**Installation Manual - Splunk Universal Forwarder**

**Install Universal Forwarder [Replace the wget command with your own account command:**

1. wget -O splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-amd64.deb 'https://download.splunk.com/products/universalforwarder/releases/8.2.4/linux/splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-amd64.deb'
3. dpkg -i [file-name]

**Step 2: Start Universal Forwarder:**

/opt/splunkforwarder/bin/splunk start

**Test the Connectivity:**

nc -zv 134.209.149.24:9997

**Basic Universal Forwarder Setup:**

1. /opt/splunkforwarder/bin/splunk add monitor /var/log
2. /opt/splunkforwarder/bin/splunk list monitor
3. /opt/splunkforwarder/bin/splunk add forward-server [IP-OF-SPLUNK]:9997

**Log File for any Troubleshooting:**

tail -f /opt/splunkforwarder/var/log/splunk/splunkd.log

**Configuration File Referenced in the video:**

cat /opt/splunkforwarder/etc/system/local/outputs.conf

**Document - Enable Deployment Server**

1. cp -R /opt/splunk/etc/apps/sample\_app/ /opt/splunk/etc/deployment-apps/
2. /opt/splunk/bin/splunk restart