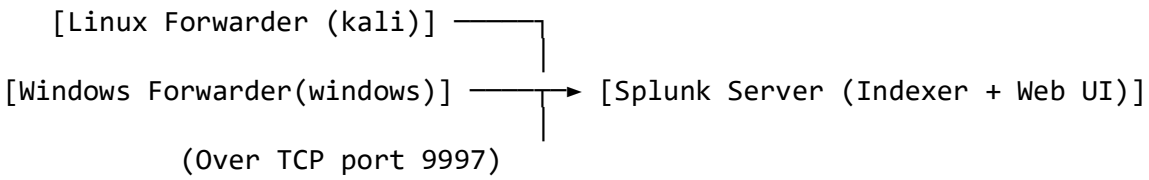
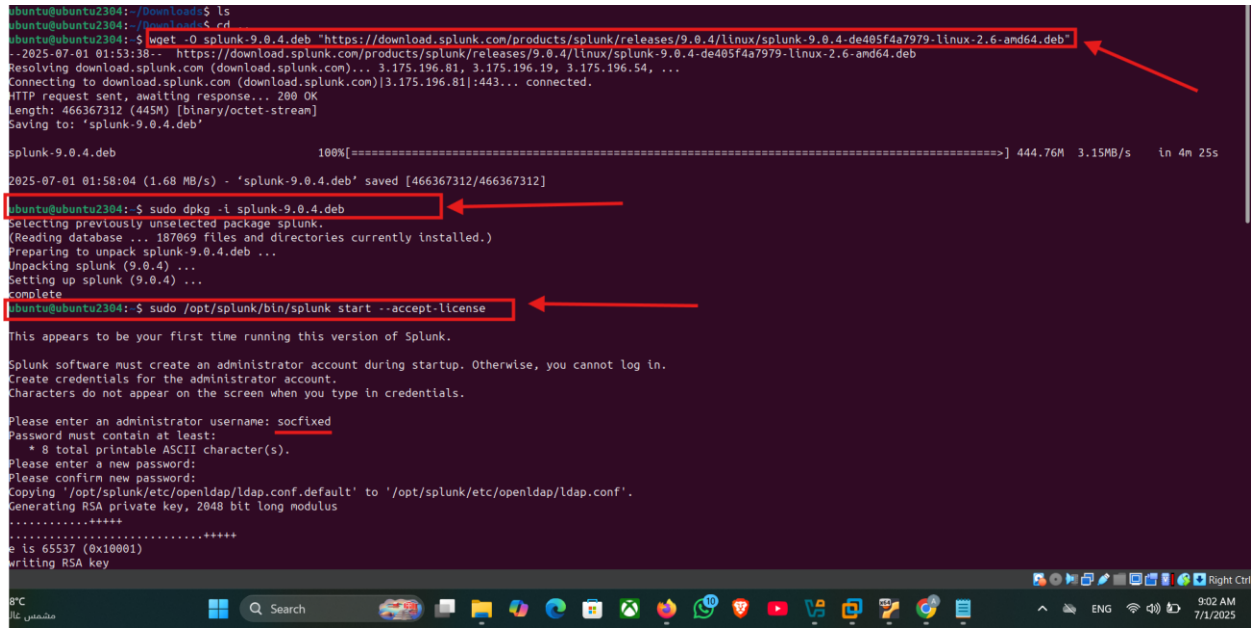
Splunk Deployment Documentation

