

# Publique

- Linux
  - Chiffrement Luks
  - Scripts Linux utiles
  - Wi-Fi
  - Network Manager
  - Tmux
  - Gluster
  - Crowdsec
  - ZSH
  - Wireguard
  - Debian
  - firewalld
  - vim
  - Screen
  - MySQL - MariaDB
  - Hardened ssh
  - Arch Linux
- Wi-Fi
- Ceph
  - Cephfs
- BeeGFS
  - Configurations
- hping3

# Linux

# Chiffrement Luks

## Chiffrer une partition

```
#sudo cryptsetup -y -v luksFormat /dev/sdc1
ATTENTION: Le périphérique /dev/sdc1 contient déjà une signature pour un superblock « crypto_LUKS ».

WARNING!
=====
Cette action écrasera définitivement les données sur /dev/sdc1.

Are you sure? (Type uppercase yes): YES
Saisissez la phrase secrète pour /dev/sdc1 :
Vérifiez la phrase secrète :
```

## Formater la partition

```
#sudo mkfs.ntfs -f /dev/mapper/Samsung
Cluster size has been automatically set to 4096 bytes.
Creating NTFS volume structures.
mknfts completed successfully. Have a nice day.
```

## Lister les blocs et identifier les blocs luks

```
#lsblk --fs
```

NAME	FSTYPE	LABEL	UUID	FSAVAIL	FSUSE%	MOUNTPOINT
sda						
├─sda1	vfat	6FE5-9D8C		163,2M	18%	/boot/efi
├─sda2	ext4	f56409e9-43af-41d4-bf9e-1b3ce3cb11e0		713,9M	20%	/boot
└─sda3	crypto_LUKS	6eb090b6-7304-4843-b357-857c5d92962e				
└─luks-6eb090b6-7304-4843-b357-857c5d92962e	LVM2_member	pMkBCr-iN2G-XsPH-4ECF-0zhc-M8uA-wrdQ				
├─fedora-root	ext4	d53e789d-3b19-4314-8fd8-6536e094740d		25G	44%	/
├─fedora-swap	swap	d4261e47-edb0-4abc-9131-cf8dbc751c7e				[SWAP]
└─fedora-home	ext4	5acd1096-bbde-404f-9122-bec03451397d		146,4G	59%	/home
sdc						
└─sdc1	crypto_LUKS	bd80f01b-bfd0-4bc6-a2bb-bc0a25935ccb				

## Saisir la clef de déchiffrement du disque

```
#sudo cryptsetup luksOpen /dev/sdc1 Samsung
Saisissez la phrase secrète pour /dev/sdc1 :
```

# Oublier la clef de chiffrement du disque

```
#sudo cryptsetup luksClose Samsung
```

## Dump de l'entête

```
sudo cryptsetup luksDump /dev/sdc1          SIGINT(2) ← 10396 15:57:10
LUKS header information
Version:      2
Epoch:       3
Metadata area: 16384 [bytes]
Keyslots area: 16744448 [bytes]
UUID:        f2c5df1a-a6cb-46d9-a5b9-50c233089cc2
Label:       (no label)
Subsystem:   (no subsystem)
Flags:       (no flags)

Data segments:
 0: crypt
  offset: 16777216 [bytes]
  length: (whole device)
  cipher: aes-xts-plain64
  sector: 512 [bytes]

Keyslots:
 0: luks2
  Key:      512 bits
  Priority: normal
  Cipher:   aes-xts-plain64
  Cipher key: 512 bits
  PBKDF:    argon2i
  Time cost: 6
  Memory:   1048576
  Threads:  4
  Salt:     6c 79 ac 83 62 0b b4 27 8a 51 6f 07 c7 51 ae 48
           d2 8b 70 88 c0 2a f2 a8 81 2b 9f 5f 05 21 ee 00
  AF stripes: 4000
  AF hash:   sha256
  Area offset: 32768 [bytes]
  Area length: 258048 [bytes]
  Digest ID: 0
Tokens:
Digests:
 0: pbkdf2
  Hash:     sha256
```

```
Iterations: 115380
Salt:      d5 23 f6 2a 06 ea 92 19 45 12 2a 54 d7 a5 2c ee
          ae 64 f9 2c 85 34 d5 2f a1 3e 71 21 c1 1c e2 07
Digest:    c1 7b 22 74 2e c7 54 6f 73 39 77 2a 1e 5f 67 65
          54 80 07 43 d3 3d a0 08 d4 f0 b8 6f 76 be 44 70
```

# Ajouter une clef

On ajoute une clef supplémentaire en slot 2 sur la base d'un mot de passe

```
sudo cryptsetup luksAddKey --key-slot 1 /dev/sdc1
Entrez une phrase secrète existante :
Entrez une nouvelle phrase secrète pour l'emplacement de clé :
Vérifiez la phrase secrète :
```

Ou sur la base d'un fichier qui fait office de clef (cette méthode est préférable afin de rendre la chose plus robuste et automatisé pour le montage) :

```
dd if=/dev/urandom of=/home/dugravot6/Securite/Samsung_disk_secret_key bs=512 count=8
sudo cryptsetup -v luksAddKey /dev/sdc1 /home/dugravot6/Securite/Samsung_disk_secret_key
```

