

## Table of Contents

<b>ABSTRACT .....</b>	2
<b>Splunk Installation in CentOS and adding Agents .....</b>	3
<b>Splunk Adds on and running a query .....</b>	18
<b>Conclusion .....</b>	42
<b>Summary .....</b>	43
<b>Achievement .....</b>	44
<b>References .....</b>	45

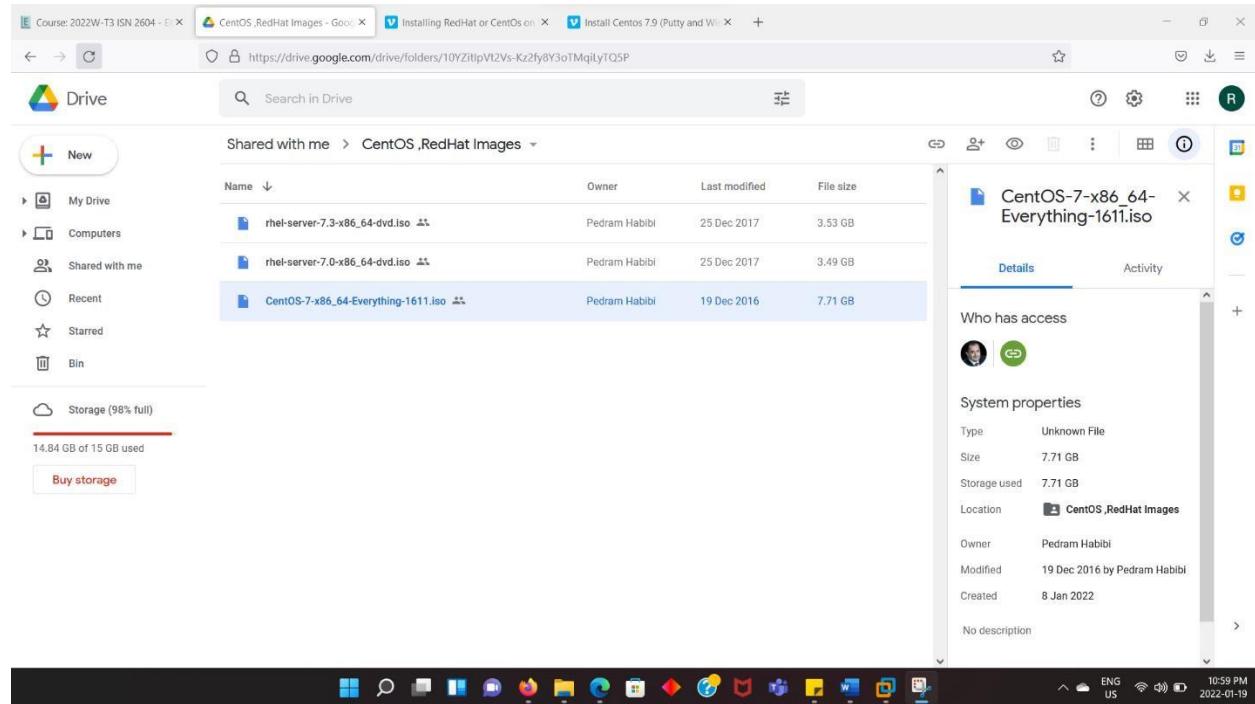
## Abstract

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.

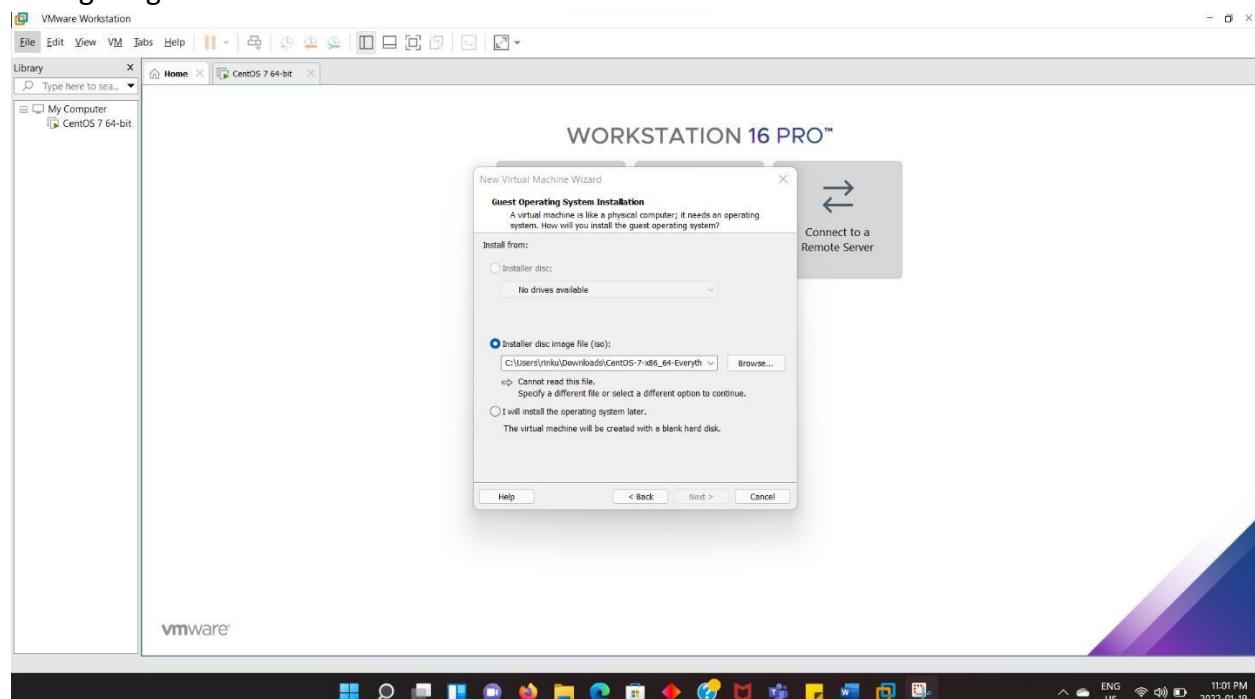
## Part 1

### Splunk Installation in CentOS and adding Agents

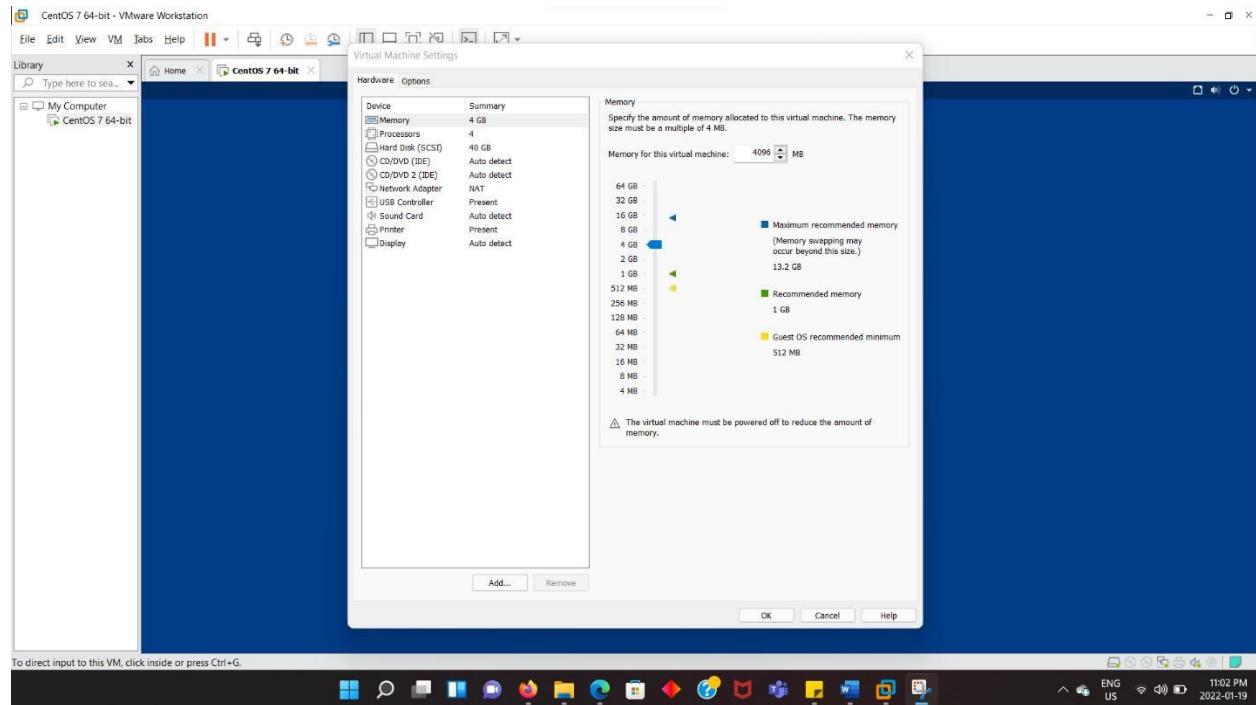
#### CentOS .iso file download



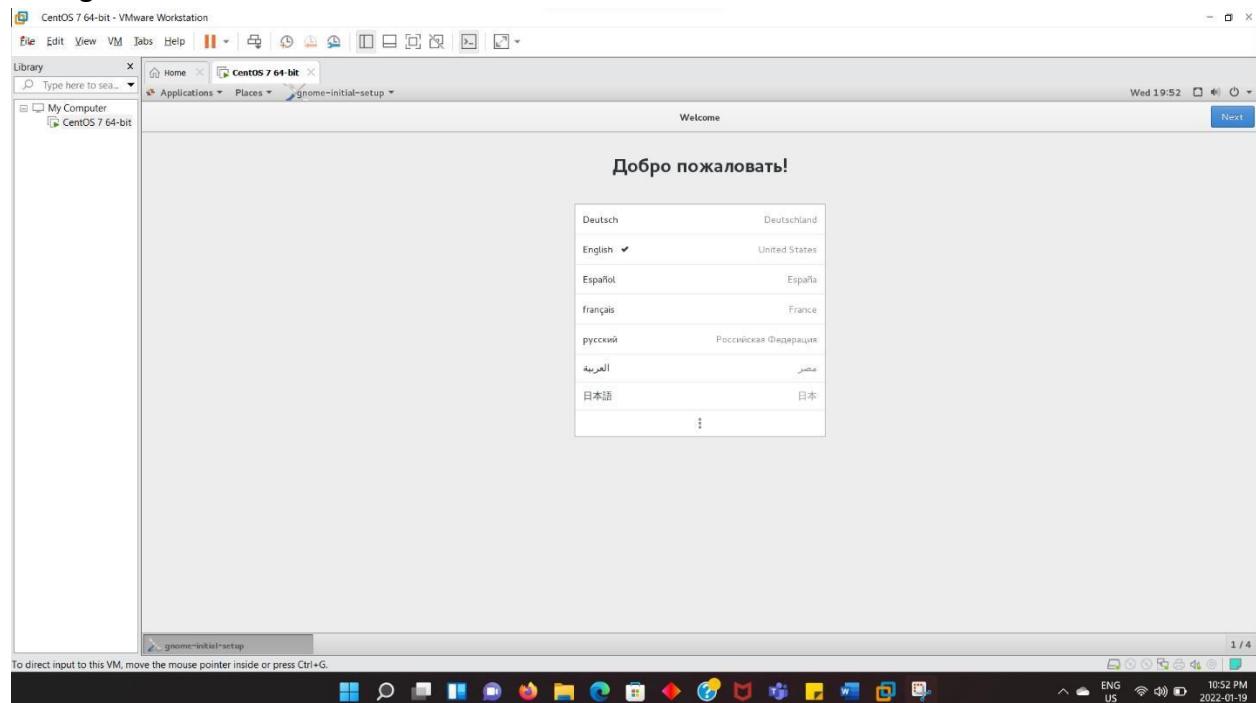
#### Configuring the iso file



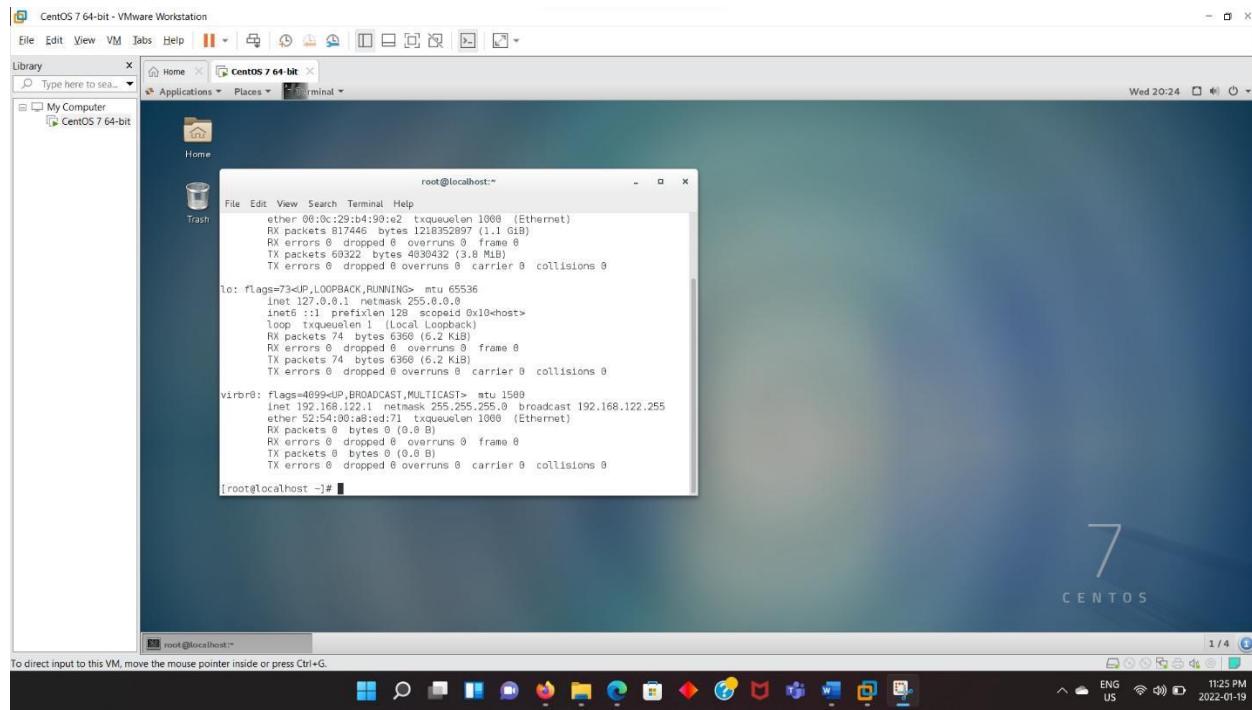
## Selecting the memory size, processor, and network adapter



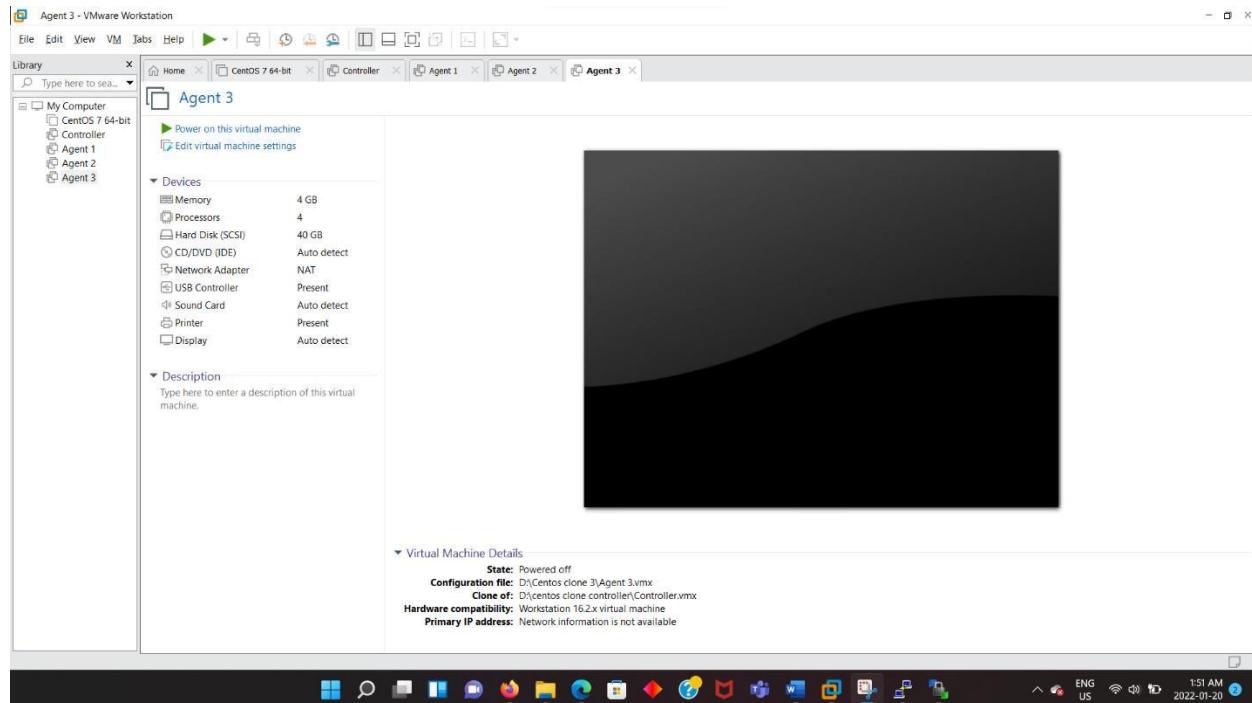
## Configuration after restart



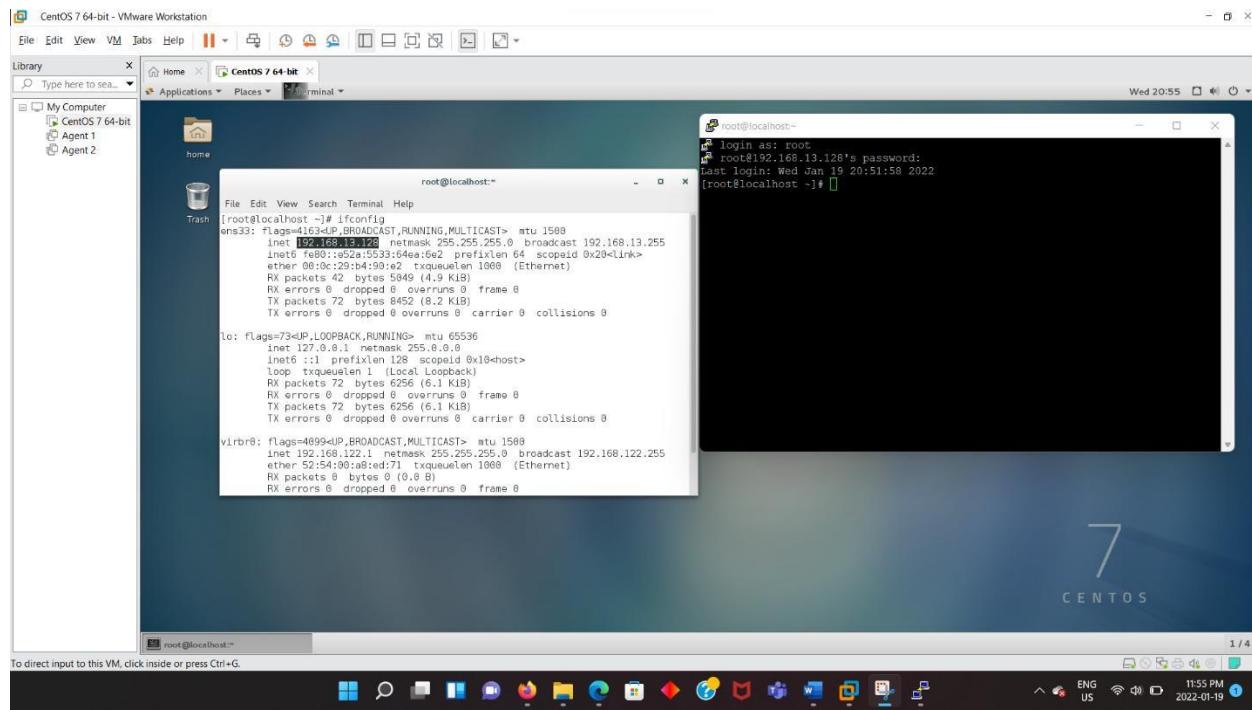
Centos installed successfully.



