

Hello Christophe,

Le domaine lovelace.network est bien configuré pour SPF et DKIM, mais pas pour DMARC.

Cela pourrait être une raison pour laquelle les messages de partage de Filelace arrivent encore en spam pour les adresses @gmail.

Info remontées par gmail :

Original Message

Message ID	<c1e2e291-3f91-d1a3-3ba4-082ee7a521c0@lovelace.network>
Created at:	Thu, Aug 27, 2026 at 7:17 PM (Delivered after 2 seconds)
From:	Lovelace Network <christophe@lovelace.network>
To:	laurent.beaubiat@gmail.com
Subject:	laurent.beaubiat@digitaltrust.fr a partagé un fichier avec vous sur Filelace
SPF:	PASS with IP 87.98.180.241 Learn more
DKIM:	'PASS' with domain lovelace.network Learn more
DMARC:	'FAIL' Learn more

Vérification :

SPF est ok, vérification avec NSLOOKUP :

```
nslookup -type=txt lovelace.network
```

réponse :

```
lovelace.network    text = "v=spf1 include:mx.ovh.com ~all"
```

DKIM est ok, on peut le lire dans les header SMTP :

notamment :

```
ARC-Authentication-Results:
i=1; mx.google.com;
dkim=pass
header.i=@lovelace.network
header.s=ovhmo5179379-selector1
header.b=SP75jgbg; spf=pass
(google.com: domain of
christophe@lovelace.network
designates 87.98.180.241 as
permitted sender)
smtp.mailfrom=christophe@lovelace.network
```

ou encore

```
DKIM-Signature: a=rsa-sha256;
bh=6xeJp+bX7ikrs5ghmd10ILAp
yqQkpqJ0k2h1HMRVZaU=;
c=relaxed/relaxed;
d=lovelace.network; h=From;
s=ovhmo5179379-selector1;
t=1787851075; v=1;
b=SP75jgbgrYSiD8+Y6PbsxoBbe
vEEhYeSJNQB8x5Y6synXC9VTPlb
8/v9Ptr4wdzx8uW+/Z9w
0n923B2gMSsY46m2f3Tm0AvJR7
L9igDiIUMyyEk17aoXXecpbEJrr
/zM0g8mA+Nsq6XFBvzLam
LNdj9dkrJAoB0y+zDCqsMMMa8vx
Ycuye6Jkc4HmnUNve06AAk3i+OE
Hag+Uui7SJU786kvLKkt4
1coXd2e6cG/aKXTeo6Uprg/fUmk
ym6X0KdyavXxCRSruJGb/r6fkTn
noyw20qTvFtYLet0vT960
YF2LVReX4KeWNDGgl1I1oACCFEB
4RJL+9NT7bjqGdSwLQ==
```

mais pour DMARC, il n'y a rien !

vérification avec NSLOOKUP :

```
nslookup -type=txt _dmarc.lovelace.network
```

Serveur : livebox.home

Address: 2a01:cb1d:182:9300:12e9:92ff:fecc:8370

*** livebox.home ne parvient pas à trouver _dmarc.lovelace.network : Non-existent domain

Il faudrait a minima avoir ceci (exemple du domaine digitaltrust.fr)

```
nslookup -type=txt _dmarc.digitaltrust.fr
```

Serveur : livebox.home

Address: 2a01:cb1d:182:9300:12e9:92ff:fecc:8370

Réponse ne faisant pas autorité :

```
_dmarc.digitaltrust.fr text = "v=DMARC1; p=none; pct=100; rua=mailto:dmarc@digitaltrust.fr; aspf=r"
```

Tu peux facilement configurer cet enregistrement DNS dans ta zone file lovelace.network, surtout avec l'interface d'OVH :

Tableau de bord

Bare Metal Cloud

Hosted Private Cloud

Public Cloud

Web Cloud

Télécom

Sunrise

Marketplace

Navigation classique

Navigation beta

Découvrez notre nouveau Manager Beta

Français

Laurent Beaublat

Commander

Noms de domaine

Opérations en cours

Mes noms de domaine

digitaltrust.fr

Sites internet

Hébergements

Managed hosting for WordPress

Web Cloud Databases

Video Center

Zimbra Mail

Email Pro

Emails

Rechercher

digitaltrust.fr

Microsoft

digitaltrust.fr

Roadmap & Changelog

Guides

Retour à la liste de services

Informations générales

Zone DNS

Serveurs DNS

Redirection

DynHost

Hosts

DS Records

Gestion des contacts

Une ou plusieurs actions ont été réalisées récemment dans la zone DNS. Pour tout ajout, modification, suppression ou réinitialisation, veuillez noter que le changement peut nécessiter un temps de propagation de 24 heures maximum.

Vous pouvez voir ici la configuration des diverses entrées de votre domaine.

Vous avez également la possibilité de configurer ces entrées pour relier votre domaine à vos différents services (bouton « Ajouter une entrée »).

Ajouter une entrée

Actions sur ma zone

Filter

	Sous-domaine	Type	Cible	TTL (en secondes)	
	_autodiscover_tcp	SRV	0 0 443 autodiscover.mail.ovh.net.	Par défaut	
	dmarc	DMARC	v=DMARC1; p=none; pct=100; rua=mailto:dmarc@digitaltrust.fr; aspf=r	Par défaut	

L'entrée DMARC permet de définir la politique d'authentification des e-mails de votre domaine, en spécifiant comment traiter les messages échouant les vérifications SPF et DKIM. Une fois la configuration validée, la politique DMARC sera appliquée aux e-mails envoyés depuis _dmarc.digitaltrust.fr.

Sous-domaine

_dmarc

TTL

Par défaut

Version

DMARC1

Règle pour le domaine - Champ obligatoire

None

Pourcentage des messages filtrés

100

URI de création de rapports globaux

mailto:dmarc@digitaltrust.fr

Règle pour les sous-domaines

Sélectionnez

Mode d'alignement pour SPF

R (Relaxed)

Aperçu de l'enregistrement

_dmarc.digitaltrust.fr. IN DMARC v=DMARC1; p=none; pct=100; rua=mailto:dmarc@digitaltrust.fr; aspf=r