Le dump présentera le slot2 occupé :

```
LUKS header information
Version:      2
Epoch:       4
Metadata area: 16384 [bytes]
Keyslots area: 16744448 [bytes]
UUID:        f2c5df1a-a6cb-46d9-a5b9-50c233089cc2
Label:       (no label)
Subsystem:   (no subsystem)
Flags:       (no flags)

Data segments:
 0: crypt
offset: 16777216 [bytes]
length: (whole device)
cipher: aes-xts-plain64
sector: 512 [bytes]

Keyslots:
 0: luks2
Key:      512 bits
Priority:  normal
Cipher:   aes-xts-plain64
Cipher key: 512 bits
PBKDF:    argon2i
Time cost: 6
Memory:   1048576
```

```
□Threads: 4
□Salt: 6c 79 ac 83 62 0b b4 27 8a 51 6f 07 c7 51 ae 48
□ d2 8b 70 88 c0 2a f2 a8 81 2b 9f 5f 05 21 ee 00
□AF stripes: 4000
□AF hash: sha256
□Area offset:32768 [bytes]
□Area length:258048 [bytes]
□Digest ID: 0
  1: luks2
□Key: 512 bits
□Priority: normal
□Cipher: aes-xts-plain64
□Cipher key: 512 bits
□PBKDF: argon2i
□Time cost: 4
□Memory: 1020932
□Threads: 4
□Salt: 6d 0f 29 10 c8 5b 9a e3 58 30 f4 3e 8e 8f 2d 60
□ 0b f8 17 5f 18 fa dd 42 9c fe 38 d7 07 7d 2c d4
□AF stripes: 4000
□AF hash: sha256
□Area offset:290816 [bytes]
□Area length:258048 [bytes]
□Digest ID: 0
Tokens:
Digests:
  0: pbkdf2
□Hash: sha256
□Iterations: 115380
□Salt: d5 23 f6 2a 06 ea 92 19 45 12 2a 54 d7 a5 2c ee
□ ae 64 f9 2c 85 34 d5 2f a1 3e 71 21 c1 1c e2 07
□Digest: c1 7b 22 74 2e c7 54 6f 73 39 77 2a 1e 5f 67 65
□ 54 80 07 43 d3 3d a0 08 d4 f0 b8 6f 76 be 44 70
```

## Supprimer une clef

On précise le slot a supprimer :

```
sudo cryptsetup luksKillSlot /dev/sdc1 1
Entrez toute phrase secrète restante :
```

## Monter automatiquement la partition

Le fichier `/etc/crypttab` permet de définir les entrées et les options de montage :

```
Samsung UUID=5ab227f5-f69e-4a2f-b85a-32b7637d42be /home/dugravot6/Securite/Samsung_disk_secret_key luks
```

Le format est le suivant :

```
<target name> <source device> <key file> <options>
```

Ici, l'UUID correspondant sera monté grâce à la clef  
(/home/dugravot6/Securite/Samsung\_disk\_secret\_key) que l'on a associée précédemment en slot 2.

# Scripts Linux utiles

# Scripts Linux utiles

## Usage mémoire/swap

### Utilisation du swap par processus

```
for file in /proc/*/status ;
do awk '/Tgid|VmSwap|Name/{printf $2 " " $3}END{ print ""}' $file;
done | grep kB | sort -k 3 -n
```

### Utilisation de la mémoire totale par processus

```
for file in /proc/*/status ;
do awk '/Tgid|VmSize|Name/{printf $2 " " $3}END{ print ""}' $file;
done | grep kB | sort -k 3 -n
```

A noter :

- what do the fields VmSize, VmLck, VmRSS, VmData, VmStk, VmExe, and VmLib mean?

## Wait

# Processus

Identifier les processus qui provoquent du wait

```
while true; do date; ps auxf | awk '{if($8=="D") print $0;}'; sleep 1; done
```

## Wait disques

## Wait Proc

Informations sur le processus

```
ls -l -p PID
```

## Conditions shell

Existence du fichier logwatch ?

```
[ -e logwatch ] && echo "ok"
```

# Wi-Fi

## Afficher les réseaux Wi-Fi et leur signal

```
nmcli dev wifi list
```

IN-USE	BSSID	SSID	MODE	CHAN	RATE	SIGNAL	BARS	SECURITY
	8C:97:EA:D9:E6:08	Freebox-32127D	Infra	11	130 Mb/s	100		WPA2
*	8C:97:EA:D9:E6:0C	Freebox-32127D	Infra	104	540 Mb/s	100		WPA2
	B4:E2:65:B1:B8:6D	SFR_B86B	Infra	6	260 Mb/s	44		WPA1 WPA2
	2C:08:23:2B:D8:EE	Livebox-D8EE	Infra	1	195 Mb/s	30		WPA2
	B4:E2:65:B1:B8:6E	SFR_B86B	Infra	52	540 Mb/s	27		WPA1 WPA2
	08:87:C6:62:A8:80	Livebox-A880	Infra	1	195 Mb/s	24		WPA2

Linux

# Network Manager

## Création d'une connexion

```
nmcli connection add type ethernet con-name esn19 ifname ens19
```

Après l'ajout d'une interface depuis proxmox, NetworkManager ne prenait pas en compte cette interface. Il a fallu la créer ...

# Tmux

## FAQ

Copier/coller le buffer

```
CTRL B  
capture-pane -S -20000  
  
CTRL B  
save-buffer /tmp/buf.txt
```

## Ecrire dans plusieurs terminaux en même temps

```
Ctrl-B :  
setw synchronize-panes on  
clear history
```

## Redimensionner un pane

```
:resize-pane -D (Resizes the current pane down by one cell)  
  
:resize-pane -R (Resizes the current pane right by one cell)  
  
:resize-pane -U (Resizes the current pane upward by one cell)  
  
:resize-pane -L (Resizes the current pane left by one cell)  
  
:resize-pane -U 10 (Resizes the current pane upward by ten cells)  
  
:resize-pane -R 10 (Resizes the current pane right by ten cells)  
  
:resize-pane -D 10 (Resizes the current pane down by ten cells)
```

```
:resize-pane -L 10 (Resizes the current pane left by ten cells)
```

If you wish to configure your keybindings, then open the `tmux.conf` file and append the following lines of code:

```
bind -n M-H resize-pane -L 2  
  
bind -n M-L resize-pane -R 2  
  
bind -n M-K resize-pane -U 2  
  
bind -n M-J resize-pane -D 2
```

## Faire une recherche dans un panel

```
setw -g mode-keys vi  
bind-key -n C-f copy-mode \; send-key ?
```

Alors on fait CTRL-F, puis le pattern.

