# Pourquoi l'ESA manipule-t-il le permfail de résultat d'authentification DKIM comme incident permanent ?

## Contenu

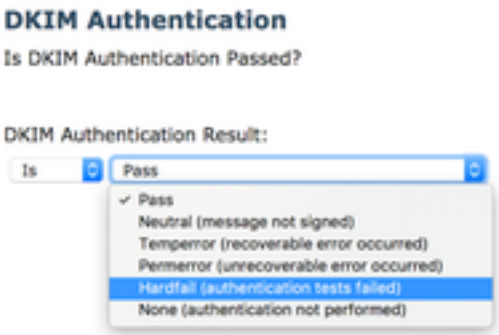


## Introduction

Ce document décrit des détails au sujet des résultats d'authentification DKIM manipulant sur l'appliance de sécurité du courrier électronique (ESA).

## Pourquoi l'ESA manipule-t-il le permfail de résultat d'authentification DKIM comme incident permanent ?

L'authentification de l'état DKIM de filtre de contenu ESA a plusieurs options disponibles pendant que l'image ci-dessous met en valeur.




Si le résultat d'authentification de l'état DKIM est configuré pour s'assortir sur l'incident permanent il inclura les messages qui révèlent comme permfail dans le fichier journal et le message de messagerie dépistant suivant les indications de l'exemple ci-dessous :

```
Message 815204 DKIM: permfail body hash did not verify [final] (d=sub.example.com s=selector1-sub-com i=@sub.example.com)
```

L'ESA considère le permfail comme incident permanent et met le résultat dans l'en-tête d'Authentification-résultats comme dkim=hardfail. Il y a une différence entre nommer de l'ESA des événements DKIM et nommer RFC6376. Dans les en-têtes d'Authentification-résultats (et le message dépistant) l'ESA doit afficher les chaînes RFC6376 appropriées, alors que le filtre satisfait utilise différents noms d'événement.

Le mappage d'événement pour l'incident permanent de filtre de contenu ESA de == RFC6376.PERMFAIL

La majorité de pannes de vérification sont due aux pannes de vérification d'informations parasites de signature et de corps du message. Les erreurs de vérification d'informations parasites de corps indiquent que le corps du message n'est pas conforme à la valeur d'informations parasites (condensé) dans la signature. Les erreurs de vérification de signature indiquent que la valeur de signature ne vérifie pas correctement les champs d'en-tête signés (signature y compris elle-même) sur le message. Il y a plusieurs causes pour ces deux erreurs : le message a pu avoir été modifié (peut-être par une liste de diffusion ou un expéditeur) en transit ; la signature ou les valeurs de hachage a pu avoir été calculée ou appliquée inexactement par le signataire ; la valeur principale publique fausse a pu avoir été éditée dans des DN ; ou le message a pu avoir été charrié par une entité pas en possession de la clé privée requise pour calculer une signature correcte. Il est très difficile de distinguer ces causes par l'analyse du message, bien que l'adresse IP d'origine puisse fournir quelques médecines légales utiles dans le cas de la mystification. Cependant, parce que des raisons d'intimité nous n'avons pas accès aux messages eux-mêmes, ainsi une telle analyse n'est pas possible. Il y a un certain nombre de messages dont les signatures ne vérifient pas pour assurer d'autres raisons, souvent en raison des erreurs facilement évitées de configuration dans les enregistrements de clé publique (sélecteur) édités dans des DN. Pour plus de détails veuillez se rapportent au lien ci-dessous.

## Informations connexes

- Erreurs communes entraînant des pannes de vérification DKIM