

# Linux

## Obsługa systemu



# Cześć!

Daniel Kossakowski

DevOps Engineer @ CloudPanda.io

1.

# Wyszukiwanie plików

# Wyszukiwanie plików Konfiguracja

- `find /katalog` - wyszukuje wszystkie pliki w danym miejscu
- `find / -name "syslog"` - wyszukuje pliki o nazwie *syslog*
- `find / -name "*log"` - znajduje pliki z nazwą kończącą się na *log*
- `find / -name "*log*"` - znajduje pliki zawierające frazę *log*
- `find / -mtime N` - pliki zmodyfikowane N dni temu
- `find / -mtime +N` - pliki zmodyfikowane N dni temu i później
- `find / -mtime -N` - pliki zmodyfikowane N dni temu i wcześniej

# ĆWICZENIE!

- Przejdź do katalogu /
- Znajdź listę plików zmodyfikowanych w przeciągu ostatnich 7 dni

# Wyszukiwanie plików Konfiguracja

- `find / -type f` - szukaj tylko plików
- `find / -type d` - szukaj tylko katalogów
  
- `find / -name "*log*" -type f` - szukaj plików zawierających „log”
- `find / -name "*log*" -type d` - szukaj katalogów zawierających „log”
  
- A co kiedy chcemy coś zrobić ze znalezionymi plikami?

# Wyszukiwanie plików Konfiguracja

- `find /tmp -type d -exec chmod u=rwx,g=rx,o= {} \;`
  - `find /tmp -type f -exec chmod u=rw,g=r,o= {} \;`
  - `find /tmp -type f -exec echo {} +`
- 
- `{}` - zamieniane jest na nazwę znalezionej pliku
  - `;` - przetwarzanie każdego pliku z osobna (poprzedzone ukośnikiem)
  - `+` - przetwarzanie wszystkich plików naraz

# ĆWICZENIE!

- Utwórz folder `/tmp/shared`
- Znajdź w katalogu `/var` wszystkie pliki z rozszerzeniem `.log`
- Skopiuj znalezione pliki do katalogu `/tmp/shared`



## 2. Pobieranie plików

# Wyszukiwanie plików Konfiguracja

- `wget http://www.wp.pl/index.html` - pobranie pliku
- `wget http://www.wp.pl/index.html -O plik.txt` - j.w. + nowa nazwa
- `--limit-rate=1k` - ograniczenie prędkości pobierania
- `--no-check-certificate` - ignoruj niepoprawne certyfikaty SSL

# ĆWICZENIE!

- Znajdź link do najnowszej wersji biblioteki Bootstrap.
- Pobierz bibliotekę w postaci archiwum ZIP.
- Wypakuj pliki do katalogu /tmp/jquery (komenda unzip).

# 3. Analiza logów

# 1.284.046

- Średnia liczba linii pliku z logami większego serwisu.

# Analiza logów Filtrowanie

- `grep "text" nginx.log` - szuka frazy *text* w pliku *nginx.log*
- `grep --color "text" plik` - pokoloruje wszystkie wystąpienia frazy
- `grep -i "text" plik` - ignorowanie wielkości znaków
- `grep -i "text" *.log` - przeszukuje wszystkie pliki z rozszerzeniem *.log*
- `grep -R "text" /var/log` - przeszukuje wszystkie pliki w podanym katalogu

# Analiza logów Przekierowania

- Linux pozwala "w locie" przekazywać dane do innych programów / plików.
  - `> plik` - zapisuje wyświetlone dane do pliku
  - `>> plik` - dopisuje dane na koniec pliku
  - `< plik` - ładuje do programu dane z pliku
  - `|` - przekazuje dane do innego programu
- `cat < /var/log/bootstrap`
- `cat /var/log/bootstrap | grep "test"`
- `cat /var/log/bootstrap | grep "test" | wc -l`

# Analiza logów Przykład

- Adres IP
- Data
- Zapytanie HTTP
- Kod
- Rozmiar pliku
- User agent

```
66.249.66.250 - - [06/May/2017:23:21:32 +0000] "GET /admin HTTP/1.1" 200 5372 "-" "Mozilla/5.0  
(compatible; Googlebot/2.1; +http://www.google.com/bot.html),,
```

```
104.192.74.46 - - [09/May/2017:09:27:42 +0000] "GET / HTTP/1.1" 200 5372 "-" "Mozilla"
```



# ĆWICZENIE!

- Sklonuj repozytorium (link na slacku)
- Sprawdź ile linii znajduje się w pliku *examples/nginx.log*.
- Policz ile razy łączono się do strony z adresu *66.249.66.145* oraz *87.161.152.33*.
- Sprawdź ile razy pobierano stronę 13 maja 2017 w godzinach 18 - 19.