N permet de passer au suivant, SHIFT N au précédent.

## Copier/Coller

En mode clavier

```
# Entrer en mode copie  
CTRL+B [  
  
# Débuter la sélection  
SPACE  
  
# Fin de sélection  
ENTRER  
  
# Coller  
CTRL+B ]
```

En mode souris

## 1. Nécessite xclip

## 2. Sélection par la souris, appuyer sur ENTRER pour copier

```
set -g mouse on
bind -n WheelUpPane if-shell -F -t = "#{mouse_any_flag}" "send-keys -M" "if -Ft= '#{pane_in_mode}' 'send-
keys -M' 'select-pane -t=; copy-mode -e; send-keys -M'"
bind -n WheelDownPane select-pane -t= \; send-keys -M
bind -n C-WheelUpPane select-pane -t= \; copy-mode -e \; send-keys -M
bind -T copy-mode-vi C-WheelUpPane send-keys -X halfpage-up
bind -T copy-mode-vi C-WheelDownPane send-keys -X halfpage-down
bind -T copy-mode-emacs C-WheelUpPane send-keys -X halfpage-up
bind -T copy-mode-emacs C-WheelDownPane send-keys -X halfpage-down

# To copy, left click and drag to highlight text in yellow,
# once you release left click yellow text will disappear and will automatically be available in clipboard
# # Use vim keybindings in copy mode
setw -g mode-keys vi
# Update default binding of `Enter` to also use copy-pipe
unbind -T copy-mode-vi Enter
bind-key -T copy-mode-vi Enter send-keys -X copy-pipe-and-cancel "xclip -selection c"
bind-key -T copy-mode-vi MouseDragEnd1Pane send-keys -X copy-pipe-and-cancel "xclip -in -selection clipboard"
```

# Gluster

## Configuration

```
gluster volume set v0 network.ping-timeout 5
```

Faut il ? :

```
sudo gluster volume set v0 cluster.server-quorum-type server
```

## Commandes utiles

Options du volume

```
sudo gluster volume get v0 all
```

```
# sudo gluster volume status v0
detail
                                dugarvot6@minipc1 21:10:03

Status of volume: gv0
-----
Brick          : Brick minipc1:/data/brick1/v0
TCP Port       : 49153
RDMA Port      : 0
Online         : Y
Pid            : 91087
File System    : xfs
Device         : /dev/mapper/minipc1--vg-brick1
Mount Options  : rw,relatime,attr2,inode64,logbufs=8,logbsize=32k,noquota
Inode Size     : 512
Disk Space Free : 9.4GB
```

Total Disk Space : 10.0GB

Inode Count : 5242880

Free Inodes : 5170060

-----  
Brick : Brick minipc2:/data/brick1/v0

TCP Port : 49152

RDMA Port : 0

Online : Y

Pid : 865

File System : xfs

Device : /dev/mapper/minipc2--vg-brick1

Mount Options : rw,relatime,attr2,inode64,logbufs=8,logbsize=32k,noquota

Inode Size : 512

Disk Space Free : 9.4GB

Total Disk Space : 10.0GB

Inode Count : 5242880

Free Inodes : 5170060

-----  
Brick : Brick pi1:/data/brick1/v0

TCP Port : 49152

RDMA Port : 0

Online : Y

Pid : 1089

File System : ext4

Device : /dev/root

Mount Options : rw,noatime

Inode Size : N/A

Disk Space Free : 53.4GB

Total Disk Space : 58.2GB

Inode Count : 3852672

Free Inodes : 3644730

```
sudo gluster volume status
```

```
v0
```

```
dugravot6@minipc1 ⚡ 21:06:48
```

```
Status of volume: gv0
```

```
Gluster process          TCP Port  RDMA Port  Online  Pid
```

```
-----  
Brick minipc1:/data/brick1/gv0      49153    0          Y      91087
```

```
Brick minipc2:/data/brick1/gv0      49152    0          Y      865
```

```

Brick pi1:/data/brick1/gv0          49152  0    Y    1089
Self-heal Daemon on localhost      N/A    N/A   Y    91110
Self-heal Daemon on minipc2       N/A    N/A   Y    876
Self-heal Daemon on pi1           N/A    N/A   Y    1188

```

Task Status of Volume gv0

-----

There are no active volume tasks

```

sudo gluster volume status v0

```

```

clients

```

```

                dugravot6@minipc1 ⚡ 21:08:53

```

```

Client connections for volume gv0

```

-----

```

Brick : minipc1:/data/brick1/gv0

```

```

Clients connected : 2

```

Hostname	BytesRead	BytesWritten	OpVersion
-----	-----	-----	
127.0.0.1:49145	4940	5344	90000
127.0.0.1:49144	121252	107068	90000

-----

```

Brick : minipc2:/data/brick1/gv0

```

```

Clients connected : 7

```

Hostname	BytesRead	BytesWritten	OpVersion
-----	-----	-----	
192.168.1.142:49136	2024	1596	90000
192.168.1.133:49140	3072	2956	90000
192.168.1.133:49138	2662750	11976	90000
192.168.1.141:49144	60717900	46588484	90000
192.168.1.142:49134	17660	19124	90000
192.168.1.141:49147	1688	1792	90000
192.168.1.141:49141	121308	107068	90000

-----

```

Brick : pi1:/data/brick1/gv0

```

```

Clients connected : 7

```

Hostname	BytesRead	BytesWritten	OpVersion
-----	-----	-----	
192.168.1.141:49142	69540850	59101132	90000
192.168.1.133:49142	75000	59132	90000

