This Document will guide you about how you can install the ubuntu server and Splunk on the ubuntu server. Ubuntu is a great distribution of Linux, used for many tasks. Splunk is licensed SIEM solutions used by many cybersecurity firms and multinational Organizations.

Objective: -

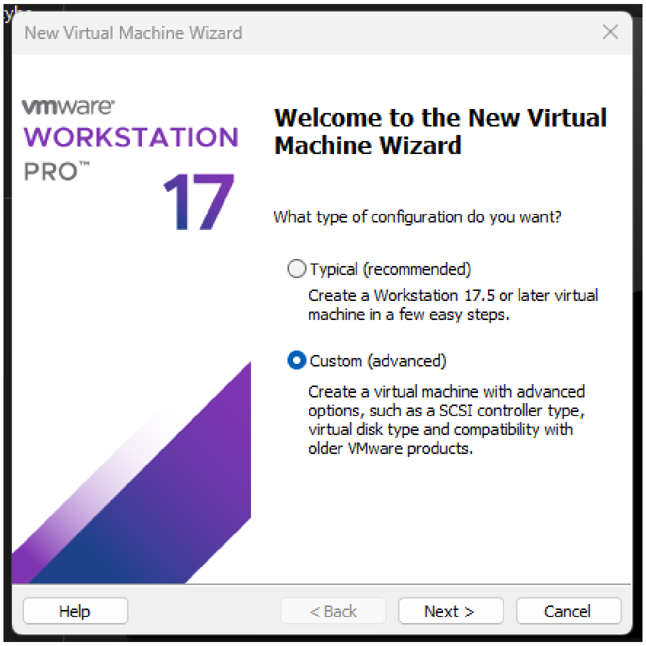
Installing Ubuntu on VMware workstations.

Installing Splunk on ubuntu server using command line.

Installing Ubuntu: -

1. Go to the ubuntu website and download the latest ubuntu live server image. Here is the link for iso download: - https://ubuntu.com/download/server

2. Now, head to VMware workstation>click file> new virtual machine > Custom.



New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

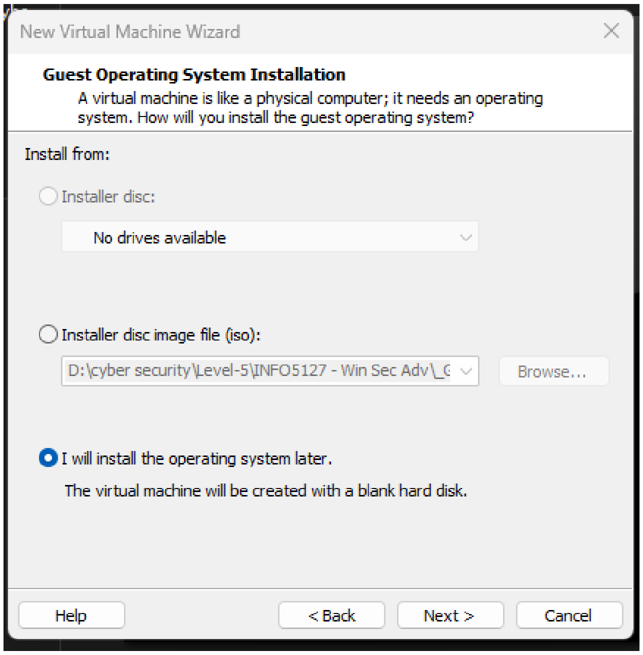
○ Typical (recommended)

Create a Workstation 17.5 or later virtual machine in a few easy steps.

● Custom (advanced)

Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

3. Click the latest workstation version > Click Next > I will install the operating system later.



Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

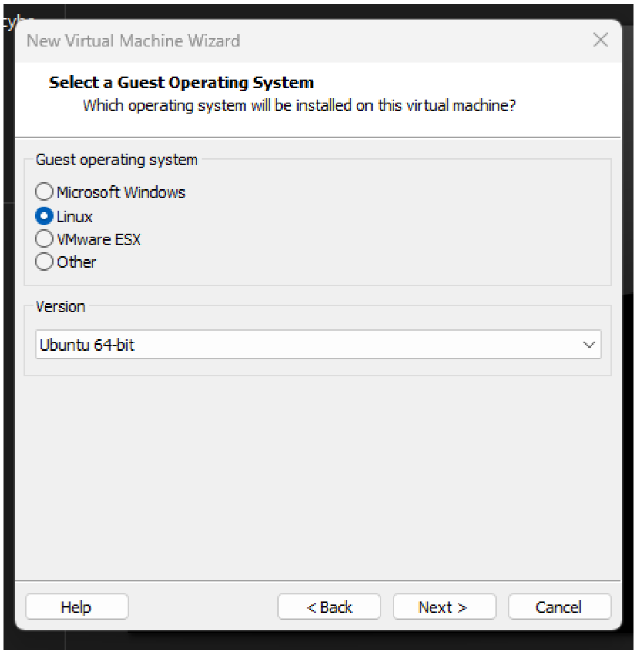
○ Installer disc image file (iso):

D:\cyber security\Level-5\INFO5127 - Win Sec Adv_C

● I will install the operating system later.

The virtual machine will be created with a blank hard disk.

4. Select a guest operating system > Linux > Version Ubuntu 64-bit.



Select a Guest Operating System

Which operating system will be installed on this virtual machine?

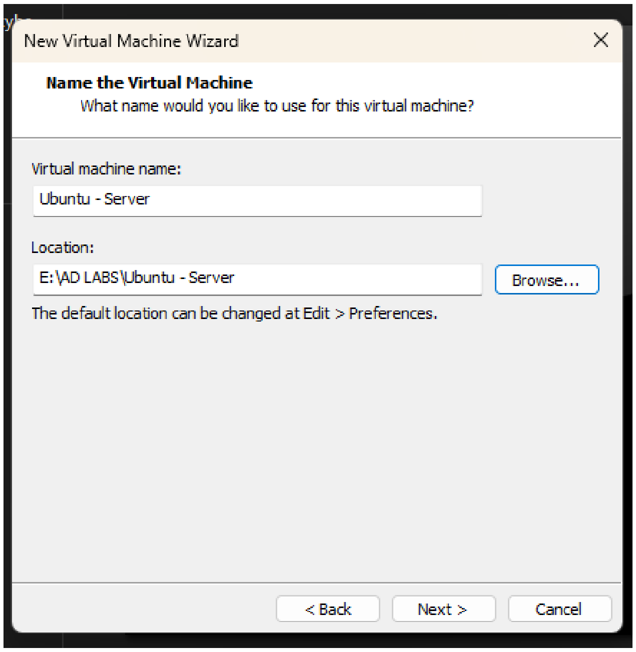
Guest operating system

○ Microsoft Windows
● Linux
○ VMware ESX
○ Other

Version

Ubuntu 64-bit

5. Give a virtual machine name and location to save the virtual machine.


New Virtual Machine Wizard

Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name:

