

## **Splunk setup and splunk forwarder setup on windows also open rdp port in windows and create bruteforce attack from kali**

use the following link to directly download Splunk v9.1.2:

[Splunk Enterprise 9.1.2 - Linux \(.deb\) - Direct Download Link](#)

Once the download is complete we will have a **.deb** file. Open the Terminal (**Ctrl+Alt+t**) and navigate to the Downloads folder.

**cd Downloads**

then install curl using this command

**sudo apt install curl**

```
root@gopal-VMware-Virtual-Platform:/home/gopal/Downloads# sudo apt install curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
curl is already the newest version (8.5.0-2ubuntu10.6).
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
```

Run the following command to install Splunk:

**sudo dpkg -i splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb**

```
root@gopal-VMware-Virtual-Platform:/home/gopal/Downloads# sudo dpkg -i splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 152830 files and directories currently installed.)
Preparing to unpack splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb ...
Unpacking splunk (9.1.2) ...
Setting up splunk (9.1.2) ...
complete
```

After the installation is completed use the following command to launch Splunk:

**sudo /opt/splunk/bin/splunk start --accept-license --answer-yes**

Provide username and password for creating account.

```
root@gopal-VMware-Virtual-Platform:/home/gopal/Downloads# sudo /opt/splunk/bin/splunk start --accept-license --answer-yes
s
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.

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:
Copying '/opt/splunk/etc/openldap/ldap.conf.default' to '/opt/splunk/etc/openldap/ldap.conf'.
Generating RSA private key, 2048 bit long modulus
.....+++++
..+++++
e is 65537 (0x10001)
writing RSA key
```

Once the setup is complete we see the Splunk is running on <http://127.0.0.1:8000>

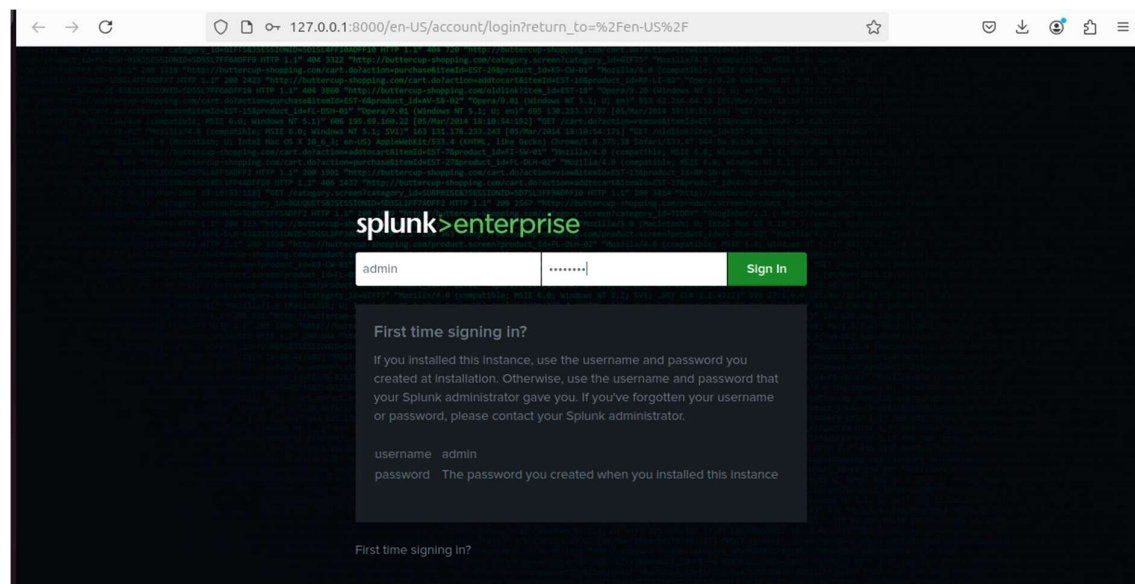
```
If you get stuck, we're here to help.  
Look for answers here: http://docs.splunk.com  
  
The Splunk web interface is at http://gopal-VMware-Virtual-Platform:8000
```

Run the following to allow Splunk to start automatically when the system is booted.

