

# Administration systèmes

L'administration systèmes au sens large : les outils de base du système, mais aussi comment installer certains logiciels.

- Bases de données : MySQL
  - Défragmenter les tables
  - Optimiser MySQL avec Mysqltuner
- Bases de données : PostgreSQL
  - Donner des droits read-only à un utilisateur
  - Migration d'une version majeure de PostgreSQL à une autre
  - Utiliser Barman pour sauvegarder la base PostgreSQL d'un Gitlab Omnibus
- Logiciels
  - Créer une boutique en ligne avec Wordpress
  - Gitlab
  - Gramps Web
  - RequestTracker
  - TinyTinyRSS : rétablir la consultation web des articles publiés (+ bonus)
  - Une web radio avec MPD
  - Vaultwarden
  - Wisemapping
- Mail
  - Postfix
  - Rspamd

- Vade Secure (antispam propriétaire)
- Outils pour les rapports DMARC
- Outils pour générer et vérifier ses enregistrements SPF/DKIM/DMARC

- Système

- Ajouter une clé GPG de dépôt Debian sans apt-key
- Borg
- Borgmatic
- Crypsetup
- Curl
- Débloquer un RAID coincé en resync=PENDING
- Empêcher l'activation d'un service à son installation
- Exécuter une action à la mise en veille / au réveil
- Firewalld : un firewall simple à utiliser
- Lancer des commandes sudo avec authentification par agent SSH
- LVM
- Monter une ou des partitions contenues dans un fichier qcow2
- Réinstaller les modules Perl installés avec la version précédente de Perl
- Salt
- Sed
- Tmux
- Trucs et astuces
- Supprimer une clé SSH stockée par gpg-agent
- Swap
- Systemd

- Divers

- Avoir les émojis dans Konsole
- Envoyer un fichier sur Nextcloud avec cURL
- Manipuler un ou plusieurs fichiers PDF : PDFtk

# Bases de données : MySQL

# Défragmenter les tables

## Si vous avez accès au terminal

```
mysqlcheck --optimize --all-databases
```

## Si vous n'avez pas accès au terminal

Pour trouver les tables à défragmenter :

```
USE information_schema;  
  
SELECT TABLE_SCHEMA, TABLE_NAME FROM TABLES  
WHERE TABLE_SCHEMA NOT IN ("information_schema", "mysql") AND Data_free > 0;
```

Pour défragmenter les tables :

```
OPTIMIZE TABLE nom_de_la_table;
```

# Optimiser MySQL avec Mysqltuner

[mysqltuner.pl](#) est un script Perl qui va analyser vos bases, la configuration de MySQL et ses statistiques pour vous fournir des indications de modifications de configuration, des actions à prendre, des conseils pour vos requêtes SQL...

C'est très simple à installer et utiliser, même si ça ne fait pas de miracles, MySQL étant ce qu'il est (quoi, ça se voit que j'aime pas MySQL ? ☹)

Ça se passe là pour l'installation : <https://github.com/major/MySQLTuner-perl#downloadinstallation>

Et pour l'utilisation : <https://github.com/major/MySQLTuner-perl#specific-usage>

# Bases de données :

## PostgreSQL

# Donner des droits read-only à un utilisateur

Tiré de <https://stackoverflow.com/questions/760210/how-do-you-create-a-read-only-user-in-postgresql/762649#762649>.

Pour donner un droit read-only sur une table :

```
GRANT SELECT ON mytable TO xxx;
```

Pour donner le droit sur toutes les tables :

```
GRANT SELECT ON ALL TABLES IN SCHEMA public TO xxx;
```

Ceci ne donne le droit que sur les tables existantes. Pour que le droit sur toutes les tables, même celles à venir :

```
ALTER DEFAULT PRIVILEGES IN SCHEMA public  
GRANT SELECT ON TABLES TO xxx;
```

Pour supprimer le droit :

```
REVOKE SELECT ON mytable FROM xxx;  
REVOKE SELECT ON ALL TABLES IN SCHEMA public FROM xxx;  
ALTER DEFAULT PRIVILEGES IN SCHEMA public  
REVOKE SELECT ON TABLES FROM xxx;
```

# Migration d'une version majeure de PostgreSQL à une autre

**NB** : instructions pour le passage de PostgreSQL 13 à PostgreSQL 15 (Debian Bookworm). Voir [ici](#) pour de 9.1 à 9.4 (Debian Jessie), [ici](#) pour de 9.4 à 9.6 (Debian Stretch), [ici](#) pour de 9.6 à 11 (Debian Buster) et [ici](#) pour de 11 à 13 (Debian Bullseye).

**NB** : mettez vous dans un `tmux` avant de commencer la procédure. Prudence est mère de sûreté.

**NB** : si vous utilisez l'extension PostGis, optez pour la méthode moins rapide. N'oubliez pas d'installer le paquet de l'extension postgres pour la nouvelle version de PostgreSQL !

**Attention** : si vous avez des fichiers de configuration dans `/etc/postgresql/XX/main/conf.d`, ils ne seront pas copiés dans le dossier de configuration de la nouvelle version par `pg_upgrade_cluster` ! Pensez à les copier à la main.

## Pré-requis

Vérifiez les paquets PostgreSQL installés sur votre système avec la commande suivante :

```
dpkg -l | grep postgresql
```

Ça vous permettra de voir si vous avez des extensions installées, comme `postgresql-13-repack`, et donc d'installer la version qui va bien pour la nouvelle version de PostgreSQL (en l'occurrence, `postgresql-15-repack`).

## Méthode rapide

On stoppe les clusters PostgreSQL



```
systemctl stop postgresql
```

On vire le cluster de la nouvelle version (normalement vide si on vient juste de l'installer : faire gaffe à ne pas laisser passer de temps entre l'installation de la nouvelle version et la migration des données, pour que personne n'utilise le nouveau cluster)

```
pg_dropcluster --stop 15 main
```

On migre les données

```
pg_upgradecluster -m upgrade 13 main
```

## ATTENTION

Si vous avez mis des `shared_preload_libraries` dans la configuration de votre ancien cluster, il y a des chances que `pg_upgradecluster -m upgrade 13 main` se foire (mais pas si on utilise la méthode `dump` décrite plus bas).

La solution est simple : créez le répertoire `/etc/postgresql/15/main/conf.d` et mettez-y un fichier dont le nom se termine par `.conf` (genre `shared_preload_libraries.conf`).

Dans ce fichier, mettez la configuration de vos `shared_preload_libraries` et ça devrait être bon.

Il faut savoir que cette commande copie les données de l'ancien cluster vers le nouveau. Il vous faut donc avoir au moins une fois la place de `/var/lib/postgresql/13` de disponible. Un contournement est d'utiliser l'option `--link` qui utilisera des *hard links* plutôt qu'une copie. Par contre, si quelque chose foire, vous foirez votre ancien cluster avec, c'est donc dangereux.

On redémarre le cluster (le 15 pour le coup) :

```
systemctl start postgresql
```

On lance l'analyse du nouveau cluster :

```
sudo -u postgres /usr/lib/postgresql/15/bin/vacuumdb --all --analyze-in-stages
```

Si vous utilisiez des extensions, allez dans `/var/log/postgresql`, vous aurez un dossier qui commence par `pg_upgrade` et qui contiendra un script un autre pour supprimer l'ancien cluster et un autre pour mettre à jour vos extensions. Faites alors (**Attention** : je n'ai pas encore testé cette partie, ça vient des tutos des versions précédentes mais vu que la commande précédente a changé, il est possible que celle-ci aussi) :

```
sudo -u postgres psql -f /var/log/postgresql/pg_upgradecluster-13-15-main*/update_extensions.sql
```

# Méthode moins rapide

Cette méthode fait un `pg_dump` et un `pg_restore`. C'est infiniment plus long quand on a de grosses bases de données, mais ça donne un cluster bien propre. Tellement propre que des fois ça foire pour cause de clés dupliquées ?

Vous aurez compris, je n'aime pas tellement cette méthode. Elle a cependant l'avantage d'éviter les problème d'index, vu que ça reconstruit les indexes (ce qui participe à la lenteur de la méthode).

```
systemctl start postgresql  
pg_upgradecluster -m dump 13 main
```

# Fin de migration, partie commune aux deux méthodes

On teste les applis qui utilisent PostgreSQL.

Si ça fonctionne, on vire les anciennes données

```
pg_dropcluster 13 main --stop
```

On vire l'ancienne version de PostgreSQL

```
apt-get autoremove --purge postgresql-13 postgresql-client-13
```

[Source](#)

# Utiliser Barman pour sauvegarder la base PostgreSQL d'un Gitlab Omnibus

Barman est un super logiciel de sauvegarde d'un *cluster* PostgreSQL au fil de l'eau.

**Attention** : ça ne sauvegarde pas les bases de données une à une, ça sauvegarde **tout** le *cluster* PostgreSQL. C'est un peu embêtant de devoir remonter un *cluster* entier pour récupérer une base ou juste quelques données mais comme c'est un outil surpuissant qui permet de récupérer ses données à la milliseconde près, il est facile de passer outre cet inconvénient.

Pour le côté « au fil de l'eau », ça veut dire que les modifications sont répliquées du *cluster* PostgreSQL à Barman en temps quasi réel par le biais des WAL.

Il est fort simple de mettre en place la sauvegarde d'un *cluster* PostgreSQL par Barman. Je vous laisse lire la documentation officielle.

Ce tutoriel vise le cas particulier de la sauvegarde du *cluster* PostgreSQL d'un serveur Gitlab installé via les paquets Omnibus. Avec cette méthode d'installation, c'est Gitlab qui installe sa version de PostgreSQL, à l'endroit qu'il a choisi, et qui le configure. Toute modification directe des fichiers de configuration de PostgreSQL serait supprimée à la mise à jour suivante. Ma méthode configure proprement PostgreSQL de façon à conserver les modifications par-delà les mises à jour.

## Création des utilisateurs

Pas d'utilisateur `postgres` pour Gitlab, mais `gitlab-psql`, et les chemins habituels des outils ont changé.

On se logue :

```
su gitlab-psql -s /bin/bash
```

Et on crée les utilisateurs :

```
/opt/gitlab/embedded/bin/createuser -h /var/opt/gitlab/postgresql/ -s -P barman  
/opt/gitlab/embedded/bin/createuser -h /var/opt/gitlab/postgresql/ -P --replication streaming_barman
```

# Modification de la configuration

Il faut modifier le fichier `/etc/gitlab/gitlab.rb` pour que Gitlab configure PostgreSQL pour nous.

De façon un peu bête, dès qu'on fait écouter PostgreSQL sur une interface réseau, Gitlab n'essaye plus de se connecter en *socket* unix mais par le réseau... donc on va le forcer à utiliser la *socket* :

```
gitlab_rails['db_host'] = "/var/opt/gitlab/postgresql/"
```

Ensuite, c'est l'équivalent de la documentation officielle de Barman :

```
postgresql['listen_address'] = '0.0.0.0'  
postgresql['wal_level'] = "replica"  
postgresql['max_wal_senders'] = 3  
postgresql['max_replication_slots'] = 3
```

À l'exception de la façon de créer des entrées dans

```
postgresql['custom_pg_hba_entries'] = {  
  'barman': [{  
    type: 'hostssl',  
    database: 'all',  
    user: 'barman',  
    cidr: '203.0.113.42/32',  
    method: 'md5'  
  }],  
  'streaming_barman': [{  
    type: 'hostssl',  
    database: 'replication',
```

```
user: 'streaming_barman',  
cidr: '203.0.113.42/32',  
method: 'md5'  
}]  
}
```

Puis il suffit de lancer la commande suivante pour que Gitlab reconfigure PostgreSQL (et tout le reste de Gitlab, mais ce n'est pas ce qui nous intéresse) :

```
gitlab-ctl reconfigure
```

# Logiciels

# Créer une boutique en ligne avec Wordpress

On commence par installer un Wordpress. Je ne vais pas détailler, c'est un sujet fort bien traité sur les Internetz.

## Les extensions

Pour transformer Wordpress en boutique en ligne, il faut installer quelques modules. Mais avant ça, voici ceux que j'ai installé pour la sécurité, les performances... :

- Antispam Bee, pour l'antispam ;
- iThemes Security, pour la sécurité ;
- Smush, pour réduire la taille des images ;
- WP Super Cache, pour les performances.

Ensuite, des extensions pour améliorer la boutique, mais pas obligatoires :

- Contact Form 7, pour le formulaire de contact ;
- Google XML Sitemaps, pour améliorer le référencement (normalement plus nécessaire depuis quelques versions de Wordpress) ;
- Mastodon Autopost, pour pouetter automatiquement quand on ajoute un article à la boutique.

Voici les extensions pour la boutique elle-même :

- WooCommerce, l'extension principale, proposée par la boîte qui développe Wordpress, donc ça va, j'ai assez confiance sur la compatibilité ;
- WooCommerce Blocks, pour faire fonctionner WooCommerce avec le nouvel éditeur de Wordpress ;
- WooSwipe, pour avoir une galerie d'image sur les pages des produits (quand on clique sur l'image pour zoomer, pis pour voir les autres images, vous voyez le genre) ;
- WooCommerce Weight Based Shipping, pour gérer les frais d'envoi selon le poids de la commande ;
- Payment Gateway Based Fees and Discounts for WooCommerce, pour pouvoir ajouter des frais selon la méthode de paiement choisie.

# Le thème

Il va de soit qu'un thème pour un blog a peu de chance d'aller pour faire une boutique. J'ai choisi le thème Shop Isle, que je trouve simple et bien foutu. J'en ai néanmoins fait un thème enfant pour dégager ces cochonneries de google fonts.

## Les frais d'envoi

L'extension « WooCommerce Weight Based Shipping » me permet de définir des frais d'envoi selon le poids de la commande ainsi que sa destination (vous imaginez bien qu'envoyer deux cartes postales en France ne coûte pas le même prix qu'en envoyer 15 dans un autre pays).

Cette extension est parfaite, à l'exception de l'interface pour choisir les pays de destination quand on crée les règles : ça va bien quand on ajoute une ou deux destinations, mais pas quand on doit en sélectionner 12 (France métropolitaine + DOM/TOM) ou plus (les pays de l'UE).

Personnellement, j'ai choisi de faire des frais d'envoi à prix plus ou moins coûtant : le tarif des timbres, arrondi un peu au-dessus pour faire le prix de l'enveloppe. Je ne dis pas que je ne fais pas un peu de bénéfice dessus, mais ça se compte à coup de centimes.

## Le paiement

WooCommerce embarque déjà plusieurs moyens de paiements, je dois dire que c'est très bien foutu !

J'ai activé le virement SEPA, parce que ça ne coûte rien, ni à l'expéditeur, ni au destinataire. Par contre, comme ça prend du temps (le virement prend généralement 24h pour apparaître sur les comptes, sans compter que certaines banques mettent plusieurs jours pour accepter un nouvel IBAN et permettre des virements vers celui-ci), j'ai ajouté la possibilité d'utiliser Paypal : ça propose d'utiliser son compte Paypal (et c'est assez répandu pour que ça soit pratique pour un paquet de gens) pour payer ou la carte bancaire. Par contre, ça m'a fait deux blagounettes :

- pour effectivement pouvoir récupérer les paiements, j'ai dû passer mon compte en compte *business*. Rien de bien méchant, mais la récupération des sous ne fonctionnait pas et rien n'indiquait sur Paypal que c'était ce qu'il fallait faire (il y avait juste un message d'erreur complètement inutile). Une fois mon compte passé en *business*, plus de souci ;
- mais du coup, des frais s'appliquent (pas pour le client, qui paie bien ce que ma boutique lui indiquait, mais pour moi : je ne récupère pas autant d'argent que ce qu'a payé le



client). Comme je ne souhaite pas en être de ma poche, j'ai installé « Payment Gateway Based Fees and Discounts for WooCommerce » qui me permet d'ajouter le pourcentage (3,4%) et le forfait (0,25€) de la commission lorsqu'on choisit Paypal pour payer.

# Conditions générales de vente

Pour les rédiger, j'ai d'abord cherché sur le web, et je suis tombé sur

<https://www.donneespersonnelles.fr/cgv>, qui propose carrément une extension Wordpress. Après l'avoir installée, je me suis contenté de repomper les CGV qu'elle proposait : ça m'a permis, tout d'abord, de les lire, et ensuite de corriger des typos.

Après quoi, j'ai désinstallé l'extension ☐☐

## Conclusion

Je ne pense pas qu'il soit nécessaire pour moi de trop détailler le réglage des différentes extensions : les infos se trouvent assez facilement sur le web, et même si les réglages sont touffus, c'est assez intuitif. La plus grosse partie du temps fut perdue dans la recherche des extensions et du thème kionbien.

Après quelques tâtonnements, la mise en place de ma boutique fut assez simple. J'espère que cet article servira à d'autres pour leur éviter de chercher autant que moi.

# Gitlab

## Recalculer la taille d'un dépôt

Tapez ceci dans la console rails ( `gitlab-rails console` ) :

```
project = Project.find_by_id(24495)
pp project.statistics.repository_size
pp project.repository.size
pp project.repository._uncached_size
project.repository.expire_all_method_caches
pp project.repository.size
project.statistics.refresh!
```

## Recalculer la taille des artefacts

Il y a parfois un bug avec le calcul de la taille des projets, comme par exemple des artefacts virés (pour cause de suppression des *pipelines* afférents) dont le poids n'a pas été enlevé de la taille du projet.

Pour recalculer la taille des artefacts d'un projets, tapez ceci dans la console rails ( `gitlab-rails console` ) :

```
project = Project.find_by_id(23002)
stat = project.statistics.build_artifacts_size
old = project.builds.sum(:artifacts_size).to_i
real = Ci::JobArtifact.artifacts_size_for(project).to_i
diff = real + old - stat
puts "#{Time.now} : ID #{project.id} => stat = #{stat}; old = #{old}; real = #{real}; diff = #{diff}"
ProjectStatistics.increment_statistic(project, :build_artifacts_size, diff)
```

Méthode trouvée sur [https://gitlab.com/gitlab-org/gitlab-foss/-/merge\\_requests/20697#note\\_91526778](https://gitlab.com/gitlab-org/gitlab-foss/-/merge_requests/20697#note_91526778)



# Gramps Web

Gramps Web est un logiciel de généalogie basé sur Gramps et interopérable avec celui-ci.

Son installation est normalement basée sur Docker mais comme j'ai horreur de cette technologie, j'ai décidé de l'installer à la main.

Gramps et Gramps Web utilisent normalement des bases SQLite mais on peut leur faire utiliser des bases PostgreSQL. Cependant, lorsque j'ai tenté ceci, Gramps n'a pas utilisé une base dédiée mais a créé des tables... je ne sais pas très bien où. Bref, cela ne m'a pas l'air très propre (et ce n'est pas grave si on utilise Docker, j'en conviens) et je ne voulais pas pourrir mon serveur PostgreSQL, donc SQLite ira très bien.

## Attention, petit bug avec les gestionnaires de mot de passe

Si vous n'arrivez pas à vous connecter alors que votre gestionnaire de mot de passe remplit bien les champs, c'est à cause de ce bug. Il suffit de modifier l'entrée à la main (un caractère dans chaque champ, et on l'efface) et ça fonctionne.

## Dépendances

```
apt install gramps graphviz gir1.2-gexiv2-0.10 gir1.2-osmgpsmap-1.0 python3-icu python3-virtualenv
```

## Sur votre machine

Installez `gramps`, lancez et créez un arbre familial. Comme nom, j'ai utilisé mon nom de famille, pour ce tutoriel, considérons qu'il s'agit de `Foobar`.