Ubuntu - Server

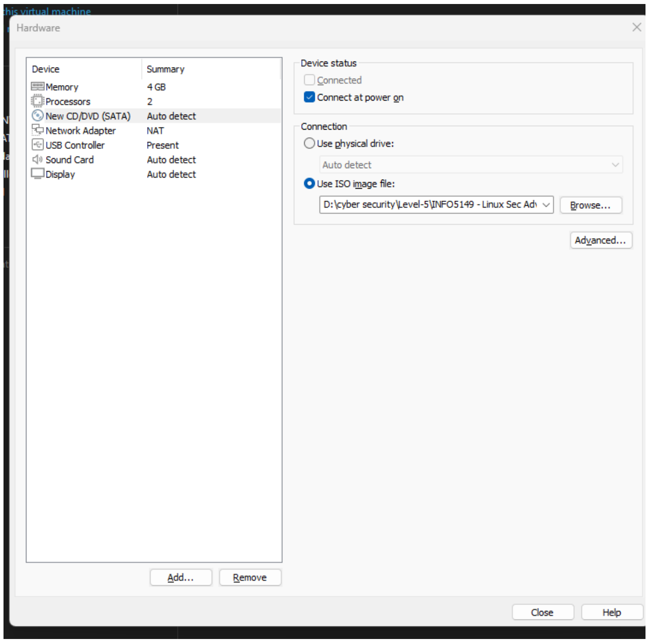
Location:

E:\AD LABS\Ubuntu - Server

The default location can be changed at Edit > Preferences.

6. Give the 2 cores of processors > 4gb ram > Nat as a network type > everything as a default. For disk size it gives it about 40gb of ram.

7. Now click the customize hardware > CD/DVD > mount the ubuntu live server iso


Hardware

Device	Summary
Memory	4 GB
Processors	2
New CD/DVD (SATA)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

☐ Connected

☑ Connect at power on

Connection

○ Use physical drive:

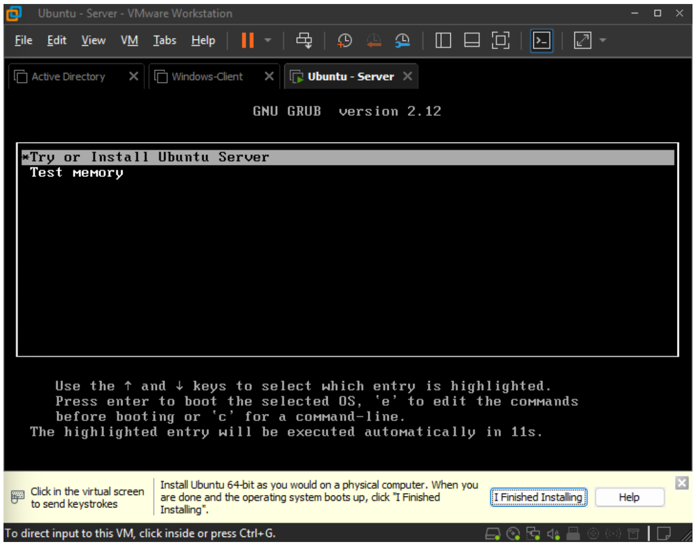
Auto detect

● Use ISO image file:

D:\cyber security\Level-5\INFO5149 - Linux Sec Adv

8. Now close the hardware customize dialog and power on the virtual machine. Wait for the machine to boot up.

9. Now click the try or install Ubuntu Server



```
                    GNU GRUB  version 2.12

 *Try or Install Ubuntu Server
  Test memory

     Use the ↑ and ↓ keys to select which entry is highlighted.
     Press enter to boot the selected OS, `e' to edit the commands
     before booting or `c' for a command-line.
  The highlighted entry will be executed automatically in 11s.
```

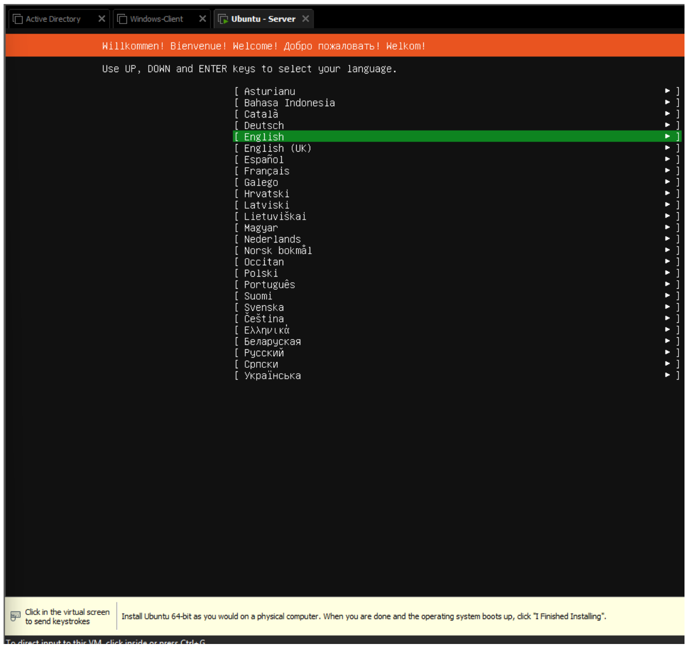
Click in the virtual screen to send keystrokes

Install Ubuntu 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".

To direct input to this VM, click inside or press Ctrl+G.

