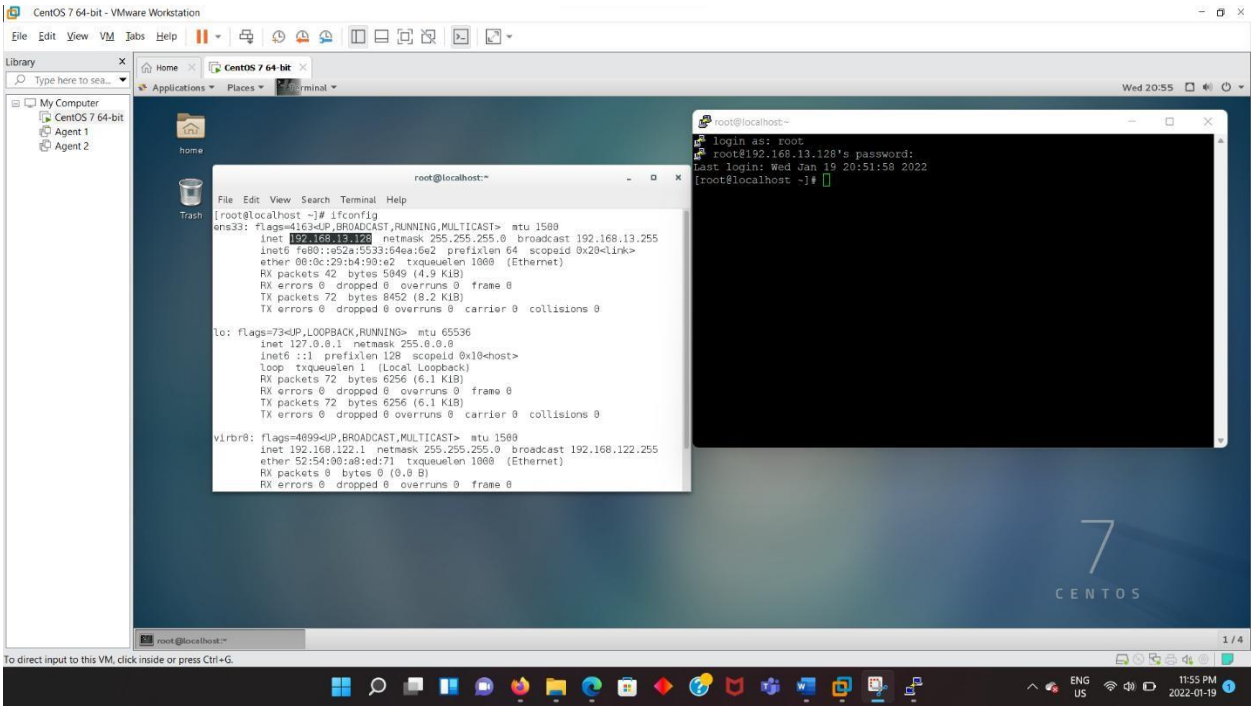
Centos installed successfully.



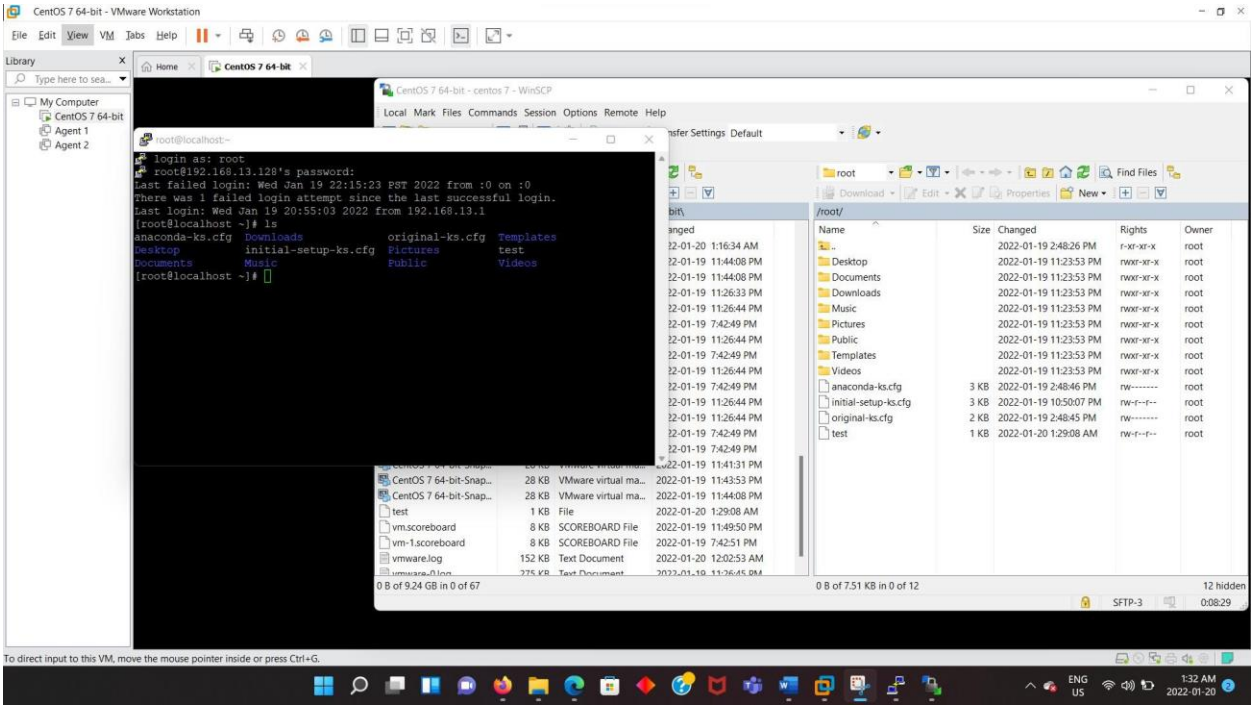
Created controller by cloning centos and 3 agents by cloning controller.

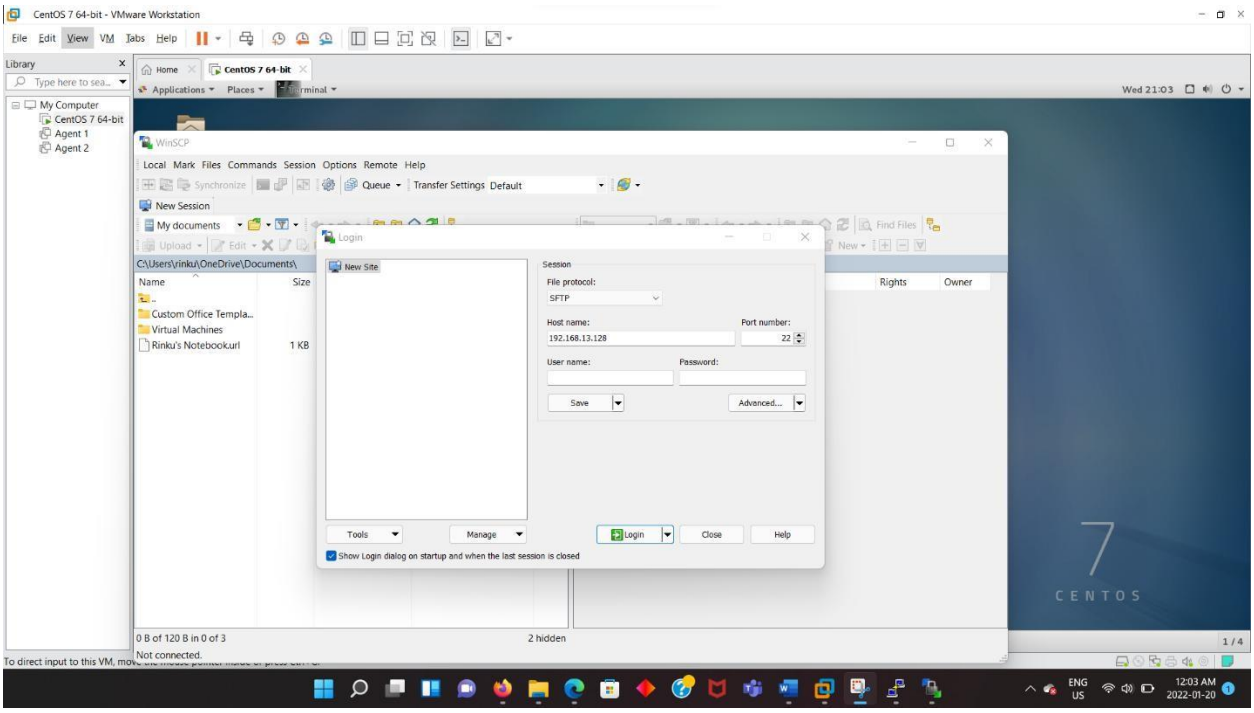


Installed putty and checking the functionality by pasting the IP address of centos and accepting the license.

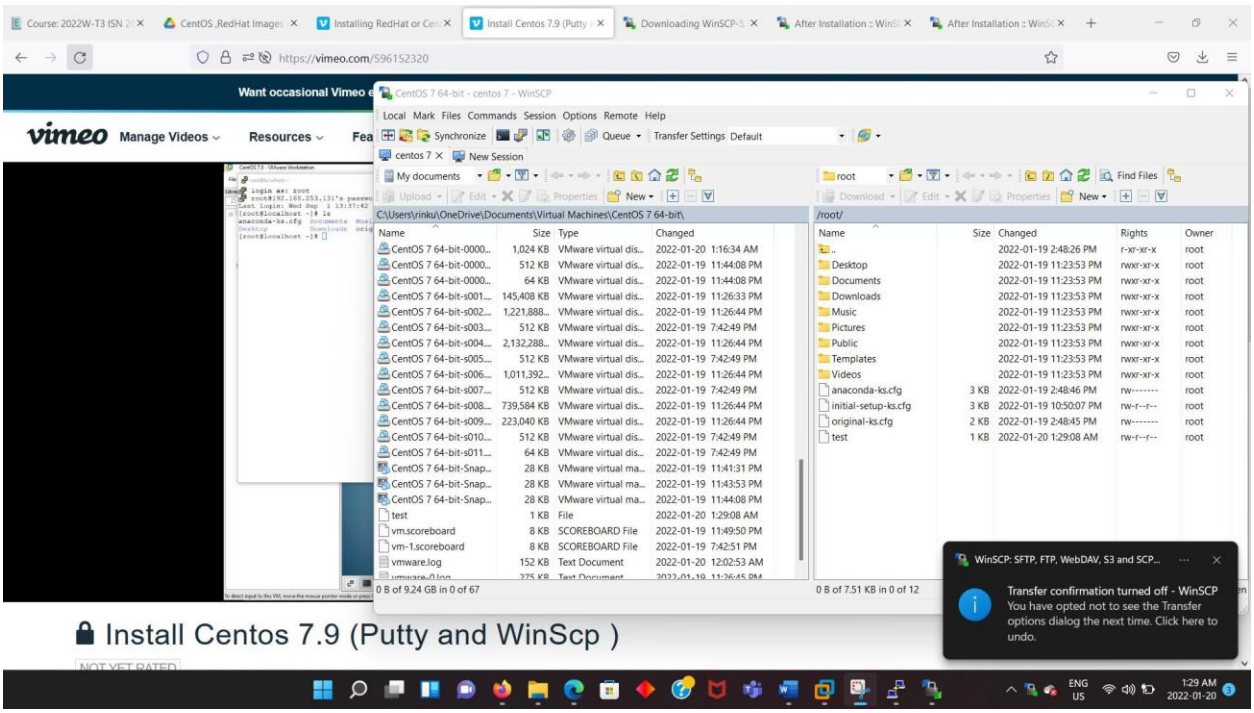


Installed and configured WinSCP by adding the IP address of centos.

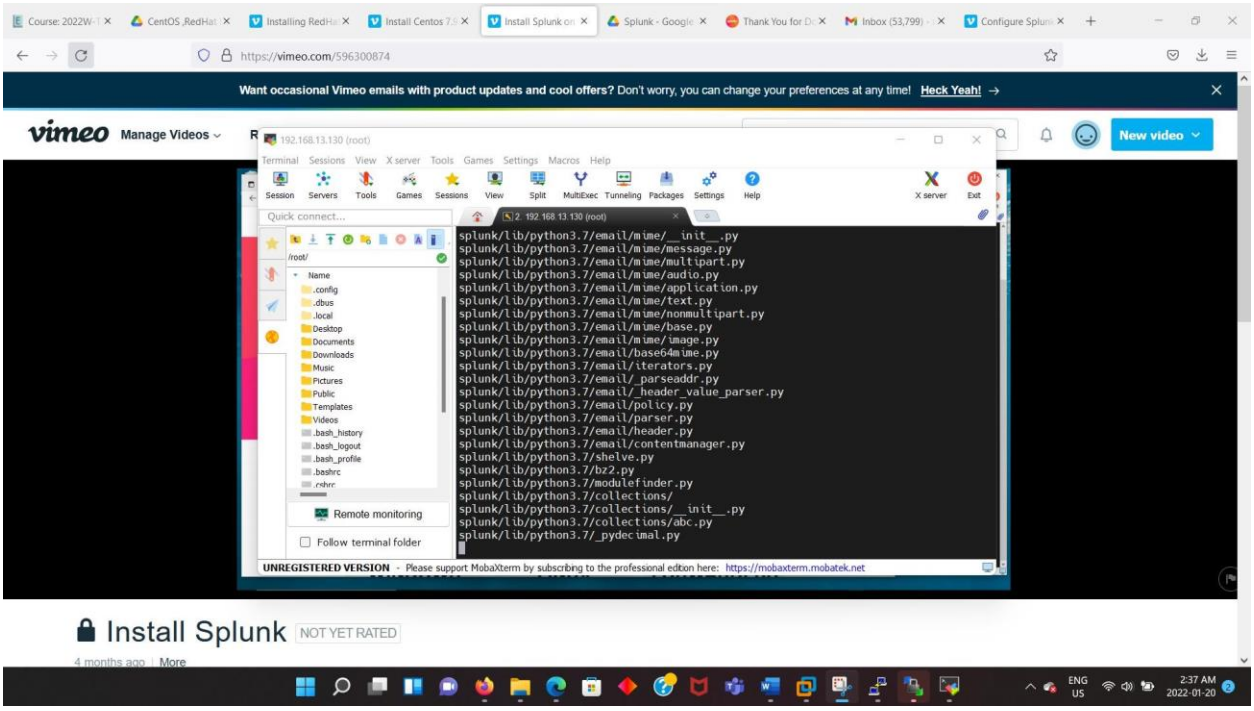




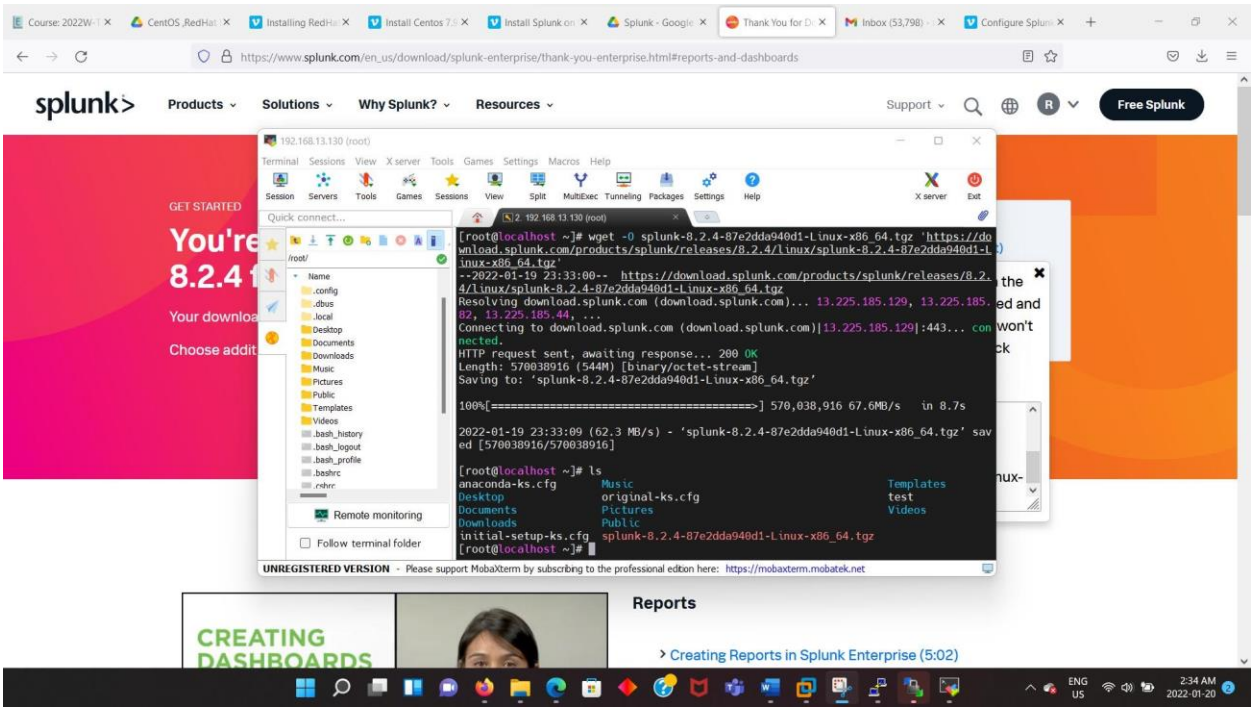
Created a test file on centos to check if the test file can be moved to the root server using the WinSCP tool. From the screenshot, it is evident that the test file was created and moved to the root server successfully.



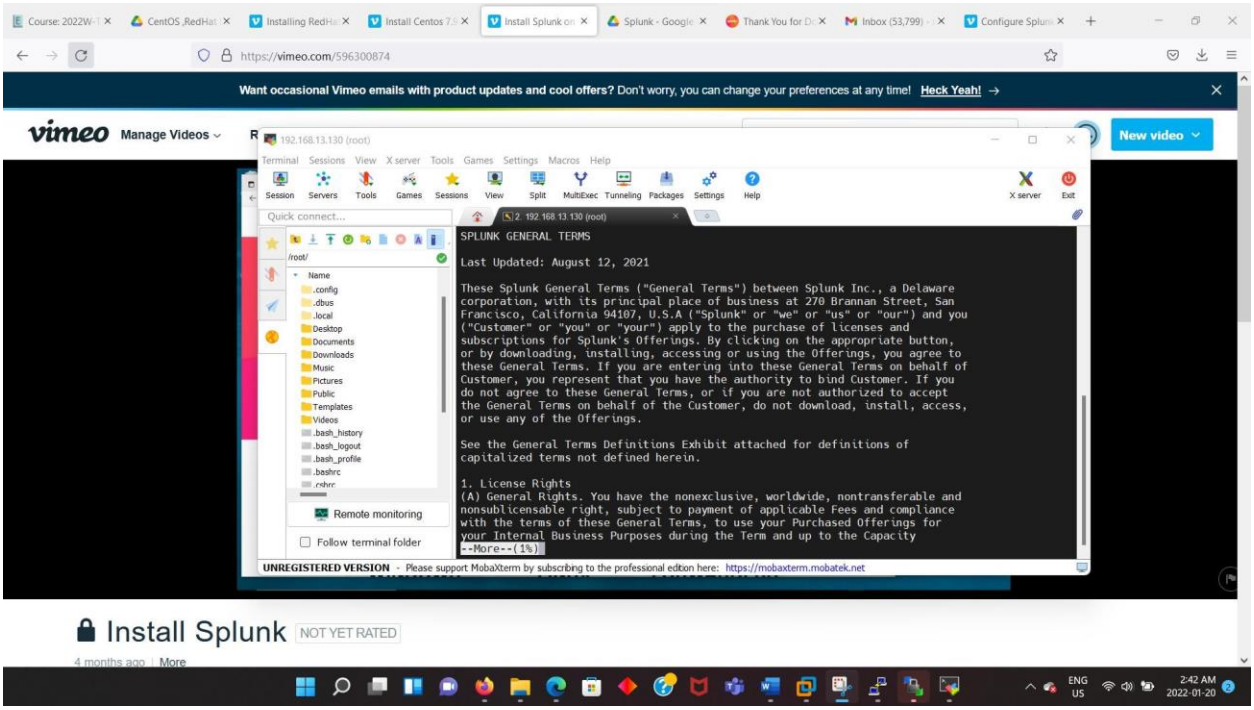
Extracting Splunk file



Listing Splunk file

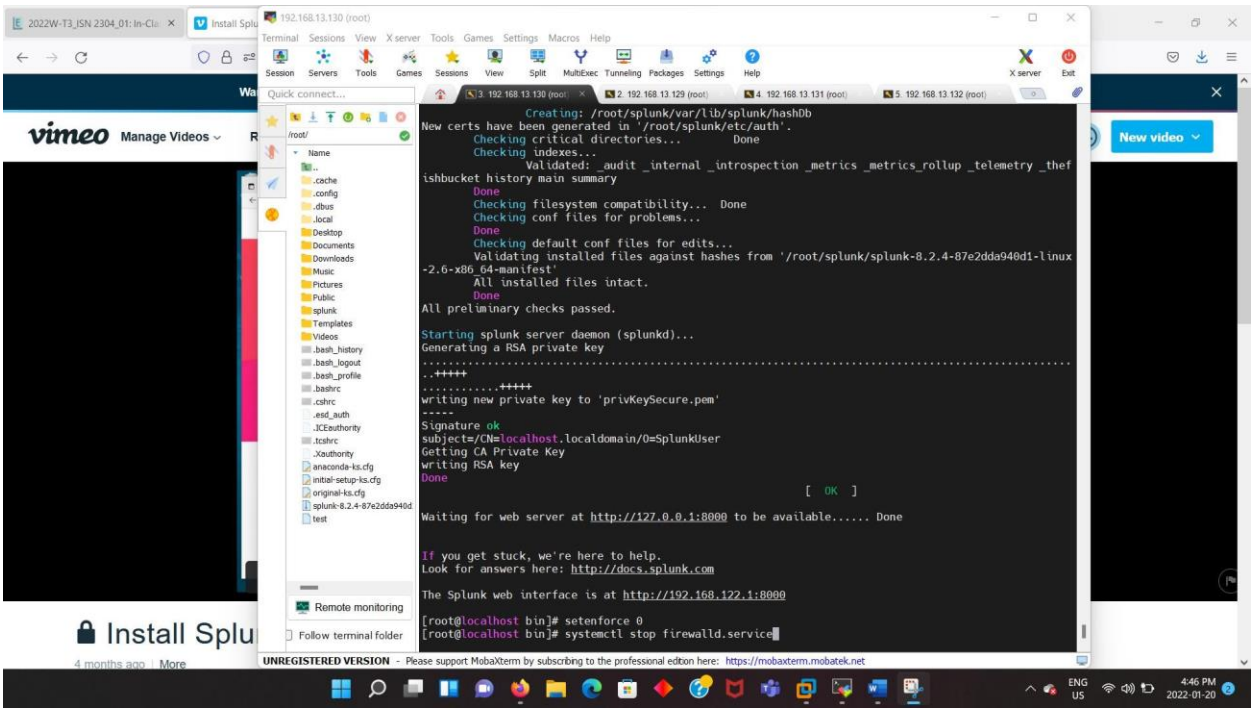


Launching Splunk

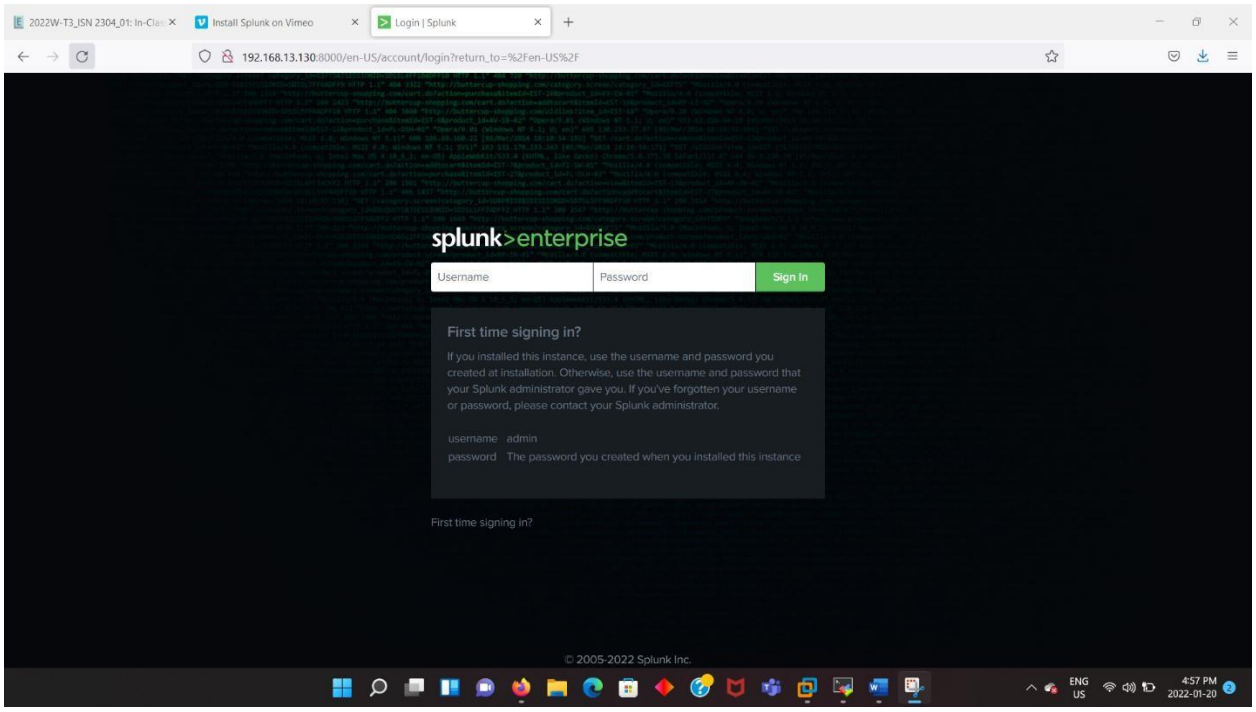


Initiated Splunk web interface and disabling the firewall by entering the command setenforce 0, systemctl stop firewalld.service.

