Configurer le remplacement de clé DKIM sur ESA sans temps d'arrêt

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Créer une nouvelle clé de signature DKIM](#)

[Générer un nouveau profil de signature DKIM](#)

[Publier l'enregistrement DNS sur DNS](#)

[Supprimer l'ancien profil de signature et l'utilisateur Espace réservé du nouveau profil de signature](#)

[Tester le flux de messages pour confirmer les réussites DKIM](#)

Introduction

Ce document décrit comment remplacer la clé de signature DKIM existante sur une clé publique ESA et DKIM dans DNS sans temps d'arrêt.

Conditions préalables

1. Accès à l'appliance de sécurisation de la messagerie (ESA).
2. Accès au DNS pour ajouter/supprimer des enregistrements TXT.
3. L'ESA doit déjà signer des messages avec un profil DKIM.

Créer une nouvelle clé de signature DKIM

Vous devez d'abord créer une nouvelle clé de signature DKIM sur l'ESA :

1. Accédez à Politiques de messagerie > Clés de signature et sélectionnez Ajouter une clé.
2. Nommez la clé DKIM et générez une nouvelle clé privée ou collez-en une existante.

> Remarque : Dans la plupart des cas, il est recommandé de choisir une taille de clé privée de 2 048 bits.

3. Validez les modifications.

> Remarque : Cette modification n'affecte pas la signature DKIM ni le flux de messagerie. Nous ajoutons simplement une clé de signature DKIM et ne l'appliquons pas encore à un profil de signature DKIM.

Générer un nouveau profil de signature DKIM

Ensuite, assurez-vous de créer un nouveau profil de signature DKIM, de générer un enregistrement DNS DKIM à partir de ce profil de signature DKIM et de publier cet enregistrement dans DNS :

1. Accédez à Politiques de messagerie > Profils de signature et sélectionnez Ajouter un profil.
2. Attribuez un nom descriptif au profil dans le champ Nom du profil.
3. Entrez votre domaine dans le champ Domain Name.
4. Entrez une nouvelle chaîne de sélection dans le champ Sélecteur.

✎ Remarque : Le sélecteur est une chaîne arbitraire utilisée pour autoriser plusieurs enregistrements DNS DKIM pour un domaine donné. Nous allons utiliser le sélecteur pour autoriser plus d'un enregistrement DNS DKIM dans DNS pour votre domaine. Il est important d'utiliser un nouveau sélecteur différent du profil de signature DKIM existant.

---

5. Sélectionnez la clé de signature DKIM créée dans la section précédente dans le champ Clé de signature.
6. En bas du profil de signature, ajoutez un nouvel utilisateur. Cet utilisateur doit être une adresse e-mail d'espace réservé inutilisée.

⚠ Mise en garde : Il est important d'ajouter une adresse e-mail inutilisée en tant qu'utilisateur pour ce profil de signature. Sinon, ce profil pourrait signer des messages sortants avant la publication de l'enregistrement DKIM TXT, ce qui entraînerait l'échec de la vérification DKIM. L'ajout d'une adresse e-mail inutilisée en tant qu'utilisateur garantit que ce profil de signature ne signe aucun message sortant.

---

7. sélectionnez Envoyer.

Publier l'enregistrement DNS sur DNS

1. À partir d'ici, sélectionnez Generate dans la colonne DNS Text Record pour le profil de signature que vous venez de créer et copiez l'enregistrement DNS qui est généré. Il doit ressembler à :

```
selector2._domainkey.example.com. IN TXT "v=DKIM1; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAw
```

2. Validez les modifications.
3. Soumettez l'enregistrement DKIM DNS TXT à DNS à l'étape 2.
4. Patientez jusqu'à ce que l'enregistrement DNS TXT DKIM ait été entièrement propagé.

Supprimer l'ancien profil de signature et l'utilisateur Espace

réservé du nouveau profil de signature

Une fois que l'enregistrement DKIM TXT a été envoyé au DNS et que vous avez vérifié qu'il a été propagé, l'étape suivante consiste à supprimer l'ancien profil de signature et à supprimer l'utilisateur de l'espace réservé du nouveau profil de signature :

 Remarque : Il est vivement recommandé de sauvegarder le fichier de configuration ESA avant de procéder à ces étapes. En effet, si vous supprimez l'ancien profil de signature DKIM et que vous devez revenir à la configuration précédente, vous pouvez facilement charger le fichier de configuration sauvegardé.

---

1. Naviguez dans Politiques de messagerie > Profils de signature, sélectionnez l'ancien profil de signature DKIM et sélectionnez Supprimer.
2. Accédez au nouveau profil de signature DKIM, sélectionnez l'utilisateur de l'espace réservé actuel et sélectionnez Supprimer.
3. sélectionnez Envoyer.
4. Dans la colonne Test Profile, sélectionnez Test pour le nouveau profil de signature DKIM. Si le test réussit, passez à l'étape suivante. Si ce n'est pas le cas, vérifiez que l'enregistrement DNS TXT DKIM a été entièrement propagé.
5. Validez les modifications apportées.

Tester le flux de messages pour confirmer les réussites DKIM

À ce stade, vous avez terminé la configuration de DKIM. Cependant, vous devez tester la signature DKIM pour vous assurer qu'elle signe vos messages sortants comme prévu et qu'elle réussit la vérification DKIM :

1. Envoyez un message via l'ESA en vous assurant que DKIM est signé par l'ESA et que DKIM est vérifié par un autre hôte.
2. Une fois le message reçu à l'autre extrémité, vérifiez les en-têtes du message pour l'en-tête Authentication-Results. Recherchez la section DKIM de l'en-tête pour vérifier si elle a réussi ou non la vérification DKIM. L'en-tête doit ressembler à
   <#root>

   ```
   Authentication-Results: mx1.example.net; spf=SoftFail smtp.mailfrom=user1@example.net;
   dkim=pass
    header.i=none; dmarc=fail (p=none dis=none) d=example.net
   ```

3. Recherchez l'en-tête DKIM-Signature et vérifiez que le sélecteur et le domaine corrects sont utilisés :

   <#root>

   ```
   DKIM-Signature: a=rsa-sha256;
   d=example.net
   ```

```
;
s=selector2

;
   c=simple; q=dns/txt; i=@example.net;
   t=1117574938; x=1118006938;
   h=from:to:subject:date;
   bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
   b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
            VoG4ZHRNiYzR
```

4. Une fois que vous êtes convaincu que DKIM fonctionne comme prévu, attendez au moins une semaine avant de supprimer l'ancien enregistrement DKIM TXT. Cela permet de s'assurer que tous les messages signés par l'ancienne clé DKIM ont été traités.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.