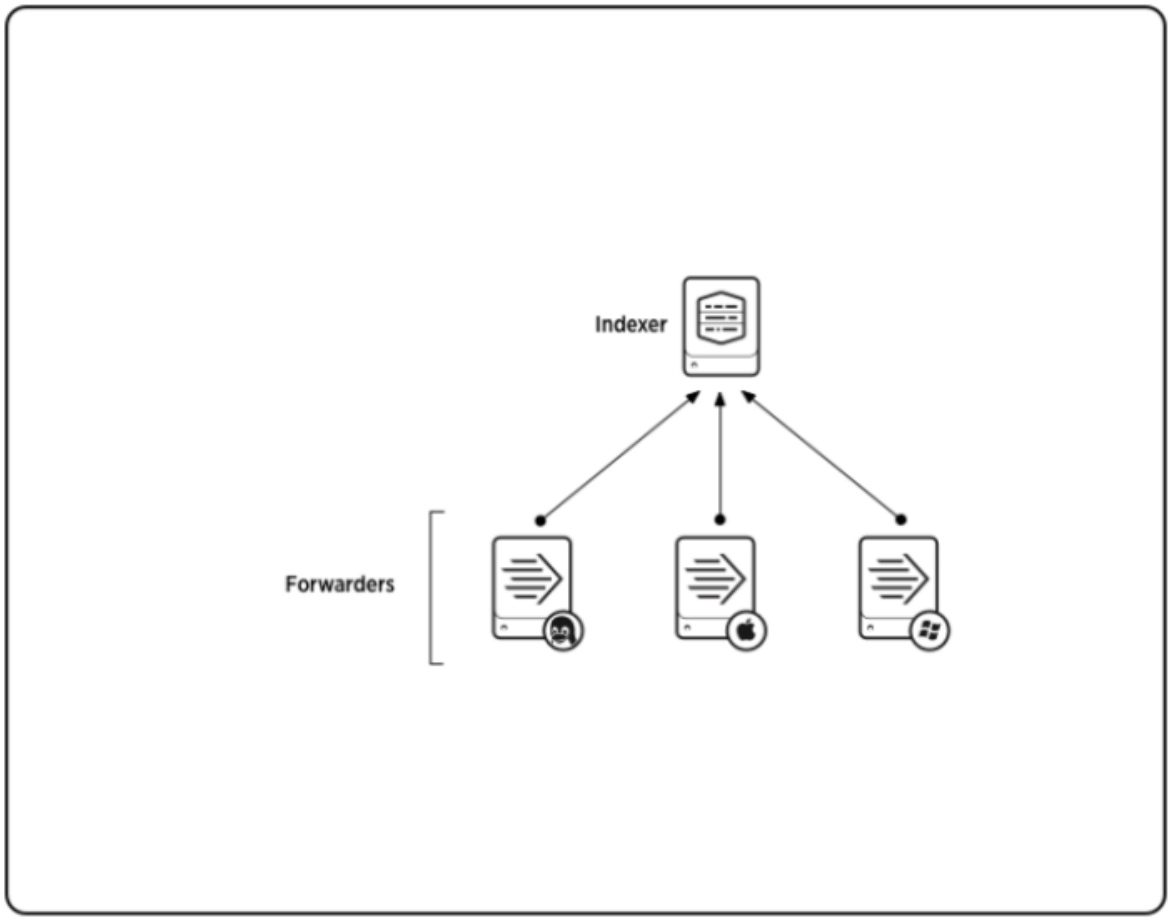
3 Vms

1. Controller
2. Agen1
3. Agent2
4. Agent3

Splunk Enterprise Commander (Indexer)

Splunk Enterprise is a software product that enables you to search, analyze, and visualize the data gathered from the components of your IT infrastructure or business. Splunk Enterprise takes in data from websites, applications, sensors, devices, and so on. After defining the data source, Splunk Enterprise indexes the data stream and parses it into a series of individual events you can view and search.

