تكوين تكامل QRadar باستخدام إدارة سجل S3 و Umbrella

المحتويات

المقدمة

يصف هذه الوثيقة كيفية أن يشكل QRadar أن يجلب سجل من AWS S3 دلو ل Umbrella سجل إدارة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- يفترض هذا المستند أنه قد تم تكوين دلو Amazon AWS S3 في Umbrella (الإعدادات > إدارة السجل) وهو يظهر اللون الأخضر مع تحميل السجلات الحديثة. لمزيد من المعلومات حول كيفية تكوين هذه الميزة، أقرأ هذه المقالة: تنزيل السجلات من إدارة سجل Umbrella في AWS S3

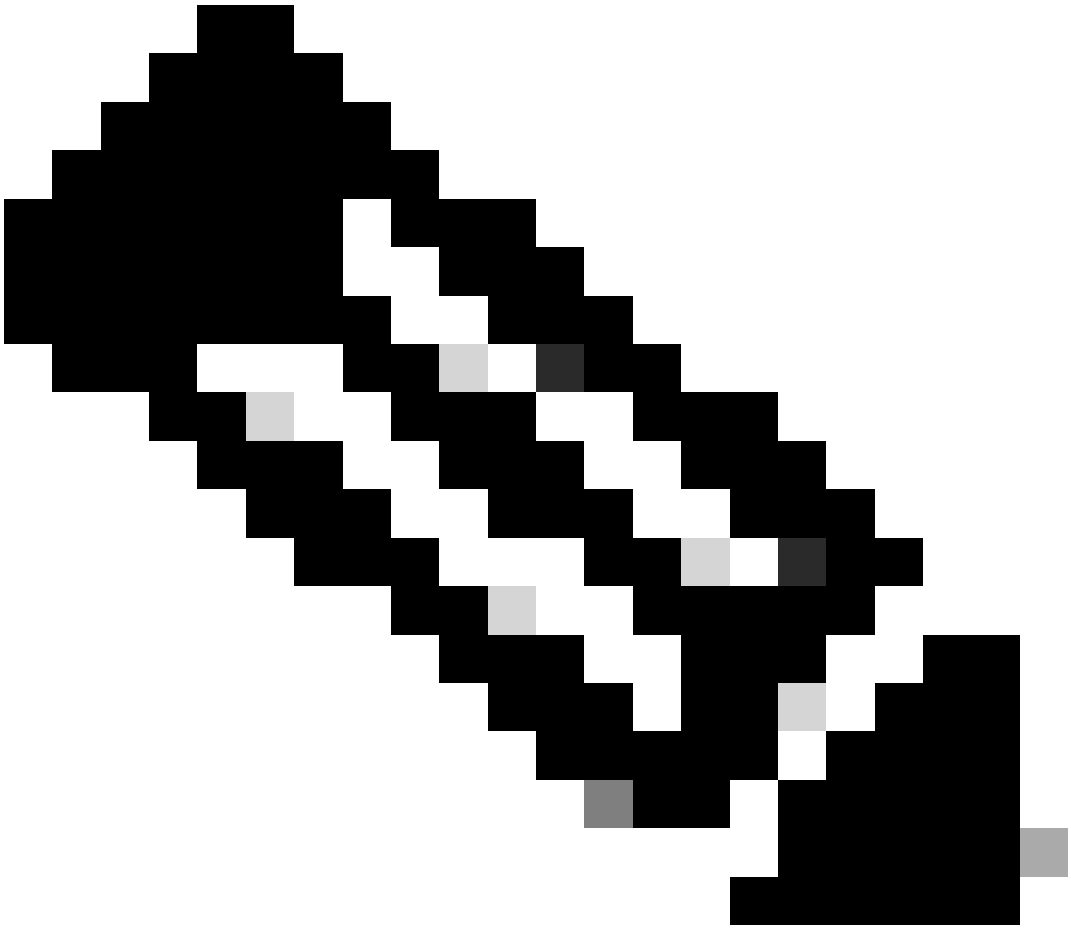
- بالإضافة إلى الحقوق الإدارية الخاصة بجهاز (أجهزة) QRadar والتكوين S3 من Amazon ولوحة معلومات المظلة، يفترض هذا التعليمات أن مسؤول QRadar على دراية بإنشاء ملفات LSX (ملحق مصدر السجل).