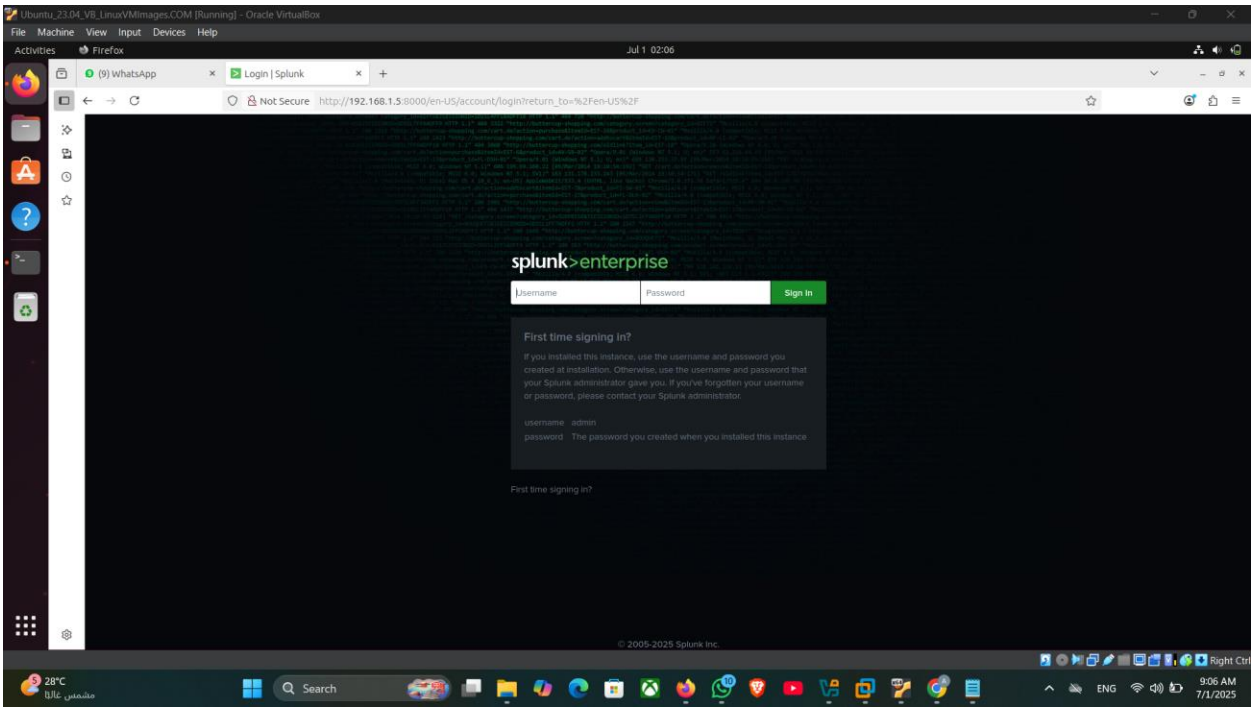
🖥️ Overview Diagram: 🖥️ Overview Diagram:

