

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

Domaine	TTL	Type	Cible
<input type="checkbox"/> _autodiscover._tcp.savelifedata.com.	0	SRV	0 0 443 mailconfig.ovh.net.
<input type="checkbox"/> ftp.savelifedata.com.	0	CNAME	savelifedata.com.
<input type="checkbox"/> imap.savelifedata.com.	0	CNAME	ssl0.ovh.net.
<input type="checkbox"/> _imaps._tcp.savelifedata.com.	0	SRV	0 0 993 ssl0.ovh.net.

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)

^ [SPF] savelifedata.com n'autorise pas votre serveur 54.38.35.112 à utiliser contact@savelifedata.com

-3

Sender Policy Framework (SPF) est un système de validation d'e-mail conçu pour empêcher le spamming en détectant l'usurpation d'adresse e-mail, une vulnérabilité classique, en vérifiant les adresses IP de l'expéditeur.

Ce que nous avons retenu comme votre enregistrement SPF actuel est :

v=spf1 include:mx.ovh.com ~all

Cela devrait être changé en :

v=spf1 include:mx.ovh.com ip4:54.38.35.112 ~all

Le serveur de nom qui gère le domaine **savelifedata.com** est **dns104.ovh.net**.

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 :

Ajouter une entrée à la zone DNS Étape 1 sur 3

Sélectionnez un type de champ DNS :

Champs de pointage

A **AAAA** **NS** **CNAME** **DNAME**

Champs étendus

CAA **TXT** **NAPTR** **SRV** **LOC** **SSHFP** **TLSA**

Champs mails

MX **SPF** **DKIM** **DMARC**

Annuler **Suivant**

Ajouter une entrée à la zone DNS Étape 2 sur 3

* Les champs suivis d'un astérisque sont obligatoires.

Sous-domaine

TTL

Valeur *

Le champ TXT actuellement généré est le suivant :

IN TXT

Annuler **Précédent** **Suivant**

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:

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-----
MIICXQIBAAKBgQCn5tKqy017LfU80rjWp+uCz8bzz8+DH1ZGDMbjIXqq/fcbeVZa
GtV864yVLjp0rL2mxSiznbEejRpQts9dznIUn5ZLuxdkLExCMHNqC+1PAV8PHN
eA8r5+7U+4eW0NXMsjgedBAeej87P+1AKJV+UkOvMnipt17nm1tKyrVrJwIDAQAB
AoGBAIB3tHBL1EyKyN0In3rqXP9YI91KTKOm9xYKOL4d0dJv1J7T9r88PQo/SYY6/
vSXeew1lw39DubyKlpxu4bRg6MUV0CRn+Y8oCFVLCgtDhcdkXkP5dyjYEqnVgx6
drVsMmKo2x81NNQn/R+OcM7izLfOysM7DnZ5oskiK81MbGBAkEA4EmgnW2ce80i
NXq16g5dE1f4xc0KrNYtjMup/nXCCjOSWIdIOqt3m0CAYhIXVrQXPgK9WUQeGrW
tvhtIayPkWJBAMQ1BRUy5vXp+WDPI8vBdJmaTsysX4s852SG4+bD38Jv15Y1A7Z7
pju5rKsITWk1CSFT03IsuI535EGJ5nn6p0CQDHBZBMCuemQKidxquw+j6WcZV5
Q70n03XbCEjKQ85+z2Zkiz39NP0v7yV4j1a1kpVMB5GaGvBtrXekXwAcDTAKAm
6r1KXiFPb4wmNqRs0r9U5DVzBVgi7X9kAh1cIUfVohq4djlXtY9IU2kMcNih4Ii
GQc2e0ZUA9XDZf8X1NdFAkAnYNR2Umoahy1aZ6KK4XuB5mL5BE5NUHU14ESeth7v
BrcF1C4xV6Mcbmm/tcjhjjs0MZKo83MnbFutNe4+tfK1
-----END RSA PRIVATE KEY-----
```

[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