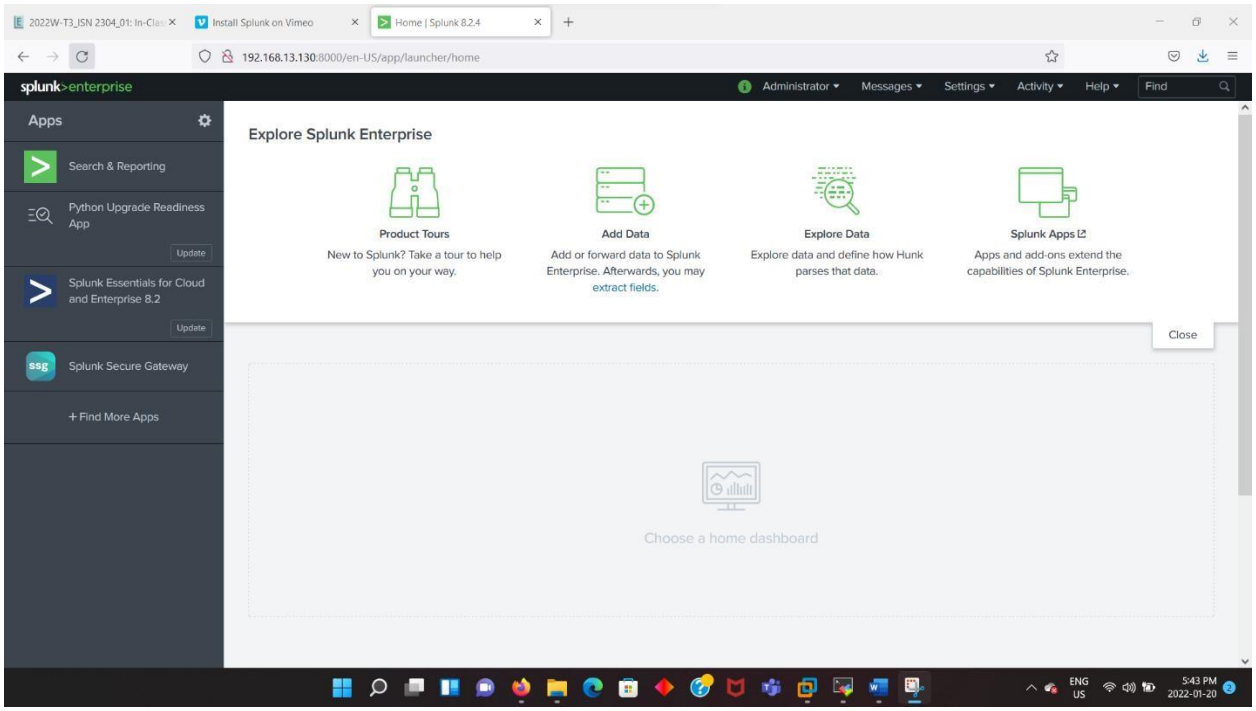
After that we again run ifconfig to check if the controller IP is the same.



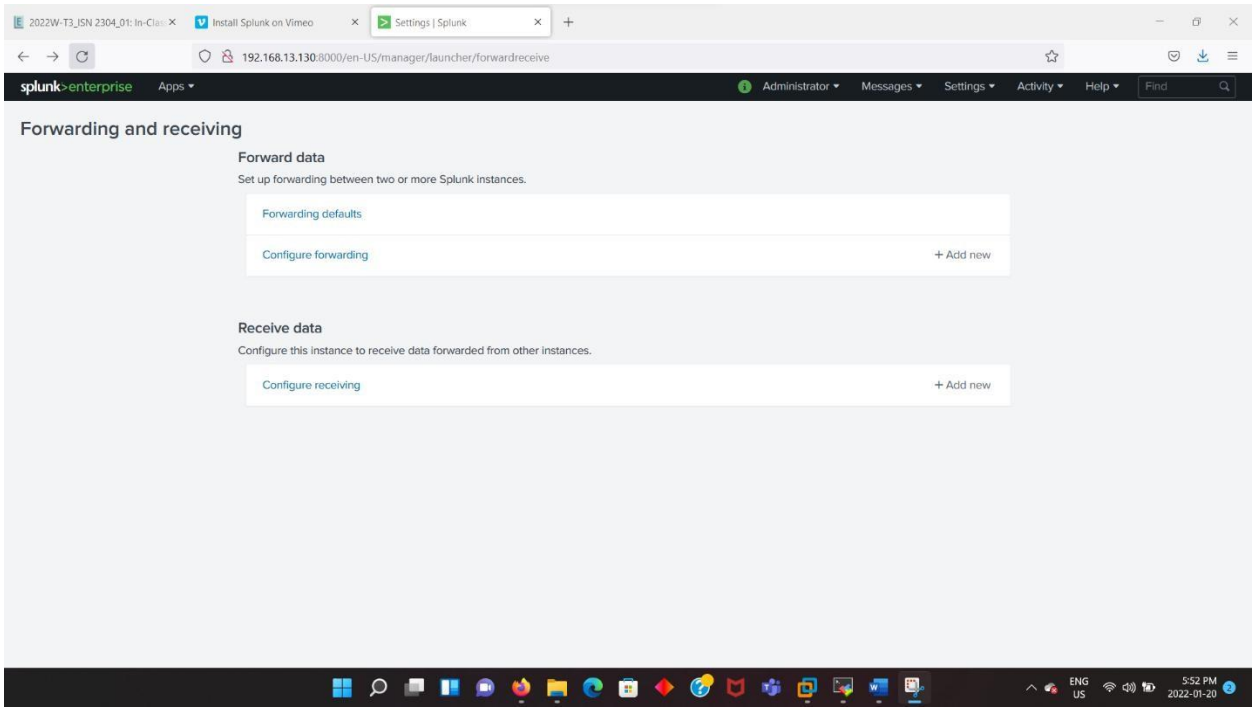
Once confirmed, open a web browser, and paste the IP address along with the port number 8000 and launch Splunk page as shown below.



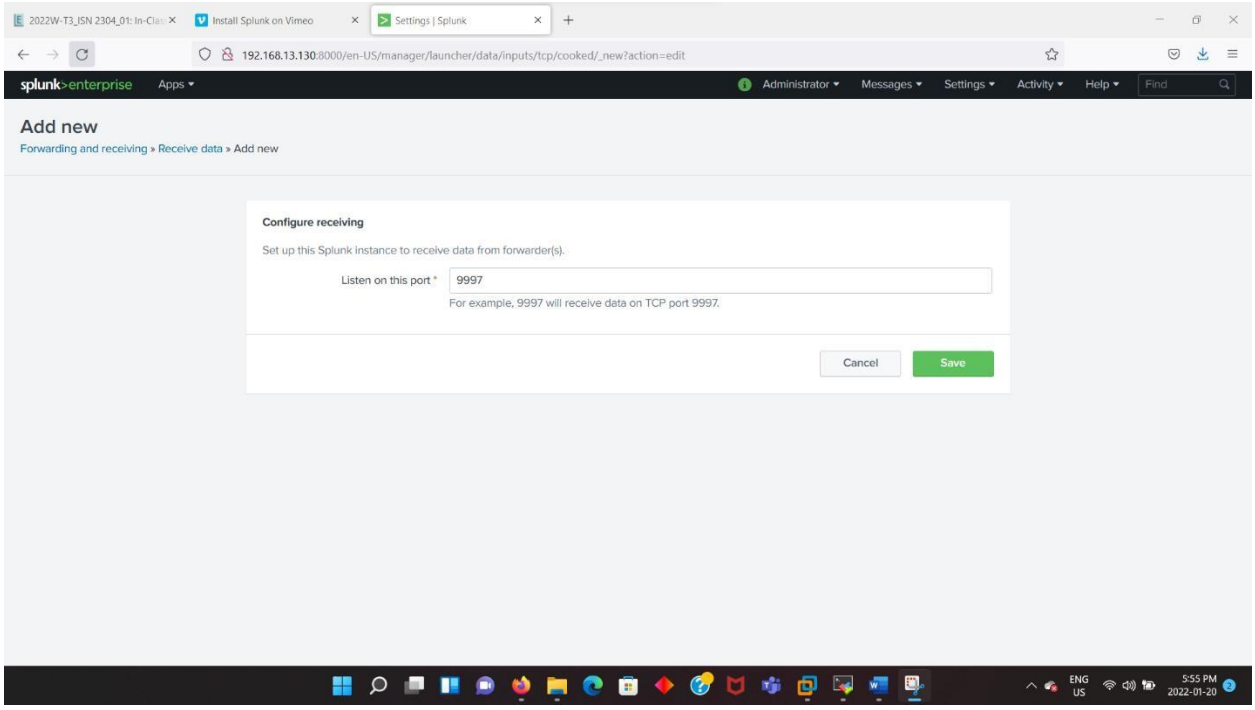
Logging in Splunk using the administrator password which was created during installation.



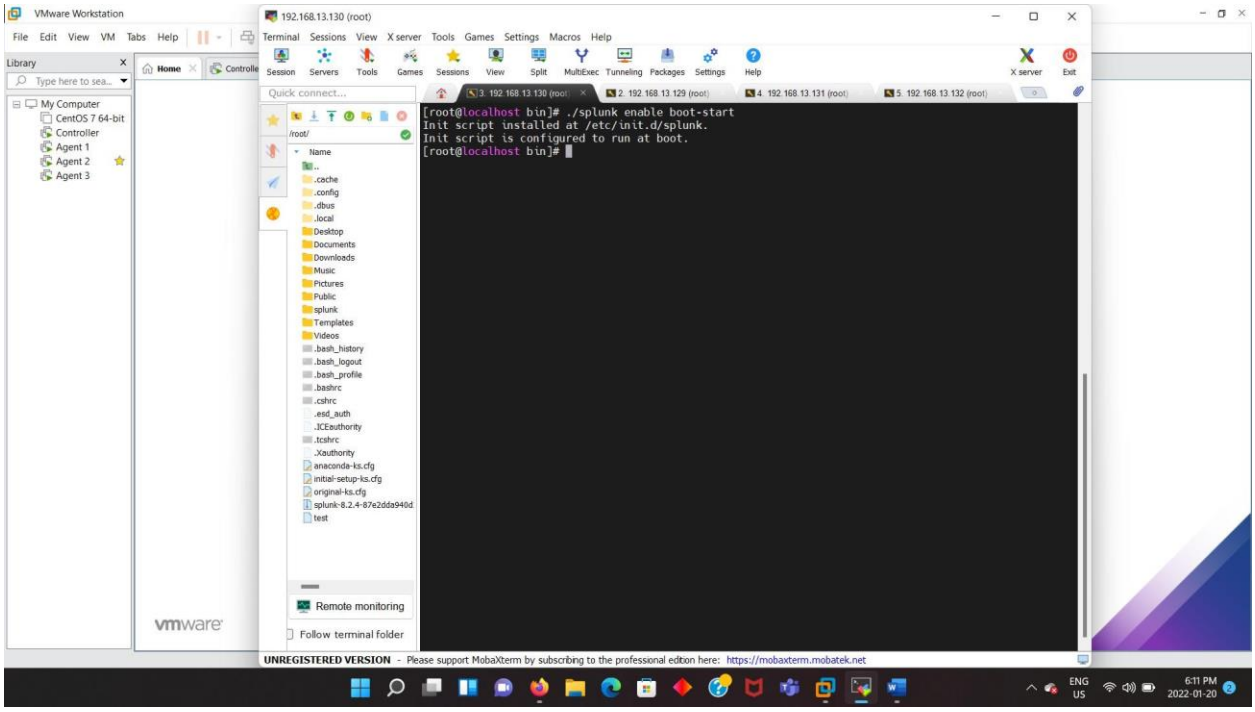
Configuring forwarding and receiving ports



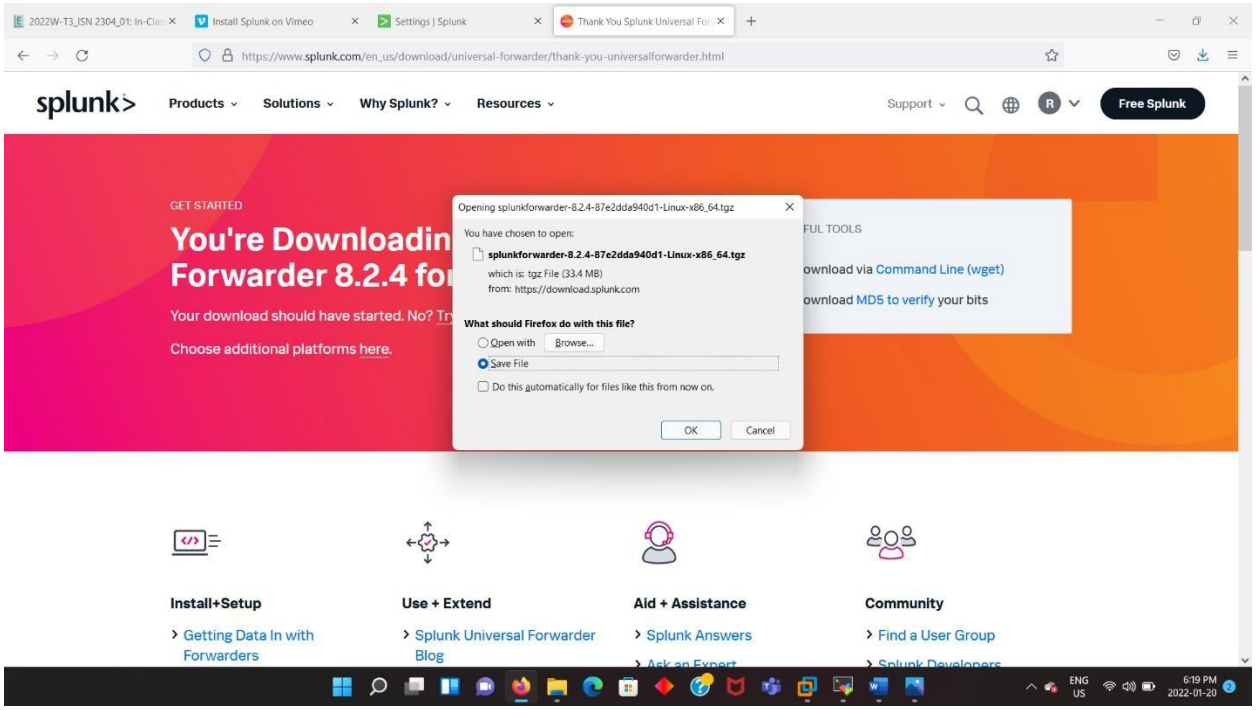
Configuring receiving port 9997 so that all the logs from other servers will get received to this port.



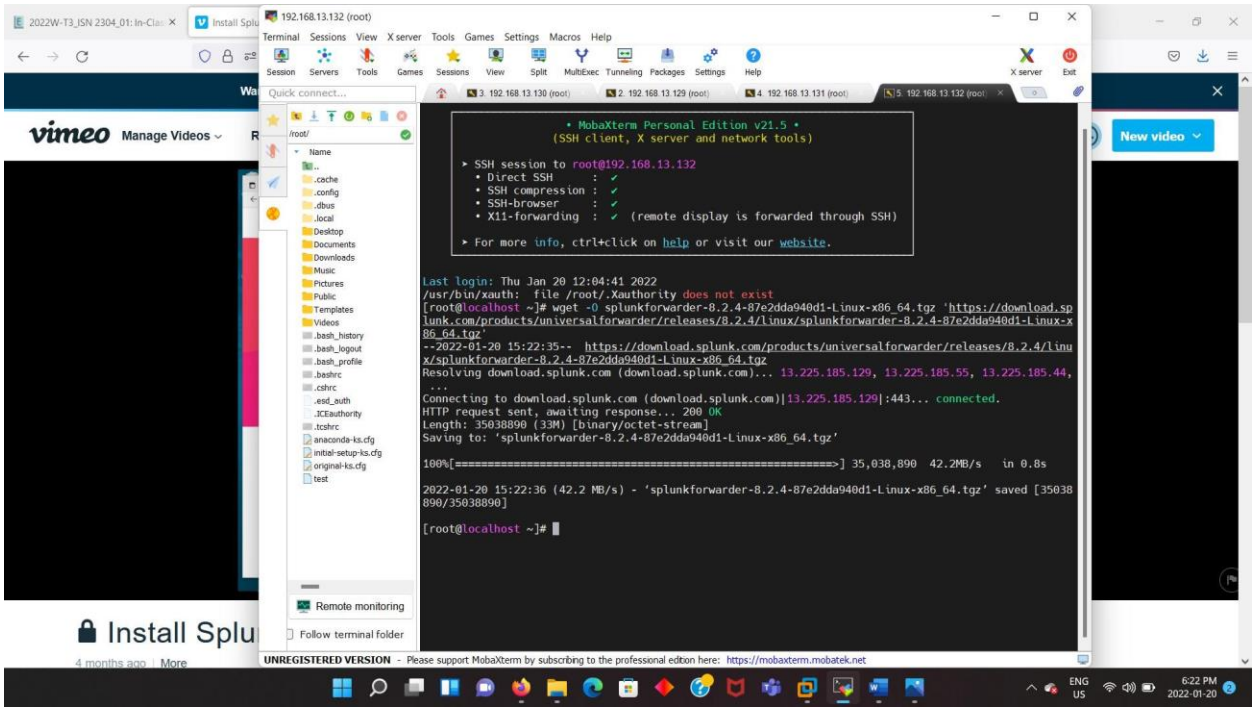
Enabling the boot start command in the controller console by using ./splunk enable boot-start

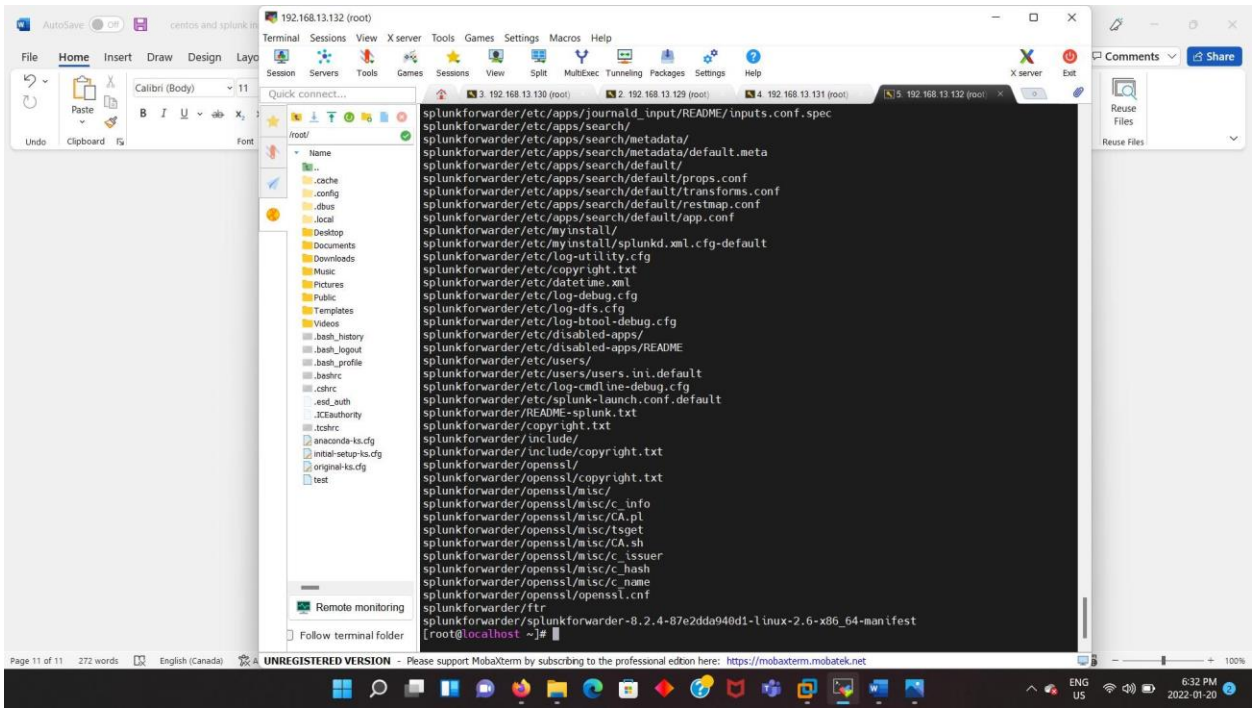


Install Splunk universal forwarder for Agent 1



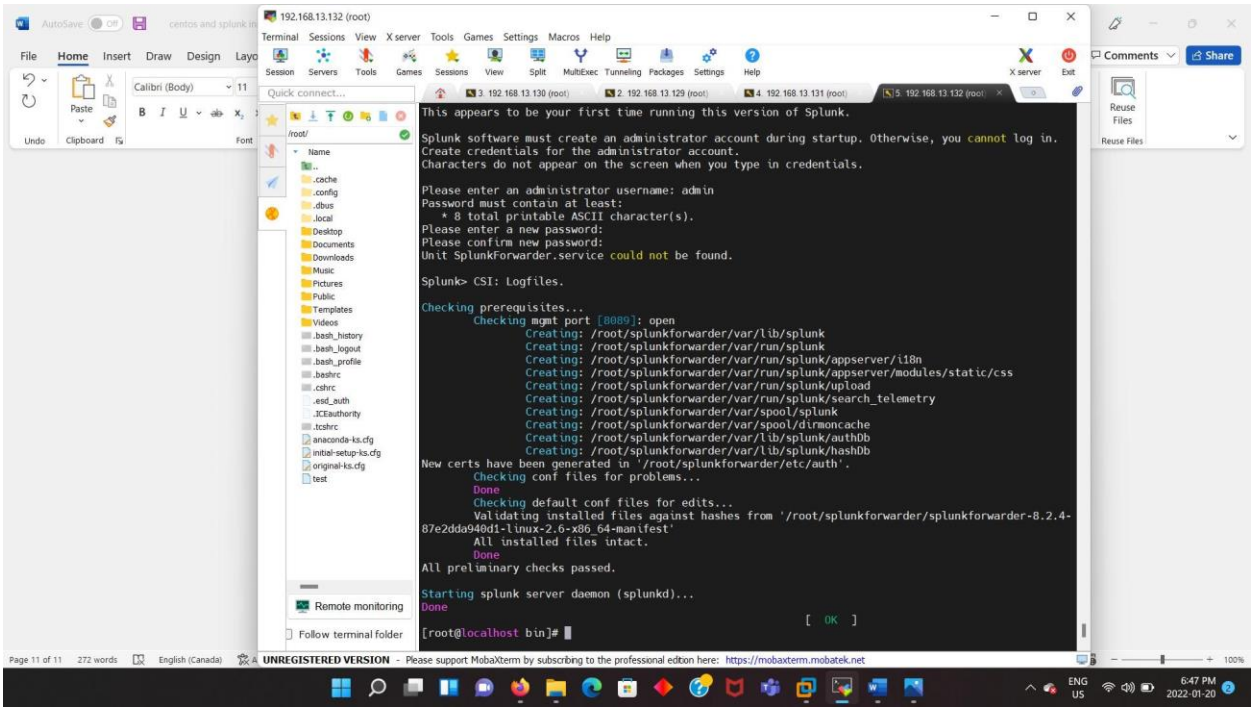
Install universal forwarder on agent 1, 2 and 3 by extracting the command line file



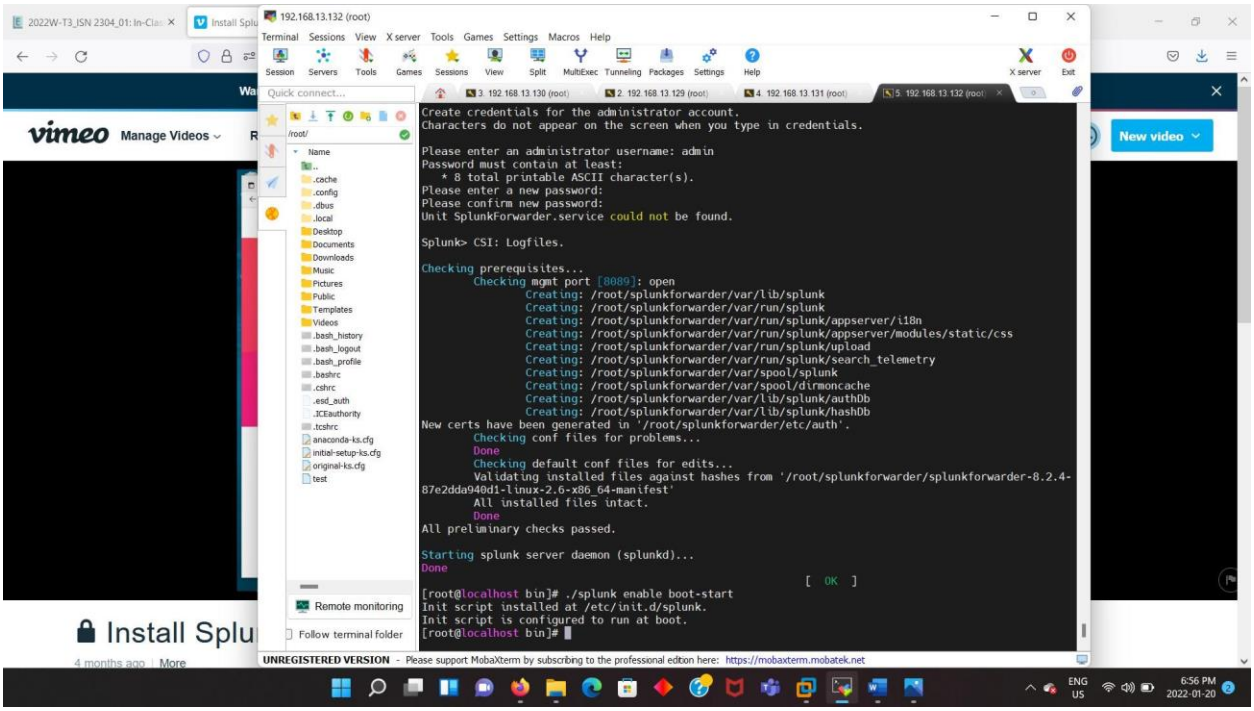


Launching Splunk in Splunk forwarder following the previous method and then the management Port 8089 gets identified.