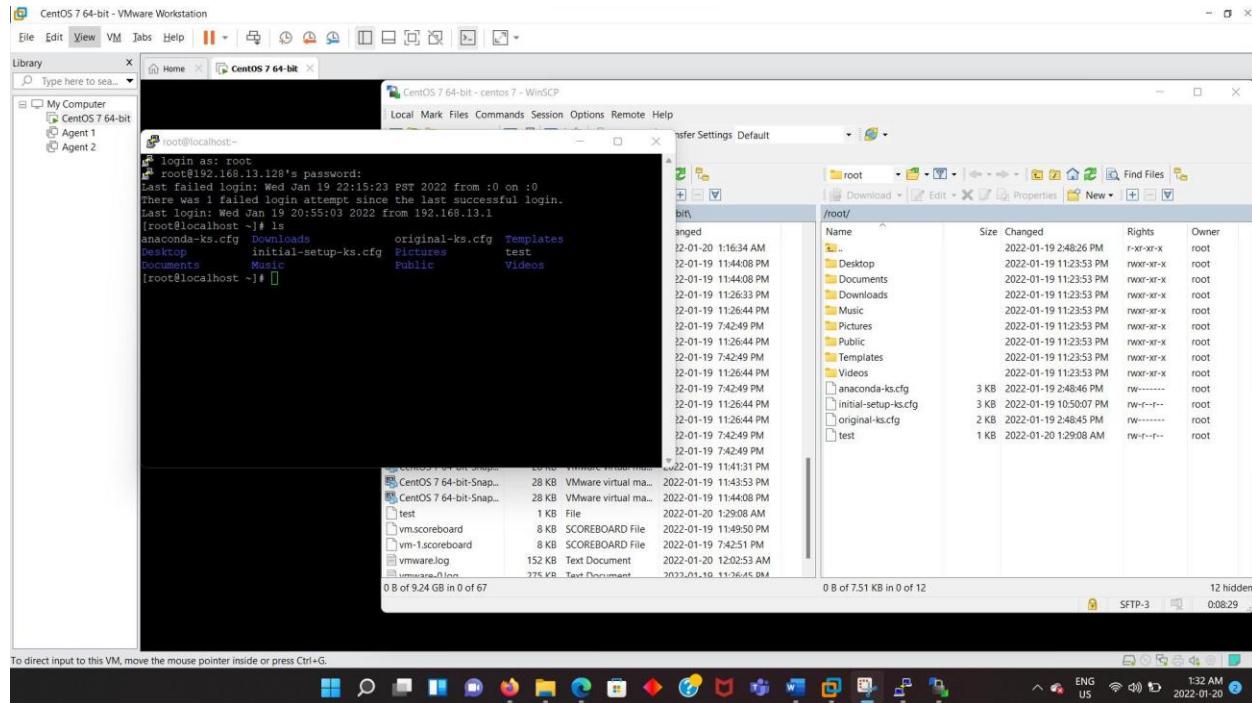
Created controller by cloning centos and 3 agents by cloning controller.

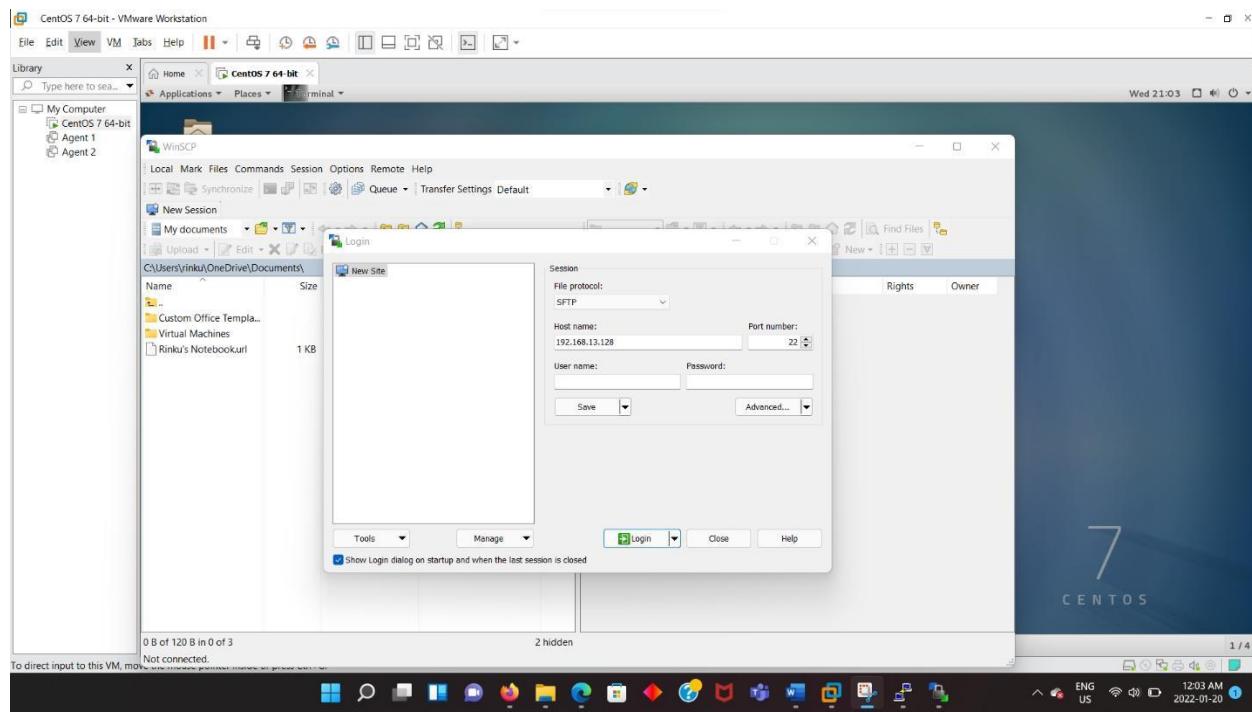


Installed putty and checking the functionality by pasting the IP address of centos and accepting the license.

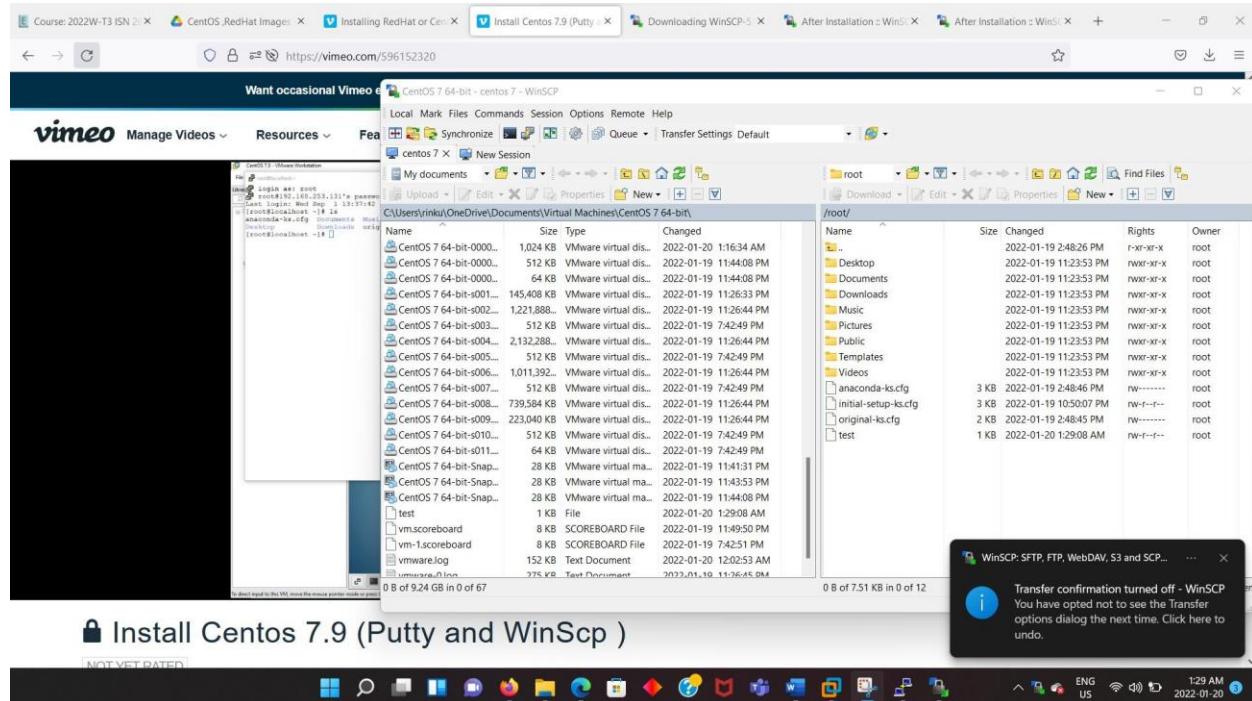


## Installed and configured WinSCP by adding the IP address of centos.

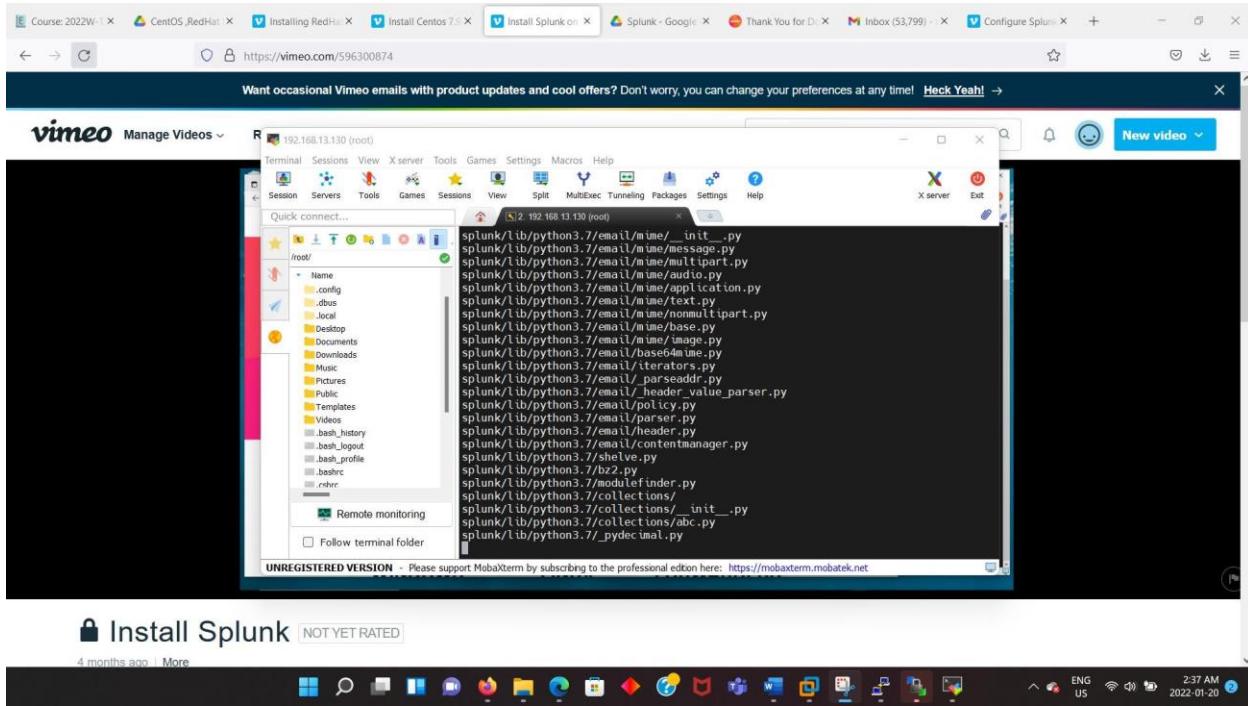




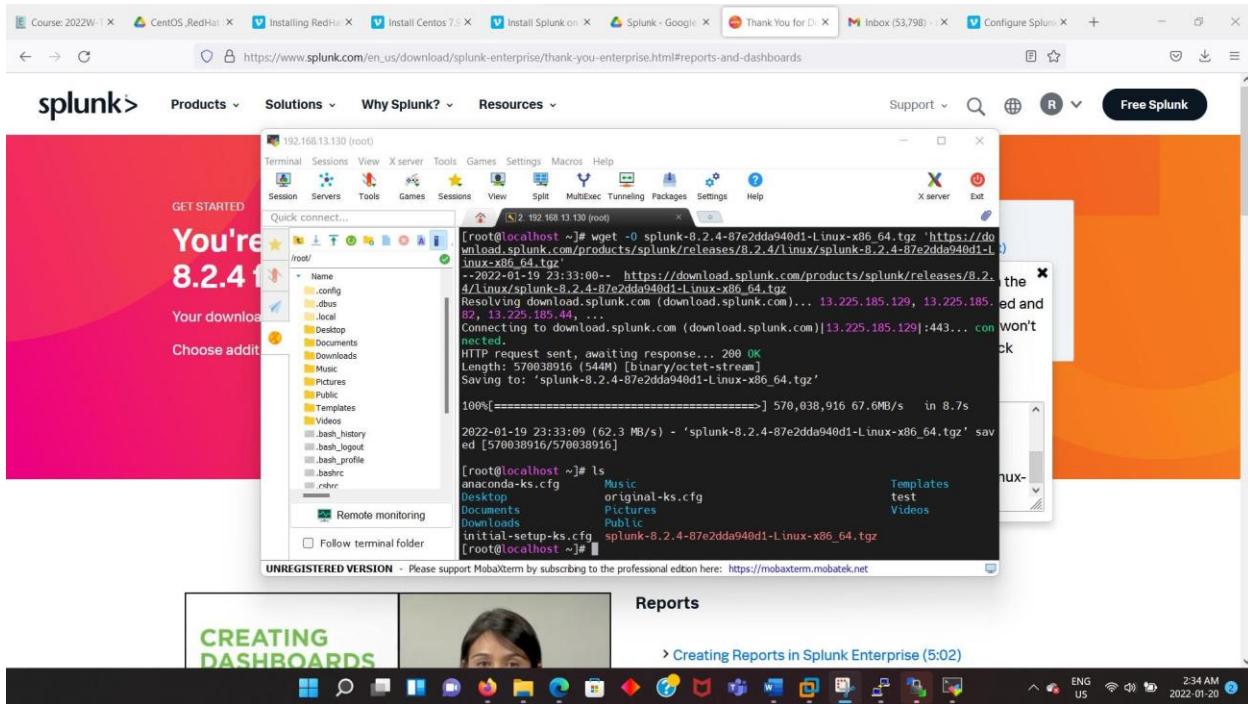
Created a test file on centos to check if the test file can be moved to the root server using the WinSCP tool. From the screenshot, it is evident that the test file was created and moved to the root server successfully.



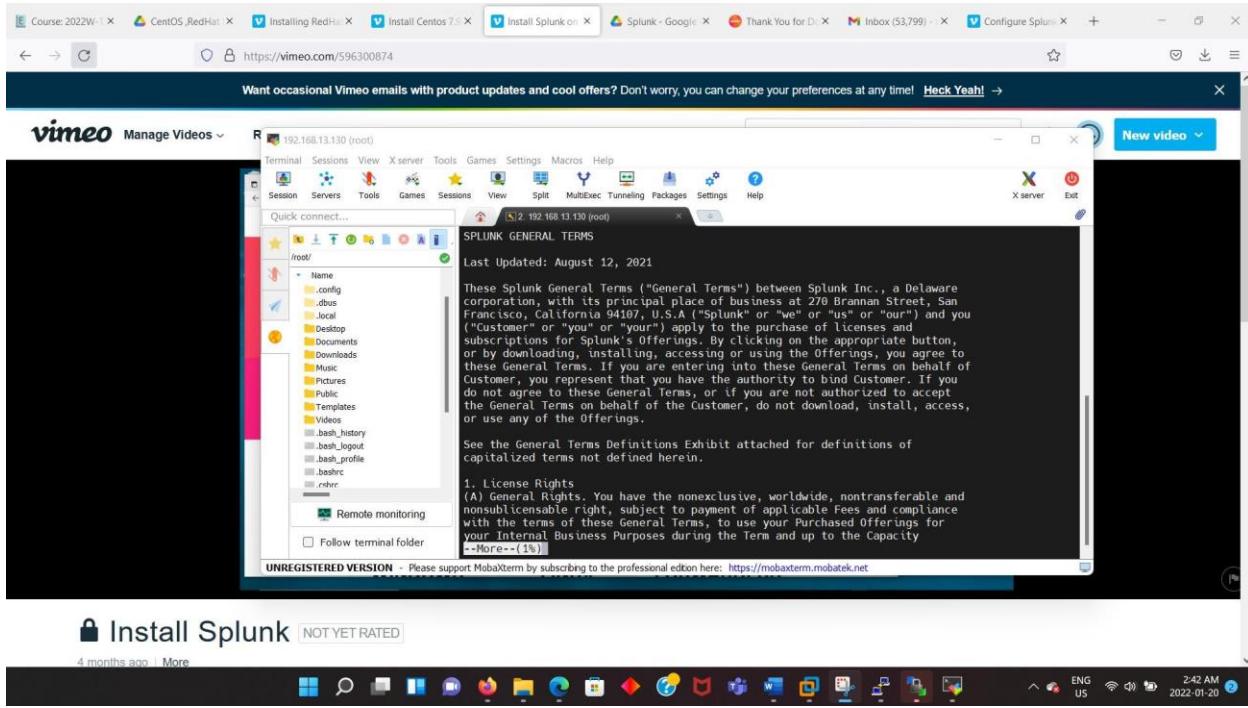
Extracting Splunk file



## Listing Splunk file

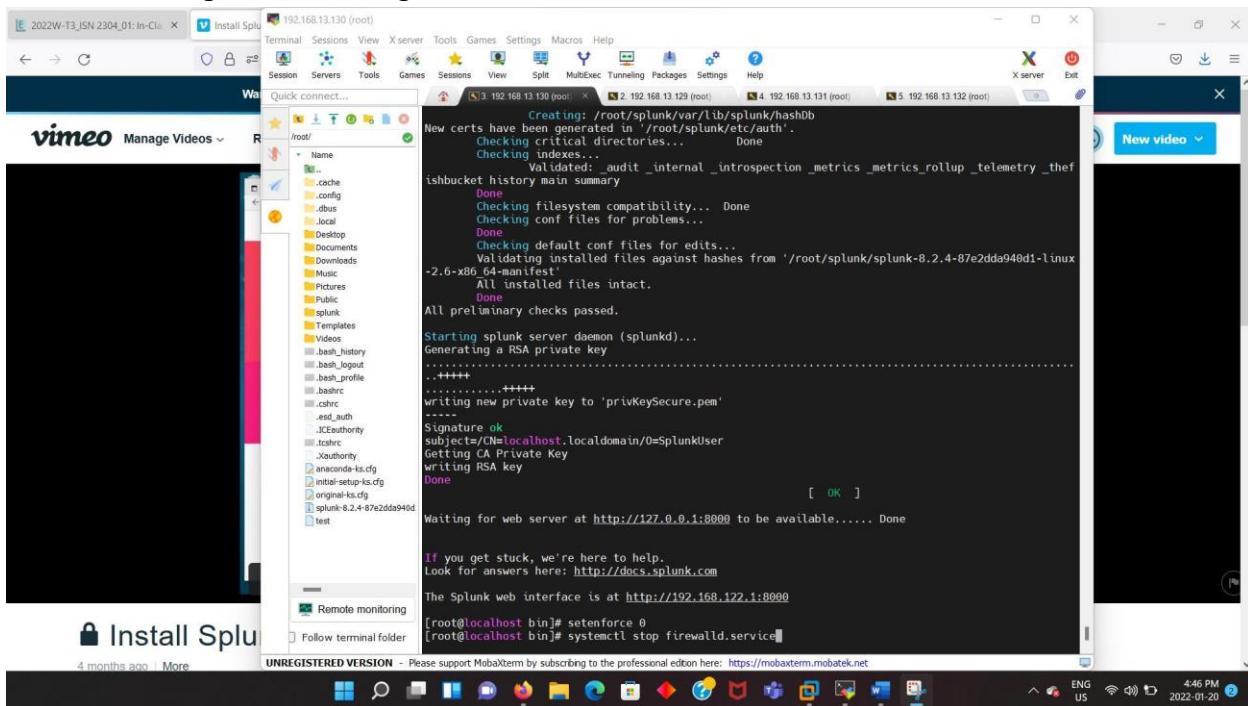


## Launching Splunk

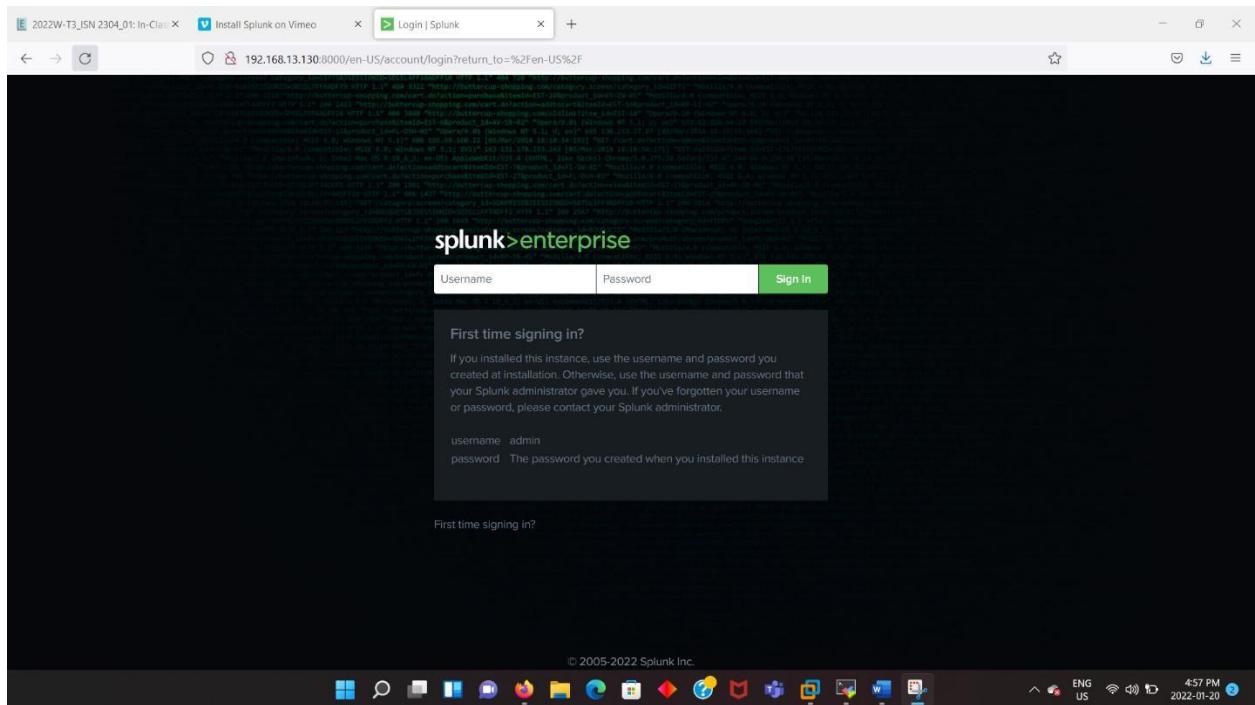


Initiated Splunk web interface and disabling the firewall by entering the command setenforce 0, systemctl stop firewalld.service.

