A **Splunk Universal Forwarder (UF)** is a lightweight, high-performance version of Splunk Enterprise specifically designed to collect and send data. Unlike the full Splunk Enterprise, it doesn't have a web interface and consumes very little system memory and CPU.

Key Characteristics

- **Lightweight:** It only contains the essential components needed to forward data, making it safe to install on production servers without slowing them down.
- **No Parsing:** It sends **unparsed (raw)** data. The heavy lifting (parsing and indexing) is done later by the Indexer.
- **Resource Efficient:** It has a tiny footprint and does not include Splunk Web or Python by default.
- **Secure:** Supports SSL/TLS encryption for data in transit.
- **Reliable:** If the Indexer goes down, the UF can buffer data locally and send it once the connection is restored.

Common Use Cases

- **Log Collection:** Monitoring system logs (like /var/log/syslog) or application logs.
- **Endpoint Monitoring:** Gathering data from thousands of workstations or servers simultaneously.
- **Real-time Streaming:** Sending data to a central Splunk Indexer or Splunk Cloud as it happens.

SPLUNK FORWARDER → INDEXER (UBUNTU)

❖ ARCHITECTURE

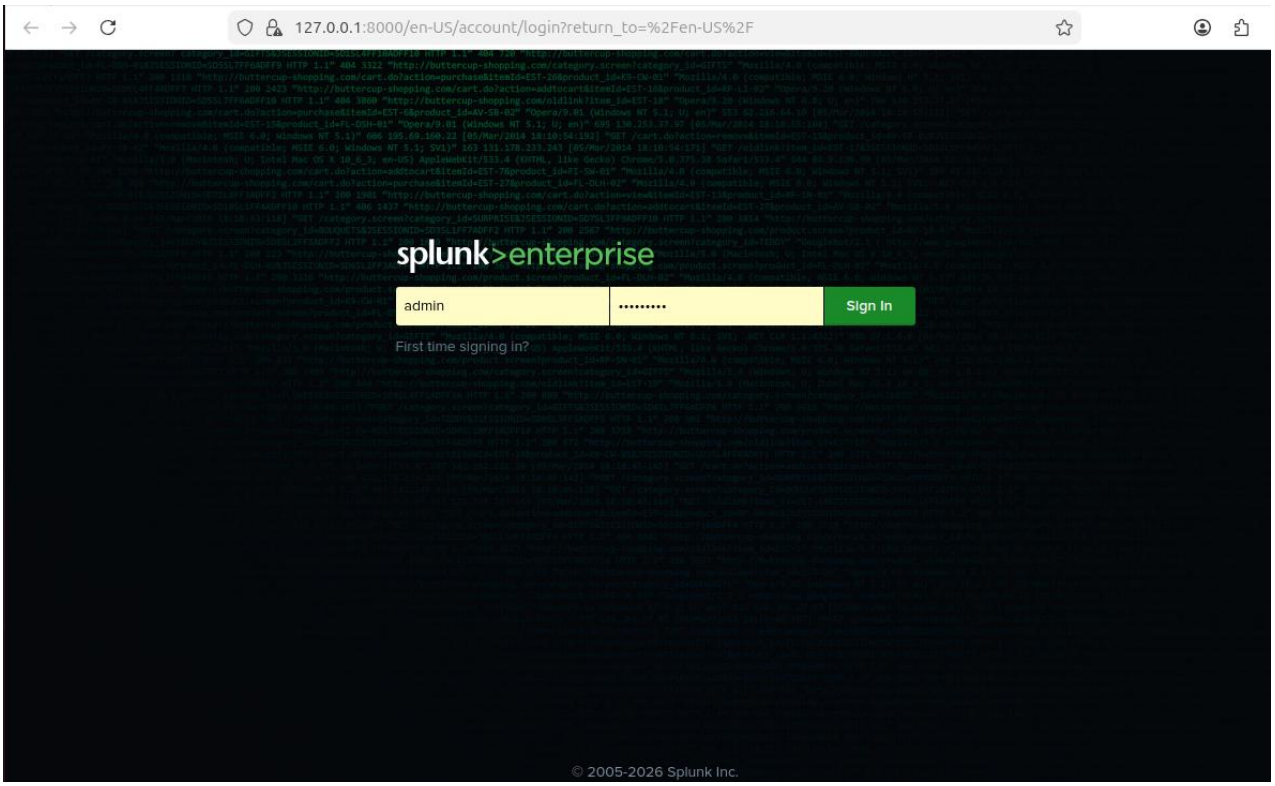
Ubuntu Server (Forwarder) ——► Splunk Indexer (Port 9997)

