

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

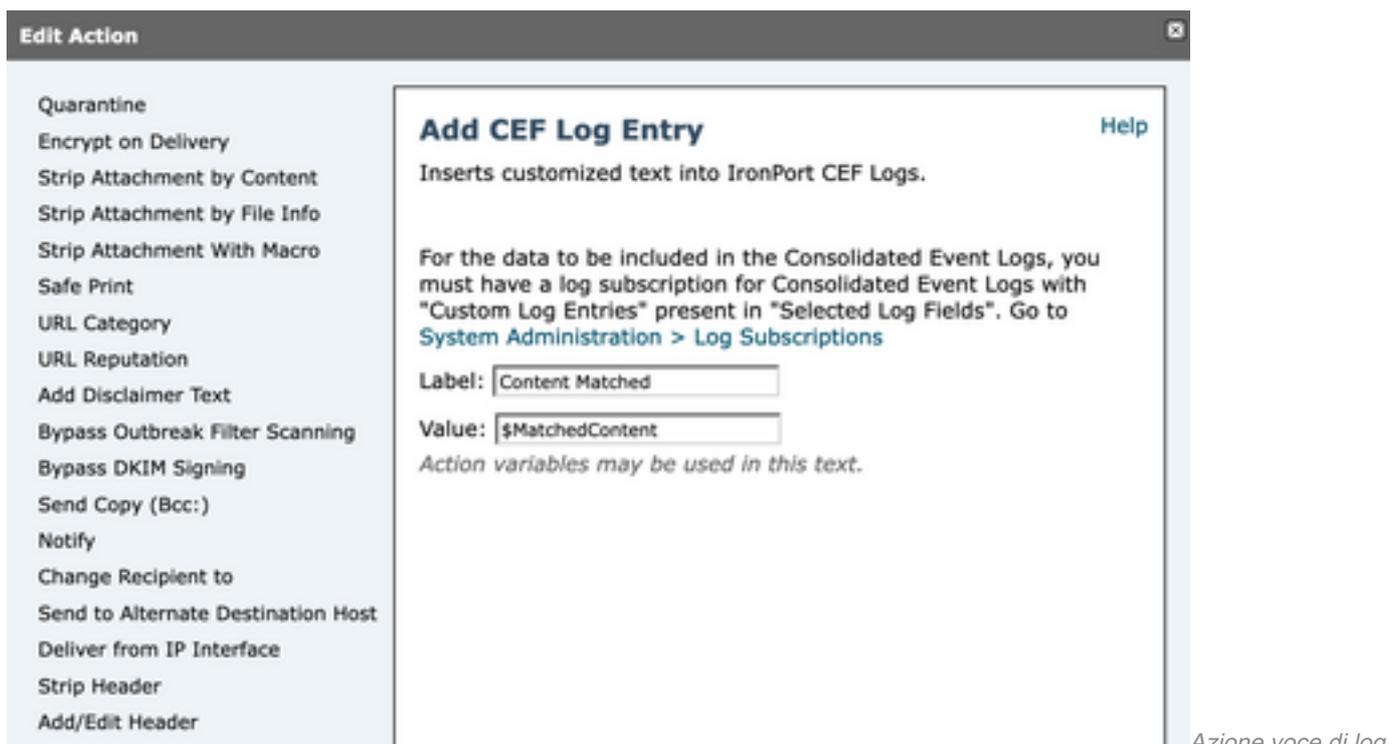
Voce di log CEF

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:



The screenshot shows the 'Edit Action' dialog box with a sidebar of actions. The 'Add CEF Log Entry' action is selected and detailed in the main pane. The sidebar lists various actions such as Quarantine, Encrypt on Delivery, Strip Attachment by Content, Strip Attachment by File Info, Strip Attachment With Macro, Safe Print, URL Category, URL Reputation, Add Disclaimer Text, Bypass Outbreak Filter Scanning, Bypass DKIM Signing, Send Copy (Bcc:), Notify, Change Recipient to, Send to Alternate Destination Host, Deliver from IP Interface, Strip Header, and Add/Edit Header. The 'Add CEF Log Entry' action is highlighted in blue. The main pane for this action includes a 'Help' link, a description: 'Inserts customized text into IronPort CEF Logs.', and instructions: 'For the data to be included in the Consolidated Event Logs, you must have a log subscription for Consolidated Event Logs with "Custom Log Entries" present in "Selected Log Fields". Go to [System Administration > Log Subscriptions](#)'. Below this, there are two input fields: 'Label:' with the value 'Content Matched' and 'Value:' with the value '\$MatchedContent'. A note states: 'Action variables may be used in this text.'

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**

Log Subscription

Log Type: Consolidated Event Logs

Log Name: CEF_test
(will be used to name the log directory)

Log Fields:

Available Log Fields	Selected Log Fields
AV Verdict	Serial Number
Content Filters Verdict	MID
Custom Log Headers	ICID
DANE Host	DCID
DANE Status	Custom Log Entries
DCID Timestamp	
DHA IP	
DKIM Verdict	
DLP Verdict	
DMARC Verdict	
Data IP	
File(s) Details	
Friendly From	
Graymail Verdict	
ICID Timestamp	
Listener Name	
Mail Direction	

Buttons: Add >, < Remove, Move Up, Move Down

personalizzate nella sottoscrizione di log CEF

Voci di log

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**

Log Subscriptions Global Settings

Mode --Cluster: Hosted_Cluster Change Mode...

Centralized Management Options

Edit Global Settings

System metrics frequency:	60 seconds
Logging Options:	<input checked="" type="checkbox"/> Message-ID headers in Mail Logs <input checked="" type="checkbox"/> Original subject header of each message <input checked="" type="checkbox"/> Remote response text in Mail Logs
Headers (Optional):	List any headers you want to record in the log files: X-IronPort-Anti-Spam-Result, To, From, Reply-To, Sender, X-IronPort-Anti-Spam-Result
CEF Headers (Optional):	List any headers you want to record in the CEF log files: Message-ID, Mime-version, Content-type, Content-disposition, Content-transfer-encoding, Thread-Topic, Thread-Index, X-IronPort-Anti-Spam-Result, To, From, Reply-To, Sender

Cancel Submit

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**

Log Subscription

Log Type: Consolidated Event Logs

Log Name:
(will be used to name the log directory)

Log Fields:

Available Log Fields	Selected Log Fields
AMP Verdict AS Verdict AV Verdict Content Filters Verdict DANE Host DANE Status DCID Timestamp DHA IP DKIM Verdict DLP Verdict DMARC Verdict Data IP File(s) Details Friendly From Graymail Verdict ICID Timestamp	Serial Number MED ICID DCID Custom Log Entries Custom Log Headers
Add > < Remove	Move Up Move Down

sottoscrizione di log CEF

Intestazioni di log CEF nella

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).