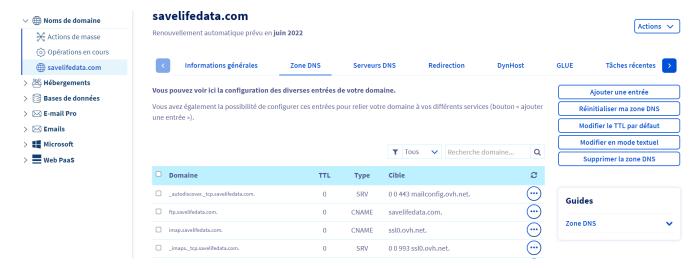
#### Bouti-Mazouz Samy/Kapri Anish

# Rapport solutions aux problèmes envoi et réception mail OVH

Attention à ne pas corriger les « erreurs » Word pour les informations à saisir !!!

D'après le support de chez OVH, les différents problèmes d'envoi et réception que nous rencontrons sur OVH sont liés à la zone DNS sur OVH : ou l'on configure les différentes entrées DNS du nom de domaine



En omettant que le service de messagerie Gmail puisse possiblement bloquer les mails entrants et sortant de notre domaine, il faudrait réaliser une démarche spécifique dans notre espace client pour régler les problèmes d'envoi et de réception :

#### SPF

-Il faudrait dans un premier temps, créer manuellement une nouvelle authentification SPF différente de la précédente plus restrictif en remplaçant le tilde "~" par un tiret "-" (-all à la place de ~all), via cette fois-ci une entrée en « TXT »

Le SPF (Sender Policy Framework) permet à un serveur qui reçoit un e-mail de s'assurer que ce dernier a bien été envoyé par un serveur qui en a le droit.

Pour cela, veuillez suivre cette démarche depuis votre espace client :

Cliquer sur votre nom de domaine sous la section "Domaines",

Aller dans l'onglet "Zone DNS"

Cliquer sur le bouton "Ajouter une entrée" et sélectionner le type "TXT",

Saisir dans le champ "Valeur" votre SPF: "v=spf1 include:mx.ovh.com -all"

# (NB : Nous pouvons ajouter « ip4:54.38.35.112 » l'IP du serveur avant le « -all » si cette erreur apparaît lors d'un test )



Supprimer les entrées de type "SPF" et garder uniquement cette nouvelle entrée de type "TXT".

Patienter un délai de 4 à 24 heures (temps de propagation DNS).

Ajouter une nouvelle entrée DNS sur OVH:



#### **DKIM**

-Dans un second temps, nous pourrions mettre en place une identification DKIM, qui est une signature permettant d'authentifier le domaine expéditeur. Cette authentification se fait par une clé DKIM que l'on peut générer simplement sur ce site : http://dkimcore.org/tools/keys.html

# Generate a DKIM Core Key

Domain name: savelifedata.com
Generate

#### DKIM Core tokens for savelifedata.com

Generated at Tue May 24 06:16:18 2022 for selector 1653398178.savelifedata

You can bookmark this page and all your keys will be kept here (for at least a month, probably forever).

#### Private key

This is the private key that needs to be entered into your DKIM signer. It must be kept secret - anyone with access to it can stamp tokens pretending to be you.

----BEGIN RSA PRIVATE KEY---MIICXQIBAAKBgQC-5\*KAy017LfUB0rjWp+uCz8bzz8+DH1ZGDmbjIxqq/fcbeVZa
6\*V864VV1j0rb-12mx5iznjbeijRqbf\*s9dzr\*IUnN5ZluxdkLExcMMNqc+lPAV8PHN
eABr5+7U+4eW0KNX8\*jgedBaeej3FP+1AKJV+UKOVMnipTl7nmltKyr-Vr-JurDaQAB
AoGBAIb3+tHB1LEyKyW0ln3rqXP9Y191KTKOm9xYKOL4d0dJv1JT9r88PQo/SYY6/
vSXeew1lu39DubyKNpxu4bRg6MUV0Krn+78oCfVLCgtdHcdkXuKp5dyjYfcnVgx6
drVsXMmKo2x8lNNQn/R+OcM7izLfOysMJDnz5oskiK8lMbgBAKEA4EmgnNZce80i
NXQf6g5df14Acx6KrNtYfWmp/rNZCCj0SW1IdT0qt3maCx4TNIxvYcXFgX9MUQe6r0
tvhtIayPkw3BAWQ1BRUy5vXp+WDP18vBdJmaTsysX4s852S64+DD38JV15Y1A7Z7
piJsrkStTM4LCSFT031su53SEG3S5nn6p6CQQDH5RQLemQKidxqux+j6WcZV5
Q70n03XbCEjKQq8S+z2ZkLz39NPOv7yV4jlaikpVMBSGaGv8trXekXxwAcDTAkAm
6rlXxiFP04vmNqRsor9U5DVzBVGiJX9kAhlcIUfVohqdvJlxTy9TUZkNcHihiAfII
6Qc2e2U2MDXf78XlMdFAKAnYNRZUmoaMy1aCKKAXUS5m15BE5NUHU14ESeth7v
BrcFlC4xV6MCBmm/tcjhjjsOMZKo83MnbFUtNe4+tfK1