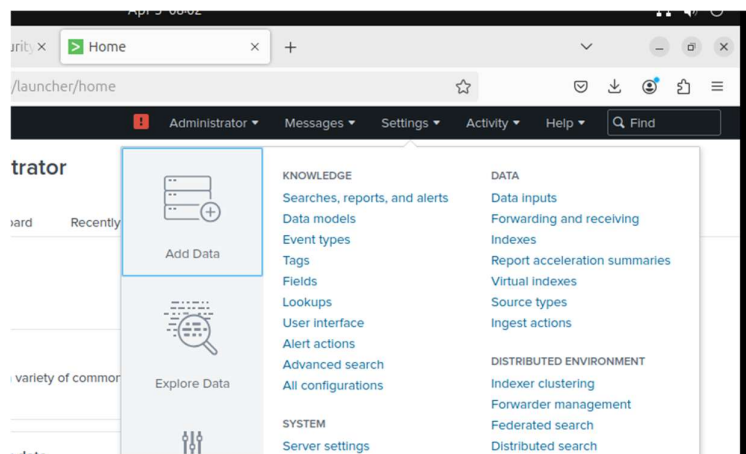
```
sudo /opt/splunk/bin/splunk enable boot-start
```

```
root@gopal-VMware-Virtual-Platform:/home/gopal/Downloads# sudo /opt/splunk/bin/splunk enable boot-start  
Init script installed at /etc/init.d/splunk.  
Init script is configured to run at boot.  
root@gopal-VMware-Virtual-Platform:/home/gopal/Downloads#
```

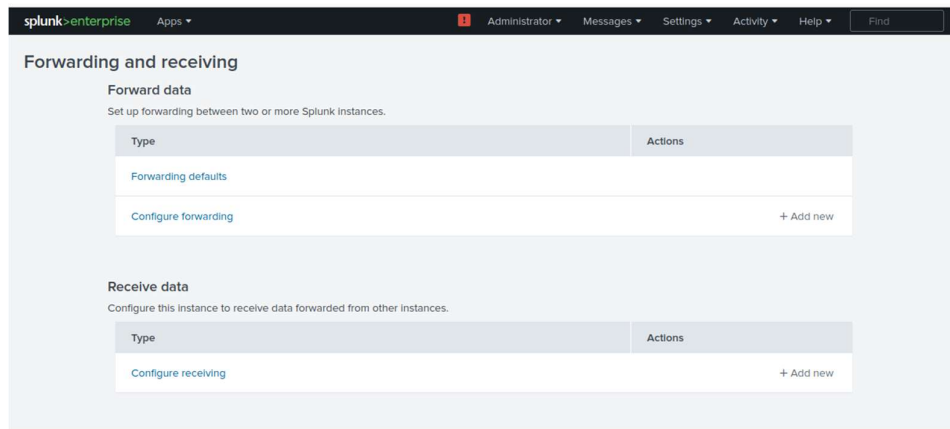
Then **open link** and add **username** and **password** that made when prompted