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Cisco Umbrella.

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.

نظرة عامة



ملاحظة: أفضل طريقة لتكوين QRadar للاستخدام مع Cisco Umbrella هي من خلال تطبيق أمان السحابة من Cisco. قم باستخدام هذا الأسلوب فقط في حالة تعذر تكوين التطبيق.

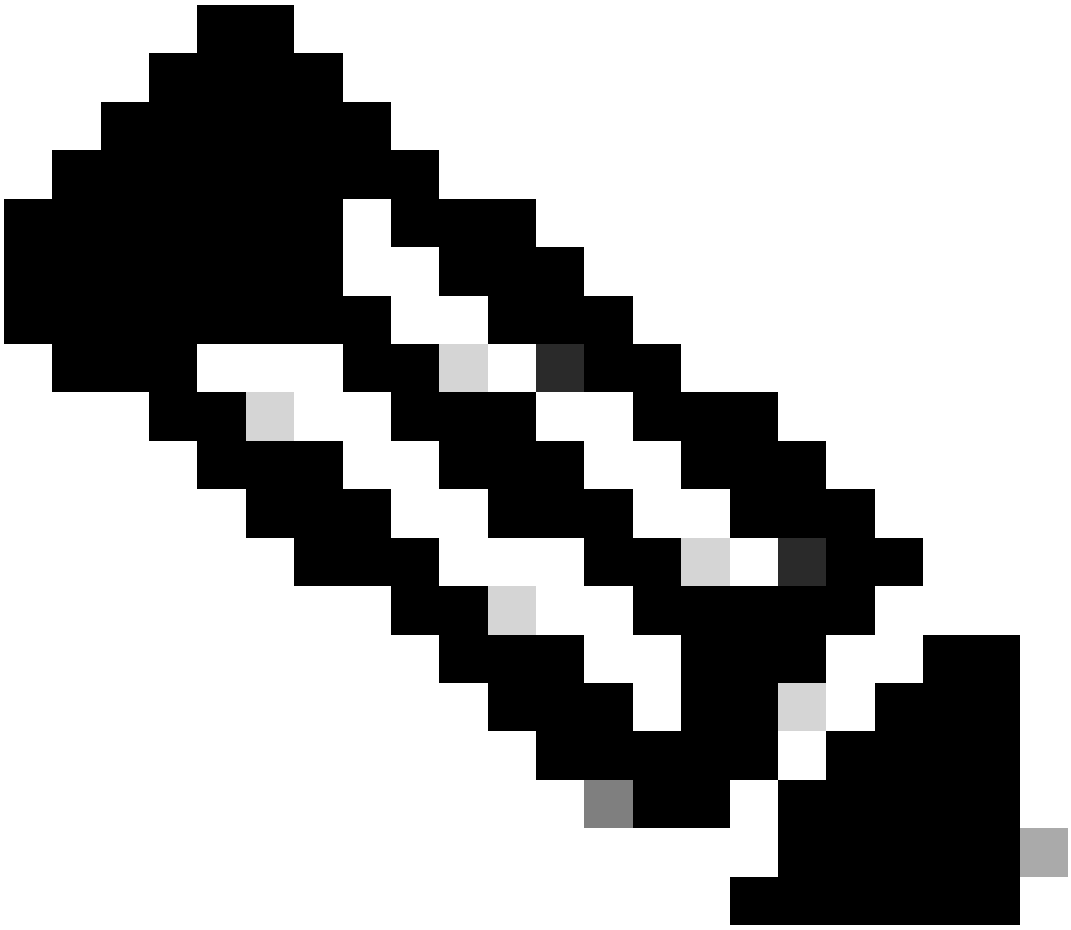
QRadar من IBM وهو SIEM شائع لتحليل السجل. وهو يوفر واجهة قوية لتحليل مجموعات كبيرة من البيانات، مثل السجلات المقدمة من Cisco Umbrella لحركة مرور DNS في

مؤسستك.