Download private key

#### **Public key**

This is the public key that needs to be published via DNS before you start using the tokens to send mail.

#### **Bind 9 Format**

This is the public key in a format for use in a bind 9 zone file

Voici la clé DKIM (à saisir dans l'onglet « valeur ») :

 $v=DKIM1; k=rsa; t=s; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC4\\ stHQICo9KyHe4DYAKXFuJl3MafRX78LRR2LKfYK5jB/FhmOMY3XERylhisA4A\\ 2b+eoPYs3QV5px1CKd+Rv/9+m6wZEODIJkgthY+oxDcD5VUfGeoZOVZxpJ6T23\\ RjbEaeywl2JeLfEs0lLR43TVxiChLgswN+0DJqPcK3X61VwIDAQAB\\$ 

Nous allons à présent la vérifier grâce à l'outil de DkimCore (la clé est valide)

# DKIM Record v=DKIM1:k=rsa;t=s:p=MIGfMA0GCSqGSlb3DQEBAQUAA4GNADCBiOKBgQC4stHQICo9KyHe4D YAKXFuJI3MafRX78LR32LKfYK5jBjFhmOMY3XERylhisA4A2b+eoPYs3QV5px1CKd+Rv/9+m6w ZEODJJkgthY+oxDcD5VUfGeoZOVZxpJ6T23RjbEaeywl2JeLfEs0lLR43TVxiChLgswN+0DJqP ck3X61VwIDAQAB This is a valid DKIM key record Version v= DKIM1 Key type k=rsa Flags t= s Public key p=MIGfMA0GCSqGSlb3DQEBAQUAA4GNADCBiQKBgQC4stHQICo9KyHe4DYAKXFuJI3MafRX78LRR2LKfYK5jB/FhmOMY3XERylhisA4A2b+eoPYs3QV5px1CKd+Rv/9+m6wZEODJJkgthY+oxDcD5

La clé est à saisir dans une nouvelle zone d'entrée DNS de type « TXT »

1653398016.savelifedata.\_domainkey est à saisir dans l'onglet « sous domaine »

## **DMARC**

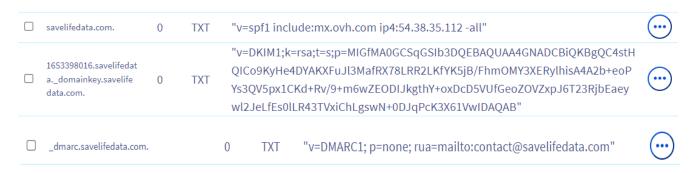
-Enfin nous allons également ajouter une entrée DMARC qui peut faciliter la réception des e-mails si le destinataire est chez un service de messagerie qui nécessite cela (Gmail par exemple)

Nous allons refaire une entrée DNS de type « TXT » dans laquelle il faut saisir ces informations :

-Nom de domaine : \_dmarc

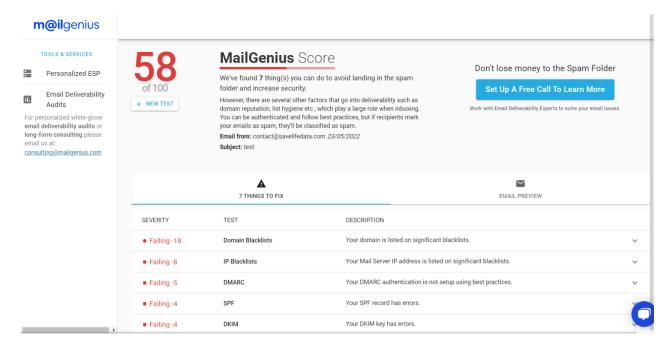
-Valeur : v=DMARC1; p=none; rua=mailto:VOTRE@EMAIL.COM (contact@savelifedata.com)

