

# log parsing cheat sheet

## LOG PARSING CHEAT SHEET

 <b>GREP</b>	GREP allows you to search patterns in files. ZGREP for GZIP files. <code>#grep &lt;pattern&gt; file.log</code>	-n: Number of lines that matches -i: Case insensitive -v: Invert matches -E: Extended regex -c: Count number of matches -l: Find filenames that matches the pattern
 <b>NGREP</b>	NGREP is used for analyzing network packets. <code>#ngrep -I file.pcap</code>	-d: Specify network interface -i: Case insensitive -X: Print in alternate hexdump -t: Print timestamp -I: Read pcap file
 <b>CUT</b>	The CUT command is used to parse fields from delimited logs. <code>#cut -d '*' -f 2 file.log</code>	-d: Use the field delimiter -f: The field numbers -c: Specifies characters position
 <b>SED</b>	SED (Stream Editor) is used to replace strings in a file. <code>#sed s/regex/replace/g</code>	S: Search      -E: Execute command g: Replace     -n: Suppress output d: Delete W: Append to file
 <b>SORT</b>	SORT is used to sort a file. <code>#sort foot.txt</code>	-o: Output to file      -C: Check if ordered -r: Reverse order      -u: Sort and remove -n: Numerical sort     -f: Ignore case -k: Sort by column     -h: Human sort
 <b>UNIQ</b>	UNIQ is used to extract uniq occurrences. <code>#uniq foot.txt</code>	-c: Count the number of duplicates -d: Print duplicates -i: Case insensitive
 <b>DIFF</b>	DIFF is used to display differences in files by comparing line by line. <code>#diff foo.log bar.log</code>	How to read output? a: Add      #: Line numbers c: Change    <: File 1 d: Delete    >: File 2
 <b>AWK</b>	AWK is a programming language use to manipulate data. <code>#awk {print \$2} foo.log</code>	Print first column with separator ** <code>#awk -F '{print \$1}' /etc/passwd</code> Extract uniq value from two files: <code>awk 'FNR==NR {a[\$0]=1; next} !(\$0 in a) {f1.txt f2.txt}</code>

From:

<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:

<https://miguelangel.torresegea.es/wiki/linux:log:log-parsing>

Last update: 18/04/2023 03:23