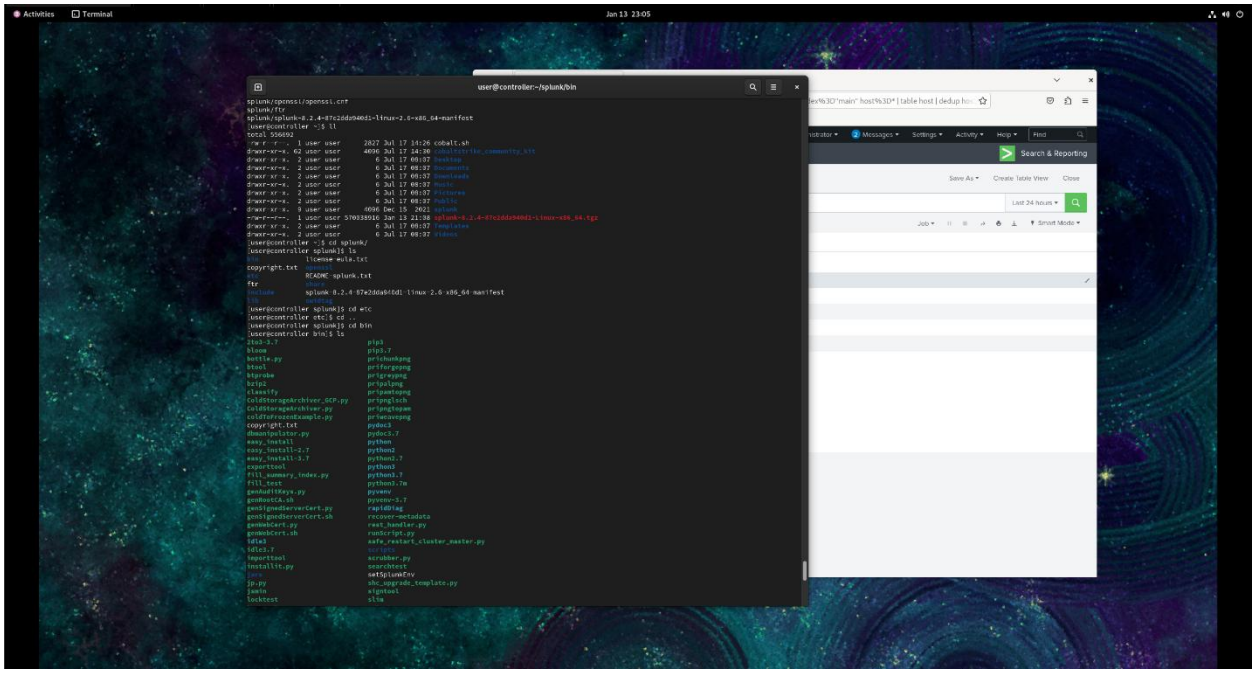


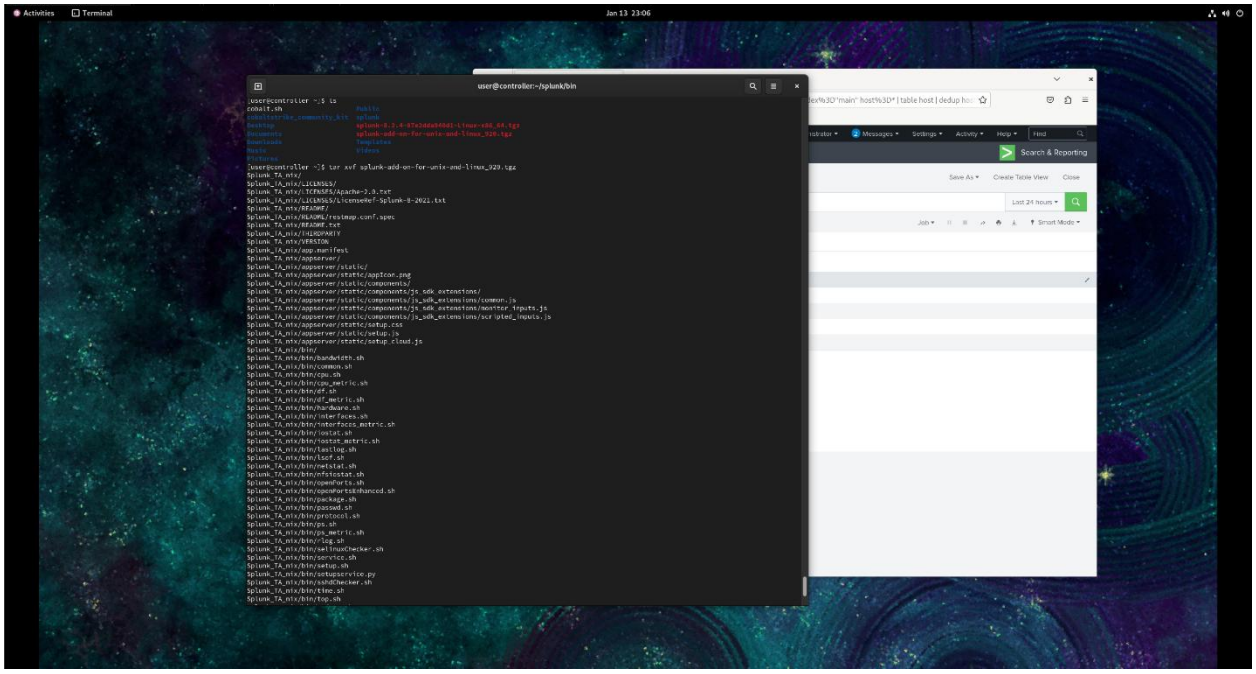
This diagram shows three universal forwarders sending data to a single receiver (an indexer), which then indexes the data and makes it available for searching. This layout is basic, but you can define many forwarding combinations based on your specific environment and network topology.

