تكوين إدخال سجل CEF ورؤوس CEF في ESA

المحتويات

المقدمة

يصف هذا المستند تكوين إدخال سجل تنسيق الحدث المشترك (CEF) ورؤوس عبارة البريد الإلكتروني الآمنة (SEG) من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بمعرفة الموضوعات التالية:

- عبارة البريد الإلكتروني الآمنة من Cisco / جهاز أمان البريد الإلكتروني (SEG / ESA)
- معرفة عوامل تصفية المحتوى
- تسجيل معرفة الاشتراك

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- جهاز Email Security Appliance، الإصدار 14.3

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

توجز "سجلات الأحداث المدمجة" كل حدث رسالة في سطر سجل واحد. أستخدم نوع السجل هذا لتقليل عدد وحدات البايت للبيانات (معلومات السجل) المرسلة إلى مورد "معلومات الأمان وإدارة الأحداث" (SIEM) أو التطبيق للتحليل. توجد السجلات بتنسيق رسائل سجل CEF الذي يتم إستخدامه بشكل واسع من قبل معظم موردي SIEM.

تتم إضافة إدخال سجل CEF ورؤوس CEF لتوفير معلومات إضافية لتعقب أحداث البريد وتنظيمها.

التكوين

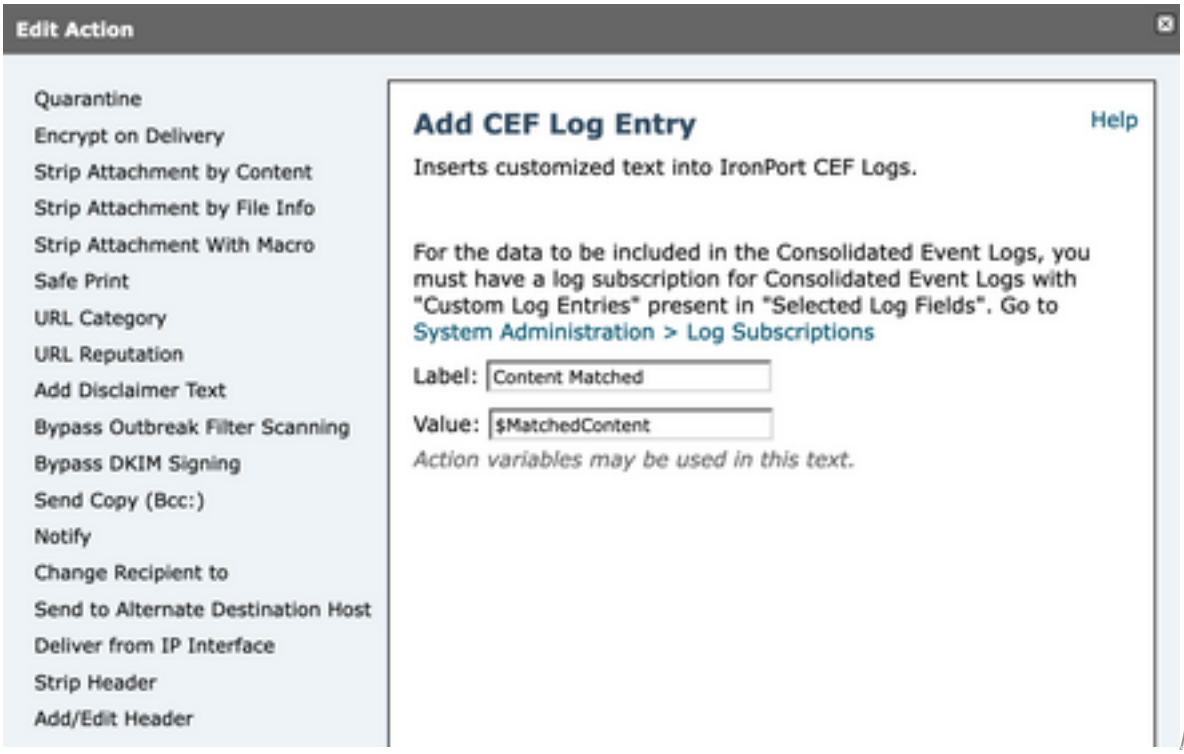
إدخال سجل CEF

إضافة عامل تصفية المحتوى الوارد/الصادر

أولا، قم بإنشاء مرشح المحتوى على ESA:

1. الانتقال إلى **Mail Policies > Incoming/Outgoing content filters**
2. انقر في **Add Filter**
3. تسمية عامل التصفية
4. إضافة شرط مرغوب
5. انقر في **Add Action**
6. تحديد **Add CEF Log Entry**
7. قم بتسمية التسمية واستخدامها **Action Variables** لمربع القيمة
8. **Submit and Commit**

مثال التوثيق هذا الذي نستخدمه **$MatchedContent** متغير الإجراء، كما هو موضح في الصورة:



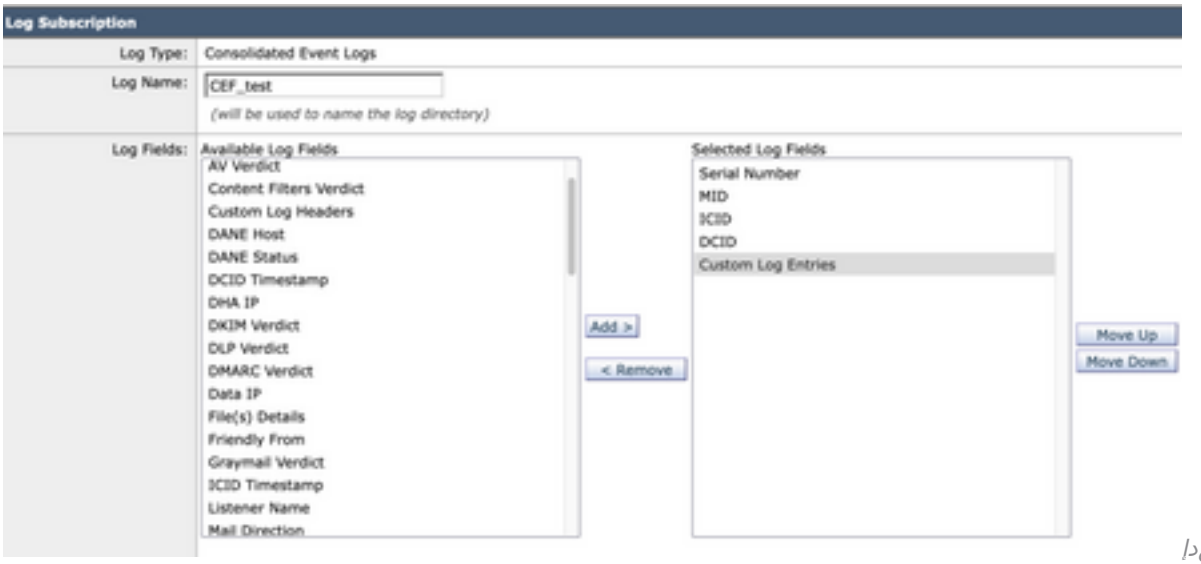
إجراء إدخال سجل CEF في عوامل تصفية المحتوى

إضافة إدخال سجل CEF في الاشتراك في سجل الأحداث المجمع

بعد ذلك، قم بإنشاء أو تعديل الاشتراك في سجل الأحداث الموحد لإضافة إدخال سجل CEF

الذي تم إنشاؤه مسبقا:

1. الانتقال إلى **System Administration > Log Subscriptions**
2. إضافة سجلات أحداث موحدة أو تحديدها
3. تحديد **Custom Log Entries** وانقر فوق **Add**
4. **Submit and Commit**



