

Lecture 8: Installing Splunk and Splunk Universal Forwarder

Notes:

- To create new user you need to switch to root user first

Linux commands used in this lecture:

Command	Description
sudo su	To switch to root user
useradd -s /bin/bash -d /opt/splunk -m splunk	Create new user called splunk with home directory at this location /opt/splunk
su - splunk	To switch to splunk user
whoami	To displays the username of the current user
cd /tmp	Change directory to /tmp
pwd	To display the current working directory
Ctrl+d	To logout from the current session
Splunk Enterprise commands (on Splunk server)	
tar -xzvf splunk-8.0.4.1-ab7a85abaa98-Linux-x86_64 -C /opt/	To extract Splunk Enterprise tgz package to /opt/splunk, please change package name according the actual file you downloaded
/opt/splunk/bin/splunk start	To start Splunk service
/opt/splunk/bin/splunk status	To check Splunk service status
/opt/splunk/bin/splunk stop	To stop Splunk service
/opt/splunk/bin/splunk restart	To restart Splunk service
Splunk Universal Forwarder commands (on Apache server)	
sudo su	To switch to root user
useradd -s /bin/bash -d /opt/splunkforwarder -m splunk	Create new user called splunk with home directory at this location /opt/splunkforwarder
su - splunk	To switch to splunk user
tar -xzvf splunkforwarder-8.0.4-767223ac207f-Linux-x86_64.tgz -C /opt/	To extract Splunk Universal Forwarder tgz package to /opt/ splunkforwarder, please change package name according the actual file you downloaded
/opt/splunkforwarder/bin/splunk start	To start Splunk UF service
/opt/splunkforwarder/bin/splunk status	To check Splunk UF service status
/opt/splunkforwarder/bin/splunk stop	To stop Splunk UF service
/opt/splunkforwarder/bin/splunk restart	To restart Splunk UF service