تكوين تقسيم باستخدام دلو S3 ذاتي الإدارة

المحتويات

المقدمة

يصف هذا وثيقة كيف أن يشكل Splunk مع إدارة ذاتية S3 دلو.

نظرة عامة

SPLUNK هو أداة مشتركة لتحليل السجل. وهو يوفر واجهة قوية لتحليل مجموعات كبيرة من البيانات، مثل السجلات المقدمة من Cisco Umbrella لحركة مرور DNS في مؤسستك.

يوضح هذا المقال الأساسيات اللازمة لإعداد Splunk وتشغيلها حتى تتمكن من سحب السجلات من دلو S3 واستهلاكها. هناك مرحلتان رئيسيتان، الأولى هي تكوين بيانات اعتماد أمان AWS S3 للسماح بوصول الفواصل إلى السجلات، والثانية هي تكوين Splunk نفسه للإشارة إلى دلو الخاص بك.

توجد هناك الوثائق الخاصة بالوظيفة الإضافية لـ AWS S3، والتي تم نسخ بعضها حرفياً في هذا المستند. للحصول على أسئلة خاصة حول إعداد Splunk، يرجى الرجوع إلى http://docs.splunk.com/Documentation/AddOns/latest/AWS/Description

تحتوي هذه المقالة على الأقسام التالية:

- المتطلبات الأساسية
- المرحلة الأولى: تكوين بيانات اعتماد الأمان في AWS (دلو ذاتي الإدارة فقط)
- المرحلة الثانية: إعداد Splunk لسحب بيانات سجل DNS من دلو S3
  - الخطوة 1: إعداد Splunk لسحب بيانات سجل DNS من دلو S3 المدار ذاتيا
- المرحلة الثالثة: تكوين مدخلات البيانات لـ Splunk

المتطلبات الأساسية

تدعم الأداة الإضافية Splunk لخدمات الويب من Amazon هذه الأنظمة الأساسية.