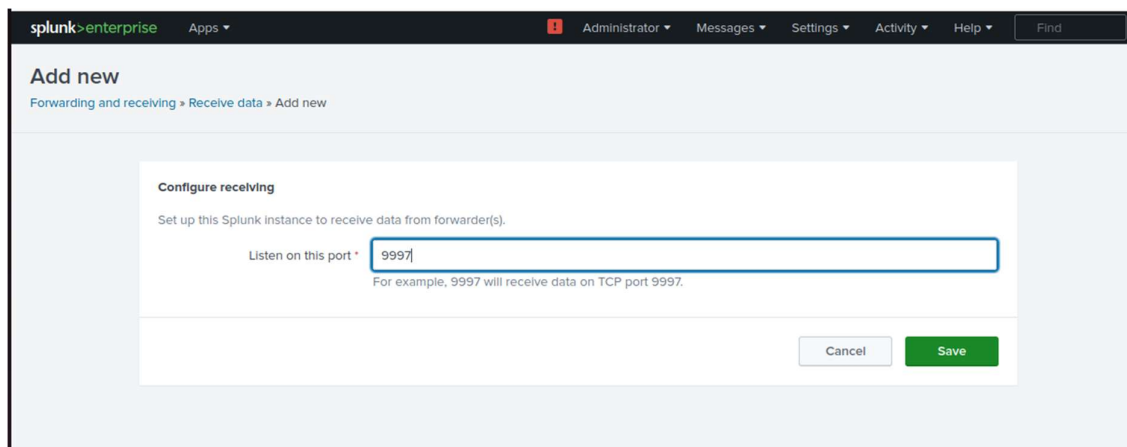
Click on **settings** and **forwarding and receiving** button



Then click on **configure receiving section add new** button

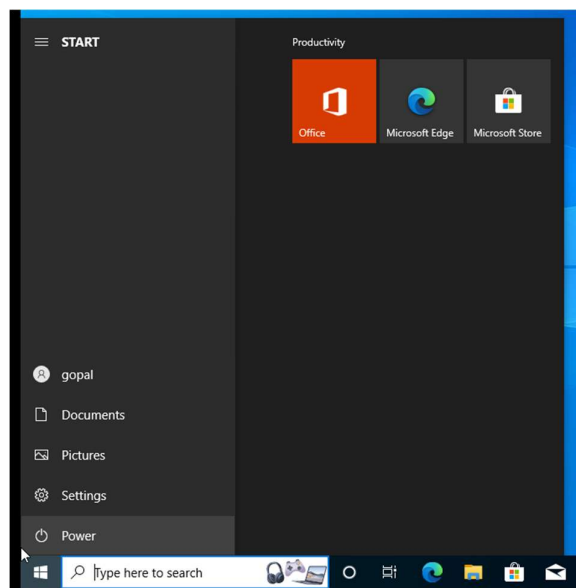


Then add port number default is **9997** and click on **save** button.

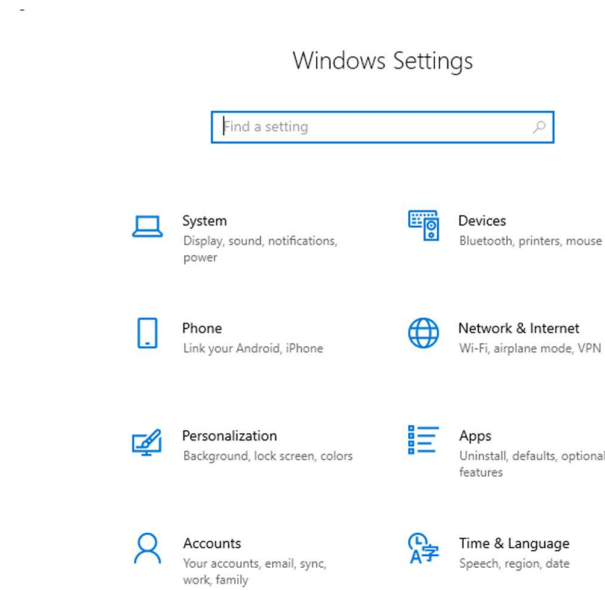


Now open windows and install splunk universal forwarder using this link [Splunk Universal Forwarder 9.1.2 - Windows \(.msi\) - Direct Download Link](#)

