دمج Splunk مع إدارة سجل Umbrella باستخدام S3 والمزامنة المحلية

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين Splunk لتحليل سجلات حركة مرور DNS من مستودع S3 المدار من Cisco.

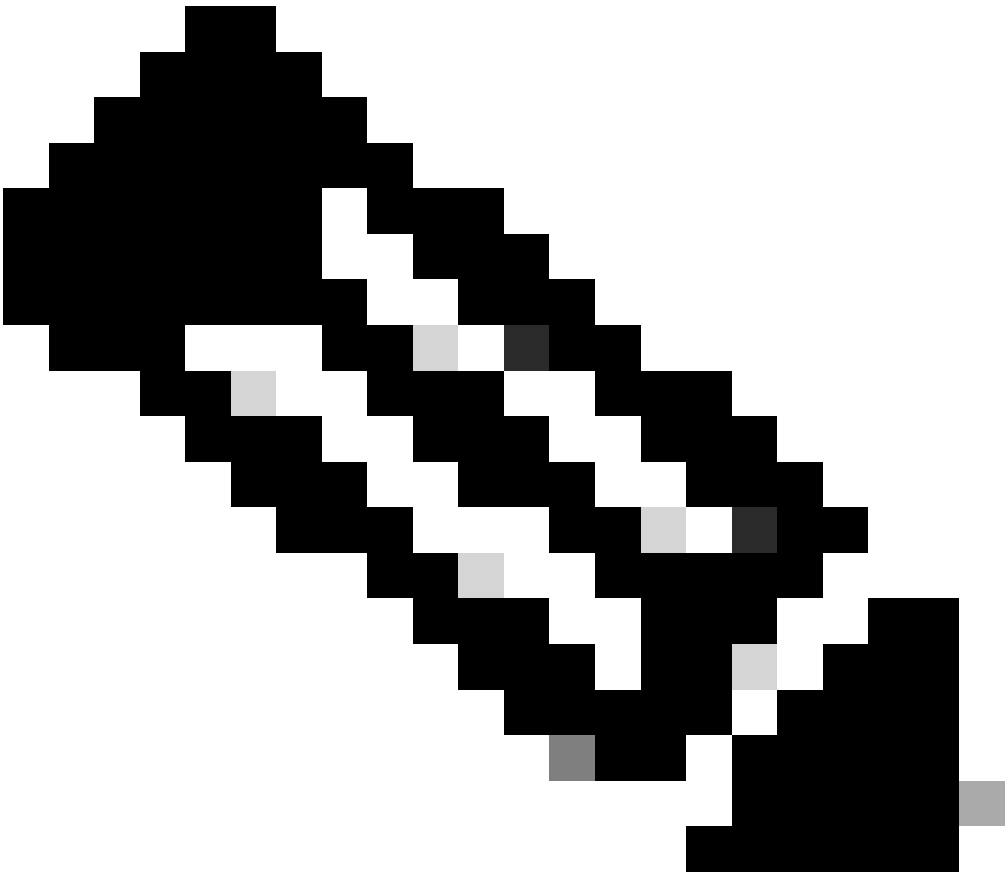
نظرة عامة

Splunk هي أداة لتحليل السجل. وهو يوفر واجهة قوية لتحليل مجموعات كبيرة من البيانات، مثل السجلات المقدمة من Cisco Umbrella لحركة مرور DNS الخاصة بك. تصف هذه المقالة كيفية:

- قم بإعداد دلو S3 المدار من قبل Cisco في لوحة معلوماتك.
- تأكد من استيفاء المتطلبات الأساسية لواجهة سطر الأوامر (AWS CLI) الخاصة بـ AWS.
- قم بإنشاء مهمة cron لاسترداد الملفات من الدلو وتخزينها محليا على الخادم.
- قم بتكوين Splunk للقراءة من دليل محلي.

المتطلبات الأساسية

- تنزيل [واجهة سطر أوامر AWS](#) وتثبيتها (AWS CLI).
- [قم بإنشاء دلو S3 المدار من Cisco](#).



ملاحظة: يمكن لعملاء أنظمة Umbrella Insights و Umbrella Platform الموجودة حالياً الوصول إلى إدارة السجلات باستخدام Amazon S3 من خلال لوحة المعلومات. إدارة السجل غير متوفرة في جميع الحزم. اتصل بمدير حسابك إذا كنت مهتماً بهذه الميزة.

إنشاء مهمة cron على خادم Splunk

1. قم بإنشاء نص تنفيذي لقشرة مسمى **pull-umbrella-logs.sh** باستخدام المحتويات المتوفرة، والتي يتم تشغيلها على مهمة cron مجدولة:

```
#!/bin/sh
cd <local data dir>
AWS_ACCESS_KEY_ID=<accesskey> AWS_SECRET_ACCESS_KEY=<secretkey> aws s3 sync <data path> .
```

استبدل المواضع المؤقتة بالقيم الحقيقية الخاصة بك:

-

: الدليل الموجود على القرص لتخزين ملفات السجل التي تم تنزيلها.