1. **Login to Splunk Indexer**

   Open your browser:

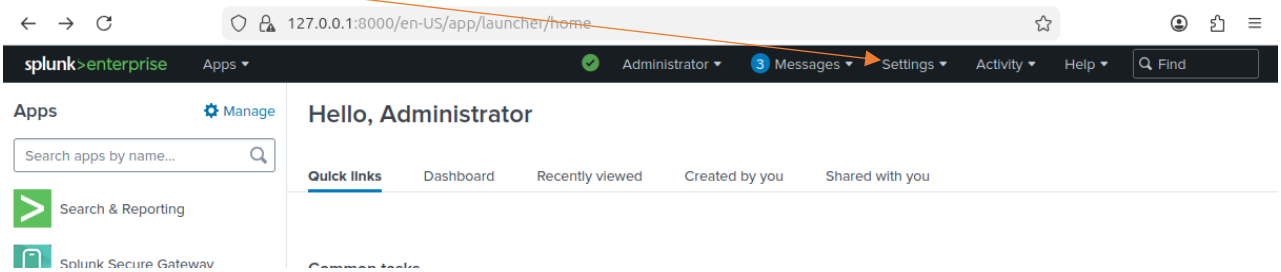
   http://<INDEXER_IP>:8000

   Login as **admin**.