```
1653398178.savelifedata._domainkey.savelifedata.com. IN TXT (
    "v=DKIM1;t=s;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCn5tKqy017LfU80rjWp+uCz8bzz8+DH1ZGDMbjIXqq/fcbeVZaGtV864yVLjp0rL2mxSiznbEejRpQts9dznIUn5ZLuxdkLExCMHNqC+1PAV8PHNeA8r5+7U+4eW0NXMsjgedBAeej87P+1AKJV+UkOvMnipt17nm1tKyrVrJwIDAQAB"
)
```

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

v=DKIM1;k=rsa;t=s;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC4stHQC09KyHe4DYAKXFuJl3MafRX78LRR2LKfYK5jB/FhmOMY3XERYlhisA4A2b+eoPYs3QV5px1CKd+Rv/9+m6wZEODIJkgtY+oxDcD5VUfGeoZOVZxpJ6T23RjbEaeywl2JeLfEs0ILR43TVxiChLgswN+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=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC4stHQC9KyHe4D  
YAKXFuJl3MafRX78LRR2LKfYK5jB/FhmOMY3XERYlhisA4A2b+eoPYs3QV5px1CKd+Rv/9+m6w  
ZEODIJkgthY+oxDcD5VUfGeoZOVZxpJ6T23RjbEaeywI2JeLfEs0ILR43TVxiChLgswN+0DJqP  
ck3X61VwIDAQAB
```

This is a valid DKIM key record

Version

v= DKIM1

Key type

k= rsa

Flags

t= s

Public key

p= MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC4stHQC9KyHe4DYAKXFuJl3MafRX78LRR2LKfYK5jB/FhmOMY3XERYlhisA4A2b+eoPYs3QV5px1CKd+Rv/9+m6wZEODIJkgthY+oxDcD5VUfGeoZOVZxpJ6T23RjbEaeywI2JeLfEs0ILR43TVxiChLgswN+0DJqPck3X61VwIDAQAB

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 :

<input type="checkbox"/>	savelifedata.com.	0	TXT	"v=spf1 include:mx.ovh.com ip4:54.38.35.112 -all"	...
<input type="checkbox"/>	1653398016.savelifedata._domainkey.savelifedata.com.	0	TXT	"v=DKIM1;k=rsa;t=s;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC4stHQC9KyHe4DYAKXFuJl3MafRX78LRR2LKfYK5jB/FhmOMY3XERYlhisA4A2b+eoPYs3QV5px1CKd+Rv/9+m6wZEODIJkgthY+oxDcD5VUfGeoZOVZxpJ6T23RjbEaeywI2JeLfEs0ILR43TVxiChLgswN+0DJqPck3X61VwIDAQAB"	...
<input type="checkbox"/>	_dmarc.savelifedata.com.	0	TXT	"v=DMARC1; p=none; rua=mailto:contact@savelifedata.com"	...

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) :

mailgenius

TOOLS & SERVICES

Personalized ESP

Email Deliverability Audits

For personalized white-glove email deliverability audits or long-form consulting please email us at: consulting@mailgenius.com

58 of 100

[+ NEW TEST](#)

MailGenius Score

We've found 7 thing(s) you can do to avoid landing in the spam folder and increase security.

However, there are several other factors that go into deliverability such as domain reputation, list hygiene etc., which play a large role when inboxing. You can be authenticated and follow best practices, but if recipients mark your emails as spam, they'll be classified as spam.

Email from: contact@savelifedata.com 23/05/2022
Subject: test

Don't lose money to the Spam Folder

[Set Up A Free Call To Learn More](#)

Work with Email Deliverability Experts to solve your email issues.

7 THINGS TO FIX

SEVERITY	TEST	DESCRIPTION
Failing -18	Domain Blacklists	Your domain is listed on significant blacklists.
Failing -8	IP Blacklists	Your Mail Server IP address is listed on significant blacklists.
Failing -5	DMARC	Your DMARC authentication is not setup using best practices.
Failing -4	SPF	Your SPF record has errors.
Failing -4	DKIM	Your DKIM key has errors.

EMAIL PREVIEW

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

mailgenius

TOOLS & SERVICES

Personalized ESP

Email Deliverability Audits

For personalized white-glove email deliverability audits or long-form consulting please email us at: consulting@mailgenius.com

91 of 100

[+ NEW TEST](#)

MailGenius Score

We've found 4 thing(s) you can do to avoid landing in the spam folder and increase security.

However, there are several other factors that go into deliverability such as domain reputation, list hygiene etc., which play a large role when inboxing. You can be authenticated and follow best practices, but if recipients mark your emails as spam, they'll be classified as spam.