10. Wait for some background code to run.

11. Click the language as English or which suite you.



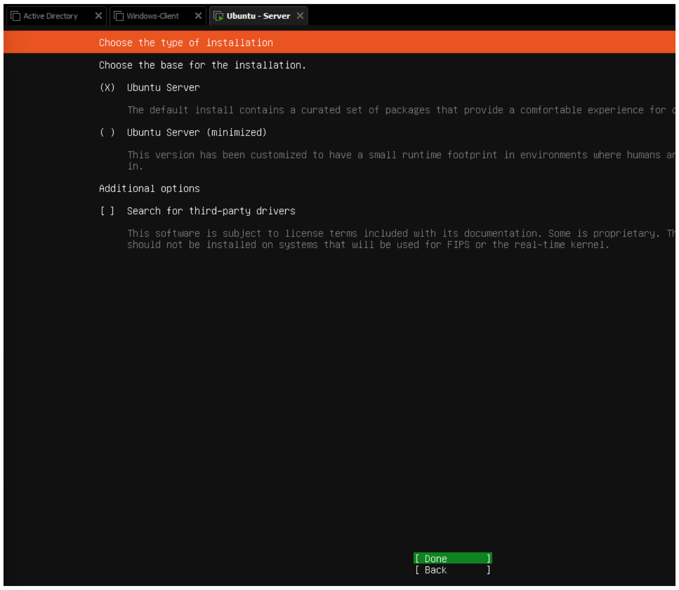
```
Willkommen! Bienvenue! Welcome! Добро пожаловать! Welkom!

Use UP, DOWN and ENTER keys to select your language.

                    [ Asturianu                              ▸ ]
                    [ Bahasa Indonesia                       ▸ ]
                    [ Català                                 ▸ ]
                    [ Deutsch                                ▸ ]
                    [ English                                ▸ ]
                    [ English (UK)                           ▸ ]
                    [ Español                                ▸ ]
                    [ Français                               ▸ ]
                    [ Galego                                 ▸ ]
                    [ Hrvatski                               ▸ ]
                    [ Latviski                               ▸ ]
                    [ Lietuviškai                            ▸ ]
                    [ Magyar                                 ▸ ]
                    [ Nederlands                             ▸ ]
                    [ Norsk bokmål                           ▸ ]
                    [ Occitan                                ▸ ]
                    [ Polski                                 ▸ ]
                    [ Português                              ▸ ]
                    [ Suomi                                  ▸ ]
                    [ Svenska                                ▸ ]
                    [ Čeština                                ▸ ]
                    [ Ελληνικά                               ▸ ]
                    [ Беларуская                             ▸ ]
                    [ Русский                                ▸ ]
                    [ Српски                                 ▸ ]
                    [ Українська                             ▸ ]
```

Click in the virtual screen to send keystrokes

Install Ubuntu 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".

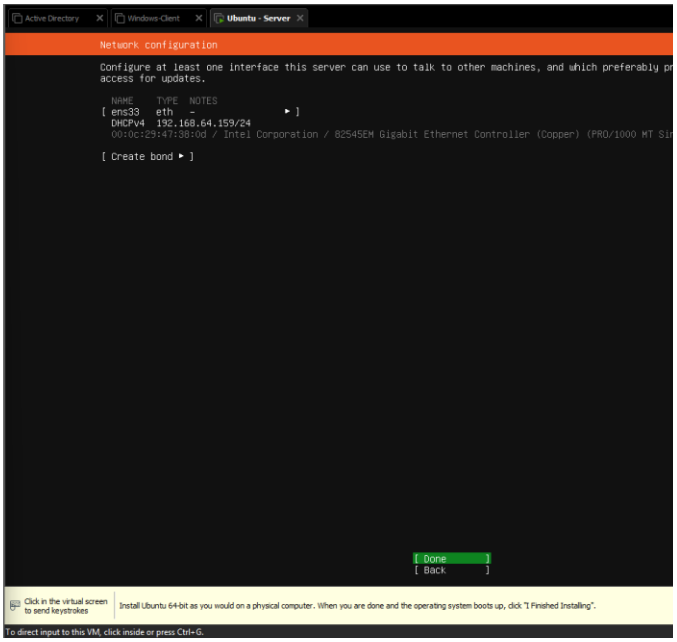
To direct input to this VM, click inside or press Ctrl+G.

12. Keep everything as default, until choose the based for the installation > click the ubuntu server (For click use space bar.)



```
Choose the type of installation

Choose the base for the installation.

(X)  Ubuntu Server

     The default install contains a curated set of packages that provide a comfortable experience for o

( )  Ubuntu Server (minimized)

     This version has been customized to have a small runtime footprint in environments where humans ar
     in.

Additional options

[ ]  Search for third-party drivers

     This software is subject to license terms included with its documentation. Some is proprietary. Th
     should not be installed on systems that will be used for FIPS or the real-time kernel.
```

13. Click done and you will see a network configuration page, wait for the dhcp server to give the ip address.



```
Network configuration

Configure at least one interface this server can use to talk to other machines, and which preferably pr
access for updates.

  NAME    TYPE  NOTES
[ ens33   eth   -                  ► ]
  DHCPv4  192.168.64.159/24
  00:0c:29:47:38:0d / Intel Corporation / 82545EM Gigabit Ethernet Controller (Copper) (PRO/1000 MT Sin

[ Create bond ► ]
```

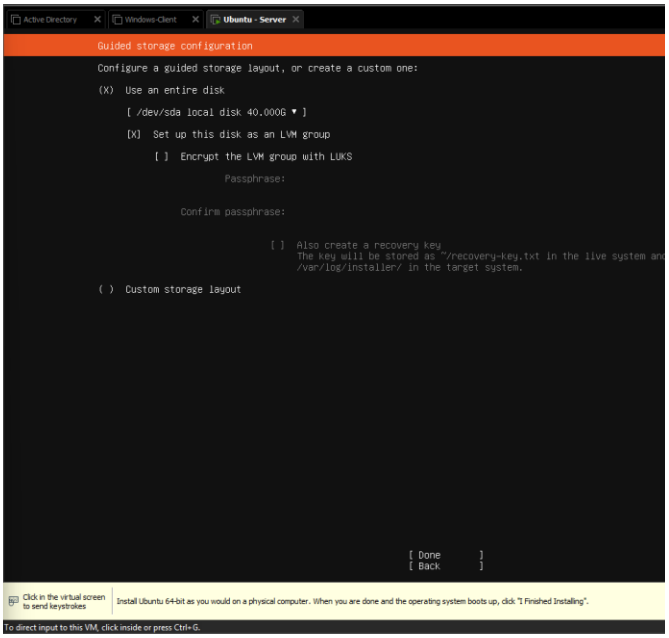
Click in the virtual screen to send keystrokes

Install Ubuntu 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".

To direct input to this VM, click inside or press Ctrl+G.

