Install Splunk Universal Forwarder on Linux

Login as root to the host
type: sudo useradd splunk
type: sudo passwd splunk
type: <PWD_IN_LOGIN_SHEET>

type: sudo visudo

(locate: ## Allows people in group wheel to run all commands)
type: i
(Under this label, hit enter to create new line)

copy:

```
splunk ALL=(ALL) NOPASSWD: /opt/splunkforwarder/bin/splunk restart
splunk ALL=(ALL) NOPASSWD: /opt/splunkforwarder/bin/splunk stop
splunk ALL=(ALL) NOPASSWD: /opt/splunkforwarder/bin/splunk start
splunk ALL=(ALL) NOPASSWD: /opt/splunkforwarder/bin/splunk status
splunk ALL=(ALL) NOPASSWD: /usr/bin/systemctl restart Splunkd.service
splunk ALL=(ALL) NOPASSWD: /usr/bin/systemctl stop Splunkd.service
splunk ALL=(ALL) NOPASSWD: /usr/bin/systemctl start Splunkd.service
splunk ALL=(ALL) NOPASSWD: /usr/bin/systemctl status Splunkd.service
```

paste: (right click)

hit: esc
type: :wq
type: wget -O splunkforwarder-8.2.4-87e2dda940d1-Linux-x86_64.tgz 'https://download.splunk.com/products/universalforwarder/releases/8.2.4/linux/splunkforwarder-8.2.4-87e2dda940d1-Linux-x86_64.tgz'
type: sudo tar xvzf splunkforwarder-8.2.4-87e2dda940d1-Linux-x86_64.tgz -C /opt
type: sudo vi /etc/environment
type: i
copy:

```
export SPLUNK_HOME=/opt/splunkforwarder
```

paste: (right click)
hit: esc
type: :wq
type: sudo $SPLUNK_HOME/bin/splunk start --accept-license
type: admin
type: asstastic
type: asstastic
type: sudo $SPLUNK_HOME/bin/splunk stop
type: sudo $SPLUNK_HOME/bin/splunk enable boot-start -user splunk -systemd-managed 1
type: vi /opt/splunkforwarder/etc/system/local/deploymentclient.conf
type: i

copy:

```
## BASE SYSTEM
[target-broker:deploymentServer]
targetUri = lm-spl-a06.corp.net.bcbsaz.com:8089
```

paste: (right click)
hit: esc

type: :wq
type: sudo chown -R splunk:splunk $SPLUNK_HOME
type: su splunk
type: sudo $SPLUNK_HOME/bin/splunk start
type: ps -u splunk (verifies splunk is running)