Configurazione della voce di log CEF e delle intestazioni CEF in ESA

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Configurazione](#)
[Voce di log CEF](#)
[Aggiungere il filtro dei contenuti in arrivo/in uscita](#)
[Aggiungi voce di registro CEF nella sottoscrizione del registro eventi consolidato](#)
[Intestazioni CEF](#)
[Aggiungere le intestazioni CEF al log:](#)
[Aggiungi voce di registro CEF nella sottoscrizione del registro eventi consolidato](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritta la configurazione delle voci e delle intestazioni del log CEF (Common Event Format) per Cisco Secure Email Gateway (SEG).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Email Gateway / Email Security Appliance (SEG / ESA)
- Filtri dei contenuti
- Registra informazioni di sottoscrizione

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Email Security Appliance versione 14.3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

I registri eventi consolidati riepilogano ogni evento messaggio in un'unica riga di registro. Utilizzare questo tipo di log per ridurre il numero di byte di dati (informazioni di log) inviati a un fornitore o a un'applicazione SIEM (Security Information and Event Management) per l'analisi. I log sono nel formato di log messaggio CEF ampiamente utilizzato dalla maggior parte dei fornitori SIEM.

Le voci di log CEF e le intestazioni CEF vengono aggiunte per fornire informazioni aggiuntive per tenere traccia e organizzare gli eventi di posta.

Configurazione

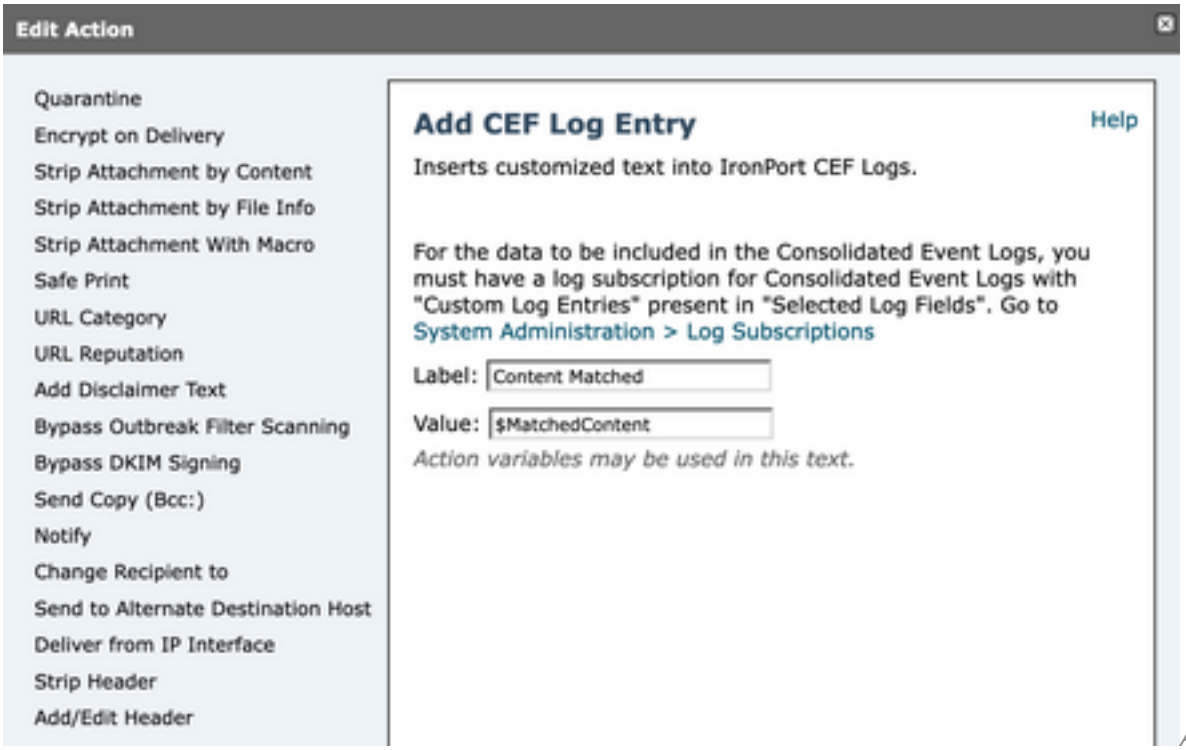
Voce di log CEF

Aggiungere il filtro dei contenuti in arrivo/in uscita

Innanzitutto, creare il filtro contenuti sull'ESA:

1. Vai a **Mail Policies > Incoming/Outgoing content filters**
2. Fare clic su **Add Filter**
3. Denominazione filtro
4. Aggiungi condizione desiderata
5. Fare clic su **Add Action**
6. Seleziona **Add CEF Log Entry**
7. Assegnare un nome all'etichetta e utilizzare **Action Variables** per la casella valore
8. **Submit and Commit**

Esempio di documentazione utilizzato **$MatchedContent** Variabile di azione, come illustrato nell'immagine:

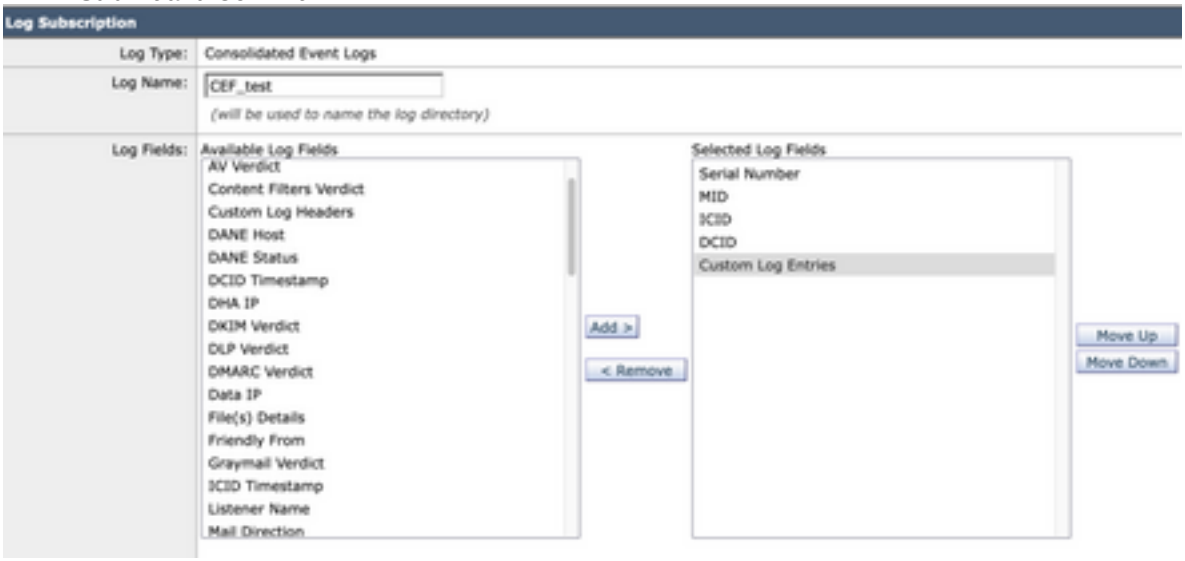


Azione voce di log CEF nei filtri contenuti

Aggiungi voce di registro CEF nella sottoscrizione del registro eventi consolidato

Creare o modificare la sottoscrizione del log eventi consolidato per aggiungere la voce di log CEF creata in precedenza:

1. Vai a **System Administration > Log Subscriptions**
2. Aggiungere o selezionare i registri eventi consolidati
3. Seleziona **Custom Log Entries** e fare clic su **Add**
4. **Submit and Commit**