Le lancement de gramps et la création de l'arbre familial ont créé un dossier dans `~/gramps/`. Copiez ce dossier sur votre serveur web :

```
scp -r ~/.gramps votre_serveur:
```

# Création de dossiers divers

```
mv ~votre_user_de_connexion/.gramps/ ~www-data/
mkdir -p /var/www/gramps/config \
        /var/www/gramps/static \
        /var/www/gramps/db \
        /var/www/gramps/media \
        /var/www/gramps/indexdir \
        /var/www/gramps/users \
        /var/www/gramps/thumbnail_cache \
        /var/www/gramps/cache \
        /var/www/gramps/cache/reports \
        /var/www/gramps/cache/export \
        /var/www/gramps/tmp \
        /var/www/gramps/persist \
        /var/www/gramps/secret
touch /var/www/gramps/static/index.html
chown -R www-data: /var/www/gramps/ /var/www/.gramps/
```

# Installation d'un virtualenv

```
sudo -u www-data -s /bin/bash
```

Puis, en tant que `www-data`

```
cd ~/gramps
virtualenv venv
. ./venv/bin/activate
pip install gunicorn gramps-webapi
if [ ! -s /var/www/gramps/secret/secret ]; then
    python3 -c "import secrets;print(secrets.token_urlsafe(32))" | tr -d "\n" > /var/www/gramps/secret/secret
fi
GRAMPSWEB_SECRET_KEY=$(cat /var/www/gramps/secret/secret)
```

```

cat <<EOF >config/config.cfg
TREE="Foobar"
DISABLE_AUTH=False
SECRET_KEY="$GRAMPSWEB_SECRET_KEY"
MEDIA_BASE_DIR="/var/www/gramps/media"
SEARCH_INDEX_DIR="/var/www/gramps/indexdir"
STATIC_PATH="/var/www/gramps/static"
BASE_URL="https://gramps.example.org"
EMAIL_HOST="127.0.0.1"
EMAIL_PORT="25"
EMAIL_USE_TLS=False
DEFAULT_FROM_EMAIL="no-reply+gramps@example.org"
THUMBNAIL_CACHE_CONFIG__CACHE_DIR="/var/www/gramps/thumbnail_cache"
USER_DB_URI="sqlite:///var/www/gramps/users/users.sqlite"
REPORT_DIR="/var/www/gramps/cache/reports"
EXPORT_DIR="/var/www/gramps/cache/export"
EOF

export PYTHONPATH="/var/www/gramps/venv/lib/python3.11/site-packages:/usr/lib/python3/dist-packages"
if [ -z "$(ls -A /var/www/gramps/indexdir)" ]; then
    python3 -m gramps_webapi --config /var/www/gramps/config/config.cfg search index-full
fi

wget https://github.com/gramps-project/gramps-webapi/archive/refs/tags/v1.4.0.tar.gz \
    https://github.com/gramps-project/Gramps.js/releases/download/v23.11.0/grampsj-s-v23.11.0.tar.gz

tar xvf v1.4.0.tar.gz
ln -s gramps-webapi-1.4.0/ gramps-webapi
cd gramps-webapi
python3 -m gramps_webapi --config /var/www/gramps/config/config.cfg user migrate

tar xvf grampsj-s-v23.11.0.tar.gz
ln -s grampsj-s-v23.11.0 grampsj-s

rm v1.4.0.tar.gz grampsj-s-v23.11.0.tar.gz
exit

```

# Nginx

Voici la configuration Nginx que j'utilise, tirée de <https://github.com/gramps-project/Gramps.js/blob/main/default.conf.template>, à mettre dans `/etc/nginx/sites-available/gramps.example.org`.

```
server {
    listen 80;
    listen [::]:80;
    listen 443 http2 ssl;
    listen [::]:443 http2 ssl;

    server_name gramps.example.org;

    ssl_certificate    /etc/letsencrypt/live/gramps.example.org/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/gramps.example.org/privkey.pem;

    access_log /var/log/nginx/gramps.example.org.access.log;
    error_log  /var/log/nginx/gramps.example.org.error.log;

    index index.html;
    root /var/www/gramps/grampsjs;

    location / {
        try_files $uri $uri/ $uri.html /index.html;
    }

    location /api {
        add_header    "Access-Control-Allow-Origin" $http_origin;
        proxy_redirect off;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;

        # WebSocket
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";

        proxy_pass http://127.0.0.1:5000;
    }
}
```

```
}
```

Puis :

```
In -s ../sites-available/gramps.example.org /etc/nginx/sites-enabled
nginx -t && nginx -s reload
```

# Systemd

Voici le service systemd que j'utilise, à mettre dans `/etc/systemd/system/gramps-webapi.service` :

```
[Unit]
Description=Shortened URLs service
Requires=network.target postgresql.service
After=network.target postgresql.service

[Service]
User=www-data
EnvironmentFile=/etc/default/gramps-webapi
WorkingDirectory=/var/www/gramps
ExecStart=/var/www/gramps/venv/bin/gunicorn -w $GUNICORN_NUM_WORKERS -b 127.0.0.1:5000
gramps_webapi.wsgi:app --timeout 120 --limit-request-line 8190
SyslogIdentifier=gramps-webapi
Restart=always

[Install]
WantedBy=multi-user.target
```

Et dans `/etc/default/gramps-webapi` :

```
GRAMPS_API_CONFIG=/var/www/gramps/config/config.cfg
PYTHONPATH="/var/www/gramps/venv/lib/python3.11/site-packages:/usr/lib/python3/dist-packages"
GUNICORN_NUM_WORKERS=2
```

Créez les fichiers puis :

```
systemctl daemon-reload
systemctl enable --now gramps-webapi
```



# Première connexion

Connectez-vous à votre serveur, créez l'utilisateur administrateur et normalement, c'est tout bon !

# RequestTracker

RequestTracker (RT) est un outil de tickets extrêmement puissant et flexible. Tellement flexible qu'on en vient à se prendre la tête pour faire des trucs de oufs.

Petit tour des trucs que j'ai mis en place sur un RT 4.4.0.

## Utiliser le *plus addressing*

De façon simple, pour que RT traite les tickets qui arrivent sur l'adresse email dédiée, on la met dans le `/etc/aliases` de sa machine. Ça fait un truc comme ça :

```
rt:      "|/opt/rt4/bin/rt-mailgate --queue general --action correspond --url https://rt.example.org/"
rt-comment: "|/opt/rt4/bin/rt-mailgate --queue general --action comment --url https://rt.example.org/"
```

Vous noterez que cela met les mails à destination de cette adresse dans la *queue* (ou file) `general`. Or on utilise généralement plus d'une *queue* dans un système de ticket : cela permet de diriger automatiquement vers les personnes les plus à même d'y répondre.

Le problème avec ce système, c'est qu'il faudrait ajouter une adresse dédiée à chaque fois que l'on crée une nouvelle file. Ça peut vite devenir usant.

On va donc utiliser le *plus addressing*. Cette technique, toute bête, consiste à ajouter un discriminant à une adresse mail, précédé généralement d'un `+` (mais on peut configurer son serveur de mail pour utiliser n'importe quel caractère). `rt@example.org` aura alors pour alias (par exemple) `rt+file_bidule@example.org`.

Pour que RT puisse utiliser cette technique, il faut ajouter `--extension=queue` dans la commande du `/etc/aliases` :

```
rt:      "|/opt/rt4/bin/rt-mailgate --extension=queue --queue general --action correspond --url
https://rt.example.org/"
rt-comment: "|/opt/rt4/bin/rt-mailgate --extension=queue --queue general --action comment --url
https://rt.example.org/"
```

Voilà ! Il ne vous reste plus qu'à créer vos files via l'interface web. Attention, créez-les avec un nom qui passera dans une adresse mail. Pas d'espace par exemple.

RT récupérera le nom de la file kivabien dans la partie entre le `+` et le `@` et placera automatiquement le ticket dans cette file, tout en gardant la file `general` par défaut.

# Les articles

Quoi de plus casse-pieds que de se répéter encore et encore en donnant toujours la même réponse ? Heureusement il y a les articles qui peuvent vous servir de réponses pré-enregistrées :-)

## Création des classes et des articles

Allez dans le menu `Administration > Articles > Classes > Ajouter`, créez vos classes (j'en ai créé une par file, n'ayant pas réussi à assigner automatiquement des articles aux files), cochez `Tous les articles de cette classe doivent être disponibles sous forme de liste sur la page de réponse d'un ticket`, décochez `Inclure le résumé de l'article` et `Inclure le nom de l'article` et cochez `Include le champs personnalisé 'Content' > Value` (oh la belle typo de traduction) qui apparaîtra après avoir enregistré la classe (pour ces trois derniers, vous faites comme vous le sentez hein).

Liez la classe à une file via le menu `S'applique à`.

Voilà, vous n'avez plus qu'à créer vos articles dans la classe que vous venez de créer via le menu `Articles > Ajouter`.

Et là, magie, lorsque vous répondez via l'interface web, vous pourrez choisir une réponse pré-enregistrée.

## Placement des articles dans la réponse

Je suis un grand fan du *bottom-posting*, mais RT place l'article au-dessus de la citation du message précédent. Remédions à cela.

```
cd /opt/rt4
mkdir -p local/html/Elements/
cp share/html/Elements/MessageBox local/html/Elements/
vi local/html/Elements/MessageBox
```

Cherchez la ligne contenant

```
% $m->comp('/Articles/Elements/IncludeArticle', %ARGS) if $IncludeArticle;
```

et remplacez-la par

```
% if ($IncludeArticle) {
%   my $article = $m->scomp('/Articles/Elements/IncludeArticle', %ARGS);
%   $article   =~ s{\n}{<br />}g;
%   $article   = RT::Interface::Email::ConvertHTMLToText($article);
%   $Default   .= $article unless ($Default =~ s/(.*) (-- .*)/$1$article$2/m);
% }
```

Hop ! votre article se trouve maintenant entre la citation et votre signature :-)

(un redémarrage de RT est peut-être nécessaire pour que cela soit pris en compte)

## Ajout des articles pertinents dans le mail de notification d'un nouveau message

Une des forces de RT est de permettre aux intervenants de répondre aux tickets par mail. Le problème est que cela empêche de piocher dans les réponses pré-enregistrées.

Qu'à cela ne tienne, ajoutons-les au mail de notification envoyé aux membres du support.

Allez dans [Administration > Global > Modèles > Choisir](#). Il faut modifier le modèle [Notification de modification HTML](#) (oui, j'ai traduit le nom de mes modèles, mais il est simple à repérer, il est utilisé par les *scripts* 8 et 11).

Ajoutez ceci en bas du modèle :

```
{ my $hotlist = RT::Articles->new( RT->SystemUser );
$hotlist->LimitHotlistClasses;
$hotlist->LimitAppliedClasses( Queue => $Ticket->QueueObj );
my $content = "-- \n<p><b>Réponses pré-enregistrées pour cette catégorie de tickets:</b></p>";

if ($hotlist->Count) {
while (my $article = $hotlist->Next) {
$content .= '<p><b>'. $article->Name. '</b><br/>';
my $class = $article->ClassObj;
my $cfs = $class->ArticleCustomFields;
my %include = (Name => 1, Summary => 1);
$include{"CF-Title-".$_->Id} = $include{"CF-Value-".$_->Id} = 1 while $_ = $cfs->Next;
$include{$_} = not $class->FirstAttribute("Skip-$_") for keys %include;

while (my $cf = $cfs->Next) {
```

```

next unless $include{"CF-Title-".$cf->Id} or $include{"CF-Value-".$cf->Id};
my $values = $article->CustomFieldValues($cf->Id);
if ($values->Count == 1) {
    my $value = $values->First;
    if ($value && $include{"CF-Value-".$cf->Id}) {
        $content .= '<br/>';
        my $c    = $value->Content || $value->LargeContent;
        $c =~ s/\r?\n/<br\/>/g;
        $content .= $c;
    }
} else {
    my $val = $values->Next;
    if ($val && $include{"CF-Value-".$cf->Id}) {
        $content .= '<br/>';
        my $c    = $value->Content || $value->LargeContent;
        $c =~ s/\r?\n/<br\/>/g;
        $content .= $c;
    }
    while ($val = $values->Next) {
        if ($include{"CF-Value-".$cf->Id}) {
            $content .= '<br/>';
            my $c    = $value->Content || $value->LargeContent;
            $c =~ s/\r?\n/<br\/>/g;
            $content .= $c;
        }
    }
}
$content .= "<br/>-----</p>\n";
}
}
$content;
}
{$content}

```

C'est moche et long, je sais. Dites-vous que j'ai passé plus d'une après-midi pour trouver ça, la [documentation](#) est inexistante pour faire ça.

Les intervenants n'auront plus qu'à copier-coller l'article qui se trouve au bas de leur mail de notification dans leur réponse :-)

# Commandes par mail

C'est beau de répondre par mail, mais il faut encore se connecter à l'interface web pour effectuer certaines actions. Comme je suis fier d'être fainéant, j'ai créé un *scrip* pour autoriser certaines actions par mail.

Mais avant ça, précisions :

- RT permet aux intervenants de discuter du ticket *sans que cela soit vu par le créateur du ticket* : c'est le but de l'adresse `rt-comment@example.org` du début de l'article. On va utiliser cette adresse pour piloter RT par mail
- un *scrip* est une action effectuée par RT en réponse à un évènement, en utilisant de façon optionnelle un modèle. Typiquement, il y a un *scrip* qui envoie (action) un mail (d'après un modèle) aux membres du support lorsqu'un ticket est créé (évènement).

Créons donc un *scrip*. Menu `Administration > Scripts > Ajouter`.

- Condition (évènement) => Lors d'un commentaire
- Action => définie par l'utilisateur
- Modèle => Modèle vide

Dans le `Programme de préparation d'action personnalisé` :

```
if ($self->TransactionObj->Attachments->First->Content =~ m/#(JePrends|Fermeture|Spam|Move:.*)/i) {  
    return 1;  
} else {  
    return 0;  
}
```

Oui, j'aurais pu faire un *one-liner*, mais il faut que ça reste lisible facilement, et quand on passe des heures à faire des bidouilles comme ça, on apprécie les codes lisibles en un coup d'œil.

Dans le `Code d'action personnalisée (commit)` :

```
if ($self->TransactionObj->Attachments->First->Content =~ m/#JePrends/i) {  
    if ( $self->TicketObj->OwnerAsString eq " " ) {  
        my $id = $self->TransactionObj->Creator;  
        $RT::Logger->info("Setting owner to ".$id);  
        $self->TicketObj->SetOwner($id, 'SET');  
    }  
} elsif ($self->TransactionObj->Attachments->First->Content =~ m/#Fermeture/i) {  
    $RT::Logger->info("Closing ticket");  
}
```

```

    $self->TicketObj->SetStatus('resolved');
} elsif ($self->TransactionObj->Attachments->First->Content =~ m/#Spam/i) {
    my $ticket = $self->TicketObj;
    my ($status, $msg) = $ticket->SetStatus('rejected');
    $RT::Logger->error("Couldn't delete ticket: $msg") unless $status;

    my $requestors = $ticket->Requestor->UserMembersObj;
    while (my $requestor = $requestors->Next) {
        $requestor->SetDisabled(1);
        $RT::Logger->info("Disabling user ".$requestor->Format." because he's likely a spammer");
    }
} elsif ($self->TransactionObj->Attachments->First->Content =~ m/#Move:(.*)/i) {
    my $new_queue = $1;
    my $ticket = $self->TicketObj;

    my ($result, $msg) = $ticket->SetQueue($new_queue);
    if ($result) {
        $RT::Logger->info("Moving ticket to queue ".$new_queue);
    } else {
        $RT::Logger->error("Error while moving ticket to queue ".$new_queue." : ".$msg);
    }
} elsif ($self->TransactionObj->Attachments->First->Content =~ m/#Merge:(.*)/i) {
    my $target = $1;
    my $ticket = $self->TicketObj;

    $ticket->MergeInto($target);
    $RT::Logger->info("Merging ticket into ticket ".$target);
}

return 1;

```

Voilà, enregistrez et c'est bon.

Lorsqu'un commentaire contiendra une commande, elle sera exécutée :

- `#JePrends` => l'intervenant s'assigne le ticket
- `#Fermeture` => le ticket est marqué comme résolu
- `#Spam` => le ticket est supprimé et son auteur ne pourra plus ouvrir de tickets, son adresse mail sera blacklistée
- `#Move:file_de_tickets` => le ticket est basculé vers la file de tickets spécifiée
- `#Merge:no_ticket` => fusionne le ticket avec le ticket dont on donne le n°

# Et le spam alors ?

Pour le spam, préparez d'abord un `spamassassin` pour votre serveur de mails. Ce n'est pas l'objet de cet article, il n'y a qu'à fouiller un peu le web pour trouver des tutos.

On va recréer un *scrip*, mais avant cela on va créer une nouvelle file nommée `spam` (menu `Administration > Files > Ajouter`).

Pour notre nouveau *scrip* :

- Condition (évènement) => Lors d'une création
- Action => définie par l'utilisateur
- Modèle => Modèle vide

Dans le `Programme de préparation d'action personnalisé` :

```
if ( $self->TicketObj->Subject !~ /\[ .* \]/i ) {  
    my $inMessage = $self->TransactionObj->Attachments->First;  
  
    # if no message attachment - assume web UI  
    return 0 if (!$inMessage);  
  
    # exit if not email message  
    return 0 if (!$inMessage->GetHeader('Received'));  
  
    return ($inMessage->GetHeader('X-Spam-Level') =~ m/\*+/) ? 1 : 0;  
} else {  
    return 1;  
}
```

Dans le `Code d'action personnalisée (commit)` :

```
my $spamlevel = $self->TransactionObj->Attachments->First->GetHeader('X-Spam-Level');  
if ($spamlevel =~ m/\*\*\*+/) {  
    if ($spamlevel =~ m/\*\*\*\*\*/) {  
        $RT::Logger->info("This mail seems to be a spam => deleting");  
        $self->TicketObj->Delete();  
    } else {  
        $RT::Logger->info("This mail seems to be a spam => queue spam");  
        $self->TicketObj->SetQueue('spam');  
    }  
}
```



```
}  
return 1;
```

Avec cela, les mails ayant un score de 5 ou plus au *spamLevel* seront supprimés, et ceux qui ont entre 3 et 5 vont au purgatoire, dans la file `spam`.

Prenez soin de déplacer ce *scrip* tout en haut de la liste pour qu'il soit le premier exécuté.

# Plugins

En vrac, les plugins que j'utilise :

- RT::Authen::ExternalAuth::LDAP
- RT::Extension::LDAPImport
- RT::Extension::ReportSpam

Les deux premiers sont maintenant intégrés à RT, il n'y a pas besoin de les installer, juste de les configurer. Ils servent respectivement à assurer l'authentification LDAP à l'interface web, et à importer en masse les comptes du LDAP pour permettre à l'administrateur de mettre les collaborateurs dans les bons groupes sans attendre qu'ils se soient logués une première fois.

Le dernier plugin ajoute un `S` dans le menu des tickets, permettant de les déclarer comme spam d'un simple clic.

# Conclusion

On peut faire de merveilleuses choses avec RT, pour peu que l'on ait le temps de fouiller dans la documentation officielle... et dans le code !

Une fois bien configuré, il devrait permettre d'alléger la charge de travail du groupe de support et je peux vous dire que pour en faire depuis plus de deux ans pour Framasoft et bien plus pour mon ancien boulot, ce n'est pas quelque chose à négliger ☐☐

NB : bien évidemment, ce superbe logiciel est en Perl :D

# TinyTinyRSS : rétablir la consultation web des articles publiés (+ bonus)

On peut, dans TTRSS, publier des articles de ses flux RSS. Cela permet de partager aisément des articles. Les articles sont publiés dans un flux RSS que d'autres personnes pourront à leur tour mettre dans un lecteur de flux RSS.

Je couple cette fonctionnalité avec [Feed2toot](#), qui me permet d'envoyer un pouet sur [Mastodon](#) pour chaque nouvel article que je publie.

Le flux RSS généré a longtemps eu un document [XSLT](#) associé afin de rendre le flux lisible dans un navigateur web. Ce document XSLT a été supprimé le [28 mars 2020](#) par le projet TTRSS, mais il est fort simple de le remettre en place.

## Ajouter la référence au document XSLT

On va commencer par copier le fichier modèle du flux dans le dossier `templates.local` : cela permettra de conserver les modifications de ce fichier malgré les mises à jour de TTRSS.

```
cp templates/generated_feed.txt templates.local/generated_feed.txt
```

On ajoute alors cette ligne à la ligne 2 du fichier copié :

```
<?xml-stylesheet type="text/xsl" href="templates.local/atom-to-html.xsl"?>
```

Vous noterez que je place le document XSLT dans le dossier `templates.local` : il me semble logique de mettre mes modifications dans un dossier `*.local`.

# Créer le document XSLT

Je suis parti du fichier précédemment fourni par TTRSS, mais je l'ai un peu modifié pour :

- ajouter une feuille de style qui permet d'avoir un thème sombre pour les visiteurs qui utilisent un thème sombre sur leur système d'exploitation (voir la caractéristique média `prefers-color-scheme`). Attention, ça ne fonctionne pas sur tous les navigateurs et tous les système d'exploitation.
- ajouter une ancre sur les titres des articles, me permettant ainsi de mettre un lien qui enverra les visiteurs au bon article, quand bien même d'autres ont été publiés depuis (tant que l'article est dans le flux RSS, bien sûr, les flux RSS ne contenant qu'un nombre fini d'articles)

Voici mon fichier `templates.local/atom-to-html.xsl` :

```
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet
  xmlns:atom="http://www.w3.org/2005/Atom"
  xmlns:xsl="http://www.w3.org/1999/XSL/Transform" version="1.0">

  <xsl:output method="html"/>

  <xsl:template match="/atom:feed">
    <html>
      <head>
        <title><xsl:value-of select="atom:title"/></title>
        <link rel="stylesheet" type="text/css" href="themes/light.css"/>
        <link rel="stylesheet" type="text/css" href="themes.local/dark-mode.css"/>
        <script language="javascript" src="lib/xsl_mop-up.js"></script>
      </head>

      <body onload="go_decoding()" class="ttrss_utility">

        <div id="cometestme" style="display:none;">
          <xsl:text disable-output-escaping="yes">&amp;&amp;</xsl:text>
        </div>

        <div class="rss">

          <h1><xsl:value-of select="atom:title"/></h1>
```

```

<p class="description">This feed has been exported from
  <a target="_new" class="extlink" href="http://tt-rss.org">Tiny Tiny RSS</a>.
  It contains the following items:</p>

<xsl:for-each select="atom:entry">
  <h2 id="{atom:id}"><a target="_new" href="{atom:link/@href}"><xsl:value-of
select="atom:title"/></a></h2>

  <div name="decodeme" class="content">
    <xsl:value-of select="atom:content" disable-output-escaping="yes"/>
  </div>

  <xsl:if test="enclosure">
    <p><a href="{enclosure/@url}">Extra...</a></p>
  </xsl:if>

</xsl:for-each>

</div>

</body>
</html>
</xsl:template>

</xsl:stylesheet>

```

Et voici la feuille de style pour le thème sombre automatique, que je place dans `themes.local/dark-mode.css` :

```

@media (prefers-color-scheme: dark) {
  * {
    scrollbar-color: #2a2c2e #1c1e1f;
  }
  html, body, input, textarea, select, button {
    background-color: #181a1b;
  }
  html, body, input, textarea, select, button {
    border-color: #575757;
  }
}

```

```

    color: #e8e6e3;
}
body.ttrss_utility {
    background-image: initial;
    background-color: rgb(27, 29, 30);
    color: rgb(232, 230, 227);
}
body.ttrss_utility .content {
    background-image: initial;
    background-color: rgb(24, 26, 27);
    border-top-color: rgb(58, 58, 58);
    border-right-color: rgb(58, 58, 58);
    border-bottom-color: rgb(58, 58, 58);
    border-left-color: rgb(58, 58, 58);
    box-shadow: rgba(0, 0, 0, 0.1) 0px 1px 1px -1px;
}
}

```

# Configuration Feed2toot

Pour l'installation de Feed2toot, je vous laisse regarder la [documentation officielle](#), ce n'est pas l'objet de cet article.

Voici ma configuration Feed2toot, qui poste le lien vers mon flux, le titre de l'article, l'adresse d'origine de l'article et le résumé de l'article :

[mastodon]

instance\_url=https://framapiaf.org

user\_credentials=/etc/feed2toot/feed2toot\_usercred.txt

client\_credentials=/etc/feed2toot/feed2toot\_clientcred.txt

[cache]

cachefile=/opt/feed2toot.db

[rss]

uri=https://ttrss.fiat-tux.fr/public.php?op=rss&id=-2&key=60c63a21c2928546b4485017876fe850c6ebcebd

toot=[veille] https://lstu.fr/veille-luc#{id} « {title} » {link} {summary}

Notez le `#{id}` après `https://lstu.fr/veille-luc` (qui est une URL raccourcie vers mon flux RSS) : cela permet de renvoyer pile à l'article plutôt que de laisser les gens descendre et rechercher l'article ☐☐

# Une web radio avec MPD

Rien de plus simple que de faire une web radio pour diffuser sa musique.