1. I created 3 VMs and downloaded Splunk in them.
2. I used Splunk Enterprise in the controller, and in the 3 agents, I used Splunk Universal Forwarder.

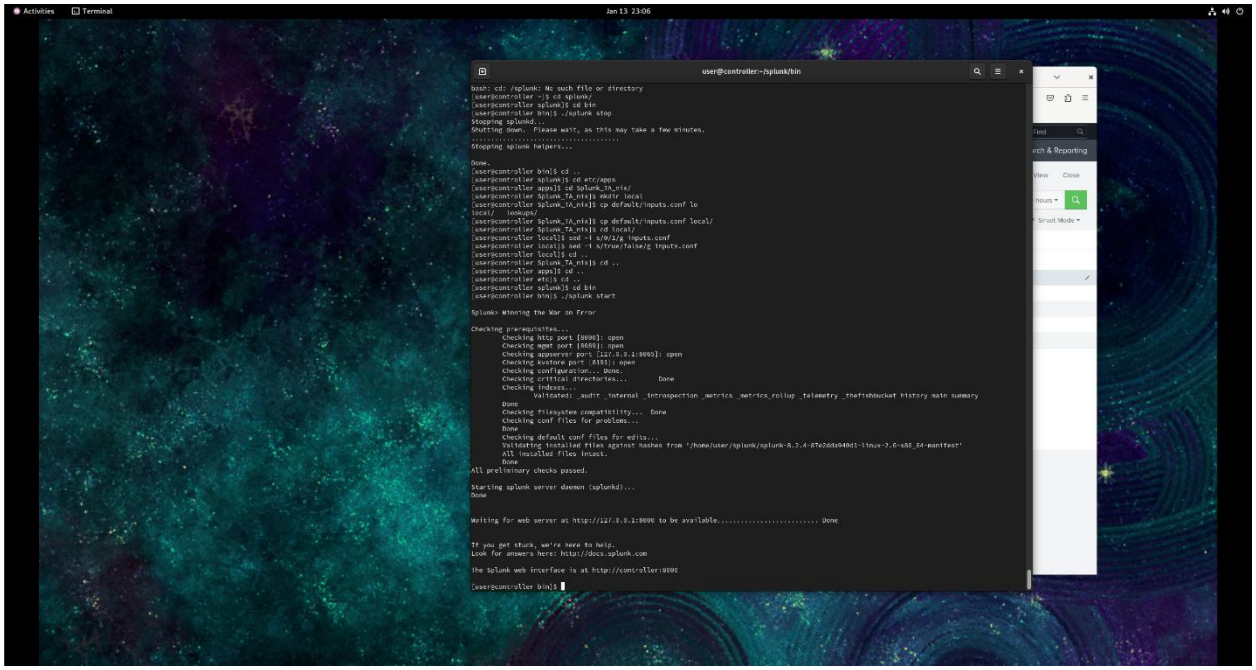
Controller:

1. I extracted the file, and then I extracted the splunk-add-on-for-linux file.

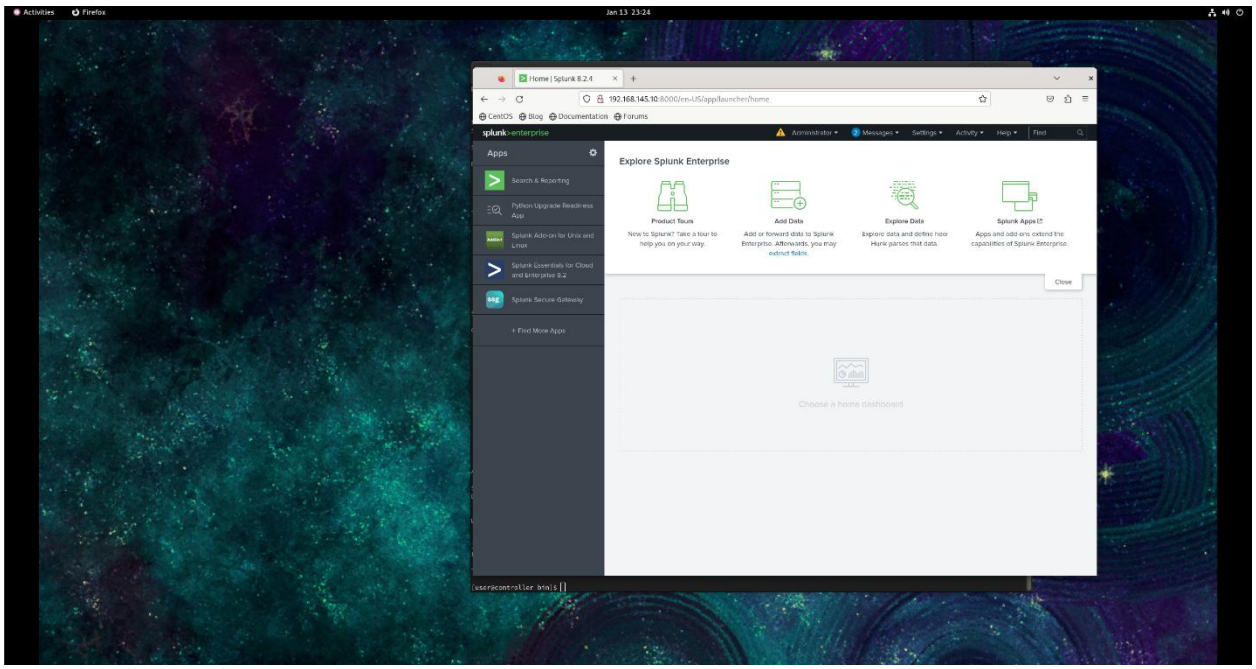




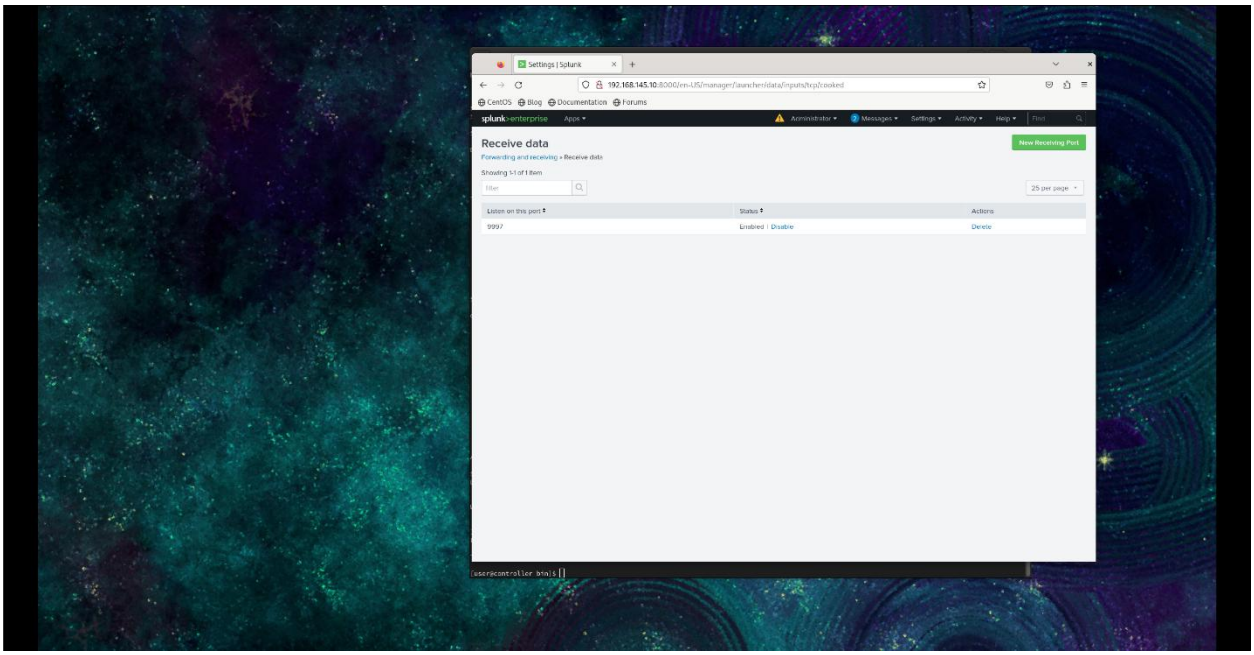
2. I configured the inputs.conf file and started Splunk



