Linux Cheatsheet for Splunk Classes

Command	Description	Example
cd *dir*	Change directory to *dir* (As in Windows, **..** is the parent directory and **.** is the current directory)	cd /opt cd /opt/splunk/bin
cd ~	Change directory to your home directory	cd ~
chmod *p fname*	Changes the permissions of the file *fname* based on *p* (see **man** command for more info) The example adds execute permissions to a file	chmod +x myScript.sh
cp *fname newname*	copy the file *fname* to *newname*; *newname* can include a directory path	cp 1.txt 2.txt
echo *msg*	Display the *msg* (after command line variable substitution and file name expansion)	echo $PATH
find . –name “*name***”**	Look for the file *name*, starting in the current directory. The example uses a wildcard.	find . –name “input*”
ls *dirname*	List the files in the named directory; if no directory is named, list the files in the current directory	ls splunk/etc/users
ls –l	Display a “long” (detailed) list of the files	ls -l
man *cmd*	Provides help for the command *cmd*	man cd
mkdir *dirname*	Creates a new directory named *dirname*	mkdir change
more *fname*	Displays the contents of *fname*, a page at a time. Hit space to move to the next page and **q** to quit.	ps -ef | more more myFile.txt
mv *fname newname*	rename or move the file *fname* to *newname; newname* can specify a new file name (rename) or a directory name (move) or both The example moves a file into a subdirectory	mv 1.txt ~/myDir
nano *fname* **ctrl-X**	Starts the nano editor, editing *fname* Use **ctrl-X** to save your edits	nano inputs.conf
ps –ef	ps displays the status of running processes; the –ef provides a **f**ull listing for **e**very process	ps -ef
pwd	Displays the name of the current directory	pwd
rm *fname*	delete (remove) the file *fname*	rm 1.txt
rmdir *dirname*	removes the empty directory *dirname*	rmdir myDir
source *fname*	Executes the script *fname* within the current process; can be used to reload the .bashrc profile	source ~/.bashrc
su - *username*	Switch to the user account named *username* If you are not logged in as root, you will be prompted for the password.	su - user3
sudo *command*	Execute the *command* as root. Your account must have special privileges for this to work, otherwise you must provide the root password. **sudo su** is used to switch to the root login, but this is generally regarded as an unsafe practice in production.	sudo rm /tmp/x.txt
touch *fname*	If the file exists, update its modification time. If the file does not exist, create an empty file called *fname*.	touch 1.txt
wget *args*	Downloads a file from a web site. The args can usually be cut-and-pasted from the **wget** command example on the web site that is supplying the file.	See download page at splunk.com

Running Scripts or Programs

To run a program or script, simply type its name (including the extension, if any). Depending on how you have set the $PATH variable, you may need to include the path. For example, to execute myScript – a shell script that is located in the current directory:

./myScript.sh