Admins - Demande #4442

Mauvais records SSHFP

26/04/2020 14:34 - François Poulain

Statut:	Fermé	**Début:**	26/04/2020
Priorité:	Normale	**Echéance:**	
Assigné à:	François Poulain	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Novembre 2021	**Temps passé:**	0.00 heure
Difficulté:	2 Facile		

Description

J'ai régulièrement des blague du genre :

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
SHA256:Y4VJta0pCoebsbPvX4N/D6L6+gs/fEQpu25vrkR44sI.
Please contact your system administrator.
Update the SSHFP RR in DNS with the new host key to get rid of this message.
```

Ça fait pas très sérieux. :)

Historique

#1 - 26/04/2020 16:08 - Christian P. Momon

Depuis 2016, ni les clés, ni les déclarations SSHFP DNS n'ont été modifiées.
Du coup, pourquoi les valeurs du DNS ne sont plus bonnes ?
À quelle occasion ce message d'avertissement ?

#2 - 02/09/2020 22:14 - Quentin Gibeaux

- Assigné à mis à François Poulain

#3 - 02/09/2020 22:14 - Quentin Gibeaux

- Version cible changé de Backlog à Septembre 2020

#4 - 30/09/2020 21:32 - Quentin Gibeaux

- Version cible changé de Septembre 2020 à Octobre 2020

#5 - 28/10/2020 21:23 - Quentin Gibeaux

- Version cible changé de Octobre 2020 à Novembre 2020

#6 - 25/11/2020 21:20 - Quentin Gibeaux

- Version cible changé de Novembre 2020 à Décembre 2020

#7 - 27/11/2020 22:51 - François Poulain

Christian P. Momon a écrit :

> Depuis 2016, ni les clés, ni les déclarations SSHFP DNS n'ont été modifiées.
> Du coup, pourquoi les valeurs du DNS ne sont plus bonnes ?

Je ne sais plus mais je crois que les host keys ont changé entre temps.

> À quelle occasion ce message d'avertissement ?

Il faut ajouter -o VerifyHostKeyDNS=ask à ton client. Chez moi je l'avait en config globale. C'est un peu l'équivalent de DANE mais pour ssh. Sans recours à DNSSEC c'est d'un intérêt mineur. Mais avec l'arrivée de DoH/DoT ça peut avoir un intérêt certain (j'ai pas creusé).

#8 - 30/12/2020 22:07 - Quentin Gibeaux

- Version cible changé de Décembre 2020 à Janvier 2021

#9 - 27/01/2021 21:31 - Quentin Gibeaux

- Version cible changé de Janvier 2021 à Février 2021

#10 - 24/02/2021 21:43 - Quentin Gibeaux

- Version cible changé de Février 2021 à Mars 2021

#11 - 31/03/2021 21:54 - Quentin Gibeaux

- Version cible changé de Mars 2021 à Avril 2021

#12 - 28/04/2021 21:37 - Quentin Gibeaux

- Version cible changé de Avril 2021 à Mai 2021

#13 - 26/05/2021 21:39 - Quentin Gibeaux

- Version cible changé de Mai 2021 à Juin 2021

#14 - 30/06/2021 21:10 - Quentin Gibeaux

- Version cible changé de Juin 2021 à Été 2021

#15 - 01/09/2021 22:03 - Quentin Gibeaux

- Version cible changé de Été 2021 à Septembre 2021

#16 - 29/09/2021 22:05 - Quentin Gibeaux

- Version cible changé de Septembre 2021 à Octobre 2021

#17 - 27/10/2021 21:46 - Quentin Gibeaux

- Version cible changé de Octobre 2021 à Novembre 2021

#18 - 20/11/2021 15:13 - François Poulain

- Statut changé de Nouveau à Résolu

Non beh les records SSHFP sont OK. C'est ma conf SSH pour accéder à félicette qui était KO. Vérifié suite à la migration chez Hetzner.

#19 - 24/11/2021 21:18 - Quentin Gibeaux

- Statut changé de Résolu à Fermé