# Analiza logów **Obróbka danych**

- Awk - przetwarzanie plików tekstowych
- awk '{print \$1}' - wypisanie pierwszej kolumny tekstu
- awk '{print \$1, \$2}' - wypisanie pierwszej kolumny tekstu
  
- cat nginx.log | awk '{print \$1}' - lista adresów IP w logu
- cat nginx.log | awk '{print \$1}' | sort - sortowanie listy
  
- sort - sortowanie alfabetyczne
- sort -u - usunięcie duplikatów

# ĆWICZENIE!

- Sprawdź w logu *examples/nginx.log* z ilu różnych adresów IP łączono się do strony.

4.

## Instalowanie aplikacji

# Instalowanie aplikacji **Teoria**

- Instalacja przebiega inaczej w zależności od dystrybucji systemu.
- Skupimy się na Ubuntu.
- Ubuntu ma swoje repozytoria z aplikacjami.
- Dostępne są tylko sprawdzone programy open source.

# Instalowanie aplikacji **Praktyka**

- apt-get update - odświeżenie repozytoriów
- apt-get install vim - instalacja programu vim
- apt-get install vim nano mcedit - instalacja kilku programów naraz
- apt-get remove mcedit - usunięcie programu
- apt-get --purge remove mcedit - usunięcie programu z konfiguracją

# ĆWICZENIE!

- Zainstaluj w systemie paczki vim, nano, git, mc, htop.
- Sprawdź czy zainstalowane programy działają.
- Znajdź lokalizację ich plików wykonywalnych.

5.

# Zdalne zarządzanie systemem



# Zdalne zarządzanie systemem



# Zdalne zarządzanie systemem

- Koncepcja zdalnego terminala.
- Możliwość logowania na każdego użytkownika.
- Szyfrowany protokół.
- Działa na porcie 22.

# Zdalne zarządzanie systemem

- `ssh maciek@127.0.0.1` - połączenie na użytkownika maciek  
`ssh 127.0.0.1 -l maciek`
- SSH dla bezpieczeństwa umieszcza się czasami na innym porcie  
`ssh 127.0.0.1 -l maciek -p 8022`
- SSH pozwala też wykonać pojedyncze polecenie  
`ssh 127.0.0.1 -l maciek "uname -a"`

# ĆWICZENIE!

- Utwórz w systemie użytkownika *remote* wraz z katalogiem domowym (useradd -m).
- Ustaw hasło Tajne1 dla użytkownika *remote*.
- Połącz się przy pomocy SSH do komputera obok na użytkownika *remote*.
- W katalogu /tmp utwórz plik o nazwie test i wpisz do niego swoje imię.

# 6. Transfer plików

# Transfer plików

- `scp [plik źródłowy] [miejsce docelowe]`
- `scp /home/plik remote@127.0.0.1:/tmp` - przesłanie pliku do serwera
- `scp remote@127.0.0.1:/tmp/plik /home` - pobranie pliku od serwera

# ĆWICZENIE!

- Prześlij z komputera obok stworzony wcześniej plik `/tmp/test` przy pomocy SCP.
- Zapisz go w katalogu `/home`.

# 7.

## Przydatne narzędzia



# htop

Sprawdzanie  
obciążenia  
systemu

```
 1  [|||||||||||||||||] 5  [|||||||||||||||||]
 2  [|||||||||||||||||] 6  [|||||||||||||||||]
 3  [|||||||||||||||||] 7  [|||||||||||||||||]
 4  [|||||||||||||||||] 8  [|||||||||||||||||]
Mem[|||||||||||||||||] Tasks: 289, 0 thr; 4 running
Swp[|||||||||||||||||] Load average: 4.44 5.10 5.20
                                Uptime: 23 days, 07:56:18
```