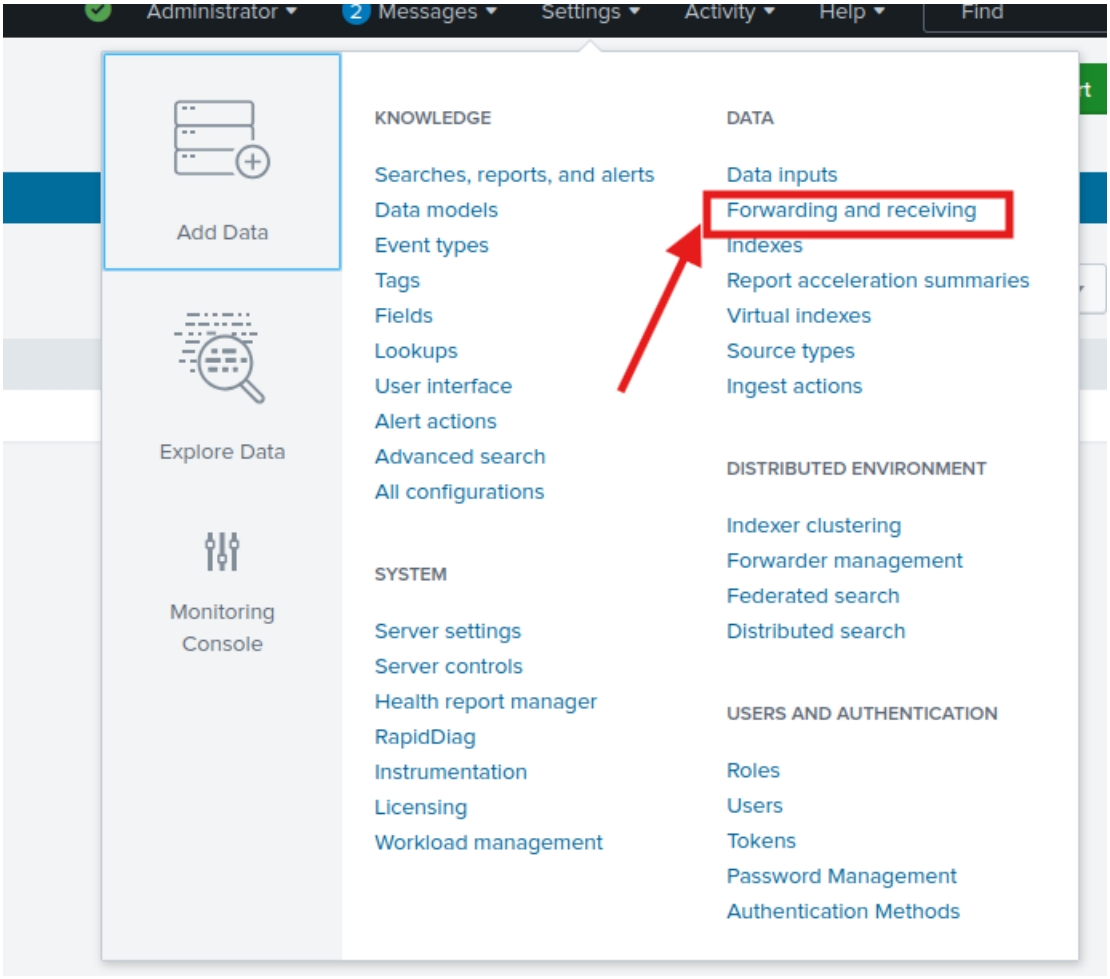