3. I successfully hosted the Splunk web on the local server



4. I configured a receiving port (9997)



Agents

1. I installed and started the Splunk forwarder

```
               Creating: /home/user/splunkforwarder/var/run/splunk/appserver/i18n
               Creating: /home/user/splunkforwarder/var/run/splunk/appserver/modules/static/css
               Creating: /home/user/splunkforwarder/var/run/splunk/upload
               Creating: /home/user/splunkforwarder/var/run/splunk/search_telemetry
               Creating: /home/user/splunkforwarder/var/spool/splunk
               Creating: /home/user/splunkforwarder/var/spool/dirmoncache
               Creating: /home/user/splunkforwarder/var/lib/splunk/authDb
               Creating: /home/user/splunkforwarder/var/lib/splunk/hashDb
New certs have been generated in '/home/user/splunkforwarder/etc/auth'.
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/home/user/splunkforwarder/splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

[user@Agent1 bin]$ ./splunk add forward-server 192.168.145.10:9997 -auth user:P@ssw0rd
Added forwarding to: 192.168.145.10:9997.
[user@Agent1 bin]$ ./splunk set deploy-poll 192.168.145.11:9997 -auth user:P@ssw0rd
Configuration updated.
[user@Agent1 bin]$ ./splunk add monitor /var/log/
Added monitor of '/var/log'.
[user@Agent1 bin]$ ./splunk restart
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
.......
Stopping splunk helpers...

Done.

Splunk> Winning the War on Error

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 '/home/user/splunkforwarder/splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

[user@Agent1 bin]$ ./splunk start --accept-license
```

2. I added the forward server

```
               Creating: /home/user/splunkforwarder/var/run/splunk/upload
               Creating: /home/user/splunkforwarder/var/run/splunk/search_telemetry
               Creating: /home/user/splunkforwarder/var/spool/splunk
               Creating: /home/user/splunkforwarder/var/spool/dirmoncache
               Creating: /home/user/splunkforwarder/var/lib/splunk/authDb
               Creating: /home/user/splunkforwarder/var/lib/splunk/hashDb
New certs have been generated in '/home/user/splunkforwarder/etc/auth'.
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/home/user/splunkforwarder/splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

[user@Agent1 bin]$ ./splunk add forward-server 192.168.145.10:9997 -auth user:P@ssw0rd
Added forwarding to: 192.168.145.10:9997.
[user@Agent1 bin]$ ./splunk set deploy-poll 192.168.145.11:9997 -auth user:P@ssw0rd
Configuration updated.
[user@Agent1 bin]$ ./splunk add monitor /var/log/
Added monitor of '/var/log'.
[user@Agent1 bin]$ ./splunk restart
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
.......
Stopping splunk helpers...

Done.

Splunk> Winning the War on Error

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 '/home/user/splunkforwarder/splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

[user@Agent1 bin]$ ./splunk start --accept-license
The splunk daemon (splunkd) is already running.
[user@Agent1 bin]$ ./splunk add forward-server 192.168.145.10:9997 -auth user:P@ssw0rd_
```