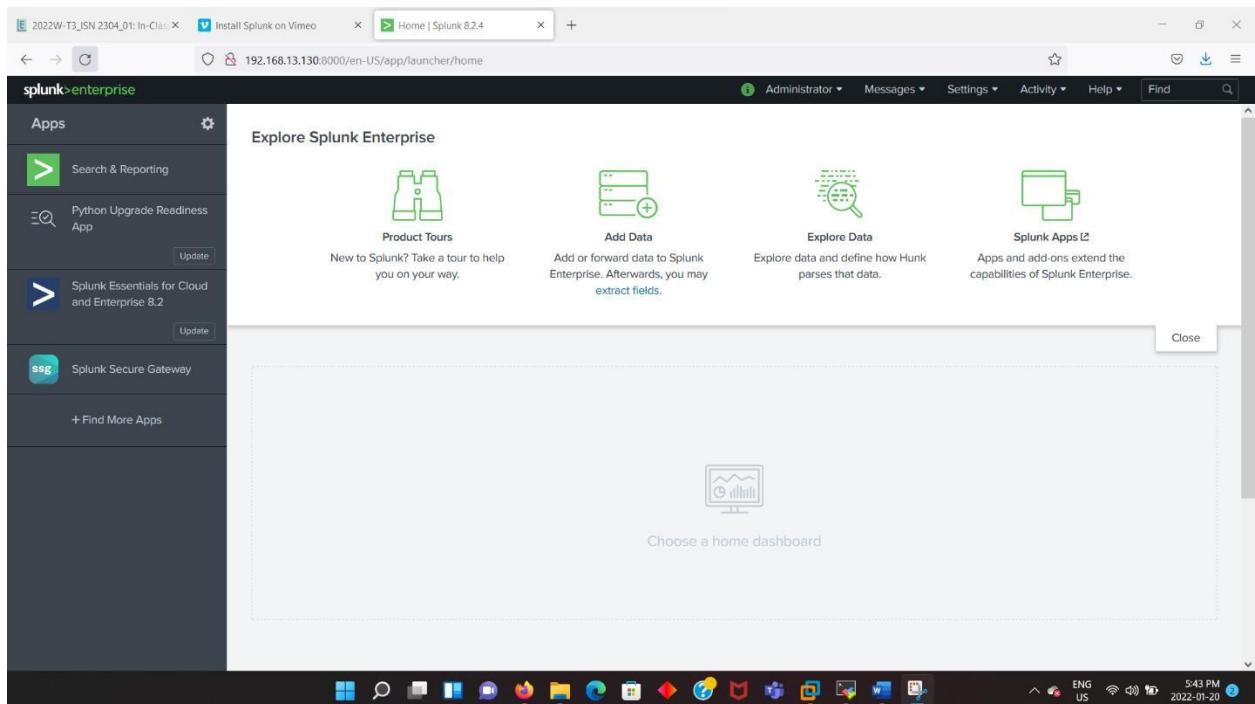
After that we again run ifconfig to check if the controller IP is the same.



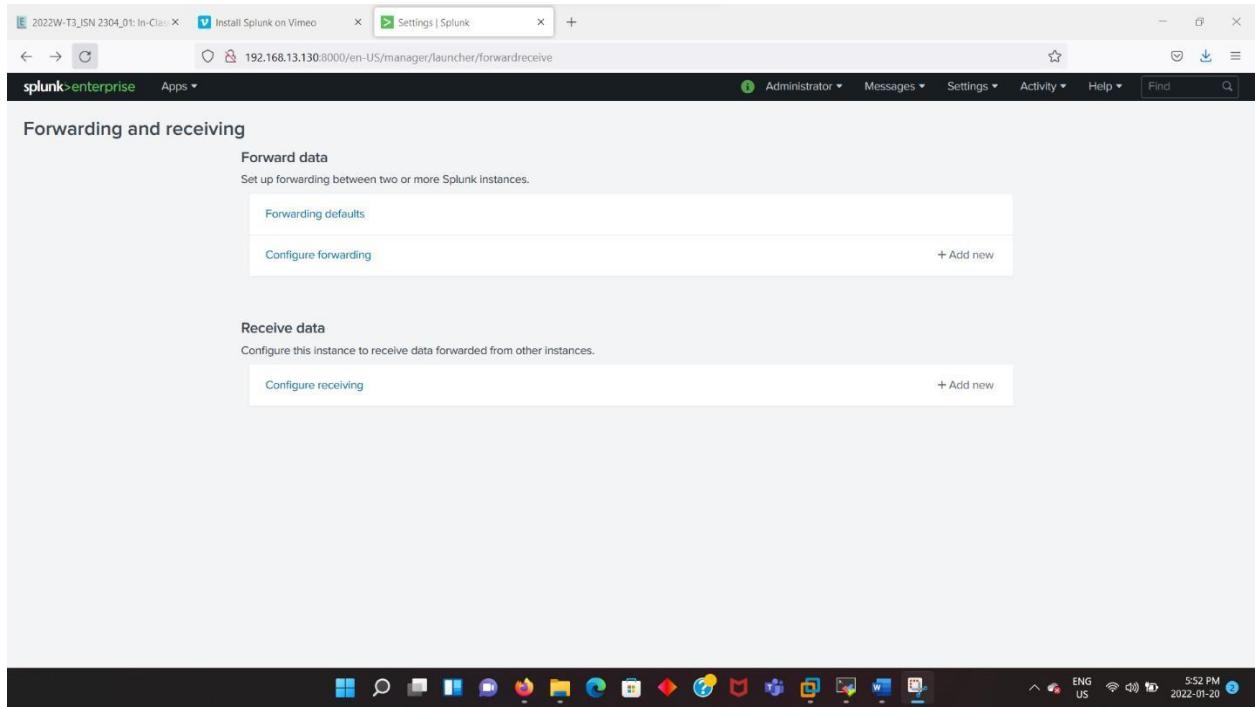
Once confirmed, open a web browser, and paste the IP address along with the port number 8000 and launch Splunk page as shown below.



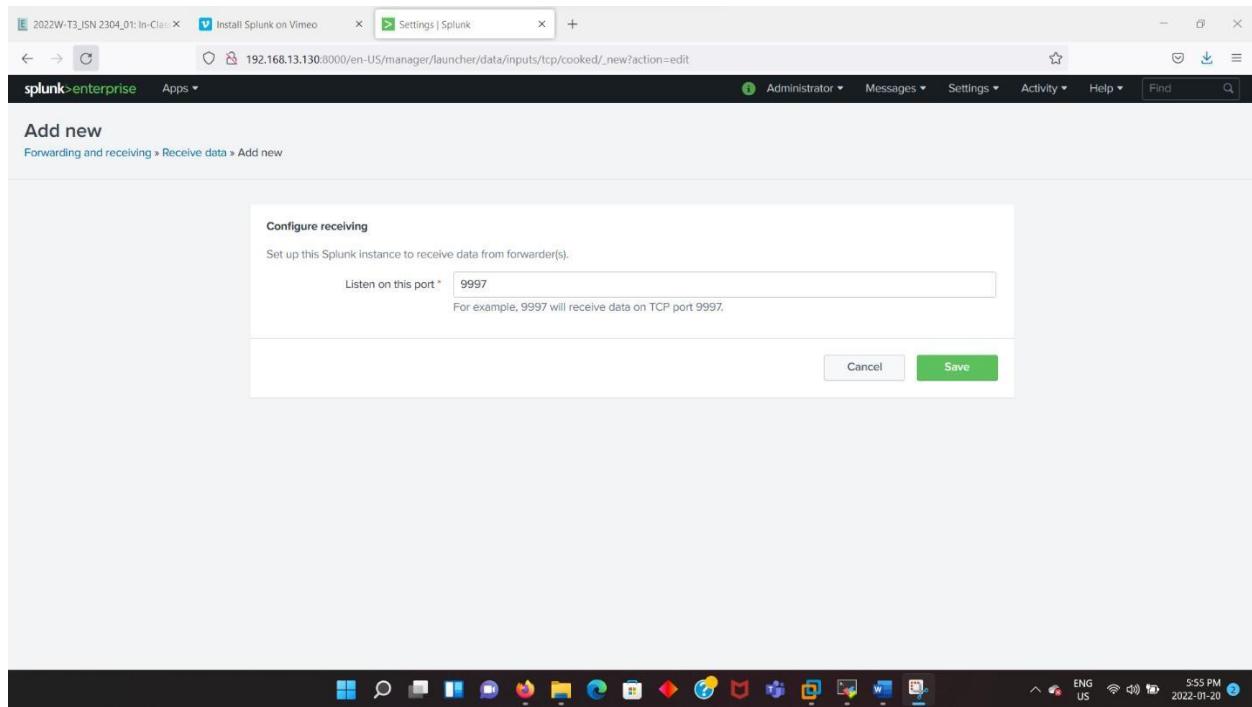
Logging in Splunk using the administrator password which was created during installation.



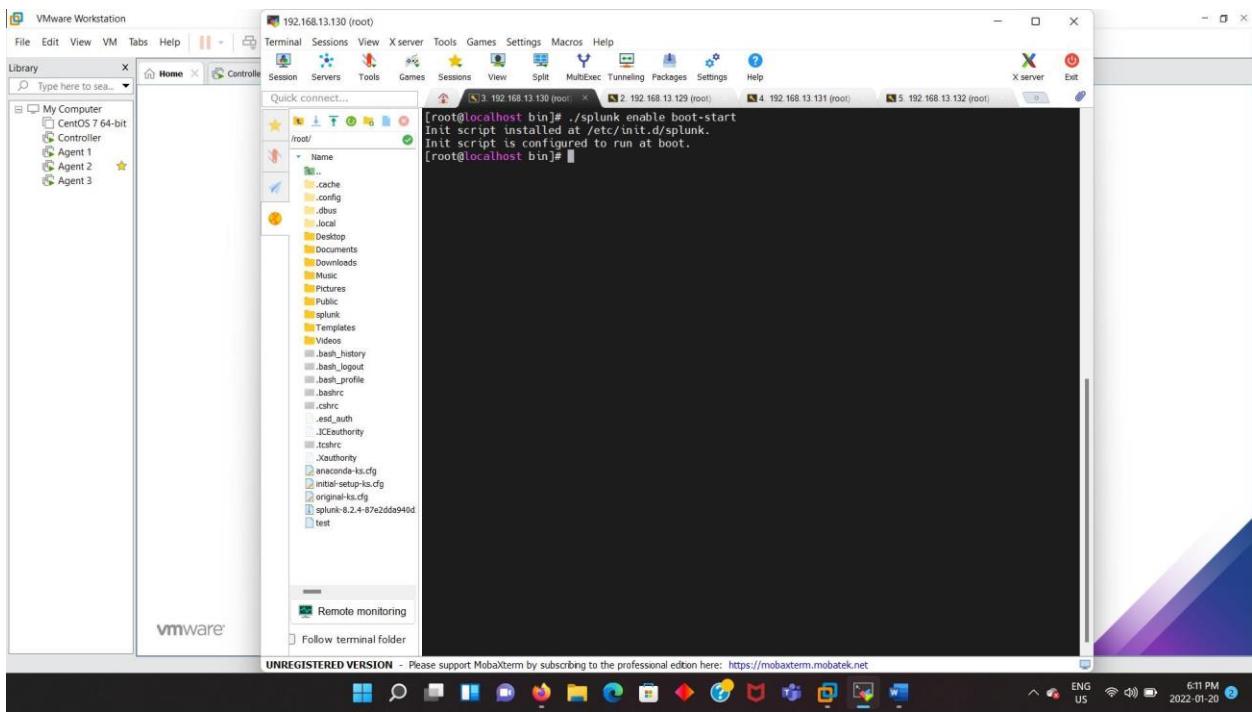
Configuring forwarding and receiving ports



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



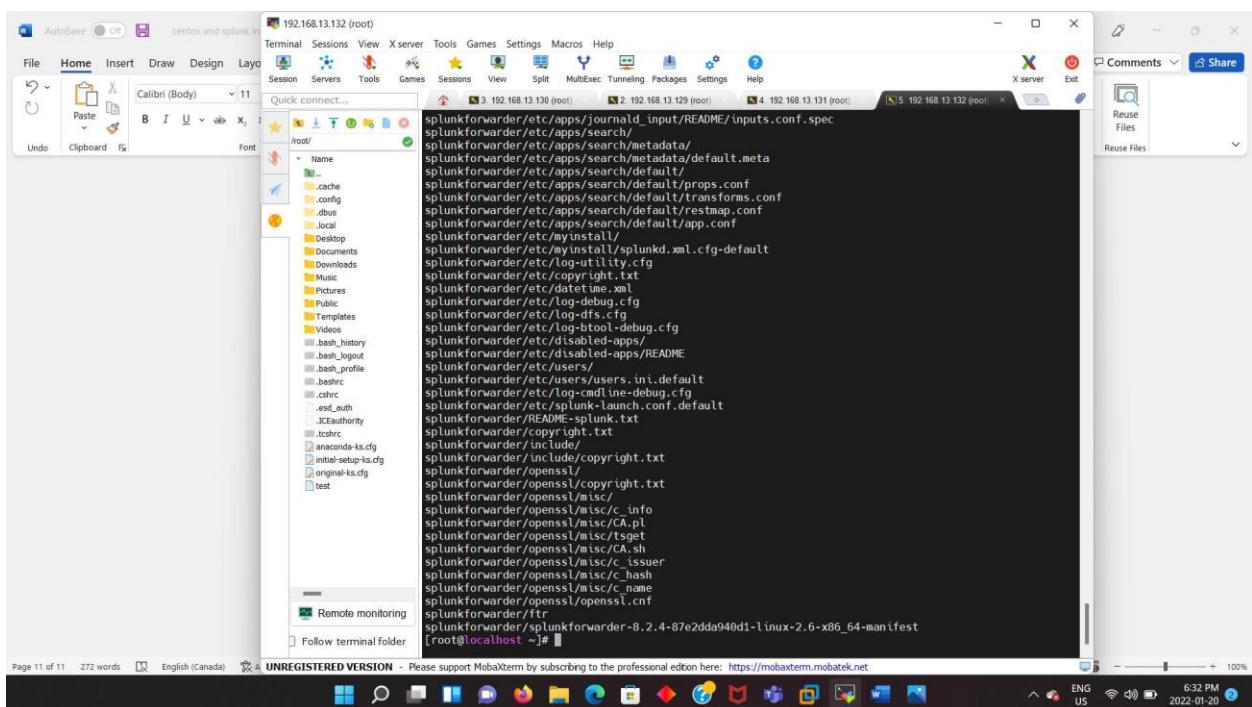
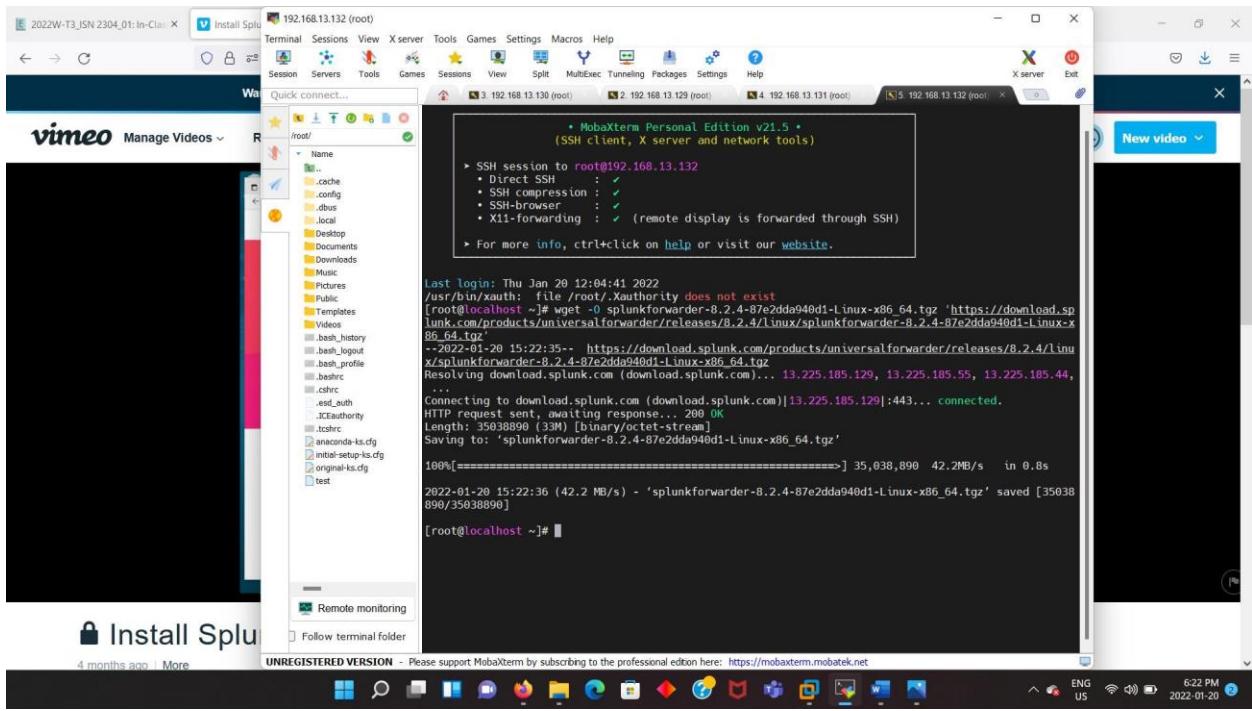
Enabling the boot start command in the controller console by using ./splunk enable boot-start



## Install Splunk universal forwarder for Agent 1

The screenshot shows a web browser window with the URL [https://www.splunk.com/en\\_us/download/universal-forwarder/thank-you-universalforwarder.html](https://www.splunk.com/en_us/download/universal-forwarder/thank-you-universalforwarder.html). The page is titled "GET STARTED" and "You're Downloading Splunk Universal Forwarder 8.2.4 for Linux". It includes instructions to "Your download should have started. No? Try again." and "Choose additional platforms here." Below the main content is a download dialog box from Firefox asking "What should Firefox do with this file?". The "Save File" option is selected. To the right of the dialog, there are links for "FULL TOOLS" such as "download via Command Line (wget)" and "download MD5 to verify your bits". At the bottom of the page, there are four navigation sections: "Install+Setup", "Use + Extend", "Aid + Assistance", and "Community".