## MPD

On installe MPD :

```
apt install mdp
```

On modifie sa configuration dans `/etc/mpd.conf` (je ne mets que les paramètres intéressants à modifier) :

```
# chemin vers le dossier contenant la musique
music_directory "/var/lib/mpd/music"

# Là c'est vous qui voyez. Moi je mets à off pour pas que ça surveille le dossier en permanence
# Je déclenche la mise à jour de la bibliothèque via le client MPD
auto_update "no"

# Zeroconf/avahi, c'est intéressant dans un réseau local, beaucoup moins sur un serveur
zeroconf_enabled "no"

# On commente l'audio_output de type `alsa`
# et on décommente celui de type `httpd`
audio_output {
    type            "httpd"
    name            "Ma radio perso"
    #   encoder      "vorbis"           # optional, vorbis or lame
    port            "8000"
    bind_to_address "127.0.0.1"         # optional, IPv4 or IPv6
    #   quality      "5.0"              # do not define if bitrate is defined
    bitrate         "128"               # do not define if quality is defined
    #   format       "44100:16:1"
    #   max_clients   "0"                # optional 0=no limit
}
```

On redémarre MPD :

```
systemctl restart mpd
```

# Un client

J'ai tendance à préférer les outils en CLI :

```
apt install ncmpcpp
```

Lancez-le.

- **F1** pour afficher l'aide.
- **u** pour mettre à jour la mise à jour de la bibliothèque.
- **z** pour utiliser le mode aléatoire
- **r** pour mettre la file d'attente en boucle
- **1** pour voir la file d'attente des fichiers. Dans cette vue :
  - **Entrée** pour lancer un morceau
- **2** pour voir la liste des fichiers (suivant l'arborescence de votre dossier de musique).

Dans cette vue :

- **Espace** pour ajouter à la file d'attente,
- **Entrée** pour aller dans un dossier.

Pour le reste, lisez l'aide.

# Proxifier via Nginx

Pas grand chose de particulier, c'est de la proxification classique :

```
location / {  
    proxy_set_header Host $host;  
    proxy_connect_timeout 300s;  
    proxy_read_timeout 300s;  
    proxy_send_timeout 300s;  
    proxy_pass http://127.0.0.1:8000/;  
}
```

(je mets pas toute la configuration Nginx, c'est pas le sujet ici)



# Vaultwarden

Comment compiler et installer proprement le clone de [Bitwarden](#) en [Rust](#). Les bases de données disponibles à ce jour sont PostgreSQL, MySQL et SQLite.

**NB:** Vaultwarden s'appelait précédemment Bitwarden\_rs et a été renommé le 27 avril 2021. Cette page a été remaniée en conséquence. N'hésitez pas à me signaler des soucis (voir l'adresse mail sur [ma page de présentation](#)).

**NB:** J'ai supprimé les informations pour compiler soit-même l'interface web, il fallait NodeJs 14 minimum, ce qui implique de rajouter les explications pour installer cette version de Nodejs. Bref, flemme. Le tutoriel utilise maintenant les *releases* créées par Dani Garcia (auteur de Vaultwarden).

## Compilation

Installation des dépendances :

```
sudo apt install pkg-config libssl-dev build-essential
```

Si vous voulez utiliser MySQL comme base de données :

```
sudo apt install default-libmysqlclient-dev
```

Si vous voulez utiliser PostgreSQL comme base de données :

```
sudo apt install libpq-dev
```

## Installation de Rust

Installation de rustup, qui nous fournira le compilateur Rust :

```
curl https://sh.rustup.rs -sSf > rustup.sh
```

On n'exécute pas direct un script tiré du web ! On regarde d'abord s'il ne va pas faire de saloperies :

```
vi rustup.sh
```

On le rend exécutable :

```
chmod +x rustup.sh
```

On installe le compilateur Rust (il sera dans notre `$HOME`) :

```
./rustup.sh --default-host x86_64-unknown-linux-gnu --default-toolchain stable
```

Attention ! Ceci n'est valable que pour l'architecture x86\_64 ! Si vous voulez installer Vaultwarden sur une architecture ARM (comme les Raspberry Pi), il faut adapter la commande, a priori en remplaçant `x86\_64-unknown-linux-gnu` par `armv7-unknown-linux-gnueabi`.

On source un fichier qui nous permet de l'appeler

```
source $HOME/.cargo/env
```

## Mise à jour de Rust (si vous l'avez déjà installé via rustup)

```
rustup update
```

## Compilation

Clonez le projet vaultwarden.

```
git clone https://github.com/dani-garcia/vaultwarden
```

Compilation de Vaultwarden :

```
cd vaultwarden
# Pour les mises à jour
git fetch
git checkout -b "v$(git tag --sort=v:refname | tail -n1)" "$(git tag --sort=v:refname | tail -n1)"
# on supprime les artefacts de la compilation précédente
cargo clean
```

```
cargo build --release --features postgresql
# ou sqlite, ou mysql, selon la bdd que vous souhaitez utiliser
cd -
```

Le résultat de la compilation est dans `vaultwarden/target/release/`.

## Récupération de l'interface web

D'abord, si vous ne l'avez pas déjà fait, récupérez la clé GPG de Dani Garcia et de Black Dex, un contributeur :

```
gpg --keyserver keyserver.ubuntu.com --recv-keys B9B7A108373276BF3C0406F9FC8A7D14C3CD543A \
3C5BBC173D81186CFFDE72A958C80A2AA6C765E1 \
13BB3A34C9E380258CE43D595CB150B31F6426BC
```

On va utiliser une variable pour le numéro de version, c'est plus simple pour les mises à jour (on change la variables, mais pas les commandes) :

```
VERSION=v2025.4.0
```

Ensuite, il faut aller sur [https://github.com/dani-garcia/bw\\_web\\_builds/releases](https://github.com/dani-garcia/bw_web_builds/releases) pour récupérer la dernière version de l'interface web patchée par Dani Garcia. Ou utiliser `wget` :

```
wget https://github.com/dani-garcia/bw_web_builds/releases/download/$VERSION/bw_web_$VERSION.tar.gz \
https://github.com/dani-garcia/bw_web_builds/releases/download/$VERSION/bw_web_$VERSION.tar.gz.asc
```

On vérifie la signature de l'archive:

```
gpg --verify bw_web_$VERSION.tar.gz.asc bw_web_$VERSION.tar.gz
```

On décompresse l'archive :

```
tar xvf bw_web_$VERSION.tar.gz
```

Si vous faites une mise à jour, supprimez l'ancienne version de l'interface web :

```
rm -rf vaultwarden/target/release/web-vault/
```

Et on déplace l'interface web dans le dossier où attend le résultat de la compilation de vaultwarden :

```
mv web-vault/ vaultwarden/target/release/web-vault/
```

Si vous faites une mise à jour :

```
sudo rm -rf /opt/vaultwarden/web-vault/ &&  
sudo rsync -a --info=progress2 vaultwarden/target/release/web-vault/ /opt/vaultwarden/web-vault/ &&  
sudo chown -R www-data: /opt/vaultwarden/web-vault/
```

# Pour une mise à jour

Suivez le tuto d'installation avec ces précautions préalables :

- coupez le service vaultwarden ;
- faites des sauvegardes de votre installation (fichiers, données de la base de données) avant de faire le `rsync` d'installation (voir plus bas). Pour les fichiers :

```
sudo rsync -a --info=progress2 /opt/vaultwarden/ /opt/vaultwarden_$(date +%F).bak/
```

# Installation

On va installer Vaultwarden dans `/opt/vaultwarden` et on le fera tourner avec l'utilisateur `www-data` :

```
sudo rm -rf /opt/vaultwarden/deps/* /opt/vaultwarden/build/*  
sudo rsync -a --info=progress2 vaultwarden/target/release/ /opt/vaultwarden/  
sudo chown -R www-data: /opt/vaultwarden
```

Puis on va créer un service `systemd` , `/etc/systemd/system/vaultwarden.service` :

```
[Unit]  
Description=Vaultwarden Server (Rust Edition)  
Documentation=https://github.com/dani-garcia/vaultwarden  
After=network.target  
  
[Service]  
# The user/group vaultwarden is run under. the working directory (see below) should allow write and read  
access to this user/group  
User=www-data  
Group=www-data
```

```
# The location of the .env file for configuration
EnvironmentFile=/etc/vaultwarden.env

# The location of the compiled binary
ExecStart=/opt/vaultwarden/vaultwarden

# Set reasonable connection and process limits
LimitNOFILE=1048576
LimitNPROC=64

# Isolate vaultwarden from the rest of the system
PrivateTmp=true
PrivateDevices=true
ProtectHome=true
ProtectSystem=strict

# Only allow writes to the following directory and set it to the working directory (user and password data are
stored here)
WorkingDirectory=/opt/vaultwarden/
ReadWriteDirectories=/opt/vaultwarden/

[Install]
WantedBy=multi-user.target
```

Pour l'interface d'administration, on va créer un token avec :

```
/opt/vaultwarden/vaultwarden hash
```

La configuration se fait via des variables d'environnement qu'on va mettre dans `/etc/vaultwarden.env` :

```
SIGNUPS_ALLOWED=false
WEBSOCKET_ENABLED=true
ADMIN_TOKEN=Un token généré avec `/opt/vaultwarden/vaultwarden hash`
ROCKET_ADDRESS=127.0.0.1
WEBSOCKET_ADDRESS=127.0.0.1
SMTP_HOST=127.0.0.1
SMTP_FROM=vaultwarden@example.org
SMTP_PORT=25
SMTP_SSL=false
```

Vous remarquerez que je dis à Vaultwarden d'envoyer les mails via le serveur SMTP local. À vous de faire en sorte qu'il fonctionne. Allez voir le [wiki](#) du projet ou le [modèle de fichier d'environnement](#) pour voir quelles variables vous pourriez ajouter, enlever, modifier... Vous pouvez faire ça pour voir les nouveautés :

```
sudo vimdiff -c 'map <F2> :diffget<cr>]czz | map <F3> ]czz | syn off | windo set wrap | winc h' \  
/etc/vaultwarden.env vaultwarden/.env.template
```

Puis :

```
sudo systemctl daemon-reload  
sudo systemctl enable --now vaultwarden  
sudo systemctl status vaultwarden
```

# Nginx

On installe Nginx s'il n'est pas déjà installé :

```
sudo apt install nginx
```

Configuration du virtualhost :

```
# The `upstream` directives ensure that you have a http/1.1 connection  
# This enables the keepalive option and better performance  
#  
# Define the server IP and ports here.  
upstream vaultwarden-default {  
    zone vaultwarden-default 64k;  
    server 127.0.0.1:8080;  
    keepalive 2;  
}  
  
# Needed to support websocket connections  
# See: https://nginx.org/en/docs/http/websocket.html  
# Instead of "close" as stated in the above link we send an empty value.  
# Else all keepalive connections will not work.  
map $http_upgrade $connection_upgrade {  
    default upgrade;  
    "" "";  
}  
  
server {  
    listen 80;  
    listen [::]:80;
```

```
listen 443 ssl http2;
listen [::]:443 ssl http2;
server_name vaultwarden.example.org;


access_log /var/log/nginx/vaultwarden.access.log;
error_log /var/log/nginx/vaultwarden.error.log;


ssl_certificate /etc/letsencrypt/live/vaultwarden.example.org/fullchain.pem;
ssl_certificate_key /etc/letsencrypt/live/vaultwarden.example.org/privkey.pem;


ssl_session_timeout 5m;
ssl_session_cache shared:SSL:5m;


ssl_prefer_server_ciphers On;
ssl_protocols TLSv1.2;
ssl_ciphers
'EECDH+aRSA+AESGCM:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH:+CAMELLIA256:+AES256:+CAM
ELLIA128:+AES128:+SSLv3:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ECDSA';


ssl_dhparam /etc/ssl/private/dhparam4096.pem;
add_header Strict-Transport-Security max-age=15768000; # six months
gzip off;


# Redirect HTTP to HTTPS
if ($https != 'on') {
    rewrite ^/(.*)$ https://vaultwarden.example.org/$1 permanent;
}


root /var/www/html;


# Allow large attachments
client_max_body_size 525M;


location ^~ '/.well-known/acme-challenge' {
    default_type "text/plain";
    root /var/www/certbot;
}


location / {
    proxy_http_version 1.1;
```

```
proxy_set_header Upgrade $http_upgrade;
proxy_set_header Connection $connection_upgrade;


include /etc/nginx/proxy_params;
## /etc/nginx/proxy_params contient normalement ceci :
#proxy_set_header Host $http_host;
#proxy_set_header X-Real-IP $remote_addr;
#proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
#proxy_set_header X-Forwarded-Proto $scheme;


proxy_pass http://vaultwarden-default;
}
}
```

Pour créer `/etc/ssl/private/dhparam4096.pem` :

```
sudo openssl dhparam -out /etc/ssl/private/dhparam4096.pem 4096
```

Pour le certificat Let's Encrypt, on commente le brol relatif à `ssl` puis :

```
sudo nginx -t && sudo nginx -s reload
sudo apt install certbot
sudo mkdir /var/www/certbot/
certbot certonly --rsa-key-size 4096 --webroot -w /var/www/certbot/ --agree-tos --text --renew-hook
"/usr/sbin/nginx -s reload" -d vaultwarden.example.org
```

Une fois qu'on a le certificat, on décommente le brol `ssl` puis :

```
sudo nginx -t && sudo nginx -s reload
```

# Sauvegarde

Créer le script de sauvegarde `/opt/backup_vaultwarden.sh` :

```
#!/bin/bash
function vwbackup {
    DATE=$(date '+%a%H')

    # Database, ONLY FOR SQLITE!
```



```

if [[ ! -d /opt/backup_vaultwarden/sqlite-backup/ ]]; then
    mkdir -p /opt/backup_vaultwarden/sqlite-backup/
fi

echo ".backup /opt/backup_vaultwarden/sqlite-backup/db.${DATE}.sqlite3" | sqlite3
/opt/vaultwarden/data/db.sqlite3 2>> /opt/backup_vaultwarden/backup.log

if [[ "$?" -ne "0" ]]; then
    echo "Something went wrong with Vaultwarden database backup, please see
/opt/backup_vaultwarden/backup.log on "$(hostname) | mail -s "Vaultwarden database backup"
youraddress@mail.example.org
    vwbackup
fi

# Files
if [[ ! -d /opt/backup_vaultwarden/files-backup/ ]]; then
    mkdir -p /opt/backup_vaultwarden/files-backup/
fi

rsync -a --delete --exclude db.sqlite3 /opt/vaultwarden/data/ /opt/backup_vaultwarden/files-backup/${DATE}/
2>> /opt/backup_vaultwarden/backup.log

if [[ "$?" -ne "0" ]]; then
    echo "Something went wrong with Vaultwarden files backup, please see
/opt/backup_vaultwarden/backup.log on "$(hostname) | mail -s "Vaultwarden files backup"
youraddress@mail.example.org
    vwbackup
fi
}
vwbackup

```

Puis :

```

sudo chmod +x /opt/backup_vaultwarden.sh
sudo mkdir /opt/backup_vaultwarden
sudo chown www-data: /opt/backup_vaultwarden
sudo apt install sqlite3 ## Si vous utilisez SQLite

```

Puis, dans le cron de l'utilisateur `www-data` :

```
42 4 * * * /opt/backup_vaultwarden.sh
```

# Logs

J'aime bien avoir mes logs dans un dossier dédié pour ce genre de service.

Dans `/etc/rsyslog.d/vaultwarden.conf` :

```
if $programname == 'vaultwarden' then /var/log/vaultwarden/vaultwarden.log
if $programname == 'vaultwarden' then ~
```

Dans `/etc/logrotate.d/vaultwarden` :

```
/var/log/vaultwarden/vaultwarden.log
{
    rotate 52
    dateext
    weekly
    missingok
    notifempty
    compress
    sharedscripts
    postrotate
        invoke-rc.d rsyslog rotate > /dev/null
    endscript
}
```

Puis :

```
sudo mkdir /var/log/vaultwarden
sudo chown root:adm /var/log/vaultwarden
sudo systemctl restart rsyslog
```bash
```

```
## Fail2ban
```

Un fail2ban qui surveille les logs, ça permet de bloquer les petits malins qui font du bruteforce

```
```bash
sudo apt install fail2ban
```

Dans `/etc/fail2ban/filter.d/vaultwarden.conf` :

```
[INCLUDES]
before = common.conf
```

[Definition]

failregex = ^.\*Username or password is incorrect\. Try again\. IP: <HOST>\. Username:.\*\$

ignoreregex =

Dans `/etc/fail2ban/jail.d/vaultwarden.local` :

[vaultwarden]

enabled = true

port = 80,443

filter = vaultwarden

action = iptables-allports[name=vaultwarden]

logpath = /var/log/vaultwarden/vaultwarden.log

maxretry = 3

bantime = 14400

findtime = 14400

Pour la page d'admin, dans `/etc/fail2ban/filter.d/vaultwarden-admin.conf` :

[INCLUDES]

before = common.conf

[Definition]

failregex = ^.\*Unauthorized Error: Invalid admin token\. IP: <HOST>.\*\$

ignoreregex =

Dans `/etc/fail2ban/jail.d/vaultwarden-admin.local` :

[vaultwarden-admin]

enabled = true

port = 80,443

filter = vaultwarden-admin

action = iptables-allports[name=vaultwarden]

logpath = /var/log/vaultwarden/vaultwarden.log

maxretry = 3

bantime = 14400

findtime = 14400

Finalement :

```
sudo systemctl restart fail2ban
```

# Conclusion

Voilà, vous devriez avoir un serveur Vaultwarden fonctionnel. Plus qu'à aller sur l'interface web que vous venez de mettre en place ou télécharger les clients et à les utiliser !

Pour importer vos mots de passe de Firefox, il faut passer par une application pour les exporter, puis aller dans les outils de votre client (ou de l'interface web).

# Wisemapping

Installation de quelques outils dont on a besoin

```
sudo apt install jetty9 maven git nodejs npm
```

Récupération des sources

```
git clone https://github.com/wisemapping/wisemapping-open-source.git
```

Configuration et compilation

```
cd wisemapping-open-source
# On configure
vi wise-webapp/src/main/webapp/WEB-INF/app.properties
mvn package
```

Pour virer les appels à *Google analytics*, après la compilation :

```
for i in $(grep -Rcl google-analytics)
do
    sed -i -e "s@https://www\.google-analytics\.com/analytics\(_debug\)\?.js@@g" $i
done
for i in $(grep -Rcl googletagmanager); do
    sed -i -e "s@https://www\.googletagmanager\.com/@#@g" $i
done
mvn package
```

Pour créer et initialiser la base de données, regarder dans `config/database/`, modifier les fichiers (parce que le mot de passe `password`, c'est très bof, et ça force le nom de la base de données utilisée) et exécuter le SQL.

Installation dans Jetty

```
cp -a wise-webapp/target/wisemapping.war /usr/share/jetty9/webapps/root.war
chown jetty: /usr/share/jetty9/webapps/root.war
systemctl restart jetty9.service
```

Jetty devrait écouter de base sur `http://127.0.0.1:8080` (il me semble), y a plus qu'à mettre un nginx devant avec, pour l'essentiel :

```
location / {  
    include proxy_params;  
    proxy_pass http://127.0.0.1:8080;  
}
```

Pour que Jetty prenne en compte les en-têtes `X-Forwarded` envoyés par Nginx (configurés dans `/etc/nginx/proxy_params`), il faut ajouter `http-forwarded` à la liste des modules de Jetty, dans `/etc/jetty9/start.ini`. Par exemple, il faut passer de

```
--module=deploy,http,jsp,jstl,websocket,ext,resources
```

à

```
--module=deploy,http,jsp,jstl,websocket,ext,resources,http-forwarded
```

et redémarrer Jetty :

```
systemctl restart jetty9.service
```

Cela permet à Jetty de rediriger vers la bonne adresse (sans ça, à la connexion, il renvoie vers la version non-sécurisée (`http`) du site quand bien même on a pris soin de mettre en place du `https`).

# Mail

Tout ce qui concerne le mail

# Postfix

## Autoriser le point pour faire du *plus addressing*

Le *plus addressing* est une solution simple pour donner des adresses mail différentes selon les sites auxquels vous donnez votre adresse. Cela permet de faire des filtres selon la destinataire et éventuellement de retrouver l'origine de la fuite si vous commencez à recevoir du spam sur une adresse *plus-adressée*.

Concrètement, vous pouvez donner `foo+truc@exemple.org` à la place de `foo@exemple.org`, vous recevrez les mails envoyés à l'adresse avec un `+`.

Certains sites mal codés considèrent malheureusement qu'une adresse mail avec un `+` est invalide. Pour contourner ces sites de gougnaftiers, on peut utiliser le point (`.`) à la place du caractère `+`.

## N'autoriser que le point

Là, c'est tout simple : il suffit de changer le paramètre `recipient_delimiter` dans `/etc/postfix/mail.cf` et de recharger `postfix`.

Si vous n'avez pas encore utilisé le *plus addressing*, je vous conseille de faire ça, c'est le plus simple.

## Autoriser les deux : le point et le plus

Il semblerait qu'on puisse, depuis Postfix 2.11, mettre plusieurs caractères dans `recipient_delimiter` (genre `recipient_delimiter = +.`). Mais ça ne fonctionne pas chez moi, sans doute à cause de mon



groupware ([Bluemind](#)) qui fait plein de trucs tout seul (et ça me va très bien) mais qui, du coup, n'aime pas trop certaines modifications manuelles. Il semblerait aussi qu'il faille bidouiller Dovecot si vous l'utilisez derrière postfix.

Donc on va faire une réécriture de l'adresse de destination des mails.