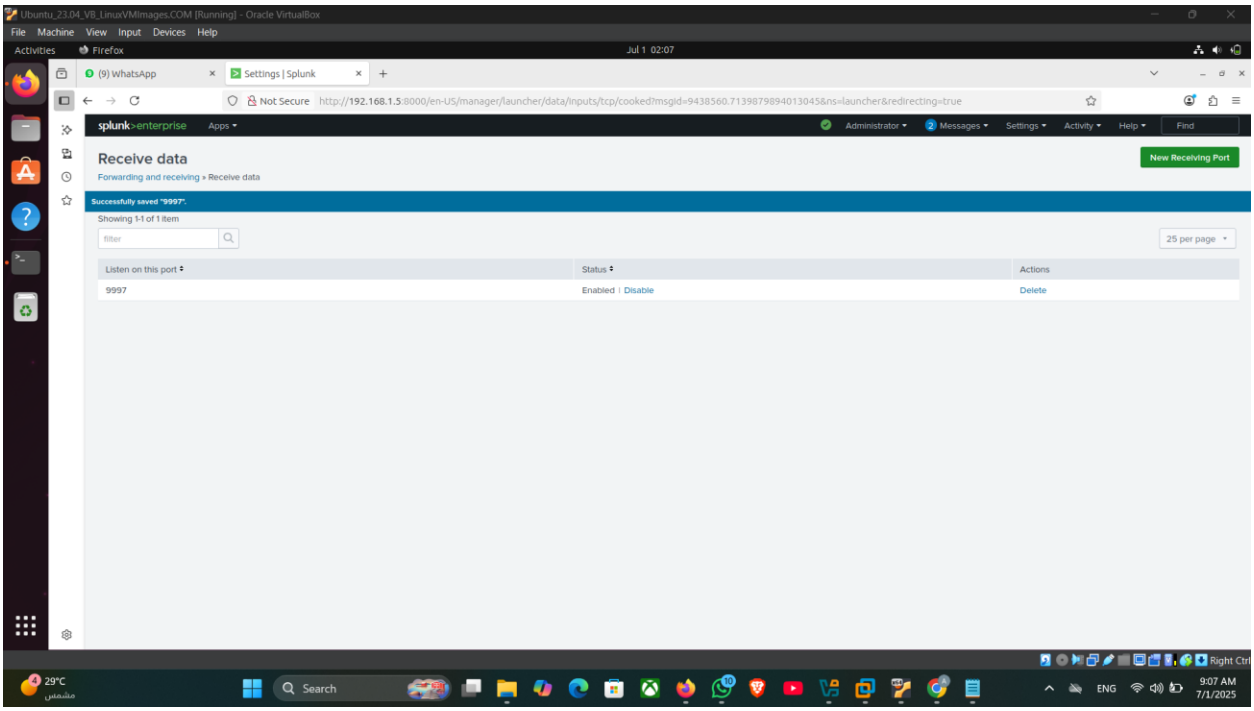
💻 Machine 1: Ubuntu (Splunk Server)