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.

The screenshot shows a terminal window in MobaXterm connected to a Splunk forwarder at 192.168.13.132. The terminal session is titled "192.168.13.132 (root)". The terminal output shows the following steps:

- The system prompts for an administrator account creation.
- The user creates a new password.
- The system attempts to start the SplunkForwarder service but fails to find it.
- The user runs the command "Splunk> CSI: Logfiles" to check log files.
- The user runs "Checking prerequisites..." which includes creating various configuration and log files in /root/splunkforwarder.
- A message indicates new certificates have been generated in /root/splunkforwarder/etc/auth.
- The user runs "Checking conf files for problems..." and finds no issues ("Done").
- The user runs "Starting splunk server daemon (splunkd)...".

The terminal window has tabs for multiple sessions, including "Calibri (Body)" and other local sessions. A sidebar on the left shows a file tree for the current directory, and a right-hand panel displays "Comments" and "Share" options. The bottom status bar shows the page number (Page 11 of 11), word count (272 words), language (English (Canada)), and a watermark for "UNREGISTERED VERSION".

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

The screenshot shows a terminal window titled 'Install Splunk' with the IP address '192.168.13.132 (root)'. The terminal interface includes a navigation bar with 'Terminal', 'Sessions', 'View', 'X server', 'Tools', 'Games', 'Settings', 'Macros', and 'Help'. A sidebar on the left lists directory contents under '/root/'. The main pane displays a command-line session:

```
Create credentials for the administrator account.  
Characters do not appear on the screen when you type in credentials.  
Please enter an administrator username: admin  
Password must contain at least:  
* 8 total printable ASCII character(s).  
Please enter a new password:  
Please confirm new password:  
Unit SplunkForwarder.service could not be found.  
Splunk> CSI: Logfiles.  
Checking prerequisites...  
Checking agent port [8089]: open  
Creating: /root/splunkforwarder/var/lib/splunk  
Creating: /root/splunkforwarder/var/run/splunk  
Creating: /root/splunkforwarder/var/run/splunk/appserver/i18n  
Creating: /root/splunkforwarder/var/run/splunk/appserver/modules/static/css  
Creating: /root/splunkforwarder/var/run/splunk/upload  
Creating: /root/splunkforwarder/var/run/splunk/search_telemetry  
Creating: /root/splunkforwarder/var/spool/splunk  
Creating: /root/splunkforwarder/var/spool/dimoncache  
Creating: /root/splunkforwarder/var/lib/splunk/authDb  
Creating: /root/splunkforwarder/var/lib/splunk/hashDb  
New certs have been generated in '/root/splunkforwarder/etc/auth'.  
Checking conf files for problems...  
Done  
Checking default conf files for edits...  
Validating installed files against hashes from '/root/splunkforwarder/splunkforwarder-8.2.4-87e2ddaa940d1-linux-x86_64-manifest'  
All installed files intact.  
Done  
All preliminary checks passed.  
Starting splunk server daemon (splunkd)...  
Done  
[OK]  
[root@localhost bin]# ./splunk enable boot-start  
Init script installed at /etc/init.d/splunk.  
Init script is configured to run at boot.  
[root@localhost bin]#
```

Added the forwarder server by authenticating admin credentials

```

[8] 192.168.13.132 (root)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiTerm Tunneling Packages Settings Help
Quick connect...
[8. 192.168.13.131 (root)] [10. 192.168.13.132 (root)] [11. 192.168.13.129 (root)] [12. 192.168.13.132 (root)]
[root@localhost bin]# ./splunk add forward-server 192.168.13.133:9997 -auth admin:Venus*7979
Added Forwarding to: 192.168.13.133:9997.
[root@localhost bin]#

```

```

[10. 192.168.13.132 (root)] [12. 192.168.13.132 (root)]
[root@localhost bin]# ./splunk set deploy-poll 192.168.13.133:9997 -auth admin:Venus*7979
Configuration updated.
[root@localhost bin]#

```

```

[12. 192.168.13.132 (root)]
[root@localhost bin]# ./splunk add monitor /var/log

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

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

```

[8] 192.168.13.131 (root)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiTerm Tunneling Packages Settings Help
Quick connect...
[8. 192.168.13.131 (root)] [10. 192.168.13.132 (root)] [12. 192.168.13.131 (root)]
[root@localhost bin]# ./splunk add forward-server 192.168.13.133:9997 -auth admin:Venus*7979
Added Forwarding to: 192.168.13.133:9997.
[root@localhost bin]# ./splunk set deploy-poll 192.168.13.133:9997 -auth admin:Venus*7979
Configuration updated.
[root@localhost bin]#

```

```

[10. 192.168.13.132 (root)] [12. 192.168.13.131 (root)]
[root@localhost bin]# ./splunk add monitor /var/log

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

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

```

[192.168.13.132 (root)]
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
10. 192.168.13.132 (root) 12. 192.168.13.131 (root) 13. 192.168.13.131 (root)
[root@localhost bin]# ./splunk add forward-server 192.168.13.131:9997 -auth admin:Venus*7979
Added Forwarder to 192.168.13.131:9997.
[root@localhost bin]# ./splunk set deploy-poll 192.168.13.131:9997 -auth admin:Venus*7979
Configuration updated.
[root@localhost bin]# ./splunk add monitor /var/log/
Added monitor of '/var/log'.
[root@localhost bin]#

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

## Restarted Agents.

```

[192.168.13.131 (root)]
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
10. 192.168.13.132 (root) 12. 192.168.13.132 (root) 13. 192.168.13.131 (root)
[root@localhost bin]# ./splunk add forward-server 192.168.13.131:9997 -auth admin:Venus*7979
Added Forwarder to 192.168.13.131:9997.
[root@localhost bin]# ./splunk set deploy-poll 192.168.13.131:9997 -auth admin:Venus*7979
Configuration updated.
[root@localhost bin]# ./splunk add monitor /var/log/
Added monitor of '/var/log'.
[root@localhost bin]# ./splunk restart
Unit SplunkForwarder.service could not be found.
Unit SplunkForwarder.service could not be found.
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.
Stopping splunk helpers... [ OK ]
Done.
Unit SplunkForwarder.service could not be found.
Splunk> Take the sh out of IT.

Checking prerequisites...
    Checking mgmt port [8089]: open
    Checking conf files for problems...
    Done
    Checking default conf files for edits...
    Validating installed files against hashes from '/root/splunkforwarder/splunkforwarder-8.2.4-87e2dd940d1-linux-2.6-x86_64-manifest'
    All installed files intact.
    Done
All preliminary checks passed.
Starting splunk server daemon (splunkd)... [ OK ]
Done
[root@localhost bin]#

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

Captured logs for 2 Agents successfully

Screenshot of a Splunk search interface showing a search for events related to a specific host.

**Search URL:** 192.168.13.133:8000/en-US/app/search/search?dispatch.sample\_ratio=10&earliest=-1d%40d&latest=%40d&q=search error OR failed OR severe OR { sourcetype:\*

**Events (21) Sampling 1: 10 ▾**

**Selected Fields:**

- host
- a\_host 3
- a\_source 3
- a\_sourcetype 3

**Interesting Fields:**

- # date\_hour 3
- # date\_mday 1
- # date\_minut 4
- # 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
- #timeendsec 2

**Reports:**

Values	Count	%
192.168.13.132	8	38.09%
localhost	8	38.09%
192.168.13.131	5	23.81%

**Event Details:**

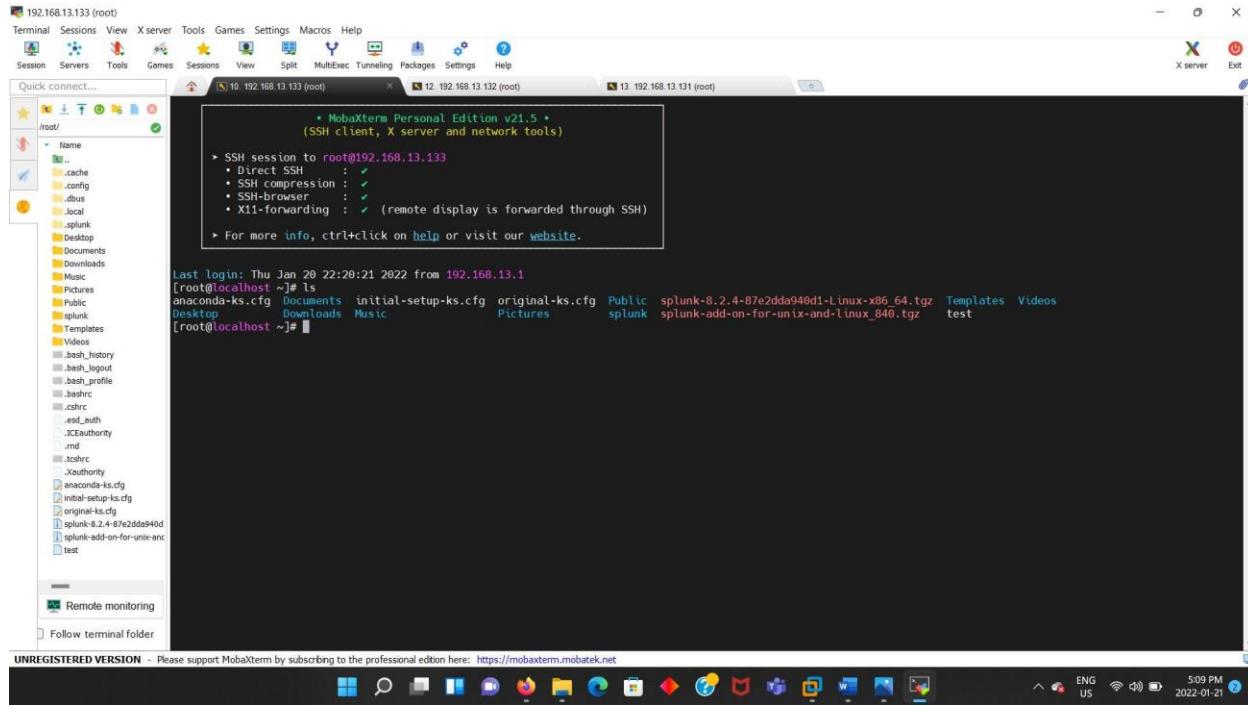
10 events at 11 AM on Thursday, January 20, 2022

- 200 183 Renew-Subscription client-error-not-found type = cups\_access GDBus.UnmappedGError.Quark.\_imsettings\_2error\_2dquark.Code5: Current desktop isn't targ
- : Error sending ATA command IDENTIFY PACKET DEVICE to /dev/sr0: ATA command failed: erro
- [ 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]
- host = 192.168.13.132 | source = /var/log/dmesg | sourcetype = dmesg
- [ 19.206096] pci 0000:00:18.4: BAR 13: failed to assign [io size 0x1000]
- host = 192.168.13.132 | source = /var/log/dmesg | sourcetype = dmesg
- [ 19.206067] pci 0000:00:18.5: BAR 13: failed to assign [io size 0x1000]

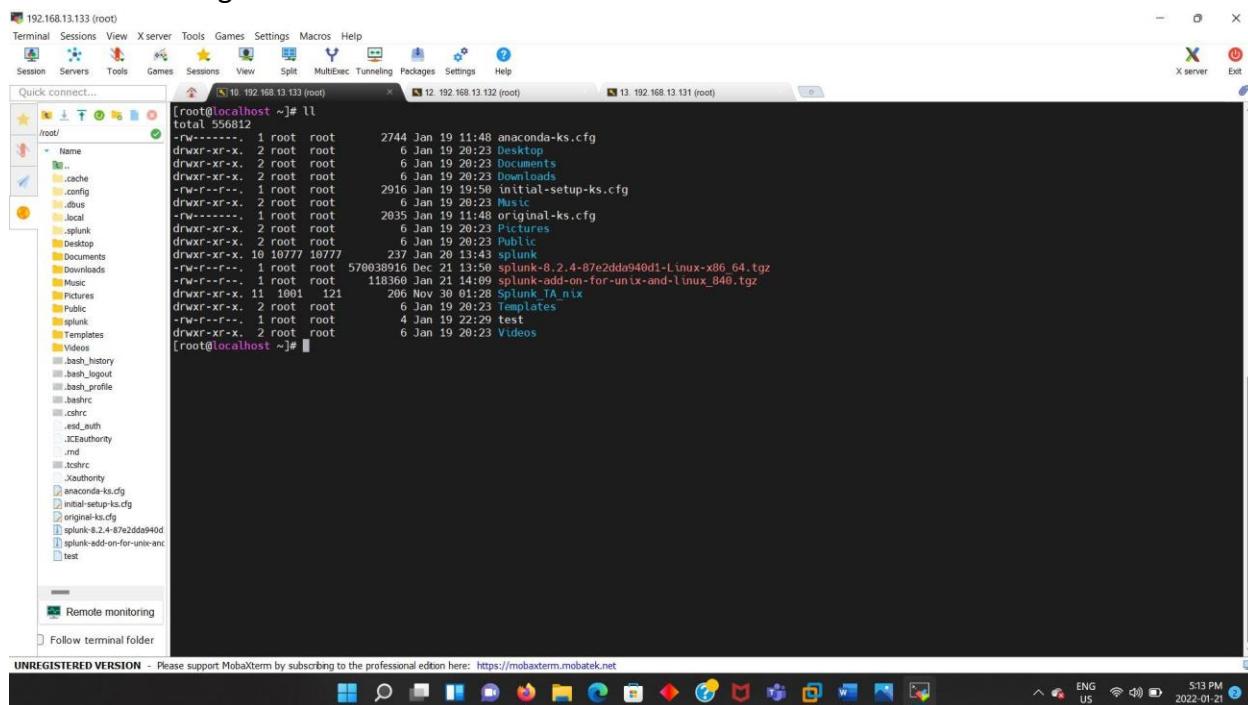
## Part 2

### Splunk Adds on and running a query

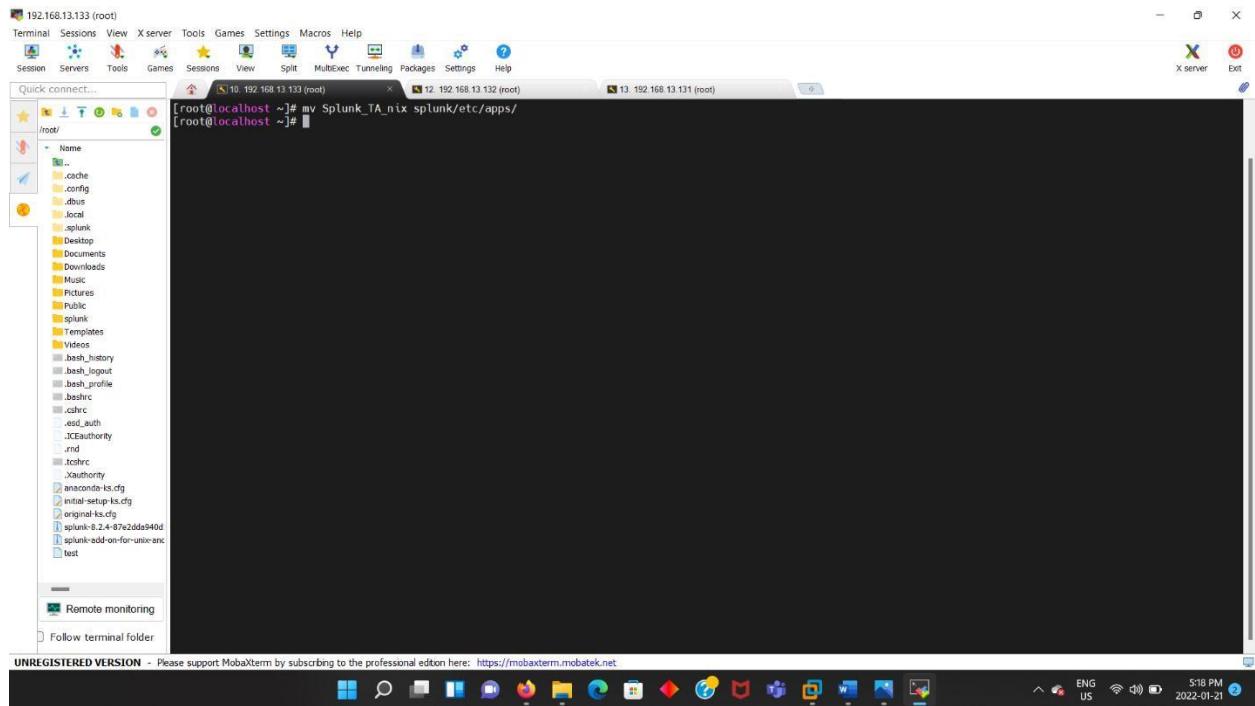
Downloaded Splunk adds – on file and listed to confirm if it is installed successfully.



Extracted the file using tar -xvf command and listed

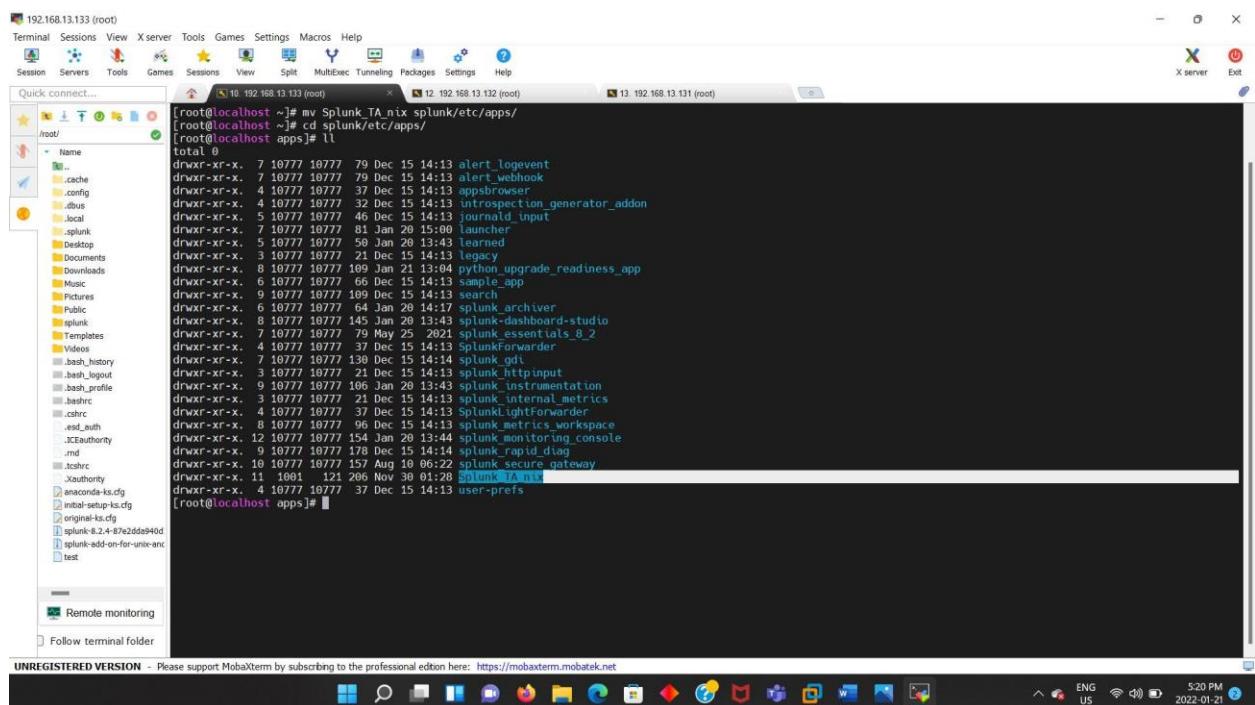


Moved the file to splunk/etc/apps/ directory



```
[root@localhost ~]# mv Splunk_TA_nix splunk/etc/apps/
[root@localhost ~]#
```

File moved successfully



```
[root@localhost ~]# cd Splunk_TA_nix
[root@localhost Splunk_TA_nix]# ll
```

