

# Ne plus passer dans les SPAMS : réglage du SPF

Pour éviter de tomber dans les spams, il est important de régler votre SPF sur le nom de domaine que vous utilisez pour envoyer vos emails.

Pour une explication du SPF, voici un lien intéressant.

"Le SPF (Sender Policy Framework) est un système de validation par courrier électronique pour empêcher les spammeurs d'envoyer des messages au nom de votre domaine. Avec le SPF, une organisation peut publier des serveurs de messagerie autorisés."

## 1- Informations pour remplir le SPF

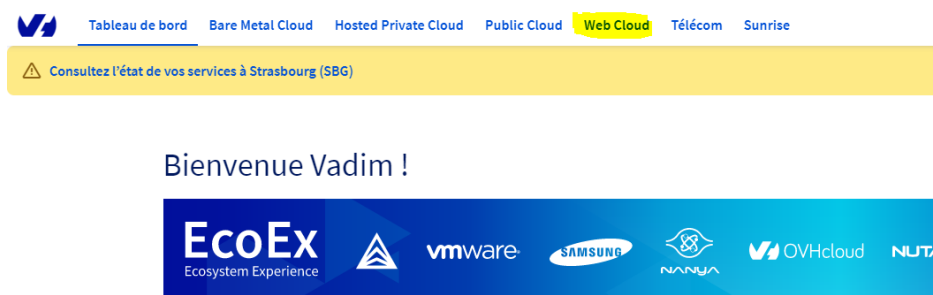
**Notre adresse d'envoi de mail : 35.181.201.72**

Utilisez cette adresse chez votre hébergeur pour prouver que l'outil Lab Event peut bien envoyer des mails en votre nom. Quand vous utilisez notre outil de messagerie intégrée, nous vous conseillons fortement de le faire.

## 2- Où remplir l'information

Nous vous donnons ici l'exemple d'OVH

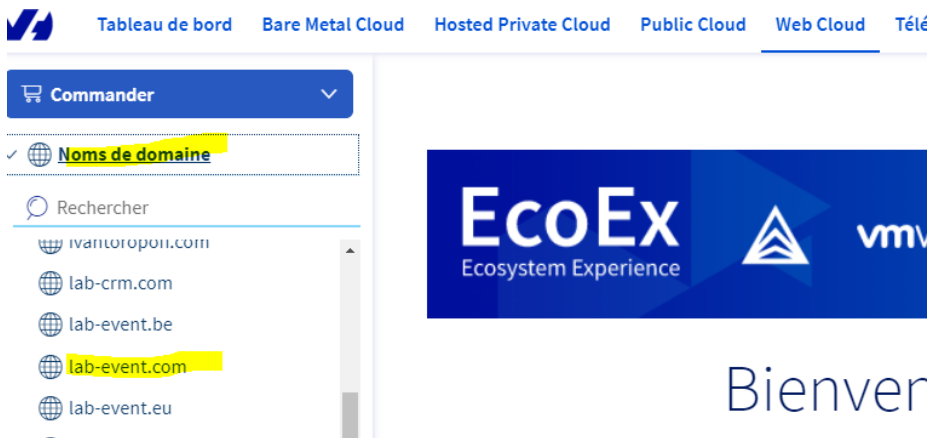
### 2-1 : Allez dans votre console : dans la partie WEB CLOUD



## 2-2 : Choisissez votre nom de domaine

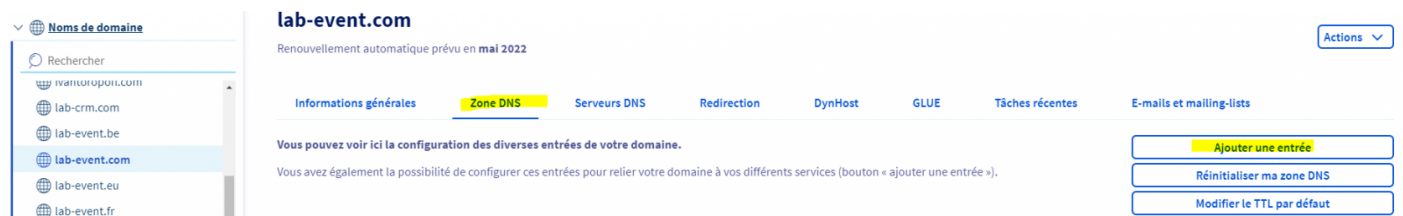
Allez sur NOM DE DOMAINE et sélectionnez votre nom de domaine

Ici nous utiliserons Lab Event mais évidemment, c'est le nom de domaine avec lequel vous envoyez des mails que vous devez sélectionner.



## 2-3 : Allez dans Zone DNS

Sur la partie Zone DNS, appuyez sur le bouton à droite "Ajouter une entrée"



Puis sélectionnez : SPIF dans la pop up qui s'ouvre

**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

## 2-4 : Rentrez les informations concernant le SPF

Sur les deux premières questions, faites OUI

Sur la troisième, faites NON

**Ajouter une entrée à la zone DNS** *Étape 2 sur 3*

Si votre domaine lab-event.com est configuré sur un serveur mutualisé OVH, le champ SPF de base à utiliser est simplement :

lab-event.com. IN TXT "v=spf1 include:mx.ovh.com ~all"

**Utiliser le SPF pour mutualisé OVH**

\* Les champs suivis d'un astérisque sont obligatoires.

Sous-domaine

TTL

Autoriser l'IP de lab-event.com à envoyer des emails ?  
☒ Oui ☐ Non

Autoriser les serveurs MX de lab-event.com à envoyer des emails ?  
☒ Oui ☐ Non

Autoriser tous les serveurs dont le nom se termine par lab-event.com à envoyer des emails ? (Cette option n'est pas recommandée)  
☐ Oui ☒ Non

Et ensuite (voir copie écran)

- IP : 35.181.201.72
- Oui, mais utiliser le safe mode

---

mx:

ptr:

ip4: **35.181.201.72**

ip6:

Est-ce que le courrier de lab-event.com provient originellement d'autres serveurs appartenant à d'autres domaines (ex.: votre FAI) ?

include:

Est-ce que les informations que vous avez indiquées décrivent tous les hôtes qui envoient du courrier de lab-event.com ?

☐ Oui, je suis sûr

☒ **Oui, mais utiliser le safe mode**

☐ Non

Le champ SPF actuellement généré est le suivant :

IN TXT "v=spf1 a mx ip4:54.36.251.33 ~all"

Annuler

Précédent

Suivant


Et ensuite il faut valider

Ajouter une entrée à la zone DNS

Étape 3 sur 3

Vous allez ajouter l'entrée suivante dans votre zone DNS :

Type de champ	SPF
Domaine	lab-event.com.
Cible	v=spf1 a mx ip4:54.36.251.33 ~all

 La modification sera immédiate dans la zone DNS, mais veuillez prendre en compte le temps de propagation (maximum 24h).

Annuler

Précédent

Valider

## 2-5 : Vérifiez que les informations concernant le SPF sont prises en compte

Cela peut prendre de 2h à 24h pour une remontée dans les DNS

Vous pourrez vérifier sur le site : <https://www.dmarcanalyzer.com/spf/checker/>

C'est fini, une fois cette manipulation faite, vos mails seront moins considéré comme des SPAMS.

La configuration du SPF est liée avec les réglages du DKIM et du DMARC. Si le problème persiste, il faudra regarder DKIM et DMARC.

---

Révision #16

Créé Thu, Oct 21, 2021 3:59 PM par Vadim

Mis à jour Wed, Feb 21, 2024 11:38 AM par Marine