Créez un fichier `/etc/postfix/point_addressing` qui contiendra ceci :

```
/^(.*)\.(.*)@(.*$) $1+$2@$3
```

**NB :** Depuis ma mise à jour de Bluemind en version 4, il a fallu que j'ajoute ça à ce même fichier :

```
/^(.*)\+(.*)@(.*$) $1@$3
```

Dans `/etc/postfix/main.cf`, ajoutez `regexp:/etc/postfix/point_addressing` au début du paramètre `virtual_alias_maps` (l'ordre est important : la recherche d'alias va regarder les fichiers dans l'ordre). Chez moi, c'est passé de

```
virtual_alias_maps = hash:/etc/postfix/virtual_alias
```

à

```
virtual_alias_maps = regexp:/etc/postfix/point_addressing, hash:/etc/postfix/virtual_alias
```

Rechargez `postfix`, profitez ☐☐

Si vous avez des utilisatrices dont l'identifiant comporte un point... là, j'avoue que c'est un peu compliqué. Il faudrait certainement adapter l'expression rationnelle, ou faire un autre fichier pour le `virtual_alias_maps`.

# Permettre l'utilisation de Postfix par un serveur distant avec authentification

Si le serveur en face a une adresse IP fixe, on peut se contenter de l'ajouter au paramètre `mynetworks`, de relancer postfix et hop, le serveur est autorisé à utiliser le serveur postfix comme relais. Mais parfois, on veut une authentification avec login et mot de passe : serveur mutualisé, adresse IP non fixe, etc.

Tout d'abord : postfix n'est pas capable de faire de l'authentification. Il délègue ça à un service externe via `SASL`. On utilise `dovecot` ou `cyrus` pour ça.

# Dovecot

## Installation

```
apt install dovecot-core
```

## Configuration

Dans le fichier `/etc/dovecot/conf.d/10-auth.conf`, changer le `auth_mechanisms` pour :

```
auth_mechanisms = plain login
```

Dans le même fichier, décommenter cette ligne à la fin du fichier :

```
!include auth-passwdfile.conf.ext
```

Et commenter celle-ci :

```
#!include auth-system.conf.ext
```

Dans `/etc/dovecot/conf.d/10-master.conf`, décommenter / ajouter ceci dans le bloc `service auth {}` :

```
unix_listener /var/spool/postfix/private/auth {  
  mode = 0666  
  user = postfix  
  group = postfix  
}
```

Et on relance le service :

```
systemctl restart dovecot.service
```

# Gestion des utilisateurs

Avec la configuration qu'on a choisi plus haut (la [doc](#) vous tend les bras si vous voulez explorer d'autres pistes), les utilisateurs sont gérés dans le fichier `/etc/dovecot/users`.

Le format est le suivant (le format est complexe, je ne traite que les champs qui nous intéressent, encore une fois la doc...) :

```
login:{FORMAT DU MOT DE PASS}mot de passe::::::
```

Pour le login `foo`, le mot de passe `bar`, le tout sans chiffrement, ça donne :

```
foo:{PLAIN}bar::::::
```

Si vous voulez (et vous le voulez) chiffrer le mot de passe :

```
doveadm pw -s sha256-crypt
```

Tapez le mot de passe deux fois, la commande vous donnera un truc du genre de :

```
{SHA256-CRYPT}$5$bMeZKE.YWD8D2F6q$JpGqMfx4G6lyRuOkN2uKdRvexzrwjXNo6dWkUuZZjV/
```

Il suffit alors d'utiliser ça en lieu et place de `{PLAIN}bar` dans le fichier `/etc/dovecot/users`.

Pour voir les algorithmes de chiffrement disponible, faites `doveadm pw -l`.

Normalement, pas besoin de recharger dovecot quand on modifie le fichier.

Pensez à modifier les permissions du fichier :

```
chown root:dovecot /etc/dovecot/users  
chmod 640 /etc/dovecot/users
```

NB : si vous utilisez [Rspamd](#) pour la signature DKIM, créez des utilisateurs avec une adresse mail contenant le domaine (ex : `foo@example.org:{PLAIN}bar::::::`) ou mettez `allow_username_mismatch = true;` dans `/etc/rsnspamd/local.d/dkim_signing.conf` et rechargez le service rspamd, sinon la signature DKIM ne sera pas ajoutée au mail.

# Postfix

Ajouter ceci à `/etc/postfix/main.cf` :

```
#### SASL ####
## specify SASL type ##
smtpd_sasl_type = dovecot

## path to the SASL socket relative to postfix spool directory i.e. /var/spool/postfix ##
smtpd_sasl_path = private/auth

## postfix appends the domain name for SASL logins that do not have the domain part ##
smtpd_sasl_local_domain = example.org

## SASL default policy ##
smtpd_sasl_security_options = noanonymous

## for legacy application compatibility ##
#broken_sasl_auth_clients = yes

## enable SMTP auth ##
smtpd_sasl_auth_enable = yes

## smtp checks ##
## these checks are based on first match, so sequence is important ##
smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination
```

Et on relance le service, bien sûr :

```
systemctl reload postfix
```

Notez le `permit_mynetworks` : on n'utilise l'authentification SASL que si le serveur n'est pas dans la liste des serveurs autorisés par adresse IP.

# Rspamd

Rspamd est plus qu'un simple antispam : il s'occupera aussi d'ajouter les signatures DKIM et ARC à vos mails sortants et pourra faire la liaison avec un antivirus. C'est un tout-en-un vraiment sympa ☐☐

## Installation

Je vous laisse aller voir ça sur le [site de rspamd](#).

# Création et utilisation de clés DKIM et ARC

## Création

NB : par défaut, Rspamd va chercher les clés dans le dossier `/var/lib/rspamd/dkim/`. Cependant, je préfère les mettre dans le dossier `/etc/dkim` : on pense plus souvent à sauvegarder `/etc` que `/var/lib/rspamd/`.

```
rspamadm dkim_keygen -k /etc/dkim/example.com.dkim.key -b 2048 -s 'dkim' -d example.com > /etc/dkim/example.com.dkim.txt
```

- `-k` => fichier qui contiendra la clé
- `-b` => nombre de bits de la clé (défaut : 1024)
- `-s` => nom du sélecteur (voir plus bas)
- `-d` => le domaine à signer

À noter, la redirection de la sortie de la commande vers `/etc/dkim/example.com.dkim.txt` : ce fichier contient l'enregistrement DNS que vous devrez créer pour votre domaine pour déclarer la clé DKIM utilisée.

Cela ressemble à :

```
dkim._domainkey IN TXT ( "v=DKIM1; k=rsa; "
```

```
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzgAF2ozDnleUGRbtwmbTEg1zmomoSLhOjsT96q0P+JOr  
TPnGX/olWwx2MkTRW46gSU7Ya1ByG9EKfEQo3V+Zfr5xeY+O0ksl8nrHUK56haW7kqVAEhyo4NPqhhTRUheAIMgL  
byYIFNOqpQDCdmfyn6fvObK6caqtNXAWy3vWTeMacBgx1JGfrYE1NFyNqKcfHcbtXXfSGNo6phVz9K"
```

```
"1TlI3wvZhdW3hBwgq49cZ5yp0IsrlLOfqMOnHcS83YHINMRVVGvPko8+ucMhKktbAoDdEMMWupxyWGs1M1xKW0  
RQxFyYi5oZhSTW53VpyzldrlWXInerDRW2hn1amA2dlWwewIDAQAB"  
);
```

Le sélecteur est une clé qui servira, on le voit, dans le nom de l'enregistrement DNS. Il sera indiqué dans l'en-tête de signature DKIM des mails, et donc utilisé par les antispams pour aller chercher le bon enregistrement DNS qui déclare la clé utilisée. Par défaut, pour DKIM, rspamd utilise le sélecteur `dkim` et je ne vois pas de raison d'en changer (en plus ça ferait des modifications de configuration supplémentaires).

Le sélecteur est aussi utilisé par défaut par rspamd pour choisir la clé à utiliser pour signer les mails.

Pour les clés ARC, c'est tout pareil, mais on change le sélecteur pour `arc`. Vous pouvez utiliser le même dossier `/etc/dkim`, c'est ce que je fais.

## Utilisation par Rspamd

Si vous avez utilisé `/var/lib/rspamd/dkim/` (et `/var/lib/rspamd/arc` pour ARC) comme chemins à la place de `/etc/dkim`, vous n'avez rien à faire : rspamd cherche les clés des domaines avec le chemin `/var/lib/rspamd/dkim/$domain.$selector.key` (et `/var/lib/rspamd/arc/$domain.$selector.key` pour ARC).

Si comme moi vous utilisez `/etc/dkim` pour ranger vos clés, il va falloir surcharger la configuration de rspamd.

Créez les fichiers `/etc/rspamd/local.d/dkim_signing.conf` et `/etc/rspamd/local.d/arc.conf` et mettez-y ceci :

```
path = "/etc/dkim/$domain.$selector.key"
```

Relancez rspamd, et c'est normalement tout bon ☺

## Ajouter les en-têtes donnant le spam score dans les mails

Certains spams passent, des mails légitimes ne passent pas... pour comprendre ça, on peut aller dans les logs pour y retrouver les infos qui vont bien, ou alors on ajoute directement ces informations dans les en-têtes des mails ☐☐

Dans le fichier `/etc/rspamd/local.d/milter_headers.conf`, mettez :

```
extended_spam_headers = true;
```

Relancez rspamd, et c'est normalement tout bon ☐☐

## Se prémunir du phishing

Rspamd est capable d'utiliser les listes d'URL de phishing d'[OpenPhish](#) et [PhishTank](#).

L'utilisation de PhishTank est activée de base dans `/etc/rspamd/modules.d/phishing.conf` (sur la version des dépôts officiels de rspamd, tout du moins).

Pour utiliser OpenPhish :

```
echo 'openphish_enabled = true;' >> /etc/rspamd/local.d/phishing.conf
systemctl reload rspamd.service
```

Notez que Rspamd est capable de gérer la liste premium d'OpenPhish (qui contient plus d'URL).

On peut aussi utiliser un fichier local contenant une liste d'adresses malveillantes.

Pour cela :

```
cat <<EOF >> /etc/rspamd/local.d/phishing.conf
generic_service_enabled = true;
generic_service_name = 'PhishStats';
generic_service_symbol = "PHISHED_PHISHSTATS";
generic_service_map = "file:///opt/phishstats_urls.txt";
EOF
```

Je prends ici les adresses de [PhishStats](#). Pour construire le fichier (le site fourni un CSV, inutilisable, donc) :

```
curl -s https://phishstats.info/phish_score.csv |
  grep -v "^#" |
  cut -f 3 -d ',' |
```

```
tr -d "" > /tmp/phishstats_urls.txt
if [[ $(wc -l /tmp/phishstats_urls.txt | cut -f 1 -d ' ') -gt 0 ]]; then
    mv /tmp/phishstats_urls.txt /opt
    systemctl reload rspamd.service
fi
```

Il suffit de mettre ce bout de code dans un script et d'appeler ce script régulièrement pour mettre à jour les adresses de PhishStats (le site dit que le fichier est mis à jour toutes les 90 minutes).

Il faut encore définir un poids pour le symbole qu'on vient d'ajouter. Éditez

```
/etc/rspamd/local.d/phishing_group.conf
```

```
symbols {
    "PHISHED_PHISHSTATS" {
        weight = 7.0;
        description = "Phished URL";
        one_shot = true;
    }
}
```

Et relancez rspamd :

```
systemctl reload rspamd.service
```

# Comprendre les symboles Rspamd

Dans les en-têtes ajoutés dans les mails via la configuration juste au-dessus, il y a les symboles rspamd. Ce sont différentes catégories de vérification antispam, avec un score. C'est la somme de ces scores qui donne le spam score qui va déclencher l'acceptation du mail, son classement en spam ou carrément son refus.

Cependant ces symboles n'ont pas forcément une signification évidente. Voici une liste de symboles expliqués (cette liste n'est pas exhaustive) :

- `ARC_REJECT` : la signature ARC est-elle valide ?
- `ARC_SIGNED` : existe-t-il une signature ARC ?
- `ASN` : score de l'IP par rapport à son ASN auquel il appartient. Rspamd fait des statistiques au niveau des adresses IP, sous-réseaux, ASN et pays
- `BAYES_SPAM` : analyse bayésienne du mail
- `CTYPE_MIXED_BOGUS` : mails `multipart/mixed` sans partie non-textuelle



- DKIM\_SIGNED : le message possède une signature DKIM (sans préjuger de sa validité)
- DKIM\_TRACE : un truc avec DKIM, c'est sûr, mais je sais pas quoi exactement
- DMARC\_POLICY\_SOFTFAIL : la vérification DMARC a échoué
- FORGED\_RECIPIENTS : les destinataires ne sont pas les mêmes que la commande mail `RCPT TO`
- FORGED\_RECIPIENTS\_MALLIST : les destinataires ne sont pas les mêmes que la commande mail `RCPT TO` mais le message vient d'une liste de diffusion
- FORGED\_SENDER : l'en-tête `Sender` est forgé (différence entre l'en-tête `From` et `MAIL FROM`)
- FORGED\_SENDER\_MALLIST : l'en-tête `Sender` est forgé (différence entre l'en-tête `From` et `MAIL FROM`) mais le message vient d'une liste de diffusion
- FROM\_NEQ\_ENVFROM : l'adresse `From` est différente de celle de l'enveloppe
- FROM\_NO\_DN : l'en-tête `From` n'a pas de *display name*
- HAS\_LIST\_UNSUB : possède l'en-tête `List-Unsubscribe`
- HAS\_REPLYTO : est-ce que le mail a bien un header `Reply-To` ?
- LOCAL\_WL\_IP : vérification de la liste blanche locale
- MALLIST : le mail semble venir d'une liste de diffusion
- MID\_RHS\_MATCH\_FROM : est-ce qu'on retrouve l'adresse `From` dans le `Message-ID` ?
- MID\_RHS\_NOT\_FQDN : le `Message-ID` ne contient pas de nom de domaine pleinement qualifié (*fqdn*)
- MIME\_GOOD : `Content-Type` connu
- MIME\_HTML\_ONLY : pas de version texte du message HTML
- MIME\_TRACE : un truc qui a à voir avec les types MIME, mais je sais pas quoi exactement
- MV\_CASE : l'en-tête `MIME-Version` n'a pas la bonne casse (ex : `Mime-Version`)
- ONCE\_RECEIVED : il n'y a qu'un seul en-tête `Received`, ce qui peut indiquer une machine compromise (d'après la doc de rspamd)
- PRECEDENCE\_BULK : envoi de mail en masse
- RCPT\_COUNT\_ONE : un seul destinataire
- RCVD\_COUNT\_THREE : le mail a entre 3 et 5 en-tête `Received` (a transité par 3/4/5 serveurs différents)
- RCVD\_IN\_DNSWL\_FAIL : fail du test `[[https://www.dnswl.org]]` (une liste blanche d'adresses IP)
- RCVD\_TLS\_LAST : le dernier serveur (*last hop*) utilise un transport sécurisé
- R\_DKIM\_ALLOW : DKIM correct
- RECEIVED\_SPAMHAUS\_FAIL : a priori, blacklisté chez Spamhaus (une RBL)
- R\_EMPTY\_IMAGE : le message contient des parties texte vides et une image
- REPLYTO\_DN\_EQ\_FROM\_DN : le *display name* de l'en-tête `Reply-To` est-il le même que celui du `From` ?
- REPLYTO\_DOM\_NEQ\_FROM\_DOM : le domaine `Reply-To` ne correspond pas à celui de `From`
- R\_SPF\_ALLOW : respect de l'enregistrement SPF
- TO\_DN\_NONE : Aucun des destinataires n'a de *display names*
- TO\_DOM\_EQ\_FROM\_DOM : le domaine `To` est le même que celui de `From`

# Mettre des domaines en liste d'autorisation pour les vérifications des SURBL

Contexte : vous avez un domaine qui se retrouve dans une SURBL (une liste noire de domaines de phishing/spam/etc). Problème : si quelqu'un souhaite vous envoyer un mail d'abuse à propos de ce domaine sans le protéger (genre en n'écrivant pas `[https://lstu [.] fr]`), ça arrive dans vos spams et vous ne voyez pas les abus.

Pour éviter ce problème, vous pouvez mettre des exceptions pour les vérifications des SURBL.

Mettez simplement vos domaines dans `/etc/rspamd/local.d/maps.d/surbl-authorized_list.inc.local` (un domaine par ligne) et rechargez `rspamd`.

Exemple de fichier `/etc/rspamd/local.d/maps.d/surbl-authorized_list.inc.local` :

```
lstu.fr
```

## Augmenter le score de spam des mails à destination d'une certaine adresse mail

Exemple d'usage : comme je publie des modules Perl sur le [CPAN](#), j'ai une adresse `@cpan.org` qui a été automatiquement créée, dont les mails sont transférés chez moi, et qui se retrouve spammée à longueur de journée. Comme il y a quand même une possibilité d'avoir des mails légitimes dessus, je ne la bloque pas complètement. Par contre, augmenter le score de spam permet de faire passer des mails qui ont déjà un petit score de spam dans la catégorie « Oui, c'est bien du spam ».

C'est le module `multimap` qui s'occupe de ça (voir la [documentation](#)).

Créer le fichier `/etc/rspamd/local.d/multimap.conf` :

```
cpanmail_to {  
    type = "header";  
}
```

```
header = "Delivered-To";
filter = "email:addr";
map = "file:///etc/rspamd/local.d/cpan_map";
symbol = "CPAN_DELIVERED_TO";
description = "Delivered-To is ldidry@cpan.org";
score = 5.0;
}
```

Le score à ajouter dépend bien évidemment des seuils que vous avez réglés dans `rspamd`.

Créer le fichier `/etc/rspamd/local.d/cpan_map` :

```
ldidry@cpan.org
```

Redémarrer `rspamd` et profiter d'une boîte mail avec moins de spam ☑

## Forcer une politique DMARC

Quand la politique DMARC n'est pas respectée, ça influence le score de spam, mais ça ne rejette pas forcément le mail. Pour forcer la politique appliquée selon ce que recommande l'enregistrement DMARC du domaine du mail, mettre ceci dans `/etc/rspamd/local.d/dmarc.conf` (adaptez selon vos envies, bien évidemment) et redémarrer `rspamd` :

```
actions = {
  quarantine = "add_header";
  reject = "reject";
}
```

## Modifier le score d'un mail selon le langage détecté

Tiré de <https://github.com/postalserver/postal/discussions/1754>

Mettre ceci dans `/etc/rspamd/local.d/lang_filter.lua` :

```
local rspamd_logger = require 'rspamd_logger'
```

```

local deny_langs = {
    ['zh'] = true,
    ['ru'] = true,
}

rspamd_config:register_symbol{
    type = 'normal',
    name = 'LANG_FILTER',
    score = 6.0,
    group = 'LANG_FILTER',
    description = 'Deny languages',
    flags = 'fine',
    callback = function(task)
        local any_ok = false
        local parts = task:get_text_parts() or {}
        local ln
        for i,p in ipairs(parts) do
            ln = p:get_language() or ""
            local dash = ln:find('-')
            if dash then
                -- from zh-cn to zh
                ln = ln:sub(1, dash-1)
            end

            if deny_langs[ln] then
                rspamd_logger.infox("lang for %1 is %2 -DENY", i, ln)
            else
                any_ok = true
                rspamd_logger.infox("lang for %1 is %2 -OK", i, ln)
                break
            end
        end
        if any_ok or not ln or #ln == 0 then
            return false
        else
            return true
        end
    end,
}

```

Mettre ceci dans `/etc/rspamd/local.d/rspamd.lua` :

```
local local_conf = rspamd_paths['LOCAL_CONFDIR']

-- filtrer selon le langage
dofile(local_conf .. '/local.d/lang_filter.lua')
```

Pour faire l'inverse et n'autoriser que certains langages, voir

<https://rspamd.com/doc/lua/examples.html#languages-filter>.

# Envoyer des rapport DMARC

Cela se fait avec la commande `rspamadm dmarc_report`, à mettre dans une tâche cron, mais il faut un peu de configuration supplémentaire.

Mettre ceci dans `/etc/rspamd/local.d/dmarc.conf` :

```
reporting {
    # Required attributes
    enabled = true; # Enable reports in general
    email = 'dmarc_reports@example.com'; # Source of DMARC reports
    domain = 'example.com'; # Domain to serve
    org_name = 'Example organisation'; # Organisation
    # Optional parameters
    bcc_addrs = ["postmaster@example.com"]; # additional addresses to copy on reports
    report_local_controller = false; # Store reports for local/controller scans (for testing only)
    helo = 'rspamd.localhost'; # Helo used in SMTP dialog
    smtp = '127.0.0.1'; # SMTP server IP
    smtp_port = 25; # SMTP server port
    from_name = 'Rspamd'; # SMTP FROM
    msgid_from = 'rspamd'; # Msgid format
    max_entries = 1k; # Maximum amount of entries per domain
    keys_expire = 2d; # Expire date for Redis keys
    #only_domains = '/path/to/map'; # Only store reports from domains or eSLDs listed in this map
    # Available from 3.3
    #exclude_domains = '/path/to/map'; # Exclude reports from domains or eSLDs listed in this map
    #exclude_domains = ["example.com", "another.com"]; # Alternative, use array to exclude reports from
    domains or eSLDs
}
```

Il est aussi nécessaire d'avoir un serveur redis et de configurer le module DMARC pour l'utiliser.

Mettre ceci dans `/etc/rspamd/local.d/dmarc.conf` :

```
servers = "127.0.0.1";
```

Mail

# Vade Secure (antispam propriétaire)

Orange, Free, SFR, LaPoste, Gandi... utilisent l'antispam Vade (anciennement Vade Secure).

Si Vade change un réglage, ça peut mettre plein de mails en spam très vite.

Pour les contacter (ils sont plutôt réactifs, entre quelques heures et 2 jours), il faut se créer un compte sur <https://sendertool.vadecure.com/fr/>, ajouter les IPs des serveurs qui envoient des mails et créer un ticket.

# Outils pour les rapports DMARC

Les rapports DMARC sont des fichiers XML, généralement compressés, envoyés par les fournisseurs de mail à l'adresse mail définie par le paramètre `rua` des enregistrements DMARC.