-
: مفتاح الوصول من لوحة معلومات Umbrella.
-
: مفتاح سري من لوحة معلومات المظلة.
-
: مسار البيانات من واجهة مستخدم إدارة السجل (على سبيل المثال، s3://cisco-managed-

/1_2xxxxxxxxxxxxxxxxxa120c73a7c51fa6c61a4b6/dnslogs/

).

2. احفظ البرنامج النصي ل Shell وقم بتعييني إذن التشغيل. يجب أن يكون البرنامج النصي مملوكا من الجذر.

```
$ chmod u+x pull-umbrella-logs.sh
```

3. قم بتشغيل **pull-umbrella-logs.sh** البرنامج النصي يدويا لتأكيد أن عملية المزامنة تعمل. الإكمال الكامل غير مطلوب؛ هذه الخطوة تؤكد أن منطق النصوص والمعطيات صحيحة.

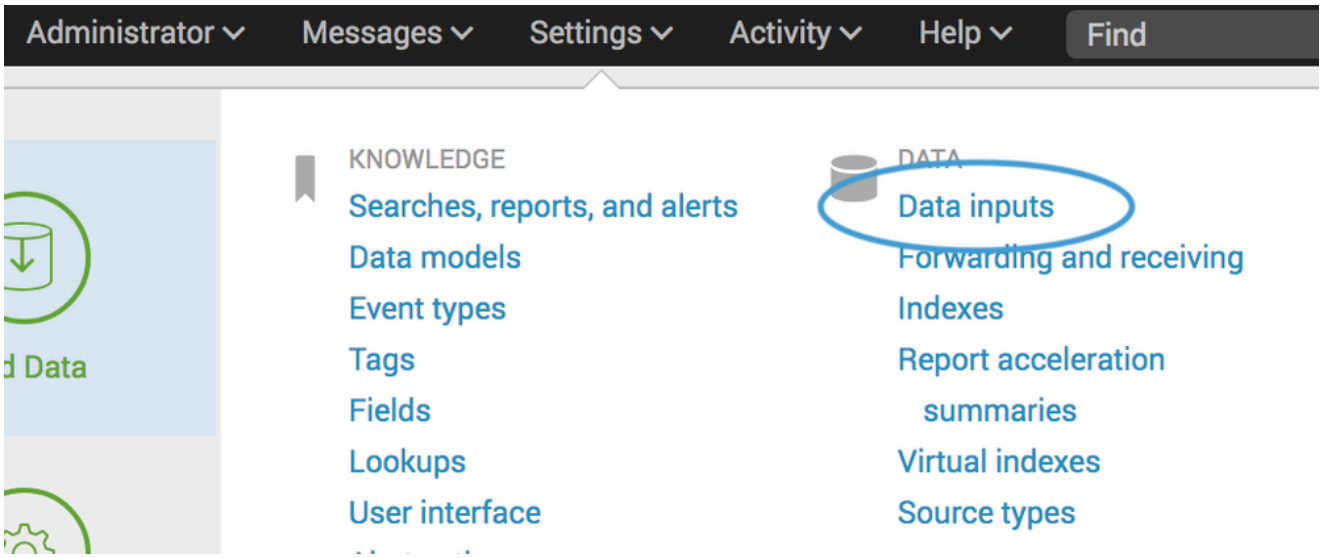
4. إضافة هذا السطر إلى crontab الخاص بخادم Splunk:

```
*/5 * * * * root root /path/to/pull-umbrella-logs.sh &2>1 >/var/log/pull-umbrella-logs.txt
```