14. Don’t give proxy address, now click done for mirror configuration page.

15. Click the use an entire disk for disk storage configuration.



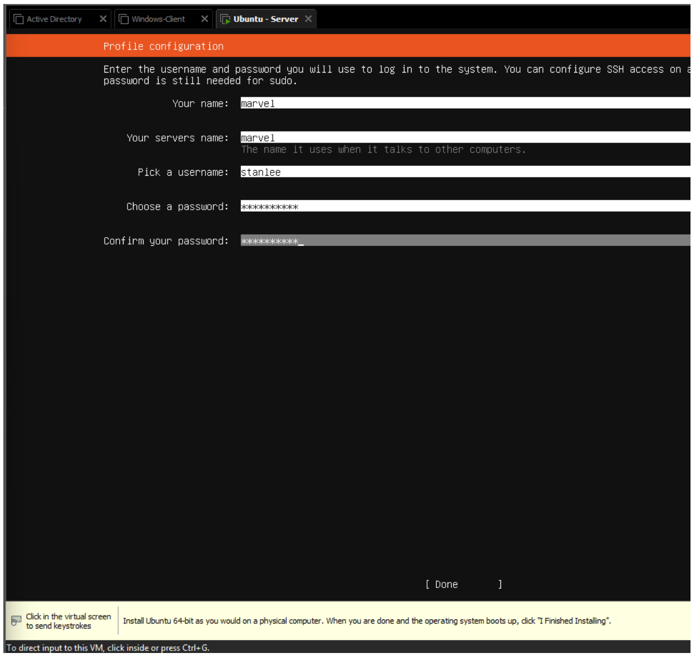
```
Guided storage configuration

Configure a guided storage layout, or create a custom one:

(X)  Use an entire disk

       [ /dev/sda local disk 40.000G ▾ ]

       [X]  Set up this disk as an LVM group

            [ ]  Encrypt the LVM group with LUKS

                        Passphrase:


                 Confirm passphrase:


                                  [ ]  Also create a recovery key
                                       The key will be stored as ~/recovery-key.txt in the live system and
                                       /var/log/installer/ in the target system.

( )  Custom storage layout
```

Click in the virtual screen to send keystrokes

Install Ubuntu 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".

To direct input to this VM, click inside or press Ctrl+G.

16. Click everything as a default, now you will see profile configuration. Give name, username and password.



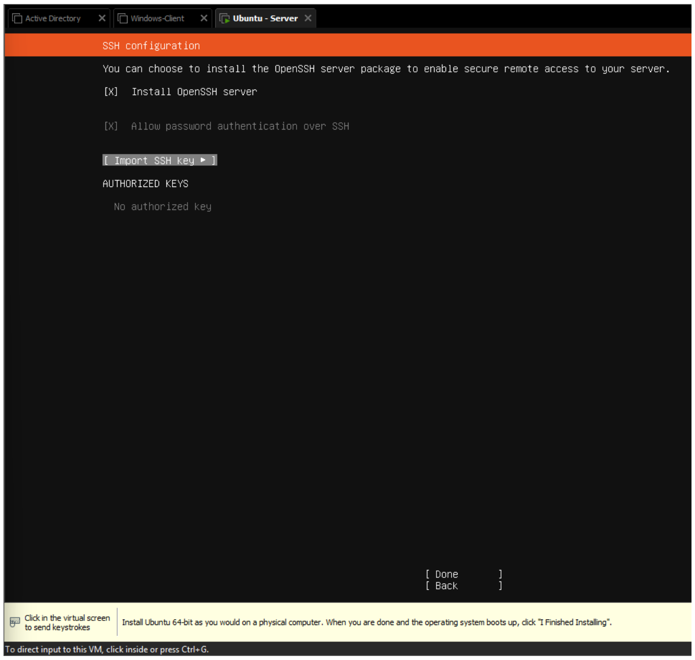
```
Profile configuration

Enter the username and password you will use to log in to the system. You can configure SSH access on a
password is still needed for sudo.

           Your name: marvel

   Your servers name: marvel
                      The name it uses when it talks to other computers.

     Pick a username: stanlee

   Choose a password: **********

Confirm your password: **********_
```

Click in the virtual screen to send keystrokes

Install Ubuntu 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".

To direct input to this VM, click inside or press Ctrl+G.

17. Click the install OpenSSH Server and click done.



```
SSH configuration

You can choose to install the OpenSSH server package to enable secure remote access to your server.

[X]  Install OpenSSH server

[X]  Allow password authentication over SSH

[ Import SSH key ► ]

AUTHORIZED KEYS

  No authorized key

                                                      [ Done       ]
                                                      [ Back       ]
```

Click in the virtual screen to send keystrokes

Install Ubuntu 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".

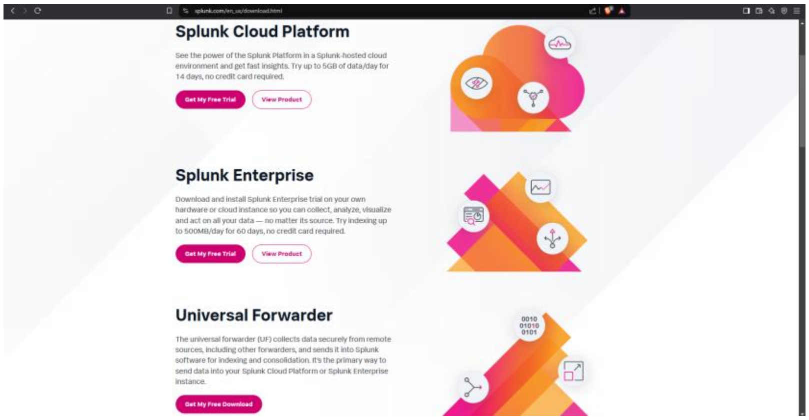
To direct input to this VM, click inside or press Ctrl+G.

18. Install any other software if you want to, if not click done and wait for the server to install it.

Downloading Splunk

1. Go to the Splunk official website using any web browser of your choice. Website: https://www.splunk.com/

2. Head to the products page.



Splunk Cloud Platform

See the power of the Splunk Platform in a Splunk-hosted cloud environment and get fast insights. Try up to 5GB of data/day for 14 days, no credit card required.

Splunk Enterprise

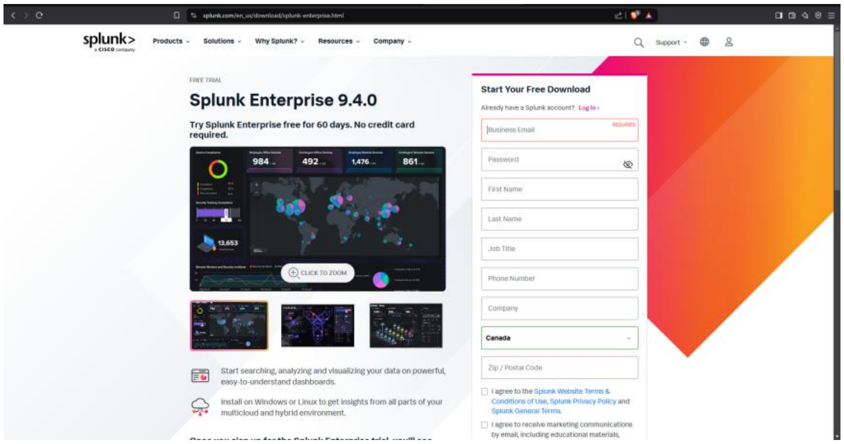
Download and install Splunk Enterprise trial on your own hardware or cloud instance so you can collect, analyze, visualize and act on all your data — no matter its source. Try indexing up to 500MB/day for 60 days, no credit card required.