يوضح هذا المقال كيفية إعداد QRadar وتشغيله حتى يتمكن من سحب السجلات من دلو S3 واستهلاكها. هناك مرحلتان رئيسيتان:

- قم بتكوين بيانات اعتماد أمان AWS S3 للسماح بوصول QRadar إلى السجلات.
- قم بتكوين QRadar نفسه ليشير إلى دلتك.

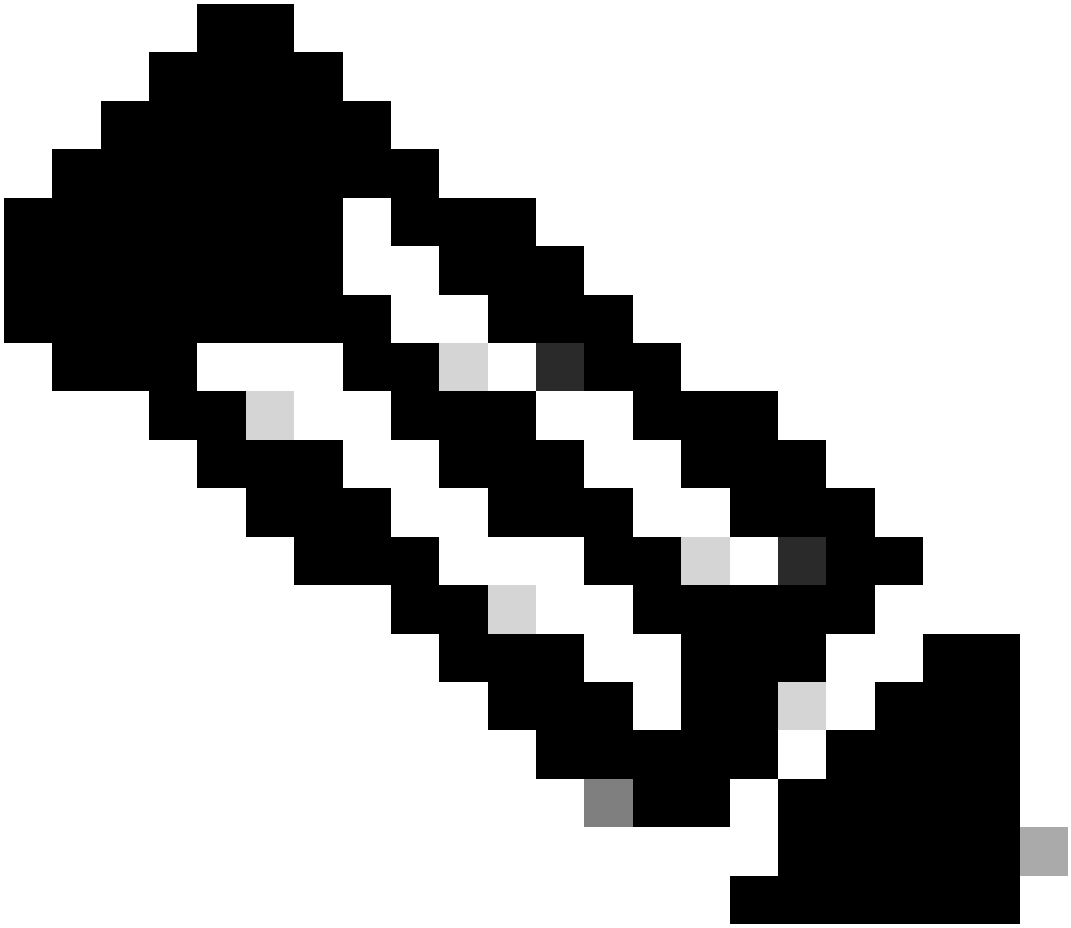
إذا كنت تستخدم دلو S3 المدار من Cisco، فيرجى إستخدام هذه الإرشادات في المقال Download Log Log Management من Umbrella باستخدام واجهة سطر الأوامر (CLI) الخاصة ب AWS.