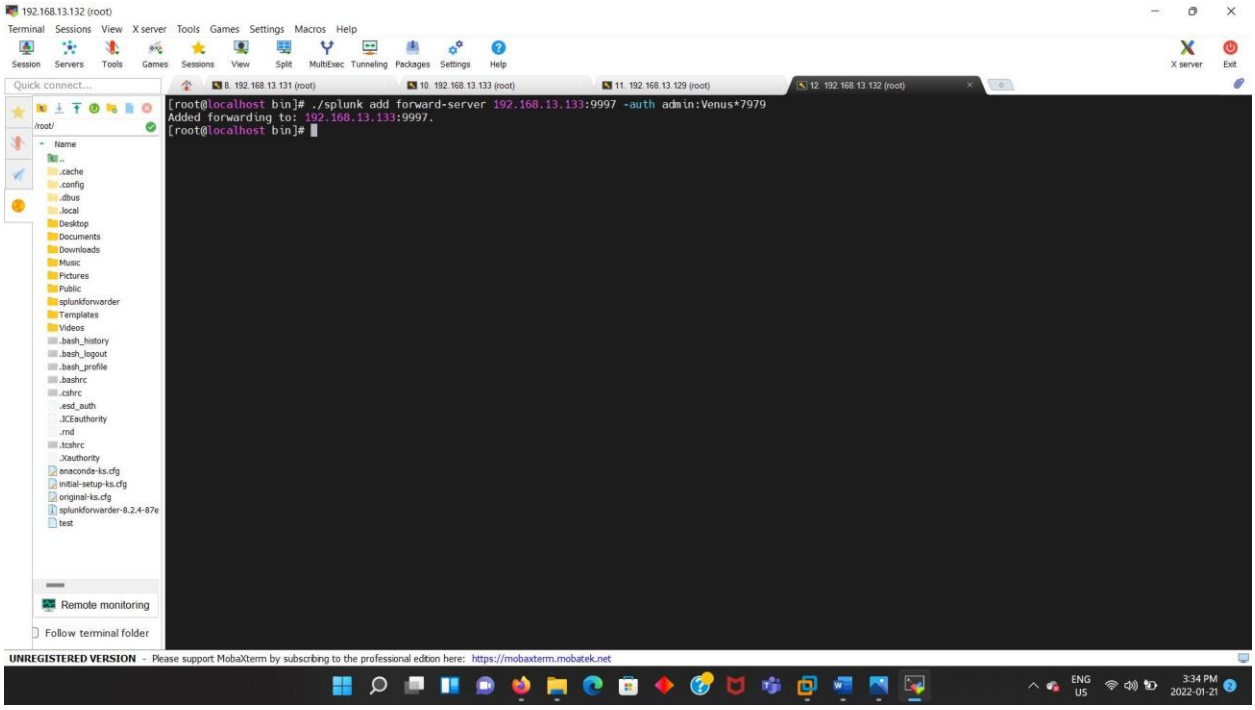
Follow the same steps on all 3 agents.



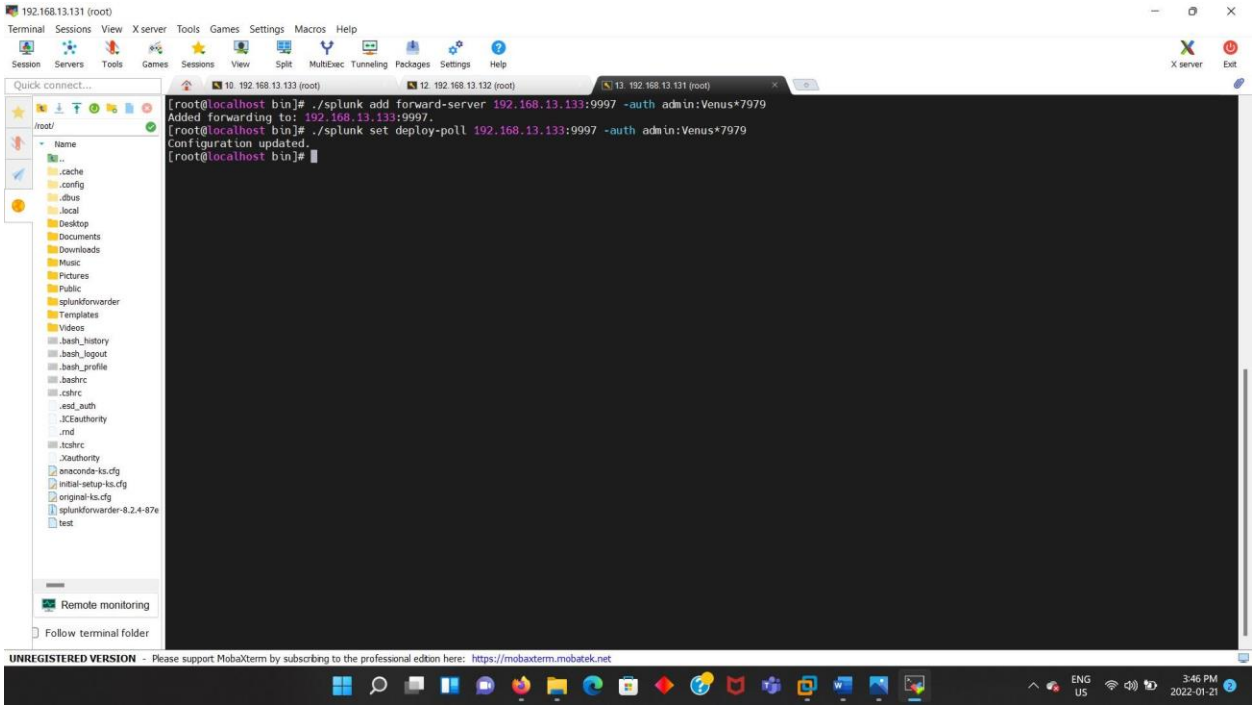
Start the services manually on all 3 agents by using ./splunk enable boot-start



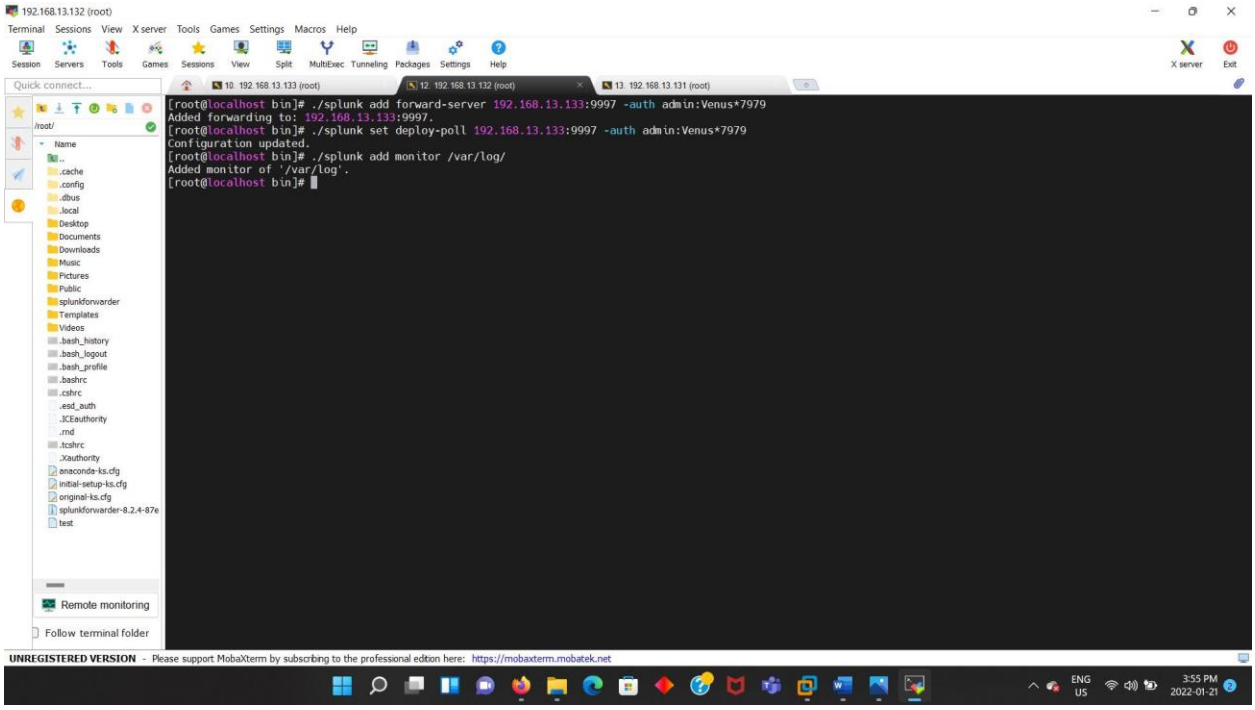
Added the forwarder server by authenticating admin credentials



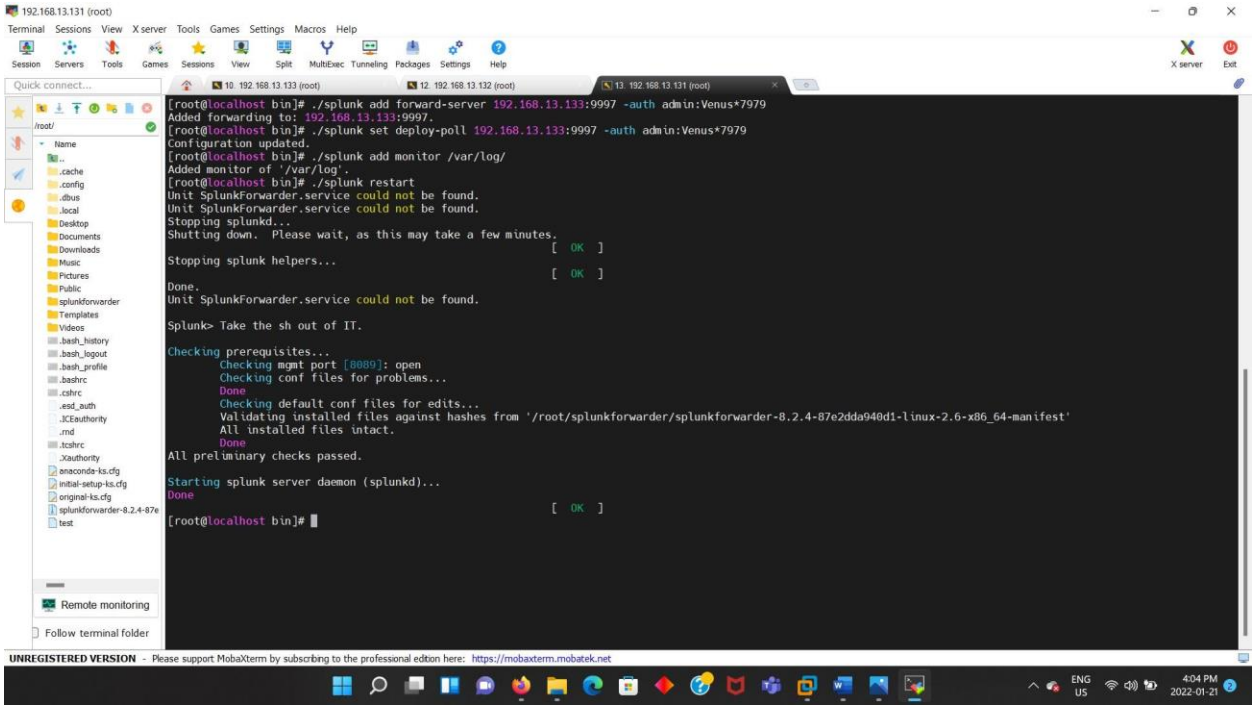
Deployed to make sure the data is sent from client to the server.



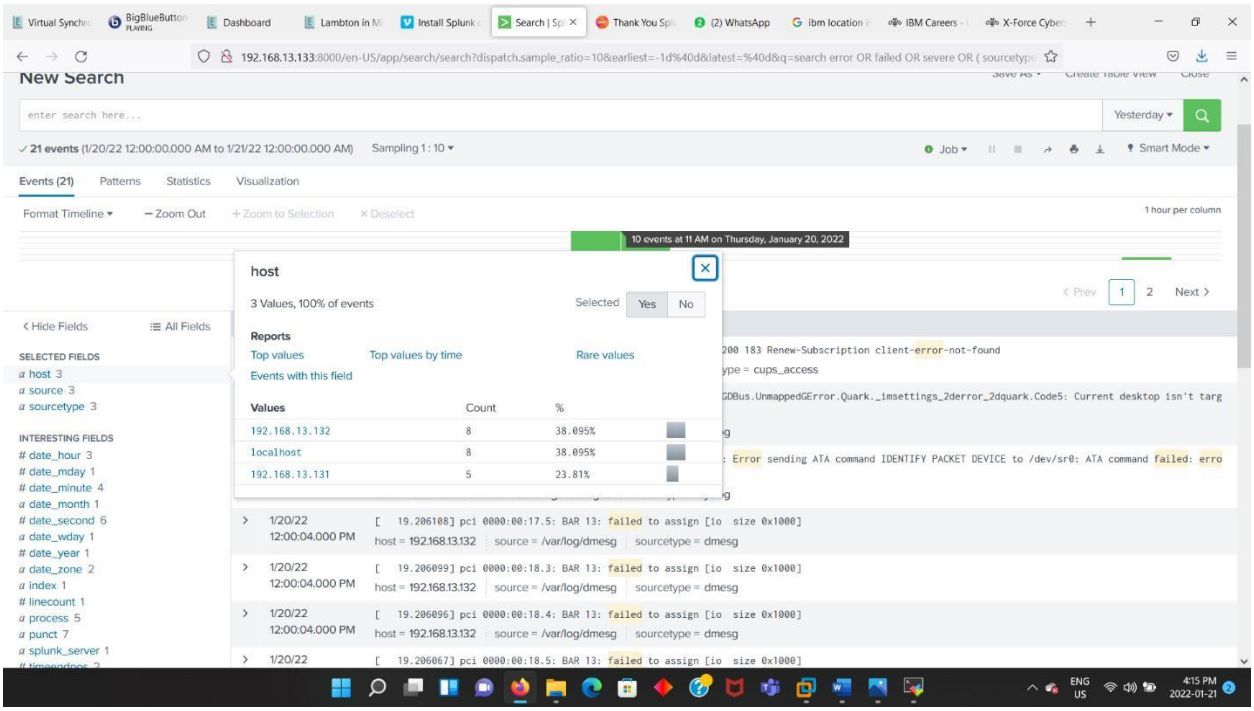
To monitor the logs, we add the agents that has to be monitored by executing the command ./splunk add monitor /var/log



Restarted Agents.



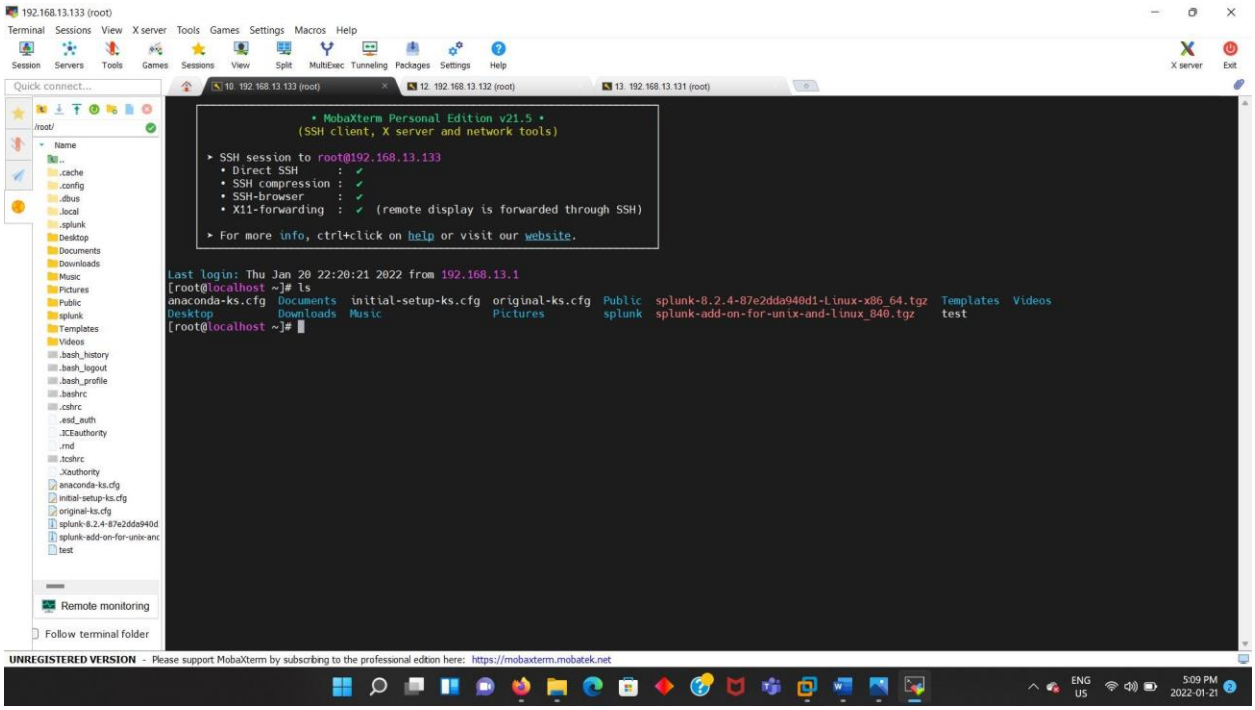
Captured logs for 2 Agents successfully


New Search
enter search here...
Yesterday
21 events (1/20/22 12:00:00.000 AM to 1/21/22 12:00:00.000 AM)
Sampling 1 : 10
Job
Smart Mode
Events (21)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
10 events at 11 AM on Thursday, January 20, 2022
host
3 Values, 100% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Values
Count
%
192.168.13.132
8
38.095%
localhost
8
38.095%
192.168.13.131
5
23.81%
Hide Fields
All Fields
SELECTED FIELDS
a host 3
a source 3
a sourcetype 3
INTERESTING FIELDS
date_hour 3
date_mday 1
date_minute 4
a date_month 1
date_second 6
a date_wday 1
date_year 1
a date_zone 2
a index 1
linecount 1
a process 5
a punct 7
a splunk_server 1
Prev
1
2
Next
1/20/22 12:00:04.000 PM
[19.206108] pci 0000:00:17.5: BAR 13: failed to assign [io size 0x1000]
host = 192.168.13.132 source = /var/log/dmesg sourcetype = dmesg
[19.206099] pci 0000:00:18.3: BAR 13: failed to assign [io size 0x1000]
[19.206096] pci 0000:00:18.4: BAR 13: failed to assign [io size 0x1000]
[19.206067] pci 0000:00:18.5: BAR 13: failed to assign [io size 0x1000]
ENG
US
4:15 PM
2022-01-21

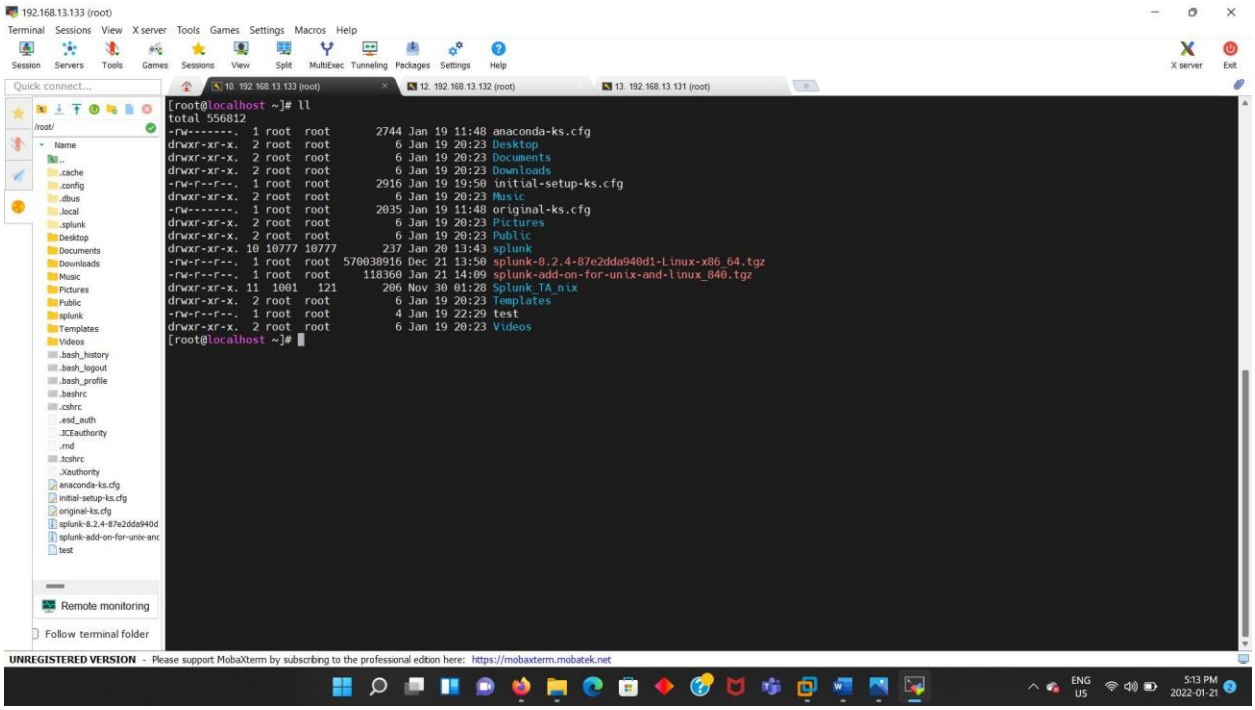
Part 2

Splunk Adds on and running a query

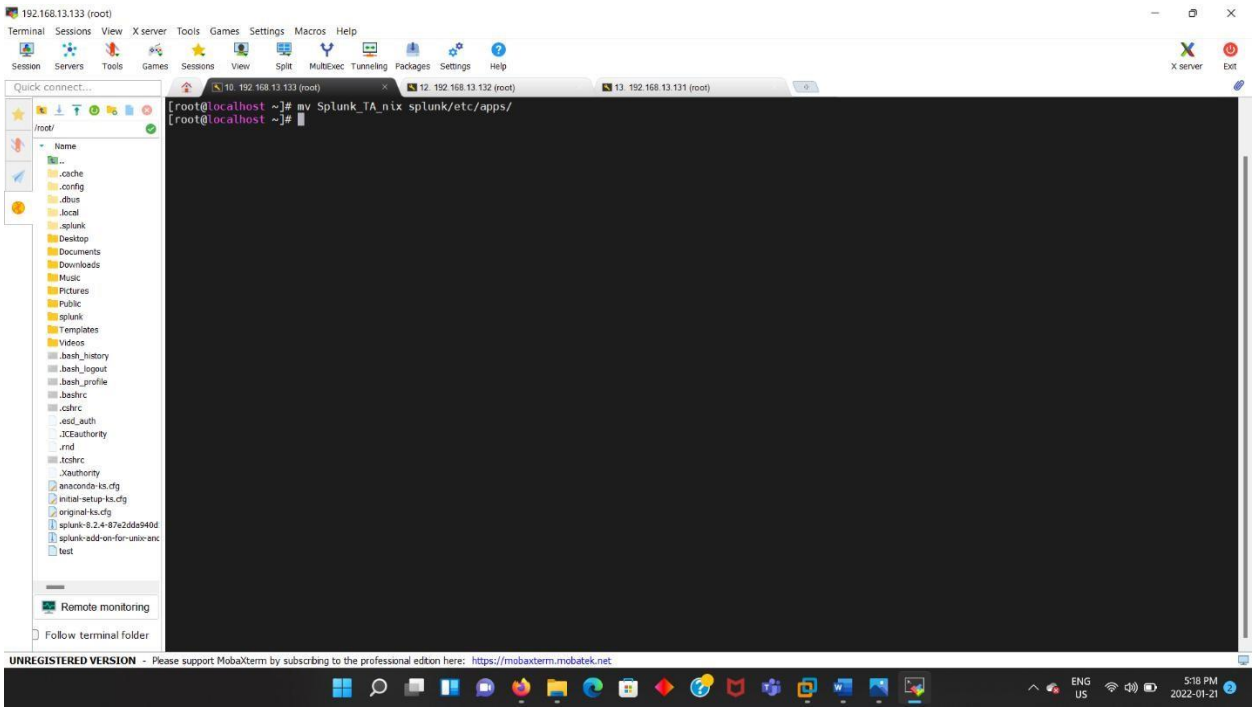
Downloaded Splunk adds – on file and listed to confirm if it is installed successfully.