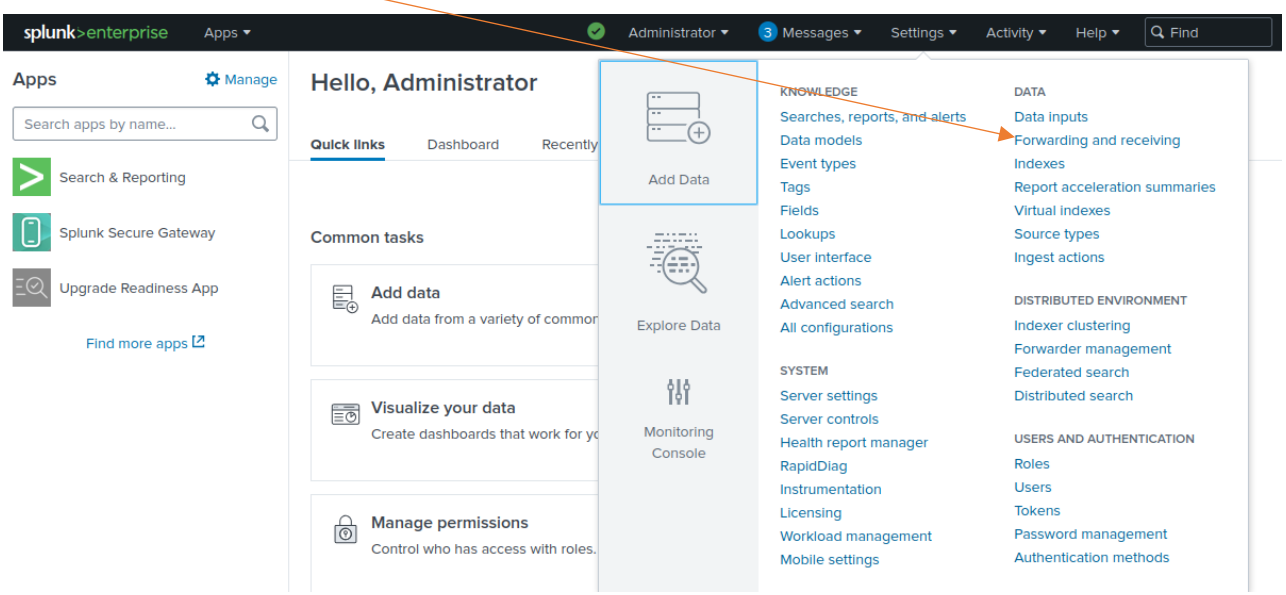


2. Enable Receiving Port (9997)

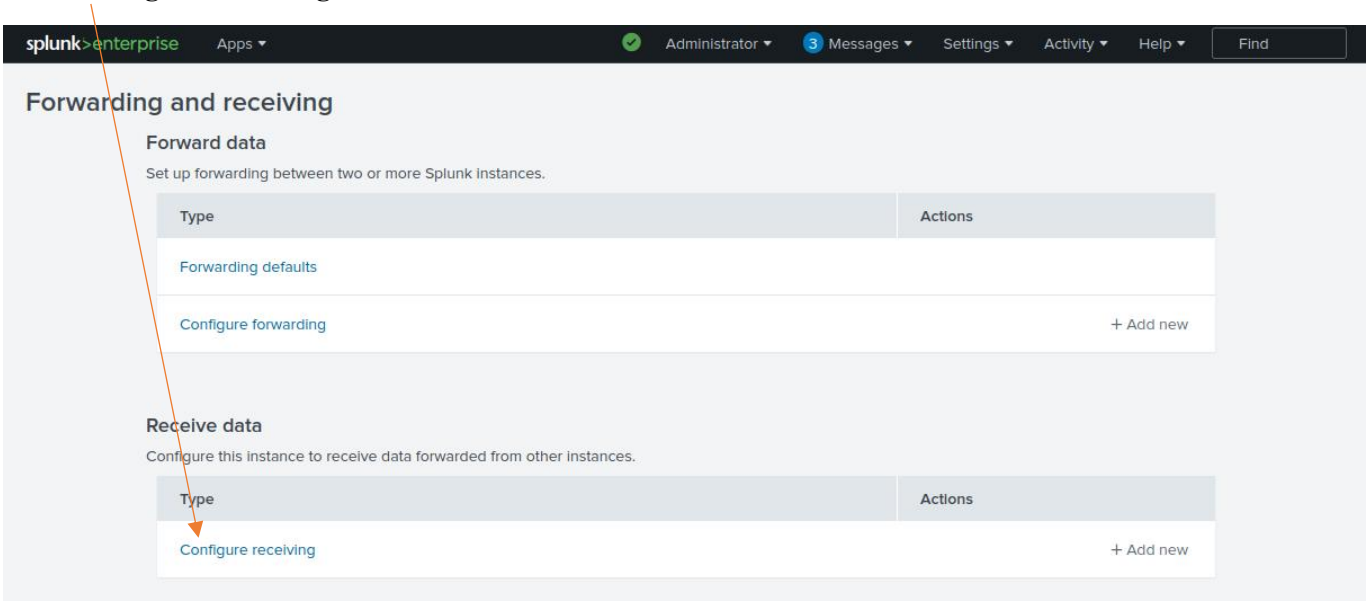
1. Go to **Settings**.



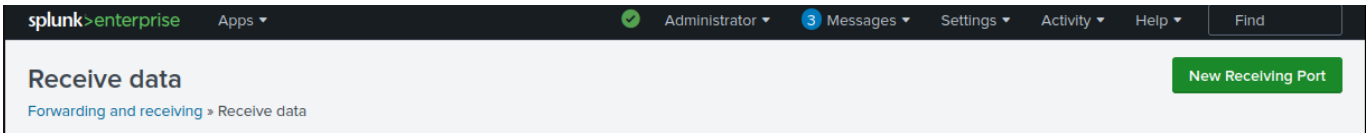
2. Click **Forwarding and Receiving**.