- إيه دبليو إس لينكس
- ريد هات
- Windows 2008R2، 2012R2

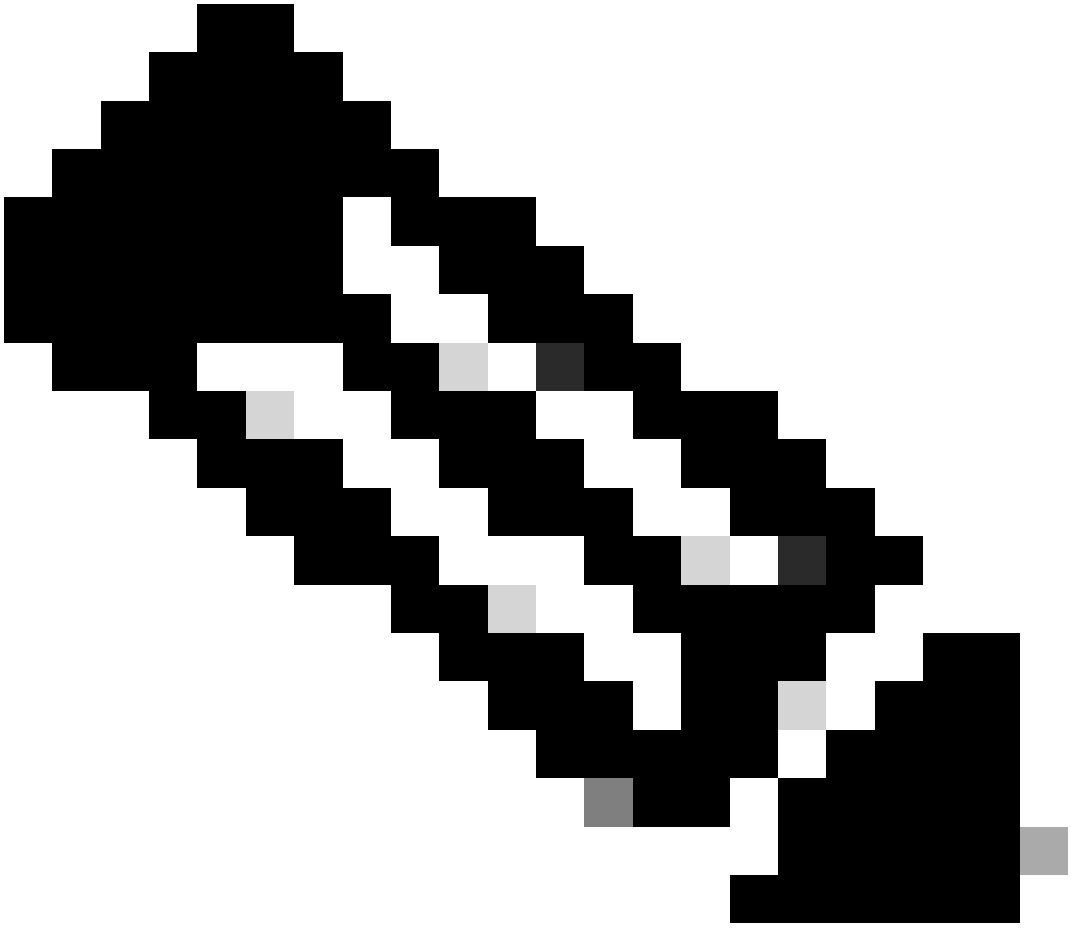
متطلبات نظام Splunk للمؤسسات

نظرا لتشغيل هذه الوظيفة الإضافية على Splunk Enterprise، يتم تطبيق جميع متطلبات نظام Splunk Enterprise. انظر دليل تثبيت "متطلبات النظام" في وثائق Splunk Enterprise. هذه التعليمات خاصة بالإصدار 6.2.1 من Splunk Enterprise.

متطلبات المظلة

يفترض هذا المستند أنه قد تم تكوين مستودع Amazon AWS S3 في لوحة معلومات Umbrella (إدارة سجل Admin>) وهو يظهر اللون الأخضر مع تحميل السجلات الحديثة. للحصول على مزيد من المعلومات حول إدارة السجل، راجع إدارة سجل Cisco Umbrella في Amazon S3.

المرحلة الأولى: تكوين بيانات اعتماد الأمان الخاصة بك في AWS



ملاحظة: هذه الخطوات هي نفسها لكل الموضحة في المقالة التي تصف كيفية تكوين أداة لتنزيل السجلات من الدلو الخاص بك (كيفية: تنزيل السجلات من إدارة سجل Cisco Umbrella في AWS S3). إذا قمت بالفعل بإجراء هذه الخطوات، فيمكنك ببساطة التخطي إلى الخطوة 2، رغم أنك تحتاج إلى بيانات اعتماد الأمان من مستخدم IAM لمصادقة مكون Splunk الإضافي إلى دلو الخاص بك.

الخطوة 1

1. قم بإضافة مفتاح وصول إلى حساب Amazon Web Services للسماح بالوصول عن بعد إلى الأداة المحلية الخاصة بك وإعطاء إمكانية تحميل الملفات وتنزيلها وتعديلها في S3. قم بتسجيل الدخول إلى AWS وانقر فوق اسم حسابك في الزاوية العلوية اليمنى. في القائمة المنسدلة، أختر مسوغات التأمين.
2. تتم مطالبتك باستخدام أفضل ممارسات Amazon وإنشاء مستخدم AWS لإدارة الوصول والهوية (IAM). في الأساس، يضمن مستخدم IAM أن الحساب الذي يستخدمه S3cmd للوصول إلى دلو الخاص بك ليس الحساب الأساسي (على سبيل المثال، حسابك) لتكوين S3 بالكامل. من خلال إنشاء مستخدمين أفراد لـ IAM للأشخاص الذين يمكنهم الوصول إلى حسابك، يمكنك منح كل مستخدم IAM مجموعة فريدة من بيانات

اعتماد الأمان. يمكنك أيضا منح أذونات مختلفة لكل مستخدم IAM. إذا كان ضروري، يمكنك تغيير وأ إبطال أذون مستخدم IAM في أي وقت.
لمزيد من المعلومات حول مستخدمي IAM وأفضل ممارسة AWS، يرجى القراءة هنا على العنوان https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

الخطوة 2

1. قم بإنشاء مستخدم IAM للوصول إلى مستودع S3 بالنقر فوق بدء إستخدام مستخدمي IAM. يتم نقلك إلى شاشة حيث يمكنك إنشاء مستخدم IAM.
2. انقر فوق إنشاء مستخدمين جدد، ثم قم بالمضي قدما وقم بتعبئة الحقول. لاحظ أنه ال يمكن أن يحتوي حساب المستخدم على مسافات.
3. بعد إنشاء حساب المستخدم، يتم منحك فرصة واحدة فقط للحصول على معلوماتين مهمتين تحتويان على بيانات اعتماد أمان مستخدم Amazon. نوصي بشدة بتنزيل هذه المعلومات باستخدام الزر الموجود في أسفل اليمين لنسخها إحتياطيا. ال تتوفر بعد هذه المرحلة في الإعداد. تأكد من إنشاء ملاحظة لكل من معرف مفتاح الوصول ومفتاح الوصول السري كما نحتاج إليهما لاحقا عند إعداد Splunk.