إدخالات السجل

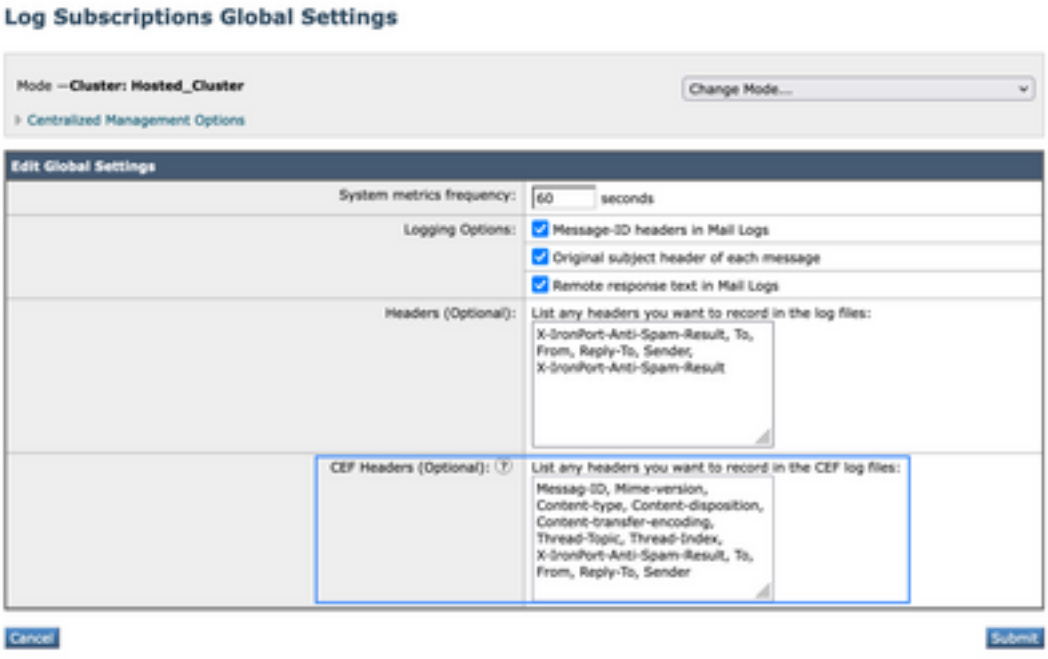
المخصصة في اشتراك سجل CEF

عناوين CEF

إضافة رؤوس CEF إلى السجل:

قم أولا بإضافة رؤوس CEF في ESA

1. الانتقال إلى **System Administration > Logs Subscription**
2. انقر في **Edit Settings** ضمن الإعدادات العمومية
3. تحت رؤوس CEF، قم بسرد الرؤوس التي سيتم تسجيلها
4. **Submit and Commit**

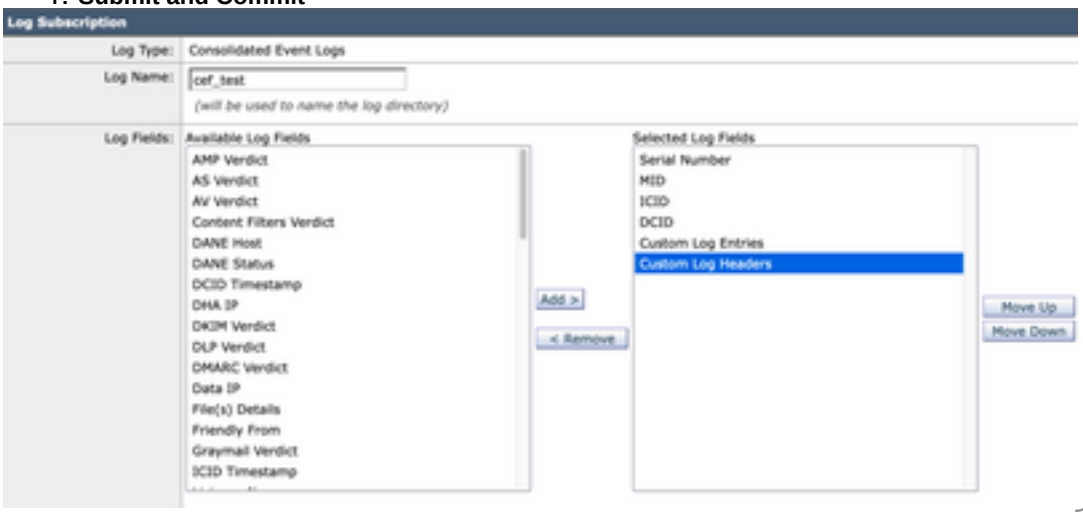


تكوين رؤوس CEF

إضافة إدخال سجل CEF في الاشتراك في سجل الأحداث المجمع

بعد ذلك، قم بإنشاء أو تعديل الاشتراك في سجل الأحداث المدمج لإضافة رؤوس CEF المسجلة مسبقا:

1. الانتقال إلى **System Administration > Logs Subscription**
2. إضافة سجلات أحداث موحدة أو تحديدها
3. تحديد **Custom Log Entries** وانقر فوق **Add**
4. **Submit and Commit**



اشتراك سجل CEF

رؤوس سجل CEF في

معلومات ذات صلة

- دليل المستخدم النهائي ESA 14.3
- ملاحظات الإصدار ESA، الإصدار 14.3
- الدعم الفني - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).