Universal Forwarder

The universal forwarder (UF) collects data securely from remote sources, including other forwarders, and sends it into Splunk software for indexing and consolidation. It's the primary way to send data into your Splunk Cloud Platform or Splunk Enterprise instance.

3. Under the Splunk enterprise, click the get free trial button.

4. After clicking the free trial button, you will be forwarded to fill up a form.



FREE TRIAL

Splunk Enterprise 9.4.0

Try Splunk Enterprise free for 60 days. No credit card required.

Start searching, analyzing and visualizing your data on powerful, easy-to-understand dashboards.

Install on Windows or Linux to get insights from all parts of your multicloud and hybrid environment.

Start Your Free Download

Already have a Splunk account? Log In ›

Business Email REQUIRED

Password

First Name

Last Name

Job Title

Phone Number

Company

Canada

Zip / Postal Code

□ I agree to the Splunk Website Terms & Conditions of Use, Splunk Privacy Policy and Splunk General Terms.

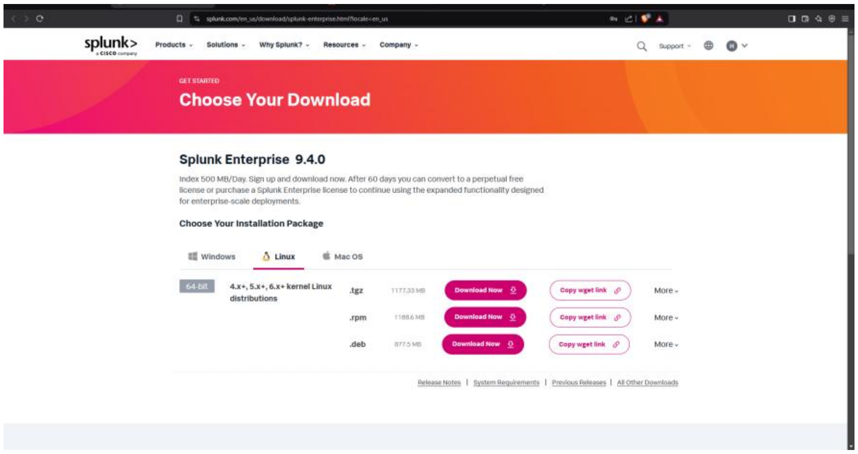
□ I agree to receive marketing communications by email, including educational materials,

5. Fill the form, click to create an account

6. Verify account using email id you provided.

7. After verifying, you will be redirected to download now button.

8. In the download page, click the Linux operating system.



GET STARTED

Choose Your Download

Splunk Enterprise 9.4.0

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

Windows | Linux | Mac OS

64-bit	4.x+, 5.x+, 6.x+ kernel Linux distributions	.tgz	1177.33 MB	Download Now	Copy wget link	More
		.rpm	1188.6 MB	Download Now	Copy wget link	More
		.deb	877.5 MB	Download Now	Copy wget link	More

Release Notes | System Requirements | Previous Releases | All Other Downloads

9. Now click the copy wget link for .deb install and copy the wget link.

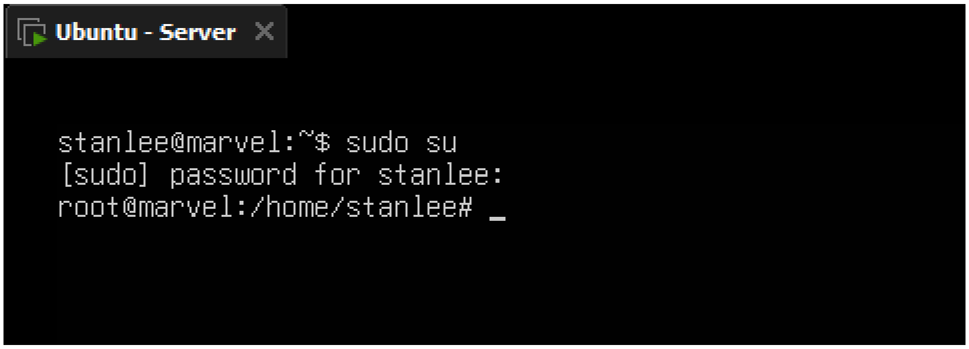
Installing Splunk in Ubuntu.

1. Head to VMware workstation, reboot the ubuntu.

2. Wait for the ubuntu machine to reboot.

3. After the vm is rebooted, login to the machine using the username you created earlier.

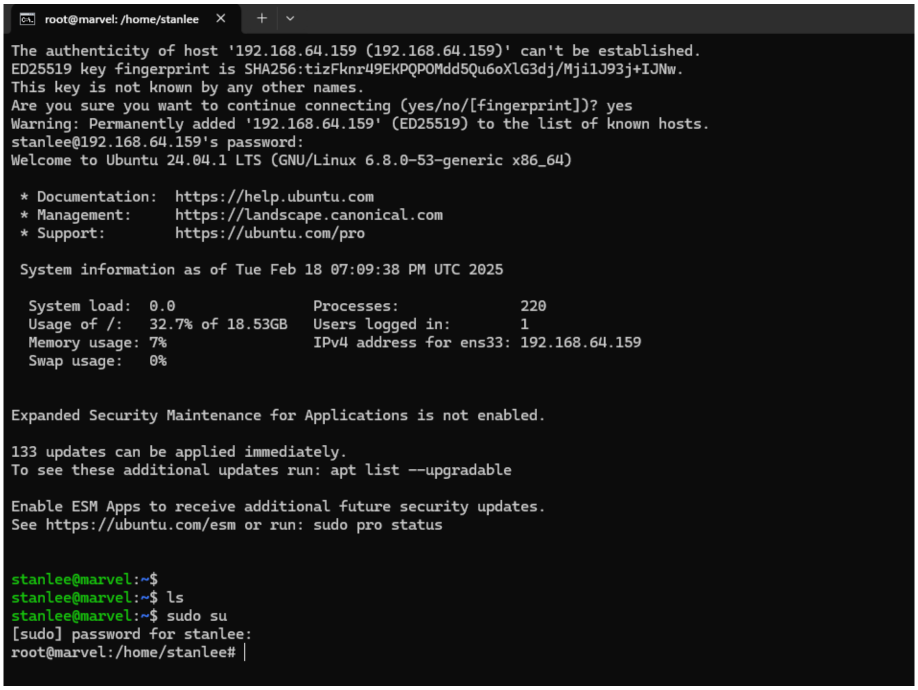
4. After login to the machine, use the sudo su command to get root.



```
stanlee@marvel:~$ sudo su
[sudo] password for stanlee:
root@marvel:/home/stanlee# _
```

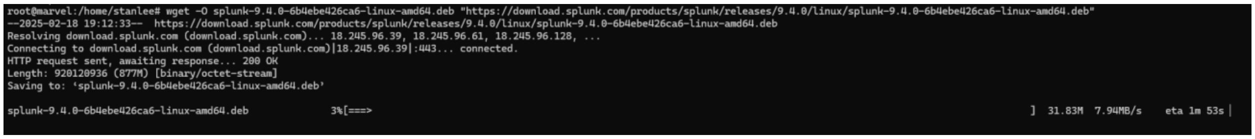
5. Paste the command you copied earlier using Ctrl + shift + V. now if you are unable to copy. SSH the machine for the host.

