

Comment est-ce que je le recherche et visualiser la messagerie ouvre une session l'ESA ?

TAC

ID de document : 118552

Mis à jour : Oct. 10, 2014

Contribué par des ingénieurs TAC Cisco.



[PDF de téléchargement](#)



[Copie](#)

[Commentaires](#)

[Produits connexes](#)

- [Appliance de sécurité du courrier électronique de Cisco](#)

Contenu

[Introduction](#)

[Comment est-ce que je le recherche et visualiser la messagerie ouvre une session l'ESA ?](#)

[Cisco relatif prennent en charge des discussions de la Communauté](#)

Introduction

Ce document décrit comment rechercher les entrées de journal qui affichent comment l'ESA (appliance de sécurité du courrier électronique) a traité un message.

Comment est-ce que je le recherche et visualiser la messagerie ouvre une session l'ESA ?

Vous pouvez rechercher les logs pour recueillir plus d'informations au sujet de, à, *sujet des* emails provenant cette adresse IP que vous êtes intéressé dedans.

Le nom du log est des *mail_logs*. Vous pouvez voir ceci dans l'**administration système > les abonnements > les mail_logs** de log.

Il y a plusieurs manières d'accéder à ces logs.

1. Par l'intermédiaire du navigateur Web. Allez à l'**administration système > à l'abonnement de**

log. Pour les mail_logs, cliquez sur en fonction le lien de FTP à la droite des mail_logs. S'il te donne une erreur, allez au **réseau > à l'interface IP**, sélectionnent l'interface que vous normalement accès à l'ESA en fonction et activez le service FTP/port 21.

2. De la ligne de commande : Utilisant un client de ssh comme le mastic, connectez-vous le CLI de l'appliance ESA par l'intermédiaire du port 22/ssh. De la ligne de commande, **grep** d'utilisation pour rechercher l'IP. Vous devrez entrer dans # associé aux mail_logs de vos appareils, puis écrivez le modèle pour rechercher, IE. 192.168.1.1 ou joe@example.com. Pour les trois prochaines questions, appuyez sur écrivent et gardent les par défaut. La recherche pourrait prendre un bit d'heure de se terminer. Une fois que la sortie revient, vous pouvez rechercher l'ICID ou le MID.

```
grep "ICID 123456" mail_logs
```

Une fois que la sortie revient, vous pouvez rechercher le MID

```
grep "MID 78901234" mail_logs
```

Vous devriez pouvoir voir *de*, *à*, *sujet du* MID. Vous devriez voir l'adresse IP et le groupe d'expéditeur de CHAPEAU de l'ICID.

3. Une autre option est au FTP les mail_logs à un ordinateur local (appareil de bureau) et emploie votre propres fichier/éditeur de texte pour rechercher les adresses IP.

Ce document était-il utile ? [Oui aucun](#)

Merci de votre feedback.

[Ouvrez une valise de support](#) (exige un [contrat de service Cisco](#).)

Cisco relatif prennent en charge des discussions de la Communauté

[Cisco prennent en charge la Communauté](#) est un forum pour que vous posiez et pour répondez à des questions, des suggestions de partage, et collabore avec vos pairs.

Référez-vous au [Conventions relatives aux conseils techniques Cisco](#) pour les informations sur des conventions utilisées dans ce document.

Mis à jour : Oct. 10, 2014

ID de document : 118552