

Lecture 11: Collecting logs from remote nodes

Linux commands used in this lecture:

Command	Description
<code>/etc/init.d/apache2 start</code>	To start apache web server (on Linux all services are here /etc/init.d/)
<code>/etc/init.d/apache2 status</code>	To check the status of apache service (this applies to any other service in Linux)
<code>/var/log/apache2/access.log</code>	Location of Apache access logs
<code>tail -f /var/log/apache2/access.log</code>	To monitor new log lines added to the file
<code>Ctrl+Shift+t</code>	To open new terminal
<code>Ctrl+Shift+c</code>	To copy text from terminal
<code>Ctrl+Shift+v</code>	To paste text to terminal
<code>apt-get install curl</code>	To install curl package
<code>find / -name *.jpg</code>	To find all files that have .jpg extension under / directory
<code>find / -name *.jpg > /tmp/test</code>	To write all results of find command to /tmp/test file
<code>cat /tmp/test</code>	To display the content of this file on the screen
<code>for i in `cat /tmp/test`; do curl localhost/\$i; done</code>	For loop on bash shell to iterate on the entries of the file /tmp/test, and execute this command <code>curl localhost/\$i</code> , variable <code>\$i</code> contains an entry from /tmp/test at every iteration
<code>Apt-get install vim</code>	To install vim text editor
<code>su splunk</code>	To switch to splunk user
<code>ls -altr</code>	To display all details of files
<code>vim /etc/group</code>	To modify groups file (refer to table below for Vim keys)

Vim quick tutorial:

Command	Description
<code>vim /opt/splunkforwarder/etc/system/local/inputs.conf</code>	To open inputs.conf file for editing
<code>press i</code>	To switch to insert mode
<code>press Esc then :q</code>	To exit vim
<code>press Esc then :wq</code>	To save changes and exit
<code>press Esc then :q!</code>	To exit without saving

Splunk configurations files contents on universal forwarder to read logs and forward to Splunk server:

- [/opt/splunkforwarder/etc/system/local/inputs.conf](#)

```
[default]
host = osboxes
[monitor:///var/log/apache2/access.log]
source= apache
sourcetype= apache_access
index= web
_TCP_ROUTING= indexers
```

- [/opt/splunkforwarder/etc/system/local/outputs.conf](#)

```
[tcpout]
defaultGroup= indexers
[tcpout:indexers]
server = 192.168.219.10:9997
```