PID	USER	PRI	NI	VIRT	RES	S	CPU%	MEM%	TIME+	Command									
84835	stream	27	0	87656	26024	S	5.5	0.2	23h29:41	liquidsoap 2102.lcf ../pilot									
86734		26	0	85608	25852	S	5.2	0.2	22h05:07	liquidsoap 1715.lcf ../pilot									
84926		52	0	89704	26080	S	5.1	0.2	21h27:46	liquidsoap 2476.lcf ../pilot									
84895		29	0	87656	27024	S	4.9	0.2	23h15:39	liquidsoap 2449.lcf ../pilot									
84821		24	0	83560	24428	S	4.8	0.1	23h02:22	liquidsoap 1714.lcf ../pilot									
86117		27	0	83560	27148	S	4.7	0.2	8h09:50	liquidsoap 2524.lcf ../pilot									
32167		28	0	83560	28180	S	4.7	0.2	11h50:47	liquidsoap 2517.lcf ../pilot									
84854		49	0	79464	23988	S	4.7	0.1	22h05:51	liquidsoap 2387.lcf ../pilot									
88157		32	0	81508	26388	S	4.2	0.2	3h21:08	liquidsoap 2527.lcf ../pilot									
33524		32	0	79460	25248	S	4.1	0.2	34:13.02	liquidsoap 2484.lcf ../pilot									
12136		20	0	1692M	11080	S	4.0	0.1	1h35:22	/opt/shoutcast/sc_serv2 daem									
45800		28	0	75364	26900	S	4.0	0.2	0:31.52	liquidsoap 2514.lcf ../pilot									
27364		26	0	79460	25412	S	4.0	0.2	52:11.24	liquidsoap 2244.lcf ../pilot									
45276		26	0	77412	28380	S	3.9	0.2	2:27.77	liquidsoap 2500.lcf ../pilot									
40496		23	0	75364	27484	S	3.8	0.2	17:58.77	liquidsoap 2471.lcf ../pilot									
0	root	-16	0	0	4464	S	3.2	0.0	15h57:16	kernel									
55536		20	0	1690M	14412	S	2.8	0.1	1h43:57	/opt/shoutcast/sc_serv2 daem									
78112		20	0	58692	9684	S	2.7	0.1	11h00:55	/opt/shoutcast/sc_trans 2499									
44261		20	0	58692	9000	S	2.7	0.1	7h24:37	/opt/shoutcast/sc_trans 2451									
84832		20	0	58692	7084	S	2.5	0.0	17h18:26	/opt/shoutcast/sc_trans 2099									
40191		20	0	64836	12508	S	2.4	0.1	10h44:16	/opt/shoutcast/sc_trans 2510									
F1	Help	F2	Setup	F3	Search	F4	Filter	F5	Tree	F6	SortBy	F7	Nice	-F8	Nice	+F9	Kill	F10	Quit

# mc

Konsolowy  
graficzny menedżer  
plików

Left	File	Command	Options	Right					
<- ~				<- /tmp					
.n	Name	Size	Modify time	.n	Name	Size	Modifi		
/..		UP--DIR	Sep 28 11:55	/..		UP--DIR	Sep 2		
/.cache		3	Mar 19 2017	/.ICE-unix		2	Sep 2		
/.config		5	Apr 5 2017	/.X11-unix		2	Sep 2		
/.local		3	Mar 19 2017	/.XIM-unix		2	Sep 2		
/.spamassassin		2	Apr 15 2017	/.font-unix		2	Sep 2		
/.ssh		4	Apr 25 17:49	/hsperfdata_kacper		2	Oct 1		
/VirtualBox VMs		3	Jun 22 08:32	/hsperfdata_root		2	Oct		
.cshrc		957	Sep 29 2016	/jfdz7-linux		5	Oct 1		
.gitconfig		161	Oct 14 15:45	/mc-root		3	Oct 2		
.history		35656	Oct 21 19:49	/screens		3	Sep 2		
.k5login		149	Sep 28 11:55	4str_017jrqb		202	Oct		
.lessht		63	Jun 15 11:01	4str_03niv7ht		210	Oct 1		
.login		295	Sep 28 11:55	4str_074sh65t		224	Oct 1		
.lsof_krolnet		1533	Jun 6 07:35	4str_08w9lp5d		200	Sep 2		
.profile		249	Sep 29 2016	4str_09ramyu6		204	Oct 2		
.wget-hsts		237	Jun 15 10:16	4str_0bw7tgch		203	Oct 1		
VBoxHeadless.core		4559M	Jul 5 20:22	4str_0ebr3mij		218	Oct		
index.html		302284	Oct 14 11:36	4str_0hdz6ijo		212	Oct		
test		46430	Oct 14 11:40	4str_0j9au7m3		218	Oct		
				4str_0l6mlr29		210	Oct		
				4str_0s1w6td8		209	Oct		
				4str_0tdewb6q		203	Oct 1		
				4str_0thqvi2b		200	Sep 2		
UP--DIR				UP--DIR					
			435G/738G (58%)				435G/435G		
Hint: Want to do complex searches? Use the External Panelize command.									
root@krolnet:/tmp#									
1Help	2Menu	3View	4Edit	5Copy	6RenMov	7Mkdir	8Delete	9PullDn	10