3. Click **Configure Receiving**.

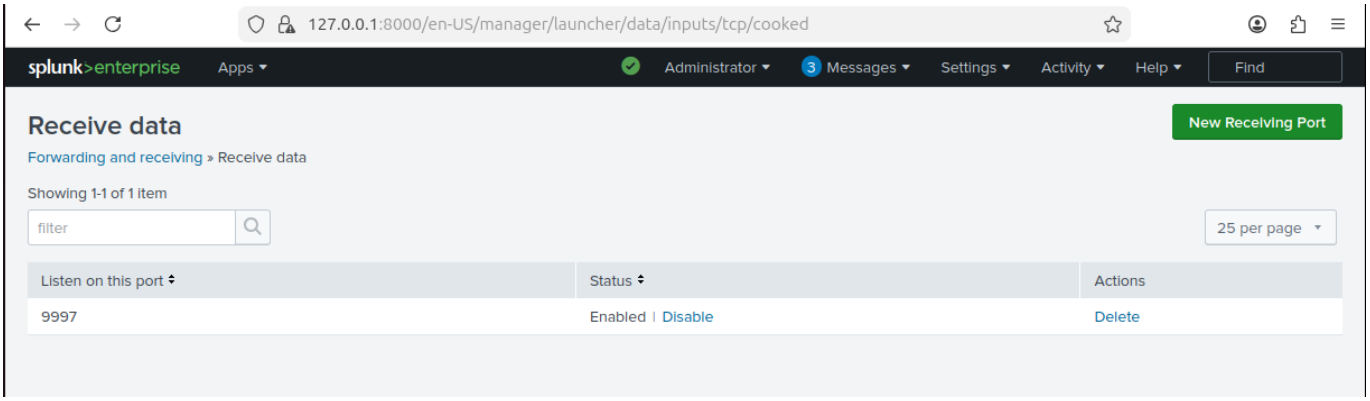


4. Click **New Receiving Port**.



5. Enter: 9997

   Click **Save**.



➢ Your Indexer is now ready to listen for incoming data.

UBUNTU FORWARDER INSTALLATION

1. Update Ubuntu System

```
sudo apt update
sudo apt upgrade -y
```

2. **Download Splunk Universal Forwarder (.deb)**

wget -O splunkforwarder.deb
"https://download.splunk.com/products/universalforwarder/releases/10.2.0/linux/splunkforwarder-10.2.0-d749cb17ea65-linux-2.6-amd64.deb"

```
root@workstaion:/home/shubham# wget -O splunkforwarder-10.2.0-d749cb17ea65-linux-amd64.deb "https://download.splunk.com/
products/universalforwarder/releases/10.2.0/linux/splunkforwarder-10.2.0-d749cb17ea65-linux-amd64.deb"
--2026-01-19 17:15:48--  https://download.splunk.com/products/universalforwarder/releases/10.2.0/linux/splunkforwarder-1
0.2.0-d749cb17ea65-linux-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 54.240.162.35, 54.240.162.21, 54.240.162.92, ...
Connecting to download.splunk.com (download.splunk.com)|54.240.162.35|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 82498966 (79M) [binary/octet-stream]
Saving to: ‘splunkforwarder-10.2.0-d749cb17ea65-linux-amd64.deb’

splunkforwarder-10.2.0-d749cb 100%[================================================>]  78.68M  2.77MB/s    in 27s

2026-01-19 17:16:16 (2.95 MB/s) - ‘splunkforwarder-10.2.0-d749cb17ea65-linux-amd64.deb’ saved [82498966/82498966]
```

3. **Install the Forwarder**

sudo dpkg -i splunkforwarder.deb

```
root@workstaion:/home/shubham# sudo dpkg -i splunkforwarder-10.2.0-d749cb17ea65-linux-amd64.deb
Selecting previously unselected package splunkforwarder.
(Reading database ... 150576 files and directories currently installed.)
Preparing to unpack splunkforwarder-10.2.0-d749cb17ea65-linux-amd64.deb ...
verify that this sytem has all the commands we will require to perform the preflight step
no need to run the splunk-preinstall upgrade check
Unpacking splunkforwarder (10.2.0) ...
Setting up splunkforwarder (10.2.0) ...
find: ‘/opt/splunkforwarder/lib/python3.7/site-packages’: No such file or directory
find: ‘/opt/splunkforwarder/lib/python3.9/site-packages’: No such file or directory
complete
root@workstaion:/home/shubham#
```

(If errors occur, run: sudo apt --fix-broken install -y)

4. **Start Splunk Forwarder**

sudo /opt/splunkforwarder/bin/splunk start --accept-license

```
root@workstaion:/home/shubham# sudo /opt/splunkforwarder/bin/splunk start --accept-license
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.
```

You will be prompted to:

- Create an **admin username**.
- Create a **password**.

```
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:
Creating unit file...
Important: splunk will start under systemd as user: splunkfwd
The unit file has been created.


Splunk> Needle. Haystack. Found.

Checking prerequisites...
        Checking mgmt port [8089]: open
                Creating: /opt/splunkforwarder/var/lib/splunk
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
                Creating: /opt/splunkforwarder/var/run/splunk/upload
                Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
                Creating: /opt/splunkforwarder/var/run/splunk/search_log
                Creating: /opt/splunkforwarder/var/spool/splunk
                Creating: /opt/splunkforwarder/var/spool/dirmoncache
                Creating: /opt/splunkforwarder/var/lib/splunk/authDb
```