Différents outils existent pour lire et exploiter ces rapports :

- lire un rapport en CLI : <https://github.com/keltia/dmarc-cat> ;
- avec un semblant de GUI, et qui se base sur le précédent : <https://framagit.org/flat-tux/dmarc-cat-ui> (juste histoire de pouvoir lire un rapport depuis un mail) ;
- pour stocker plein de rapports, les filtrer et pouvoir les lire : <https://github.com/techsneeze/dmarcts-report-viewer> ;
- dans le même style, on m'a signalé <https://github.com/liuch/dmarc-srg> ;
- pour avoir des stats agrégées avec plein de jolis graphiques : <https://github.com/debricked/dmarc-visualizer>.



# Outils pour générer et vérifier ses enregistrements SPF/DKIM/DMARC

Le site qui propose une panoplie complète de génération et de vérification de ces enregistrements et que je trouve trop pratique est <https://dmarcly.com/tools/>. Il y a tout ce qu'il faut dessus, et c'est bien expliqué.

Simple. Basique.

# Systeme

# Ajouter une clé GPG de dépôt Debian sans apt-key

L'ajout de clé GPG de dépôt Debian avec `apt-key` est une méthode dépréciée. On ajoute maintenant la clé (au bon format) dans le dossier `"/etc/apt/trusted.gpg.d"` :

```
curl -s https://deb.nodesource.com/gpgkey/nodesource.gpg.key |  
gpg --dearmor |  
sudo tee /etc/apt/trusted.gpg.d/deb.nodesource.com.gpg >/dev/null
```

# Borg

<https://borgbackup.readthedocs.io/>

## Quelques mots sur Borg

- il est **très** simple d'usage ;
- les données sont dédupliquées ;
- les sauvegardes peuvent être compressées ;
- les sauvegardes peuvent être effectuées en local ou à distance ;
- les sauvegardes peuvent être montées (et donc utilisées) comme un système de fichiers classiques.

Pour se simplifier la vie, on peut utiliser Borgmatic qui est un *wrapper* de Borg.

## Installation

```
apt-get install borgbackup
```

On peut aussi utiliser `pip`, c'est vous qui voyez.

## Initialisation

On doit d'abord initialiser le répertoire qui accueillera les sauvegardes :

```
mkdir /opt/backup  
borg init /opt/backup/
```

Au cas où l'on souhaiterait utiliser un serveur distant pour accueillir les sauvegardes, il faut que celui-ci soit joignable par SSH et dispose lui-aussi de Borg.

```
borg init <username>@<server>:/remotepath
```

Dans le cas où il n'est pas possible d'y installer Borg (un espace de stockage fourni par un hébergeur par exemple), il est possible de le monter en *sshfs* :

```
apt-get install sshfs  
sshfs <username>@<server>:/remotepath /opt/backup/
```

Sshfs possède de multiples options améliorant les performances et la stabilité du point de montage, je vous laisse chercher car je ne les ai pas sous la main.

Par défaut, l'initialisation vous demandera un mot de passe qui servira à chiffrer les sauvegardes. Il est possible de désactiver le chiffrement via les options de `borg init`.

```
borg help init
```

Le chiffrement nécessite deux choses pour fonctionner : le mot de passe et une clé de chiffrement. Dans le cas d'une initialisation par défaut (sans options), la clé de chiffrement sera dans le fichier `/opt/backup/config`.

**Il est impératif de sauvegarder cette clé sans laquelle vos sauvegardes seraient inutiles** ! On peut l'exporter via `borg key export /opt/backup` et l'importer via `borg key import /opt/backup keyfile`.

Le mot de passe vous sera demandé pour toute opération sur les sauvegardes (création, restauration, etc). Pour éviter de le taper toutes les cinq minutes, vous pouvez exporter la variable d'environnement `BORG_PASSPHRASE` :

```
export BORG_PASSPHRASE="mot_de_passe"
```

N'oubliez pas que cet `export` se retrouvera dans votre historique bash (ou zsh, ou ce que vous utilisez) ! Je vous conseille de le supprimer de votre historique après usage.

# Création d'une sauvegarde

Rien de plus simple :

```
borg create /opt/backup::nom_de_la_sauvegarde /chemin/a/sauvegarder
```

L'option `--stats` est très appréciable car elle fournit des informations sur la sauvegarde créée (comme sa taille par exemple).

Le nom de la sauvegarde doit être unique et ne doit pas se terminer par `.checkpoint`. On peut utiliser des *placeholders* comme `{hostname}` dans le nom de la sauvegarde. Voir `borg help placeholders` pour plus de détails.

# Manipulation des sauvegardes

## Lister les sauvegardes

```
borg list /opt/backup
```

## Supprimer une sauvegarde

```
borg delete /opt/backup::
```

## Renommer une sauvegarde

```
borg rename /opt/backup::
```

## Extraire le contenu d'une sauvegarde

Attention ! Le contenu sera extrait dans le répertoire où vous vous trouvez !

```
borg extract /opt/backup::
```

Il est possible de n'extraire que certains fichiers :

```
borg extract /opt/backup::borg extract /opt/backup::
```

## Monter une sauvegarde

```
borg mount /opt/backup::
```

Vous pourrez alors parcourir et utiliser (`cp`, `cat` ...) la sauvegarde en parcourant le dossier `/mnt`.

Pour démonter la sauvegarde :

```
borg umount /mnt
```

# Voir les informations détaillées d'une sauvegarde

```
borg info /opt/backup::
```

## Supprimer les vieilles sauvegardes

Même si l'espace disque ne coûte aujourd'hui pas très cher, on ne va quand même pas garder 30 ans de sauvegardes

```
borg prune -w 4 --prefix='{hostname}-' /opt/backup
```

Cette commande ne gardera que 4 sauvegardes hebdomadaires. L'option `--prefix='{hostname}-'` permet de discriminer les sauvegardes à éliminer d'après un préfixe (ici le nom de la machine), ceci afin d'éviter de supprimer les sauvegardes d'une autre machine si jamais le répertoire de sauvegarde servait pour plusieurs machines.

Je vous laisse regarder les autres options de `borg prune` dans le manuel.

## Vérifier une sauvegarde (ou toutes)

```
borg check /opt/backup::
borg check /opt/backup
```

Attention ! Cela vérifie que la sauvegarde n'est pas corrompue, pas que vous avez ciblé les bons répertoires à sauvegarder ! :P

## Vérification des sauvegardes

“ « Une sauvegarde est à la fois valide et corrompue tant qu'on n'a pas essayé de la restaurer »

*La sauvegarde de Schrödinger*

Et oui, tant qu'on n'a pas essayé de restaurer des fichiers depuis la sauvegarde, comment savoir si celle-ci a fonctionné ? Les déboires de la société Gitlab qui a perdu 6 heures d'enregistrements en base de données pour cause de dysfonctionnement des 5(!) méthodes de sauvegardes nous en donnent la preuve.

Il existe cependant un outil qui permet de vérifier que vos sauvegardes respectent un certain nombre de critères : Backup Checker

Avec cet outil, on pourra s'assurer que la sauvegarde comporte bien tel ou tel fichier, soit d'une certaine taille, etc.

À défaut d'avoir le temps de mettre en place un tel outil, on pourra ponctuellement essayer de restaurer localement un fichier. Même si cela ne vérifie pas grand chose, c'est toujours mieux que pas de vérification du tout !

## Un peu de lecture

<http://sebsauvage.net/wiki/doku.php?id=borgbackup>

## Plutôt que d'écrire un script qui utilise borg...

Il y a un soft qui fait une surcouche à Borg, le rendant plus simple à utiliser : Borgmatic.



Systeme

# Borgmatic

Borgmatic est un *wrapper* autour de Borg qui en simplifie infiniment l'utilisation.

## Installation

Il nous faut d'abord Borg (utilisez la version des backports Debian si vous êtes encore en *stretch*) :

```
apt install borgbackup
```

D'habitude, je préfère utiliser les paquets Debian, mais la version pip de Borgmatic apporte une option en plus que j'apprécie particulièrement.

```
apt install python3-pip
pip3 install borgmatic
```

## Configuration

C'est là que Borgmatic est pratique : il permet une configuration très simple de Borg.

Générez un fichier de configuration :

```
generate-borgmatic-config
```

Cela créera le fichier `/etc/borgmatic/config.yaml`. Si vous souhaitez que la configuration soit dans un autre fichier :

```
generate-borgmatic-config -d /etc/borgmatic/autre_config.yaml
```

La configuration générée (exemple) est très simple à comprendre et auto-documentée, je ne vais l'expliquer, je vais me contenter d'en mettre certains points en valeur

## Le dépôt

On le verra plus bas, j'utilise un serveur distant pour faire les sauvegardes. Donc :

```
location:
  repositories:
    - borg@server:/var/lib/borg/depot/
```

## La *passphrase*

Choisissez quelque chose de costaud et sauvegardez-là quelque part !

```
storage:
  encryption_passphrase: "foo-bar-baz"
```

## Utilisation d'une clé SSH particulière

Je crée plus bas une clé SSH dédiée pour Borg pour faire les sauvegardes sur le serveur distant. Il faut donc que j'indique à Borgmatic que je souhaite utiliser cette clé.

```
storage:
  ssh_command: ssh -i /root/.ssh/id_borgmatic
```

## Les hooks

Situés à la fin du fichier de configuration, il s'agit d'actions qui seront effectuées avant et après la sauvegarde, ou en cas de problème lors de l'exécution.

Personnellement, j'aime bien avoir la liste de mes sauvegardes après qu'une sauvegarde soit effectuée. Je vais donc écrire :

```
hooks:
  after_backup:
    - /usr/local/bin/borgmatic list
```

Comme il est conseillé d'exporter la clé du dépôt borg, je mets aussi ceci dans les `hooks` :

```
before_backup:
  - borg key export borg@server:/var/lib/borg/depot/ /etc/ssl/private/borg.key
```

# Rétention et vérification du dépôt et des archives

Je fais ça sur le serveur, j'y reviendrai plus loin.

## Cron

On crée un petit cron (avec l'utilisateur `root`) pour sauvegarder régulièrement l'ordinateur :

```
35 0 * * * borgmatic create -c /etc/borgmatic/mon_pc.yaml --stats 2>&1
```

Si ce n'est pas un serveur allumé 24h/24, il est préférable de mettre ça dans `/etc/anacrontab` :

```
@daily 15    backup borgmatic create -c /etc/borgmatic/mon_pc.yaml --stats 2>&1
```

Cela lancera le backup tous les jours, 15 minutes après le démarrage du pc. Ou plus tard.

Attention, sur Debian, les tâches anacron ne sont lancées que si vous êtes sur secteur ! Pour changer ça, reportez-vous au fichier `/usr/share/doc/anacron/README.Debian`.

## Préparation du serveur du dépôt distant

Je préfère faire mes sauvegardes sur un disque distant : si mon disque lâche, j'aurai toujours mes sauvegardes.

Pour ce faire, je crée une clé dédiée sur l'ordinateur à sauvegarder, sans mot de passe vu que borgmatic va tourner automatiquement :

```
ssh-keygen -o -a 100 -t ed25519 -f /root/.ssh/id_borgmatic -N ''
```

**Sur le serveur de sauvegarde**, j'installe Borg et Borgmatic comme précédemment puis je crée un utilisateur `borg` :

```
adduser --system --home /var/lib/borg --shell /bin/bash --disabled-password borg
mkdir /var/lib/borg/.ssh
chmod 700 /var/lib/borg/.ssh
```

```
touch /var/lib/borg/.ssh/authorized_keys
chmod 600 /var/lib/borg/.ssh/authorized_keys
chown -R borg: /var/lib/borg/.ssh
```

Et je mets la clé publique créée précédemment dans `/var/lib/borg/.ssh/authorized_keys`, avec quelques restrictions :

```
command="/usr/bin/borg --umask=077 --info serve --append-only --restrict-to-repository
/var/lib/borg/becky2/",restrict ssh-ed25519
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX root@mon_pc
```

On génère une configuration :

```
generate-borgmatic-config -d /etc/borgmatic/mon_pc.yaml
```

Et c'est dans cette configuration qu'on va configurer les durées de rétention et les vérifications du dépôt et des archives.

## Rétention

C'est très simple. Pour garder un backup par mois sur les 6 derniers mois, un par semaine sur les 8 dernières semaines et un par jour sur les 14 derniers jours, il suffit de :

```
retention:
  keep_daily: 14
  keep_weekly: 8
  keep_monthly: 6
```

Comme Borg déduplique comme un monstre, cela ne prendra pas énormément de place (sauf si vous sauvegardez des trucs qui changent tout le temps)

## Vérification du dépôt et des archives

Cela permet de s'assurer que votre dépôt et vos archives sont utilisables et non corrompus. Je me contente de décommenter la configuration proposée :

```
consistency:
  checks:
    - repository
    - archives
  check_last: 3
```

J'ai laissé `check_last` à 3 car vérifier toutes les archives peut être fort long. Donc une vérification des 3 dernières devrait faire l'affaire, surtout si on vérifie quotidiennement.

# Dépôt

Attention, comme on est là sur le serveur distant, il faut lui donner un dossier local !

```
location:
  repositories:
    - /var/lib/borg/depot/
```

## Script de suppression d'anciennes sauvegardes / vérification des archives

Il y a des éléments dans ce script qui prendront tout leur sens plus tard.

**NOTA BENE** : ce script est tout à fait adaptable à un usage à Borg sans Borgmatic.

On prépare le terrain :

```
apt install libcpupanel-json-xs-perl
mkdir -P /opt/borgmatic-stats/tmp/ /opt/borgmatic-stats/json/
cd /opt/borgmatic-stats/
wget https://framagit.org/snippets/3716/raw -O verify-archives.pl
chmod 700 -R /opt/borgmatic-stats/
chown borg: -R /opt/borgmatic-stats/
```

Puis on met ceci dans `/opt/borgmatic_prune_and_check.sh` :

```
#!/bin/bash
cat <<EOF
=====
== mon_pc
=====
EOF

/usr/local/bin/borgmatic list -c /etc/borgmatic/mon_pc.yaml --json > /opt/borgmatic-stats/tmp/mon_pc.json.tmp
CONTINUE=0
if [[ -e /opt/borgmatic-stats/json/mon_pc.json ]]
```

```

then
    echo "Checking repository consistency."
    CONTINUE=$(/opt/borgmatic-stats/verify-archives.pl --old /opt/borgmatic-stats/json/mon_pc.json --new
/opt/borgmatic-stats/tmp/mon_pc.json.tmp)
    echo "Repository consistency checked."
else
    CONTINUE=1
fi

if [[ $CONTINUE == '1' ]]
then
    ## Check
    /usr/local/bin/borgmatic check -c /etc/borgmatic/mon_pc.yaml 2>&1 && \
    echo "Repository checked." && \
    ## Allow pruning
    borg config /var/lib/borg/depot/ append_only 0 && \
    ## Prune
    /usr/local/bin/borgmatic prune -c /etc/borgmatic/mon_pc.yaml --stats 2>&1 && \
    echo "Repository pruned."
    ## List
    echo "Borg archives of mon_pc:"
    /usr/local/bin/borgmatic list -c /etc/borgmatic/mon_pc.yaml 2>&1

    /usr/local/bin/borgmatic list -c /etc/borgmatic/mon_pc.yaml --json > /opt/borgmatic-stats/json/mon_pc.json

    ## Disallow pruning
    borg config /var/lib/borg/depot/ append_only 1

    echo "
else
    cat <<EOF

*****
* ALERT ON mon_pc! *
*****

All of the old archives can't be retrieved from the repository (/var/lib/borg/depot/)!

Someone may have deleted an archive from mon_pc.

Pruning has been aborted. Please manually review the repository.

```

```
$CONTINUE  
EOF  
fi
```

On n'oublie pas de le rendre exécutable :

```
chmod +x /opt/borgmatic_prune_and_check.sh
```

## Cron

Attention ! Il faut éditer la *crontab* de l'utilisateur `borg` :

```
crontab -e -u borg
```

Et son contenu :

```
15 3 * * * /opt/borgmatic_prune_and_check.sh
```

# Initialisation du dépôt de sauvegarde

**Sur l'ordinateur à sauvegarder :**

```
borgmatic init -c /etc/borgmatic/mon_pc.yaml --append-only -e repokey
```

Le dépôt est initialisé en **append-only** (mais de toute façon, on le force dans le `.ssh/authorized_keys` du serveur distant) et avec un chiffrement par mot de passe mais avec la clé dans le dossier du dépôt distant.

# Lancement d'une sauvegarde

**Sur l'ordinateur à sauvegarder :**

```
borgmatic create -c /etc/borgmatic/mon_pc.yaml --stats
```

Le `--stats` est l'option que j'affectionne et dont je parlais au début : cela affiche des statistiques sur la sauvegarde qui a été faite : sa taille, sa taille compressée, sa taille dédupliquée, le temps que ça a pris...

# Afficher la liste des sauvegardes

```
borgmatic list -c /etc/borgmatic/mon_pc.yaml
```

# Restauration de sauvegardes

Voir la section [kivabien](#) de l'article sur [Borg](#).

## Explication de l'option `--append-only`

Contrairement à ce qu'on pourrait croire, `--append-only` n'empêche pas de supprimer des sauvegardes ([Ce ticket Github](#) m'en a fait prendre conscience). Ainsi, un attaquant ayant pris le contrôle de l'ordinateur à sauvegarder pourra supprimer des sauvegardes. Sauf qu'elles ne seront pas vraiment supprimées : l'attaquant aura créé des transactions qui indiquent la suppression des sauvegardes mais ces transactions ne seront réellement appliquées que lors d'une action comme `prune` depuis un ordinateur qui aura le droit de faire sauter le **append-only**. C'est comme un `BEGIN TRANSACTION;` sans `COMMIT;` en SQL ☐

C'est le cas du script `/opt/borgmatic_prune_and_check.sh` qui fait effectivement sauter (et le remet après) le verrou avec :

```
borg config /var/lib/borg/depot/ append_only 0
```

Comme on automatise la suppression des anciennes sauvegardes avec `cron`, il nous faut un moyen de repérer de tels changements. C'est tout le but de `/opt/borgmatic-stats/verify-archives.pl` qui compare la liste des archives du dépôt avec la liste créée la dernière fois que `/opt/borgmatic_prune_and_check.sh` a supprimé les anciennes archives. Comme le serveur distant est le seul à normalement pouvoir supprimer des archives, il est logique de retrouver toutes les anciennes archives au lancement suivant.

Ainsi, en cas d'incohérence, la suppression des anciennes archives ne s'effectue pas.



**NOTA BENE** : ceci n'empêchera pas un attaquant de changer la configuration de borgmatic pour lui faire sauvegarder des trucs inutiles plutôt que ce qui vous intéresse. Ou de couper les sauvegardes. C'est un inconvénient des sauvegardes en *push* plutôt qu'en *pull*. Je n'ai pas encore trouvé de solution à ça. Peut-être un script qui analyserait la sortie de `borgmatic create --stats --json` qui me permettrait de repérer des changements importants dans la taille de la sauvegarde, le temps de sauvegarde ou le ratio de déduplication ?

# En cas d'incohérence : restaurer des sauvegardes supprimées par un attaquant

Sur le serveur distant :

```
su - borg  
cd /var/lib/borg/depot/
```

Regarder le log des transactions pour trouver les n° des transactions suspectes : `cat transactions`

Ce qui nous donne un truc du genre :

```
transaction 23, UTC time 2019-08-01T13:40:34.435019  
transaction 25, UTC time 2019-08-01T13:42:05.662188  
transaction 27, UTC time 2019-08-01T13:43:18.403771  
transaction 29, UTC time 2019-08-01T13:43:53.306636  
transaction 31, UTC time 2019-08-01T13:44:51.831937  
transaction 33, UTC time 2019-08-01T13:45:17.786886  
transaction 35, UTC time 2019-08-01T22:17:12.044179  
transaction 37, UTC time 2019-08-02T08:02:55.005430  
transaction 43, UTC time 2019-08-02T22:17:10.068843  
transaction 45, UTC time 2019-08-03T22:17:09.625745  
transaction 47, UTC time 2019-08-04T22:17:09.673447  
transaction 49, UTC time 2019-08-05T22:17:13.709208  
transaction 51, UTC time 2019-08-06T10:11:26.301496  
transaction 53, UTC time 2019-08-06T10:20:46.178014  
transaction 55, UTC time 2019-08-06T10:26:47.940003
```

Là, il faut savoir quand a eu lieu le problème. Ici, c'était le 6 août à partir de 10h. Donc les transactions 51 à 55. Mais **attention** ! Il s'agit en fait des transactions **50** à 55 : le numéro indiqué dans le fichier est celui du dernier fichier modifié par la transaction. Il faut donc partir du n+1 de la dernière transaction correcte.

Après, c'est facile :

```
rm hints.* index.* integrity.*  
rm data/**/{50..55}
```

On finit par rafraîchir le cache du dépôt :

```
borg delete --cache-only /var/lib/borg/depot/
```

Sur l'ordinateur sauvegardé, par contre, je n'arrivais pas à supprimer le cache, j'avais ce message :

```
Cache, or information obtained from the security directory is newer than repository - this is either an attack or  
unsafe (multiple repos with same ID)
```

Ceci m'a réglé le problème :

```
rm -rf ~/.cache/borg/le_dossier_avec_un_nom_monstrueux  
rm -rf ~/.config/borg/security/un_autre_dossier_avec_un_nom_monstrueux
```

# Crypsetup

Tiré de <https://www.thegeekstuff.com/2016/03/cryptsetup-lukskey/>.

## Identifier la partition chiffrée

```
sudo lsblk -o name,size,fstype,label,mountpoint
```

Chez moi, ça donne ça :

NAME	SIZE	FSTYPE	LABEL	MOUNTPOINT
sda	238.5G			
└─sda1	512M	vfat		/boot/efi
└─sda2	244M	ext2		/boot
└─sda3	237.7G	crypto_LUKS		
└─sda3_crypt	237.7G	LVM2_member		
└─foo--vg-swap_1	6.8G	swap		[SWAP]
└─foo--vg-root	27.9G	ext4		/
└─foo--vg-home	203G	ext4		/home

La partition chiffrée est donc `/dev/sda3`.