# df

Zapełnienie dysków  
i partycji

```
zroot/backup          754G    319G    435G    42%    /backup
zroot/tmp              435G      23M    435G     0%    /tmp
zroot/usr/home         698G    264G    435G    38%    /usr/home
zroot/usr/ports        439G     4.3G    435G     1%    /usr/ports
zroot/usr/src          435G    637M    435G     0%    /usr/src
zroot/var/audit        435G      96K    435G     0%    /var/audit
zroot/var/crash        435G      96K    435G     0%    /var/crash
zroot/var/db           436G     1.3G    435G     0%    /var/db
zroot/var/db/mysql     440G     5.0G    435G     1%    /var/db/mysql
zroot/var/log          435G    566M    435G     0%    /var/log
zroot/var/mail         435G    128K    435G     0%    /var/mail
zroot/var/tmp          436G     1.0G    435G     0%    /var/tmp
zroot                  435G      96K    435G     0%    /zroot
root@krolnet:/usr/local # df -h
Filesystem            Size      Used    Avail Capacity  Mounted on
zroot/ROOT/default    738G    303G    435G     41%      /
devfs                 1.0K      1.0K       0B    100%    /dev
linprocfs             4.0K      4.0K       0B    100%    /compat/linux/proc
zroot/backup          754G    319G    435G     42%    /backup
zroot/tmp              435G      23M    435G     0%    /tmp
zroot/usr/home         698G    264G    435G    38%    /usr/home
zroot/usr/ports        439G     4.3G    435G     1%    /usr/ports
zroot/usr/src          435G    637M    435G     0%    /usr/src
zroot/var/audit        435G      96K    435G     0%    /var/audit
zroot/var/crash        435G      96K    435G     0%    /var/crash
zroot/var/db           436G     1.3G    435G     0%    /var/db
zroot/var/db/mysql     440G     5.0G    435G     1%    /var/db/mysql
zroot/var/log          435G    566M    435G     0%    /var/log
zroot/var/mail         435G    128K    435G     0%    /var/mail
zroot/var/tmp          436G     1.0G    435G     0%    /var/tmp
zroot                  435G      96K    435G     0%    /zroot
root@krolnet:/usr/local #
```



# du

Rozmiar plików i  
katalogów

```
drwxr-xr-x  5 root  wheel    9 Oct  3 10:20 openssl
drwxr-xr-x  2 root  wheel   63 Oct 16 00:58 sbin
drwxr-xr-x 83 root  wheel   83 Oct 16 00:56 share
drwxr-xr-x  4 root  wheel    4 Jul  7 18:56 var
drwxr-xr-x  9 www   www    10 Oct 16 00:58 www
drwxr-xr-x  4 root  wheel    4 Apr 15  2017 x86_64-portbld-freebsd11.0
root@krolnet:/usr/local # du -hs *
233M    bin
 49M    bootstrap-openjdk
1.7M    dcc
3.7M    etc
111M    include
 12M    info
1.2G    lib
5.8M    lib32
1.2M    libdata
146M    libexec
560M    llvm39
664M    llvm40
 31M    man
 90M    openjdk7
 99M    openjdk8
596K    openssl
9.8M    sbin
286M    share
 21K    var
132G    www
 24M    x86_64-portbld-freebsd11.0
root@krolnet:/usr/local # du -hs www/
132G    www/
```



# Koniec!

Dziękuję za uwagę

Pytania?