6. Ssh the machine from the host. Open command prompt in host. Note the virtual machine ip address. Use the command ssh username@ip-address. *Sudo su* for root access.



```
The authenticity of host '192.168.64.159 (192.168.64.159)' can't be established.
ED25519 key fingerprint is SHA256:tizFknr49EKPQPOMdd5Qu6oXlG3dj/Mji1J93j+IJNw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.64.159' (ED25519) to the list of known hosts.
stanlee@192.168.64.159's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-53-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Tue Feb 18 07:09:38 PM UTC 2025

  System load:  0.0               Processes:               220
  Usage of /:   32.7% of 18.53GB  Users logged in:         1
  Memory usage: 7%                IPv4 address for ens33: 192.168.64.159
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

133 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


stanlee@marvel:~$
stanlee@marvel:~$ ls
stanlee@marvel:~$ sudo su
[sudo] password for stanlee:
root@marvel:/home/stanlee# |
```

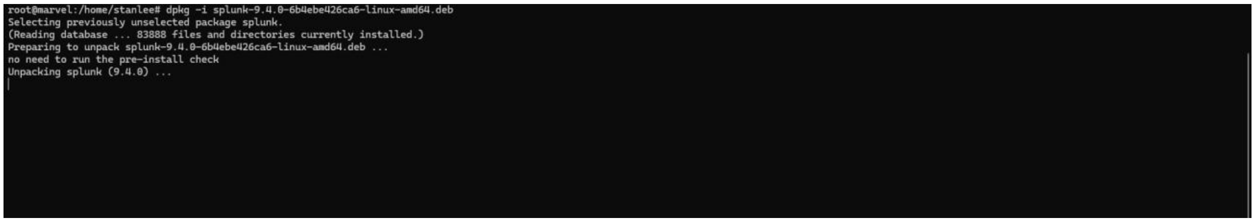
7. Now the paste the command you copied earlier.



```
root@marvel:/home/stanlee# wget -O splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb "https://download.splunk.com/products/splunk/releases/9.4.0/linux/splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb"
--2025-02-18 19:12:33--  https://download.splunk.com/products/splunk/releases/9.4.0/linux/splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 18.245.96.39, 18.245.96.61, 18.245.96.128, ...
Connecting to download.splunk.com (download.splunk.com)|18.245.96.39|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 920120936 (877M) [binary/octet-stream]
Saving to: ‘splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb’

splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb            3%[===>                                                                                      ]  31.83M  7.94MB/s    eta 1m 53s
```

8. Wait for the downloading process to be completed. After the downloading process is completed, use *ls* command to check for the downloaded file.

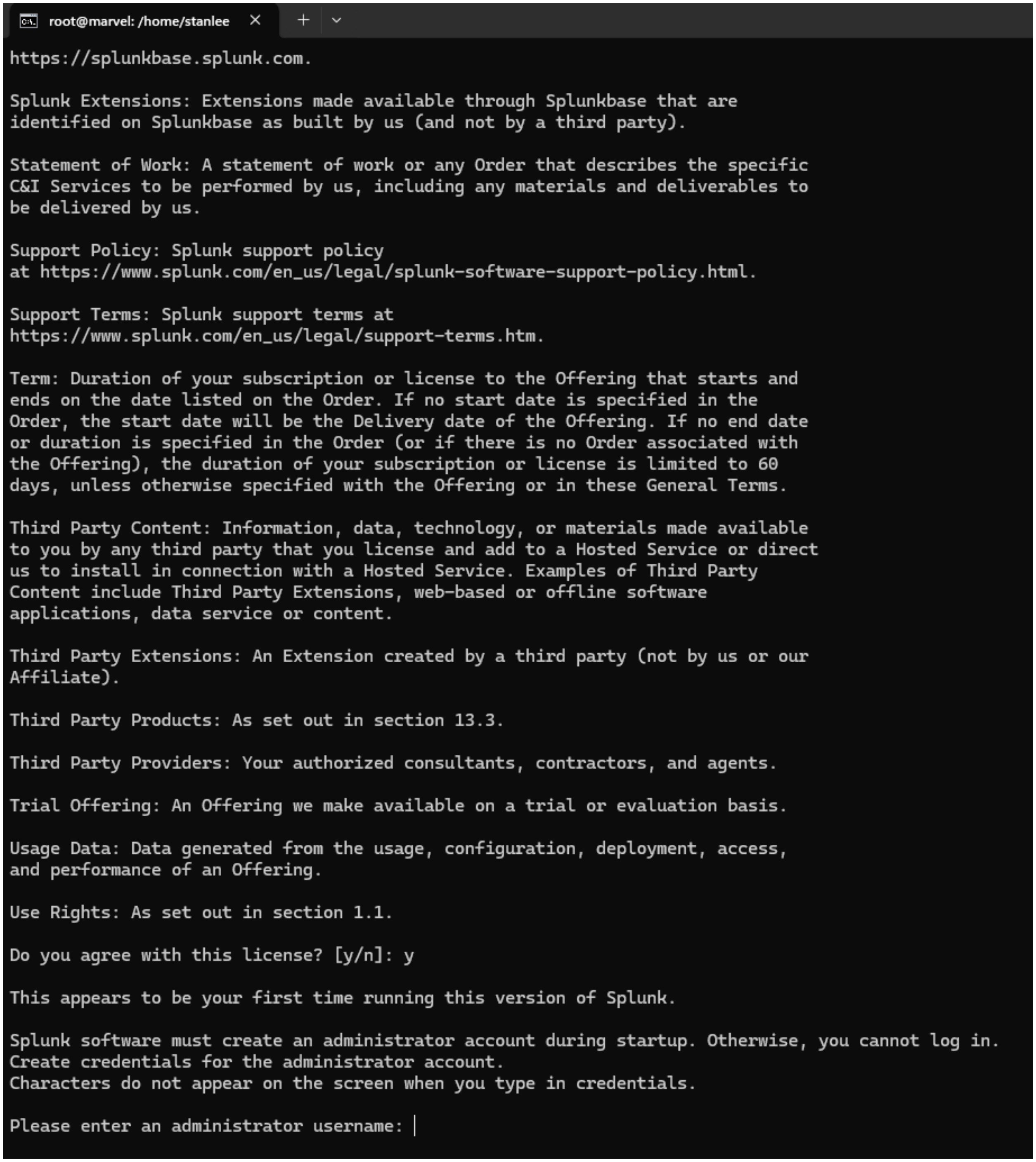
9. Now to install Splunk use *dpkg -i* splunk file command.



```
root@marvel:/home/stanlee# dpkg -i splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 83888 files and directories currently installed.)
Preparing to unpack splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb ...
no need to run the pre-install check
Unpacking splunk (9.4.0) ...
```