File	Permissions	Last Modified	Size
total 0			
drwxr-xr-x..	7 10777 10777 79 Dec 15 14:13	alert_logevent	
drwxr-xr-x..	7 10777 10777 79 Dec 15 14:13	alert_webhook	
drwxr-xr-x..	4 10777 10777 37 Dec 15 14:13	appsbrowser	
drwxr-xr-x..	4 10777 10777 32 Dec 15 14:13	introspection_generator_addon	
drwxr-xr-x..	5 10777 10777 46 Dec 15 14:13	journald_input	
drwxr-xr-x..	7 10777 10777 81 Jan 28 15:00	launcher	
drwxr-xr-x..	5 10777 10777 58 Jan 28 13:43	learned	
drwxr-xr-x..	3 10777 10777 21 Dec 15 14:13	legacy	
drwxr-xr-x..	8 10777 10777 189 Jan 21 13:04	python_upgrade_readiness_app	
drwxr-xr-x..	6 10777 10777 66 Dec 15 14:13	sample_app	
drwxr-xr-x..	9 10777 10777 109 Dec 15 14:13	sample_app	
drwxr-xr-x..	6 10777 10777 64 Jan 28 14:17	splunk_archiver	
drwxr-xr-x..	8 10777 10777 145 Jan 28 13:43	splunk-dashboard-studio	
drwxr-xr-x..	7 10777 10777 79 May 25 2021	splunk_essentials_8_2	
drwxr-xr-x..	4 10777 10777 37 Dec 15 14:13	SplunkForwarder	
drwxr-xr-x..	7 10777 10777 138 Dec 15 14:14	splunk_gdi	
drwxr-xr-x..	3 10777 10777 21 Dec 15 14:13	splunk_httpinput	
drwxr-xr-x..	9 10777 10777 106 Jan 28 13:43	splunk_instrumentation	
drwxr-xr-x..	3 10777 10777 21 Dec 15 14:13	splunk_internal_metrics	
drwxr-xr-x..	4 10777 10777 37 Dec 15 14:13	SplunkLightForwarder	
drwxr-xr-x..	12 10777 10777 154 Jan 28 13:43	splunk_metrics_workspace	
drwxr-xr-x..	10 10777 10777 11 Dec 15 14:14	splunk_monitoring_console	
drwxr-xr-x..	10 10777 10777 57 Aug 10 06:22	splunk_rapid_dtag	
drwxr-xr-x..	11 10801 123 206 Nov 30 01:20	splunk_secure_gateway	
drwxr-xr-x..	4 10777 10777 37 Dec 15 14:13	user-prefs	

Listing the files under Splunk directory using cd Splunk\_TA\_nix

```

drwxr-xr-x . 7 10777 10777 79 Dec 15 14:13 alert_webhook
drwxr-xr-x . 4 10777 10777 37 Dec 15 14:13 appsbrowser
drwxr-xr-x . 4 10777 10777 32 Dec 15 14:13 introspection_generator_addon
drwxr-xr-x . 5 10777 10777 46 Dec 15 14:13 launcher
drwxr-xr-x . 5 10777 10777 58 Jan 20 15:00 learned
drwxr-xr-x . 3 10777 10777 21 Dec 15 14:13 legacy
drwxr-xr-x . 8 10777 10777 109 Jan 21 13:04 python_upgrade_readiness_app
drwxr-xr-x . 6 10777 10777 66 Dec 15 14:13 sample_app
drwxr-xr-x . 9 10777 10777 109 Dec 15 14:13 search
drwxr-xr-x . 6 10777 10777 64 Jan 20 14:17 splunk_archiver
drwxr-xr-x . 8 10777 10777 145 Jan 20 13:43 splunk-dashboard-studio
drwxr-xr-x . 7 10777 10777 79 May 25 2021 splunk_essentials_8_2
drwxr-xr-x . 4 10777 10777 37 Dec 15 14:13 SplunkForwarder
drwxr-xr-x . 3 10777 10777 139 Dec 15 14:14 splunk_gd
drwxr-xr-x . 9 10777 10777 106 Jan 20 13:43 splunk_hadoop
drwxr-xr-x . 3 10777 10777 21 Dec 15 14:13 splunk_instrumentation
drwxr-xr-x . 3 10777 10777 106 Jan 20 13:43 splunk_internal_metrics
drwxr-xr-x . 4 10777 10777 37 Dec 15 14:13 SplunkLightForwarder
drwxr-xr-x . 8 10777 10777 96 Dec 15 14:13 splunk_metrics_workspace
drwxr-xr-x . 12 10777 10777 154 Jan 20 13:44 splunk_monitoring_console
drwxr-xr-x . 9 10777 10777 178 Dec 15 14:14 splunk_rapid_diag
drwxr-xr-x . 10 10777 10777 157 Aug 10 06:22 splunk_secure_gateway
drwxr-xr-x . 11 1091 121 261 Nov 30 01:28 Splunk_TA_nix
drwxr-xr-x . 4 10777 10777 37 Dec 15 14:13 user-prefs
[root@localhost apps]# cd Splunk_TA_nix
[root@localhost Splunk_TA_nix]# ll
total 24
drwxr-xr-x . 1 1001 121 1552 Nov 30 01:28 app.manifest
drwxr-xr-x . 3 1001 121 29 Nov 30 01:28 appserver
drwxr-xr-x . 2 1001 121 4096 Nov 30 01:28 bin
drwxr-xr-x . 3 1001 121 189 Nov 30 01:28 default
drwxr-xr-x . 2 1001 121 39 Nov 30 01:28 lib
drwxr-xr-x . 2 1001 121 64 Nov 30 01:28 LICENSES
drwxr-xr-x . 2 1001 121 4096 Nov 30 01:28 lookups
drwxr-xr-x . 2 1001 121 26 Nov 30 01:28 metadata
drwxr-xr-x . 2 1001 121 31 Nov 30 01:28 README
-rw-r--r-- . 1 1001 121 164 Nov 30 01:28 README.txt
drwxr-xr-x . 2 1001 121 139 Nov 30 01:28 static
-rw-r--r-- . 1 1001 121 123 Nov 30 01:28 THIRDPARTY
-rw-r--r-- . 1 1001 121 11 Nov 30 01:28 VERSION
[root@localhost Splunk_TA_nix]# ll

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

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**

```

drwxr-xr-x . 1001 121 120 Nov 30 01:28 default
-rw-r--r-- . 1 1001 121 494 Nov 30 01:28 app.conf
drwxr-xr-x . 3 1001 121 16 Nov 30 01:28 data
-rw-r--r-- . 1 1001 121 19690 Nov 30 01:28 eventtypes.conf
-rw-r--r-- . 1 1001 121 5714 Nov 30 01:28 inputs.conf
-rw-r--r-- . 1 1001 121 217 Nov 30 01:28 macros.conf
-rw-r--r-- . 1 1001 121 33765 Nov 30 01:28 props.conf
-rw-r--r-- . 1 1001 121 219 Nov 30 01:28 restmap.conf
-rw-r--r-- . 1 1001 121 1024 Nov 30 01:28 transforms.conf
-rw-r--r-- . 1 1001 121 24502 Nov 30 01:28 web.conf
-rw-r--r-- . 1 1001 121 178 Nov 30 01:28 web.conf
[root@localhost default]# vi inputs.conf

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

The output is shown below.

```

# [script://bin/vmstat_metric.sh]
sourcetype = vmstat_metric
source = vmstat
interval = 60
disabled = 1

[script://bin/iostat_metric.sh]
sourcetype = iostat_metric
source = iostat
interval = 60
disabled = 1

[script://bin/ps_metric.sh]
sourcetype = ps_metric
source = ps
interval = 30
disabled = 1

[script://bin/df_metric.sh]
sourcetype = df_metric
source = df
interval = 300
disabled = 1

[script://bin/interfaces_metric.sh]
sourcetype = interfaces_metric
source = interfaces
interval = 60
disabled = 1

[script://bin/cpu_metric.sh]
sourcetype = cpu_metric
source = cpu
interval = 30
disabled = 1

#####
##### Event Inputs #####
#####

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

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.

```

# May require Splunk forwarder to run as root on some platforms.
[script://bin/service.sh]
disabled = true
interval = 3600
source = Unix:Service
sourcetype = Unix:Service

# Currently only supports SunOS, Linux, OSX.
# May require Splunk forwarder to run as root on some platforms.
[script://bin/sshdchecker.sh]
disabled = true
interval = 3600
source = Unix:SSHConfig
sourcetype = Unix:SSHConfig

# Currently only supports Linux, OSX.
# May require Splunk forwarder to run as root on some platforms.
[script://bin/update.sh]
disabled = true
interval = 86400
source = Unix:Update
sourcetype = Unix:Update

[script://bin/uptime.sh]
disabled = true
interval = 86400
source = Unix:Uptime
sourcetype = Unix:Uptime

[script://bin/version.sh]
disabled = true
interval = 86400
source = Unix:Version
sourcetype = Unix:Version

# This script may need to be modified to point to the VSFTPD configuration file.
[script://bin/vsftpdchecker.sh]
disabled = true
interval = 86400
source = Unix:VSFTPDConfig
sourcetype = Unix:VSFTPDConfig

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

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

```

192.168.13.133 (root)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
[14 192.168.13.133 (root)] 14. 192.168.13.133 (root) [16 192.168.13.132 (root)] 16. 192.168.13.132 (root) [18 192.168.13.134 (root)] 18. 192.168.13.134 (root)
[root@localhost default]# ll
total 120
-rw-r--r--. 1 1001 121 494 Nov 30 01:28 app.conf
drwxr-xr-x. 3 1001 121 16 Nov 30 01:28 data
-rw-r--r--. 1 1001 121 5714 Nov 30 01:28 eventtypes.conf
-rw-r--r--. 1 1001 121 217 Nov 30 01:28 macros.conf
-rw-r--r--. 1 1001 121 33765 Nov 30 01:28 props.conf
-rw-r--r--. 1 1001 121 219 Nov 30 01:28 restmap.conf
-rw-r--r--. 1 1001 121 13151 Nov 30 01:28 tags.conf
-rw-r--r--. 1 1001 121 24502 Nov 30 01:28 transforms.conf
-rw-r--r--. 1 1001 121 178 Nov 30 01:28 web.conf
[root@localhost default]# vi inputs.conf
[root@localhost default]#

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

Now we go back by executing cd ..

```

192.168.13.133 (root)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
[14 192.168.13.133 (root)] 14. 192.168.13.133 (root) [16 192.168.13.132 (root)] 16. 192.168.13.132 (root) [18 192.168.13.134 (root)] 18. 192.168.13.134 (root)
[root@localhost default]# ll
total 120
-rw-r--r--. 1 1001 121 494 Nov 30 01:28 app.conf
drwxr-xr-x. 3 1001 121 16 Nov 30 01:28 data
-rw-r--r--. 1 1001 121 5714 Nov 30 01:28 eventtypes.conf
-rw-r--r--. 1 1001 121 217 Nov 30 01:28 macros.conf
-rw-r--r--. 1 1001 121 33765 Nov 30 01:28 props.conf
-rw-r--r--. 1 1001 121 219 Nov 30 01:28 restmap.conf
-rw-r--r--. 1 1001 121 13151 Nov 30 01:28 tags.conf
-rw-r--r--. 1 1001 121 24502 Nov 30 01:28 transforms.conf
-rw-r--r--. 1 1001 121 178 Nov 30 01:28 web.conf
[root@localhost default]# cd
[root@localhost Splunk_A_nix]#

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

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

```

192.168.13.133 (root)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
14 192.168.13.133 (root) 16 192.168.13.132 (root) 18 192.168.13.134 (root)
[root@localhost default]# ll
total 120
drwxr-xr-x. 1 1001 121 494 Nov 30 01:28 app.conf
drwxr-xr-x. 1 1001 121 19690 Nov 30 01:28 data
-rw-r--r--. 1 1001 121 5714 Nov 30 01:28 eventtypes.conf
-rw-r--r--. 1 1001 121 217 Nov 30 01:28 macros.conf
-rw-r--r--. 1 1001 121 33765 Nov 30 01:28 props.conf
-rw-r--r--. 1 1001 121 219 Nov 30 01:28 restmap.conf
-rw-r--r--. 1 1001 121 13151 Nov 30 01:28 tags.conf
-rw-r--r--. 1 1001 121 24502 Nov 30 01:28 transforms.conf
-rw-r--r--. 1 1001 121 178 Nov 30 01:28 web.conf
[root@localhost default]# vi inputs.conf
[root@localhost default]# cd ..
[root@localhost Splunk_1A.nix]# mkdir local
[root@localhost Splunk_1A.nix]# cp default/inputs.conf local/
[root@localhost Splunk_1A.nix]#

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

Now we get into local directory by typing **cd local**

```

192.168.13.133 (root)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
14 192.168.13.133 (root) 16 192.168.13.132 (root) 18 192.168.13.134 (root)
[root@localhost default]# ll
total 120
drwxr-xr-x. 1 1001 121 494 Nov 30 01:28 app.conf
drwxr-xr-x. 1 1001 121 19690 Nov 30 01:28 data
-rw-r--r--. 1 1001 121 5714 Nov 30 01:28 eventtypes.conf
-rw-r--r--. 1 1001 121 217 Nov 30 01:28 macros.conf
-rw-r--r--. 1 1001 121 33765 Nov 30 01:28 props.conf
-rw-r--r--. 1 1001 121 219 Nov 30 01:28 restmap.conf
-rw-r--r--. 1 1001 121 13151 Nov 30 01:28 tags.conf
-rw-r--r--. 1 1001 121 24502 Nov 30 01:28 transforms.conf
-rw-r--r--. 1 1001 121 178 Nov 30 01:28 web.conf
[root@localhost default]# vi inputs.conf
[root@localhost default]# cd
[root@localhost Splunk_1A.nix]# mkdir local
[root@localhost Splunk_1A.nix]# cp default/inputs.conf local/
[root@localhost Splunk_1A.nix]# cd local
[root@localhost local]#

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

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.

```
[root@localhost default]# ll
total 120
-rw-r--r-- 1 1001 121 494 Nov 30 01:28 app.conf
drwxr-xr-x 3 1001 121 16 Nov 30 01:28 data
-rw-r--r-- 1 1001 121 5714 Nov 30 01:28 eventtypes.conf
-rw-r--r-- 1 1001 121 217 Nov 30 01:28 macros.conf
-rw-r--r-- 1 1001 121 33765 Nov 30 01:28 props.conf
-rw-r--r-- 1 1001 121 219 Nov 30 01:28 restmap.conf
-rw-r--r-- 1 1001 121 13151 Nov 30 01:28 tags.conf
-rw-r--r-- 1 1001 121 24502 Nov 30 01:28 transforms.conf
-rw-r--r-- 1 1001 121 178 Nov 30 01:28 web.conf
[root@localhost default]# vi inputs.conf
[root@localhost default]# cd ..
[root@localhost Splunk_TA_nix]# cp default/inputs.conf local/
[root@localhost Splunk_TA_nix]# cd local
[root@localhost local]# sed -i 's/true/false/g' inputs.conf
[root@localhost local]# sed -i 's/1/0/g' inputs.conf
[root@localhost local]#
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

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

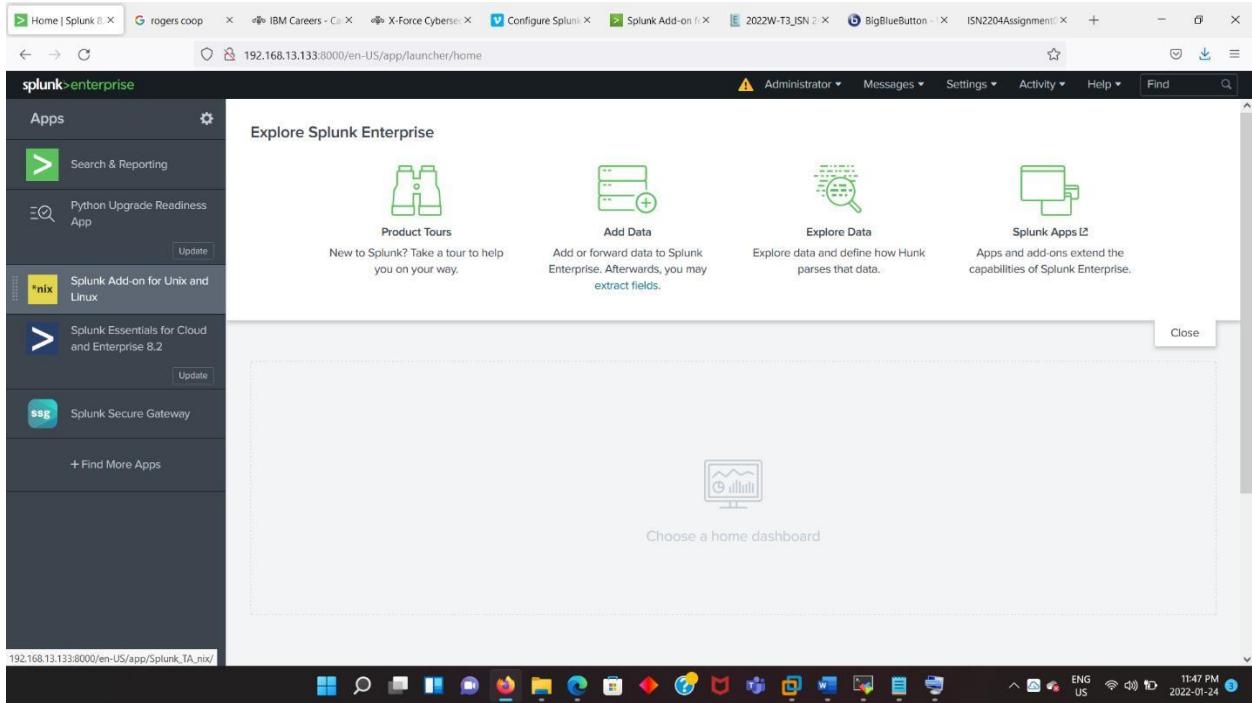
So, we type `cd ~` and then type `cd splunk/`

```
[root@localhost default]# ll
total 120
-rw-r--r-- 1 1001 121 494 Nov 30 01:28 app.conf
drwxr-xr-x 3 1001 121 16 Nov 30 01:28 data
-rw-r--r-- 1 1001 121 5714 Nov 30 01:28 eventtypes.conf
-rw-r--r-- 1 1001 121 217 Nov 30 01:28 macros.conf
-rw-r--r-- 1 1001 121 33765 Nov 30 01:28 props.conf
-rw-r--r-- 1 1001 121 219 Nov 30 01:28 restmap.conf
-rw-r--r-- 1 1001 121 13151 Nov 30 01:28 tags.conf
-rw-r--r-- 1 1001 121 24502 Nov 30 01:28 transforms.conf
-rw-r--r-- 1 1001 121 178 Nov 30 01:28 web.conf
[root@localhost default]# vi inputs.conf
[root@localhost default]# cd ..
[root@localhost Splunk_TA_nix]# mkdir local
[root@localhost Splunk_TA_nix]# cp default/inputs.conf local/
[root@localhost local]# cd local
[root@localhost local]# sed -i 's/true/false/g' inputs.conf
[root@localhost local]# sed -i 's/1/0/g' inputs.conf
[root@localhost ~]# cd splunk/
[root@localhost splunk]# cd bin
[root@localhost bin]#
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

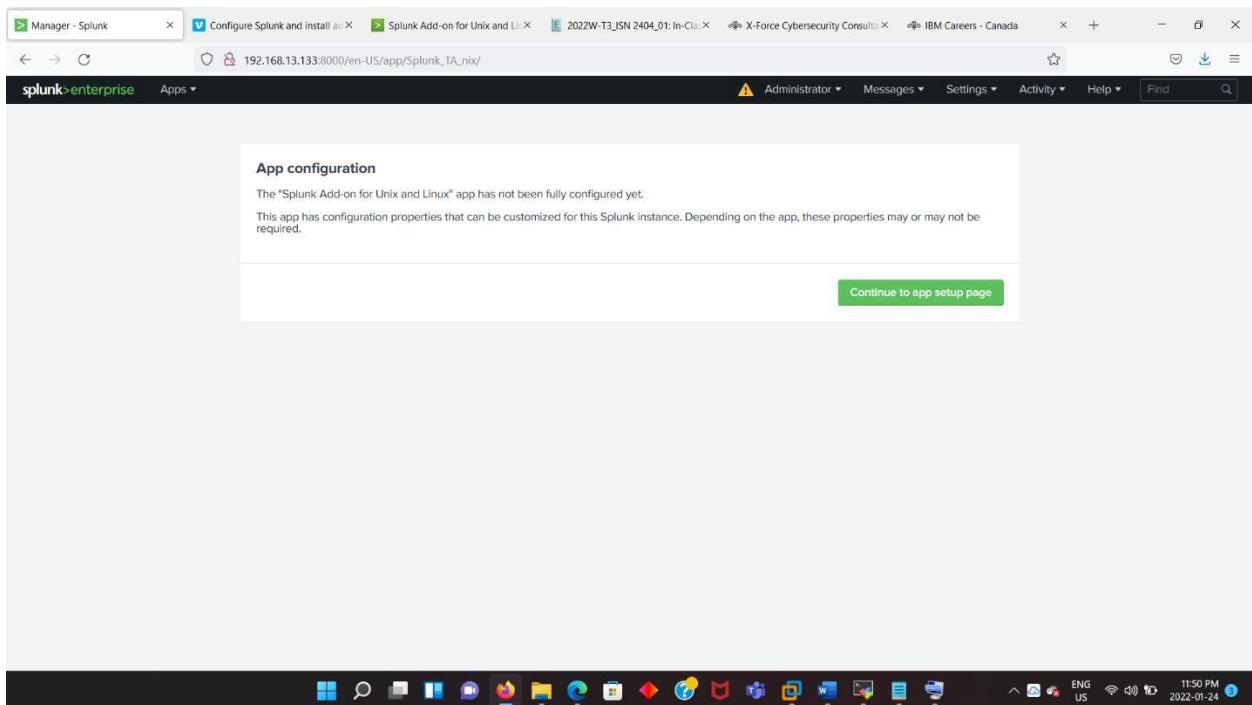
Use `cd bin` and then restart splunk by executing `./splunk restart`

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 screenshot shows the 'Splunk Add-on for Unix and Linux: Setup' page. It displays two main sections: 'File and Directory Inputs' and 'Scripted Metric Inputs'.  
**File and Directory Inputs:**  

Name	Enable (All)	Disable (All)
/etc	<input checked="" type="radio"/>	<input type="radio"/>
/home/*/.bash_history	<input checked="" type="radio"/>	<input type="radio"/>
/Library/Logs	<input checked="" type="radio"/>	<input type="radio"/>
/root/.bash_history	<input checked="" type="radio"/>	<input type="radio"/>
/var/adm	<input checked="" type="radio"/>	<input type="radio"/>
/var/log	<input checked="" type="radio"/>	<input type="radio"/>

  
**Scripted Metric Inputs:**  

Name	Enable (All)	Disable (All)	Interval (sec)	Index
cpu_metric.sh	<input checked="" type="radio"/>	<input type="radio"/>	30	Select...
df_metric.sh	<input checked="" type="radio"/>	<input type="radio"/>	300	Select...
interfaces_metric.sh	<input checked="" type="radio"/>	<input type="radio"/>	60	Select...
iostat_metric.sh	<input checked="" type="radio"/>	<input type="radio"/>	60	Select...
ps_metric.sh	<input checked="" type="radio"/>	<input type="radio"/>	30	Select...