192.168.1.133:49139	8980	8420	90000
192.168.1.142:49145	3424	3208	90000
192.168.1.142:49139	7316	6508	90000
192.168.1.141:49146	1684	1784	90000
192.168.1.141:49140	100176	86464	90000

-----

# Volume top

Lecture de fichiers :

```
# sudo gluster volume top v0 read list-cnt 10                                dugravot6@minipc1 16:50:13
Brick: minipc1:/data/brick1/volume1
Count      filename
=====
62285      /UPTIME-KUMA/datas/kuma.db
23020      /UPTIME-KUMA/datas/kuma.db-wal
2290       /JELLYFIN/config/data/library.db
1987       /JELLYFIN/config/data/library.db-journal
725        /PORTAINER/datas/portainer.db
431        /JDOWNLOADER2/data/config/Core.jar
405        /JDOWNLOADER2/data/config/JDownloader.jar
310        /FRESHRSS/prod/data/varlibmysql/rss/dugravot6_entry.ibd
289        /FRESHRSS/prod/data/varlibmysql/ibdata1
286        /BOOKSTACK/db/config/databases/ibdata1
Brick: minipc2:/data/brick1/volume1
```

Ouverture de fichiers :

```
# sudo gluster volume top v0 open list-cnt
10
                                dugravot6@minipc1 16:51:27
Brick: minipc1:/data/brick1/volume1
Current open fds: 196, Max open fds: 198, Max openfd time: 2023-03-17 15:36:30.422556 +0000
Count      filename
=====
200        /NGINX/data/acme/acme.sh/stephane@dugravot.fr/whoami.local/whoami.local.conf
109        /NGINX/data/acme/acme.sh/stephane@dugravot.fr/http.header
```

```

66      /NGINX/data/acme/acme.sh/stephane@dugravot.fr/account.conf
24      /NGINX/data/acme/acme.sh/stephane@dugravot.fr/whoami.local/whoami.local.key
24      /NGINX/data/acme/acme.sh/stephane@dugravot.fr/whoami.local/whoami.local.csr.conf
11      /FRESHRSS/prod/data/freshrss/users/dugravot6/log.txt
8       /NGINX/data/acme/acme.sh/stephane@dugravot.fr/whoami.local/whoami.local.csr
7       /NGINX/data/certs/wiki.dugravot.fr/.companion
7       /FRESHRSS/prod/data/varlibmysql/mysql/plugin.MAI
7       /FRESHRSS/prod/data/varlibmysql/mysql/plugin.MAD
Brick: minipc2:/data/brick1/volume1
Current open fds: 196, Max open fds: 197, Max openfd time: 2023-03-17 16:06:54.886386 +0000
Count   filename
=====
25      <gfid:34f34f23-979e-46d6-b39c-
8c224b444058>/stephane@dugravot.fr/whoami.local/whoami.local.conf
17      <gfid:34f34f23-979e-46d6-b39c-8c224b444058>/stephane@dugravot.fr/http.header
12      <gfid:34f34f23-979e-46d6-b39c-8c224b444058>/stephane@dugravot.fr/account.conf
4       /JDOWNLOADER2/data/config/JDownloader.jar
4       /JDOWNLOADER2/data/config/xdg/cache/fontconfig/5ca8086aeacc9c68e81a71e7ef846b3b-
le64.cache-8
4       /JDOWNLOADER2/data/config/xdg/cache/fontconfig/386ad34c5eae46f7db63aa04756d58d-
le64.cache-8
4       /JDOWNLOADER2/data/config/xdg/cache/fontconfig/605eb33399efa08596766eba8c7361d5-
le64.cache-8
3       <gfid:34f34f23-979e-46d6-b39c-
8c224b444058>/stephane@dugravot.fr/whoami.local/whoami.local.key
3       <gfid:34f34f23-979e-46d6-b39c-
8c224b444058>/stephane@dugravot.fr/whoami.local/whoami.local.csr.conf
3       /JDOWNLOADER2/data/config/xdg/cache/fontconfig/a1c95d6dfc9a7b34f44445cf81166004-le64.cache-
8

```

## Performance en lecture (possible en écriture)

```

# sudo gluster volume top v0 read-perf bs 256 count 1 brick minipc1:/data/brick1/volume1 list-cnt
10
dugravot6@minipc1 ↵ 16:57:52
Brick: minipc1:/data/brick1/volume1
Throughput 36.57 MBps time 0.0000 secs
MBps Filename                               Time
=====
=====

```

```
2878 ...ipJBinding-732PU0OuPPzj/lib7-Zip-JBinding.so 2023-03-17 15:05:24 +0000.978307
2732 /JDOWNLOADER2/data/config/Core.jar          2023-03-17 15:04:56 +0000.519398
2528 ...2/data/config/libs/sevenzzipbindingLinux.jar 2023-03-17 15:05:24 +0000.367497
2441 /JDOWNLOADER2/data/config/tmp/hosterCache    2023-03-17 15:05:13 +0000.976603
2399 /JDOWNLOADER2/data/config/JDownloader.jar    2023-03-17 15:04:53 +0000.983716
2351 ...e815af0366dca31c28ab149bd8ed75c/backdrop.jpg 2023-03-17 15:06:58 +0000.85402
2234 .../1/10f6ec15-e9be-b988-b6d9-00dcc1ef3674.webp 2023-03-17 15:03:39 +0000.352235
2053 .../9/91ed9e05-232e-9cf5-ef55-2babb3281509.webp 2023-03-17 15:03:36 +0000.184495
1947 ...NLOADER2/data/config/libs/bcprov-jdk15on.jar 2023-03-17 15:38:36 +0000.239210
1942 .../1bf37a0f85b7c9fed7ce54b4952dcb31/poster.jpg 2023-03-17 15:06:42 +0000.912953
```

