
Mise en place DMARC

Introduction

La mise en place de DMARC va permettre de rajouter une couche de sécurité sur SPF ou DKIM par exemple pour SPF dans le cas ou le serveur smtp qui transfère le mail n'est pas un serveur autorisé quel comportement le serveur destinataire doit -il adopter ?

On pourra lui dire de ne réaliser aucune action mais juste envoyer un rapport comme quoi il y'a eu une tentative d'usurpation ou demander de mettre en quarantaine ou rejeter.

Mise en place

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	<input type="text" value="_dmarc"/>	<input type="text" value=".sadek.ovh."/>
TTL	<input type="text" value="Par défaut"/>	
Version *	DMARC1	
Règle pour le domaine *	<input type="text" value="none"/>	
Pourcentage des messages filtrés	<input type="text" value="100"/>	
URI de création de rapports globaux	<input type="text" value="mailto:asadek@sadek.ovh"/>	
Règle pour les sous-domaines	<input type="text" value="none"/>	
Mode d'alignement pour SPF	<input checked="" type="radio"/> Relaxed <input type="radio"/> Strict	

Le champ DMARC actuellement généré est le suivant :

```
_dmarc IN TXT "v=DMARC1;p=none;pct=100;rua=mailto:asadek@sadek.ovh"
```

Annuler

Précédent

Suivant

▪ aspf=s :

- "s" signifie *Strict*. Cela signifie que l'adresse de l'expéditeur dans l'en-tête "From" de l'e-mail doit correspondre exactement au nom de domaine de l'expéditeur dans l'enregistrement SPF pour que l'alignement SPF soit respecté. Idéal pour lutter contre le phishing, le spam, etc.
- "r" signifie *Relaxed* (mode par défaut). Cela signifie que l'alignement SPF est respecté tant que le domaine de l'expéditeur dans l'en-tête "From" de l'e-mail et l'adresse de l'expéditeur dans l'enregistrement SPF partagent le même domaine principal (ce qui permet d'autoriser les sous-domaines).

Résultat :

 _dmarc.sadek.ovh. 0 DMARC v=DMARC1;p=none;pct=100;rua=mailto:asadek@sadek.ovh;sp=none;spf=r; 

Le jour d'après le matin à 9h00

Je reçois ce mail

Report domain: sadek.ovh Submitter: google.com Report-ID: 192125745779191267



noreply-dmarc-support@google.com

Aujourd'hui, 09:24

Adel AS. Sadek 



Télécharger

Un rapport DMARC qui mentionne cela

```
<org_name>google.com</org_name>
<email>noreply-dmarc-support@google.com</email>
<extra_contact_info>https://support.google.com/a/answer/2466580</extra_contact_info>
<report_id>192125745779191267</report_id>
<date_range>
  <begin>1707177600</begin>
  <end>1707263999</end>
</date_range>
</report_metadata>
<policy_published>
  <domain>sadek.ovh</domain>
  <dkim>r</dkim>
  <spf>r</spf>
  <p>none</p>
  <sp>none</sp>
  <pct>100</pct>
  <np>none</np>
</policy_published>
<record>
  <row>
    <source_ip>137.74.196.172</source_ip>
    <count>1</count>
    <policy_evaluated>
      <disposition>none</disposition>
      <dkim>fail</dkim>
      <spf>pass</spf>
    </policy_evaluated>
  </row>
  <identifiers>
    <header_from>sadek.ovh</header_from>
  </identifiers>
  <auth_results>
    <spf>
      <domain>sadek.ovh</domain>
      <result>pass</result>
    </spf>
  </auth_results>
</record>
</feedback>
```

Il y'a tous les mails qui ont été envoyées récemment avec une adresse qui contient mon domaine

On y voit l'ip + le nombre de mails avec le test spf et dkim, je n'ai pas configuré DKIM c'est normal mais spf ça passe

On voit bien que ça nous permet de surveiller tous les mails envoyés avec des adresse qui comportent notre domaine.