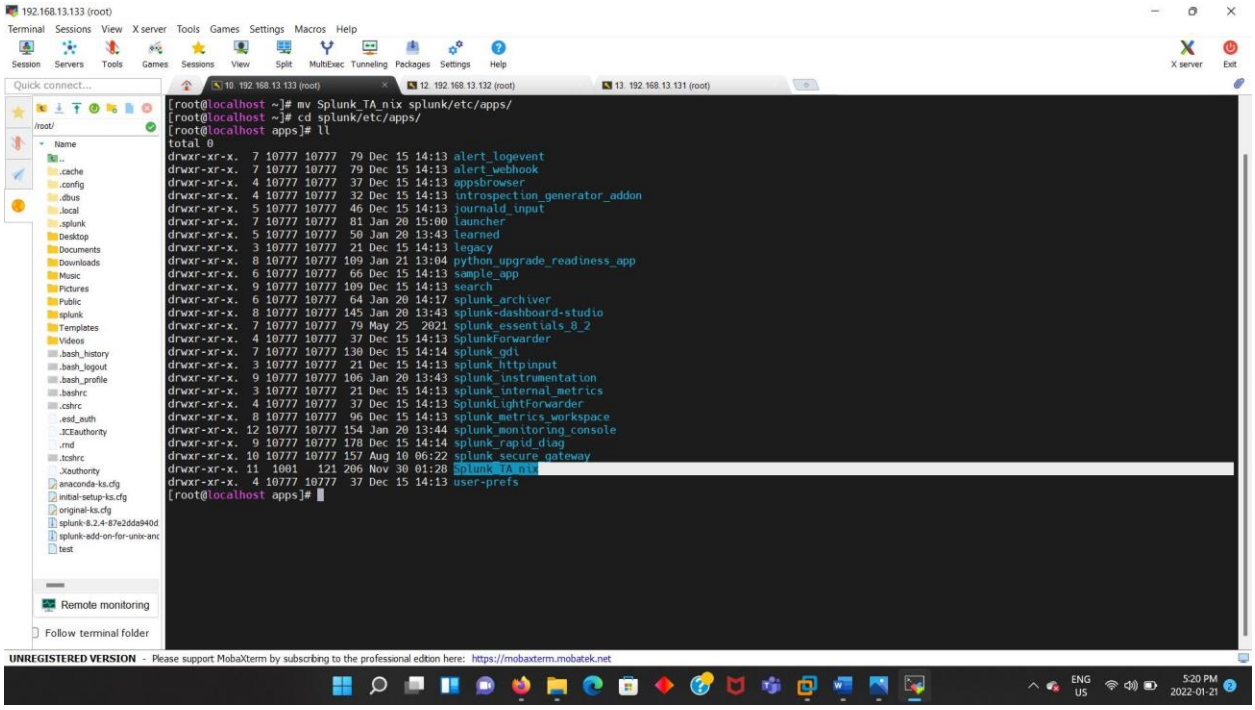
Extracted the file using tar -xvf command and listed



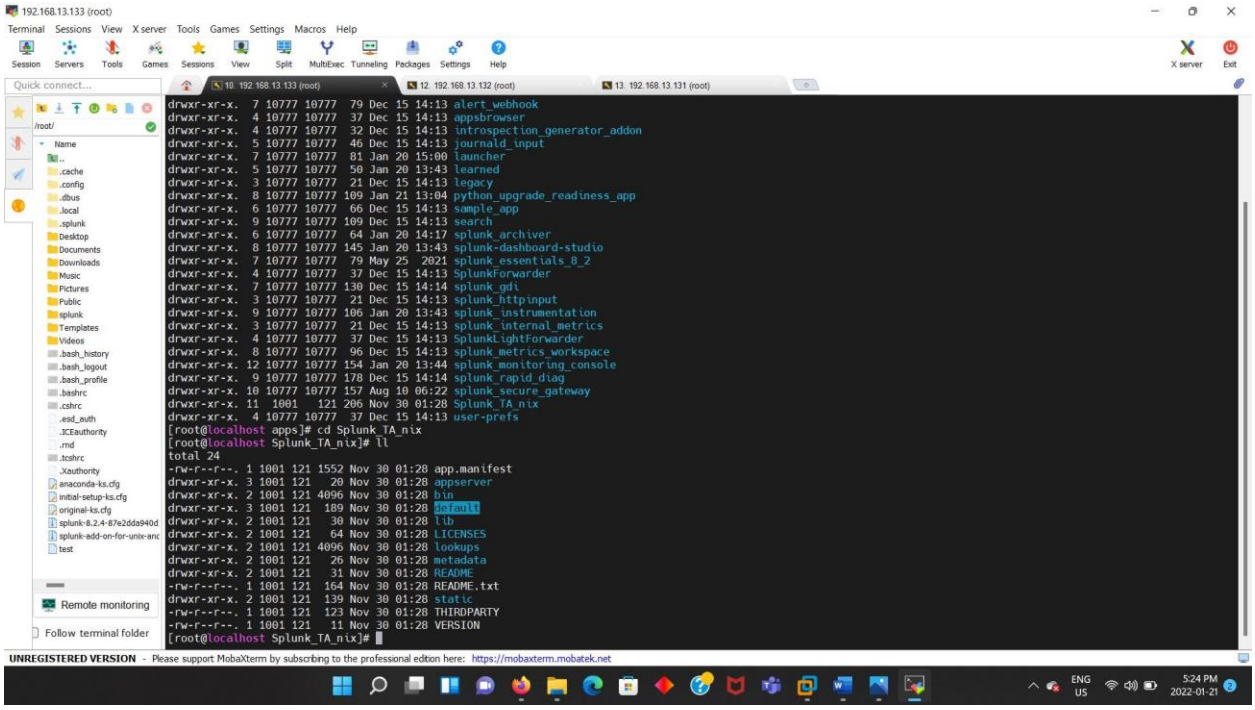
Moved the file to splunk/etc/apps/ directory



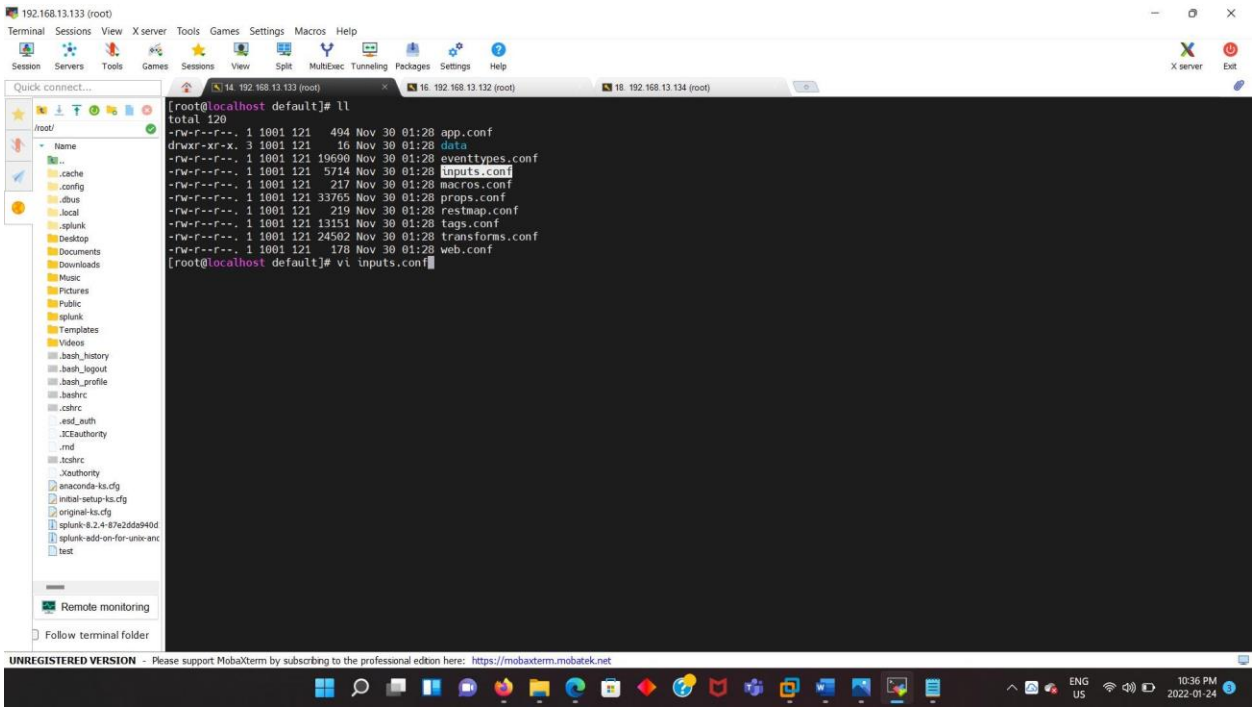
File moved successfully



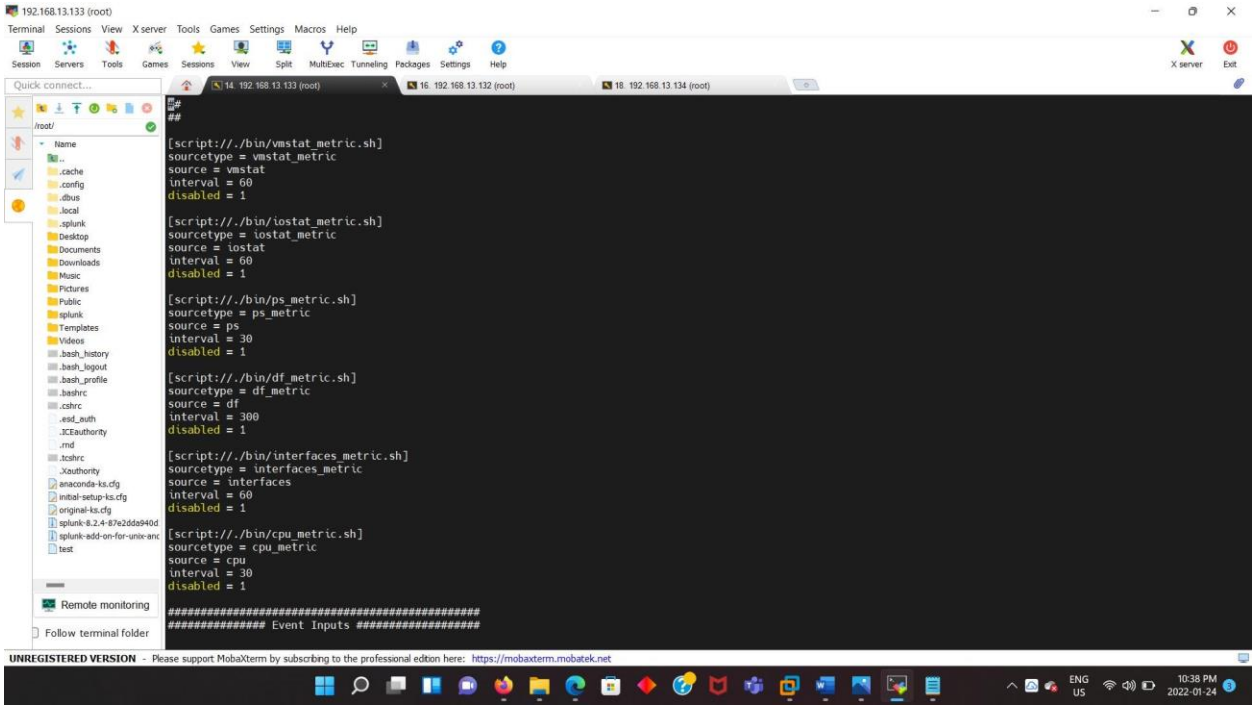
Listing the files under Splunk directory using cd Splunk_TA_nix



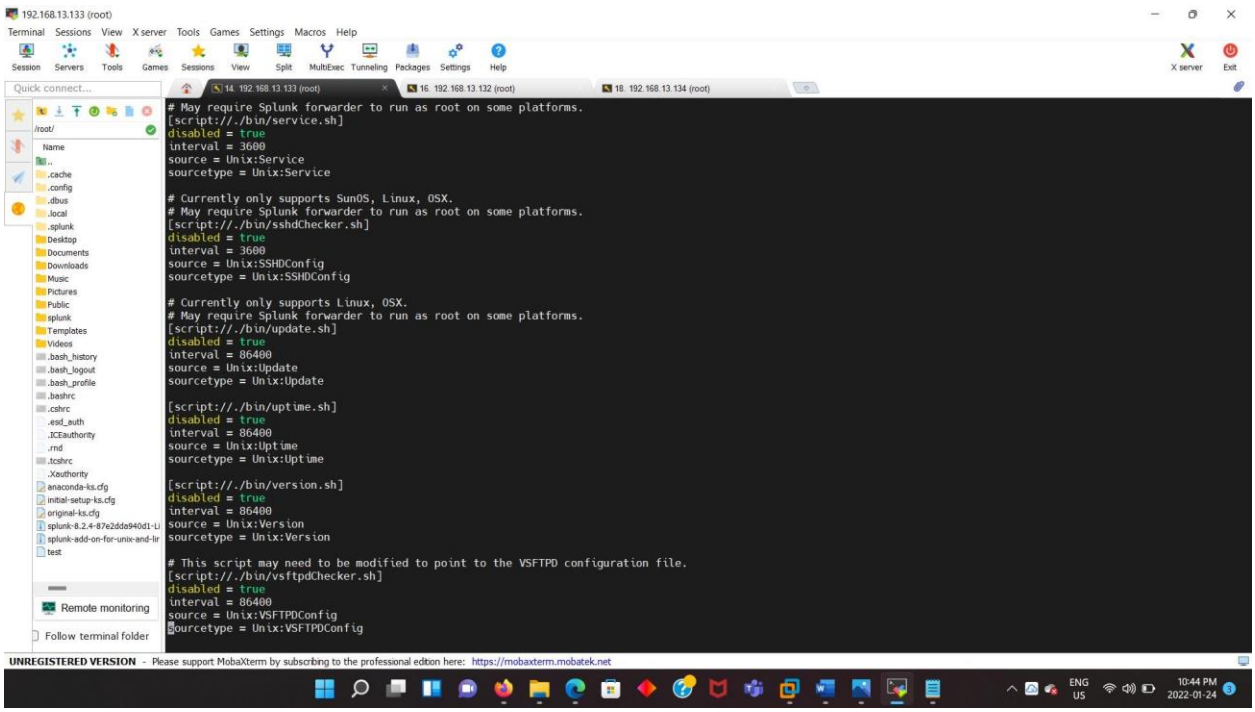
After that enter cd default and list the default directories by typing ll. We get one of the files named inputs.conf under default directory. So, we check that file in detail by entering the command vi inputs.conf



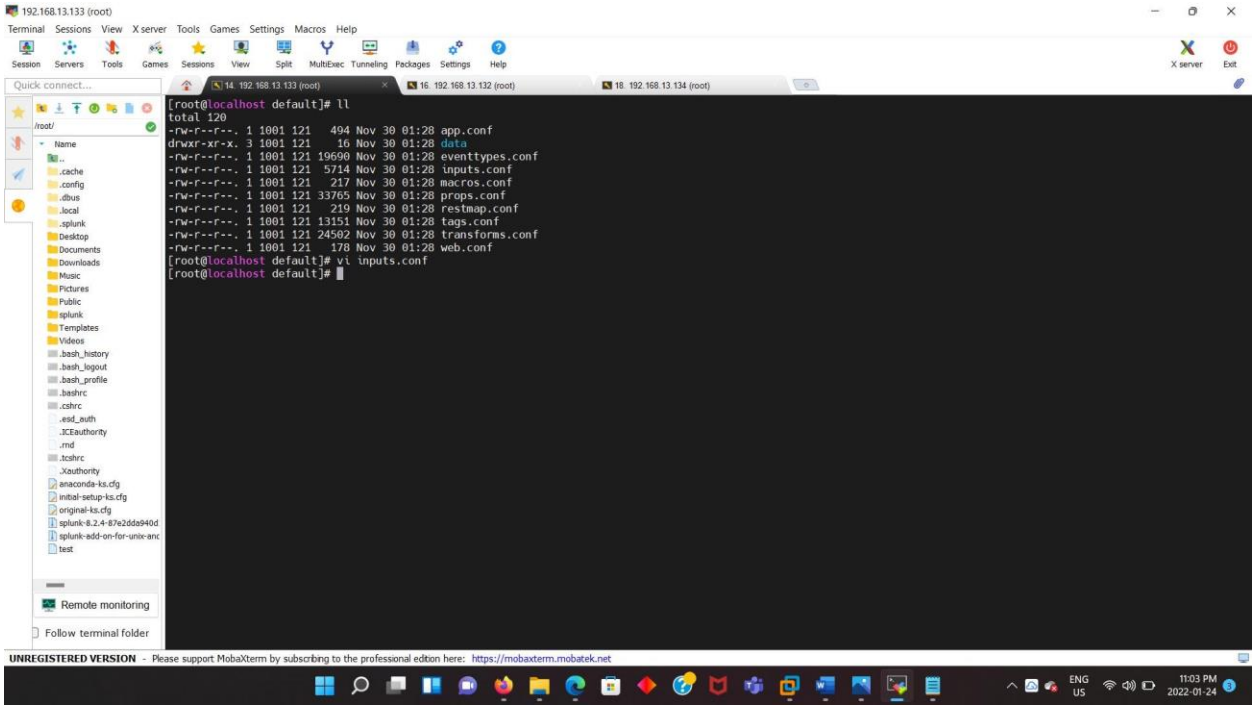
The output is shown below.



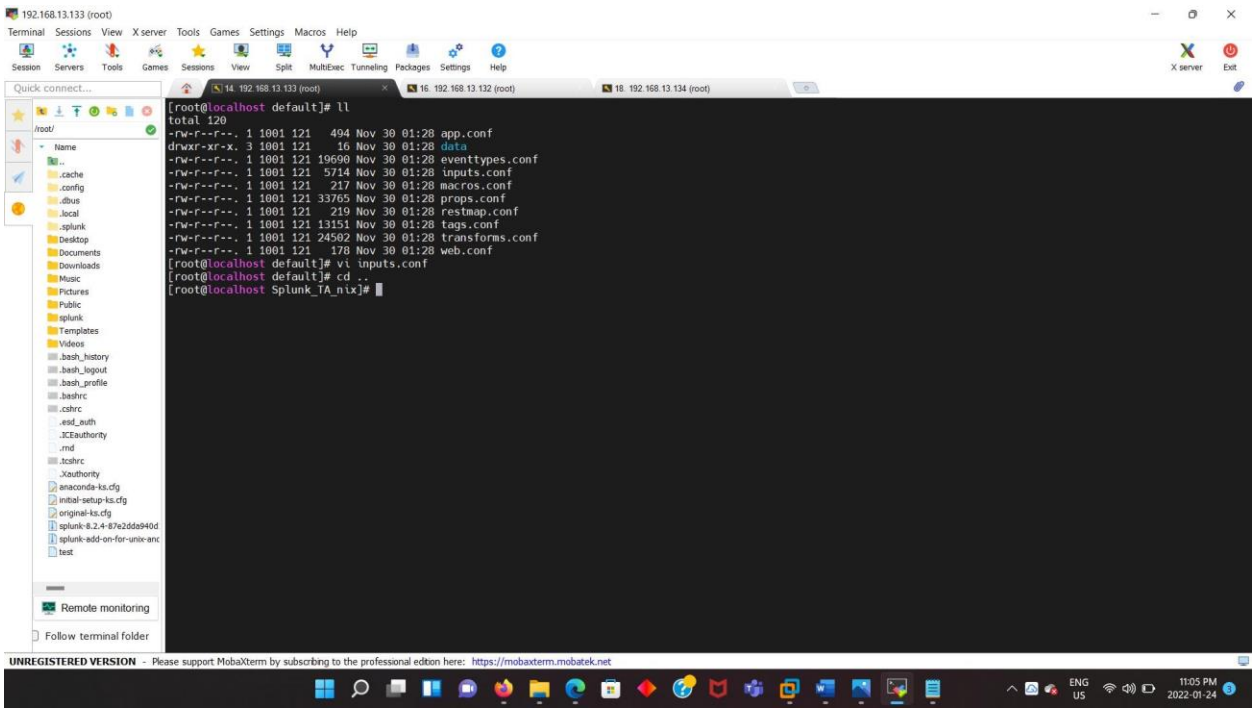
Now we are going to modify all the disabled values to 0 and if any value is true, then we will change to false value.



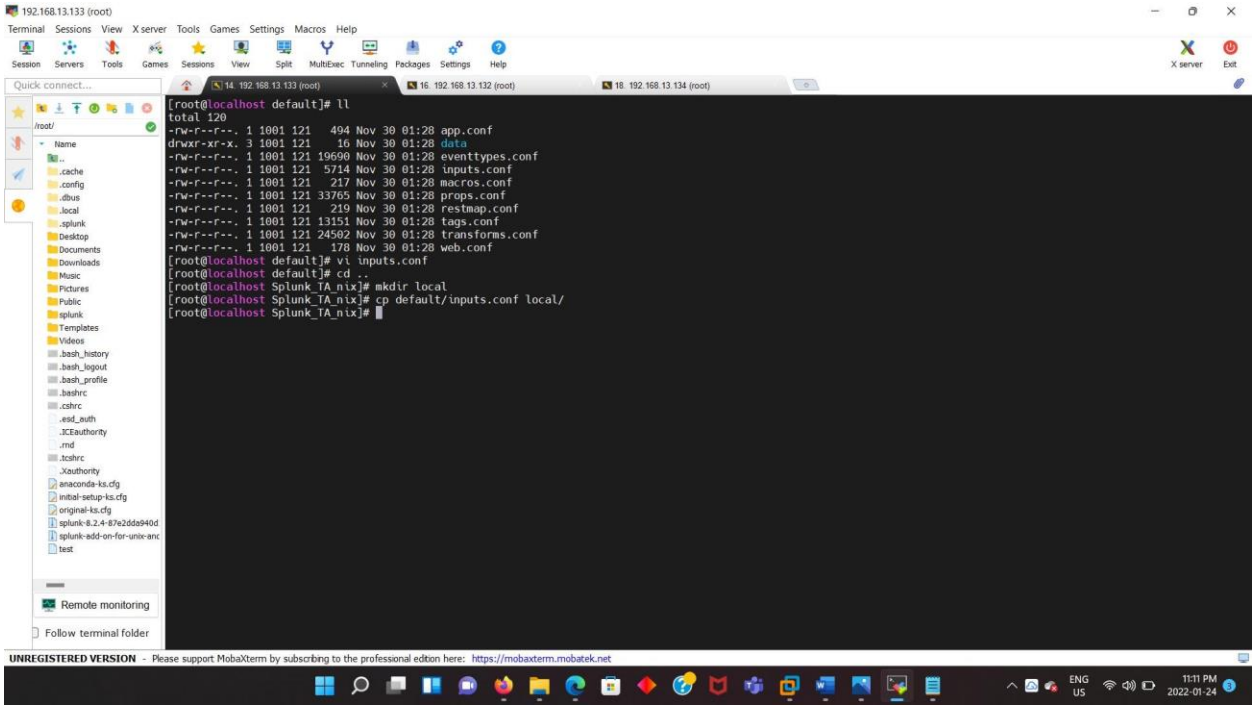
We exit from this page to the vi inputs.conf (previous page) by entering: q! and click enter.



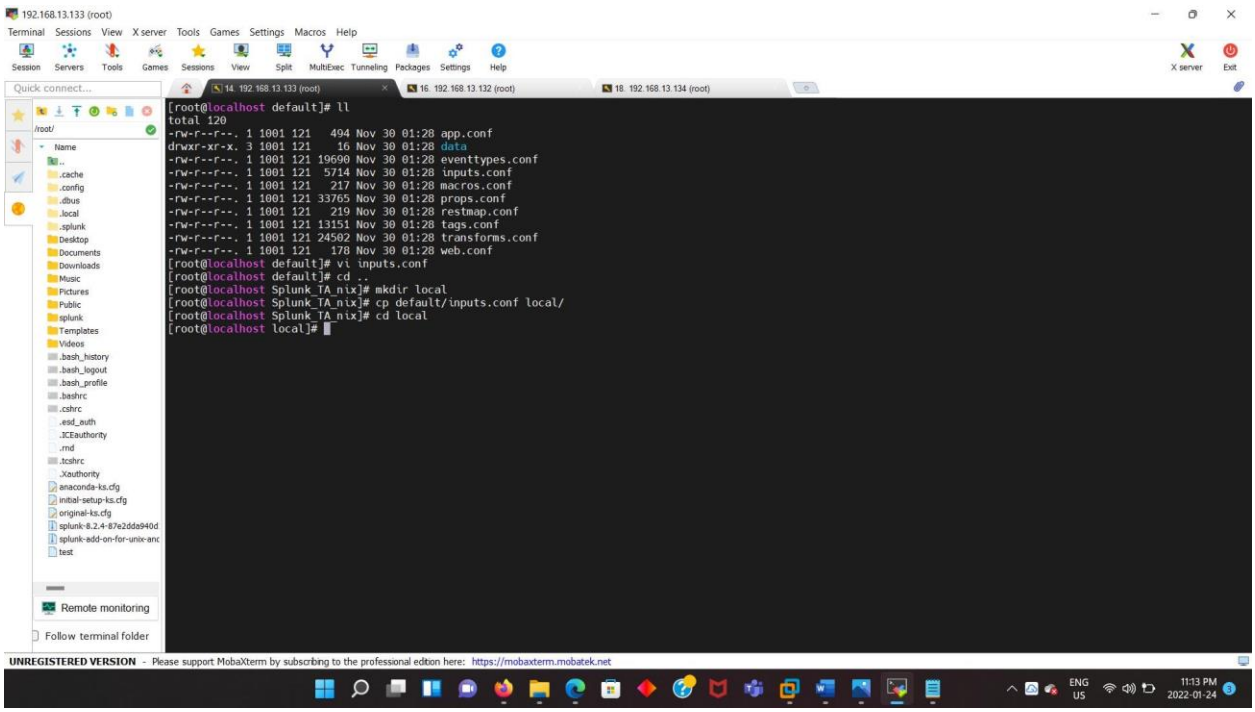
Now we go back by executing cd ..



Now we make a new directory named local by typing mkdir local and move all the inputs to the local directory.