Step 1: Download & Install Splunk Enterprise
Step 2: Start Splunk & Accept License




Ubuntu_23.04_VB_LinuxVMImages.COM [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Firefox
Jul 1 02:06
(9) WhatsApp
Login | Splunk
Not Secure
http://192.168.1.5:8000/en-US/account/login?return_to=%2Fen-US%2F
splunk>enterprise
Username
Password
Sign In
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.
Right Ctrl
28°C
مشمس غالبًا
Search
ENG
9:06 AM
7/1/2025

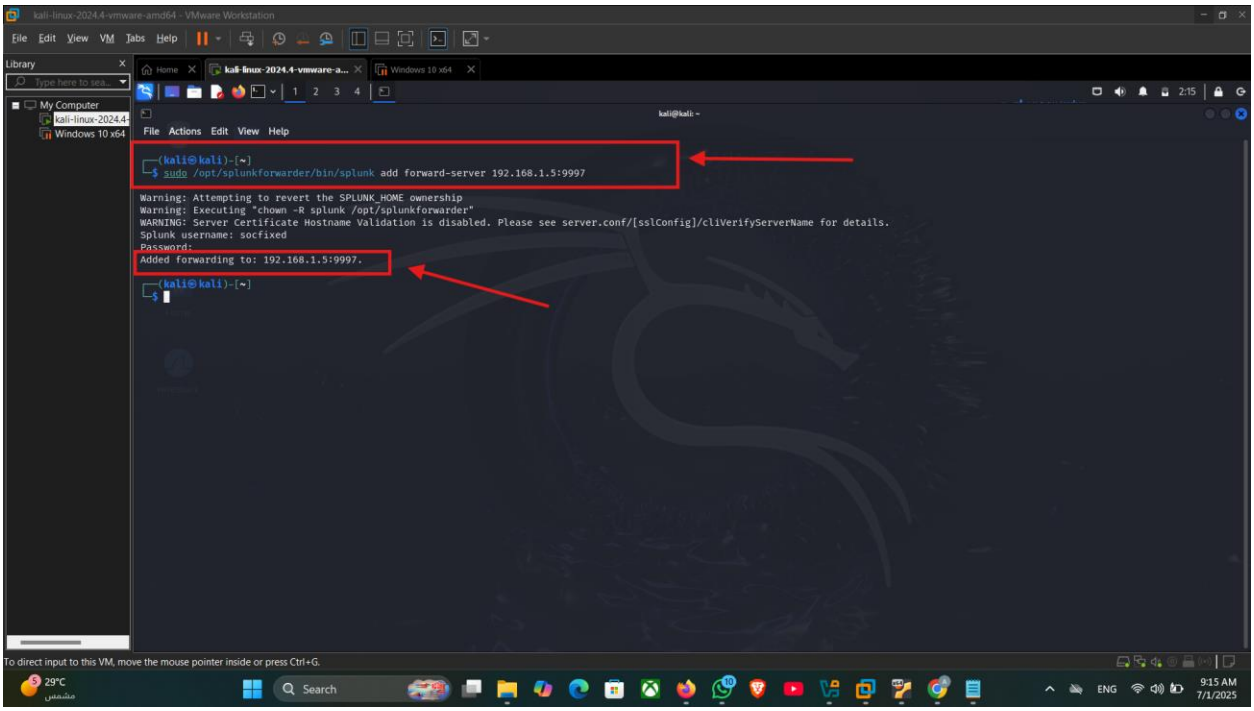

Administrator
2 Messages
Settings
Activity
Help
Find
Add Data
Explore Data
Monitoring Console
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
SYSTEM
Server settings
Server controls
Health report manager
RapidDiag
Instrumentation
Licensing
Workload management
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Virtual indexes
Source types
Ingest actions
DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Federated search
Distributed search
USERS AND AUTHENTICATION
Roles
Users
Tokens
Password Management
Authentication Methods

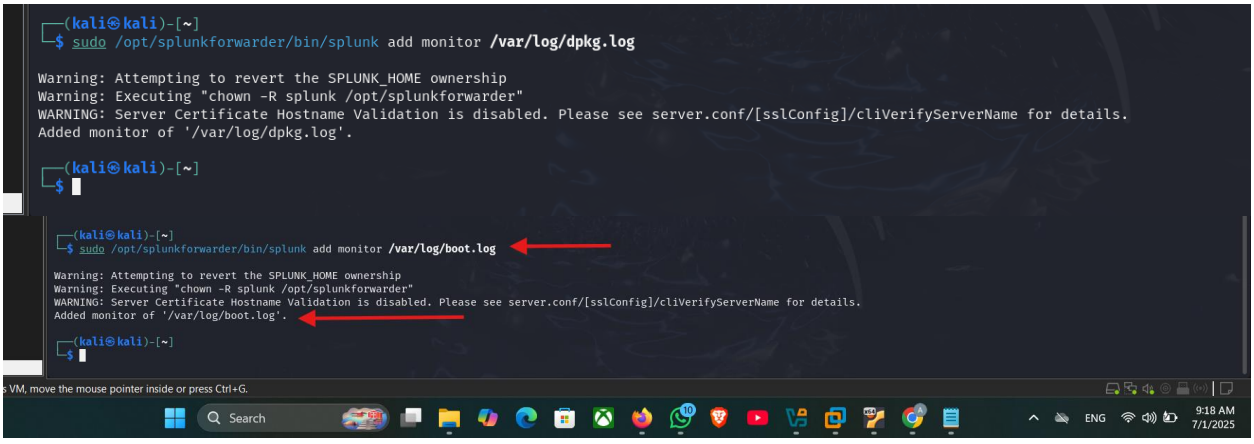


Machine 2: Linux Splunk Universal Forwarder (e.g., Kali Linux)