# Informations de profile

Activer le profiling

```
sudo gluster volume profile v0 start
```

Visualiser les résultats

```
sudo gluster volume profile v0
info
  1m 36s dugravot6@minipc1 16:16:09
Brick: minipc1:/data/brick1/volume1
-----
Cumulative Stats:
  Block Size:      1b+      2b+      4b+
No. of Reads:      0         1         0
No. of Writes:     74        10        185

  Block Size:      8b+     16b+     32b+
No. of Reads:      5         2         1
No. of Writes:    1414     1957     298

  Block Size:     64b+    128b+    256b+
No. of Reads:     34         97        16
No. of Writes:    415        847       970

  Block Size:    512b+   1024b+   2048b+
```

No. of Reads:	1361	21	58
No. of Writes:	2518	1495	1862
Block Size:	4096b+	8192b+	16384b+
No. of Reads:	45583	20217	6635
No. of Writes:	11409	3159	4280
Block Size:	32768b+	65536b+	131072b+
No. of Reads:	1196	1765	2063
No. of Writes:	2065	2354	11300
Block Size:	262144b+	524288b+	1048576b+
No. of Reads:	1	3	106
No. of Writes:	0	0	0

%-latency	Avg-latency	Min-Latency	Max-Latency	No. of calls	Fop
-----	-----	-----	-----	----	
0.00	0.00 us	0.00 us	0.00 us	141	FORGET
0.00	0.00 us	0.00 us	0.00 us	15862	RELEASE
0.00	0.00 us	0.00 us	0.00 us	38985	RELEASEDIR
0.00	33.90 us	33.90 us	33.90 us	1	FSYNCDIR
0.00	134.57 us	134.57 us	134.57 us	1	FALLOCATE
0.01	153.39 us	123.50 us	172.33 us	5	RMDIR
0.01	149.02 us	25.24 us	280.28 us	8	READDIR
0.02	256.76 us	204.28 us	329.66 us	6	MKDIR
0.02	127.72 us	63.05 us	220.73 us	15	TRUNCATE
0.02	153.44 us	101.80 us	278.24 us	15	RENAME
0.03	42.87 us	25.44 us	103.08 us	60	READLINK
0.04	135.90 us	67.24 us	296.09 us	30	XATTROP
0.04	81.48 us	15.06 us	216.84 us	51	GETXATTR
0.07	1465.94 us	128.16 us	2210.86 us	5	LINK
0.10	84.19 us	38.87 us	253.69 us	124	OPEN
0.15	37.55 us	11.16 us	299.45 us	400	FLUSH
0.17	162.50 us	92.04 us	858.68 us	103	UNLINK
0.26	48.99 us	15.22 us	2688.13 us	526	ENTRYLK
0.26	236.51 us	156.67 us	573.31 us	109	CREATE
0.26	90.69 us	32.79 us	229.81 us	291	STAT
0.37	189.38 us	86.62 us	467.67 us	196	FTRUNCATE
0.60	66.45 us	19.45 us	161.94 us	899	STATFS
0.93	70.56 us	15.45 us	1843.70 us	1321	FINODELK

2.00	152.13 us	53.12 us	5272.62 us	1321	FXATTROP
2.09	76.37 us	27.49 us	1195.45 us	2741	FSTAT
2.40	69.62 us	15.50 us	367.28 us	3465	LK
4.51	53.58 us	13.81 us	3403.97 us	8451	READ
4.75	52.41 us	1.70 us	4025.41 us	9090	OPENDIR
4.80	143.98 us	35.47 us	5199.62 us	3347	WRITE
4.81	57.25 us	17.02 us	3235.78 us	8432	INODELK
5.06	120.90 us	53.51 us	4871.59 us	4201	SETATTR
18.01	141.41 us	22.43 us	3800.04 us	12778	LOOKUP
23.92	128.27 us	16.64 us	2681.28 us	18711	REaddirP
24.30	2518.68 us	142.53 us	18229.04 us	968	FSYNC

Duration: 9943 seconds

Data Read: 1074532509 bytes

Data Written: 1979205900 bytes

## Stopper le profiling

```
sudo gluster volume profile v0 stop
```

# Crowdsec

## Installation

- [https://docs.crowdsec.net/docs/getting\\_started/install\\_crowdsec/](https://docs.crowdsec.net/docs/getting_started/install_crowdsec/)