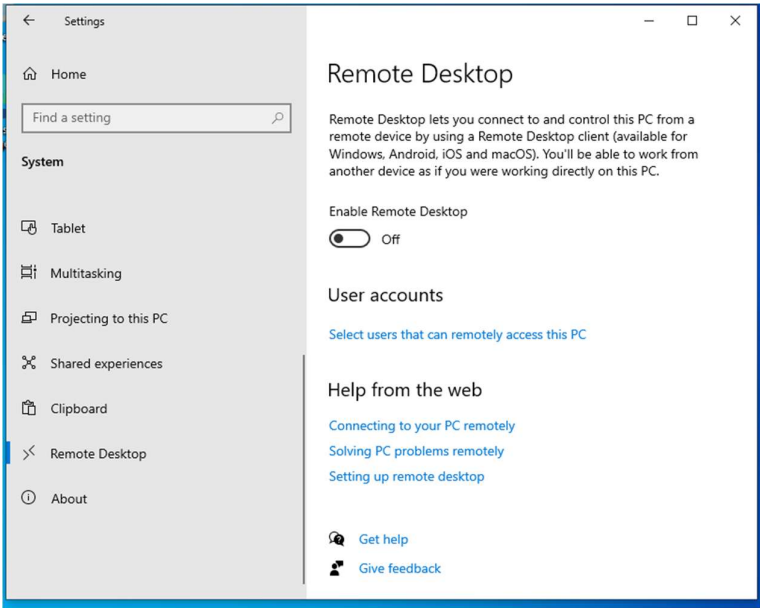
Its start downloading then double tap on windows bottom and open **settings**



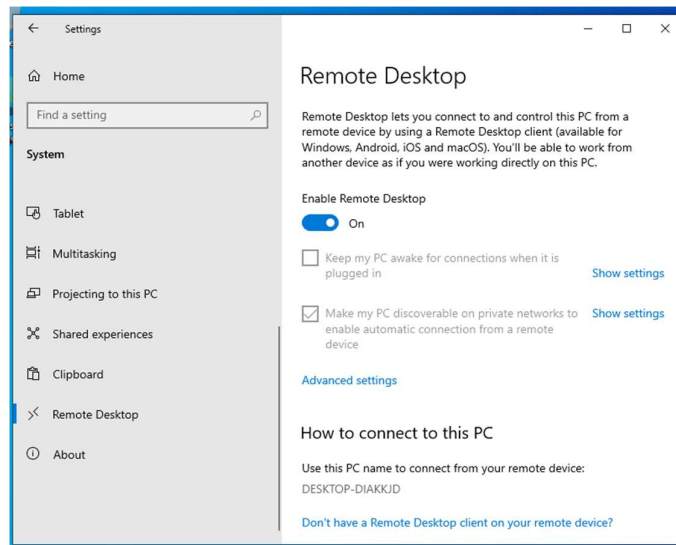
Open **system**



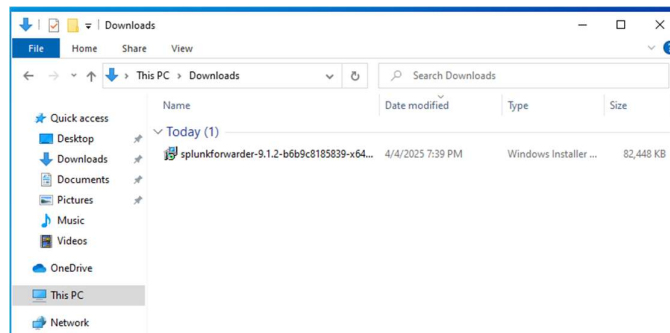
Now click on **Remote Desktop**



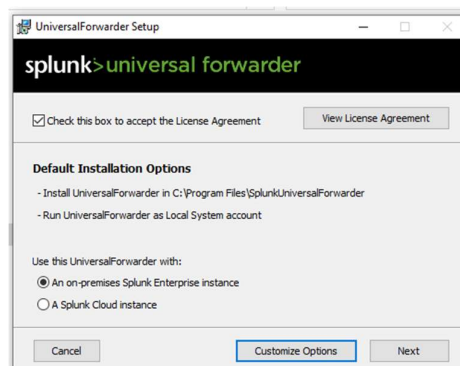
Click on **Enable Remote Desktop**.