5. Enable Auto Start on Boot

sudo /opt/splunkforwarder/bin/splunk enable boot-start

```
root@workstaion:/home/shubham# sudo /opt/splunkforwarder/bin/splunk enable boot-start
splunk is currently running, please stop it before running enable/disable boot-start
root@workstaion:/home/shubham# sudo /opt/splunkforwarder/bin/splunk status
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
splunkd is running (PID: 19939).
splunk helpers are running (PIDs: 19989).
root@workstaion:/home/shubham#
```

CONNECT FORWARDER TO INDEXER

6. Add Indexer as Forward Server

sudo /opt/splunkforwarder/bin/splunk add forward-server <INDEXER_IP>:9997

(Example: sudo /opt/splunkforwarder/bin/splunk add forward-server 192.168.1.100:9997)

```
root@workstaion:/home/shubham# sudo /opt/splunkforwarder/bin/splunk add forward-server 192.168.192.140:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
192.168.192.140:9997 forwarded-server already present
```

7. Verify Connection

sudo /opt/splunkforwarder/bin/splunk list forward-server

You should see the status as **Active**.

```
root@workstaion:/home/shubham# sudo /opt/splunkforwarder/bin/splunk list forward-server
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Your session is invalid.  Please login.
Splunk username: admin
Password:
Active forwards:
        192.168.192.140:9997
Configured but inactive forwards:
        None
```

ADD DATA TO FORWARD

8. Forward System Logs

To monitor all logs in the log directory:

sudo /opt/splunkforwarder/bin/splunk add monitor /var/log

```
root@workstaion:/home/shubham# sudo /opt/splunkforwarder/bin/splunk add monitor /var/log
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/var/log'.
```

Add also syslog for check:

sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/syslog

```
root@workstaion:/home/shubham# sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/syslog
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/var/log/syslog'.
```

9. Send to a Specific Index

sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/auth.log -index linux_auth

Ensure the index "linux_auth" is already created on the Indexer side.

```
root@workstaion:/home/shubham# sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/auth.log -index linux_auth
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/var/log/auth.log'.
root@workstaion:/home/shubham#
```

10. Restart Forwarder

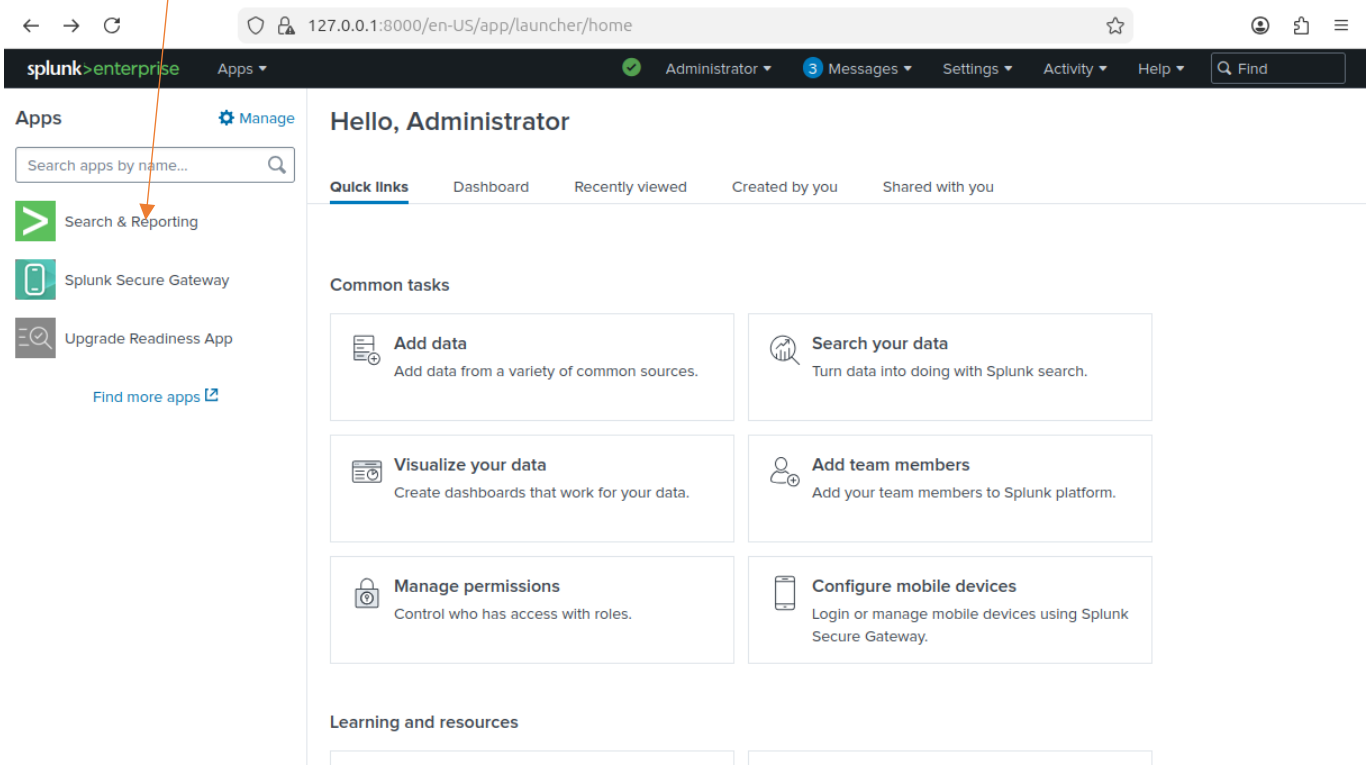
sudo /opt/splunkforwarder/bin/splunk restart

```
root@workstaion:/home/shubham# sudo /opt/splunkforwarder/bin/splunk restart
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.

Stopping splunk helpers...

Done.
splunkd.pid doesn't exist...

Splunk> CSI: Logfiles.

Checking prerequisites...
        Checking mgmt port [8089]: open
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-10.2.0-d749cb17ea65-linux-a
md64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
```