## Accès à la console

- <https://app.crowdsec.net/>

## Commandes utiles

Lister les décisions locales

```
cscli decisions
list
Wed Apr 5 15:28:48 2023

+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
| ID | Source | Scope:Value | Reason | Action | Country |
AS | Events | expiration | Alert ID |
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
| 18 | crowdsec | Ip:2a01:cb00:8906:7e00:5401:1966:20ac:69ad | crowdsecurity/http-crawl-non_statics | ban | FR | 3215 Orange | 89 | 3h59m43.090461234s | 18 |
| 17 | crowdsec | Ip:92.175.107.123 | crowdsecurity/http-crawl-non_statics | ban | FR | 3215 Orange | 49 | 3h59m13.25235483s | 17 |
| 16 | crowdsec | Ip:79.81.205.138 | crowdsecurity/http-crawl-non_statics | ban | FR | 15557 Societe Francaise Du Radiotelephone - SFR SA | 66 | 3h54m44.194349115s | 16 |
| 15 | crowdsec | Ip:212.23.165.14 | crowdsecurity/http-crawl-non_statics | ban | FR | 12566
```

```

Societe Francaise Du Radiotelephone - SFR SA | 46 | 3h52m52.665948387s | 15 |
| 14 | crowdsec | Ip:83.206.19.140 | crowdsecurity/http-crawl-non_statics | ban | FR | 3215
Orange | 43 | 3h52m47.901151072s | 14 |
| 13 | crowdsec | Ip:84.55.185.70 | crowdsecurity/http-crawl-non_statics | ban | FR | 9003
Societe Francaise Du Radiotelephone - SFR SA | 42 | 3h51m2.636570684s | 13 |
| 12 | crowdsec | Ip:194.254.79.4 | crowdsecurity/http-xss-probbing | ban | FR | 2200
Renater | 6 | 3h49m7.676288661s | 12 |
| 4 | crowdsec | Ip:2a01:cb11:6a0:2d00:bfe7:82c4:c724:9eb7 | crowdsecurity/http-crawl-non_statics | ban |
FR | 3215 Orange | 91 | 3h46m13.472584547s | 4 |
| 3 | crowdsec | Ip:176.168.162.101 | crowdsecurity/http-crawl-non_statics | ban | FR | 5410
Bouygues Telecom SA | 46 | 3h45m27.591191061s | 3 |
| 2 | crowdsec | Ip:2001:41d0:302:1000::ca9 | crowdsecurity/http-crawl-non_statics | ban | GB |
16276 OVH SAS | 47 | 3h43m25.263040245s | 2 |
| 1 | crowdsec | Ip:134.158.79.158 | crowdsecurity/http-crawl-non_statics | ban | FR | 789
Renater | 45 | 3h41m26.974324678s | 1 |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+
7 duplicated entries skipped

```

## Lister les alertes

cscli alerts list

```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+
| ID | value | reason | country | as |
+-----+-----+-----+-----+-----+
| 15 | Ip:212.23.165.14 | crowdsecurity/http-crawl-non_statics | FR | 12566 Societe
Francaise Du Radiotelephone - SFR SA | ban:1 | 2023-04-05 13:21:28.67736235 +0000 UTC |
| 14 | Ip:83.206.19.140 | crowdsecurity/http-crawl-non_statics | FR | 3215
Orange | ban:1 | 2023-04-05 13:21:35.442813467 +0000 UTC |
| 13 | Ip:84.55.185.70 | crowdsecurity/http-crawl-non_statics | FR | 9003 Societe
Francaise Du Radiotelephone - SFR SA | ban:1 | 2023-04-05 13:19:50.40175296 +0000 UTC |
| 12 | Ip:194.254.79.4 | crowdsecurity/http-xss-probbing | FR | 2200
Renater | ban:1 | 2023-04-05 13:17:56.216060733 +0000 UTC |
| 11 | Ip:194.254.79.4 | crowdsecurity/http-cve-2021-41773 | FR | 2200
Renater | ban:1 | 2023-04-05 13:17:55.755095951 +0000 UTC |

```

10   Ip:194.254.79.4	crowdsecurity/http-path-traversal-probing   FR   2200
Renater	ban:1   2023-04-05 13:17:54.292927884 +0000 UTC
9   Ip:194.254.79.4	crowdsecurity/http-sensitive-files   FR   2200
Renater	ban:1   2023-04-05 13:17:52.403785142 +0000 UTC
8   Ip:194.254.79.4	crowdsecurity/http-crawl-non_statics   FR   2200
Renater	ban:1   2023-04-05 13:17:52.017817973 +0000 UTC
7   Ip:194.254.79.4	crowdsecurity/http-probing   FR   2200
Renater	ban:1   2023-04-05 13:17:52.309312166 +0000 UTC
6   Ip:194.254.79.4	crowdsecurity/http-bad-user-agent   FR   2200
Renater	ban:1   2023-04-05 13:17:52.017572598 +0000 UTC
5   Ip:83.206.19.140	crowdsecurity/http-crawl-non_statics   FR   3215
Orange	ban:1   2023-04-05 13:17:28.44454104 +0000 UTC
4   Ip:2a01:cb11:6a0:2d00:bfe7:82c4:c724:9eb7	crowdsecurity/http-crawl-non_statics   FR   3215
Orange	ban:1   2023-04-05 13:14:35.443575184 +0000 UTC
3   Ip:176.168.162.101	crowdsecurity/http-crawl-non_statics   FR   5410 Bouygues
Telecom SA	ban:1   2023-04-05 13:14:13.380354035 +0000 UTC
2   Ip:2001:41d0:302:1000::ca9	crowdsecurity/http-crawl-non_statics   GB   16276 OVH
SAS	ban:1   2023-04-05 13:12:10.793700983 +0000 UTC
1   Ip:134.158.79.158	crowdsecurity/http-crawl-non_statics   FR   789
Renater	ban:1   2023-04-05 13:10:13.259428338 +0000 UTC

## Supprimer une décision

```

cscli decisions delete -r 1.2.3.0/24
cscli decisions delete -i 1.2.3.4
cscli decisions delete --id 42

```

# Explain

## Tester sur les dernières connexions

```

tail -10 /var/log/httpd/access.miroir.log | cscli explain --verbose --type apache2 -f -
  | s02-enrich
  |   | [ ] crowdsecurity/dateparse-enrich (+2 ~1)
  |     | create evt.Enriched.MarshaledTime : 2023-04-06T11:17:39+02:00