## Identifier les slots de clés déjà utilisés

On peut avoir 8 clés de chiffrement, chacune occupant un *slot*.

```
sudo cryptsetup luksDump /dev/sda3 | grep Slot
```

Chez moi, ça donne :

Key Slot 0: ENABLED  
Key Slot 1: DISABLED  
Key Slot 2: DISABLED  
Key Slot 3: DISABLED  
Key Slot 4: DISABLED  
Key Slot 5: DISABLED  
Key Slot 6: DISABLED  
Key Slot 7: DISABLED

## Ajouter une nouvelle clé

```
sudo cryptsetup luksAddKey /dev/sda3
```

Cryptsetup vous demandera alors de taper la *passphrase* d'une des clés existantes puis de taper (deux fois) une nouvelle *passphrase* pour la nouvelle clé.

On peut forcer le slot pour la nouvelle clé :

```
sudo cryptsetup luksAddKey /dev/sda3 -S 4
```

## Supprimer une clé

```
sudo cryptsetup luksRemoveKey /dev/sda3
```

Cryptsetup vous demandera alors de taper la *passphrase* de la clé à supprimer. Je ne sais pas ce qui se passerait si la *passphrase* était utilisée pour plusieurs clés (je ne sais même pas si c'est possible).

Si on a oublié la *passphrase* de la clé à supprimer, on peut supprimer son slot :

```
cryptsetup luksKillSlot /dev/sda3 2
```

Cryptsteup vous demandera alors de taper la *passphrase* d'une des clés existantes.

# Curl

Afin d'éviter les écueils dus aux éventuels problèmes de redirection réseau des ports des machines virtuelles, nous allons utiliser la commande `curl` pour tester les sites web que nous mettrons en place au cours des TP.

Ceci constitue un petit inventaire des commandes les plus utiles de `curl` pour notre cas.

## Utilisation de base

```
curl http://example.org
```

La commande `curl` télécharge la ressource demandée (qui n'est pas nécessairement une adresse web, car `curl` est capable de télécharger des ressources d'autres protocoles, comme `ftp` par exemple) et en affiche le contenu sur la sortie standard, si ce contenu n'est pas un contenu binaire.

## Rediriger la ressource vers un fichier

```
curl http://example.org > fichier.html  
curl http://example.org --output fichier.html  
curl http://example.org -o fichier.html
```

## Réduire la verbosité de curl

Lorsque la sortie est redirigée vers un fichier, `curl` affiche une barre de progression donnant certaines indications sur le téléchargement de la ressource (le temps restant, la taille...).

Pour ne pas afficher ces informations, on utilise l'option `--silent` ou son abbréviation `-s`.

```
curl --silent http://example.org -o fichier.html  
curl -s http://example.org -o fichier.html
```

## Faire autre chose qu'un GET

Pour utiliser une autre méthode HTTP que `GET`, on utilise l'option `--request` ou son abbréviation `-X`.

```
curl --request POST http://example.org  
curl -X POST http://example.org
```

## Faire une requête HEAD

Si on tente de faire une requête `HEAD` avec l'option `--request`, `curl` affichera un message d'erreur :

```
Warning: Setting custom HTTP method to HEAD with -X/--request may not work the  
Warning: way you want. Consider using -I/--head instead.
```

Il convient d'utiliser l'option `--head` ou son abbréviation `-I` :

```
curl --head http://example.org  
curl -I http://example.org
```

## Pour faire une requête avec authentification HTTP

On spécifie l'identifiant et le mot de passe avec l'option `--user` ou son abbréviation `-u`, en les séparant par un caractère `:`.

```
curl --user login:password http://example.org  
curl -u login:password http://example.org
```

## Forcer la connexion en IPv6 ou en IPv4

On utilise pour cela les options `-6` et `-4`.

```
curl -6 http://example.org  
curl -4 http://example.org
```

## Utilisation avancée

# Forcer la connexion sur une autre adresse IP

Il est possible de dire à `curl` d'utiliser une adresse IP particulière au lieu de la véritable adresse IP d'un domaine. Il faut voir cela comme une alternative à la manipulation du fichier `/etc/hosts`.

```
curl --resolve example.org:80:127.0.0.1 http://example.org
curl --resolve "example.org:80:[::1]" http://example.org
```

La syntaxe de l'option est `host:port:addr`. Le port est celui qui sera utilisé par le protocole. Spécifier le port `80` pour le protocole `https` serait inutile : il faut dans ce cas utiliser le port `443`.

## Forcer la connexion sur une autre adresse IP et un autre port

On utilise pour cela l'option `--connect-to`, relativement similaire à l'option `--resolve`. La syntaxe de l'option est `host1:port1:host2:port2`

```
curl --connect-to example.org:80:127.0.0.1:8080 http://example.org
curl --connect-to "example.org:80:[::1]:8080" http://example.org
```

## Forcer la connexion depuis une certaine interface réseau

On utilise pour cela l'option `--interface` suivi du nom d'une interface, d'une adresse IP ou d'un nom d'hôte.

```
curl --interface wlo1 http://example.org
curl --interface 203.0.113.42 http://example.org
curl --interface example.com http://example.org
```

## Ne pas vérifier la sécurité du certificat du site

Que ce soit parce qu'un certificat est expiré ou parce qu'on utilise un certificat autosigné, on peut avoir besoin que `curl` effectue bien la requête sans se préoccuper de la validité du certificat utilisé par le site. On utilise alors l'option `--insecure` ou son abbréviation `-k`.

```
curl --insecure https://example.org  
curl -k https://example.org
```

## Utiliser un fichier d'autorités de certification spécifique

Si on utilise, par exemple, un certificat autosigné, ou signé par une autorité de certification (AC) personnelle, et qu'on souhaite s'assurer que le certificat utilisé par le site est bien valide, on peut donner à `curl` un fichier contenant le certificat public de l'AC (il est possible d'y mettre plusieurs certificats) au format PEM. On utilise l'option `--cacert`.

```
curl --cacert fichier_AC.pem https://example.org
```

On peut aussi utiliser l'option `--capath` dont l'argument est un dossier contenant des fichiers de certificats d'AC.

```
curl --capath ~/ACs https://example.org
```



# Débloquer un RAID coincé en resync=PENDING

Il arrive des fois que certains disques RAID soient bloqués en `resync=PENDING` (utilisez votre supervision pour le détecter !), ce que l'on peut voir avec la commande suivante :

```
cat /proc/mdstat
```

Ça ressemble à ça :

```
md0 : active (auto-read-only) raid1 sda1[0] sdb1[1]
      16760832 blocks super 1.2 [2/2] [UU]
      resync=PENDING
```

Pour décoincer ça, il suffit de faire

```
mdadm --readwrite /dev/md0
```

# Empêcher l'activation d'un service à son installation

On peut vouloir installer un service mais éviter qu'il ne s'active à l'installation.

Par exemple, pour changer sa configuration avant utilisation, ou parce qu'un autre service écoute déjà sur le port que le service. J'ai cherché comment faire en voulant installer PostgreSQL sur un serveur où il y avait déjà un PostgreSQL installé par un autre paquet (le PostgreSQL fourni par Gitlab, en l'occurrence).

La solution est fort simple et utilise les preset d'activation de systemd.

Exemple avec MariaDB (le nom du fichier doit suivre le modèle `<priority>-<policy-name>.preset`, voir la page de manuel) :

```
mkdir -p /etc/systemd/system-preset
vi /etc/systemd/system-preset/85-systemd.preset
```

Et dedans, mettre :

```
disable mariadb.*
```

On peut aussi forcer l'activation avec `enable` à la place de `disable`.

Je vous laisse voir la page de manuel pour plus de détails.

# Exécuter une action à la mise en veille / au réveil

## Systemd

On mettra un script dans `/lib/systemd/system-sleep/` :

Exemple de script :

```
#!/bin/sh

case "${1}" in
    pre)
        echo "Suspension ou hibernation"
        ;;
    post)
        echo "Réveil ou dégel"
        ;;
    esac
```

Le 2e argument ( `$2` ) pourra être `suspend`, `hibernate`, `suspend-then-hibernate` ou `hybrid-sleep`, si vous voulez effectuer des actions différentes pour ces cas.

Pour plus d'informations, voir la [page de manuel de `systemd-sleep`](#).

## InitV

On mettra un script dans `/etc/pm/sleep.d/`.

Exemple de script :

```
#!/bin/sh
```

```
case "${1}" in
```

```
    suspend|hibernate)
```

```
        echo "Suspension ou hibernation"
```

```
        ;;
```

```
    resume|thaw)
```

```
        echo "Réveil ou dégel"
```

```
        ;;
```

```
esac
```

# Firewalld : un firewall simple à utiliser

Firewalld est un pare-feu que je trouve très agréable à utiliser, où on peut « cacher » la complexité de certains éléments de configuration derrière des noms simples à utiliser.

Par exemple, je peux avoir un service qui n'a pas spécialement de port dédié, donc qui n'est pas proposé par firewall. Mettons un `wireguard` qui écoute sur le port 9879. Plutôt que d'utiliser `9879/udp` dans ma configuration, je vais créer un service `wireguard`, et c'est ce service que j'autoriserai.

Ce sera bien plus parlant quand je relirai la configuration.

Liens :

- Documentation officielle : <https://firewalld.org/documentation/>
- <https://www.linuxtricks.fr/wiki/firewalld-le-pare-feu-facile-sous-linux>
- <https://www.rootusers.com/how-to-use-firewalld-rich-rules-and-zones-for-filtering-and-nat/>
- <https://kb.vander.host/security/firewalld-cheat-sheet/>

## Principes

En très gros et en très résumé, on va avoir des zones, qui sont des ensembles d'adresses IP et la zone `public` qui concerne toutes les IPs, sauf celles qui sont dans d'autres zones.

On va aussi avoir des services, qui décrivent... des services : port et protocole (ex: `5666` et `tcp` pour nrpe).

On va aussi avoir des « rich rules » dans les zones, des exceptions aux règles appliquées dans la zone.

Toute la configuration est dans des fichiers XML très simples à lire, c'est très agréable. Tant qu'on ne surcharge pas la configuration par défaut, les fichiers sont dans `/usr/lib/firewalld/` mais dès qu'on modifie un élément de configuration, celui-ci se retrouvera copié dans `/etc/firewalld/` et modifié.

# Test de configuration

Si on modifie de la configuration à la main (en écrivant dans `/etc/firewalld`, on prendra soin de tester la configuration avec les commandes suivantes :

Si `firewalld` est coupé :

```
firewall-offline-cmd --check-config
```

Si `firewalld` est lancé :

```
firewall-cmd --check-config
```

## Attention

Quand on installe `firewalld`, le firewall démarre de suite en n'autorisant en public que `ssh` (et `dhcpv6-client`).

Il est donc préférable de l'installer et de le couper directement après :

```
apt install firewalld &&  
systemctl stop firewalld
```

On pourra créer la configuration tranquillement avec la commande `firewall-offline-cmd` et lancer le service une fois la configuration terminée.

## Changements permanents

Si on veut rendre un changement permanent (c-à-d qu'il soit écrit dans la config au lieu d'être juste appliqué jusqu'au redémarrage), il faut ajouter ça aux commandes :

```
--permanent
```

Par contre, avec `--permanent`, il faut recharger la configuration pour appliquer les modifications (ou alors on applique une fois avec `--permanent` et une fois sans) :

```
firewall-cmd --reload
```

À l'inverse, on peut créer des règles sans le `--permanent` et ensuite écrire ces règles dans la configuration permanent avec la commande suivante :

```
firewall-cmd --runtime-to-permanent
```

**NB** : certaines commandes nécessitent forcément le `--permanent` .

# Bloquer une adresse IP

On peut soit ajouter les adresses aux zones `drop` ou `block` :

```
firewall-cmd --zone=drop --add-source 192.0.2.0/24
firewall-cmd --zone=drop --add-source 192.0.2.0/24 --permanent
```

Soit ajouter une `rich-rule` ( `man firewalld.richlanguage` ) à la zone `public` :

```
firewall-cmd --zone public --add-rich-rule "rule family=ipv4 source address=192.0.2.0/24 reject"
firewall-cmd --zone public --add-rich-rule "rule family=ipv4 source address=192.0.2.0/24 reject" --permanent
```

Pour enlever un blocage :

```
firewall-cmd --zone drop --remove-source 51.159.0.0/16
firewall-cmd --zone drop --remove-source 51.159.0.0/16 --permanent
```

```
firewall-cmd --zone public --remove-rich-rule "rule family=ipv4 source address=51.159.0.0/16 reject"
firewall-cmd --zone public --remove-rich-rule "rule family=ipv4 source address=51.159.0.0/16 reject" --
permanent
```

Pour voir les blocages par `rich-rule` (la 1ère commande donne les blocages actuellement activés, l'autre ceux qui sont dans les fichiers de configuration. Il peut y avoir une différence... ou pas !) :

```
firewall-cmd --list-rich-rules
firewall-cmd --list-rich-rules --permanent
```

Pour bloquer un ipset (voir plus bas) :

```
firewall-cmd --zone=drop --add-source ipset:le_nom_de_l_ipset
firewall-cmd --zone=drop --add-source ipset:le_nom_de_l_ipset --permanent
```

# Zones

Voir les zones disponibles :

```
firewall-cmd --get-zones
```

NB : la zone `public`, par défaut, n'autorise que le SSH et dhcpv6-client. L'installation de firewalld sur une machine va donc couper l'accès aux services. Il faut donc stopper firewalld juste après son installation, regarder les ports utilisés sur la machine et modifier la zone `public` soit en copiant `/usr/lib/firewalld/zones/public.xml` dans `/etc/firewalld/zones/`, soit en préparant une ligne de commande à lancer juste après le démarrage de firewalld.

NB : les zones peuvent avoir une `target`, l'action à appliquer aux connexions qui correspondent à la zone. Voir [la doc](#).

NB : Une adresse IP ne peut se trouver que dans une seule zone mais on peut ajouter dans une zone un réseau qui contient une adresse IP déjà présente dans une autre zone. Cependant, le comportement peut ne pas être celui attendu. Il vaut mieux ajouter une `rich-rule` à la zone pour faire une exception aux règles de la zone.

Voir la zone par défaut (celle sur laquelle s'appliqueront les modifications si on ne spécifie pas la zone) :

```
firewall-cmd --get-default-zone
```

Définir la zone par défaut :

```
firewall-cmd --set-default-zone work
```

Voir la configuration de la zone :

```
firewall-cmd --info-zone lazone
```

Voir la configuration de toutes les zones :

```
firewall-cmd --list-all-zones
```

Créer une zone :

```
firewall-cmd --permanent --new-zone mazonne  
firewall-cmd --reload
```



Supprimer une zone :

```
firewall-cmd --permanent --delete-zone mazonne  
firewall-cmd --reload
```

Chaque interface du système peut être attribuée à une zone. Pour ajouter l'interface ens192 à la zone work en l'enlevant de sa précédente zone :

```
firewall-cmd --change-interface ens192 --zone work [--permanent]
```

Pour retirer l'interface ens192 de la zone work :

```
firewall-cmd --remove-interface ens192 --zone work [--permanent]
```

Pour ajouter l'interface ens192 à la zone work (interface qui ne soit pas être affectée à une zone) :

```
firewall-cmd --add-interface ens192 --zone work [--permanent]
```

Ajouter des adresses IP ou un réseau à une zone :

```
firewall-cmd --zone work --add-source 192.0.2.0/24 [--permanent]  
firewall-cmd --zone work --add-source 192.0.2.200 [--permanent]
```

Retirer des adresses IP ou un réseau d'une zone :

```
firewall-cmd --zone work --remove-source 192.0.2.0/24 [--permanent]  
firewall-cmd --zone work --remove-source 192.0.2.200 [--permanent]
```

Pour basculer une adresse IP ou un réseau d'une zone à une autre :

```
firewall-cmd --zone l_autre_zone --change-source 192.0.2.0/24 [--permanent]  
firewall-cmd --zone l_autre_zone --change-source 192.0.2.200 [--permanent]
```

Si l'adresse IP / le réseau était dans une autre zone, ça équivaut à un `--remove-source` suivi d'un `--add-source`, si ce n'était pas le cas, ça fait juste comme un `--add-source`.

Voir la `target` d'une zone :

```
firewall-cmd --permanent --get-target --zone drop
```

Définir la `target` d'une zone :

```
firewall-cmd --permanent --set-target [default|ACCEPT|DROP|REJECT] --zone drop
```

Pour voir dans quelle zone est une adresse IP :

```
firewall-cmd --get-zone-of-source=<adresse IP ou réseau en notation CIDR ou adresse MAC ou ipset>
```

Si ça répond `no zone`, c'est que l'IP ou le réseau n'est pas explicitement associé à une zone.

**Attention** : si un réseau est enregistré dans une zone, lancer la commande sur une IP du réseau ne renverra pas la zone en question !

# Services

Voir les services existants :

```
firewall-cmd --get-services
```

Voir le détail d'un service :

```
firewall-cmd --info-service ssh
```

Créer un nouveau service :

```
firewall-cmd --permanent --new-service influxdb  
firewall-cmd --permanent --service influxdb --set-description InfluxDB  
firewall-cmd --permanent --service influxdb --add-port 8086/tcp
```

Ajouter un service à une zone :

```
firewall-cmd --zone public --add-service nrpe [--permanent]
```

Retirer un service d'une zone :

```
firewall-cmd --zone public --remove-service nrpe [--permanent]
```

Voir les services d'une zone :

```
firewall-cmd --list-services --zone work
```

Si on ne souhaite pas créer de service mais autoriser un certain port et protocole, on peut les ajouter directement à la zone :

```
firewall-cmd --zone work --add-port 1234/udp [--permanent]
```

Et pour les supprimer :

```
firewall-cmd --zone work --remove-port 1234/udp [--permanent]
```

Pour voir les ports/protocoles d'une zone (ça ne listera pas les services !) :

```
firewall-cmd --list-ports --zone work
```

# IPSet : groupes d'adresses

Doc : [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html/security\\_guide/sec-setting\\_and\\_controlling\\_ip\\_sets\\_using\\_firewalld](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-setting_and_controlling_ip_sets_using_firewalld)

Cas d'usage : on voit plein de spammeurs venant du VPN d'Avast. On fait un `whois`, on voit le numéro d'**AS** des serveurs d'Avast, on va sur <https://asnlookup.com/> pour choper leur liste d'adresses IP et on en fait un ipset pour les bloquer.

NB : un ipset ne peut contenir qu'un type d'adresses, IPv4 ou IPv6, pas les deux.

NB : **Fail2ban**, lorsqu'il utilise firewalld, utilise des ipset, mais à un niveau un peu plus bas (nftables). Ces ipset ne sont pas vus par firewalld. On peut voir tous les ipset, même bas niveau avec la commande `ipset list -name` ( `ipset list le_nom_de_l_ipset` pour voir les adresses et le détail de l'ipset).

Un ipset sert à regrouper des adresses pour leur appliquer des règles facilement.

Voir les types d'ipset disponibles :

```
firewall-cmd --get-ipset-types
```

Voir les ipsets existants :

```
firewall-cmd --permanent --get-ipsets
```

Créer un ipset :

```
firewall-cmd --permanent --type hash:net --new-ipset test
```

Pour un ipset IPv6 :

```
firewall-cmd --permanent --type hash:net --option "family=inet6" --new-ipset test-v6
```

Supprimer un ipset :

```
firewall-cmd --permanent --delete-ipset test
```

Voir les infos d'un ipset :

```
firewall-cmd --info-ipset test [--permanent]
```

Ajouter une adresse IP à un ipset :

```
firewall-cmd --ipset test --add-entry 192.0.2.1 [--permanent]
```

Supprimer une adresse IP d'un ipset :

```
firewall-cmd --ipset test --remove-entry 192.0.2.1 [--permanent]
```

Voir les adresses IP d'un ipset :

```
firewall-cmd --ipset test --get-entries [--permanent]
```

Ajouter un paquet d'IP d'après un fichier :

```
cat > iplist.txt <<EOL
192.0.2.2
192.0.2.3
198.51.100.0/24
203.0.113.254
EOL
firewall-cmd --ipset test --add-entries-from-file iplist.txt [--permanent]
```

Supprimer un paquet d'IP d'après un fichier :

```
firewall-cmd --ipset test --remove-entries-from-file iplist.txt [--permanent]
```

Ajouter un ipset dans une zone :

```
firewall-cmd --zone drop --add-source ipset:test [--permanent]
```

Supprimer un ipset d'une zone :

```
firewall-cmd --zone drop --remove-source ipset:test [--permanent]
```

# Créer des exceptions avec des règles riches

Cas classique : on bloque un pays avec des ipset et quelqu'un a besoin d'accéder à nos services depuis là-bas.

L'ipset est dans la zone `drop`. On va ajouter une `rich-rule` pour faire une exception :

```
firewall-cmd --zone drop --add-rich-rule='rule family="ipv4" source address="192.0.2.29" port
port="443" protocol="tcp" accept'
firewall-cmd --zone drop --add-rich-rule='rule family="ipv4" source address="192.0.2.29" port port="80"
protocol="tcp" accept'
firewall-cmd --zone drop --permanent --add-rich-rule='rule family="ipv4" source address="192.0.2.29" port
port="443" protocol="tcp" accept'
firewall-cmd --zone drop --permanent --add-rich-rule='rule family="ipv4" source address="192.0.2.29" port
port="80" protocol="tcp" accept'
```

Pour supprimer l'exception :

```
firewall-cmd --zone drop --remove-rich-rule 'rule family="ipv4" source address="192.0.2.29" port
port="80" protocol="tcp" accept'
firewall-cmd --zone drop --remove-rich-rule 'rule family="ipv4" source address="192.0.2.29" port
port="443" protocol="tcp" accept'
firewall-cmd --zone drop --permanent --remove-rich-rule 'rule family="ipv4" source address="192.0.2.29" port
port="80" protocol="tcp" accept'
firewall-cmd --zone drop --permanent --remove-rich-rule 'rule family="ipv4" source address="192.0.2.29" port
port="443" protocol="tcp" accept'
```

On peut utiliser des services dans les règles riches :

```
firewall-cmd --zone drop --add-rich-rule='rule family="ipv4" source address="192.0.2.29" service name=https
accept'
```

On peut utiliser des ipset dans les règles riches :

```
firewall-cmd --zone drop --add-rich-rule='rule family="ipv4" source ipset="test-v6" service name=https accept'
```

**NB** : ajouter l'adresse IP en source dans la zone `public` ne servirait strictement à rien.

# Blocage geoIP

On peut se baser sur le script de <https://github.com/simonbouchard/geoip-blocking-w-firewalld> (le fork de Framasoft).