Step 1: Download & Install Forwarder Step 2: Start Forwarder & Accept License

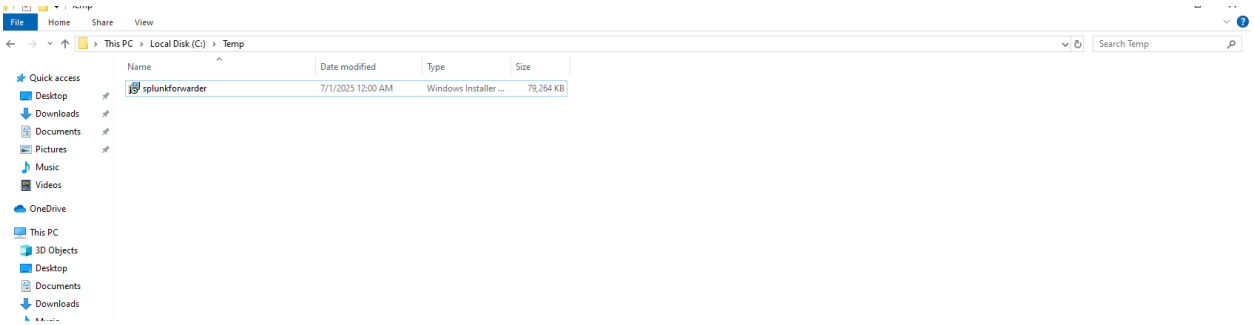
```
┌──(kali㉿kali)-[~]
└─$ wget -O splunkforwarder-9.0.4.deb "https://download.splunk.com/products/universalforwarder/releases/9.0.4/linux/splunkforwarder-9.0.4-de405f4a7979-linux-2.6-amd64.deb"

--2025-07-01 02:11:02--  https://download.splunk.com/products/universalforwarder/releases/9.0.4/linux/splunkforwarder-9.0.4-de405f4a7979-linux-2.6-amd64.deb
Resolving download.splunk.com (download.splunk.com)... ^[[B^[[B^[[B^[[B^[[B83.175.196.13, 3.175.196.19, 3.175.196.81, ...
Connecting to download.splunk.com (download.splunk.com)|3.175.196.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 32420798 (31M) [binary/octet-stream]
Saving to: 'splunkforwarder-9.0.4.deb'

splunkforwarder-9.0.4.deb                100%[=====================================================================>]  30.92M  3.43MB/s    in 8.9s

2025-07-01 02:11:17 (3.46 MB/s) - 'splunkforwarder-9.0.4.deb' saved [32420798/32420798]


┌──(kali㉿kali)-[~]
└─$ ls
 ALEAPP                          Downloads        malicious.exe      output_folder              smol_all_tcp_ports.nmap   Templates                          xlm.txt
'blocks.style.build.css%3fver=5.2.2'  hex_clean.txt    mdm_hex_dump.txt   Pictures                   smol_all_tcp_ports.xml    tx0abdo-Jr-Pentester-AD-v01.ovpn   xxxmmdcclxxxiv.ps1
 decode                          hex_output.txt   mdm.jpg            Public                     splunkforwarder-9.0.4.deb Videos
 Desktop                         hex_string.txt   Music              resources.dll              stream.raw                volatility
 Documents                       install.ps1      ncsi.txt           site.js                    _stream.raw.extracted     volatility3
 download.dat                    login.php        notepad.exe        smol_all_tcp_ports.gnmap   stuffit_part1.bin         volenv

┌──(kali㉿kali)-[~]
└─$ sudo dpkg -i splunkforwarder-9.0.4.deb

Selecting previously unselected package splunkforwarder.
(Reading database ... 401105 files and directories currently installed.)
Preparing to unpack splunkforwarder-9.0.4.deb ...
Unpacking splunkforwarder (9.0.4) ...
Setting up splunkforwarder (9.0.4) ...
complete

┌──(kali㉿kali)-[~]
└─$
```





Machine 3: Windows (Splunk Universal Forwarder)

Step 1: Download Forward & Connect to Splunk Server



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.5: bytes=32 time<1ms TTL=64
Reply from 192.168.1.5: bytes=32 time<1ms TTL=64
Reply from 192.168.1.5: bytes=32 time<1ms TTL=64
Reply from 192.168.1.5: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Windows\system32> dir C:\Temp


    Directory: C:\Temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/1/2025  12:00 AM       81166336 splunkforwarder.msi


PS C:\Windows\system32>
```

Final result :