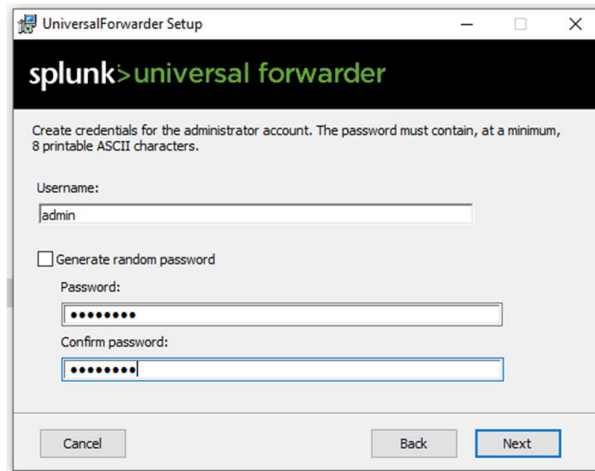
Next open **file explorer** and go to **Downloads** also double tap on **install splunk forwarder**.



Check the box on the top to accept the agreement and then click on **Next**.



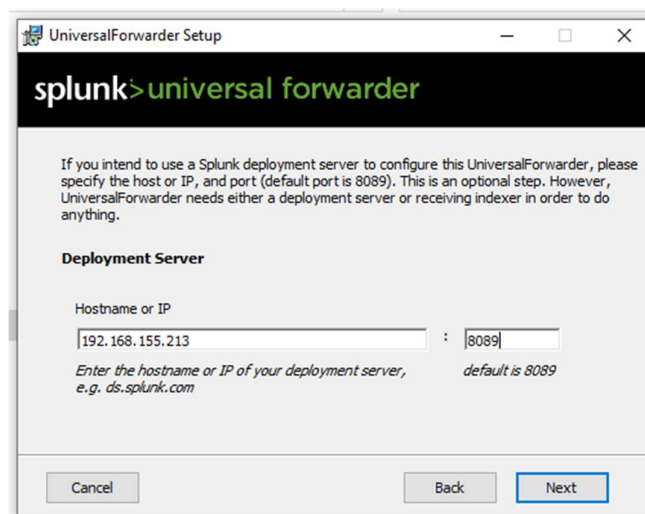
Provide a **username** and **password** for the Forwarder. I would recommend using the same credentials that were configured on Splunk.



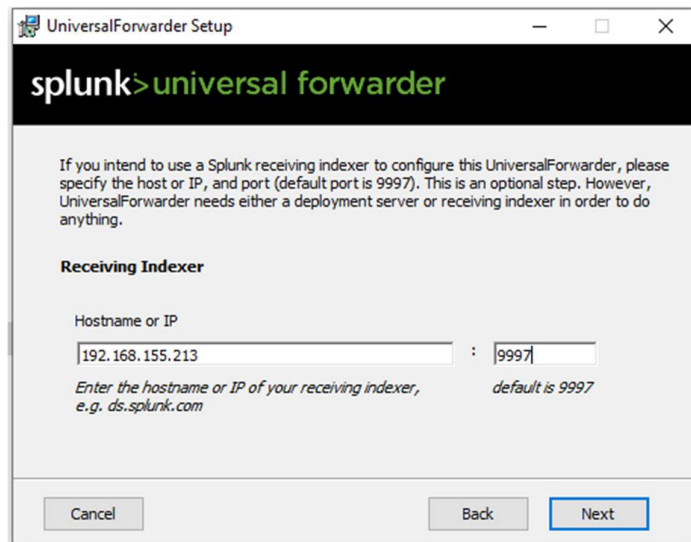
Check ip address of ubuntu for providing on next step

```
gopal@gopal-VMware-Virtual-Platform: ~/Desktop
gopal@gopal-VMware-Virtual-Platform:~/Desktop$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:d1:b7:18 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.155.213/24 brd 192.168.155.255 scope global dynamic noprefixroute ens33
        valid_lft 3526sec preferred_lft 3526sec
    inet6 2401:4900:7fa5:ebd7:ff58:8e0b:3a31:5eb9/64 scope global temporary dynamic
        valid_lft 7129sec preferred_lft 7129sec
    inet6 2401:4900:7fa5:ebd7:20c:29ff:fed1:b718/64 scope global dynamic mngtmpa
        valid_lft 7129sec preferred_lft 7129sec
    inet6 fe80::20c:29ff:fed1:b718/64 scope link
        valid_lft forever preferred_lft forever
gopal@gopal-VMware-Virtual-Platform:~/Desktop$
```