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

The screenshot shows the 'Data Summary' table view in the Splunk search interface. The table lists various source files and their counts and last update times.

Source	Count	Last Update
/etc/GeoIP.conf	1	1/24/22 8:46:56.000 PM
/etc/GeoIP.conf.default	20	1/24/22 8:46:56.000 PM
/etc/NetworkManager/NetworkManager.conf	1	1/24/22 8:47:07.000 PM
/etc/PackageKit/CommandNotFound.conf	1	1/24/22 8:47:06.000 PM
/etc/PackageKit/PackageKit.conf	1	1/24/22 8:47:06.000 PM
/etc/PackageKit/Vendor.conf	1	1/24/22 8:47:06.000 PM
/etc/PackageKit/Yum.conf	1	1/24/22 8:47:06.000 PM
/etc/UPower/UPower.conf	1	1/24/22 8:47:07.000 PM
/etc/X11/xinit/xinput.dibus.conf	1	1/24/22 8:47:10.000 PM
/etc/X11/xinit/xinput.d/none.conf	1	1/24/22 8:47:10.000 PM

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.

```

[192.168.13.132 (root)]$ ll
total 34352
drwxr-xr-x.. 1 root root 2744 Jan 19 11:48 anaconda-ks.cfg
drwxr-xr-x.. 2 root root 6 Jan 19 20:23 Desktop
drwxr-xr-x.. 2 root root 6 Jan 19 20:23 Documents
drwxr-xr-x.. 1 root root 2916 Jan 19 19:50 initial-setup-ks.cfg
drwxr-xr-x.. 2 root root 6 Jan 19 20:23 Downloads
drwxr-xr-x.. 1 root root 2035 Jan 19 11:48 original-ks.cfg
drwxr-xr-x.. 2 root root 6 Jan 19 20:23 Pictures
drwxr-xr-x.. 2 root root 6 Jan 19 20:23 Public
drwxr-xr-x.. 2 root root 6 Jan 19 20:23 Videos
drwxr-xr-x.. 1 root root 118360 Jan 24 22:03 splunk-add-on-for-unix-and-linux_840.tgz
drwxr-xr-x.. 10 10777 10777 246 Jan 21 13:03 splunkforwarder
drwxr-xr-x.. 1 root root 35038896 Dec 21 16:29 splunkforwarder-8.2.4-87e2dda940d1-Linux-x86_64.tgz
drwxr-xr-x.. 2 root root 6 Jan 19 20:23 Templates
drwxr-xr-x.. 1 root root 4 Jan 19 22:29 test
drwxr-xr-x.. 2 root root 6 Jan 19 20:23 Videos
[192.168.13.132 (root)]$ tar -xvf splunk-add-on-for-unix-and-linux_840.tgz

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

Now move the splunk \_TA\_nix to splunkforwarder/etc/apps

```

[192.168.13.132 (root)]$ ll
total 34352
drwxr-xr-x.. 1 root root 2744 Jan 19 11:48 anaconda-ks.cfg
drwxr-xr-x.. 2 root root 6 Jan 19 20:23 Desktop
drwxr-xr-x.. 2 root root 6 Jan 19 20:23 Documents
drwxr-xr-x.. 1 root root 2916 Jan 19 19:50 initial-setup-ks.cfg
drwxr-xr-x.. 2 root root 6 Jan 19 20:23 Downloads
drwxr-xr-x.. 1 root root 2035 Jan 19 11:48 original-ks.cfg
drwxr-xr-x.. 2 root root 6 Jan 19 20:23 Pictures
drwxr-xr-x.. 2 root root 6 Jan 19 20:23 Public
drwxr-xr-x.. 2 root root 6 Jan 19 20:23 Videos
drwxr-xr-x.. 1 root root 118360 Jan 24 22:03 splunk-add-on-for-unix-and-linux_840.tgz
drwxr-xr-x.. 10 10777 10777 246 Jan 21 13:03 splunkforwarder
drwxr-xr-x.. 11 1001 121 206 Nov 30 01:28 Splunk_TA_nix
drwxr-xr-x.. 2 root root 6 Jan 19 20:23 Templates
drwxr-xr-x.. 1 root root 4 Jan 19 22:29 test
drwxr-xr-x.. 2 root root 6 Jan 19 20:23 Videos
[192.168.13.132 (root)]$ mv Splunk_TA_nix splunk forwarder/etc/apps/
mv: target 'forwarder/etc/apps/' is not a directory
[192.168.13.132 (root)]$ mv Splunk_TA_nix splunkforwarder/etc/apps/
[192.168.13.132 (root)]$ 

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

Move to the folder splunkforwarder/etc/apps

```

[192.168.13.132 (root)]# ll
total 34352
drwxr-xr-x  1 root root 2744 Jan 11 11:48 anaconda-ks.cfg
drwxr-xr-x  2 root root 6 Jan 19 20:23 Desktop
drwxr-xr-x  2 root root 6 Jan 19 20:23 Documents
-rw-r--r--  1 root root 2916 Jan 19 19:50 initial-setup-ks.cfg
drwxr-xr-x  2 root root 6 Jan 19 20:23 Music
drwxr-xr-x  2 root root 6 Jan 19 20:23 Pictures
drwxr-xr-x  2 root root 6 Jan 19 20:23 Public
drwxr-xr-x  2 root root 6 Jan 19 20:23 Splunk
drwxr-xr-x  1 root root 118360 Jan 24 22:03 splunk-addon-for-unix-and-linux_840.tgz
drwxr-xr-x  10 10777 10777 246 Jan 21 13:03 splunkforwarder
-rw-r--r--  1 root root 3503896 Dec 21 16:29 splunkforwarder-8.2.4-87e2dd940d1-Linux-x86_64.tgz
drwxr-xr-x  11 1001 121 206 Nov 30 01:28 Splunk_TA_nix
drwxr-xr-x  2 root root 6 Jan 19 20:23 Templates
-rw-r--r--  1 root root 4 Jan 19 22:29 test
drwxr-xr-x  2 root root 6 Jan 19 20:23 Videos
[root@localhost ~]# mv Splunk_TA_nix splunkforwarder/etc/apps/
mv: target 'forwarder/etc/apps/' is not a directory
[root@localhost ~]# mv Splunk_TA_nix splunkforwarder/etc/apps/
[root@localhost ~]# cd splunkforwarder/etc/apps/
[root@localhost 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.

```

[192.168.13.132 (root)]# ll
total 9
drwxr-xr-x  2 root root 6 Jan 19 20:23 Pictures
drwxr-xr-x  2 root root 0 Jan 19 20:23 Public
drwxr-xr-x  1 root root 118360 Jan 24 22:03 splunk-addon-for-unix-and-linux_840.tgz
drwxr-xr-x  10 10777 10777 246 Jan 21 13:03 splunkforwarder
-rw-r--r--  1 root root 3503896 Dec 21 16:29 splunkforwarder-8.2.4-87e2dd940d1-Linux-x86_64.tgz
drwxr-xr-x  11 1001 121 206 Nov 30 01:28 Splunk_TA_nix
drwxr-xr-x  2 root root 6 Jan 19 20:23 Templates
-rw-r--r--  1 root root 4 Jan 19 22:29 test
drwxr-xr-x  2 root root 6 Jan 19 20:23 Videos
[root@localhost ~]# mv Splunk_TA_nix splunkforwarder/etc/apps/
mv: overwrite 'splunkforwarder/etc/apps/Splunk_TA_nix'? c
[root@localhost ~]# cd splunkforwarder/etc/apps/
[root@localhost apps]# q!
bash: q!: command not found...
[root@localhost apps]#
[root@localhost apps]#
[root@localhost apps]# ll
total 0
drwxr-xr-x  4 10777 10777 32 Dec 15 14:13 introspection_generator_addon
drwxr-xr-x  5 10777 10777 46 Dec 15 14:13 journald_input
drwxr-xr-x  5 10777 10777 58 Jan 20 15:47 learned
drwxr-xr-x  5 10777 10777 59 Jan 21 12:55 search
drwxr-xr-x  3 10777 10777 21 Dec 15 14:13 splunk_httpinput
drwxr-xr-x  3 10777 10777 21 Dec 15 14:13 splunk_internal_metrics
drwxr-xr-x  11 1001 121 206 Nov 30 01:28 Splunk_TA_nix
drwxr-xr-x  4 10777 10777 37 Dec 15 14:13 SplunkUniversalForwarder
[root@localhost apps]# cd Splunk_TA_nix
[root@localhost Splunk_TA_nix]# ll
total 24
-rw-r--r-- 1 1001 121 1552 Nov 30 01:28 app.manifest
drwxr-xr-x 3 1001 121 30 Nov 30 01:28 appserver
drwxr-xr-x 2 1001 121 4996 Nov 30 01:28 bin
drwxr-xr-x 3 1001 121 189 Nov 30 01:28 default
drwxr-xr-x 2 1001 121 30 Nov 30 01:28 lib
drwxr-xr-x 2 1001 121 64 Nov 30 01:28 LICENSES
drwxr-xr-x 2 1001 121 4996 Nov 30 01:28 lookups
drwxr-xr-x 2 1001 121 26 Nov 30 01:28 metadata
drwxr-xr-x 2 1001 121 31 Nov 30 01:28 README
-rw-r--r-- 1 1001 121 164 Nov 30 01:28 README.txt
drwxr-xr-x 2 1001 121 139 Nov 30 01:28 static
-rw-r--r-- 1 1001 121 123 Nov 30 01:28 THIRDPARTY
-rw-r--r-- 1 1001 121 11 Nov 30 01:28 VERSION
[root@localhost Splunk_TA_nix]#

```

Now we see the input file.

```

[22 192.168.13.133 (root)]$ mkdir local
[22 192.168.13.133 (root)]$ cp default/inputs.conf local/
[22 192.168.13.133 (root)]$ cd local/
[22 192.168.13.133 (root)]$ ll
total 8
-rw-r--r-- 1 root root 5714 Jan 24 22:57 inputs.conf
[22 192.168.13.133 (root)]$ 

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

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.

```

[22 192.168.13.133 (root)]$ mkdir local
[22 192.168.13.133 (root)]$ cp default/inputs.conf local/
[22 192.168.13.133 (root)]$ cd local/
[22 192.168.13.133 (root)]$ sed -i 's/true/false/g' inputs.conf
[22 192.168.13.133 (root)]$ ll
total 8
-rw-r--r-- 1 root root 5714 Jan 24 22:57 inputs.conf
[22 192.168.13.133 (root)]$ 

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

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

```

## SPDX-FileCopyrightText: 2020 Splunk, Inc. <sales@splunk.com>
## SPDX-License-Identifier: LicenseRef-Splunk-8-2020
#
#[script://bin/vmstat_metric.sh]
sourcetype = vmstat_metric
source = vmstat
interval = 60
disabled = 0

#[script://bin/iostat_metric.sh]
sourcetype = iostat_metric
source = iostat
interval = 60
disabled = 0

#[script://bin/ps_metric.sh]
sourcetype = ps_metric
source = ps
interval = 30
disabled = 0

#[script://bin/df_metric.sh]
sourcetype = df_metric
source = df
interval = 300
disabled = 0

#[script://bin/interfaces_metric.sh]
sourcetype = interfaces_metric
source = interfaces
interval = 60
disabled = 0

#[script://bin/cpu_metric.sh]
sourcetype = cpu_metric
source = cpu
interval = 30
disabled = 0

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

```

# May require Splunk forwarder to run as root on some platforms.
#[script://bin/service.sh]
disabled = false
interval = 3600
source = Unix:Service
sourcetype = Unix:Service

# Currently only supports SunOS, Linux, OSX.
# May require Splunk forwarder to run as root on some platforms.
#[script://bin/sshdchecker.sh]
disabled = false
interval = 3600
source = Unix:SSHConfig
sourcetype = Unix:SSHConfig

# Currently only supports Linux, OSX.
# May require Splunk forwarder to run as root on some platforms.
#[script://bin/update.sh]
disabled = false
interval = 86400
source = Unix:Update
sourcetype = Unix:Update

#[script://bin/uptime.sh]
disabled = false
interval = 86400
source = Unix:Uptime
sourcetype = Unix:Uptime

#[script://bin/version.sh]
disabled = false
interval = 86400
source = Unix:Version
sourcetype = Unix:Version

# This script may need to be modified to point to the VSFTPD configuration file.
#[script://bin/vsftpdChecker.sh]
disabled = false
interval = 86400
source = Unix:VSFTPDConfig
sourcetype = Unix:VSFTPDConfig

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

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

```

[22 192.168.13.132 (root)] Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiEtc Tunneling Packages Settings Help
Quick connect...
[22 192.168.13.132 (root)] [27 192.168.13.132 (root)] [29 192.168.13.132 (root)] [24 192.168.13.134 (root)]
[root@localhost Splunk_TA.nix]# mkdir local
[root@localhost Splunk_TA.nix]# cp default/inputs.conf local/
[root@localhost Splunk_TA.nix]# cd local/
[root@localhost local]# ll
total 8
-rw-r--r-- 1 root root 5714 Jan 24 22:57 inputs.conf
[root@localhost local]# sed -i 's/true/false/g' inputs.conf
sed: -e expression #1, char 14: unknown option to `s'
[root@localhost local]# sed -i 's/true/false/g' inputs.conf
[root@localhost local]# sed -i 's/l/b/g' inputs.conf
[root@localhost local]# vi inputs.conf
[root@localhost local]# cd ~
[root@localhost ~]# ll
total 34352
-rw-r--r-- 1 root root 2744 Jan 19 11:48 anaconda-ks.cfg
drwxr-xr-x 2 root root 6 Jan 19 20:23 Desktop
drwxr-xr-x 2 root root 6 Jan 19 20:23 Documents
drwxr-xr-x 2 root root 6 Jan 19 20:23 Downloads
-rw-r--r-- 1 root root 2916 Jan 19 19:50 initial-setup-ks.cfg
drwxr-xr-x 2 root root 6 Jan 19 20:23 Music
-rw-r----- 1 root root 2035 Jan 19 11:48 original-ks.cfg
drwxr-xr-x 2 root root 6 Jan 19 20:23 Pictures
drwxr-xr-x 2 root root 6 Jan 19 20:23 Public
-rw-r--r-- 1 root root 118360 Jan 24 22:03 splunk-add-on-for-unix-and-linux_840.tgz
drwxr-xr-x 10 10777 10777 246 Jan 21 13:03 splunkforwarder
-rw-r--r-- 1 root root 35038990 Dec 21 16:29 splunkforwarder-8.2.4-87e2dd940d1-Linux-x86_64.tgz
drwxr-xr-x 11 1081 121 206 Nov 30 01:28 Splunk_TA.nix
drwxr-xr-x 2 root root 6 Jan 19 20:23 Templates
-rw-r--r-- 1 root root 4 Jan 19 22:29 test
drwxr-xr-x 2 root root 6 Jan 19 20:23 Videos
[root@localhost ~]#

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

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

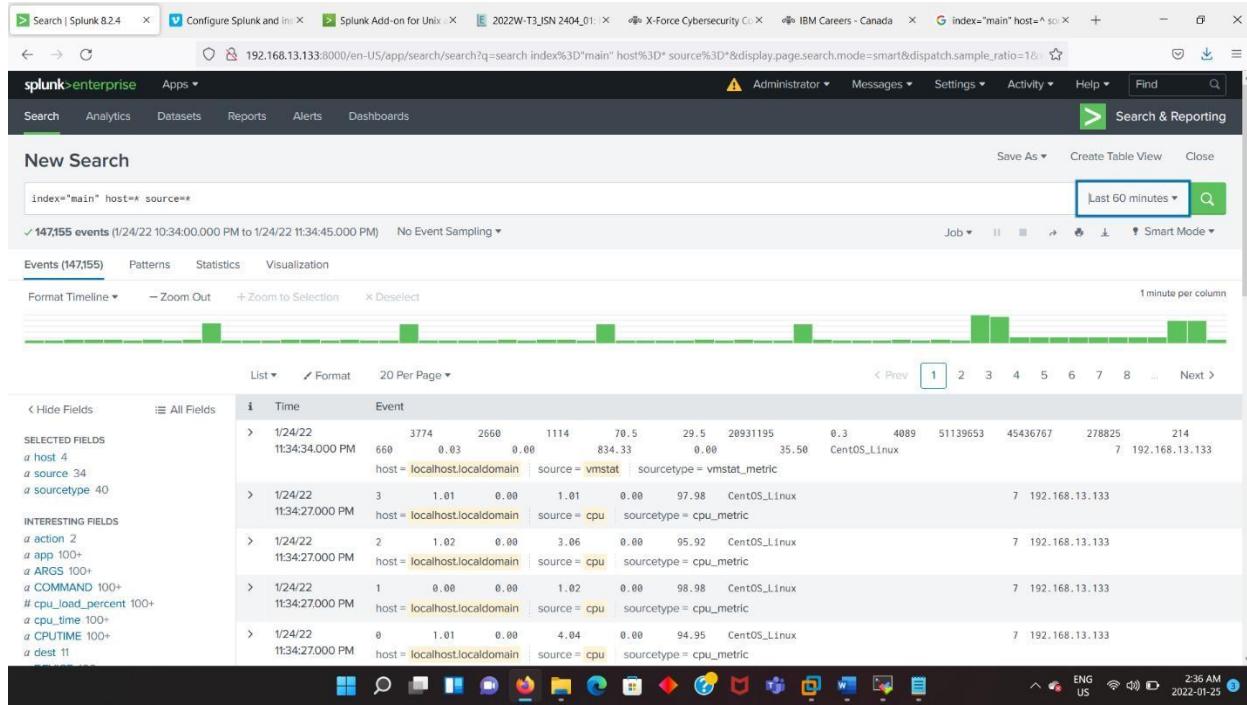
```

[22 192.168.13.132 (root)] Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiEtc Tunneling Packages Settings Help
Quick connect...
[22 192.168.13.132 (root)] [27 192.168.13.132 (root)] [29 192.168.13.132 (root)] [24 192.168.13.134 (root)]
[root@localhost Splunk_TA.nix]# mkdir local
[root@localhost Splunk_TA.nix]# cp default/inputs.conf local/
[root@localhost Splunk_TA.nix]# cd local/
[root@localhost local]# ll
total 8
-rw-r--r-- 1 root root 5714 Jan 24 22:57 inputs.conf
[root@localhost local]# sed -i 's/true/false/g' inputs.conf
sed: -e expression #1, char 14: unknown option to `s'
[root@localhost local]# sed -i 's/true/false/g' inputs.conf
[root@localhost local]# sed -i 's/l/b/g' inputs.conf
[root@localhost local]# vi inputs.conf
[root@localhost local]# cd ~
[root@localhost ~]# ll
total 34352
-rw-r--r-- 1 root root 2744 Jan 19 11:48 anaconda-ks.cfg
drwxr-xr-x 2 root root 6 Jan 19 20:23 Desktop
drwxr-xr-x 2 root root 6 Jan 19 20:23 Documents
drwxr-xr-x 2 root root 6 Jan 19 20:23 Downloads
-rw-r--r-- 1 root root 2916 Jan 19 19:50 initial-setup-ks.cfg
drwxr-xr-x 2 root root 6 Jan 19 20:23 Music
-rw-r----- 1 root root 2035 Jan 19 11:48 original-ks.cfg
drwxr-xr-x 2 root root 6 Jan 19 20:23 Pictures
drwxr-xr-x 2 root root 6 Jan 19 20:23 Public
-rw-r--r-- 1 root root 118360 Jan 24 22:03 splunk-add-on-for-unix-and-linux_840.tgz
drwxr-xr-x 10 10777 10777 246 Jan 21 13:03 splunkforwarder
-rw-r--r-- 1 root root 35038990 Dec 21 16:29 splunkforwarder-8.2.4-87e2dd940d1-Linux-x86_64.tgz
drwxr-xr-x 11 1081 121 206 Nov 30 01:28 Splunk_TA.nix
drwxr-xr-x 2 root root 6 Jan 19 20:23 Templates
-rw-r--r-- 1 root root 4 Jan 19 22:29 test
drwxr-xr-x 2 root root 6 Jan 19 20:23 Videos
[root@localhost ~]# cd splunkforwarder/bin
[root@localhost bin]# ./splunk restart

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

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.