On modifie les pays à bloquer dans `/etc/default/firewalld-geoip` et on lance le script. À mettre dans un cron pour mettre à jour les adresses.

# Faire du NAT

Voir la partie `Network Address Translation (NAT)` de <https://www.rootusers.com/how-to-use-firewalld-rich-rules-and-zones-for-filtering-and-nat/>. Je n'ai pas eu l'occasion de tester ça.

# Lancer des commandes sudo avec authentification par agent SSH

## Installation du paquet nécessaire

```
apt install libpam-ssh-agent-auth
```

## Configuration

Modifier la configuration sudo pour y ajouter cette ligne :

```
Defaults:%sudo env_keep += "SSH_AUTH_SOCK"
```

On peut éditer le fichier `/etc/sudoers` avec la commande `visudo` ou mettre ceci dans un fichier du dossier `/etc/sudoers.d` avec `visudo -f /etc/sudoers.d/keep-ssh-auth-sock`

Mettre cette ligne dans le fichier `/etc/pam.d/sudo`, au-dessus de la ligne `@include common-auth` :

```
auth sufficient pam_ssh_agent_auth.so file=/etc/security/sudo_authorized_keys
```

Enfin, mettre les clés publiques des clés SSH qui peuvent être utilisées pour cette authentification dans le fichier `/etc/security/sudo_authorized_keys`.

# LVM

LVM permet, à partir de plusieurs disque physiques, de créer des partitions qui utiliseront plusieurs disques de manière invisible.

L'autre avantage est de pouvoir rajouter du disque sans arrêter la machine ou démonter la partition.

## Bases

Le LVM est composé de plusieurs morceaux :

- les volumes physiques, listables avec `pvs`, correspondants aux partitions physiques des disques utilisés pour le LVM
- les groupes de volumes, listables avec `vgs`, qui sont des agrégats de volumes physiques
- les volumes logiques, listables avec `lvs`, qui sont des partitions utilisant des portions de groupes de volumes

On n'est pas obligé d'utiliser toute la place disponible dans un groupe de volume lorsqu'on crée un volume logique, on a tout à fait le droit de se garder de la place.

On peut augmenter la taille d'un volume physique à chaud, sans démonter la partition, mais on doit la démonter si on veut réduire la taille ! C'est pourquoi il vaut mieux mettre juste ce qu'il faut comme taille (avec une marge de sécurité, bien sûr), quitte à augmenter plus tard la taille de la partition, plutôt que de tout mettre et ne plus avoir de marge pour une autre partition.

## Créer une nouvelle partition

```
lvcreate -L 30G -n nom-partition xenvg  
mkfs.ext4 /dev/mapper/xenvg-nom-partition
```



# Augmentation de la taille d'une partition

Ajout d'un nouveau disque au groupe de volumes `xenvg` :

```
pvcreeate /dev/sdc1  
vgextend xenvg /dev/sdc1
```

Augmentation de la taille de la partition `data`, appartenant au groupe `xenvg` :

```
lvextend -L +6.5G /dev/xenvg/data  
resize2fs /dev/mapper/xenvg-data
```

Pour prendre toute la place disponible :

```
lvextend -l +100%FREE /dev/mapper/xenvg-data  
resize2fs /dev/mapper/xenvg-data
```

Si c'est une partition de "swap" qui a été étendue :

```
swapoff -a  
mkswap /dev/mapper/beta--vg-swap_1  
swapon -a
```

# Monter une ou des partitions contenues dans un fichier qcow2

J'ai des images disques qcow2 sur ma machine, qui servent à mes machines virtuelles que j'utilise pour développer.

Pour modifier des fichiers dessus sans avoir besoin de démarrer les VMs, on peut monter les images disques sur le système hôte.

## Installer l'outil nécessaire

```
sudo apt install libguestfs-tools
```

## Monter l'image disque

### Monter tout le système de fichier

L'outil `guestmount` va inspecter les disques à la recherche d'un système d'exploitation et va monter toutes les partitions comme elles seraient montées sur la machine virtuelle.

```
sudo guestmount -a /path/to/qcow2/image -i /path/to/mount/point
```

### Monter une partition en particulier

```
sudo guestmount -a /path/to/qcow2/image -m <device> /path/to/mount/point
```

Exemple réel :

```
guestmount -a ~luc/.vms/sympa.qcow2 -m /dev/sda1 /mnt/
```

- `~luc/.vms/sympa.qcow2` : le chemin vers l'image
- `/dev/sda1` : la partition de la VM à monter
- `/mnt/` : l'endroit où monter la partition

Si vous ne connaissez pas l'identifiant de la partition que vous souhaitez monter, vous pouvez mettre une partition fantaisiste (exemple: `/dev/trs`) et le message d'erreur vous indiquera les partitions existantes :

```
libguestfs : erreur : mount_options: mount_options_stub: /dev/trs: No such file or directory
guestmount: '/dev/trs' could not be mounted.
guestmount : Voulez-vous monter l'un de ces systèmes de fichiers ?
guestmount:   /dev/sda1 (ext4)
guestmount:   /dev/sda5 (swap)
```

# Démonter l'image disque

```
umount /mnt/
```

---

Tiré de <https://www.xmodulo.com/mount-qcow2-disk-image-linux.html>.

# Réinstaller les modules Perl installés avec la version précédente de Perl

Un truc con quand on installe des modules Perl avec `cpan` ou `cpanm`, c'est qu'ils sont installés dans un répertoire dont le nom est la version de Perl utilisée.

Donc quand on installe un module sur une Debian Stretch et qu'on met à jour la machine vers Debian Buster, les modules installés via `cpan` ou `cpanm` ne sont plus disponibles vu qu'on change de version de Perl.

Heureusement que les modules installés sont listés dans un coin ☐☐

Pour trouver les modules qu'on avait installé en Stretch :

```
cat /usr/local/lib/x86_64-linux-gnu/perl/5.24*/perllocal.pod | grep "C<Module>" | sed -e 's/.*C<Module>L<\(.*\)|.*>/1/' | tr '\n' ' '
```

Pour tous les réinstaller en un tour de main :

```
cpanm $(cat /usr/local/lib/x86_64-linux-gnu/perl/5.24*/perllocal.pod | grep "C<Module>" | sed -e 's/.*C<Module>L<\(.*\)|.*>/1/' | tr '\n' ' ')
```

Bien évidemment, ça marche avec les précédentes versions de Debian, et ça devrait aussi fonctionner avec les suivantes, il n'y a qu'à changer le numéro de version ☐☐

**NB** : ça ne concerne pas les modules Perl installés via les paquets Debian.

# Salt

Salt est un logiciel de gestion de configuration comme Puppet ou Ansible.

Je l'utilise chez Framasoft et sur mon infra personnelle parce que je l'aime bien :

- rapide ;
- très bien documenté ;
- syntaxe claire, accessible mais néanmoins flexible et puissante.

## Changer ses mots de passe en masse

Je change mes mots de passe régulièrement (une fois par an environ). C'est toujours galère à faire quand on gère une tripotée de serveurs (entre les serveurs physiques et les VMs, on en est à plus de 100 serveurs chez Framasoft).

Avant, je faisais ça à la main : je lançais mssh sur 4, 6 ou 8 serveurs à la fois, et je modifiais mon mot de passe à la main. Mais ça, c'était avant.

### Salt à la rescousse

Pour changer le mot de passe de l'utilisateur `bar` sur le serveur `foo` avec salt, on fait :

```
salt foo shadow.set_password bar "$6$selselse$HASHEDPASSWORD"
```

`$6$selselse$HASHEDPASSWORD` correspond à votre mot de passe salé et hashé. Vous retrouvez un brol du genre dans votre `/etc/shadow` (Oh ! Vous avez remarqué ? C'est le nom du module salt qui permet de modifier votre mot de passe ! C'est bien fait quand même ☺)

Pour créer l'ensemble `$6$selselse$HASHEDPASSWORD`, vous pouvez utiliser python (nécessite le module passlib, fourni par le paquet Debian `python3-passlib`) :

```
python3 -c "from passlib.hash import sha512_crypt; print(sha512_crypt.hash('LE_PASSWORD', rounds=5000))"
```

Bon, on sait comment faire, mais on ne va pas s'amuser à taper 100 fois ces commandes !

Salt permet de vérifier que les minions (les agents Salt) répondent bien avec cette commande :

```
salt foo test.ping
```

Ce qui donne :

```
foo:  
True
```

On va changer le format de sortie :

```
salt foo --out text test.ping
```

Ce qui nous donne :

```
foo: True
```

Bien ! On peut pinguer d'un coup tous les minions avec :

```
salt \* --out text test.ping
```

On a donc la liste des minions, la commande pour changer le mot de passe... on va mixer tout ça :

```
salt \* --out text test.ping | \  
sed -e "s@\[^\]:*\):.*@echo salt \1 shadow.set_password bar \\\\"$(python3 -c \"from passlib.hash import  
sha512_crypt; print(sha512_crypt.hash('LE_PASSWORD', rounds=5000))\")\\\\"@"
```

1ère regex : on dégage les `: True`, et la deuxième, on enrobe le nom du minion pour que ça nous donne un truc comme :

```
echo salt foo shadow.set_password bar \"$(python3 -c \"from passlib.hash import sha512_crypt;  
print(sha512_crypt.hash('LE_PASSWORD', rounds=5000))\")\"
```

Quand on exécute ça, ça donne un truc genre :

```
salt foo shadow.set_password bar  
"$6$8qJhzAi6$.O8bOisJaM9fH05aXx7xnKXOVFoI9CRzjORFWDqoPR/TBOiYVZUEJKtUKirNMyaZJvJMPVUMhNry9QP  
JgHK/"
```

Bien évidemment, on va mettre ça dans un fichier qu'on va éditer pour modifier le mot de passe (bah oui, on va quand même pas mettre le même mot de passe sur tous les serveurs).

```
salt \* --out text test.ping | \  
sed -e "s@\([^\:]*\)::.*@echo salt \1 shadow.set_password bar \\\\\\\$(python3 -c \"from passlib.hash import  
sha512_crypt; print(sha512_crypt.hash('LE_PASSWORD', rounds=5000))\\\"\\\\\\\\\\\"@\" > /tmp/chpasswd.txt
```

On édite `/tmp/chpasswd.txt` pour mettre ses mots de passe bien comme il faut puis :

```
bash /tmp/chpasswd.txt | bash
```

Le `echo` va nous sortir la commande kivabien qui sera interprétée par bash. Le bout de python transformera le mot de passe en hash dans le format kivabien pour le fichier `/etc/shadow` et la commande salt sera lancée sur chaque minion.

# Sed

C'est l'outil absolu pour modifier du texte en le passant par un pipe ! Ou pour effectuer des changements en masses sur un fichier sans l'ouvrir. Bref, comme le dit l'adage : « Sed, c'est bien »  
☐☐

Il est possible de faire des trucs de tarés avec (hey, c'est pas juste un truc pour faire des substitutions à coup d'expressions rationnelles, c'est un vrai éditeur de texte, on peut se balader dans le texte, faire des copier/coller, etc).

## Syntaxe de base

Avec un fichier :

```
sed <commande> fichier.txt [fichier2.txt] [fichier3.txt]
```

En utilisant la sortie d'une autre commande :

```
find . -name \*.txt | sed <commande>
```

**NB :** `sed`, par défaut, ne modifie pas le fichier utilisé. Il affichera sur la sortie standard le fichier modifié par la commande passée à `sed`. Si on souhaite que le fichier soit modifié, on utilise l'option `--in-place` ou son abbréviation `-i` (on peut indifféremment placer l'option avant ou après la commande) :

```
sed <commande> --in-place fichier.txt  
sed -i <commande> fichier.txt
```

## Expression régulières

Si `sed` est un éditeur de texte (son nom veut dire Stream EDitor) et qu'il est utilisable en lui donnant des commandes équivalentes à « Va à ligne 3, supprime 4 caractères, descend à la ligne suivante... », on l'utilise souvent avec des expressions régulières.



# Rappel sur les expressions régulières

Les expressions régulières permettent de rechercher des correspondances avec un motif, écrit avec une syntaxe spéciale.

Les éléments de syntaxe suivants appartiennent aux *Perl Compatible Regular Expression* (PCRE), qui sont le standard de la très grande majorité des langages de programmation. `sed` utilisant une syntaxe légèrement différente, certains caractères devront être échappés (voir plus bas).

**NB** : j'ai placé les expressions régulières de cette section entre des `/` pour les distinguer des chaînes de caractères simples.

- `.` : correspond à un caractère, n'importe lequel. `/./` correspondra à tout sauf à une chaîne vide
- `?` : quantificateur, modifie la correspondance du caractère qui le précède : celui ci peut être présent zéro ou une fois. `/a?/` correspondra à une chaîne vide ou à `a`
- `+` : quantificateur : le caractère précédent sera présent une ou plusieurs fois. `/a+/` correspondra à `a`, `aa`, `aaa`...
- `*` : quantificateur : le caractère précédent sera présent zéro ou plusieurs fois. `/a*/` correspondra à une chaîne vide, à `a`, `aa`, `aaa`...
- `{n}` : quantificateur : le caractère précédent sera présent `n` fois. `/a{3}/` correspondra à `aaa`
- `{n,m}` : quantificateur : le caractère précédent sera présent de `n` à `m` fois. `/a{3,5}/` correspondra à `aaa`, `aaaa` ou `aaaaa`
- `{n,}` : quantificateur : le caractère précédent sera présent au moins `n` fois. `/a{3,}/` correspondra à `aaa`, `aaaa`, `aaaaa`, `aaaaaa`...
- `|` : séparateur d'expression. `/bonjour|hello/` correspondra à `bonjour` ou à `hello`
- `[^liste]` : correspond aux caractères n'étant pas entre crochets. `/[^ae]/` correspondra à n'importe quel caractère sauf à `a` et à `e`
- `[liste]` : correspond à un des caractères entre crochets. `/[ae]/` correspondra à `a` ou à `e`. Pour que le caractère `^` soit un choix possible, il faut le placer à une autre place que la première place : `[liste^]`, `[lis^te]`... On peut aussi spécifier des plages de caractères : `[0-9a-zA-Z]`
- `^` : ancre, correspond au début de la ligne. `/^a/` correspondra à `a` si celui-ci est le premier caractère de la ligne
- `$` : ancre, correspond à la fin de la ligne. `/a$/` correspondra à `a` si celui-ci est le dernier caractère de la ligne
- `(...)` : groupe l'expression. On peut s'en servir, par exemple, pour capturer des éléments (ce qui permet de les réutiliser plus tard) ou faire des sous-expressions. `/Bonjour (foo|bar), ça va ?/` correspondra à `Bonjour foo, ça va ?` et à `Bonjour bar, ça va ?`

Pour utiliser les caractères de manière littérale (exemple : pour correspondre à un point), on les échappera avec un `\`. `/\./` correspondra au caractère point (`.`).

# Caractères à échapper dans sed

La version GNU de `sed` utilise les *Basic Regular Expression* (BRE), qui ont une syntaxe légèrement différentes des PCRE.

Certains caractères doivent donc être échappés dans les BRE, qui sont utilisables tels quels pour des PCRE :

- le quantificateur `+`. Exemple : `/a\+/`
- le quantificateur `?`. Exemple : `/a\?/`
- le quantificateur `{i}`. Exemple : `/a\{5\}/`
- les parenthèses `(...)`. Exemple : `/\a\(/`
- le séparateur d'expressions régulières `|`. Exemple : `/a\b/`

## Effectuer une substitution de texte

La commande à utiliser est `'s/expression régulière/substitution/'` :

```
sed 's/foo/bar/' foo.txt
```

Cette commande remplacera la **1ère occurrence** de `foo` de **chaque ligne** du fichier par `bar`.

Si on souhaite remplacer toutes les occurrences de chaque ligne, on emploie le modificateur `g` :

```
sed 's/foo/bar/g' foo.txt
```

Si on ne souhaite remplacer que l'occurrence n°X de chaque ligne :

```
sed 's/foo/bar/X' foo.txt
## Exemple avec la 2e occurrence :
sed 's/foo/bar/2' foo.txt
```

Si on ne souhaite remplacer l'occurrence n°X de chaque ligne, ainsi que les suivantes :

```
sed 's/foo/bar/gX' foo.txt
## Exemple avec la 2e occurrence et les suivantes :
sed 's/foo/bar/g2' foo.txt
```

Ajouter quelque chose au début de chaque ligne :

```
sed 's/^/FooBar /' foo.txt
```

Ajouter quelque chose à la fin de chaque ligne :

```
sed 's/$/ BazQux/' foo.txt
```

Si on souhaite que l'expression régulière soit insensible à la casse (ex : `s` qui correspond aussi à `S`), on emploie le modificateur `i` :

```
sed 's/foo/bar/i' foo.txt
```

On peut utiliser plusieurs modificateurs en même temps :

```
sed 's/foo/bar/gi' foo.txt
```

Pour réutiliser ce qui a correspondu à l'expression régulière dans la chaîne de substitution, on utilise le caractère `&` :

```
sed 's/foo/& et bar/' foo.txt
```

Pour réutiliser ce qui a correspondu à un groupe d'expression, on utilise `\1` pour le 1er groupe, `\2` pour le 2e groupe... :

```
sed 's/Bonjour (foo|bar). Il fait beau./Bonsoir \1. À demain./' foo.txt
```

**NB** : on peut utiliser d'autres séparateurs que le caractère `/`, ce qui rend l'écriture d'une commande plus simple si l'expression régulière ou la substitution comportent des `/` : plus besoin de les échapper. Exemple :

```
sed 's@/home/foo@/var/bar@' foo.txt
```

# Supprimer des lignes

Supprimer la ligne `n` :

```
sed 'nd' foo.txt  
## Exemple avec la 3e ligne :  
sed '3d' foo.txt
```

Supprimer les lignes `n` à `m` :

```
sed 'n,md' foo.txt  
## Exemple :
```

```
sed '3,5d' foo.txt
```

Supprimer toutes les lignes sauf la ligne `n` :

```
sed 'n!d' foo.txt  
## Exemple :  
sed '6!d' foo.txt
```

**NB** : attention, le caractère `!` est un caractère spécial pour `bash` (et les autres shells). Si vous utilisez des apostrophes (`'`) pour votre commande `sed`, tout ira bien, mais si vous utilisez des guillemets doubles (`"`), il faut l'échapper avec un `\`.

Supprimer toutes les lignes sauf les lignes `n` à `m` :

```
sed 'n,m!d' foo.txt  
## Exemple :  
sed '6,8!d' foo.txt
```

Supprimer les lignes qui correspondent à une expression régulière :

```
sed '/regex/d' foo.txt  
## Exemple :  
sed '/foobar/d' foo.txt
```

Pour supprimer les lignes vides, d'un fichier, il suffit d'utiliser l'expression régulière qui signifie que la ligne est vide :

```
sed '/^$/d' foo.txt
```

Pour supprimer la première ligne correspondant à une expression régulière, ainsi que toutes les lignes suivantes :

```
sed '/regex/, $d' foo.txt  
## Exemple :  
sed '/foobar/, $d' foo.txt
```

**NB** : attention encore une fois aux guillemets doubles, il faudrait échapper `$` dans cette commande car le shell essaierait d'interpréter `$d` comme une variable.

# Tmux

Tmux est un multiplexeur de terminal. Il permet d'utiliser plusieurs terminaux virtuels dans une seule fenêtre de terminal ou une session sur un terminal distant.

## Ligne de commande

### Lancement

Rien de plus simple :

```
tmux
```

Pour nommer une session :

```
tmux new-session -s <nom de la session>
```

### Voir les sessions tmux existantes

```
tmux ls
```

### Se rattacher à une session tmux existante

S'il n'y a qu'une seule session, ou si vous voulez vous rattacher à la dernière auquel vous étiez rattaché :

```
tmux at
```

Si vous souhaitez cibler une autre session :

```
tmux at -t <nom de la session>
```

Bonus : vous pouvez être plusieurs personnes sur une même session. C'est très pratique quand on doit faire des manipulations à plusieurs, ou dans un but didactique.

## Couper une session tmux existante

S'il n'y a qu'une seule session, ou si vous voulez couper la dernière auquel vous étiez rattaché :

```
tmux kill-session
```

Si vous souhaitez cibler une autre session :

```
tmux kill-session -t <nom de la session>
```

## Aide

Faites `Ctrl + b` puis `?` et tmux vous affichera une liste de commande accessibles avec des raccourcis claviers

## Raccourcis claviers usuels

### Se détacher de la session tmux

Tmux peut continuer à fonctionner même quand on est déconnecté ou qu'on se détache de la session, ce qui est très pratique pour :

- les connexions réseaux moisiées qui vous déconnectent de votre session SSH
- lancer une commande qui va durer longtemps

`Ctrl + b` puis `d`

### Ouvrir une nouvelle fenêtre

`Ctrl + b` puis `c`

### Naviguer entre les fenêtres

**Ctrl** + **b** puis **n** (-> **next**) pour passer à la fenêtre suivante.

**Ctrl** + **b** puis **p** (-> **previous**) pour passer à la fenêtre précédente

## Renommer une fenêtre

**Ctrl** + **b** puis **,**, vous aurez un prompt dans la barre en bas, tapez ce que vous voulez et appuyez sur la touche **Entrée**.

Pour sortir du prompt sans valider, appuyez sur la touche **Esc**.

## Créer un nouveau panneau

### En coupant la fenêtre horizontalement

Le nouveau panneau sera créé à droite du panneau courant.

**Ctrl** + **b** puis **%**

### En coupant la fenêtre verticalement

Le nouveau panneau sera créé en dessous du panneau courant.

**Ctrl** + **b** puis **"**

## Zoomer sur un panneau

Si les panneaux sont pratiques, on a parfois envie d'en prendre un et de l'avoir temporairement en plein écran. Pour ça :

**Ctrl** + **b** puis **z**

Et on utilise le même raccourci pour remettre le panneau en petit comme avant.

## Naviguer entre les panneaux

**Ctrl** + **b** puis utiliser les flèches du clavier

## Commandes

Pour entrer en mode commande, faites `Ctrl + b` puis `:`. Vous aurez un prompt dans la barre en bas.

## Afficher toutes les commandes disponibles

Utiliser la commande `list-commands`.