VERIFY DATA ON INDEXER

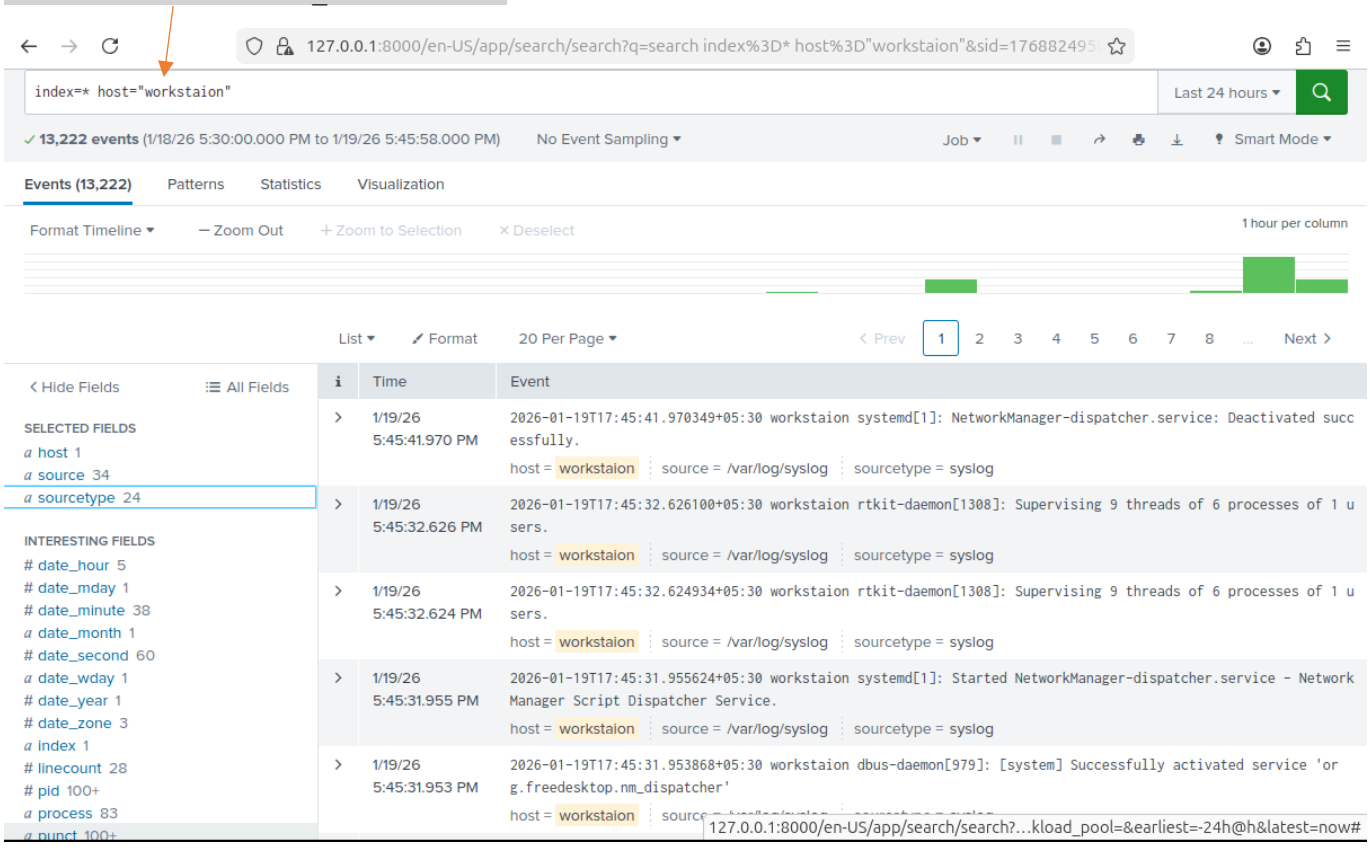
11. Search Logs