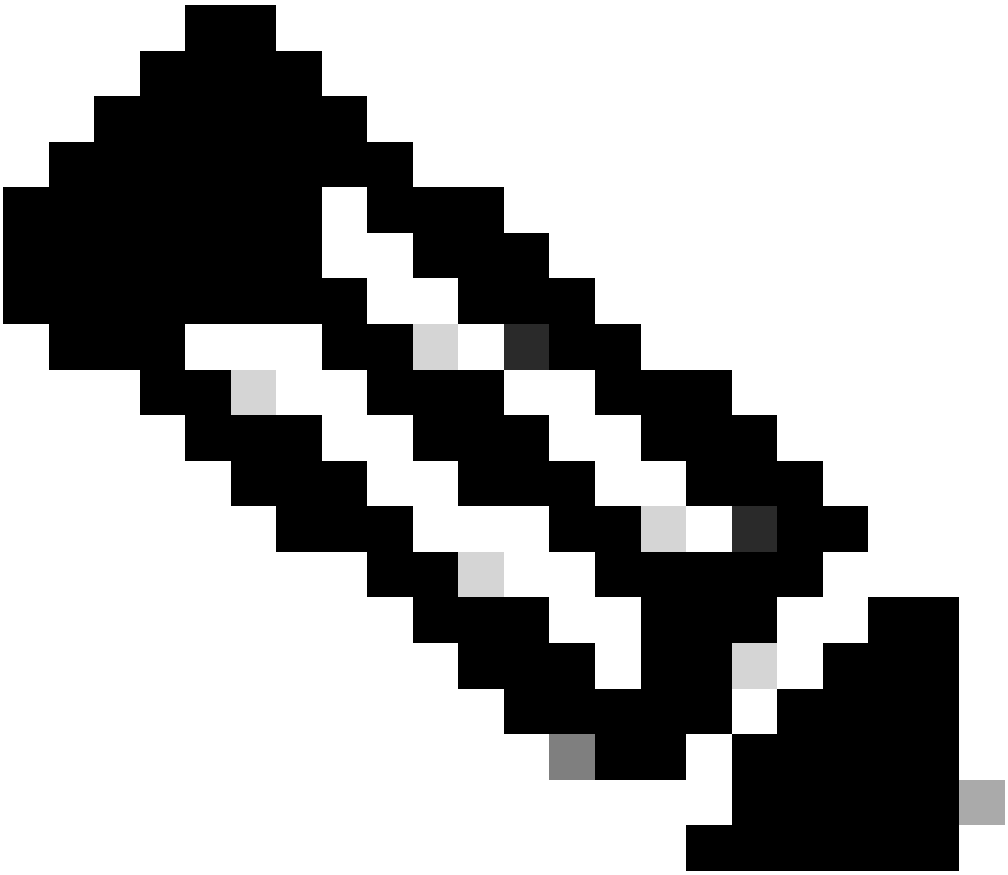
الخطوة 3

1. بعد ذلك، تريد إضافة نهج لمستخدم IAM لديك بحيث يمكنهم الوصول إلى دلو S3. انقر فوق المستخدم الذي قمت بإنشائه للتو ثم قم بالتمرير لأسفل خلال خصائص المستخدمين حتى ترى الزر "إرفاق النهج".
2. انقر فوق إرفاق النهج، ثم أدخل 's3' في عامل تصفية نوع النهج. وهذا يظهر نتيجتين: "AmazonS3FullAccess" و"AmazonS3ReadOnlyAccess".
3. حدد AmazonS3FullAccess ثم انقر فوق إرفاق سياسة.

المرحلة الثانية: إعداد Splunk لسحب بيانات سجل DNS من دلو S3

الخطوة 1: إعداد Splunk لسحب بيانات سجل DNS من دلو S3 المدار ذاتيا

1. ابدأ بتثبيت "Splunk Add-on for Amazon Web Services" على مثيل Splunk. افتح لوحة معلومات Splunk وانقر فوق Apps، أو انقر فوق Splunk Apps إذا ظهرت على لوحة المعلومات. بمجرد أن تدخل إلى قسم "التطبيقات"، اكتب "s3" في نافذة البحث للعثور على "وظيفة Splunk الإضافية ل Amazon Web Services"، وقم بتثبيت التطبيق.



