

Splunk on Linux

Install Indexer / Heavy Forwarder

```
sudo useradd -m -d /opt/splunk splunk && \  
sudo chsh -s /bin/bash splunk && \  
sudo tar xzvf ~/splunk.tgz -C /opt && \  
sudo chown -R splunk:splunk /opt/splunk && \  
sudo su -c "/opt/splunk/bin/splunk start --accept-license" splunk
```

Configure Receiver to receive data

<https://docs.splunk.com/Documentation/Splunk/9.1.2/Forwarding/Enableareceiver>

```
sudo su -c "/opt/splunk/bin/splunk enable listen 9997 -auth admin:password
```

Set-Up Forwarding

```
export user=user  
export password=password  
export host=indexer  
export port=9997  
sudo su -c "/opt/splunk/bin/splunk enable app SplunkForwarder -auth  
${user}:${password}" splunk && \  
sudo su -c "/opt/splunk/bin/splunk restart" splunk && \  
sudo su -c "splunk add forward-server ${host}:${port} -auth  
${user}:${password} && \  
sudo su -c "/opt/splunk/bin/splunk restart" splunk
```

Universal Forwarder

```
useradd -m -d /opt/splunkforwarder splunkfwd && \  
chsh -s /bin/bash splunkfwd && \  
sudo tar xzvf ~/splunk-forwarder.tgz -C /opt && \  
sudo chown -R splunkfwd:splunkfwd /opt/splunkforwarder && \  
sudo /opt/splunkforwarder/bin/splunk start --accept-license
```

[linux](#), [splunk](#)

From:

<http://fortytwo.adurias.org/> - **Fortytwo - Answer to the Ultimate Question of Life, the Universe, and Everything**

Permanent link:

<http://fortytwo.adurias.org/splunk?rev=1701273313>

Last update: **2023/11/29 16:55**