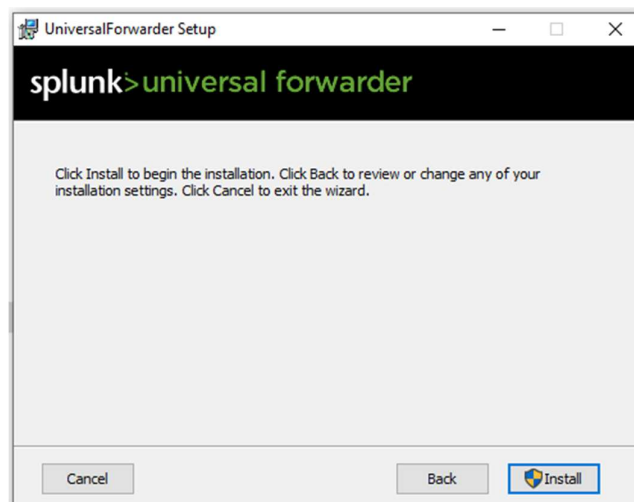
Now add ip address and default port 8089



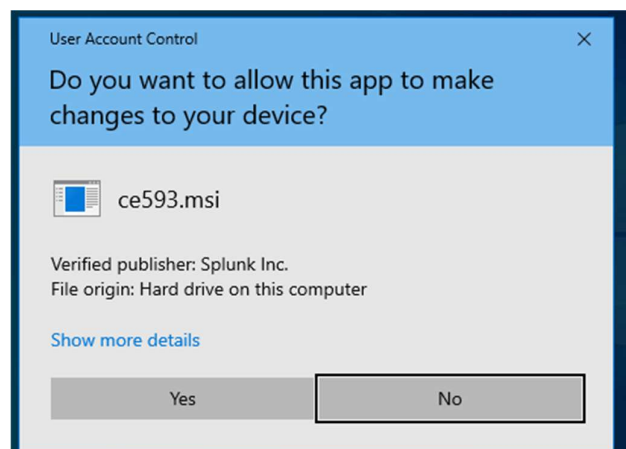
Also provide on this step ip address but default port number is changed 9997



Click on **Install**.