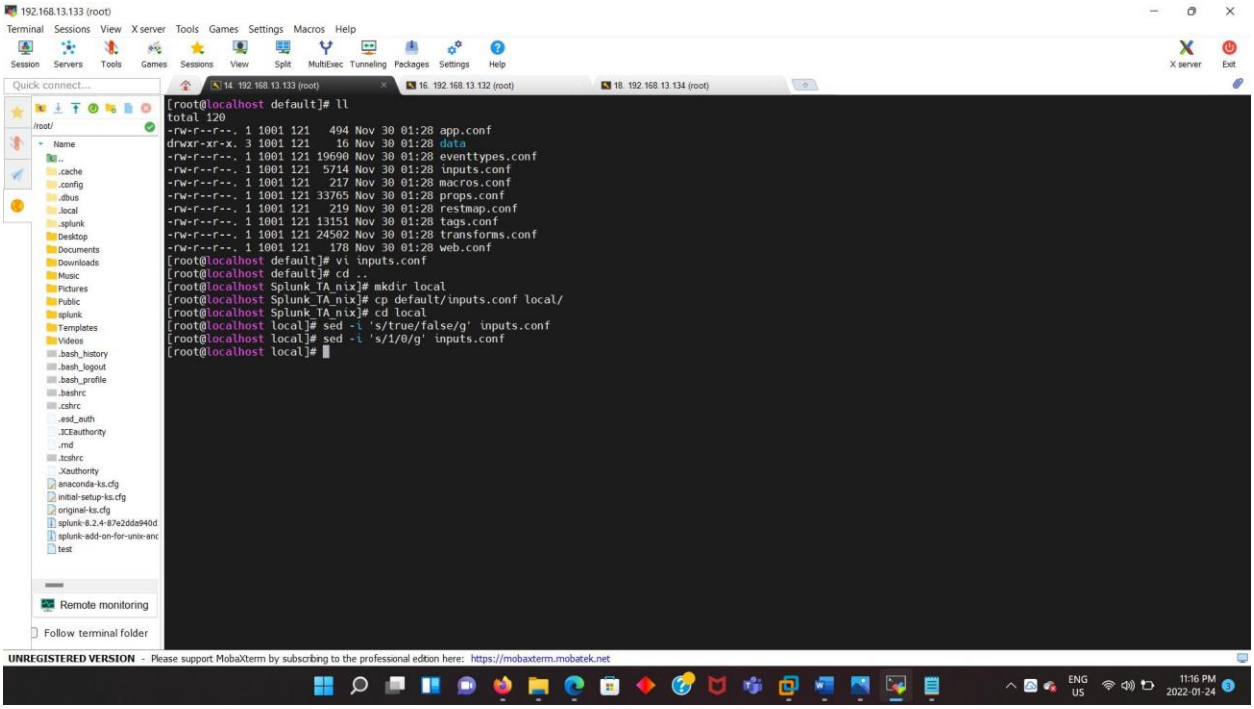


Now we get into local directory by typing cd local



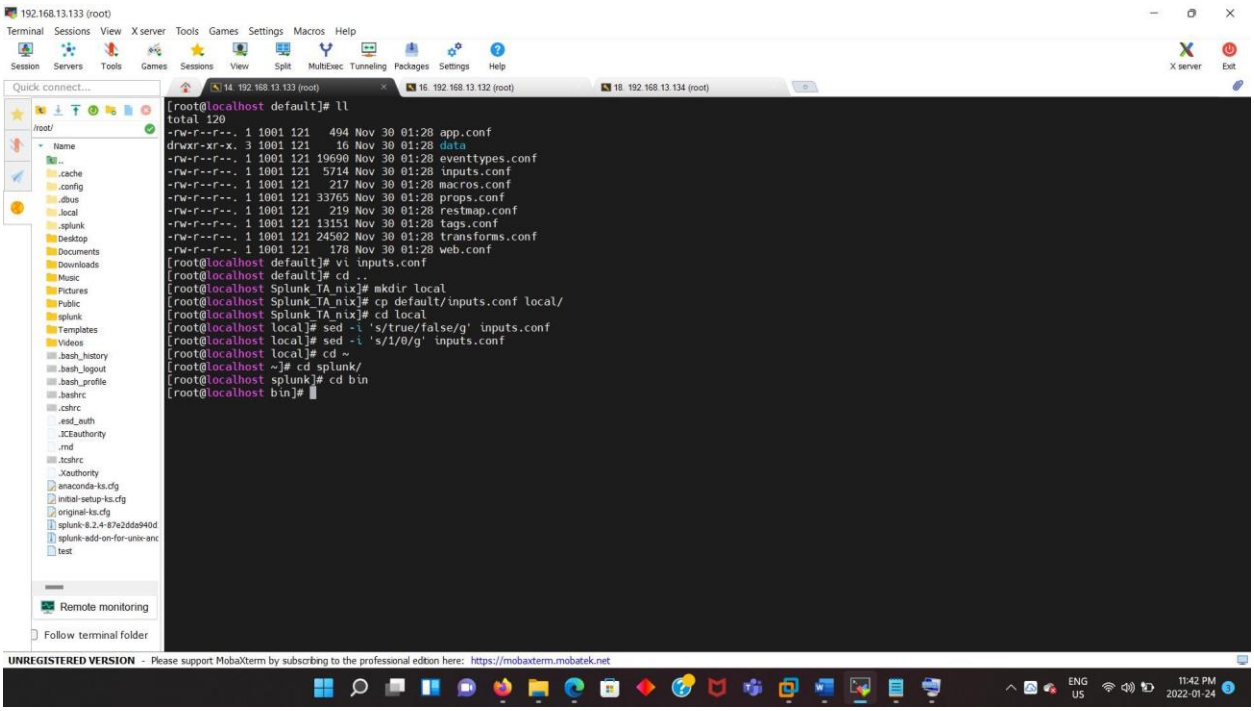
Now we enter the command sed -i ‘s/true/false/g’ inputs.conf, Sed -i ‘s/1/0/g’ inputs.conf

The purpose of this command is to change all the values that are true to false and change all the values that are 1 to 0.



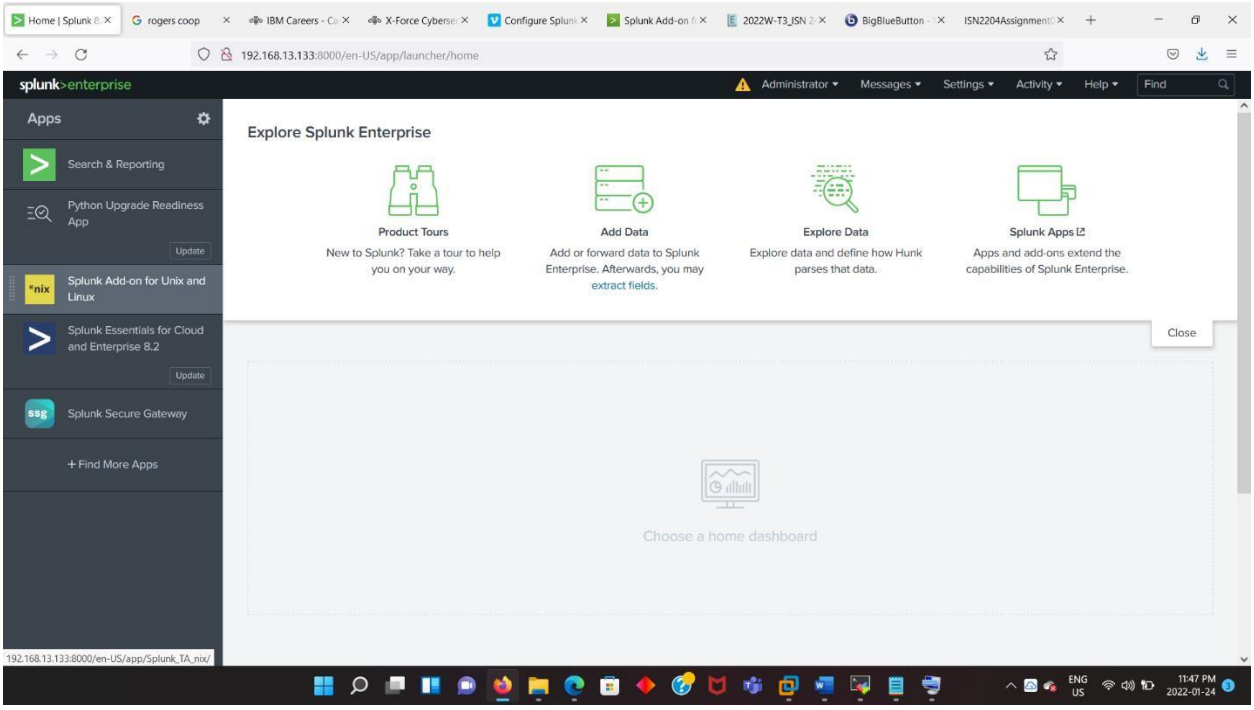
Now we must restart Splunk in order to check if the values are changed as per the command above.

So, we type cd ~ and then type cd splunk/



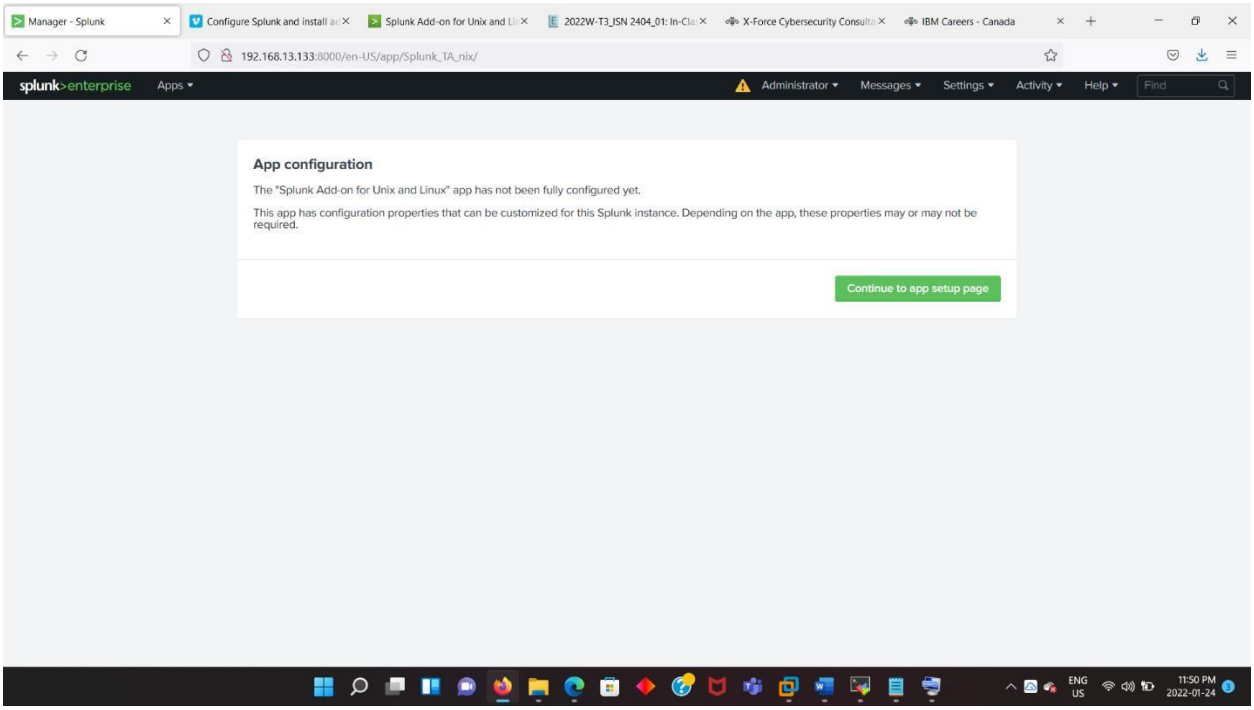
Use cd bin and then restart splunk by executing ./splunk restart

Now when we restart Splunk web page. We see that the Splunk adds on is added.

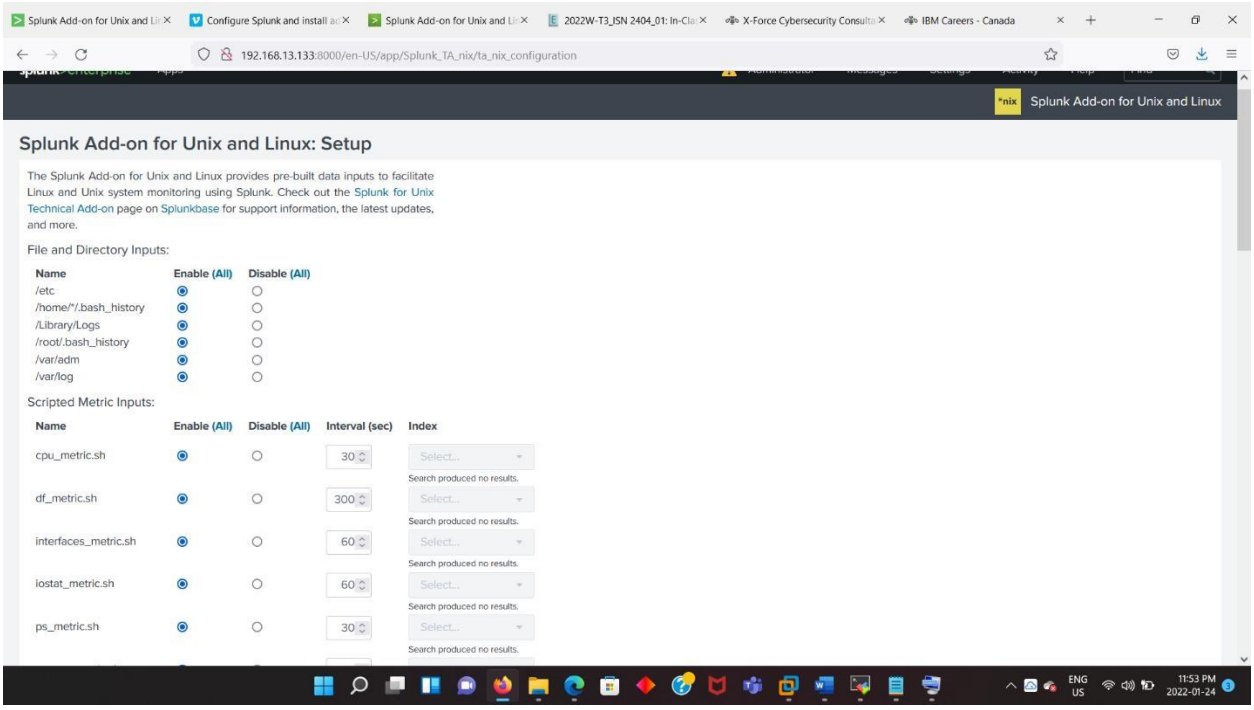


We double click on adds on and then we get app configuration page.

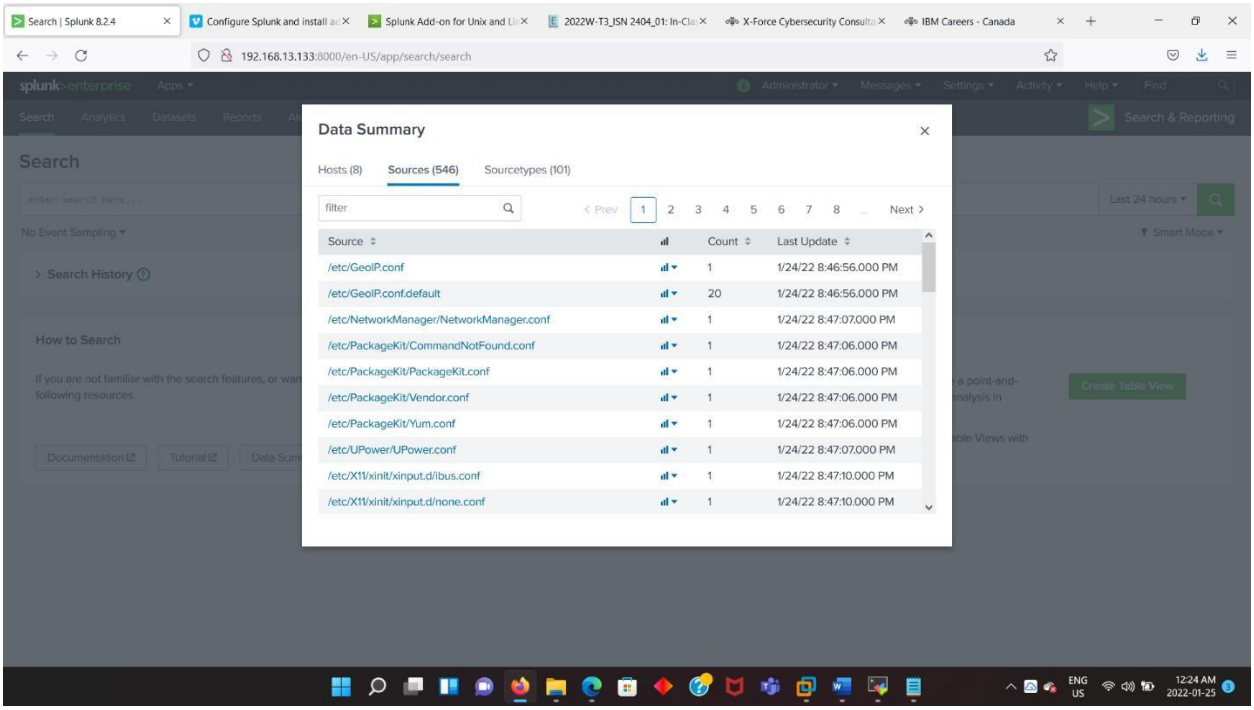
Click on the continue to app setup page and make sure all are enabled and save the settings.



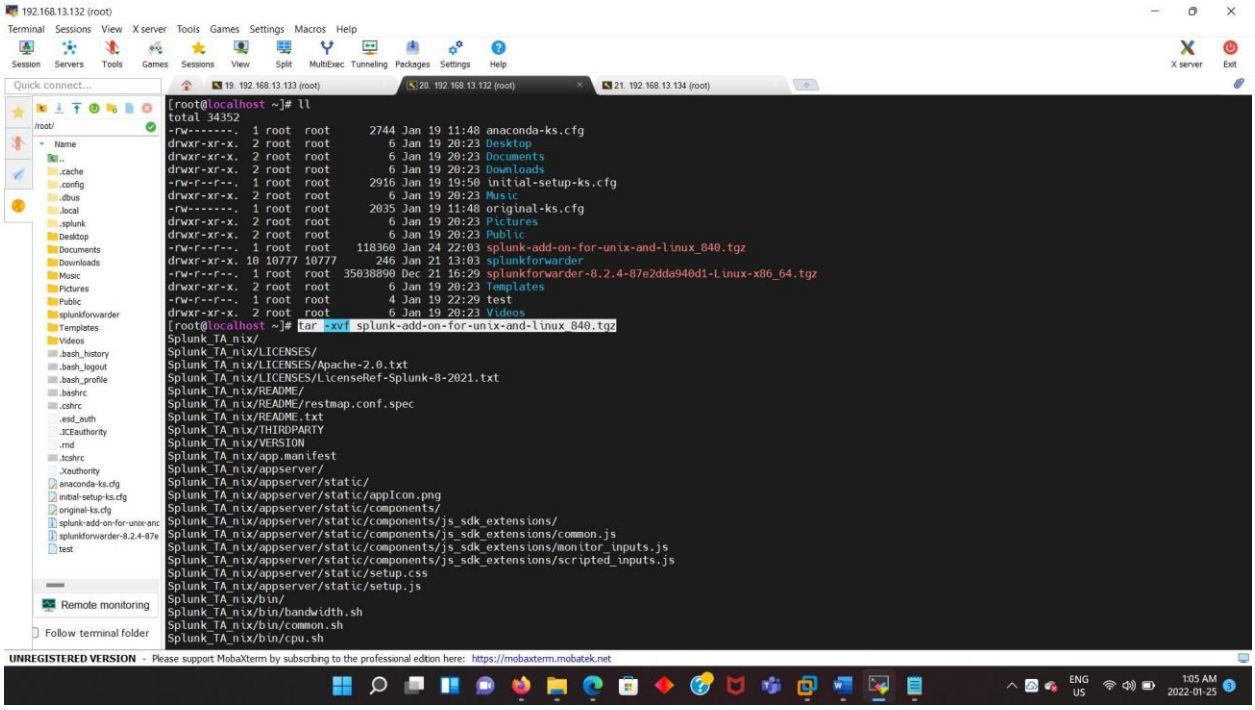
Now go back to the main page and then click on the search and reporting and then click on data summary, we can see hosts, sources from Unix and Linux, and source types compared to the raw data before. Because all the data are pulled to one controller.



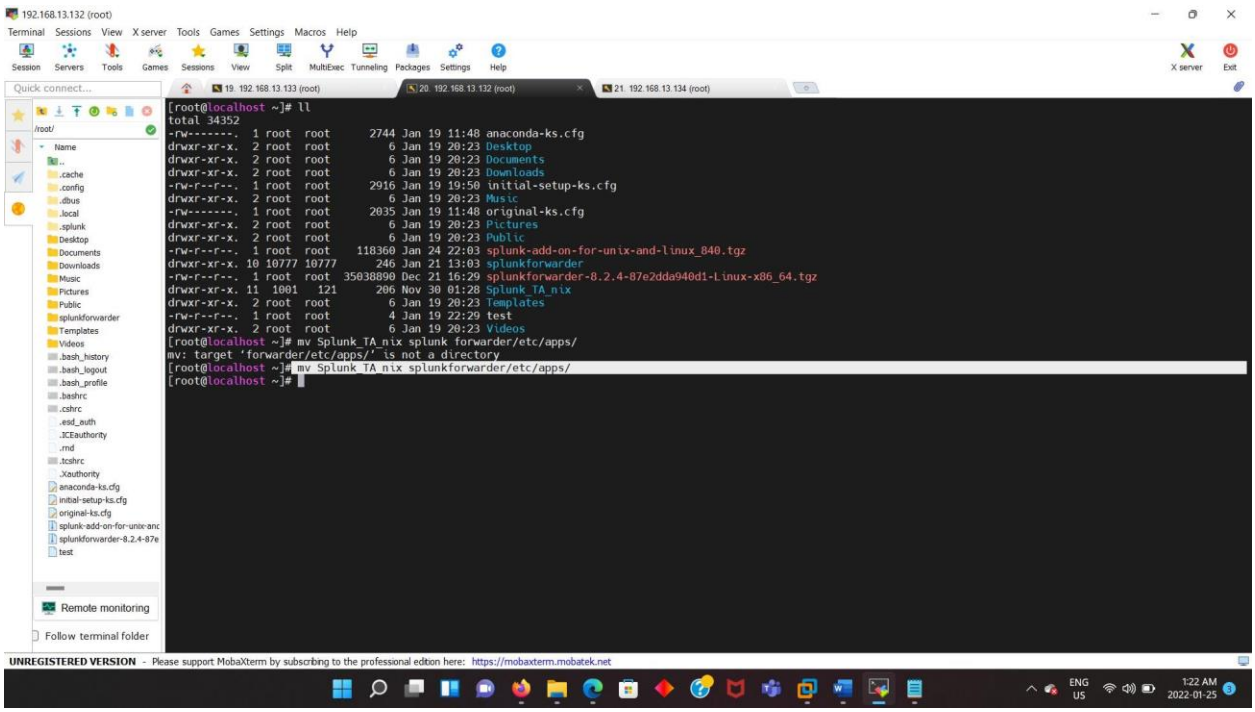
The same way, we follow the same method to all the 3 agents by downloading the Splunk adds on to the agents.



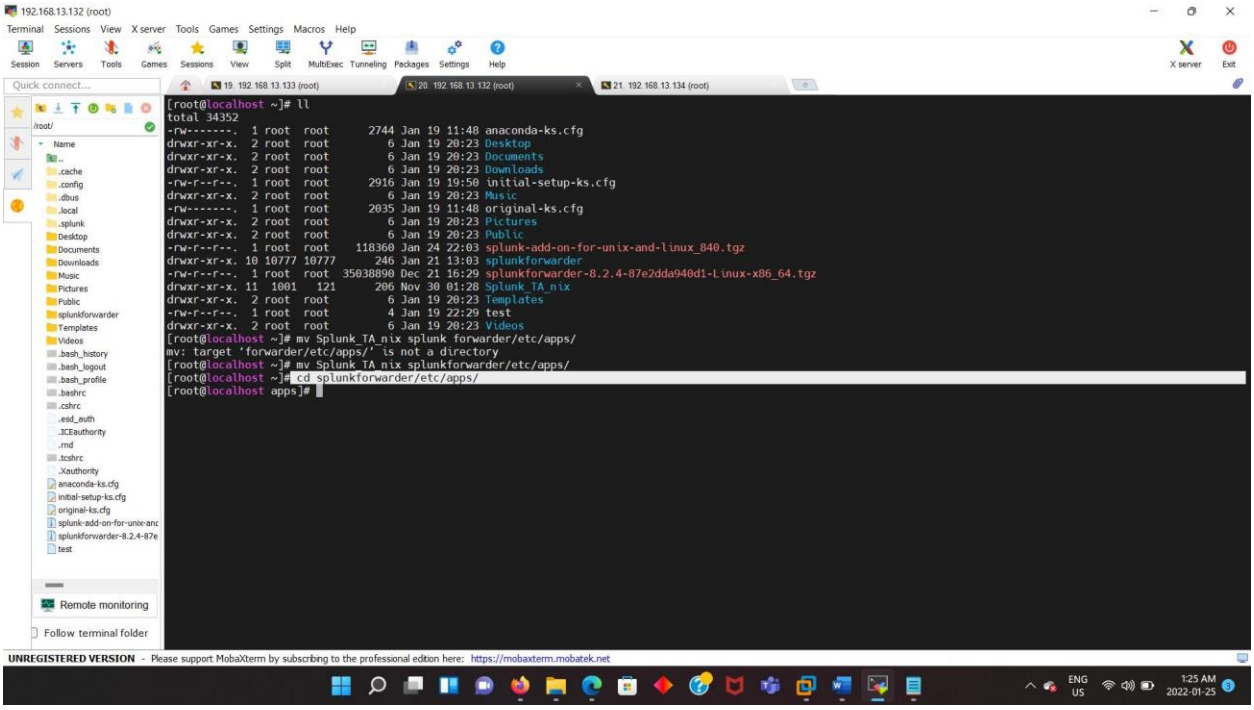
From the below picture, we see that the Splunk adds on is downloaded to the first agent and then extracted using tar -xvf command. Similarly, we follow for agent 2 as well.