ملاحظة: تم إختبار هذا التكامل مع كل من دلاء S3 المدارة من قبل العميل ودلاء Cisco Managed S3. المعلومات التي تمت مناقشتها في هذه المقالة حديثة منذ كتابة هذا المقال (أكتوبر 2019). يمكن تغييرها استنادا إلى طريقة واجهة خدمات QRadar و AWS. هذا المستند هو مستند حي. إذا كانت لديك ملاحظات أو عثرت على حيل أو تلميحات يمكن أن تساعد العملاء الآخرين، فيرجى الاتصال بدعم Cisco Umbrella.

يجب أن يأتي دعم QRadar من IBM، لأن Cisco غير قادرة على دعم الأجهزة أو البرامج التابعة لجهات خارجية مباشرة. بالنسبة لأي مشكلات تتعلق بتوصيل لوحة معلومات Umbrella الخاصة بك بحزمة S3، يمكن أن توفر Cisco Umbrella الدعم. يمكن الاطلاع أيضا على الكثير من المعلومات الواردة في هذه المقالة على موقع IBM على الإنترنت.

المرحلة الأولى: تكوين بيانات اعتماد الأمان الخاصة بك في AWS



ملاحظة: هذه الخطوات هي نفسها تلك الموضحة في المقالة التي تصف كيفية تكوين أداة لتنزيل السجلات من دلو المستخدم (تنزيل السجلات من إدارة سجل Umbrella في AWS S3). إذا قمت بالفعل بتنفيذ هذه الخطوات، يمكنك التخطي إلى المرحلة 2، رغم أنك تحتاج لاحقا إلى بيانات اعتماد الأمان من مستخدم IAM لمصادقة QRadar إلى دلو الخاص بك.

الخطوة 1

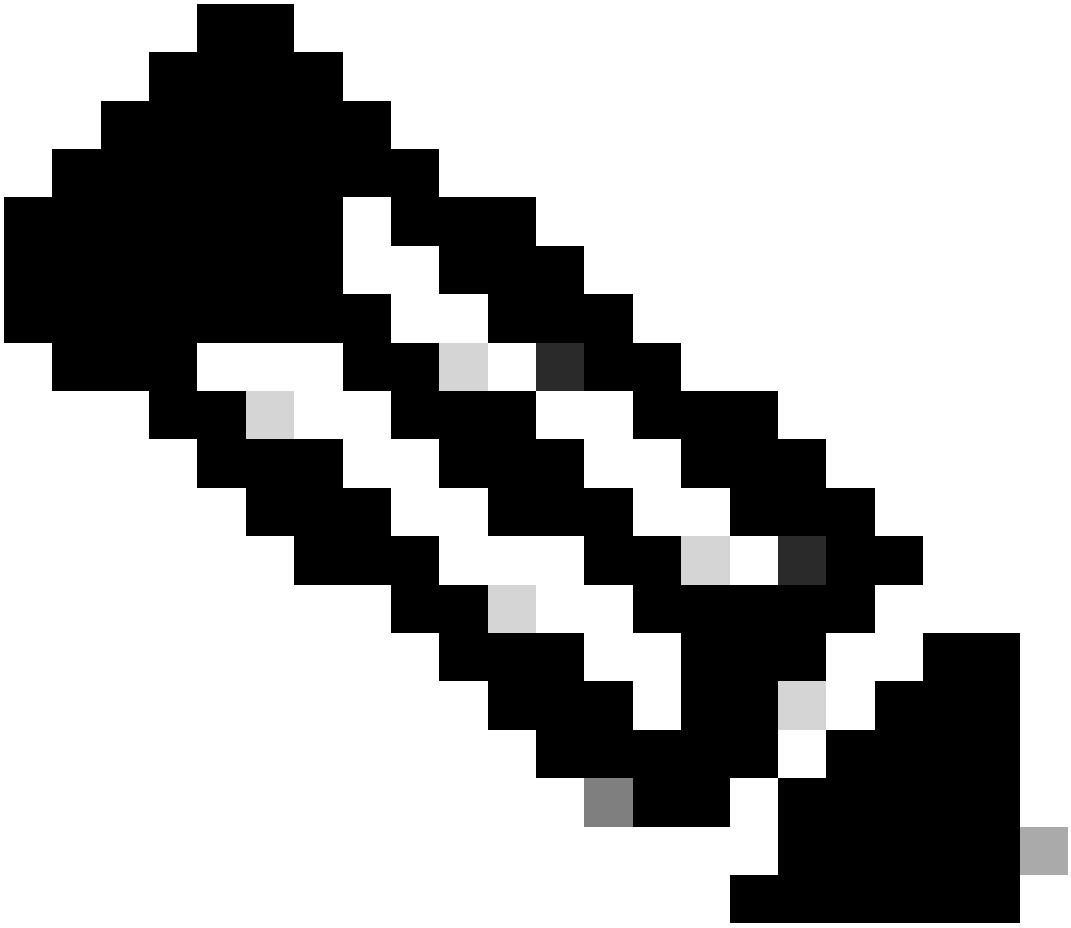
1. أضف مفاتيح وصول إلى حساب Amazon Web Services للسماح بالوصول عن بعد إلى الأداة المحلية الخاصة بك وإعطاء إمكانية تحميل الملفات وتنزيلها وتعديلها في S3:

1. تسجيل الدخول إلى AWS.
2. حدد اسم حسابك في الزاوية العلوية اليمنى.
3. في القائمة المنسدلة، حدد مسوغات التأمين.

2. يطلب منك بعد ذلك إستخدام 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 الرئيسي (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 ضروريا، يمكنك تغيير أو إبطال أذون مستخدم IAM في أي وقت. لمزيد من المعلومات حول مستخدمي IAM وأفضل ممارسات AWS، اقرأ وثائق AWS.

الخطوة 2

1. حدد بدء إستخدام مستخدمي IAM لإنشاء مستخدم IAM للوصول إلى دلو S3، ثم يتم نقلك إلى شاشة حيث يمكنك إنشاء مستخدم IAM.
2. حدد مستخدمين جدد، ثم أكمل الحقول.



ملاحظة: لا يمكن أن يحتوي حساب المستخدم على مسافات.

3. بعد إنشاء حساب المستخدم، يتم بعد ذلك منحك فرصة واحدة فقط للحصول على معلوماتين مهمتين تحتويان على بيانات اعتماد أمان مستخدم Amazon الخاصة بك. تقترح Umbrella بشدة أن تقوم بتحميلهما باستخدام الزر الموجود في أسفل اليمين لنسخهما إحتياطي. لا تتوفر بعد هذه المرحلة من الإعداد. تأكد من كتابة ملاحظة بكل من معرف مفتاح الوصول ومفتاح الوصول السري لأنهما مطلوبان في خطوة لاحقة.

الخطوة 3

بعد ذلك، قم بإضافة نهج لمستخدم IAM الخاص بك بحيث يمكنهم الوصول إلى دلو S3 الخاص بك:

1. حدد المستخدم الذي تم إنشاؤه للتو، ثم قم بالتمرير لأسفل خلال خصائص المستخدمين حتى ترى الزر إرفاق النهج.