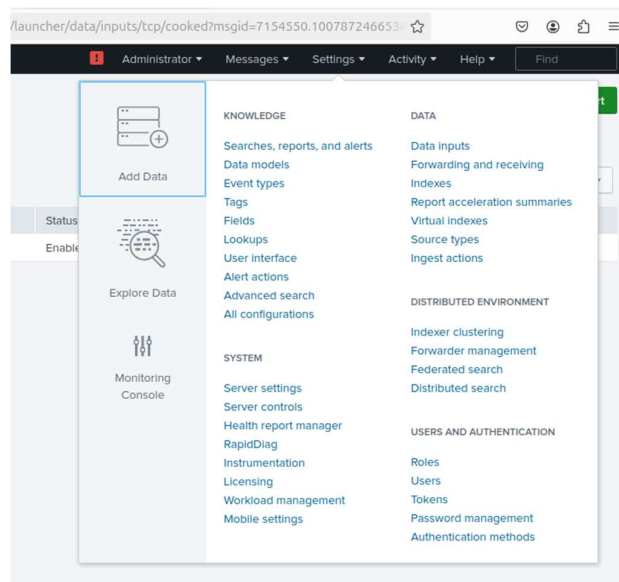
If prompt is shown then click **yes**



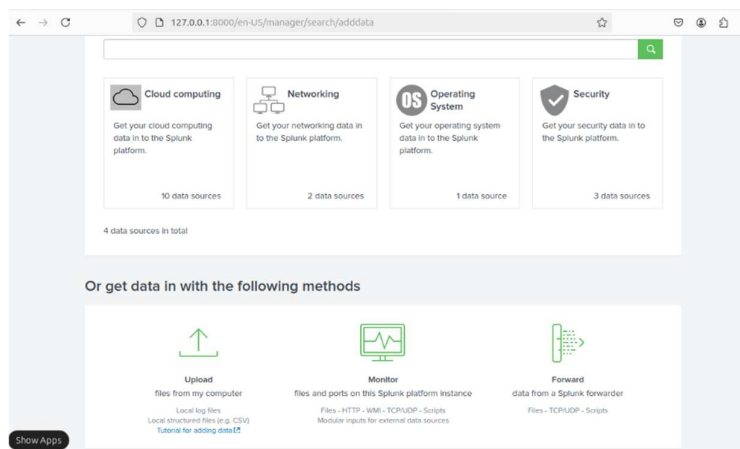
Click on **Finish** button.



Return to splunk enterprise then click on **settings** and **add data**

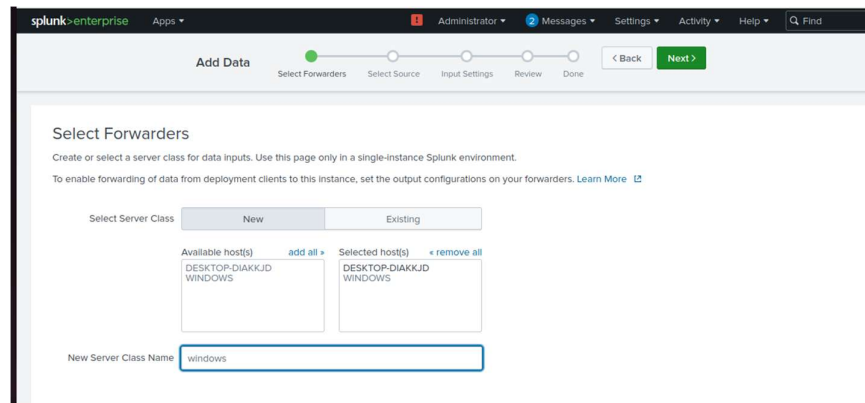


Click on **forward** option.