3. I set the deploy poll

```
                Creating: /home/user/splunkforwarder/var/spool/splunk
                Creating: /home/user/splunkforwarder/var/spool/dirmoncache
                Creating: /home/user/splunkforwarder/var/lib/splunk/authDb
                Creating: /home/user/splunkforwarder/var/lib/splunk/hashDb
New certs have been generated in '/home/user/splunkforwarder/etc/auth'.
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/home/user/splunkforwarder/splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

[user@Agent1 bin]$ ./splunk add forward-server 192.168.145.10:9997 -auth user:P@ssw0rd
Added forwarding to: 192.168.145.10:9997.
[user@Agent1 bin]$ ./splunk set deploy-poll 192.168.145.11:9997 -auth user:P@ssw0rd
Configuration updated.
[user@Agent1 bin]$ ./splunk add monitor /var/log/
Added monitor of '/var/log'.
[user@Agent1 bin]$ ./splunk restart
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
.......
Stopping splunk helpers...

Done.

Splunk> Winning the War on Error

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 '/home/user/splunkforwarder/splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

[user@Agent1 bin]$ ./splunk start --accept-license
The splunk daemon (splunkd) is already running.
[user@Agent1 bin]$ ./splunk add forward-server 192.168.145.10:9997 -auth user:P@ssw0rd
192.168.145.10:9997 forwarded-server already present
[user@Agent1 bin]$ ./splunk set deploy-poll 192.168.145.11:9997 -auth user:P@ssw0rd
```

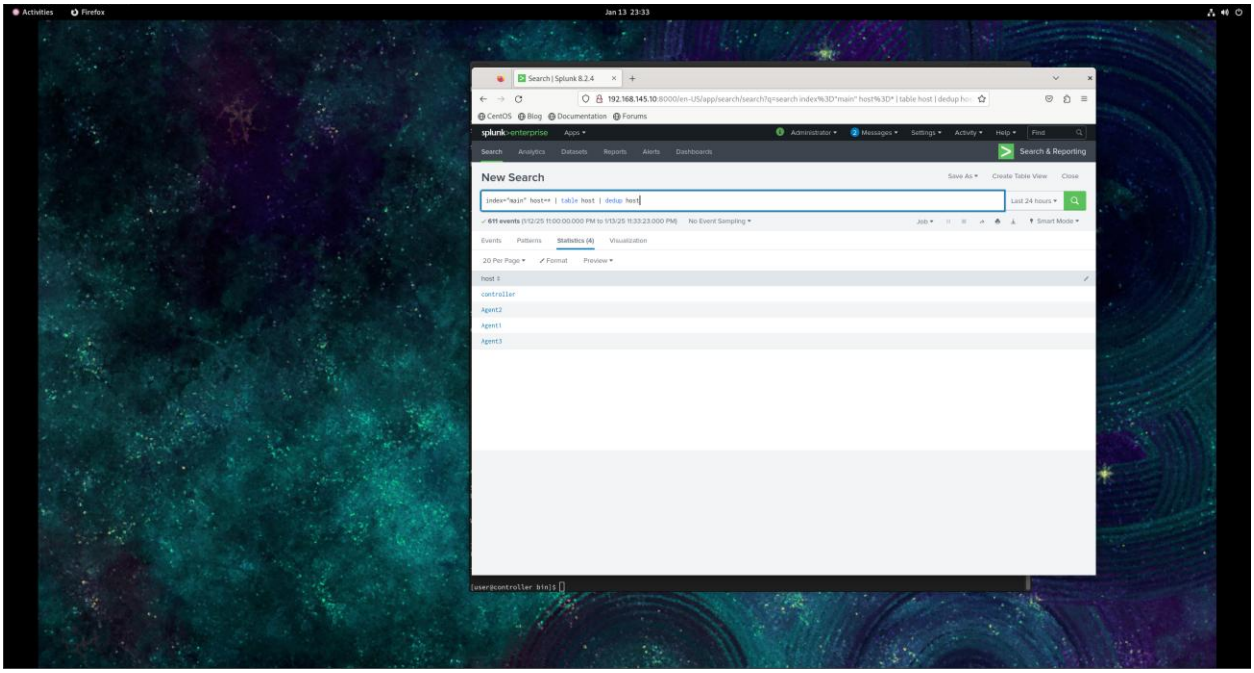
4. I add the monitor directory to send the files in Splunk

