

Mail

Tout ce qui concerne le mail

- [Postfix](#)
- [Rspamd](#)
- [Vade Secure \(antispam propriétaire\)](#)
- [Outils pour les rapports DMARC](#)
- [Outils pour générer et vérifier ses enregistrements SPF/DKIM/DMARC](#)

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_mecanisms` 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$JpGqMfx4G6lyRu0kN2uKdRvexzrwJXNo6dWkUuZZjV/
```

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/rspamd/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=MIIBIjANBgkqhkiG9w0BAQEFAAA0CAQ8AMIIBCgKCAQEAzgAF2ozDnleUGRbtwmbTEglzmmsLh0jsT96q0P+J0rTPnG  
X/oIWwx2MkTRW46gSU7Ya1ByG9EKfEQo3V+Zfr5xeY+00ks18nrHUK56haW7kqVAEhyo4NPqhhTRUheAIMgLbyYLFN0qpQ  
DCdmfyn6fv0bK6caqtNXAWy3vWTeMacBgx1JGfrYE1NFyNqKcfHcbtXXfSGNo6phVz9K"  
  
"1Tl13wvZhdW3hBwgq49cZ5yp0IsrLL0fqM0nHcS83YHlNMRVVGvPko8+ucMhKktbAoDdEMMWupxyWGs1M1xKW0RQxFyYi  
5oZhSTW53VpyzldrLWXInerDRW2hn1amA2dLWwewIDAQAB"  
  
) ;
```

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](https://phishstats.info). 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_MAILLIST : 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_MAILLIST : 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
- MAILLIST : 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 [\[\[https://www.dnswl.org\]\]](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 abuses.

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
            end
        end
    end
}
```

```
        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";
```

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/flatux/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.