Now move the splunk _TA_nix to splunkforwarder/etc/apps



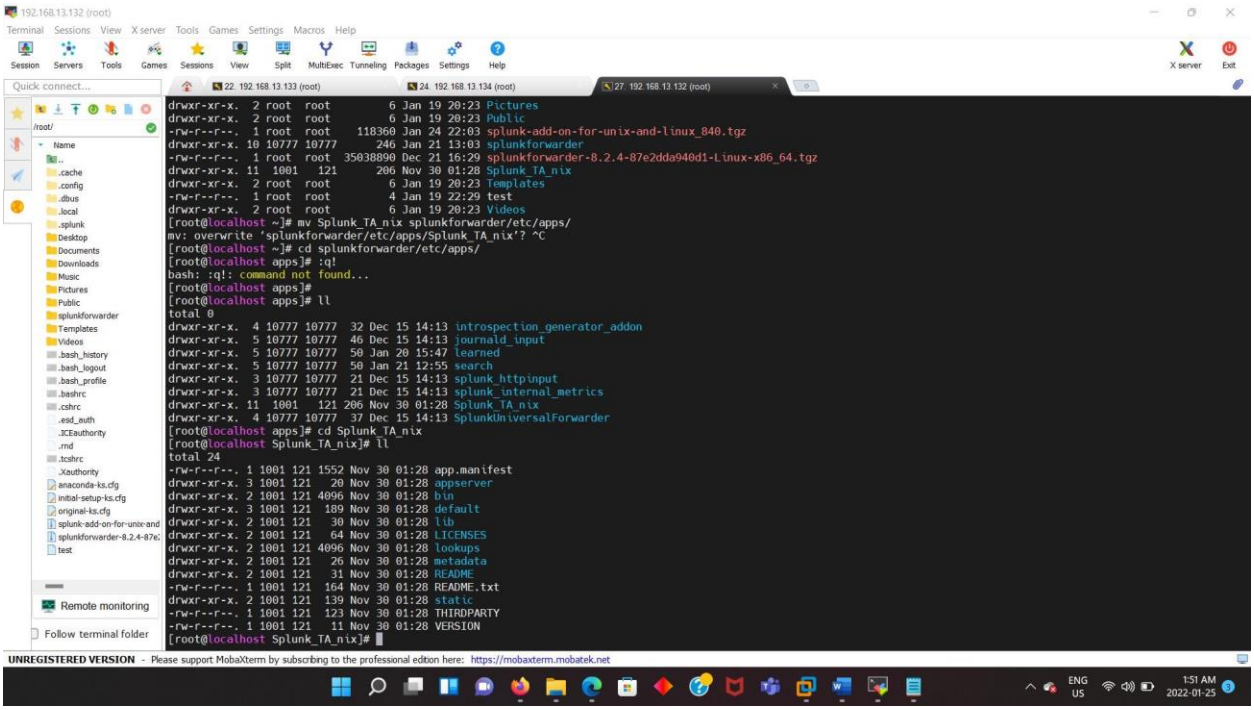
Move to the folder splunkforwarder/etc/apps



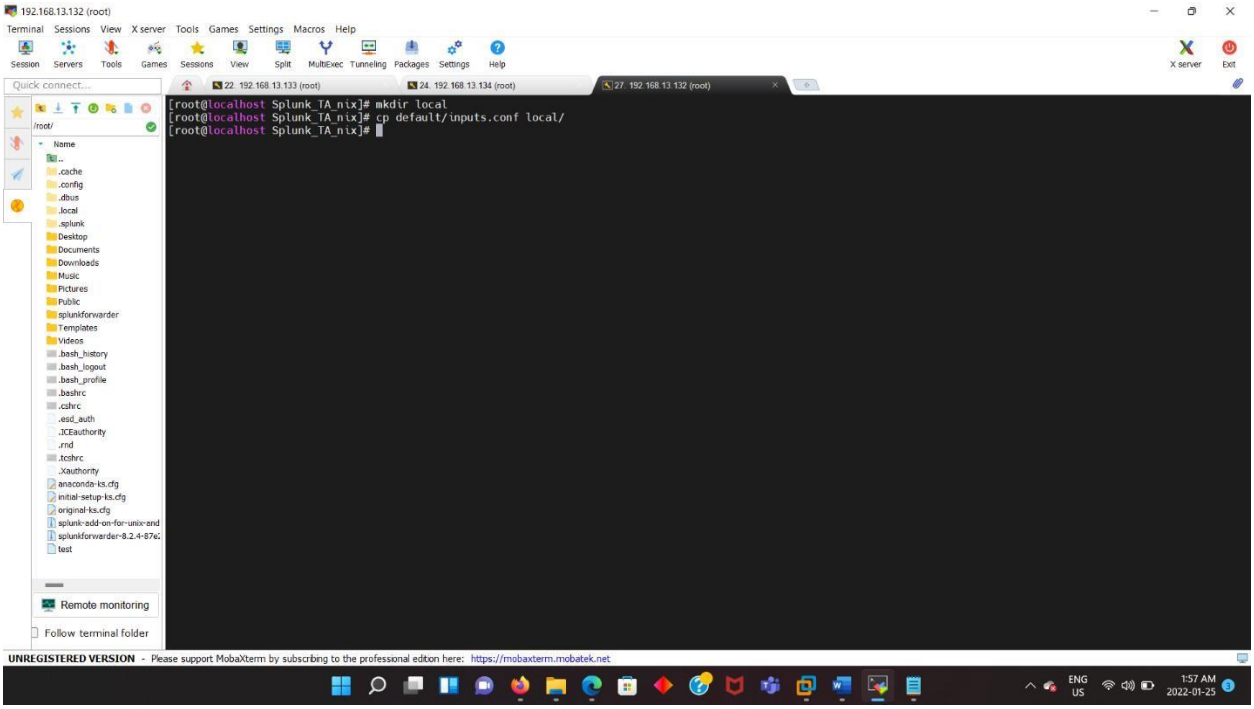
Now list the files using ll and then move to splunk_TA_nix and again list the files, now we see the default file.

Now we create a local folder.

Copy default to local folder.

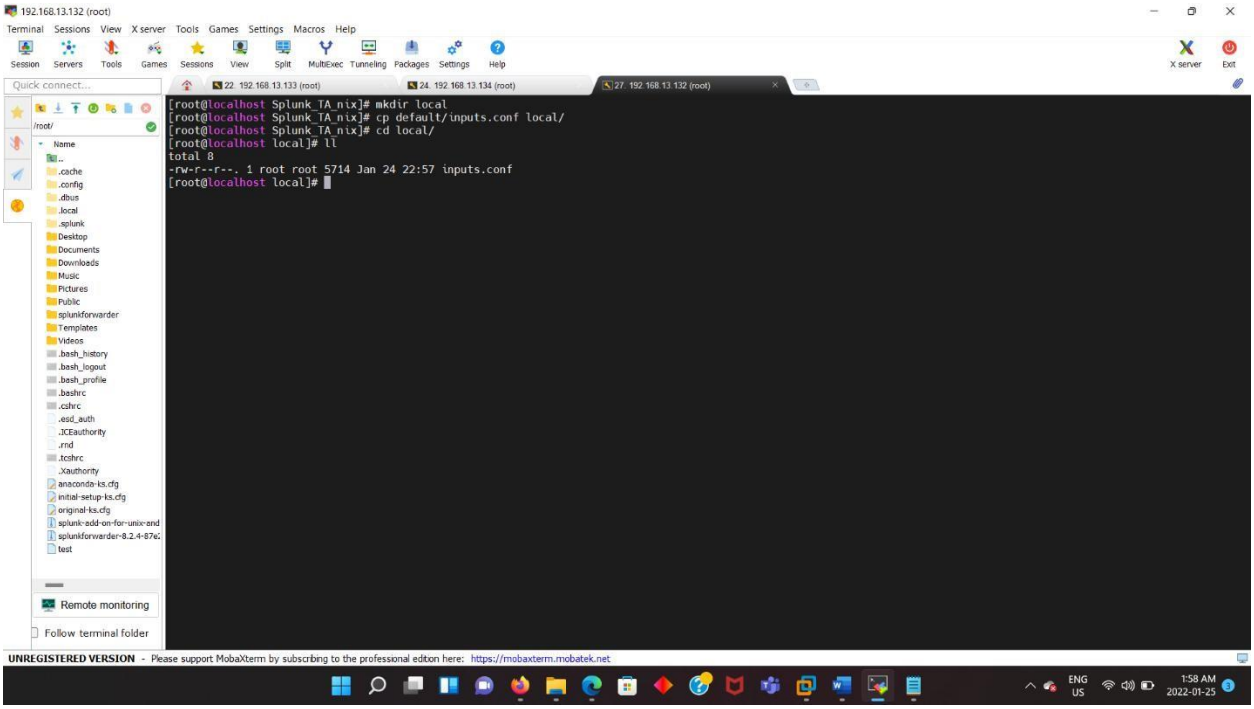


Now we see the input file.

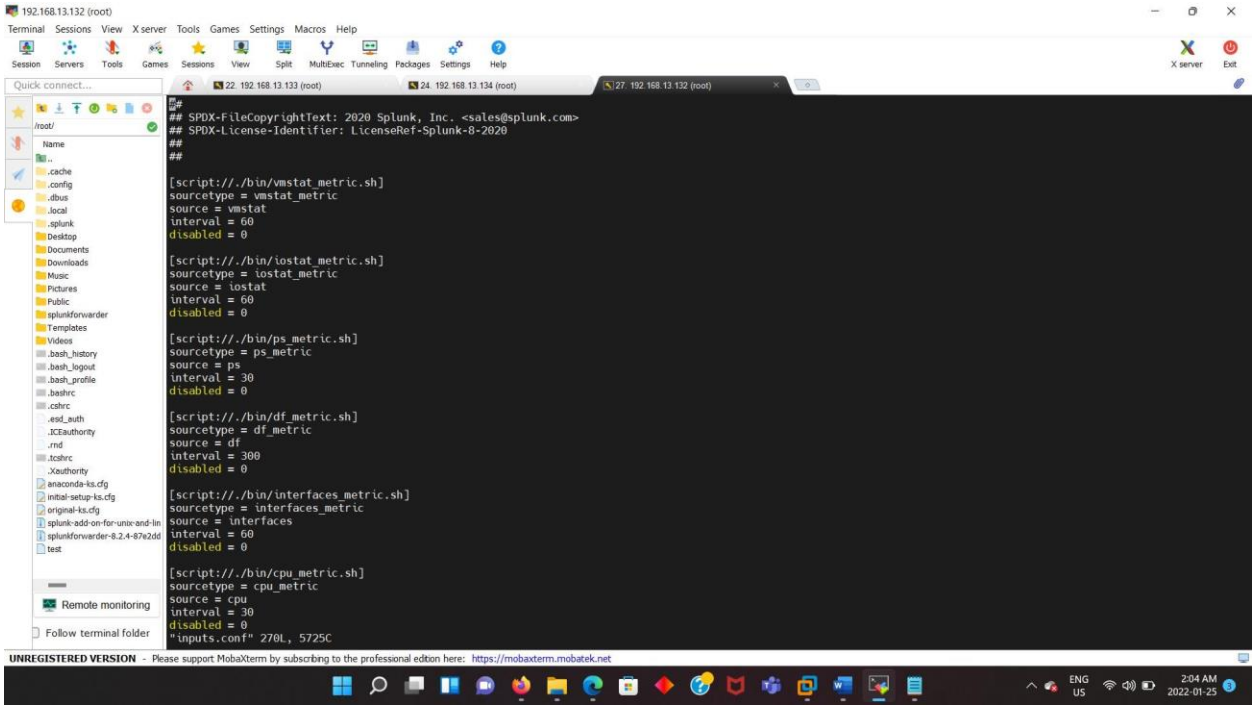


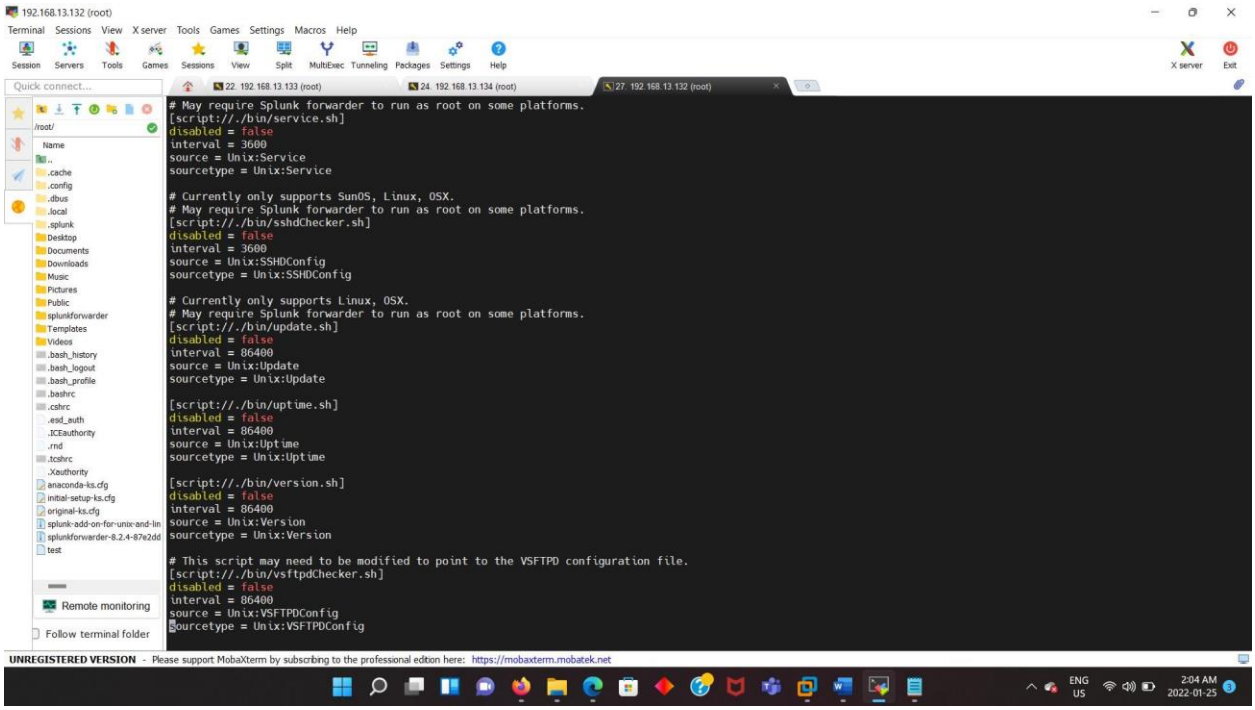
Now run the commands sed -i 's/true/false/g' inputs.conf

Sed -i 's/1/0/g' inputs.conf to check if the values are changed to 0 and false.

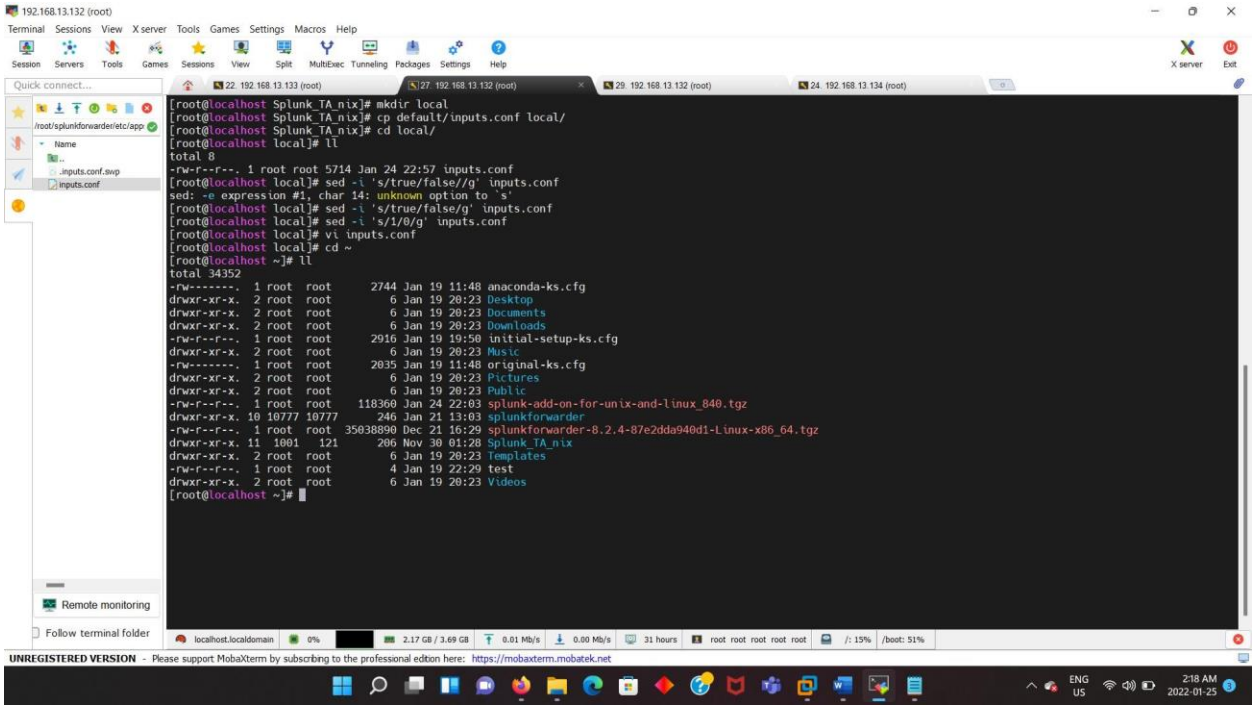


From the below screenshots we can see that all the values are changed to 1 and false.

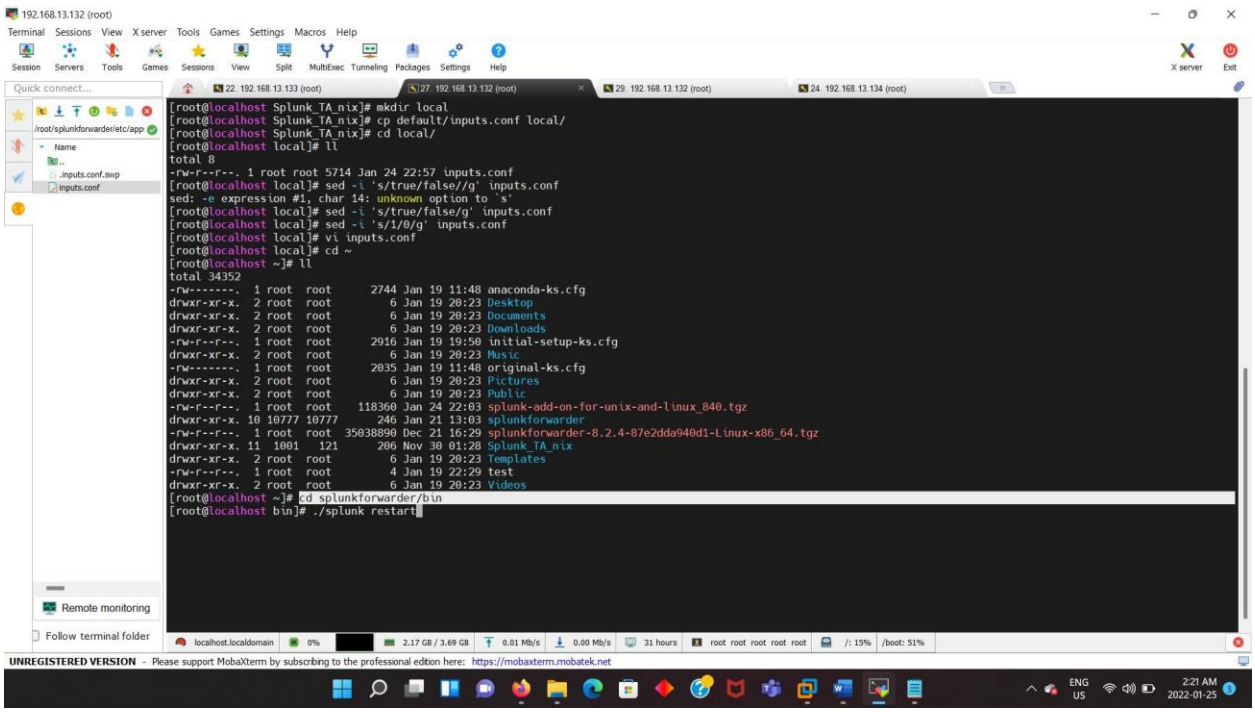




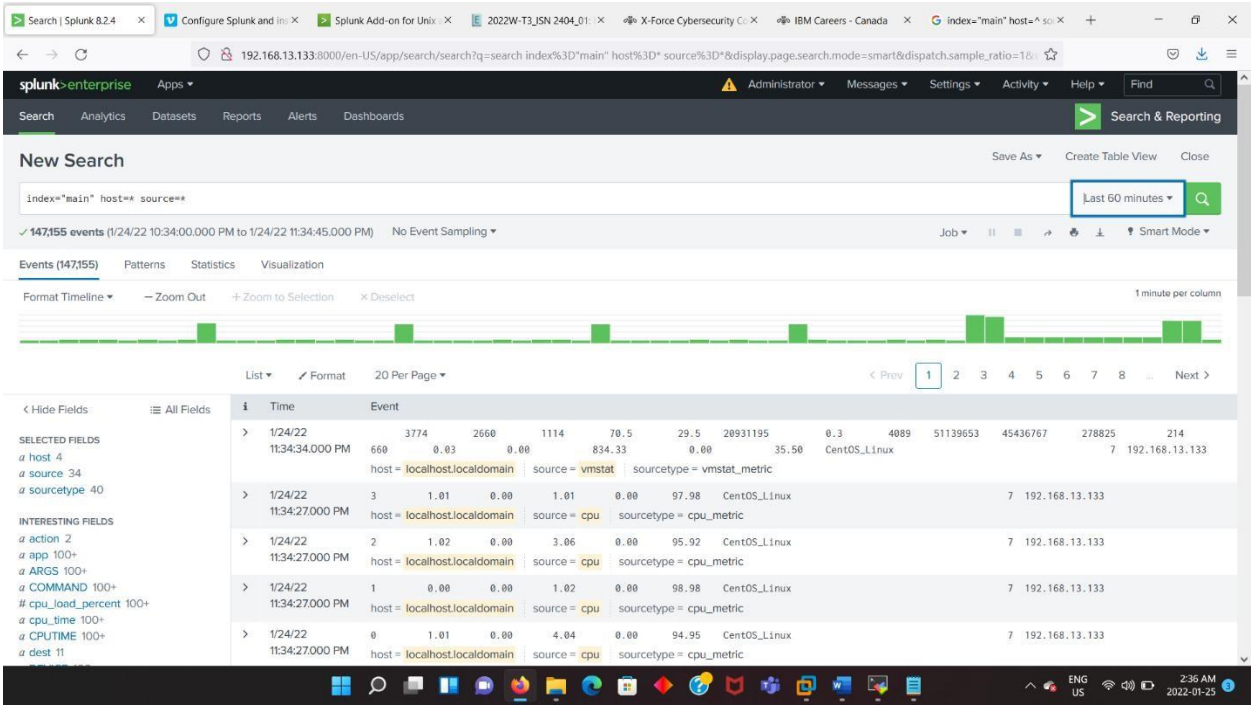
Now get back to local file and execute cd ~ and then list the files.



Now execute cd splunkforwarder/bin ,and then restart splunk.



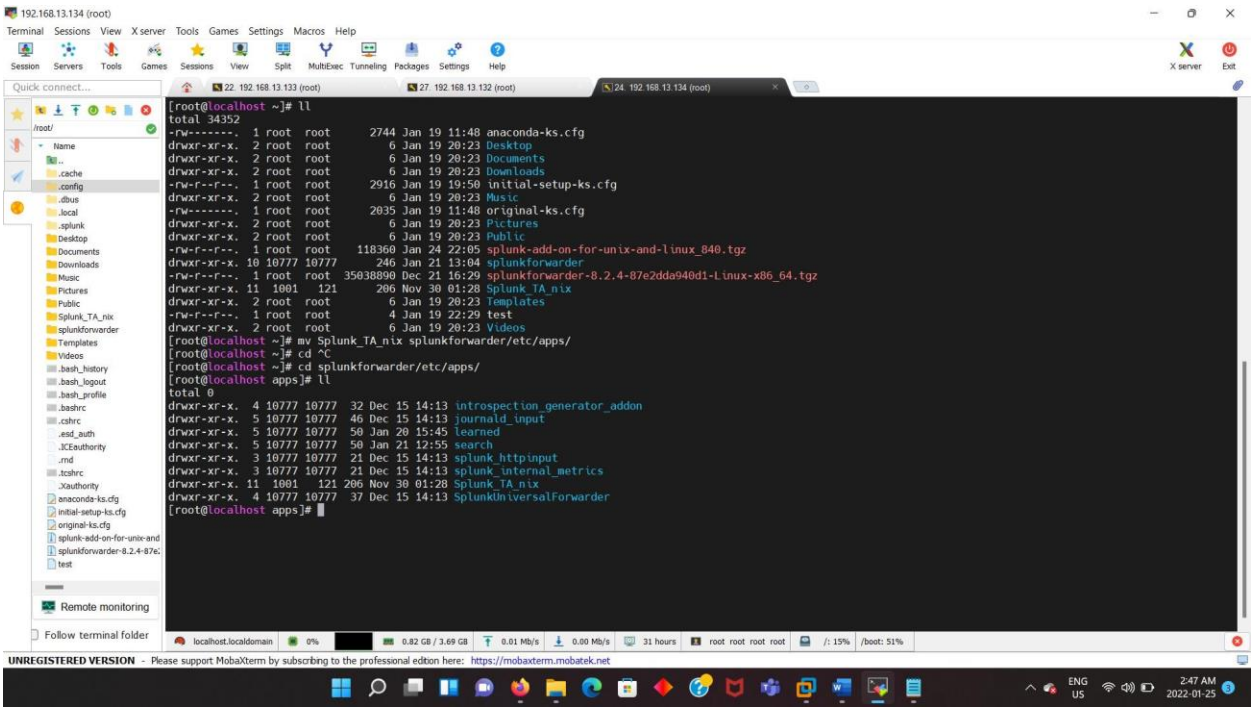
In the Splunk web, search for index=”main” host=* source=*, this time we will get double the logs as shown below.



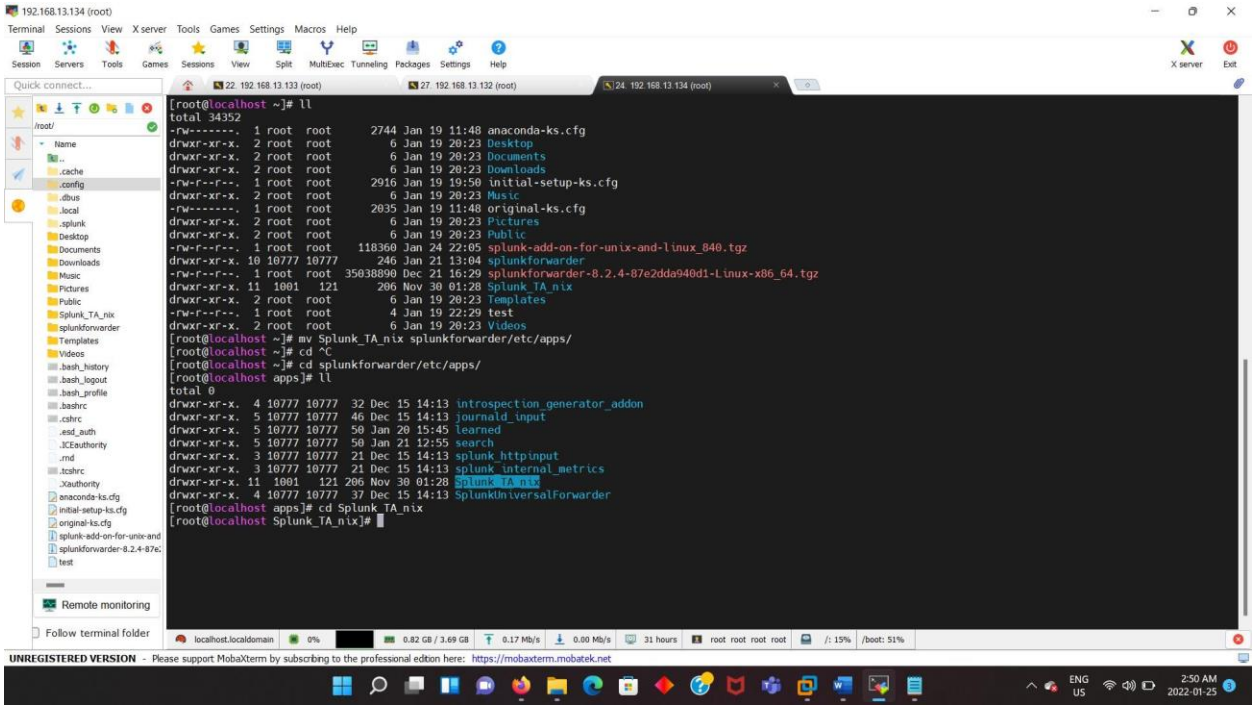
Now follow the same method on Agent 2 and 3

Download and extract Splunk adds-on, then move splunk_TX_nix to splunkforwarder/etc/apps.