Email from: contact@savelifedata.com 27/05/2022
Subject: test 27/05/22

Don't lose money to the Spam Folder

[Set Up A Free Call To Learn More](#)

Work with Email Deliverability Experts to solve your email issues.

4 THINGS TO FIX

SEVERITY	TEST	DESCRIPTION
Failing -4	DKIM	Your DKIM key has errors.
Warning -3	DMARC	Your DMARC authentication is not setup using best practices.
Warning -1	List-Unsubscribe Header	Your email is missing the List-Unsubscribe header.
Warning -1	SpamAssassin	Your SpamAssassin score is approaching the spam threshold.
Passing	SPF	Your SPF record looks great!

EMAIL PREVIEW

SSL

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.

Configuration

Version PHP globale

5.6 



Certificat SSL

Non



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

Informations générales	Multisite	Modules en 1 clic	Statistiques et logs	FTP - SSH	Bases de données
Actions ▾					
Recherche... 🔍					
Domaine	Dossier racine	Logs séparés	Firewall	SSL	
savelifedata.com	www	Désactivé	Activé	Désactivé	⋮
wpcoerh.cluster029.hosting.ovh.net	www	Désactivé	Désactivé	Désactivé	⋮
www.savelifedata.com	www	Désactivé	Activé	Désactivé	⋮

Modifier un domaine

Étape 1 sur 2

Vous allez modifier le domaine suivant :

Nom du domaine

savelifedata.com

Dossier racine

./ www

Choisissez une option

☐ SSL ?

☐ Ip du pays ?

☒ Activer le firewall ?

☐ Logs séparés ?

Annuler

Suivant

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

Commander un certificat SSL

Étape 1 sur 2

☒ Certificat gratuit (Let's Encrypt)

☐ Import de votre certificat SSL



Si vous avez ajouté des hébergements multisites il y a moins de deux heures, il est possible qu'ils ne soient pas inclus dans votre certificat SSL.

Annuler

Suivant

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 : contact@samym.fr (ou n'importe quelle autre adresse mail OVH) et de possiblement contourner l'anti-spam de Gmail.

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

Envoyer des e-mails en tant que : (Utilisez Gmail pour envoyer des messages avec vos autres adresses e-mail) En savoir plus	Samy <samymazouz3@gmail.com> contact <contact@samym.fr> Ceci n'est pas un alias. Les e-mails sont envoyés par : ssl0.ovh.net Connexion SSL sécurisée sur le port 465 Ajouter une autre adresse e-mail
--	--

Modifier l'adresse e-mail

Envoyer des messages via votre serveur SMTP

Configurez vos messages pour qu'ils soient envoyés via les serveurs SMTP de samym.fr. [En savoir plus](#)

Vous utilisez actuellement une connexion sécurisée SSL sur le port 465.
Pour effectuer une modification, veuillez ajuster vos préférences ci-dessous.

Serveur SMTP : Port :

Nom d'utilisateur :

Mot de passe :

☒ Connexion sécurisée [SSL](#) (recommandée)
☐ Connexion sécurisée [TLS](#)

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

 **Gmail Confirmation - Envoyer des e-mails en tant que contact@samym.fr**

De **L'équipe Gmail**  Date **Lun 19:52**

Vous avez demandé l'ajout de l'adresse contact@samym.fr à votre compte Gmail.
Code de confirmation : 366569978

Avant de pouvoir envoyer des messages à partir de contact@samym.fr avec votre compte Gmail (samymazouz3@gmail.com), vous devez cliquer sur le lien ci-dessous pour confirmer votre demande :

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.

Modifier le compte de messagerie

Saisissez les paramètres de messagerie pour **contact@samym.fr**. [En savoir plus](#)

Adresse e-mail : **contact@samym.fr**

Nom d'utilisateur :

Mot de passe :

Serveur POP : Port : ▼

☒ Conserver une copie du message récupéré sur le serveur [En savoir plus](#)

☒ Vous devez toujours utiliser une connexion sécurisée (SSL) lorsque vous récupérez vos e-mails. [En savoir plus](#)

☐ Ajouter un libellé aux messages entrants : ▼

☒ Archiver les messages entrants (sans passer par la boîte de réception)

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