ملاحظة: من المحتمل أن تحتاج إلى إعادة تشغيل Splunk أثناء التثبيت. بمجرد تثبيته، تظهر الوظيفة الإضافية Splunk ل AWS التي تتضمن اسم المجلد 'Splunk_TA_AWS' المدرج الآن ضمن Apps.

2. انقر فوق إعداد لتكوين التطبيق. هذه هي النقطة التي تحتاج فيها إلى بيانات اعتماد الأمان من المرحلة الأولى في هذه الوثيقة.
يتطلب الإعداد إدخال هذه الحقول:

- اسم مألوف - الاسم الذي تستخدمه للإشارة إلى هذا التكامل
- معرف مفتاح حساب AWS الخاص بك (من المرحلة 1)
- كلمة المرور الخاصة بك (مفتاح سر حساب AWS الخاص بك، أيضا من المرحلة 1)

يمكنك أيضا تعيين أي معلومات وكيل محلي إذا كانت مطلوبة للوصول Splunk إلى AWS، بالإضافة إلى ضبط التسجيل. شاشة الإعداد تبدو كما يلي:
3. بمجرد إضافة المعلومات ذات الصلة، انقر فوق حفظ وتم تكوين الوظيفة الإضافية Splunk ل Amazon Web Services بالكامل.

المرحلة الثالثة: تكوين مدخلات البيانات ل Splunk

1. بعد ذلك، ترى تكوين إدخال البيانات لـ Amazon Web Services S3. انتقل إلى الإعدادات > البيانات > مدخلات البيانات وتحت المدخلات المحلية، يمكنك الآن رؤية قائمة بمختلف مدخلات Amazon بما في ذلك S3 في أسفل القائمة.
2. انقر فوق AWS S3 لتكوين الإدخال.
3. انقر فوق جديد.
4. أنت مطالب بتوفير هذه المعلومات:

    - أدخل اسما مألوفا لتكامل S3.
    - حدد حساب AWS من القائمة المنسدلة. هذا هو الاسم المألوف الذي قمت بتوفيره في الخطوة 1.
    - حدد دلو S3 من القائمة المنسدلة. هذا هو اسم المستودع كما هو محدد في لوحة معلومات Umbrella (الإعدادات > إدارة السجل).
    - حدد اسم المفتاح S3 من القائمة المنسدلة. يتم سرد كل عنصر في الدلو الخاص بك، ونوصي باتباع دليل المستوى الأعلى \dns-log\ ، والذي يتضمن كافة الملفات والدلائل الموجودة تحته.
    - هناك العديد من الخيارات تحت "تكوين نظام الرسائل"، ونوصي بترك هذا كما هو—الإعدادات الافتراضية.
    - هناك خيارات إضافية تحت "المزيد من الإعدادات". الملاحظة هو "مصدر نوع"، أي aws:s3 افتراضيا. نحن نوصي بترك هذا كما هو، ولكن إذا قمت بتغييره، فإن عامل تصفية السجلات في البحث يتغير عما هو موصوف في الخطوة 3 من هذه التعليمات.

املأ التفاصيل، وسيبدو إدخال بياناتك مشابها لما يلي:

4. انقر فوق التالي لإنهاء التفاصيل الخاصة بك.
   يتم نقلك إلى شاشة تظهر أن الإدخال تم إنشاؤه بنجاح

الخطوة 3

قم بإجراء بحث سريع لمعرفة ما إذا كان يتم إستيراد بياناتك بشكل صحيح. قطع الصق sourcetype="aws:s3" في نافذة البحث في أعلى اليمين ثم حدد "فتح نوع المصدر="aws:s3" في البحث

ينقلك هذا إلى شاشة مماثلة للشاشة التي ترى فيها الأحداث من سجلات DNS الخاصة بمؤسستك. هنا، توقع خدمة Cisco Umbrella Mobile بحظر الوسائط الاجتماعية على iPhone. يمكنك أيضا إستخدام مصدر اسم الملف للتصفية مقابل مجموعة معينة من السجلات.

بعد هذه النقطة، تستمر وظيفة cron في الخلفية في التشغيل وسحب أحدث مجموعات من معلومات السجل من الدلو الخاص بك.

هناك الكثير الذي يمكنك القيام به مع Splunk بخلاف ما تم توضيحه في هذه المقالة، وإذا دون سنحت لك الفرصة لتجربة إستخدام هذه البيانات في إجراء الاستجابة الأمنية، فإننا نحب أن نسمع منك. قم بإرسال أي ملاحظات أو أسئلة أو اهتمامات إلى فريق umbrella-support@cisco.com وأرجع هذه المقالة.

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).