#### Nouvelles zones DNS:

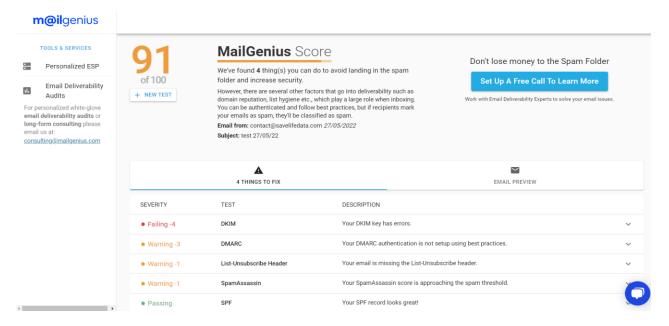


On peut alors comparer le premier test (Mail Genius qui vérifie la délivrabilité des mails) que nous avons réalisé avant ces modifications dans la zone DNS.

Avant (app.mailgenius.com/spam-test/542a5c):



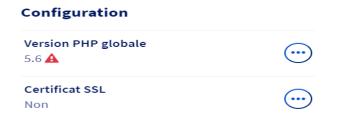
# Après (https://app.mailgenius.com/spam-test/d1548c):



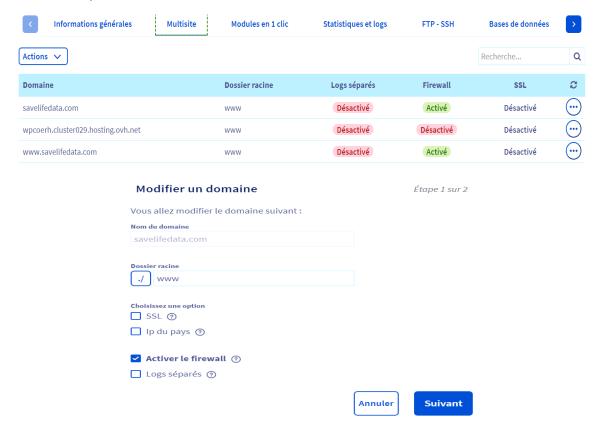
# <u>SSL</u>

Cependant, on constate que le système anti-spam de Gmail bloquent encore la réception et l'envoi, pour ce faire, je propose deux solutions qui pourraient contourner le système anti-spam de Gmail.

Dans un premier temps, nous pouvons activer le SSL sur OVH qui est pour l'instant désactiver.



Pour ce faire, il faut activer le SSL des multisites :



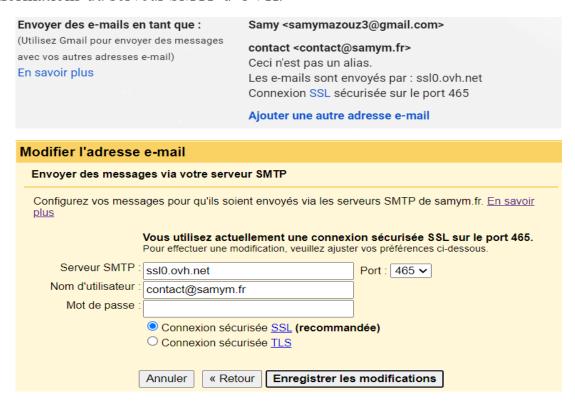
Ce qui nous permettra dans un second temps, de commander le certificat SSL gratuit d'OVH (Let's Encrypt)



## SMTP, POP 3 (Gmail)

Nous avons la possibilité de configurer le service de messagerie Gmail afin de pouvoir envoyer des mails en tant que par exemple : <a href="mailto:contact@samym.fr">contact@samym.fr</a> (ou n'importe quelle autre adresse mail OVH) et de possiblement contourner l'antispam de Gmail.

Il suffit de configurer les paramètres Gmail de son adresse mail en ajoutant les informations du serveur SMTP d'OVH.



Cela nous permettra dans un premier temps, d'envoyer des mails avec contact@samym.fr sur la messagerie Gmail.



Ensuite dans un second temps, nous allons configurer Gmail pour pouvoir consulter la messagerie d'autres comptes de messagerie, soit celle sur OVH en utilisant cette fois-ci le serveur POP d'OVH.



Nous pouvons dès à présent envoyer et recevoir des messages sur cette dernière depuis l'interface de Gmail, ce qui devrait empêcher l'anti-spam de Gmail