Go to **Search & Reporting**



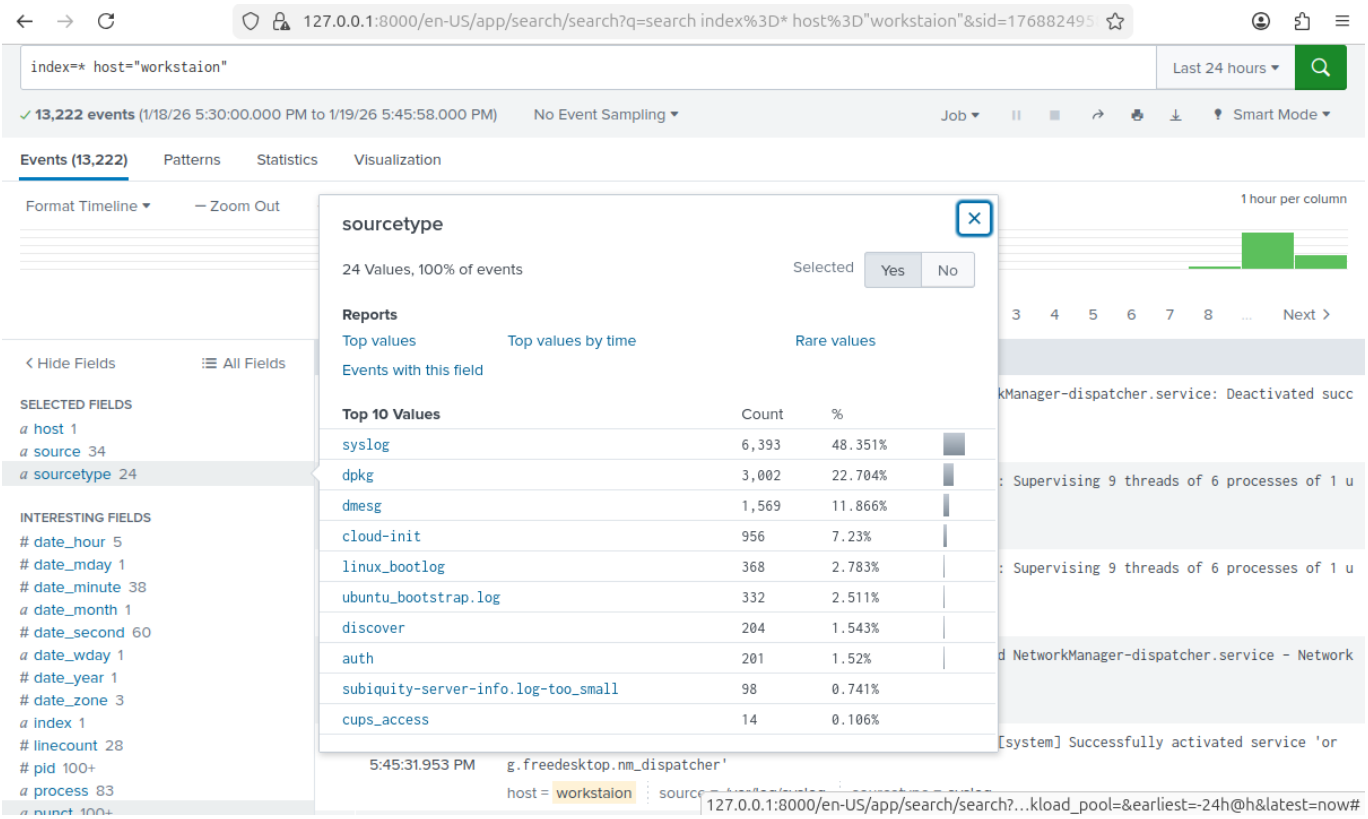
Search here:

index=* host=<UBUNTU_HOSTNAME>



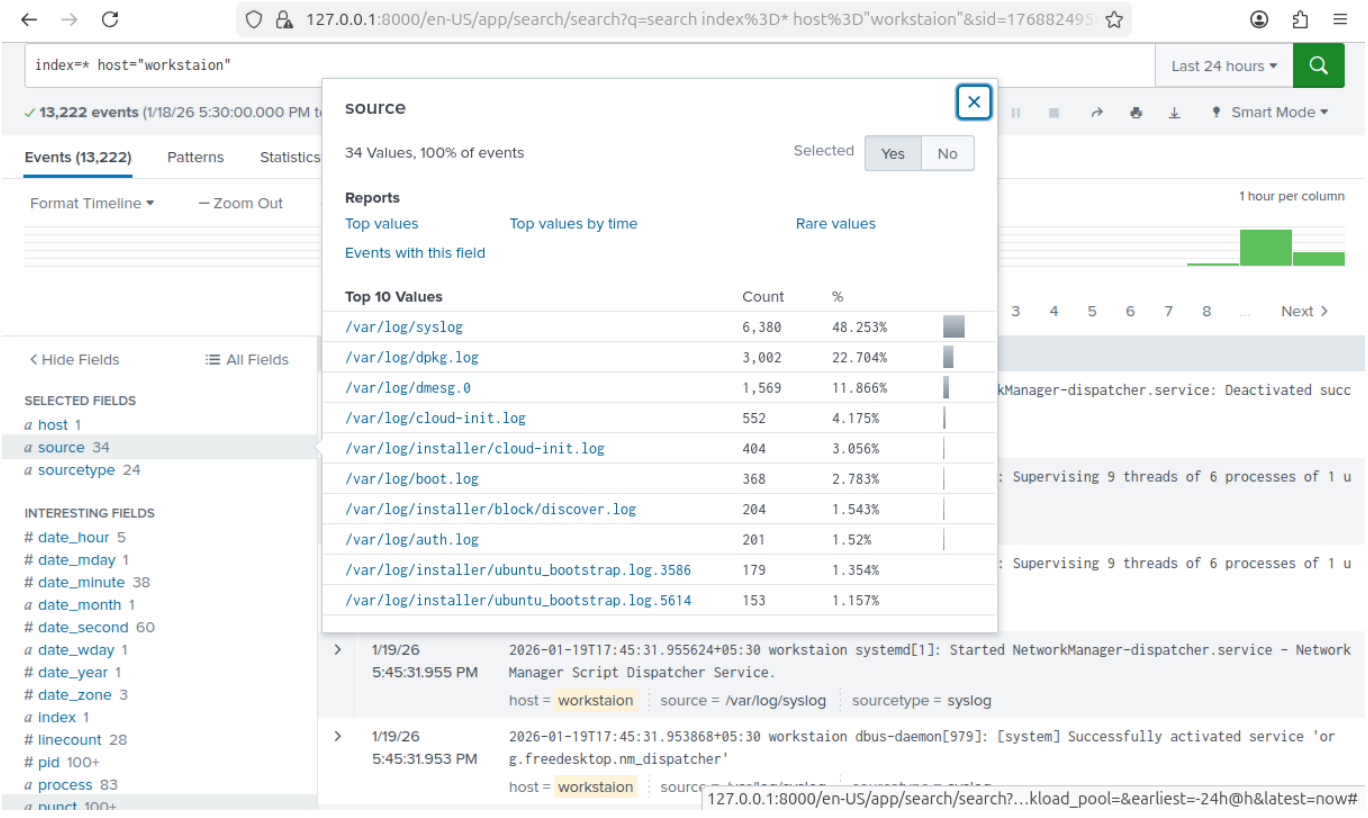
Showing here all sourcetype:

Each type has different logs



Showing here all source:

Each source has different logs



- ❖ If events appear, your data transfer is successful! 🎉