2. حدد إرفاق النهج، ثم أدخل "S3" في عامل تصفية نوع النهج. وهذا يظهر نتيجتين:

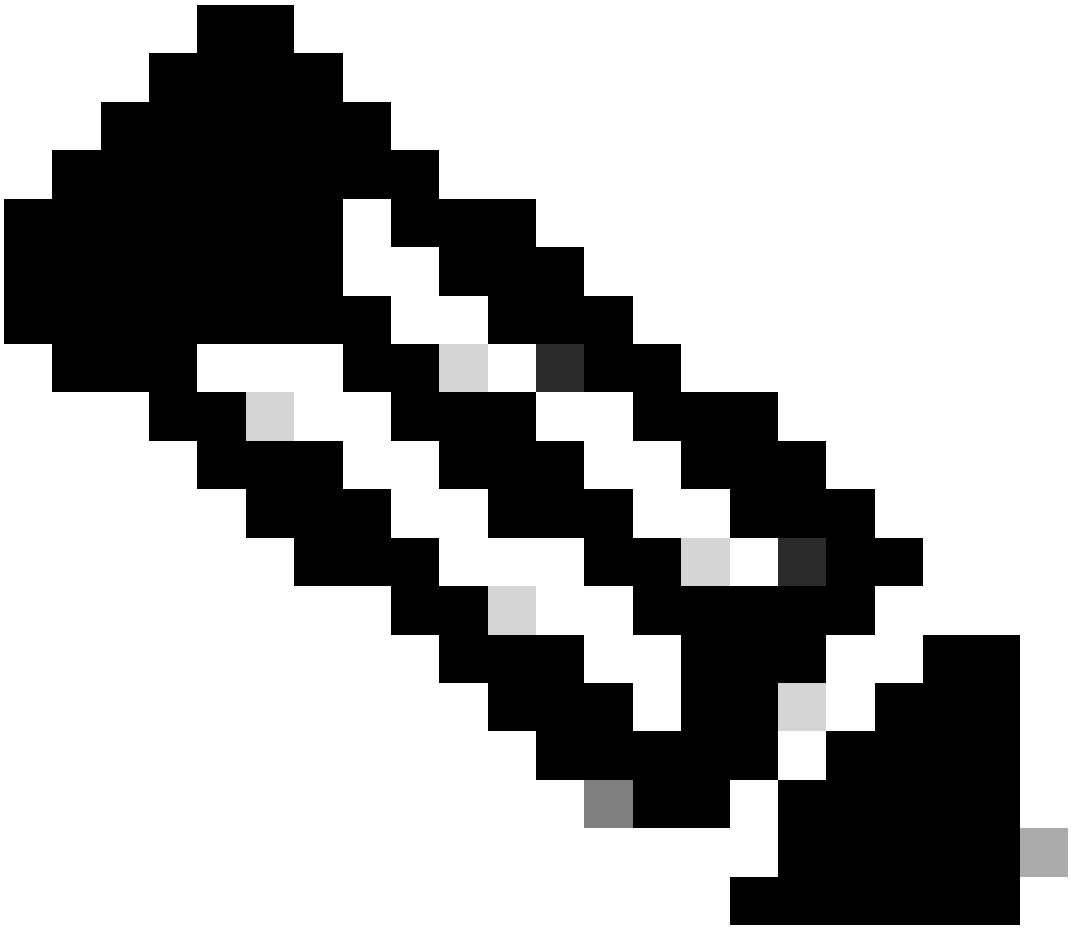
- AmazonS3FullAccess
- AmazonS3ReadOnlyAccess

3. حدد AmazonS3FullAccess، ثم حدد إرفاق النهج في الركن السفلي الأيمن.

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

يستخدم QRadar خدمة AWS CloudTrail، وهي خدمة ويب تقوم بتسجيل إستدعاءات AWS API لحسابك وتقدم ملفات السجل إليك.

قبل وصول QRadar إلى Amazon S3، أكمل هذه الإجراءات من IBM للحصول على شهادة خادم Amazon. هذا الجزء صعب، لذلك يرجى التأكد من إتمام الإرشادات بدقة.



ملاحظة: في الاختبار، يجب إستخدام متصفح Firefox حتى يعمل هذا كما هو متوقع.

للحصول على شهادة خادم Amazon، يجب نقل الشهادة بتنسيق DER إلى جهاز QRadar المناسب. جهاز QRadar الذي يتطلب الشهادة وهو الجهاز المعين في حقل مجمع الأحداث الهدف في مصدر سجل CloudTrack ل Amazon AWS.