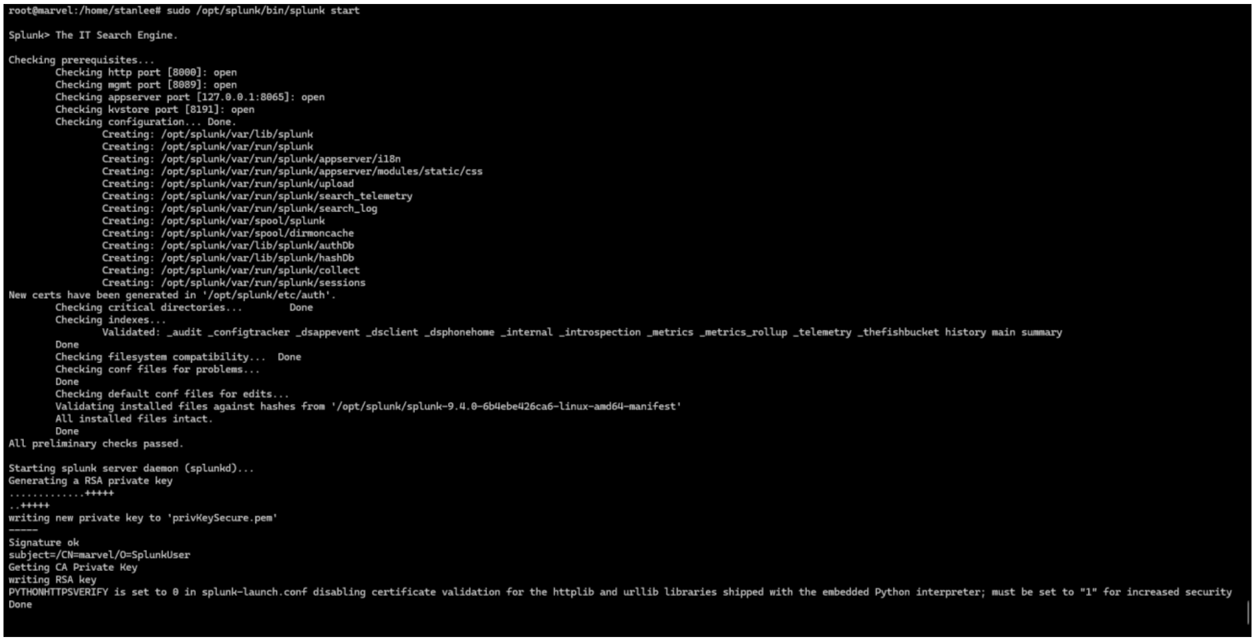
10. Wait for installation process to complete. Now after the installation is complete, using following command as next step. *sudo /opt/splunk/bin/splunk start — accept-license*

11. After using the command, you will be asked to confirm the term using y. a prompt will be appear to set the administrator username.



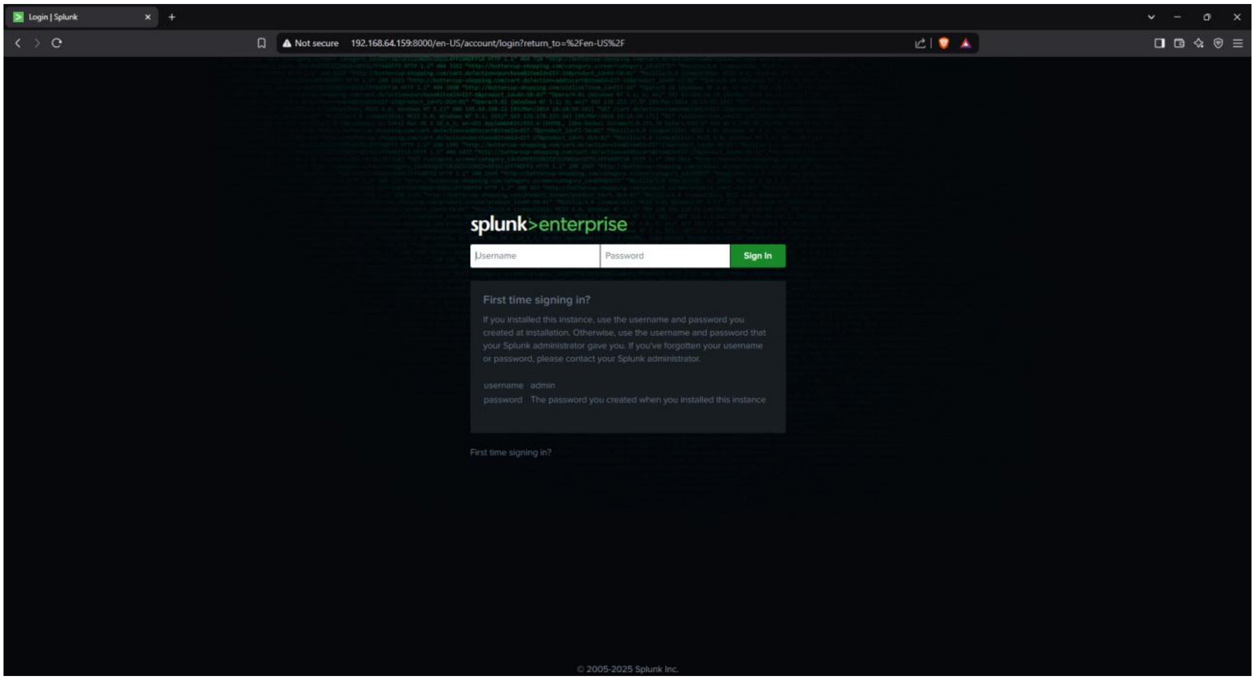
```
https://splunkbase.splunk.com.

Splunk Extensions: Extensions made available through Splunkbase that are
identified on Splunkbase as built by us (and not by a third party).

Statement of Work: A statement of work or any Order that describes the specific
C&I Services to be performed by us, including any materials and deliverables to
be delivered by us.

Support Policy: Splunk support policy
at https://www.splunk.com/en_us/legal/splunk-software-support-policy.html.

Support Terms: Splunk support terms at
https://www.splunk.com/en_us/legal/support-terms.htm.

Term: Duration of your subscription or license to the Offering that starts and
ends on the date listed on the Order. If no start date is specified in the
Order, the start date will be the Delivery date of the Offering. If no end date
or duration is specified in the Order (or if there is no Order associated with
the Offering), the duration of your subscription or license is limited to 60
days, unless otherwise specified with the Offering or in these General Terms.

Third Party Content: Information, data, technology, or materials made available
to you by any third party that you license and add to a Hosted Service or direct
us to install in connection with a Hosted Service. Examples of Third Party
Content include Third Party Extensions, web-based or offline software
applications, data service or content.

Third Party Extensions: An Extension created by a third party (not by us or our
Affiliate).

Third Party Products: As set out in section 13.3.

Third Party Providers: Your authorized consultants, contractors, and agents.

Trial Offering: An Offering we make available on a trial or evaluation basis.

Usage Data: Data generated from the usage, configuration, deployment, access,
and performance of an Offering.

Use Rights: As set out in section 1.1.

Do you agree with this license? [y/n]: y

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:
```