Move to splunkforwarder/etc/apps and then list the files.

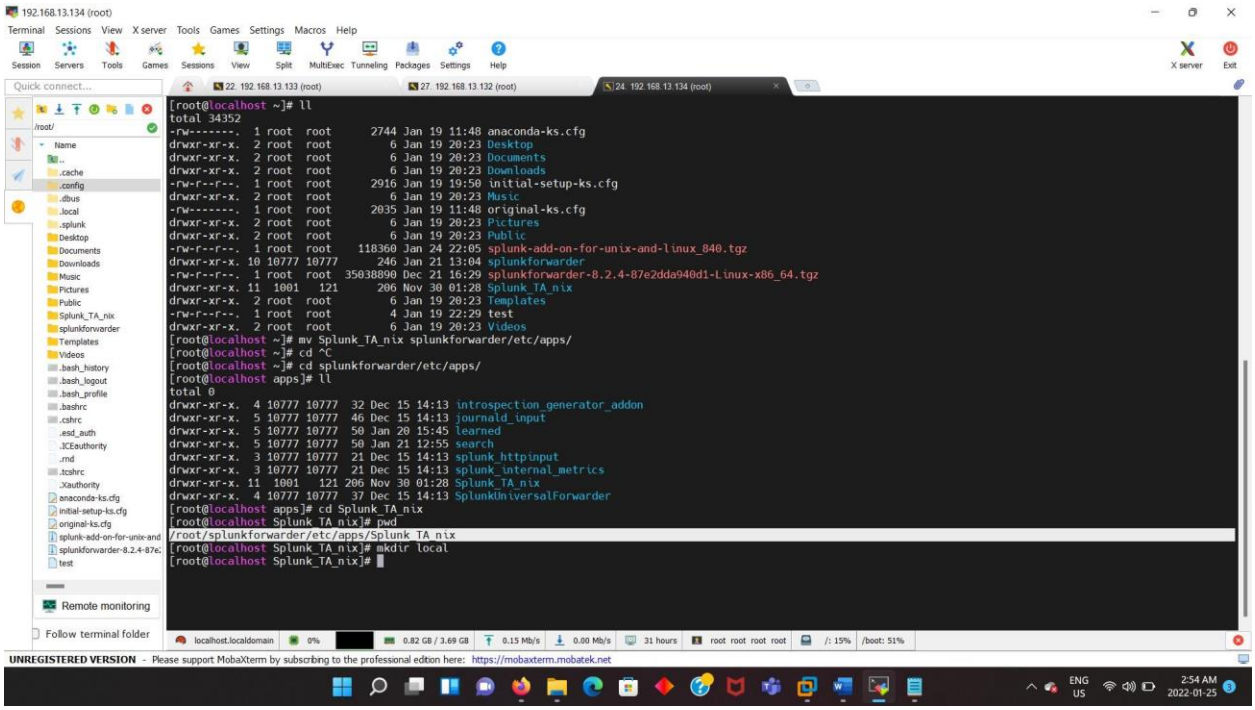


Now move the file to Splunk_TA_nix



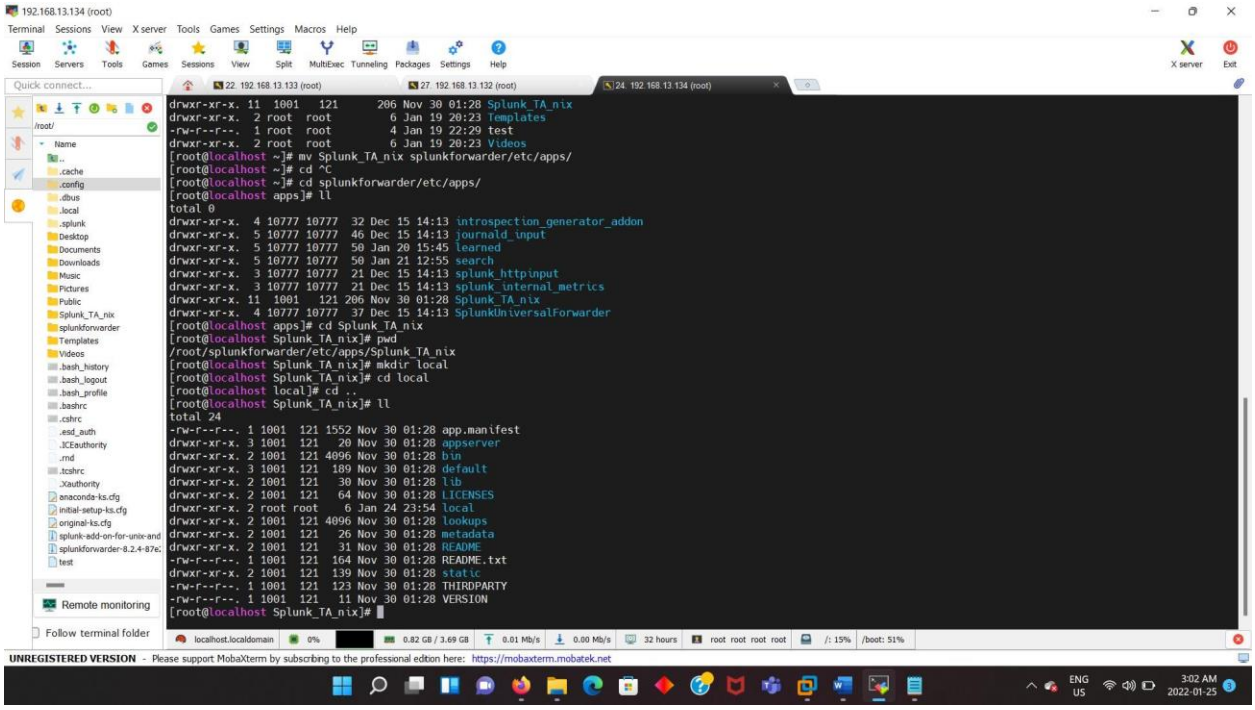
Now type pwd and then copy the path /root/splunkforwarder/etc/apps/Splunk_TA_nix

Create a new local; directory as shown below.



Now get into the local directory and enter the command that converts 1 to 0 and true to false.

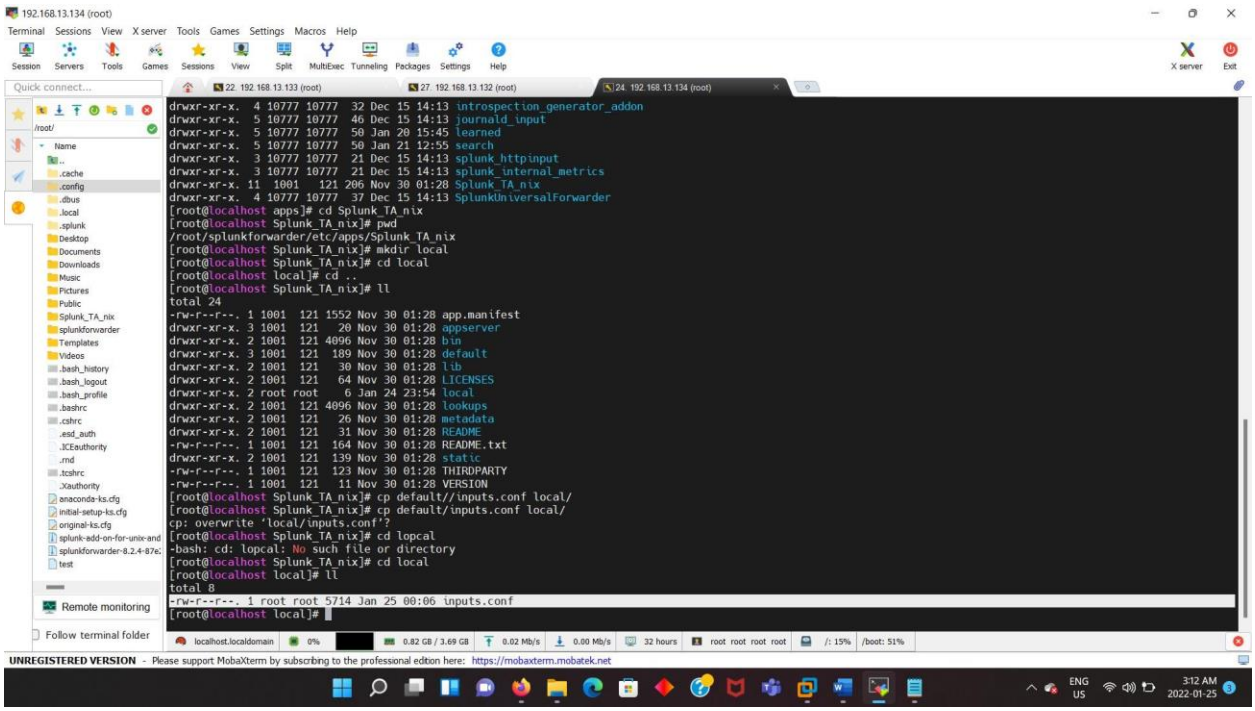
Before that enter the command cd.. and then list the files



Copy default input file to local. cp

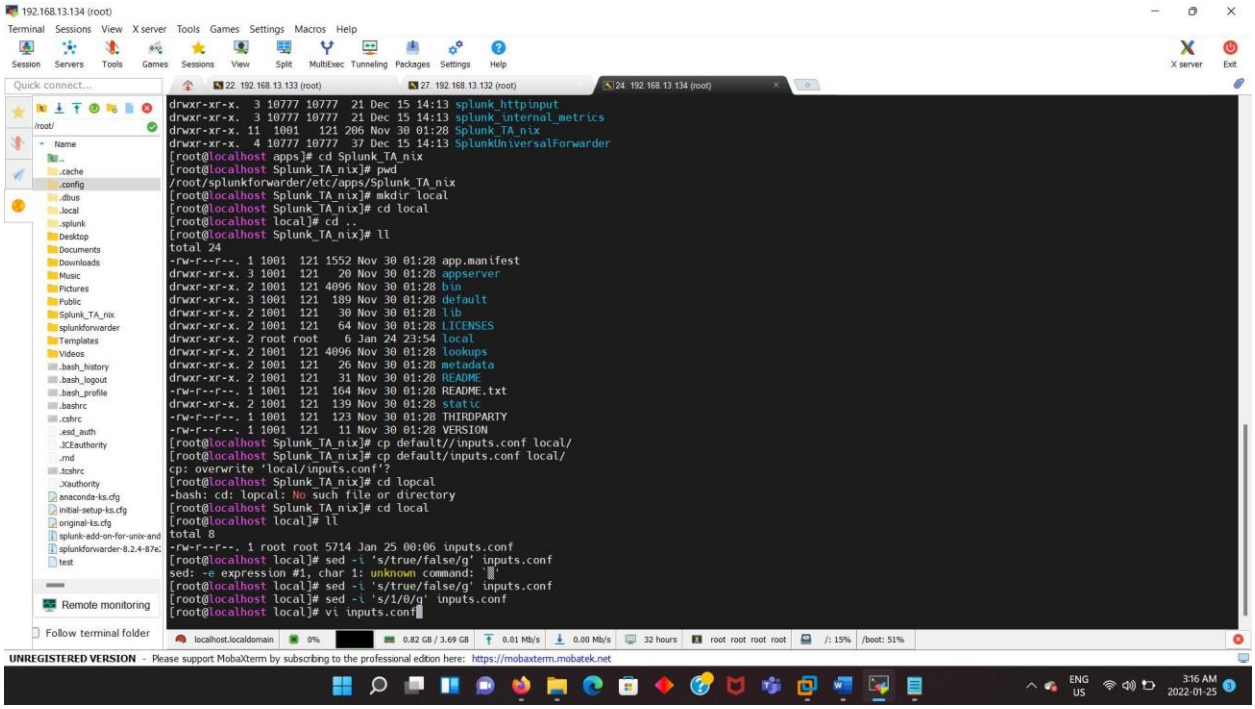
default//inputs.conf local/

Go to local directory and list the input file.

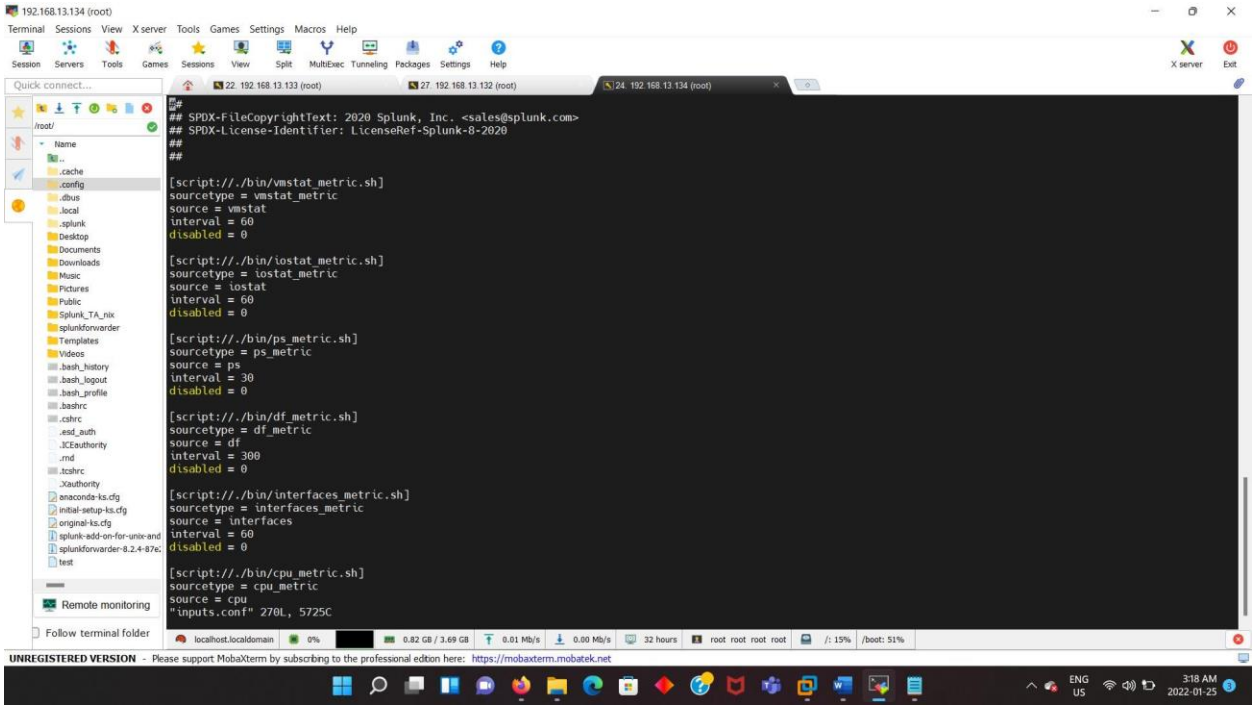


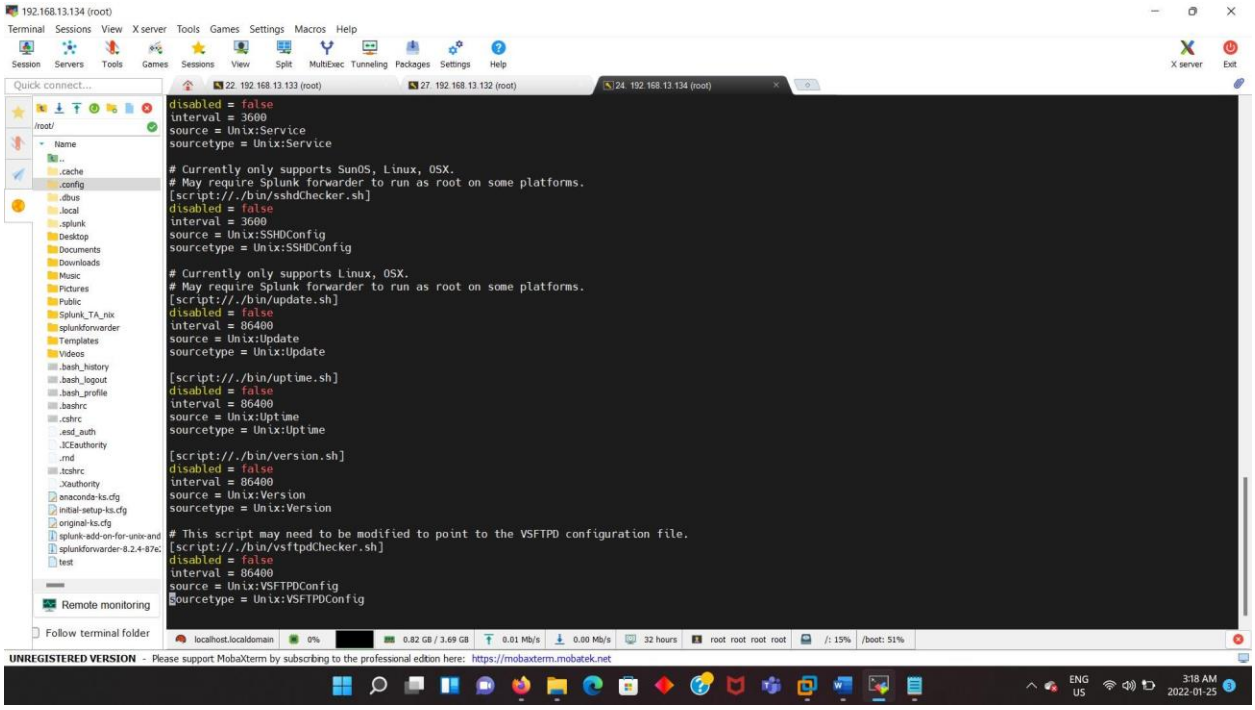
Now execute the below commands.

sed -i ‘s/true/false/g’ inputs.conf , Sed -i ‘s/1/0/g’ inputs.conf



Now check the inputs file.



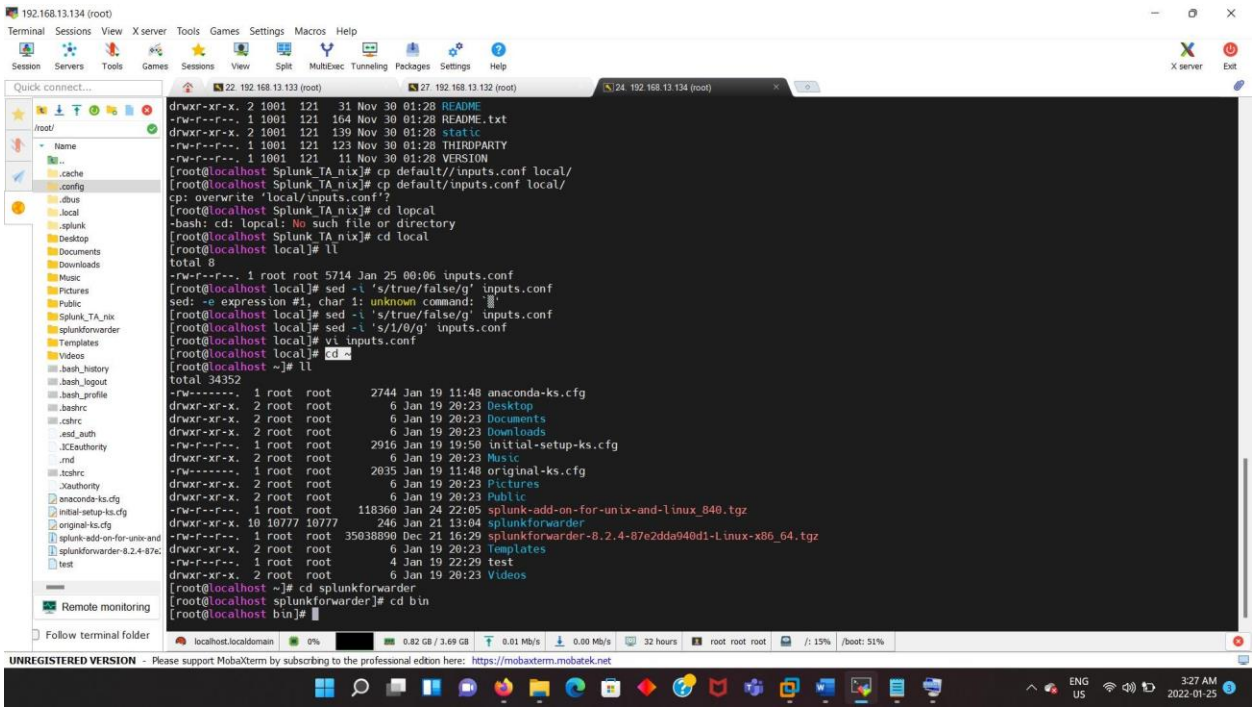


We can see that all the disabled values are changed to 0 and false.

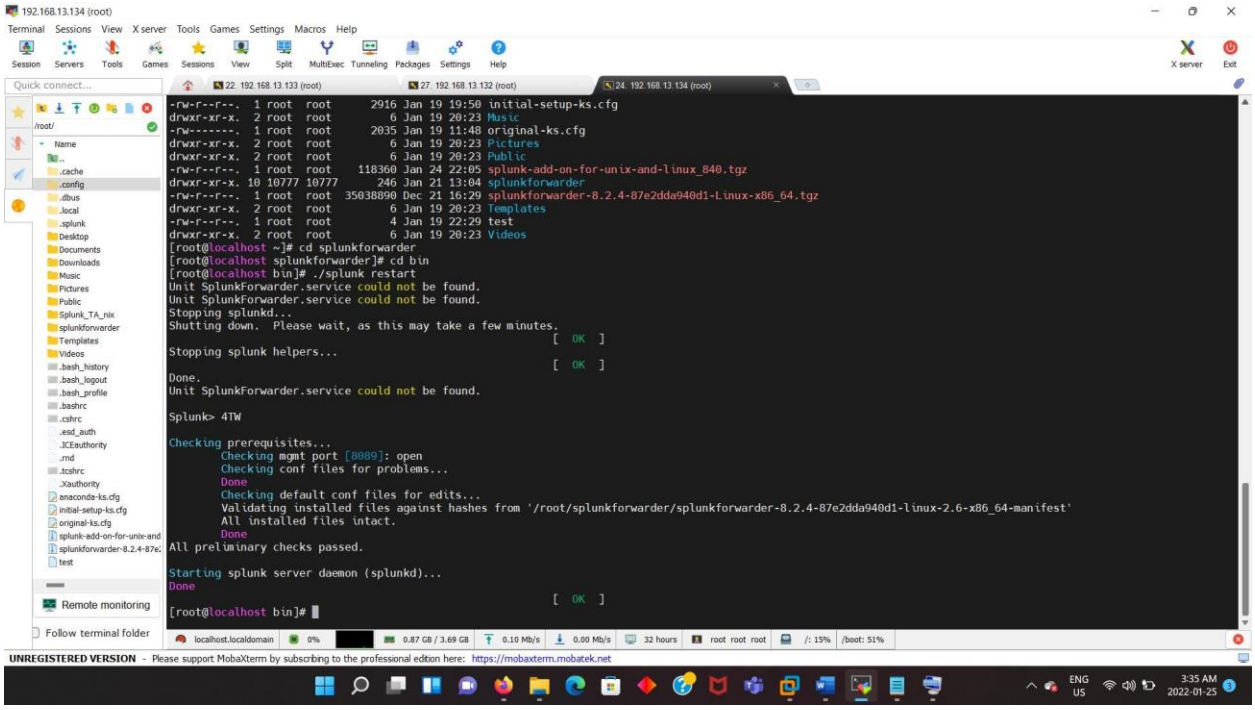
Exit from the file by typing :q!

