Hoe zoek ik de maillogs op de ESA?

Document-id: 118552

Bijgewerkt: 10 okt. 2014

Bijgedragen door Cisco TAC-engineers.

Verwante producten

- Cisco e-mail security applicatie

Inhoud

Inleiding

Dit document beschrijft hoe u naar logitems wilt zoeken die laten zien hoe het ESR (E-mail security applicatie) een bericht heeft verwerkt.

Hoe zoek ik de maillogs op de ESA?

U kunt de logbestanden doorzoeken om meer informatie te verzamelen over de *Van, To, Onderwerp* van de e-mails afkomstig van dit IP-adres waar u in geïnteresseerd bent.

De naam van het logbestand is *mail_logs*. U kunt dit zien in het **systeembeheer > Subscripties voor logbestanden > mail_logs.**

Er zijn verschillende manieren om toegang te krijgen tot deze logs.

1. Via de webbrowser. Ga naar **systeembeheer > Log abonnement**.Klik op de ftp link rechts van mail_logs voor de mail_logs.Als u een fout hebt gemaakt, gaat u naar **Network > IP interface**, selecteert u de interface waartoe u normaal toegang hebt tot het ESA ingeschakeld en zet u de FTP/poort 21-service aan.

2. Van de opdrachtregel: Wanneer u een ssh-client als Putty gebruikt, logt u via poort 22/ssh in op de CLI van het ESA-apparaat.Gebruik **grep** om naar de IP te zoeken vanuit de opdrachtregel.U dient het # dat aan de mail_logs van uw apparaat is gekoppeld in te voeren en vervolgens het patroon naar zoekactie in te voeren, dat wil zeggen. 192.168.1.1 of joe@example.com.Voor de volgende drie vragen, druk op om de standaardinstellingen in te voeren en te houden.De zoektocht kan een beetje tijd in beslag nemen. Als de uitvoer terugkomt, kunt u de ICID of de MID doorzoeken.
   ```
   grep "ICID 123456" mail_logs
   ```
   Zodra de uitvoer terugkomt, kunt u naar de MID zoeken
   ```
   grep "MID 78901234" mail_logs
   ```
   U dient de MID *te* kunnen zien *Van, To*. U dient het IP-adres en de HAT Sender-groep van het ICID te zien.
3. Een andere optie is om de mail_logs aan een lokale machine (Desktop) aan te passen en uw eigen bestand/teksteditor te gebruiken om naar de IP-adressen te zoeken.

Gerelateerde Cisco Support Community-discussies

De Cisco Support Community is een forum waar u vragen kunt stellen en beantwoorden, suggesties kunt delen en met uw collega's kunt samenwerken.

Raadpleeg Cisco Technical Tips Convention voor informatie over conventies die in dit document gebruikt worden.

Bijgewerkt: 10 okt. 2014
Document-id: 118552