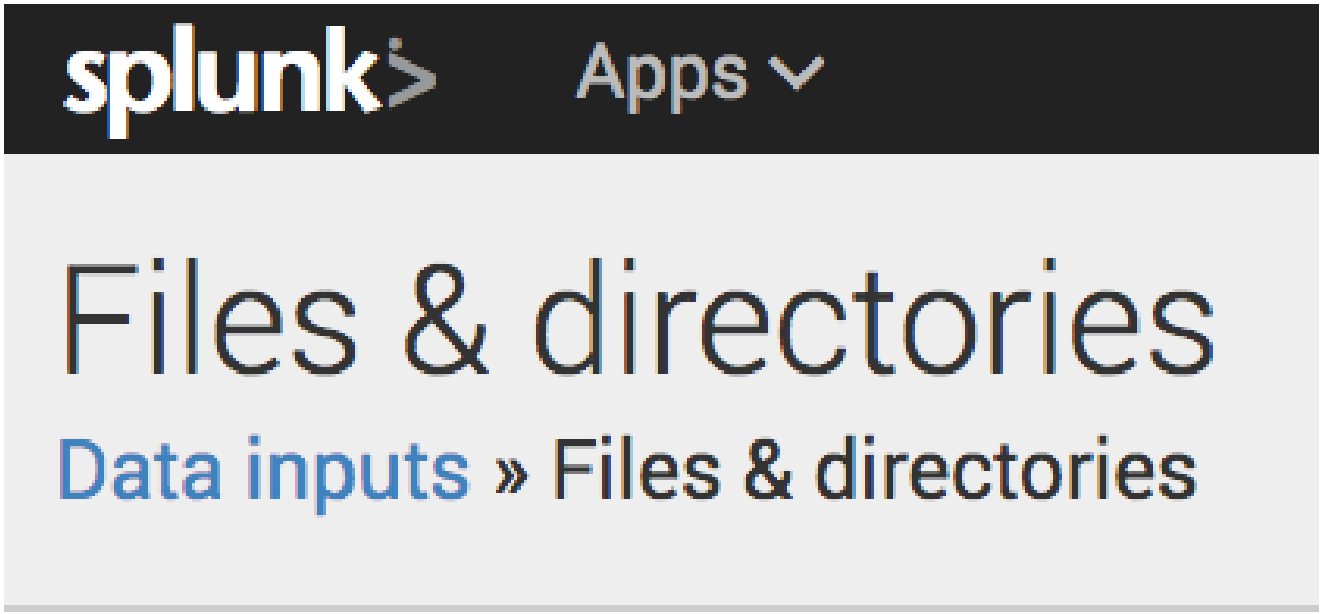
تأكد من تحرير الخط لاستخدام المسار الصحيح إلى النص التنفيذي. تقوم هذه العملية بتشغيل مزامنة كل خمس دقائق. يتم تحديث دليل وحدة التخزين S3 كل 10 دقائق وتظل البيانات موجودة على وحدة التخزين S3 لمدة 30 يوما. وهذا يؤدي إلى إستمرار التزامن بين الاثنين.

تكوين Splunk للقراءة من دليل محلي

1. في Splunk، انتقل إلى الإعدادات > مدخلات البيانات > الملفات والدلائل وحدد جديد.

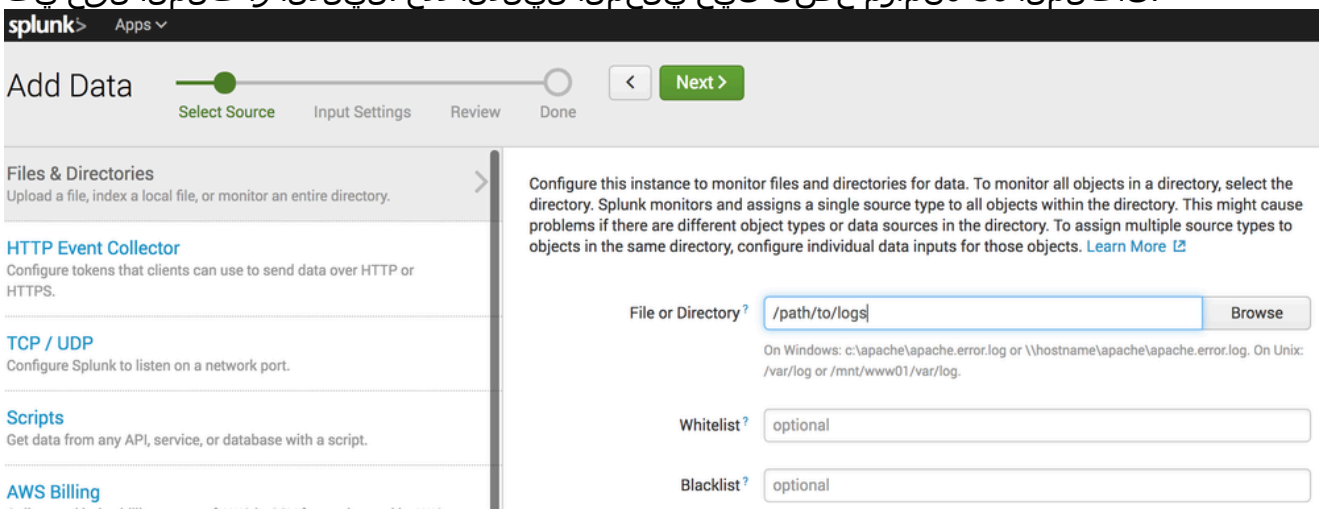


360002731126



360002731146

2. في حقل الملف أو الدليل، حدد الدليل المحلي حيث تضع مزامنة S3 الملفات.



360002731106

3. انقر فوق التالي ثم أكمل المعالج باستخدام الإعدادات الافتراضية.

بمجرد وجود بيانات في الدليل المحلي وتكوين Splunk، يمكن أن تكون البيانات متاحة للاستعلام وإعداد تقرير عنها في Splunk.

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).