```

[root@localhost ~]# ll
total 0
[root@localhost ~]# mv Splunk_TA_nix splunkforwarder/etc/apps/
[root@localhost ~]# cd ^C
[root@localhost apps]# ll
total 0
drwxr-xr-x. 4 10777 10777 32 Dec 15 14:13 introspection_generator_addon
drwxr-xr-x. 5 10777 10777 46 Dec 15 14:13 journald_input
drwxr-xr-x. 5 10777 10777 50 Dec 20 15:45 logstash
drwxr-xr-x. 5 10777 10777 50 Jan 21 12:55 search
drwxr-xr-x. 3 10777 10777 21 Dec 15 14:13 splunk_httpinput
drwxr-xr-x. 3 10777 10777 21 Dec 15 14:13 splunk_internal_metrics
drwxr-xr-x. 11 1081 121 206 Nov 30 01:28 Splunk_TA_nix
drwxr-xr-x. 4 10777 10777 37 Dec 15 14:13 SplunkUniversalForwarder

```

Now move the file to `Splunk_TA_nix`

```

[22] 192.168.13.134 (root)
[24] 192.168.13.134 (root)

[root@localhost ~]# ll
total 34352
drwxr-xr-x. 1 root root 2744 Jan 19 11:48 anaconda-ks.cfg
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Desktop
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Documents
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Downloads
-rw-r--r--. 1 root root 2916 Jan 19 19:50 initial-setup-ks.cfg
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Music
-rw-----. 1 root root 2035 Jan 19 11:48 original-ks.cfg
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Pictures
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Public
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Templates
-rw-r--r--. 1 root root 118360 Jan 24 22:05 splunk-addon-for-unix-and-linux_840.tgz
drwxr-xr-x. 10 16777 16777 246 Jan 24 13:04 splunkforwarder
-rw-r--r--. 1 root root 35038896 Dec 24 16:29 splunkforwarder-8.2.4-87e2dd940d1-Linux-x86_64.tgz
drwxr-xr-x. 11 1681 121 286 Nov 30 01:28 Splunk_TA_nix
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Templates
-rw-r--r--. 1 root root 4 Jan 19 22:29 test
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Videos
[root@localhost ~]# mv Splunk_TA_nix splunkforwarder/etc/apps/
[root@localhost ~]# cd ..
[root@localhost ~]# cd splunkforwarder/etc/apps/
[root@localhost apps]# ll
total 0
drwxr-xr-x. 4 16777 16777 32 Dec 15 14:13 introspection_generator_addon
drwxr-xr-x. 5 16777 16777 46 Dec 15 14:13 journald_input
drwxr-xr-x. 5 16777 16777 58 Jan 29 15:45 learned
drwxr-xr-x. 5 16777 16777 58 Jan 21 12:55 search
drwxr-xr-x. 3 16777 16777 21 Dec 15 14:13 splunk_httpinput
drwxr-xr-x. 3 16777 16777 24 Dec 15 14:13 splunk_internal_metrics
drwxr-xr-x. 11 1681 121 286 Nov 30 01:28 Splunk_TA_nix
drwxr-xr-x. 4 16777 16777 37 Dec 15 14:13 SplunkUniversalForwarder
[root@localhost apps]# cd Splunk_TA_nix
[root@localhost Splunk_TA_nix]# ll

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

Now type pwd and then copy the path /root/splunkforwarder/etc/apps/Splunk\_TA\_nix

Create a new local; directory as shown below.

```

[22] 192.168.13.134 (root)
[24] 192.168.13.134 (root)

[root@localhost ~]# ll
total 34352
drwxr-xr-x. 1 root root 2744 Jan 19 11:48 anaconda-ks.cfg
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Desktop
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Documents
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Downloads
-rw-r--r--. 1 root root 2916 Jan 19 19:50 initial-setup-ks.cfg
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Music
-rw-----. 1 root root 2035 Jan 19 11:48 original-ks.cfg
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Pictures
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Public
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Templates
-rw-r--r--. 1 root root 118360 Jan 24 22:05 splunk-addon-for-unix-and-linux_840.tgz
drwxr-xr-x. 10 16777 16777 246 Jan 24 13:04 splunkforwarder
-rw-r--r--. 1 root root 35038896 Dec 24 16:29 splunkforwarder-8.2.4-87e2dd940d1-Linux-x86_64.tgz
drwxr-xr-x. 11 1681 121 286 Nov 30 01:28 Splunk_TA_nix
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Templates
-rw-r--r--. 1 root root 4 Jan 19 22:29 test
drwxr-xr-x. 2 root root 6 Jan 19 20:23 Videos
[root@localhost ~]# mv Splunk_TA_nix splunkforwarder/etc/apps/
[root@localhost ~]# cd ..
[root@localhost ~]# cd splunkforwarder/etc/apps/
[root@localhost apps]# ll
total 0
drwxr-xr-x. 4 16777 16777 32 Dec 15 14:13 introspection_generator_addon
drwxr-xr-x. 5 16777 16777 46 Dec 15 14:13 journald_input
drwxr-xr-x. 5 16777 16777 58 Jan 29 15:45 learned
drwxr-xr-x. 5 16777 16777 58 Jan 21 12:55 search
drwxr-xr-x. 3 16777 16777 21 Dec 15 14:13 splunk_httpinput
drwxr-xr-x. 3 16777 16777 24 Dec 15 14:13 splunk_internal_metrics
drwxr-xr-x. 11 1681 121 286 Nov 30 01:28 Splunk_TA_nix
drwxr-xr-x. 4 16777 16777 37 Dec 15 14:13 SplunkUniversalForwarder
[root@localhost apps]# cd Splunk_TA_nix
[root@localhost Splunk_TA_nix]# mkdir local
[root@localhost Splunk_TA_nix]# pwd

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

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

```

drwxr-xr-x . 11 1001 121 206 Nov 30 01:28 Splunk_TA_nix
drwxr-xr-x . 2 root root 6 Jan 19 20:23 templates
drwxr-xr-x . 1 root root 4 Jan 19 22:20 test
drwxr-xr-x . 2 root root 6 Jan 19 20:23 Videos
[root@localhost ~]# mv Splunk_TA_nix splunkforwarder/etc/apps/
[root@localhost ~]# cd "C"
[root@localhost ~]# cd splunkforwarder/etc/apps/
[root@localhost apps]# ll
total 0
drwxr-xr-x . 4 10777 10777 32 Dec 15 14:13 introspection_generator_addon
drwxr-xr-x . 5 10777 10777 46 Dec 15 14:13 journald_input
drwxr-xr-x . 5 10777 10777 58 Jan 20 15:45 learned
drwxr-xr-x . 5 10777 10777 58 Jan 21 12:55 search
drwxr-xr-x . 3 10777 10777 21 Dec 15 14:13 splunk_httpinput
drwxr-xr-x . 3 10777 10777 21 Dec 15 14:13 splunk_internal_metrics
drwxr-xr-x . 11 1001 121 206 Nov 30 01:28 Splunk_TA_nix
drwxr-xr-x . 4 10777 10777 37 Dec 15 14:13 SplunkUniversalForwarder
[root@localhost apps]# cd Splunk_TA_nix
[root@localhost Splunk_TA_nix]# pwd
/root/splunkforwarder/etc/apps/Splunk_TA_nix
[root@localhost Splunk_TA_nix]# mkdir local
[root@localhost local]# cd ..
[root@localhost Splunk_TA_nix]# ll
total 24
-rw-r--r-- . 1 1001 121 1552 Nov 30 01:28 app.manifest
drwxr-xr-x . 3 1001 121 20 Nov 30 01:28 appserver
drwxr-xr-x . 2 1001 121 4096 Nov 30 01:28 bin
drwxr-xr-x . 1 1001 121 189 Nov 30 01:28 default
drwxr-xr-x . 2 1001 121 38 Nov 30 01:28 lib
drwxr-xr-x . 2 1001 121 64 Nov 30 01:28 LICENSES
drwxr-xr-x . 2 1001 121 64 Nov 30 01:28 lookups
drwxr-xr-x . 2 1001 121 4096 Nov 30 01:28 metadata
drwxr-xr-x . 2 1001 121 26 Nov 30 01:28 README
drwxr-xr-x . 2 1001 121 31 Nov 30 01:28 README.txt
drwxr-xr-x . 2 1001 121 139 Nov 30 01:28 static
drwxr-xr-x . 1 1001 121 123 Nov 30 01:28 THIRDOPARTY
-rw-r--r-- . 1 1001 121 11 Nov 30 01:28 VERSION
[root@localhost Splunk_TA_nix]#

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

Copy default input file to local.conf

default//inputs.conf local/

Go to local directory and list the input file.

```

drwxr-xr-x . 4 10777 10777 32 Dec 15 14:13 introspection_generator_addon
drwxr-xr-x . 5 10777 10777 46 Dec 15 14:13 journald_input
drwxr-xr-x . 5 10777 10777 58 Jan 20 15:45 learned
drwxr-xr-x . 5 10777 10777 58 Jan 21 12:55 search
drwxr-xr-x . 3 10777 10777 21 Dec 15 14:13 splunk_httpinput
drwxr-xr-x . 3 10777 10777 21 Dec 15 14:13 splunk_internal_metrics
drwxr-xr-x . 11 1001 121 206 Nov 30 01:28 Splunk_TA_nix
drwxr-xr-x . 4 10777 10777 37 Dec 15 14:13 SplunkUniversalForwarder
[root@localhost apps]# cd Splunk_TA_nix
[root@localhost Splunk_TA_nix]# pwd
/root/splunkforwarder/etc/apps/Splunk_TA_nix
[root@localhost Splunk_TA_nix]# mkdir local
[root@localhost local]# cd ..
[root@localhost Splunk_TA_nix]# ll
total 24
-rw-r--r-- . 1 1001 121 1552 Nov 30 01:28 app.manifest
drwxr-xr-x . 3 1001 121 20 Nov 30 01:28 appserver
drwxr-xr-x . 2 1001 121 4096 Nov 30 01:28 bin
drwxr-xr-x . 3 1001 121 189 Nov 30 01:28 default
drwxr-xr-x . 2 1001 121 30 Nov 30 01:28 lib
drwxr-xr-x . 2 1001 121 64 Nov 30 01:28 LICENSES
drwxr-xr-x . 2 1001 121 64 Nov 30 01:28 lookups
drwxr-xr-x . 2 1001 121 26 Nov 30 01:28 metadata
drwxr-xr-x . 2 1001 121 31 Nov 30 01:28 README
drwxr-xr-x . 2 1001 121 139 Nov 30 01:28 README.txt
drwxr-xr-x . 1 1001 121 123 Nov 30 01:28 THIRDOPARTY
-rw-r--r-- . 1 1001 121 11 Nov 30 01:28 VERSION
[root@localhost Splunk_TA_nix]# cp default//inputs.conf local/
[root@localhost Splunk_TA_nix]# cd local
cp: overwrite 'local/inputs.conf'?
bash: cd: local: No such file or directory
[root@localhost Splunk_TA_nix]# cd local
[root@localhost local]# ll
total 8
-rw-r--r-- . 1 root root 5714 Jan 25 00:06 inputs.conf
[root@localhost local]#

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

Now execute the below commands.

`sed -i 's/true/false/g' inputs.conf , Sed -i 's/1/0/g' inputs.conf`

```

22. 192.168.13.134 (root)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
22. 192.168.13.134 (root) 27. 192.168.13.132 (root) 24. 192.168.13.134 (root)
drwxr-xr-x . 3 10777 10777 24 Dec 15 14:13 splunk_httpinput
drwxr-xr-x . 2 10777 10777 23 Dec 15 14:13 Splunk_TA_nix
drwxr-xr-x . 11 1001 1021 206 Nov 30 01:28 Splunk_TA_nix
drwxr-xr-x . 4 10777 10777 37 Dec 15 14:13 SplunkUniversalForwarder
[root@localhost apps]# cd Splunk_TA_nix
[root@localhost Splunk_TA_nix]# pwd
[root@localhost Splunk_TA_nix]# mkdir local
[root@localhost Splunk_TA_nix]# cd local
[root@localhost local]# cd ..
[root@localhost Splunk_TA.nix]# ll
total 24
-rw-r--r-- . 1 1001 121 1552 Nov 30 01:28 app.manifest
drwxr-xr-x .. 3 1001 121 20 Nov 30 01:28 appserver
drwxr-xr-x .. 2 1001 121 4096 Nov 30 01:28 bin
drwxr-xr-x .. 1 1001 121 189 Nov 30 01:28 default
drwxr-xr-x .. 2 1001 121 38 Nov 30 01:28 lib
drwxr-xr-x .. 2 1001 121 64 Nov 30 01:28 LICENSES
drwxr-xr-x .. 2 root root 6 Jan 24 23:54 local
drwxr-xr-x .. 2 1001 121 4896 Nov 30 01:28 lookups
drwxr-xr-x .. 2 1001 121 26 Nov 30 01:28 metadata
drwxr-xr-x .. 2 1001 121 31 Nov 30 01:28 README
-rw-r--r-- .. 1 1001 121 164 Nov 30 01:28 README.txt
drwxr-xr-x .. 2 1001 121 139 Nov 30 01:28 static
-rw-r--r-- .. 1 1001 121 123 Nov 30 01:28 THIRDPARTY
-rw-r--r-- .. 1 1001 121 11 Nov 30 01:28 VERSION
[root@localhost Splunk_TA.nix]# cp default/inputs.conf local/
[root@localhost Splunk_TA.nix]# cp default/inputs.conf local/
cp: overwrite 'local/inputs.conf'? [y/N]
[y/N] root@localhost local]# ll
total 8
-rw-r--r-- . 1 root root 5714 Jan 25 00:06 inputs.conf
[root@localhost local]# sed -i 's/true/false/g' inputs.conf
sed: -e expression #1, char 1: unknown command: '#'
[root@localhost local]# sed -i 's/true/false/g' inputs.conf
[root@localhost local]# sed -i 's/1/0/g' inputs.conf
[root@localhost local]# vi inputs.conf

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobatxterm.mobatek.net>

Now check the inputs file.

```

22. 192.168.13.134 (root)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
22. 192.168.13.134 (root) 27. 192.168.13.132 (root) 24. 192.168.13.134 (root)
## SPDX-FileCopyrightText: 2020 Splunk, Inc. <sales@splunk.com>
## SPDX-License-Identifier: LicenseRef-Splunk-8-2020
##
[script:///bin/vmstat_metric.sh]
sourcetype = vmstat_metric
source = vmstat
interval = 60
disabled = 0

[script:///bin/iostat_metric.sh]
sourcetype = iostat_metric
source = iostat
interval = 60
disabled = 0

[script:///bin/ps_metric.sh]
sourcetype = ps_metric
source = ps
interval = 30
disabled = 0

[script:///bin/df_metric.sh]
sourcetype = df_metric
source = df
interval = 300
disabled = 0

[script:///bin/interfaces_metric.sh]
sourcetype = interfaces_metric
source = interfaces
interval = 60
disabled = 0

[script:///bin/cpu_metric.sh]
sourcetype = cpu_metric
source = cpu
"inputs.conf" 270L, 5725C

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobatxterm.mobatek.net>

```

192.168.13.134 (root)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
22 192.168.13.133 (root) 24 192.168.13.132 (root)
disabled = false
interval = 3600
source = UnixService
sourcetype = Unix:Service
# Currently only supports SunOS, Linux, OSX.
# May require Splunk forwarder to run as root on some platforms.
[script://bin/shhdchecker.sh]
disabled = false
interval = 3600
source = Unix:SSHConfig
sourcetype = Unix:SSHConfig
# Currently only supports Linux, OSX.
# May require Splunk forwarder to run as root on some platforms.
[script://bin/update.sh]
disabled = false
interval = 86400
source = Unix:Uptime
sourcetype = Unix:Uptime
[script://bin/uptime.sh]
disabled = false
interval = 86400
source = Unix:Uptime
sourcetype = Unix:Uptime
[script://bin/version.sh]
disabled = false
interval = 86400
source = Unix:Version
sourcetype = Unix:Version
# This script may need to be modified to point to the VSFTPD configuration file.
[script://bin/vsftpdchecker.sh]
disabled = false
interval = 86400
source = Unix:VSFTPDConfig
sourcetype = Unix:VSFTPDConfig
Follow terminal folder
localhost.localdomain 0% 0.82 GB / 3.69 GB 0.01 Mb/s 0.00 Mb/s 32 hours root root root root /: 15% /boot: 51%
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
ENG US 3:18 AM 2022-01-25

```

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

```

192.168.13.134 (root)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
22 192.168.13.133 (root) 24 192.168.13.132 (root)
drwxr-xr-x 2 1001 121 31 Nov 30 01:28 README
-rw-r--r-- 1 1001 121 164 Nov 30 01:28 README.txt
drwxr-xr-x 2 1001 121 139 Nov 30 01:28 static
-rw-r--r-- 1 1001 121 123 Nov 30 01:28 THIRDPARTY
-rw-r--r-- 1 1001 121 11 Nov 30 01:28 VERSION
[root@localhost Splunk_TA_nix]# cp default/inputs.conf local/
[root@localhost Splunk_TA_nix]# cp default/inputs.conf local/
cp: overwrite 'local/inputs.conf'?
[root@localhost Splunk_TA_nix]# cd local
[bash: cd: local: No such file or directory
[root@localhost Splunk_TA_nix]# cd local
[root@localhost local]# ll
total 8
-rw-r--r-- 1 root root 5714 Jan 25 00:06 inputs.conf
[root@localhost local]# sed -i 's>true/false/g' inputs.conf
sed: -e expression #1, char 1: unknown command: '#'
[root@localhost local]# sed -i 's>true/false/g' inputs.conf
[root@localhost local]# sed -i 's!/l/g' inputs.conf
[root@localhost local]# vi inputs.conf
[root@localhost local]# cd ~
[root@localhost ~]# ll
total 34352
-rw-r--r-- 1 root root 2744 Jan 19 11:48 anaconda-ks.cfg
drwxr-xr-x 2 root root 6 Jan 19 20:23 Desktop
drwxr-xr-x 2 root root 6 Jan 19 20:23 Documents
drwxr-xr-x 2 root root 6 Jan 19 20:23 Downloads
drwxr-xr-x 2 root root 2916 Jan 19 19:50 initial-setup-ks.cfg
drwxr-xr-x 2 root root 6 Jan 19 20:23 Music
-rw----- 1 root root 2035 Jan 19 11:48 original-ks.cfg
drwxr-xr-x 2 root root 6 Jan 19 20:23 Pictures
drwxr-xr-x 2 root root 6 Jan 19 20:23 Public
drwxr-xr-x 2 root root 0 Jan 19 20:23 Videos
-rw-r--r-- 1 root root 118360 Jan 24 22:05 splunk-add-on-for-unix-and-linux_840.tgz
drwxr-xr-x 10 16771 16771 246 Jan 21 13:04 splunkforwarder
-rw-r--r-- 1 root root 35038896 Dec 21 16:29 splunkforwarder-8.2.4-87e2ddda940d1-Linux-x86_64.tgz
-rw-r--r-- 2 root root 0 Jan 19 20:23 templates
-rw-r--r-- 1 root root 4 Jan 19 22:29 test
drwxr-xr-x 2 root root 0 Jan 19 20:23 Videos
[root@localhost ~]# cd splunkforwarder
[root@localhost splunkforwarder]# cd bin
[root@localhost bin]#

```

Now restart splunk by using ./splunk restart

The screenshot shows a MobaXterm window with multiple tabs open. The current tab is titled '27.192.168.13.132 (root)'. The terminal session displays the following commands and output:

```
root@localhost ~# cd splunkforwarder
[root@localhost splunkforwarder]# cd bin
[root@localhost bin]# ./splunk restart
Unit SplunkForwarder.service could not be found.
Unit SplunkForwarder.service could not be found.
Stopping splunkd...
Shutting down... Please wait, as this may take a few minutes.
[ OK ]
Stopping splunk helpers...
[ OK ]
Done.
Unit SplunkForwarder.service could not be found.