```

```

|       | update evt.MarshaledTime : -> 2023-04-06T11:17:39+02:00
|       | create evt.Meta.timestamp : 2023-04-06T11:17:39+02:00
|     | [ ] crowdsecurity/geoiip-enrich (+13)
|       | create evt.Enriched.ASNNumber : 16276
|       | create evt.Enriched.ASNOrg : OVH SAS
|       | create evt.Enriched.IsInEU : true
|       | create evt.Enriched.Latitude : 48.858200
|       | create evt.Enriched.Longitude : 2.338700
|       | create evt.Enriched.ASNumber : 16276
|       | create evt.Enriched.IsoCode : FR
|       | create evt.Enriched.SourceRange : 51.75.0.0/16
|       | create evt.Meta.SourceRange : 51.75.0.0/16
|       | create evt.Meta.IsoCode : FR
|       | create evt.Meta.ASNOrg : OVH SAS
|       | create evt.Meta.IsInEU : true
|       | create evt.Meta.ASNNumber : 16276
|     | [ ] crowdsecurity/http-logs (+7)
|       | create evt.Parsed.file_ext : .gz
|       | create evt.Parsed.file_name :
6ae72f04c86cd50a9999cb618d7dd3ec5940bb2f24ecf194c2444baaf87a0334-updateinfo.xml.gz
|       | create evt.Parsed.static_ressource : true
|       | create evt.Parsed.file_frag :
6ae72f04c86cd50a9999cb618d7dd3ec5940bb2f24ecf194c2444baaf87a0334-updateinfo.xml
|       | create evt.Parsed.impact_completion : true
|       | create evt.Parsed.file_dir : /rocky/8.7/PowerTools/x86_64/os/repdata/
|       | create evt.Meta.http_args_len : 0
|     | [ ] crowdsecurity/whitelists (~2 [whitelisted])
|       | update evt.Whitelisted : %!s(bool=false) -> true
|       | update evt.WhitelistReason : -> private ipv4/ipv6 ip/ranges
|     |----- parser failure [ ]

```

Remarques :

- Whitelise car Pays FR

## Mises à jour

csccli hub update

INFO[05-04-2023 17:02:49] hub index is up to date

```
INFO[05-04-2023 17:02:49] Wrote new 651136 bytes index to /etc/crowdsec/hub/.index.json
INFO[05-04-2023 17:02:49] dependency of crowdsecurity/base-http-scenarios : missing scenarios
crowdsecurity/http-crawl-non_statics, tainted.
INFO[05-04-2023 17:02:49] update for collection crowdsecurity/http-cve available (currently:1.9, latest:2.0)
INFO[05-04-2023 17:02:49] dependency of crowdsecurity/apache2 : sub collection crowdsecurity/base-http-
scenarios is broken : missing scenarios crowdsecurity/http-crawl-non_statics, tainted.
```

Il faut update crowdsecurity/http-cve !

```
cscli collections list
```

## COLLECTIONS

Name	☐ Status	Version	Local Path
crowdsecurity/apache2	✓ enabled	0.1	/etc/crowdsec/collections/apache2.yaml
crowdsecurity/base-http-scenarios	⚠ enabled,tainted	0.6	/etc/crowdsec/collections/base-http-scenarios.yaml
crowdsecurity/http-cve	⚠ enabled,update-available	1.9	/etc/crowdsec/collections/http-cve.yaml
crowdsecurity/linux	✓ enabled	0.2	/etc/crowdsec/collections/linux.yaml
crowdsecurity/sshd	✓ enabled	0.2	/etc/crowdsec/collections/sshd.yaml

Mise à jour :

```
cscli collections upgrade crowdsecurity/http-cve
```

# Whitelist

Pour repérer les noms sur lesquels s'appuyer, on peut consulter la [taxonomy](#).

Na pas modifier les fichiers dans le dossier hub. Créer un fichier de conf :

```
/etc/crowdsec/parsers/s02-enrich/whitelist-renater.yaml
```

Contenu :

name:

ul/whitelists

description: "Whitelist Renater"

whitelist:

reason: "Renater"

expression:

- evt.Meta.ASNNumber == '2200'

## Lists des parsers :

cscli parsers list

PARSERS

Name	Status	Version	Local Path
crowdsecurity/apache2-logs	✓ enabled	1.3	/etc/crowdsec/parsers/s01-parse/apache2-logs.yaml
crowdsecurity/dateparse-enrich	✓ enabled	0.2	/etc/crowdsec/parsers/s02-enrich/dateparse-enrich.yaml
crowdsecurity/geoip-enrich	✓ enabled	0.2	/etc/crowdsec/parsers/s02-enrich/geoip-enrich.yaml
crowdsecurity/http-logs	✓ enabled	1.1	/etc/crowdsec/parsers/s02-enrich/http-logs.yaml
crowdsecurity/sshd-logs	✓ enabled	2.0	/etc/crowdsec/parsers/s01-parse/sshd-logs.yaml
crowdsecurity/syslog-logs	✓ enabled	0.8	/etc/crowdsec/parsers/s00-raw/syslog-logs.yaml
crowdsecurity/whitelists	⚠ enabled,tainted	?	/etc/crowdsec/parsers/s02-enrich/whitelists.yaml
whitelist-renater.yaml	☐ enabled,local		/etc/crowdsec/parsers/s01-parse/whitelist-renater.yaml

## On peut tester la whitelist :

```
tail -10 /tmp/4 | cscli explain --verbose --type apache2 -f -  
|   └─ ☐ crowdsecurity/whitelists (~2 [whitelisted])  
|       └─ update evt.Whitelisted : %!s(bool=false) -> true
```

```
|      | update evt.WhitelistReason : -> Renater
|      | [ ] crowdsecurity/whitelists-ipul (~1)
|      | | update evt.WhitelistReason : Renater -> UL
|      | [ ] ul/whitelists-fr (~1)
|      | | update evt.WhitelistReason : UL -> FR
|      | [ ] ul/whitelists-renater (~1)
|      | | update evt.WhitelistReason : FR -> Renater
```

Linux

# ZSH

## Afficher la palette des couleurs

```
for i in {0..255}; do print -Pn "%K{$i} %k%F{$i}${(l:3::0)i}%f " "${(M)$((i%6)):#3}:+$\n"; done
```