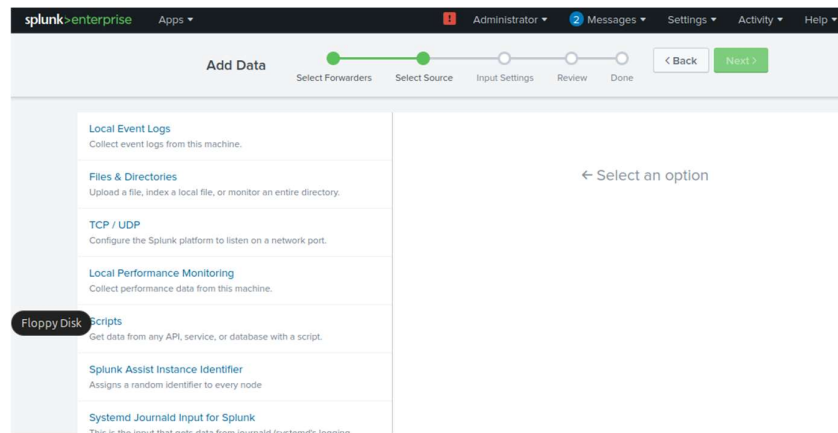




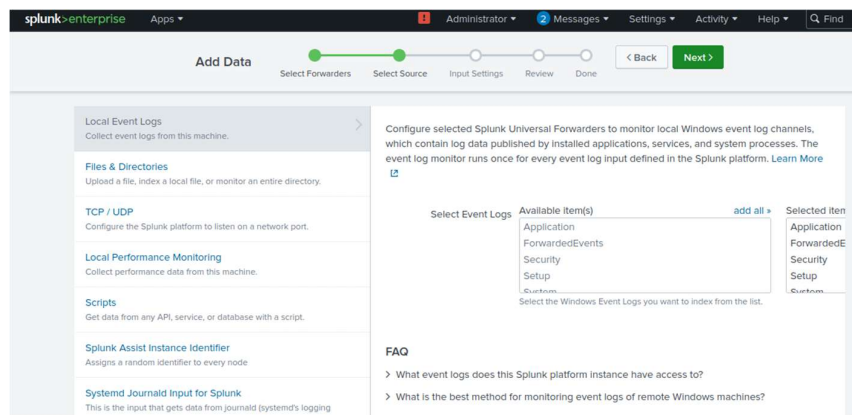
Our windows VM should automatically show up in the left box. Click on “**add all**” to move it to the right side. In the “**New Source Class Name**” field provide a name for the source. Click on **Next** to continue.



Click on **local Event logs**.



then click on the “**add all**” button above the dropdown field to ingest all the logs generated by the DC. Click on **Next** once done.



Click on “**Create a new index**”. Indexes are the Splunk equivalent of SQL Tables. It is used to store similar data.

Provide the Index a name. Keep all the other fields on their default value and click on **Save**.

then click on **Review**.

Click on **submit** button.

**Add Data**

Select Forwarders   Select Source   Input Settings   **Review**   Done

**Review**

Server Class Name ..... windows

List of Forwarders ..... WINDOWS I DESKTOP-DIAKKJD

Collection Name ..... localhost

Input Type ..... Windows Event Logs

Event Logs ..... Application, ForwardedEvents, Security, Setup, System

Index ..... windows

< Back   **Submit** >

Then this prompt shows

**Add Data**

Select Forwarders   Select Source   Input Settings   Review   Done

< Back   **Next** >

✓ **Local event logs input has been created successfully.**

Configure your inputs by going to [Settings > Data inputs](#)

**Start Searching** Search your data now or see [examples and tutorials](#).

**Add More Data** Add more data inputs now or see [examples and tutorials](#).

**Download Apps** Apps help you do more with your data. [Learn more](#).

**Build Dashboards** Visualize your searches. [Learn more](#).

From the Splunk toolbar select **Apps -> Search & Reporting**.

Then search like this **index="windows"** then it shows like this and shows logs.

**splunk>enterprise**   Apps   Administrator   Messages   Settings   Activity   Help   Find

Search   Analytics   Datasets   Reports   Alerts   Dashboards   **Search & Reporting**

**New Search**   Save As   Create Table View   Close

index="windows"   Last 24 hours   Search

✓ 461 events (4/4/25 7:30:00.000 AM to 4/5/25 8:23:39.000 AM)   No Event Sampling   Job   Fast Mode

Events (461)   Patterns   Statistics   Visualization

Format Timeline   Zoom Out   Zoom to Selection   Deselect   1 hour per column

List   Format   20 Per Page   Prev   1   2   3   4   5   6   7   8   Next

i	Time	Event
>	4/5/25 8:23:00.000 AM	LogName=Security EventCode=4634 EventType=0 ComputerName=DESKTOP-DIAKKJD Show all 22 lines host = DESKTOP-DIAKKJD   source = WinEventLogSecurity   sourcetype = WinEventLogSecurity
>	4/5/25 8:22:53.000 AM	LogName=Security EventCode=4672

< Hide Fields   All Fields   SELECTED FIELDS   INTERESTING FIELDS   + Extract New Fields

Now I am performing bruteforce attack on windows using rdp port so check ip address of windows