Splunk> 4TW

Checking prerequisites...
Checking mgmt port [8089]: open
Checking conf files for problems...
Done
Checking default conf files for edits...
Validating installed files against hashes from '/root/splunkforwarder/splunkforwarder-8.2.4-87e2dda940d1-linux-x86_64-manifest'
All installed files intact.
Done

All preliminary checks passed.

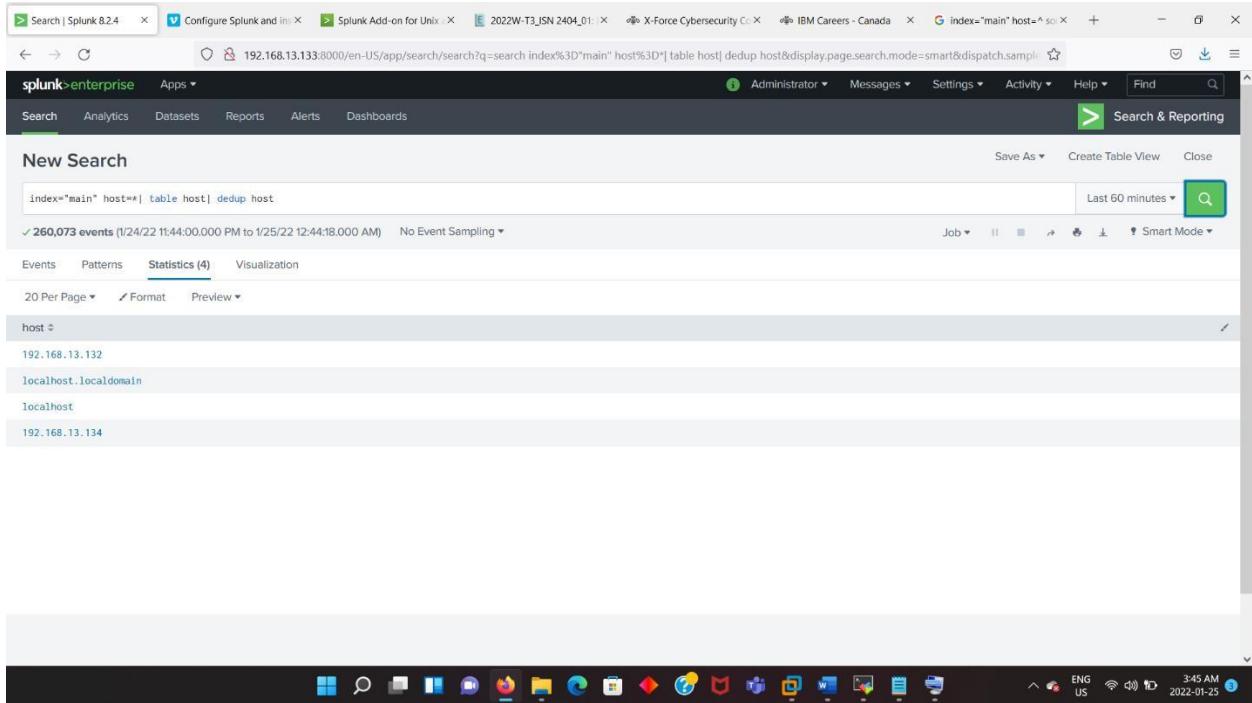
Starting splunk server daemon (splunkd)...
Done
[ OK ]
```

The terminal window also shows the system status at the bottom, including CPU usage (0%), memory (0.87 GB / 3.69 GB), network (0.10 Mb/s), disk (32 hours), and battery (15% / boot: 51%).

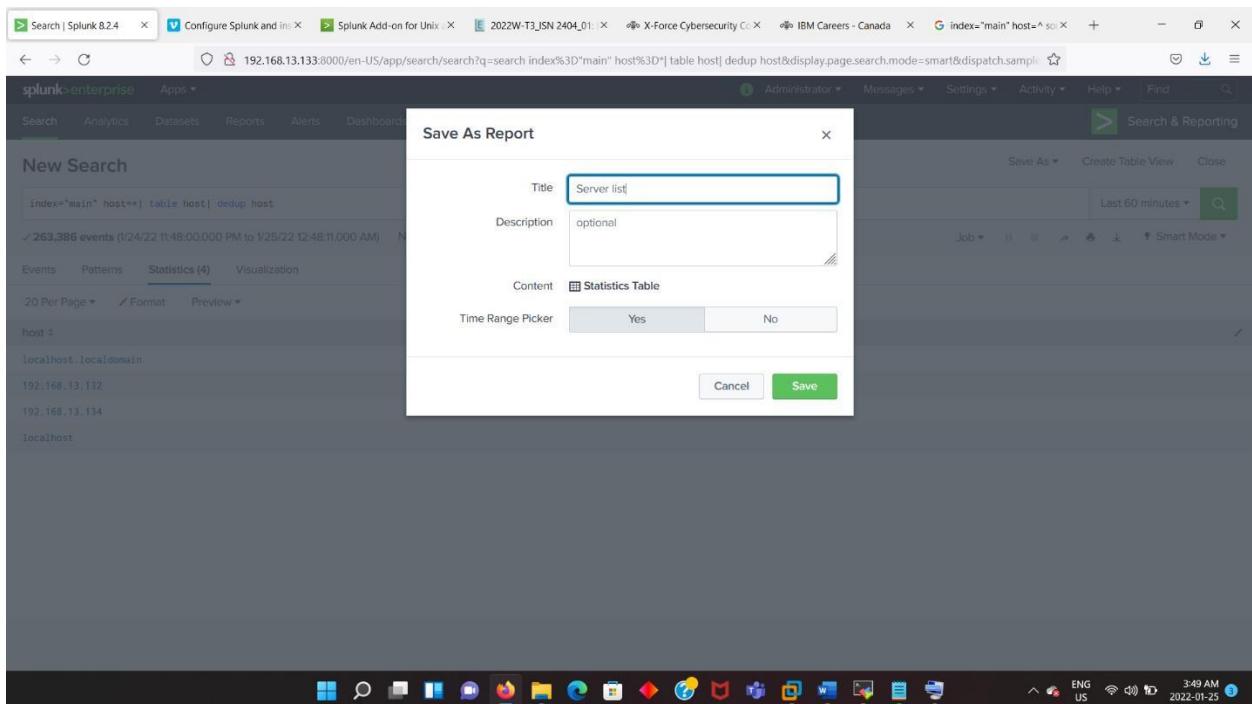
Meanwhile, access the Splunk web, this time, we get a lot of logs from all servers.

The screenshot shows the Splunk Enterprise search interface. The top navigation bar includes links for Search, Apps, Settings, Activity, Help, and Find. Below the navigation is a search bar with the query "index='main' host='\*' source='\*'". The main area displays a timeline of 239,965 events from October 24, 2022, to October 25, 2022. A green bar chart represents the event count over time. Below the timeline is a table of selected fields, which includes columns for Time, Event, and various metrics like memTotalMB, memFreeMB, and pgPageOut. The table also lists interesting fields such as action, app, and COMMAND. The bottom of the screen shows the Windows taskbar with various pinned icons.

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.

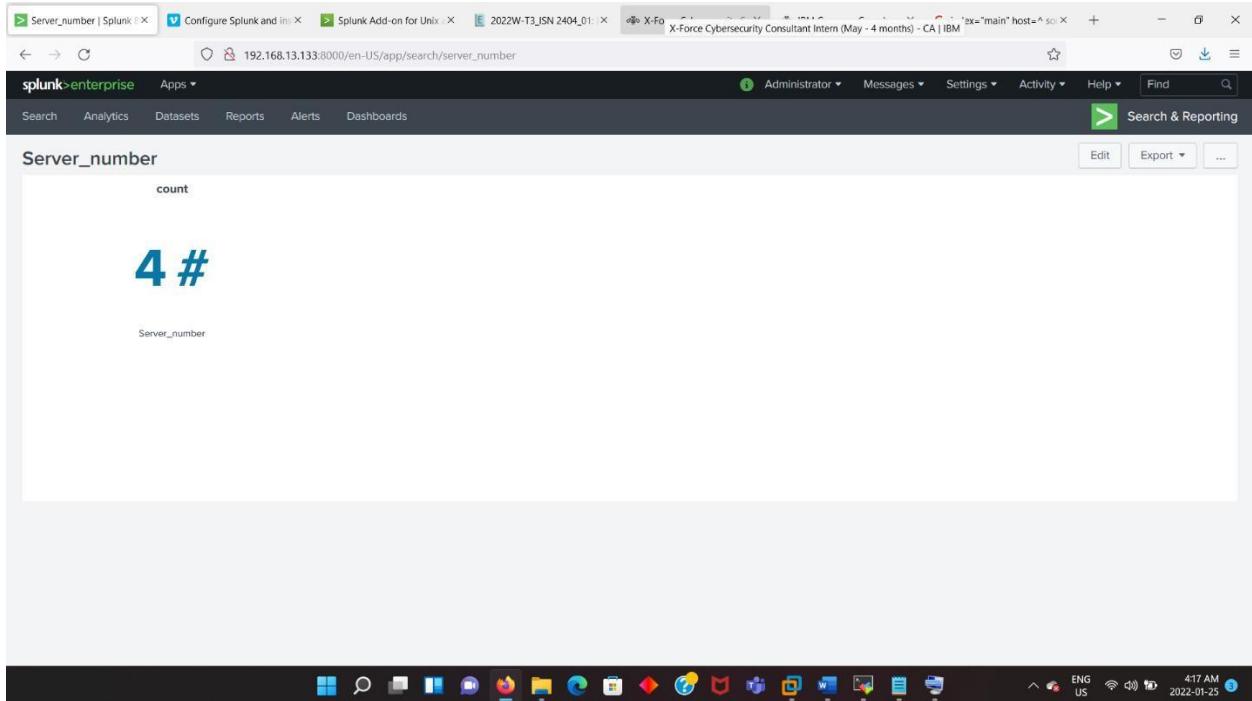


By running `index="main" host=* | table host| dedup host | stat count`, we can get the count.

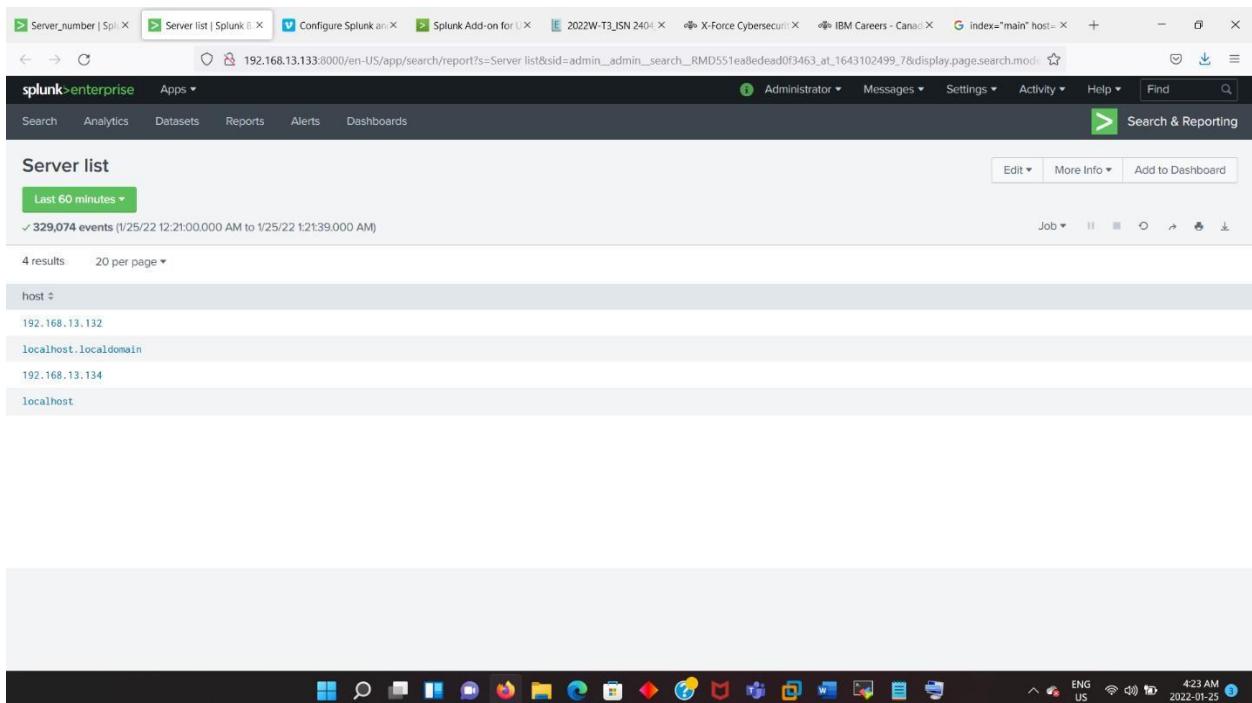
The screenshot shows a Windows desktop environment. At the top, there is a taskbar with various pinned icons. Below the taskbar, a window titled "Search | Splunk 8.2.4" is open. The window displays a search interface with a search bar containing the query "index='main' host='\*' | table host| dedup host| stats count". The results show "4 events" from "1/24/22 11:52:00.000 PM to 1/25/22 12:52:31.000 AM" with "No Event Sampling". The "Statistics" tab is selected, showing a single value of "4". The bottom right corner of the screen shows the date and time as "2022-01-25 3:53 AM".

We can also select visualization and display single digit.

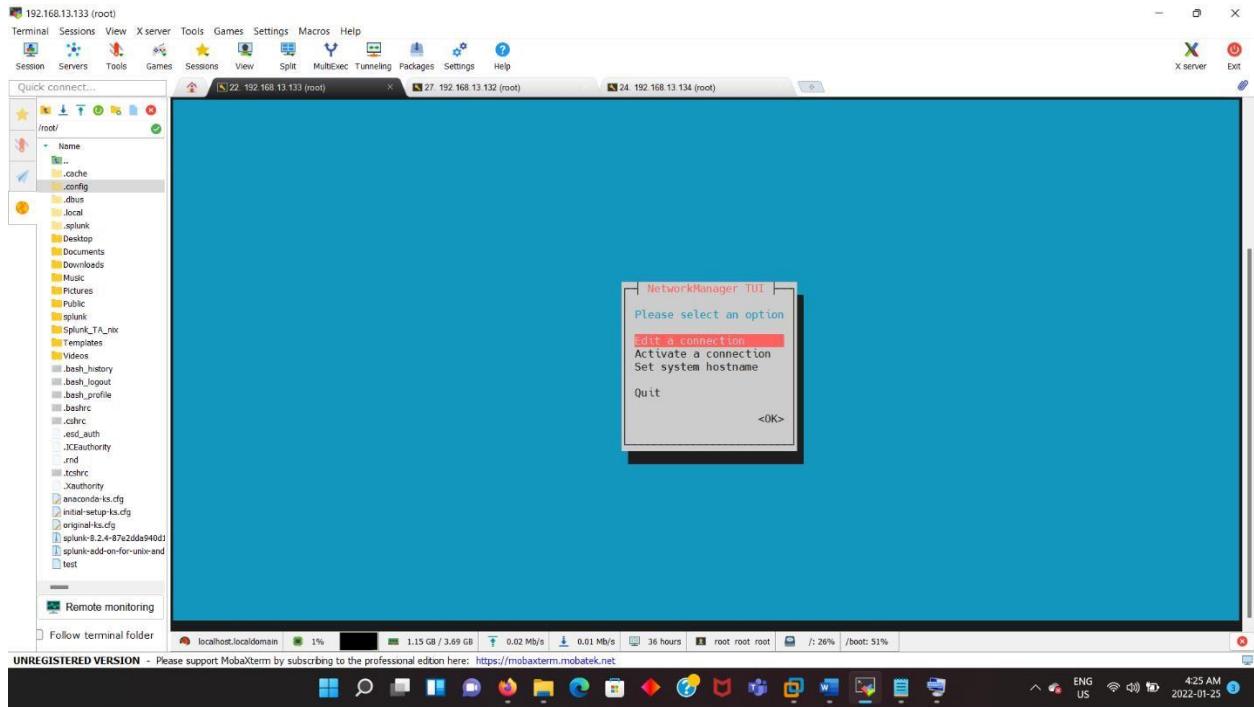
This screenshot is identical to the one above, showing the same Splunk search results and desktop environment. The difference is that the "Visualization" tab is now selected instead of "Statistics". The result "4" is displayed as a large, bold black number in the center of the search results page. The desktop taskbar and system tray are also visible at the bottom.



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.

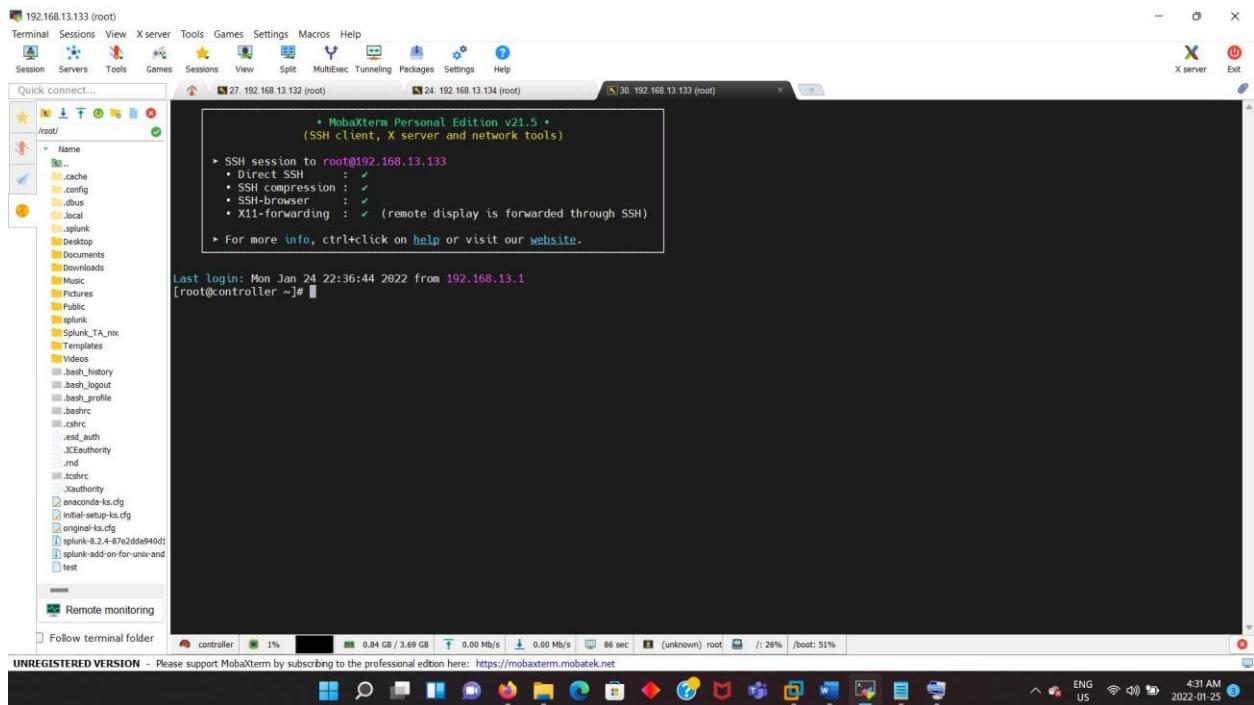


For changing the host name on controller, we can use the command nmtui



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/1zdcAPXIHtmxRr7zRXzbgoX5sVhUxFIc5?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:

All members of the group have participated in this activity.