Come posso cercare e visualizzare i log di posta sull'ESA?

Sommario

[Introduzione](#)
[Come posso cercare e visualizzare i log di posta sull'ESA?](#)

Introduzione

In questo documento viene descritto come cercare le voci del log che mostrano come l'ESA (Email Security Appliance) ha elaborato un messaggio.

Come posso cercare e visualizzare i log di posta sull'ESA?

Puoi cercare nei log per raccogliere più informazioni sui *Da, A e Soggetto* delle e-mail provenienti da questo indirizzo IP che ti interessa.

Il nome del registro è *mail_logs*. È possibile visualizzare questa informazione in **Amministrazione di sistema > Sottoscrizioni log > mail_logs.**

Èpossibile accedere a questi registri in diversi modi.

1. Tramite il browser Web. Selezionare **Amministrazione sistema > Sottoscrizione log**.Per mail_logs, fare clic sul collegamento ftp a destra di mail_logs.In caso di errore, selezionare **Network > IP interface** (Rete > interfaccia IP), selezionare l'interfaccia a cui si accede normalmente all'ESA e attivare il servizio FTP/porta 21.
2. Dalla riga di comando: Usare un client ssh come Putty per accedere alla CLI dell'appliance ESA tramite la porta 22/ssh.Dalla riga di comando, utilizzare **grep** per cercare l'indirizzo IP.Immettere il numero associato ai log di posta dell'accessorio, quindi specificare il pattern da ricercare. 192.168.1.1 o joe@example.com.Per le tre domande successive, premere Invio e mantenere le impostazioni predefinite.Il completamento della ricerca potrebbe richiedere alcuni minuti. Una volta restituito l'output, è possibile eseguire la ricerca sia nell'ICID che nel MID.
   ```
   grep "ICID 123456" mail_logs
   ```
   Una volta restituito l'output, è possibile cercare il MID
   ```
   grep "MID 78901234" mail_logs
   ```
   Dovrebbe essere possibile visualizzare i campi *Da, A e Oggetto* dal MID. Dovrebbe essere visualizzato l'indirizzo IP e il gruppo di mittenti HAT dall'ICID.
3. In alternativa, è possibile eseguire il ftp dei log di posta su un computer locale (Desktop) e utilizzare il proprio editor di file/testo per cercare gli indirizzi IP.