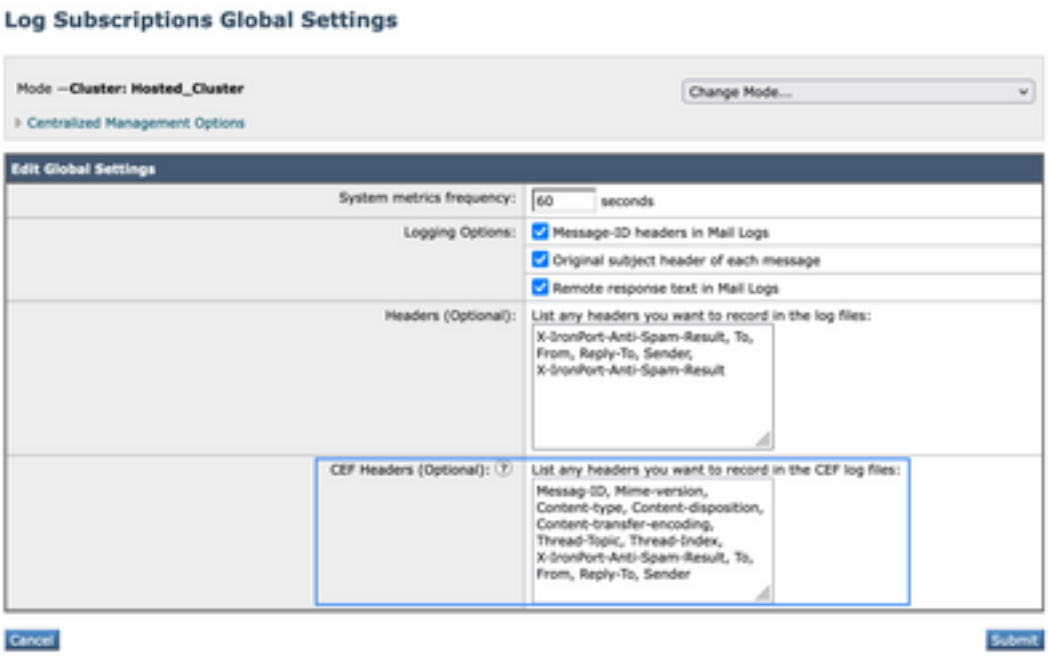
Voci di log personalizzate nella sottoscrizione di log CEF

Intestazioni CEF

Aggiungere le intestazioni CEF al log:

Aggiungere innanzitutto le intestazioni CEF nel SEC

1. Vai a **System Administration > Logs Subscription**
2. Fare clic su **Edit Settings** in Impostazioni globali
3. In Intestazioni CEF elencare le intestazioni da registrare
4. **Submit and Commit**

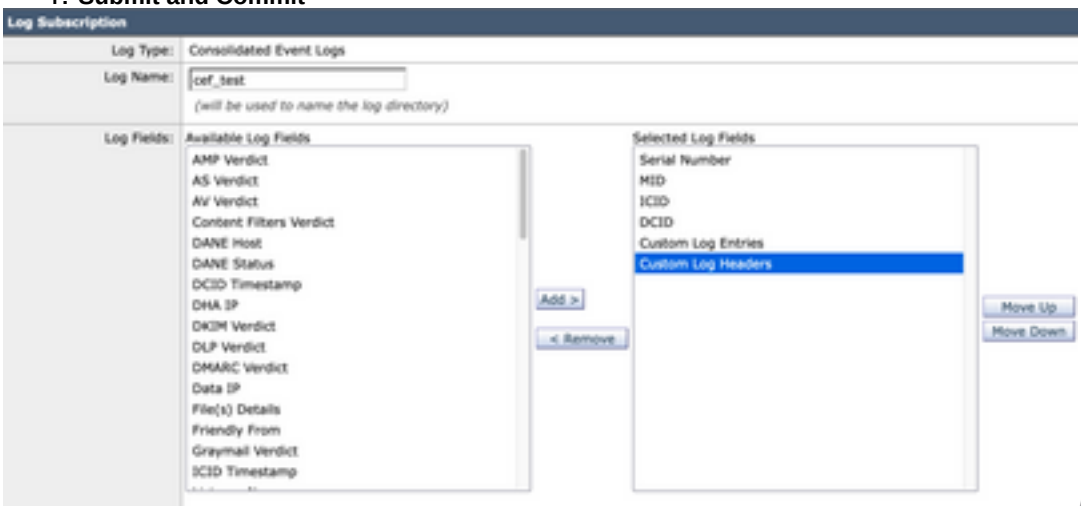


Configurazione intestazioni CEF

Aggiungi voce di registro CEF nella sottoscrizione del registro eventi consolidato

Creare o modificare la sottoscrizione del registro eventi consolidato per aggiungere le intestazioni CEF registrate in precedenza:

1. Vai a **System Administration > Logs Subscription**
2. Aggiungere o selezionare i registri eventi consolidati
3. Seleziona **Custom Log Entries** e fare clic su **Add**
4. **Submit and Commit**



Intestazioni di log CEF nella sottoscrizione di log CEF

Informazioni correlate

- Guida per l'utente finale ESA 14.3
- Note release ESA 14.3
- Supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).