## Changer le répertoire de départ

Quand on ouvre un tmux, chaque nouvelle fenêtre ou nouveau panneau s'ouvrira dans le répertoire depuis lequel vous avez créé le tmux.

Pour changer ce répertoire de départ, utiliser la commande `attach -c /le/dossier/que/vous/voulez`.

## Afficher les variables d'environnement de la session

Utilisez la commande `show-environnement` ou son alias `showenv`.

Ce sont les variables d'environnement de tmux : il y a aussi les variables d'environnement du système, qui sont copiées par tmux au démarrage d'une session et qui sont fusionnées avec les variables d'environnement de tmux, celles-ci ayant la priorité si une variable existe dans les deux environnements.

## Paramétrer une variable d'environnement pour la session

Pour modifier ou ajouter une variable d'environnement à la session, utilisez la commande `set-environnement NOM_VAR valeur` ou son alias `setenv NOM_VAR valeur`.



# Trucs et astuces

Il est un certain nombre de logiciels qu'un administrateur systèmes rencontrera au cours du temps. Ceux-ci lui permettront d'acquérir des automatismes et de gagner un temps considérable dans l'accomplissement de ses tâches.

Page aussi disponible sur <https://luc.frama.io/cours-asrall/tips/>.

## Éditer un fichier

Que votre éditeur favori soit *vim*, *nano*, *emacs* ou autre, il faut vous assurer :

- de connaître ses commandes (aller à la ligne X, faire un chercher/remplacer, réindenter)
- de savoir activer la coloration syntaxique. Ça paraît superfétatoire, mais c'est essentiel car cela vous permet de vous repérer plus rapidement dans le fichier voire de détecter des erreurs de syntaxe.

Il est nécessaire de connaître son éditeur pour être efficace.

Pour *vim*, vous pouvez lancer *vimtutor* qui vous fera passer par des exercices pour vous familiariser avec *vim*. Le site [VimCasts](#) regorge de tutoriaux et d'astuces.

**Attention** : quand bien même vous ne choisiriez pas *vim*, il vous faut en connaître les commandes de base. En effet, *emacs* n'est que rarement installé sur un serveur, et *nano* est parfois (souvent ?) trop limité pour travailler vite et bien.

## Les processus

### htop

*htop* permet de lister les processus, rechercher un processus, tuer des processus, trier les processus selon différents critères...

Il affiche également des informations sur le système : occupation mémoire, utilisation des processeurs, charge du système, etc.

Pour n'afficher que les processus de l'utilisateur `foo` :

```
htop -u foo
```

Voir <https://peteris.rocks/blog/htop/> pour comprendre les informations fournies par *htop*.

[Carl Chenet](#) a traduit ces articles en français dans une série d'article disponible sur <https://carlchenet.com/category/htop-explique/>.

## kill

La commande *kill* permet d'envoyer un signal à un processus. On peut indifféremment utiliser le n° ou le nom d'un signal pour l'utiliser. Ainsi `kill -9 <PID>` est normalement équivalent à `kill -KILL <PID>`.

Pour être bien certain du signal envoyé, il est préférable d'utiliser son nom : tous les signaux n'ont pas un n° attribué de façon certaine.

Voir [https://en.wikipedia.org/wiki/Unix\\_signal#POSIX\\_signals](https://en.wikipedia.org/wiki/Unix_signal#POSIX_signals) pour la liste des signaux POSIX.

## killall

*killall* est le petit frère de *kill*. Il permet d'envoyer des signaux aux processus sans connaître leur PID, juste avec leur nom.

Comme *killall* peut ratisser large, il vaut mieux lui préférer le couple *pgrep* / *pkill*.

## pgrep / pkill

*pgrep* permet de rechercher parmi les processus, *pkill* permet d'envoyer un signal aux processus avec la même syntaxe de recherche que *pgrep*.

Rechercher un processus par son nom :

```
pgrep nom
```

Rechercher un processus par l'intégralité de sa ligne de commande :

```
pgrep -f nom
```

Rechercher un processus par son nom, appartenant à l'utilisateur `foo` :

```
pgrep -u foo nom
```

Afficher le nom du processus en plus de son PID :

```
pgrep -l nom
```

Afficher la ligne de commande complète en plus de son PID :

```
pgrep -a nom
```

Envoyer le signal SIGTERM aux processus correspondants à la recherche :

```
pkill SIGTERM nom
```

## Isof

*Isof* permet de connaître le ou les processus utilisant une ressource.

Qui utilise `/home/foo` ?

```
Isof /home/foo
```

Qui utilise `/dev/sda` ?

```
Isof /dev/sda
```

Qui utilise le port 80 ?

```
Isof -i :80
```

## Les logs

### multitail

*multitail* permet de surveiller en temps réel les modifications d'un ou plusieurs fichiers à la manière d'un `tail -f` mais est bien plus souple d'usage.

Lire plusieurs fichiers :

```
multitail mail.log kern.log
```

Filtrer les lignes affichées d'un fichier selon une regex :

```
multitail -e regex mail.log kern.log
```

Filtrer les lignes affichées de *tous* les fichiers selon une regex :

```
multitail -E regex mail.log kern.log
```

Pour les données depuis l'entrée standard :

```
commande_qui_fait_des_logs | multitail -j
```

Une fois *multitail* lancé, un grand nombre de raccourcis claviers permet de le manipuler :

- **Entrée** : Affiche une ligne rouge avec l'heure et la date sur chaque fenêtre d'affichage de fichier (utile pour se donner un repère avant un test générant des logs)
- **O** (la lettre o en majuscule) : Efface l'affichage de toutes les fenêtres
- **/** : Effectue une recherche dans toutes les fenêtres
- **b** : Permet de revenir en arrière sur une fenêtre
- **F1** : affiche l'aide, avec tous les raccourcis claviers

## goaccess

*goaccess* va analyser en temps réel les logs d'un serveur pour fournir des statistiques.

On pourra alors voir rapidement quelle est l'adresse IP qui se connecte le plus, quelle est la page la plus visitée, etc.

## Veille technologique

Non, passer du temps sur [LinuxFR](#) ou sur le [Journal du hacker](#) n'est pas du temps perdu, quoi qu'on en dise. Il est en effet important d'effectuer une veille technologique régulière afin de découvrir de nouvelles technologies, de nouvelles astuces ou d'être averti de nouvelles failles de sécurité.

Votre meilleur ami pour cette veille sera un lecteur de flux RSS. En effet, un lecteur de flux a cet immense avantage sur les réseaux sociaux d'être asynchrone : partez en vacances deux semaines, revenez, et lisez tout ce que vous avez loupé (essayez un peu de faire cela avec Twitter : impossible). Vous pouvez aussi généralement le configurer pour qu'il vous envoie un résumé par mail de vos flux RSS... parfait quand on le couple à la liste de discussion des autres administrateurs

systèmes !

Attention : les réseaux sociaux comme Twitter peuvent aussi être utiles, de par leur propension à propager (très) rapidement l'information. Le revers de la médaille est qu'il faudra bien vérifier la véracité de la-dite information.

# SSH

## Concierge

SSH fonctionne bien de base, mais avoir un fichier de configuration SSH améliore grandement les choses.

Exemple : votre identifiant sur votre machine locale est *rim*, mais *rimd* sur la machine *mavrick.chatons.org*. Pour vous connecter, vous lancez la commande `ssh rimd@mavrick.chatons.org`

Avec un fichier de configuration ssh (`~/.ssh/config`) contenant

```
Host mavrick
  HostName mavrick.chatons.org
  User rimd
```

vous pourrez vous connecter avec un simple `ssh mavrick`,

Avec quelques serveurs, la gestion de ce fichier ne pose pas de problème, mais on s'aperçoit, au fur et à mesure que l'on a plus de serveurs à gérer que cela devient une plaie. C'est là qu'intervient *concierge*.

*concierge* permet de gérer son fichier de configuration avec un langage de *template*.

On pourra donc écrire

```
{% for i in ('dorone', 'khais') %}
Host {{i}}
  HostName {{i}}.chatons.org
  User rimd
  IdentitiesOnly yes
  IdentityFile /home/%u/.ssh/id_chatons
{% endfor %}
```

```
{% for i in ('gohan', 'diren') %}  
Host {{i}}  
    HostName {{i}}.perso.org  
    User rim  
    IdentitiesOnly yes  
    IdentityFile /home/%u/.ssh/id_perso  
{% endfor %}
```

Ce qui créera des entrées dans le fichier de configuration SSH pour les serveurs *dorone*, *khais*, *gohan* et *diren*.

Voir <https://github.com/9seconds/concierge> pour l'installation de *concierge*.

## Mssh

*mssh*, disponible habituellement dans les dépôts de votre distribution préférée, vous permettra de lancer plusieurs connexions SSH en même temps. La fenêtre contiendra autant de terminaux que de connexions SSH. Les commandes tapées seront envoyées à tous les terminaux en même temps (il est possible de n'envoyer la commande que sur un seul serveur ou de "désactiver" certains serveurs pour que les commandes ne leur soient pas envoyées).

*mssh* est très utile pour effectuer des tâches simultanément.

On lance *mssh* ainsi : `mssh gohan diren`

## Confort visuel

### redshift

*redshift*, lui aussi généralement dans les dépôts, ajuste la température de votre écran en fonction de l'heure. L'idée est de rougir graduellement l'écran afin d'éviter la fatigue visuelle due à la lumière bleue de votre écran.

## Confort dans le terminal

### bash-completion

Activer l'utilisation d'une complétion avancée des commandes se fait dans Debian en décommentant les lignes suivantes du fichier */etc/bash.bashrc* :

```
if ! shopt -oq posix; then
  if [ -f /usr/share/bash-completion/bash_completion ]; then
    . /usr/share/bash-completion/bash_completion
  elif [ -f /etc/bash_completion ]; then
    . /etc/bash_completion
  fi
fi
```

Cela permettra, par exemple, de compléter les options d'un logiciel, le nom d'un paquet à installer, etc. Sans cela, vous n'aurez que la complétion du logiciel que vous voulez utiliser et des chemins de votre système de fichiers.

## tree

*tree* affichera l'ensemble d'une arborescence... sous forme arborescente. Ce qui permet de parcourir un dossier très vite.

```
% tree foo
foo
├── bar
│   └── baz.txt

1 directory, 1 file
```

## Sécurité

### mkpasswd.pl

Fourni par le paquet *libstring-mkpasswd-perl* dans Debian, *mkpasswd.pl* permet de générer des mots de passe aléatoires, éventuellement en forçant quelques paramètres.

```
% mkpasswd.pl -l 20 -s 4
kta*vvN:g7bxM/se8a-b
```

- `-l 20` : 20 caractères

- `-s 4` : avec 4 caractères spéciaux (ponctuation, pourcent, etc)

# Manipulation de données

## Sort

Le vénérable `sort` permet de trier des données.

```
sort < fichier.txt
```

Parmi les options intéressantes :

- `-u` supprime les doublons
- `-n` fait un tri numérique, c'est-à-dire que `2` vient avant `10`, là une machine dira que `10` vient avant `2` car le premier caractère `1` vient avant `2`
- `-h` fait un tri « humain » des nombres, c'est-à-dire qu'il va lire `2K` comme `2000`, et le triera après `1G`
- `-r` trie en sens inverse
- `-k` trie selon une clé. Par exemple, avec `foo bar`, `bar` est la clé n°2
- `-t` spécifie le séparateur des clés. Par défaut, la séparation est définie par une transition entre caractère vide (espace, tabulation, etc.) en non-vide

## Jq

Le logiciel `jq` permet de manipuler du JSON directement depuis la ligne de commande.

J'avoue, je l'utilise surtout pour récupérer juste l'info qu'il me faut, je modifie très rarement du JSON avec (mais on peut !)

```
jq '.job.status' < foo.json
```

## Yq

Le logiciel `yq` est au YAML ce que `jq` est au JSON. D'ailleurs, `yq` se sert de `jq` en interne.

```
yq '.job.status' < foo.yml
```



Note : `yq` n'aime pas les clés avec un `-`. Il faut alors utiliser une autre syntaxe que la classique `.key` :

```
yq '.job["foo-bar"]' < foo.yml
```

# Divers

## ncdu

*ncdu* va regarder la taille du répertoire ciblé (celui où on se trouve par défaut) et afficher les fichiers/dossiers contenus, triés par taille. Très utile pour trouver ce qui bouffe de l'espace disque.

Petit bonus : pour avoir un *ncdu* sur un *bucket* S3, on peut utiliser le logiciel *rclone* ainsi :

```
rclone ncdu remote:path
```

## watch

*watch* permet de lancer une commande à intervalle régulier. Après une modification DNS, *watch dig chatons.org* pourra par exemple vous permettre de surveiller la prise en compte de cette modification sur votre résolveur.

## truncate

*truncate* permet de réduire ou étendre la taille d'un fichier à la taille indiquée.

```
truncate -s 1M fichier_trop_gros
```

## split

*split* permet de découper un fichier en plusieurs parties.

## wall

*wall* permet d'envoyer un message à tous les utilisateurs connectés à la machine.



# Supprimer une clé SSH stockée par gpg-agent

Gpg-agent peut servir d'agent SSH (il va donc conserver les clés en mémoire) mais si l'ajout d'une clé se fait bien classiquement avec `ssh-add ...`, la suppression d'une clé est plus complexe, `ssh-agent -d ...` ne fonctionnant pas.

## Repérer la somme MD5 de la clé à supprimer

Pour afficher les sommes MD5 des clés stockées par l'agent :

```
ssh-add -l -E md5
```

Ça donne un truc comme :

```
256 MD5:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa foo@bar (ED25519)
256 MD5:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb baz@qux (ED25519)
```

Si malheureusement vous n'avez pas spécifié le commentaire lors de la création de votre clé SSH, il y a des chances que vous vous retrouviez avec un truc comme :

```
256 MD5:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa foo@bar (ED25519)
256 MD5:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb foo@bar (ED25519)
```

Regardez bien la fin des lignes : vous ne savez pas quelle clé vous souhaitez supprimer !

Pour retrouver quelle somme MD5 correspond à quelle clé :

```
ssh-add -L
```

Ce qui affiche les clés publiques des clés SSH stockées, à savoir un truc comme :

```
ssh-ed25519 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
foo@bar  
ssh-ed25519 YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY foo@bar
```

Un coup de `grep -RF XX`  
`~/ssh` vous permettra d'identifier les clés. L'ordre entre `ssh-add -l -E md5` et `ssh-add -l` reste le  
 même (heureusement).

# Afficher le grip des clés stockées par gpg-agent

```
gpg-connect-agent 'KEYINFO --ssh-list --ssh-fpr' /bye
```

Ce qui donne un truc comme :

```
S KEYINFO VVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV D - - P
MD5:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa - S
S KEYINFO ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ D - - P
MD5:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb - S
```

Le texte après le `KEYINFO` est le grip de la clé, qui va nous servir pour supprimer la clé :

```
gpg-connect-agent 'DELETE_KEY ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ' /bye
```

Et c'est fini 

# Swap

Le swap est un espace d'échange qui recueille des données normalement en RAM lorsque l'utilisation de celle-ci dépasse un certain point.

## Gérer les espaces d'échange

### Voir l'utilisation des espaces d'échanges

```
cat /proc/swaps
```

Cela va donner quelque chose comme :

Filename	Type	Size	Used	Priority
/dev/dm-3	partition	3911676	3906776	-2
/var/swap	file	5242876	310324	-3

## Monter et démonter un espace d'échange

Les termes de montage/démontage ne sont pas corrects car les espaces d'échange ne sont pas montés sur le système. Vous ne les verrez pas avec la commande `mount`.

Pour ne plus utiliser un espace d'échange :

```
swapoff /dev/dm-3
```

Cette commande peut prendre un peu de temps car le contenu de l'espace d'échange va être déplacé dans la RAM ou dans un autre espace d'échange, ou oublié par le système s'il n'y a plus de place disponible.

Pour le réutiliser :

```
swapon /dev/dm-3
```

L'option `-a` permet d'agir sur tous les espaces d'échanges connus du système (dans `/etc/fstab` la plupart du temps. Systemd a un truc pour ça aussi, mais je ne l'ai encore jamais rencontré).

Exemple :

```
swapoff -a  
swapon -a
```

## Modifier le recours aux espaces d'échange

Les espaces d'échanges vont être utilisés avec plus ou moins d'agressivité selon la valeur de `vm.swappiness` de votre système (pour voir cette valeur : `sysctl vm.swappiness`). Cette valeur peut être comprise entre 0 et 100.

Un nombre élevé veut dire que le noyau va avoir plus tendance à décharger la RAM dans les espaces d'échanges que dans un système avec un nombre bas.

Pour modifier temporairement la valeur :

```
sysctl -w vm.swappiness=10
```

Pour la modifier de façon permanente :

```
echo "vm.swappiness = 10" > /etc/sysctl.d/99-swappiness.conf  
sysctl -p /etc/sysctl.d/99-swappiness.conf
```

(le `sysctl -p` est là pour appliquer la valeur que vous venez de mettre dans le fichier)

## Les différents supports d'espaces d'échanges

On peut avoir du *swap* avec une partition comme le propose Debian lors de l'installation ou via un fichier *swap*, comme le fait Ubuntu. On peut aussi avoir du *swap*... sur la RAM ! (voir plus bas)

L'avantage du fichier sur la partition est sa manipulation plus facile. Je pense en particulier à la modification de la taille du *swap*.

## Créer un fichier *swap*

C'est excessivement simple : on crée un fichier, on le prépare comme il faut, on le déclare dans `/etc/fstab` et on l'utilise.

```
fallocate -l 2G /var/swap
mkswap /var/swap
chmod 600 /var/swap
echo "/var/swap none swap sw 0 0" >> /etc/fstab
swapon /var/swap
```

## Utiliser de la RAM pour l'espace d'échange

Cela paraît contre-intuitif, mais c'est très simple : l'espace d'échange sera compressé et conservé en RAM. Le coût en performances de la compression/décompression des données est, avec nos processeurs actuels, généralement moindre que celui de l'utilisation d'un disque, fut-il SSD : la RAM permet des accès beaucoup, beaucoup plus rapides que n'importe quel disque.

Comme les espaces d'échanges sont utilisés comme de la RAM supplémentaire, mais lente, avoir ceux-ci sur la RAM, mais compressés équivaut plus ou moins à une augmentation de taille de RAM au prix de quelques cycles CPU.

Pour utiliser ce mécanisme, il suffit, sur Debian, d'installer le paquet `zram-tools`, de modifier `/etc/default/zramswap` à son goût et de relancer le service `zramswap`.

# Systemd

## Créer un service utilisateur

Mettre le service dans le dossier `~/.config/systemd/user/` puis :

```
systemctl --user daemon-reload  
systemctl --user enable --now monscript.service
```

## Manipuler un service utilisateur depuis le compte root

```
systemctl --user --machine=le_user@ stop monscript.service
```



# Divers

# Avoir les émojis dans Konsole

Tiré de <https://gist.github.com/IgnoredAmbience/7c99b6cf9a8b73c9312a71d1209d9bbb>.

1. Installer la police Noto Color Emoji (paquet `fonts-noto-color-emoji` sur Debian)
2. Mettre ceci dans `~/.config/fontconfig/conf.d/99-hack-color-emoji.conf` :

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<!--
Hack + Color Emoji Font Configuration.
Currently the only Terminal Emulator I'm aware that supports colour fonts is Konsole.
Usage:
0. Ensure that the Noto fonts are installed on your machine.
1. Install this file to ~/.config/fontconfig/conf.d/99-hack-color-emoji.conf
2. Run `fc-cache`
3. Set Konsole to use "Hack" as the font.
4. Restart Konsole.
-->
<fontconfig>
  <match>
    <test name="family"><string>Hack</string></test>
    <edit name="family" mode="prepend" binding="strong">
      <string>Noto Color Emoji</string>
    </edit>
  </match>
</fontconfig>
```

3. Changer `Hack` par la police actuellement utilisée par Konsole
4. Lancer `fc-cache`
5. Redémarrer Konsole

# Envoyer un fichier sur Nextcloud avec cURL

## Vers un partage public

Mettons que l'adresse du partage public où vous pouvez envoyer des fichiers est `https://example.org/s/foo-bar`.

La requête pour envoyer un fichier sera :

```
curl --silent \  
  --show-error \  
  --user "foo-bar:" \ # <-- la dernière partie de l'adresse du partage !  
  --header 'X-Requested-With: XMLHttpRequest' \  
  --upload-file fichier.txt \ # <-- le fichier à envoyer  
  https://example.org/public.php/webdav/ #
```

## Avec des identifiants

Utilisez vos identifiants sur le Nextcloud. Il est conseillé de créer un mot de passe d'application dans les paramètres personnels pour ne pas laisser son mot de passe traîner dans un script.

```
curl --silent \  
  --show-error \  
  --user "user:password" \ # <-- votre login et votre mot de passe  
  --upload-file fichier.txt \  
  https://example.org/remote.php/dav/files/votre_uid_nextcloud/le/chemin/du/dossier
```

Dans l'URL, `votre_uid_nextcloud` correspond à votre `uid` nextcloud, qui est généralement votre login, mais qui peut être différent, lors de l'utilisation d'un serveur LDAP par exemple.

# Manipuler un ou plusieurs fichiers PDF : PDFtk

Quand il s'agit de manipuler des fichiers PDF, c'est à dire en fusionner deux ensemble, supprimer une page sur deux, virer un mot de passe..., l'outil à utiliser est généralement PDFtk.

## Fusionner des fichiers PDF en un seul

```
pdftk *.pdf cat output combined.pdf
```

## Virer les pages impaires

```
pdftk input.pdf cat even output output-file.pdf
```

Pour virer les pages paires, on utilisera `odd` à la place de `even`.

## Supprimer le mot de passe sur un fichier PDF

Attention : pour ça, il faut avoir le mot de passe, hein !

```
pdftk encrypted.pdf input_pw le_mot_de_passe output unencrypted.pdf
```

Comme mettre un mot de passe dans une ligne de commande n'est généralement pas une bonne idée, on utilisera plutôt le mot de clé `PROMPT`, qui fait que PDFtk demandera le mot de passe de façon interactive :

```
pdftk encrypted.pdf input_pw PROMPT output unencrypted.pdf
```