12. Give the administrator username and password. After setting username and password. Now we need to start the splunk.
13. Using command to start the splunk sudo */opt/splunk/bin/splunk start*



```
root@marvel:/home/stanlee# sudo /opt/splunk/bin/splunk start

Splunk> The IT Search Engine.

Checking prerequisites...
        Checking http port [8000]: open
        Checking mgmt port [8089]: open
        Checking appserver port [127.0.0.1:8065]: open
        Checking kvstore port [8191]: open
        Checking configuration... Done.
                Creating: /opt/splunk/var/lib/splunk
                Creating: /opt/splunk/var/run/splunk
                Creating: /opt/splunk/var/run/splunk/appserver/i18n
                Creating: /opt/splunk/var/run/splunk/appserver/modules/static/css
                Creating: /opt/splunk/var/run/splunk/upload
                Creating: /opt/splunk/var/run/splunk/search_telemetry
                Creating: /opt/splunk/var/run/splunk/search_log
                Creating: /opt/splunk/var/spool/splunk
                Creating: /opt/splunk/var/spool/dirmoncache
                Creating: /opt/splunk/var/lib/splunk/authDb
                Creating: /opt/splunk/var/lib/splunk/hashDb
                Creating: /opt/splunk/var/run/splunk/collect
                Creating: /opt/splunk/var/run/splunk/sessions
New certs have been generated in '/opt/splunk/etc/auth'.
        Checking critical directories...        Done
        Checking indexes...
                Validated: _audit _configtracker _dsappevent _dsclient _dsphonehome _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket history main summary
        Done
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunk/splunk-9.4.0-6b4ebe426ca6-linux-amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Generating a RSA private key
.............+++++
..+++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=marvel/O=SplunkUser
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done
```

14. Now head to web browser and use the url http://ip – address of vm :8000/



192.168.64.159:8000/en-US/account/login?return_to=%2Fen-US%2F

First time signing in?

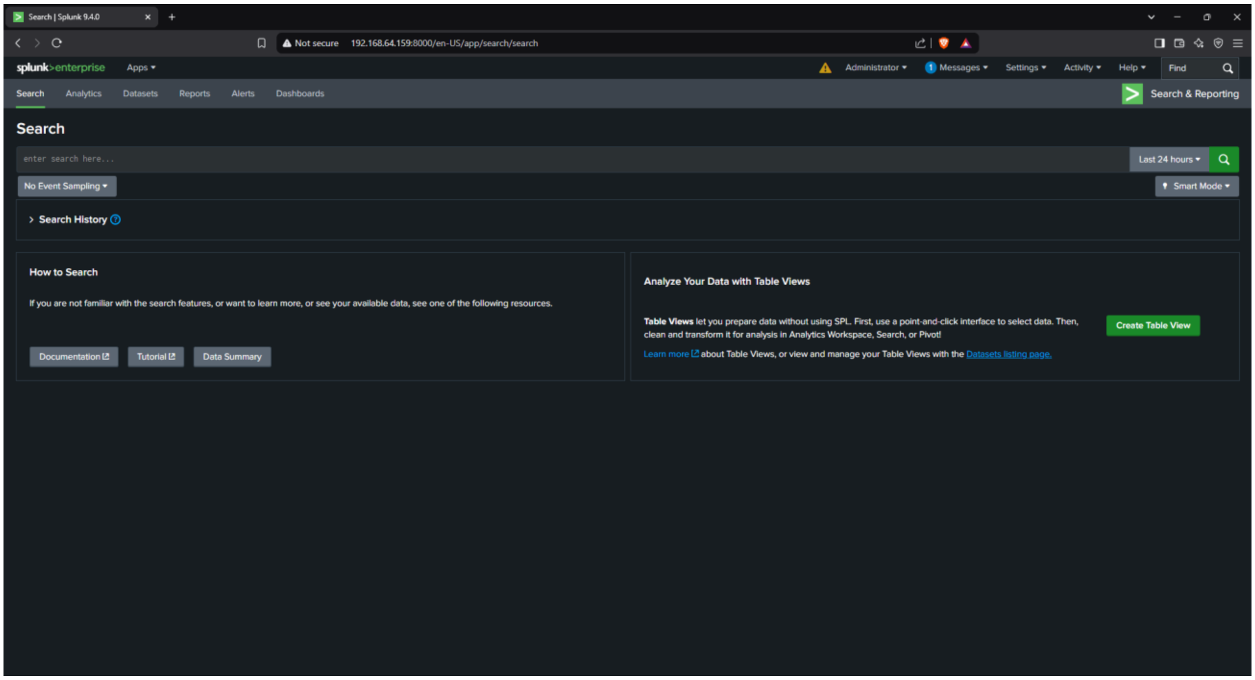
If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.

username admin
password The password you created when you installed this instance

First time signing in?

© 2005-2025 Splunk Inc.

15. Login using the administrator username and password we created earlier.



If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

I hope this guide will help you with the installation process. If you have any questions, you can ask me on my linkedin and email me. At info@byseciot.ca