Linux

# Wireguard

## Intégration a gnome

```
/git/peta-grafana
```

```
└─ sudo nmcli con import type wireguard file /etc/wireguard/proton.conf
```

```
Connexion « proton » (32a2e932-9cf4-4e4f-84e5-49cadbdeb455) ajoutée avec succès.
```

Linux

# Debian

## Importer la clef d'un repo

L'erreur

```
Err :4 http://fr.archive.ubuntu.com/ubuntu jammy InRelease
```

```
  Les signatures suivantes n'ont pas pu être vérifiées car la clé publique n'est pas disponible : NO_PUBKEY  
  871920D1991BC93C
```

Correction

```
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 871920D1991BC93C
```

Linux

# firewalld

Références :

- <https://wiki.fiat-tux.fr/books/administration-syst%C3%A8mes/page/firewalld-un-firewall-simple-a-utiliser>

Linux

# vim

## Indenter/Déindenter

Définir le nombre de caractère :

```
:set shiftwidth=4 expandtab
```

Sélectionner le bloc visuel (CTRL+V)

Indenter : ">"

Déindenter : ">"

## Debian

### Permettre le copier/coller

Décommenter la ligne suivante dans `/etc/vim/vimrc` :

```
let g:skip_defaults_vim = 1
```

Linux

# Screen

## Adapter l'écran en full screen

ECHAP, puis CTRL-A +F

# MySQL - MariaDB

## Afficher les contraintes de cascades

Exemple pour la compréhension :

- <https://mariadb.com/kb/en/foreign-keys/>

## Dans phpmyadmin

Sélectionner la table, puis **Structure**, enfin **vue relationnelle**.

Actions	Propriétés de la contrainte		Colonne	Contrainte de clé étrangère (INNODB)			
	Nom de la contrainte			Base de données	Table	Colonne	
<a href="#">Supprimer</a>	decisions_alerts_decisions	ON DELETE CASCADE	ON UPDATE RESTRICT	alert_decisions	crowdsec	alerts	id
	Nom de la contrainte	ON DELETE RESTRICT	ON UPDATE RESTRICT		crowdsec		

## En CLI

```
show create table decisions ;
KEY `simulated` (`simulated`),
CONSTRAINT `decisions_alerts_decisions` FOREIGN KEY (`alert_decisions`) REFERENCES `alerts` (`id`) ON
DELETE CASCADE
) ENGINE=InnoDB AUTO_INCREMENT=34889411 DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_bin |
```



# Hardened ssh

## Référence :

- <https://korben.info/ssh-audit-outil-indispensable-securiser-vos-serveurs.html>

## Supprimer les algos d'échange de clefs

Ajouter a sshd\_config :

```
# Key Exchange
KexAlgorithms -ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,ecdsa-sha2-nistp256,hmac-sha1,ecdsa-sha2-nistp256
```

## Supprimer les hosts key type vulnérables

Supprimer les fichiers :

- /etc/ssh/ssh\_host\_ecdsa\_key
- /etc/ssh/ssh\_host\_ecdsa\_key.pub

## Supprimer les algos MACs vulnérables

Ajouter a sshd\_config :

```
MACs -hmac-sha1,hmac-sha1-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,sntrup761x25519-  
sha512@openssh.com,umac-128@openssh.com,umac-64-etm@openssh.com,umac-64@openssh.com
```

## Résumé avec une conf adequat

```
KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org  
Ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com  
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com
```

Linux

# Arch Linux

## Gestion des touches de réglage audio

```
sudo pacman -S kglobalaccel plasma-pa
```

# Wi-Fi

## Cisco Prime

### Les rapports

#### AP Utilisation

- [AP Utilisation.pdf](#)

#### Wireless Utilisation

- [Wireless Utilization.pdf](#)

#### Busiests AP

- [Busiest AP.pdf](#)

Ceph

Ceph

# Cephfs

## Obtenir les inormations sur un montage cephfs

```
# getfattr -n ceph.dir.rfiles /data/sauve-db/20230605.0737/enquetes42
```

```
ceph.dir.entries="2" |
```

```
ceph.dir.files="0" |
```

```
ceph.dir.rbytes="41173525694691" |
```

```
ceph.dir.rctime="4294967295.000000000" |
```

```
ceph.dir.rentries="30079806" |
```

```
ceph.dir.rfiles="25700442" |
```

```
ceph.dir.rsubdirs="4379364" |
```

```
ceph.dir.subdirs="2"
```

# BeeGFS

# Configurations

## Mode réplication

Doc

- [https://doc.beegfs.io/latest/advanced\\_topics/mirroring.html](https://doc.beegfs.io/latest/advanced_topics/mirroring.html)

## Définition du buddy group

```
beegfs-ctl --addmirrorgroup --automatic --nodetype=meta --force
beegfs-ctl --addmirrorgroup --automatic --nodetype=storage
```

Vérification :

```
sudo beegfs-ctl --listtargets --
mirrorgroups
          dugravot6@minipc1 19:21:36
MirrorGroupID MGMemberType TargetID  NodeID
=====
      1  primary      1      1
      1  secondary    2      2
```

Positionnement du strip pattern sur la racine BeeGFS :

```
beegfs-ctl --setpattern --numtargets=2 --chunksize=1M --pattern=buddymirror /mnt/beegfs
```

Et vérification :

```
sudo beegfs-ctl --getentryinfo
/mnt/beegfs
          dugravot6@minipc1 19:28:15
```

Entry type: directory

EntryID: root

Metadata buddy group: 1

Current primary metadata node: minipc1 [ID: 1]

Stripe pattern details:

+ Type: Buddy Mirror

+ Chunksize: 1M

+ Number of storage targets: desired: 2

+ Storage Pool: 1 (Default)

# hping3

## Réaliser un flood (ddos)

```
sudo hping3 --flood --rand-source 192.168.1.1
```