5. I restarted the Splunk

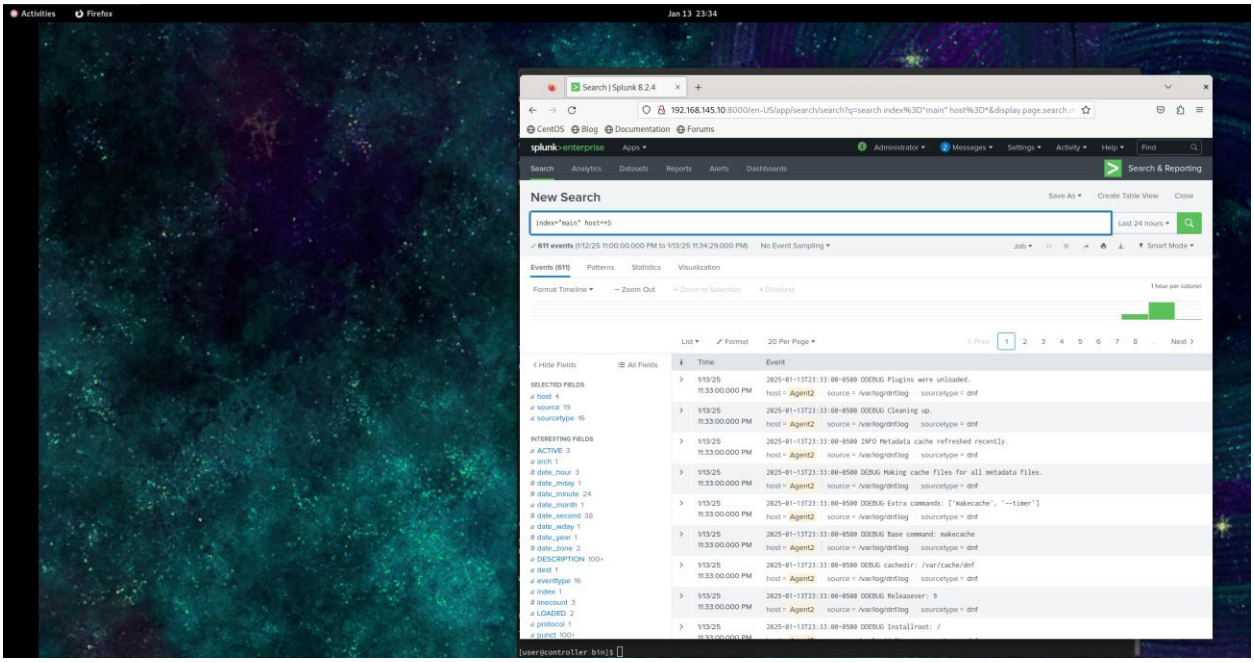
```
                Creating: /home/user/splunkforwarder/var/spool/splunk
                Creating: /home/user/splunkforwarder/var/spool/dirmoncache
                Creating: /home/user/splunkforwarder/var/lib/splunk/authDb
                Creating: /home/user/splunkforwarder/var/lib/splunk/hashDb
New certs have been generated in '/home/user/splunkforwarder/etc/auth'.
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/home/user/splunkforwarder/splunkforwarder-8.2.4-87e2da940d1-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

[user@Agent1 bin]$ ./splunk add forward-server 192.168.145.10:9997 -auth user:P@ssw0rd
Added forwarding to: 192.168.145.10:9997.
[user@Agent1 bin]$ ./splunk set deploy-poll 192.168.145.11:9997 -auth user:P@ssw0rd
Configuration updated.
[user@Agent1 bin]$ ./splunk add monitor /var/log/
Added monitor of '/var/log'.
[user@Agent1 bin]$ ./splunk restart
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
.......
Stopping splunk helpers...

Done.

Splunk> Winning the War on Error

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 '/home/user/splunkforwarder/splunkforwarder-8.2.4-87e2da940d1-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

[user@Agent1 bin]$ ./splunk start --accept-license
The splunk daemon (splunkd) is already running.
[user@Agent1 bin]$ ./splunk add forward-server 192.168.145.10:9997 -auth user:P@ssw0rd
192.168.145.10:9997 forwarded-server already present
[user@Agent1 bin]$ ./splunk restart
```

6. I did it in all the agents

Splunk web server



Showing all the controller and agents are successfully added and sending the logs



The problem I faced

1. The controller was not showing in the splunk.
   Solution: I added the splunk-add-on-for-linux and configure it and it solved the problem.
2. The agents were not showing.
   Solution: I mistakenly downloaded a different version of Splunk forward. I again downloaded and installed the right one and it worked.