Type cd ~

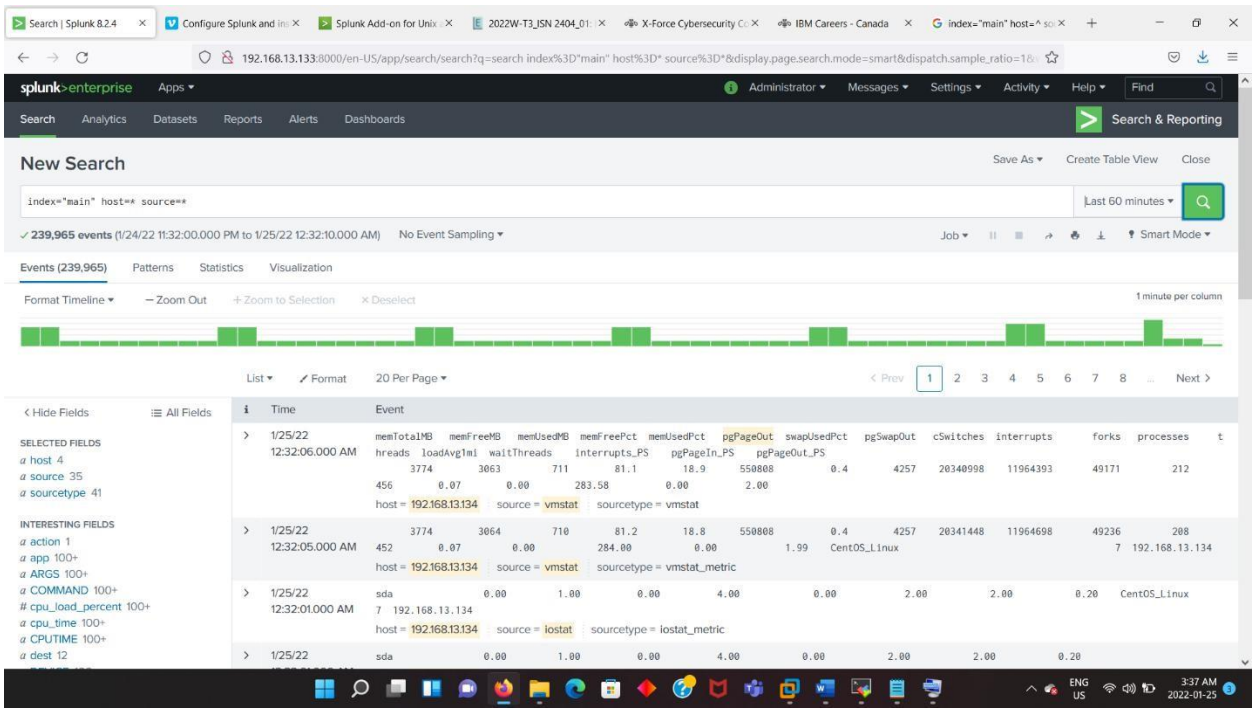
List the files, now get into cd splunkforwarder and then bin



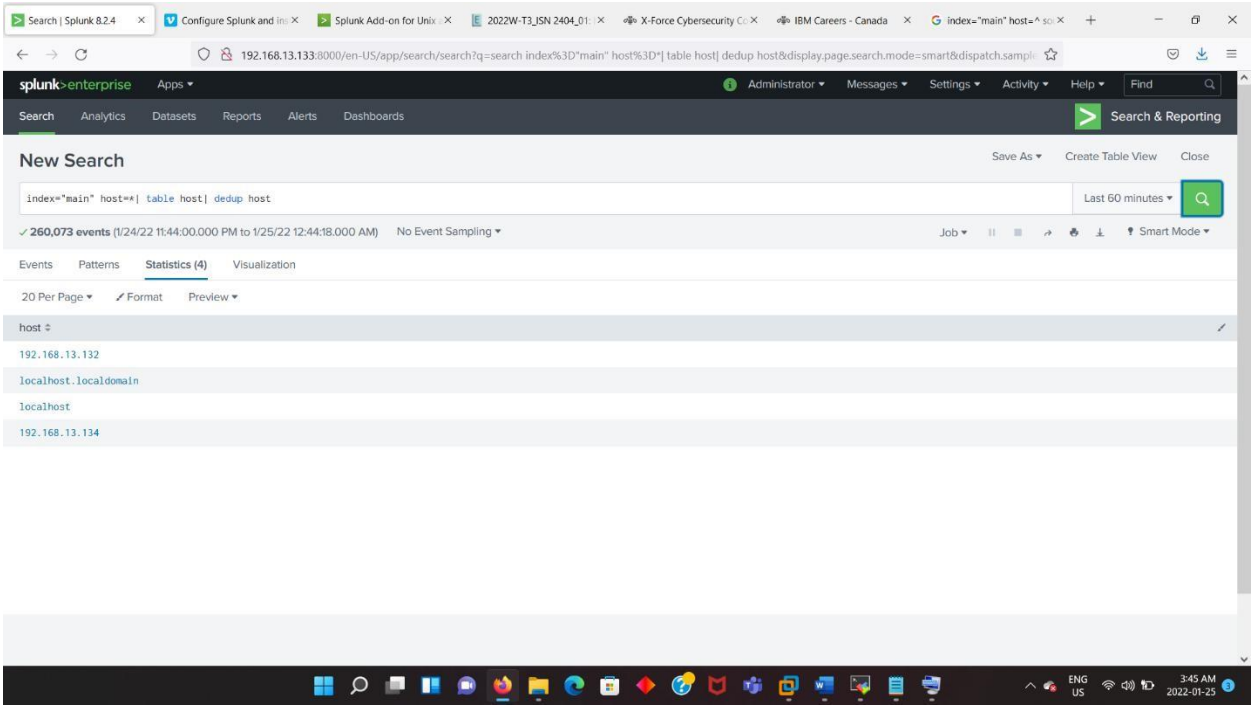
Now restart splunk by using ./splunk restart



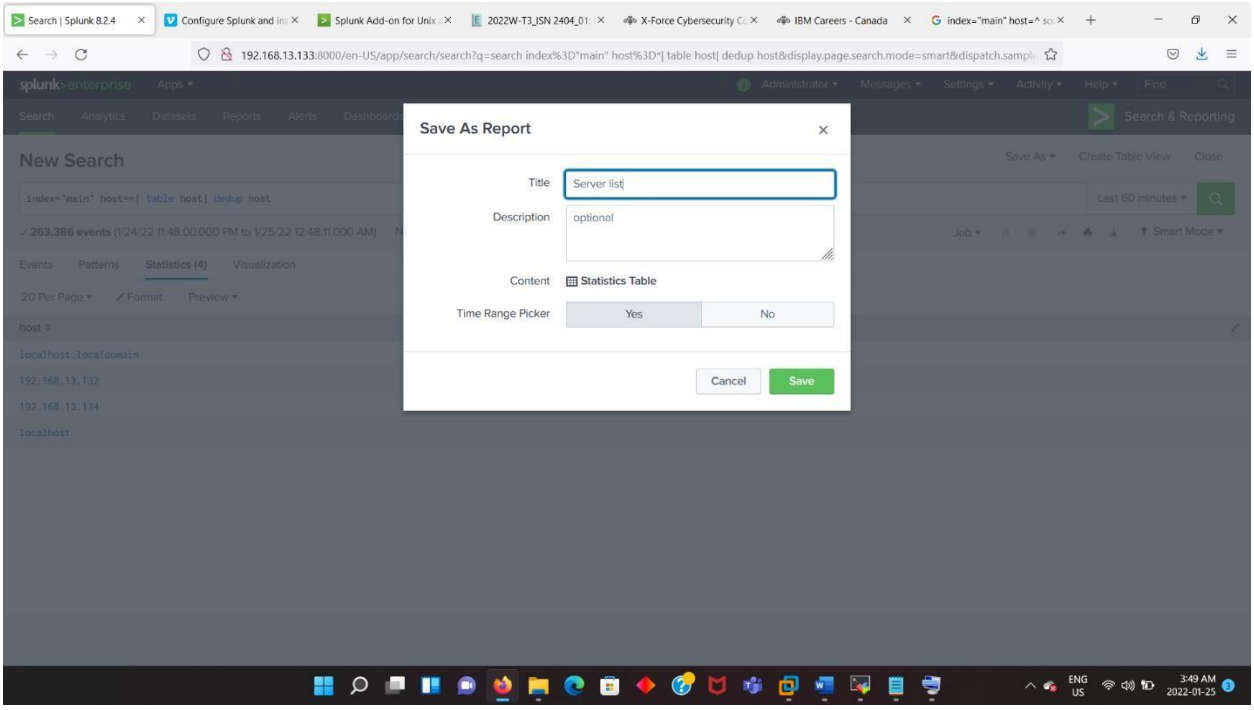
Meanwhile, access the Splunk web, this time, we get a lot of logs from all servers.



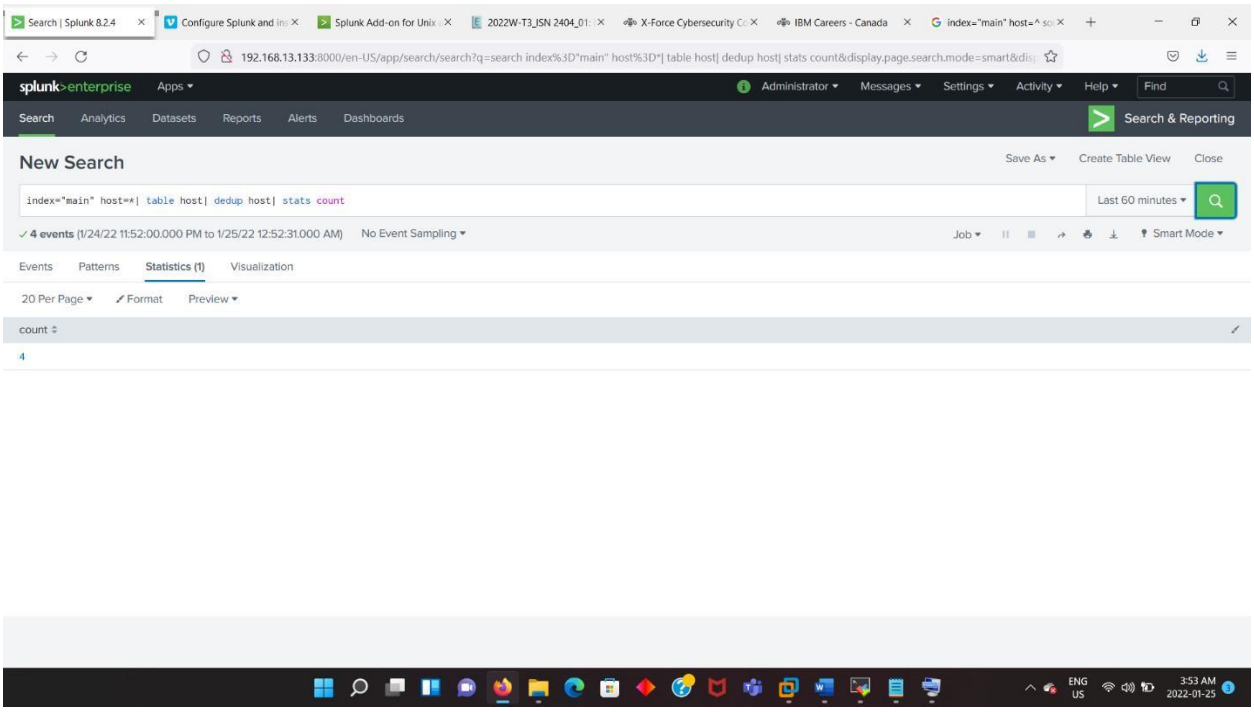
It is also possible to search the query index=”main” host=*| dedup host to avoid duplication. The output is given below.



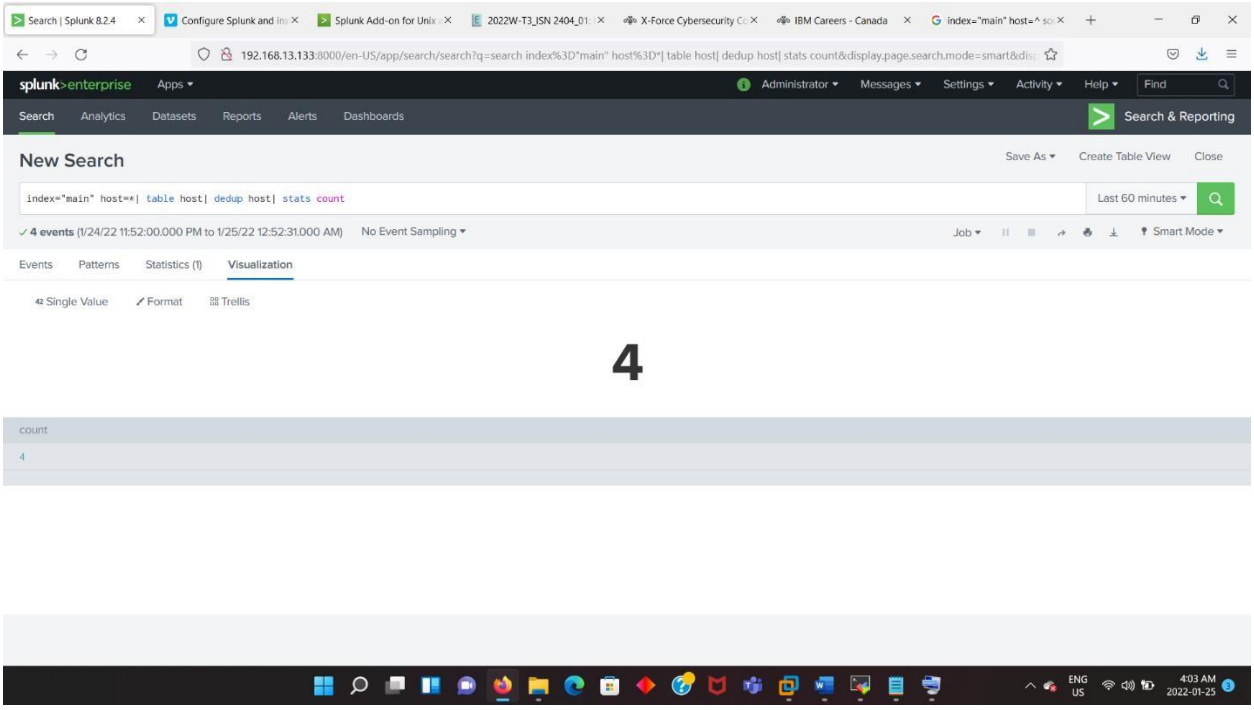
We can also save the report using save as report.

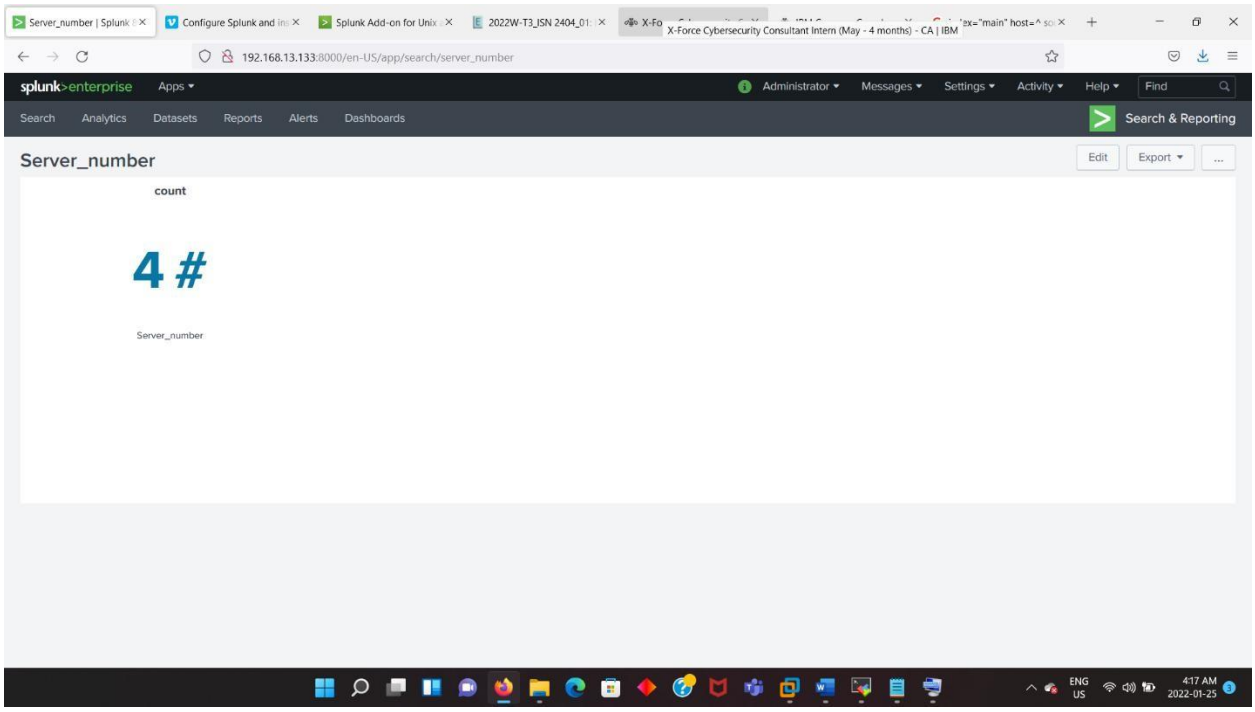


By running index=”main” host=*| table host| dedup host | stat count , we can get the count.

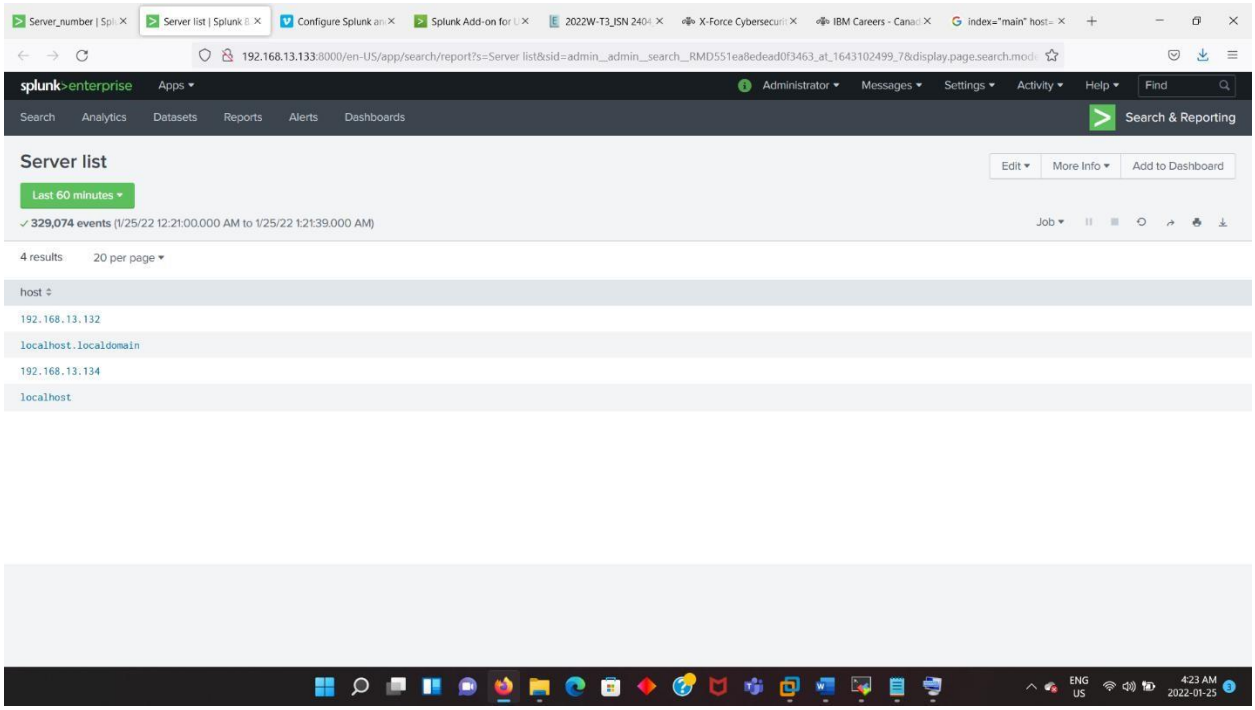


We can also select visualization and display single digit.

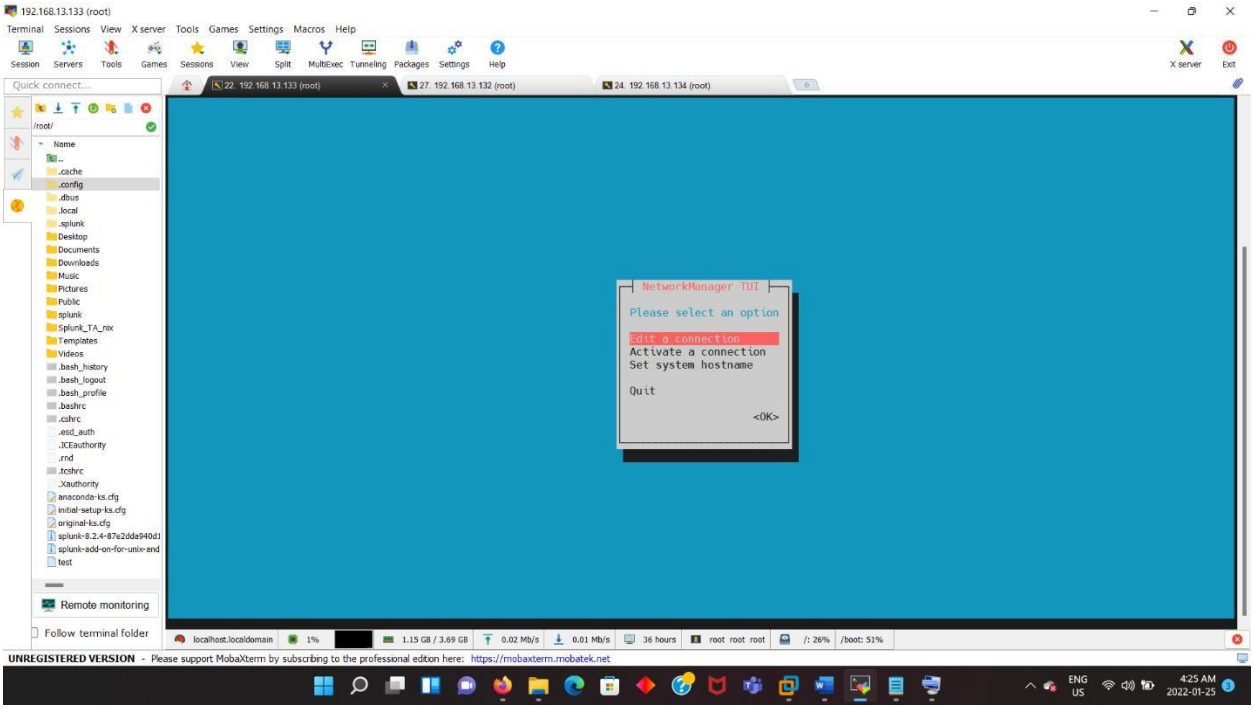




We can also save as new dashboard, also we have additional features where we can hyperlink so that it can redirect to the server page.

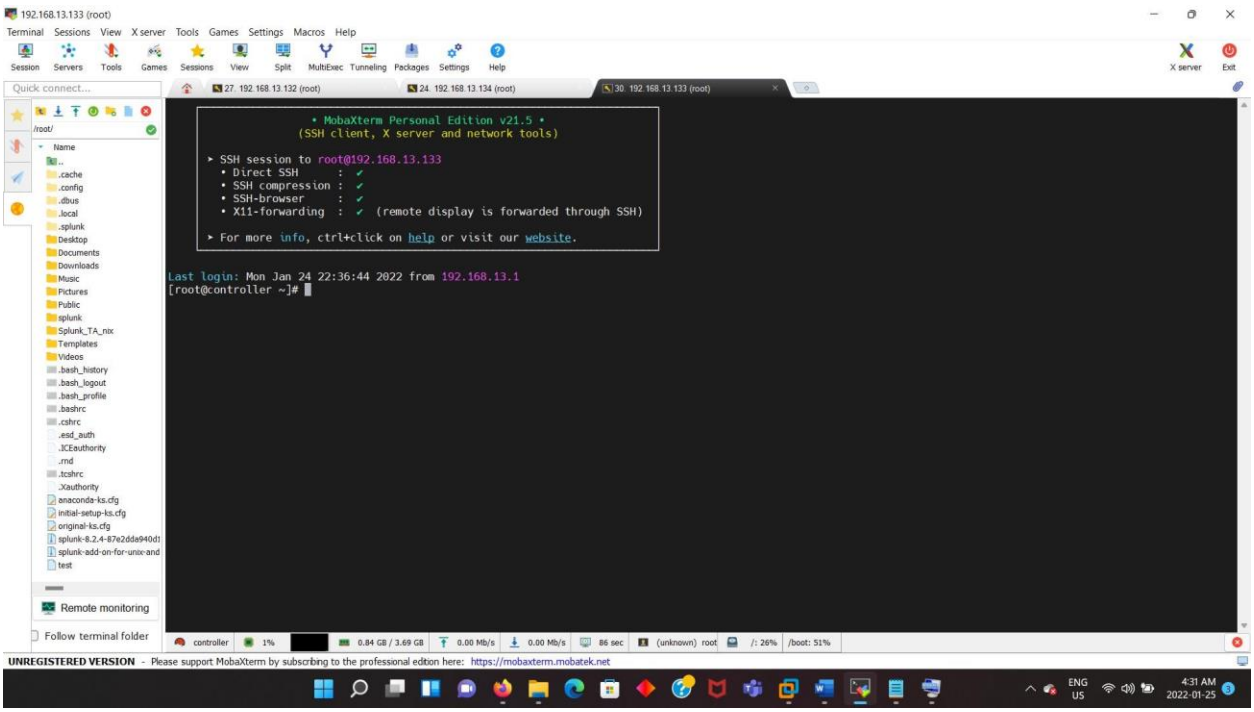


For changing the host name on controller, we can use the command nmtui



Choose set system host name and type controller. Now restart the controller from virtual machine.

We can see that the name is set to controller from the below screenshot. Same method, we can also change for all the agents, and it will get displayed in Splunk web UI as well.



Conclusion

In conclusion we were able to get server logs from all agents forwarded to the controller using Splunk forwarder. The controller captured all logs and displayed them in an intelligible dashboard in real-time. Queries can then be run on the captured data which is very useful in reducing time required to identify and solve a problem.

Summary

Multiple CentOS VMs were created with one controller and all others acting as agents. Splunk was installed on the controller which was used to successfully capture logs from agents with the help of splunk forwarder. Multiple add-on were installed on the agents. The Splunk dashboard access on host was used to run queries on the captured data to simplify the output which helped in providing the right information.

Achievement

In this exercise, we have learned how to install Splunk, add agents, adding and configuring multiple add-on to view more event logs in CentOS VM. This exercise helped us to get hands-on experience with Splunk which is widely used in most organizations. We were able to understand that real-time access to server logs provided by Splunk gives a huge advantage in keeping an infrastructure operating at its optimal performance. Splunks presentable format for displaying captured logs and the ability to run queries on the data helped in traversing through the data easily. We also learned that Splunk also has multiple cyber security tools which can help in identifying threats at an early stage.

References

1. https://www.putty.org/
2. https://drive.google.com/drive/folders/10YZitIpVt2Vs-Kz2fy8Y3oTMqiLyTQ5P?usp=sharing
3. https://drive.google.com/drive/folders/1zdcAPXIHtmxRr7zRXzbgoX5sVhUxFlc5?usp=sharing
4. https://www.youtube.com/watch?v=A-VZwc-0Y1M
5. https://vimeo.com/663519007
6. https://vimeo.com/596300874

Name of students who has not participated in the assignment.
Student name:
Student name:
Student name:
Student name:
Student name:

All members of the group have participated in this activity.