قبل البدء

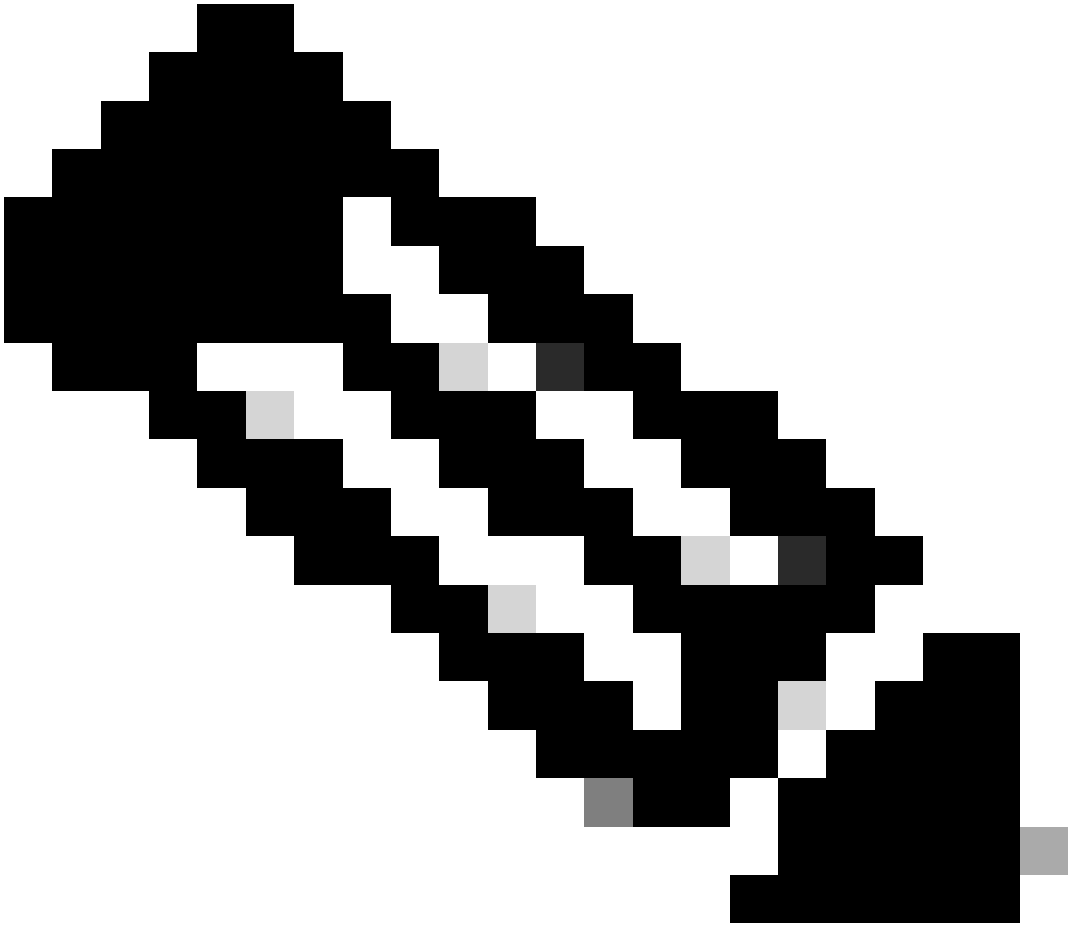
- يجب أن تكون الشهادة بتنسيق .DER.
- الامتداد .der حساس لحالة الأحرف ويجب أن يكون أحرف كبيرة.
- إذا تم تصدير الشهادة في أحرف صغيرة، فيمكن أن يواجه مصدر السجل مشاكل في مجموعة الأحداث.

الخطوات الأولية

1. الوصول إلى مستودع AWS CloudTrail S3: `https://<bucketname>.s3.amazonaws.com`

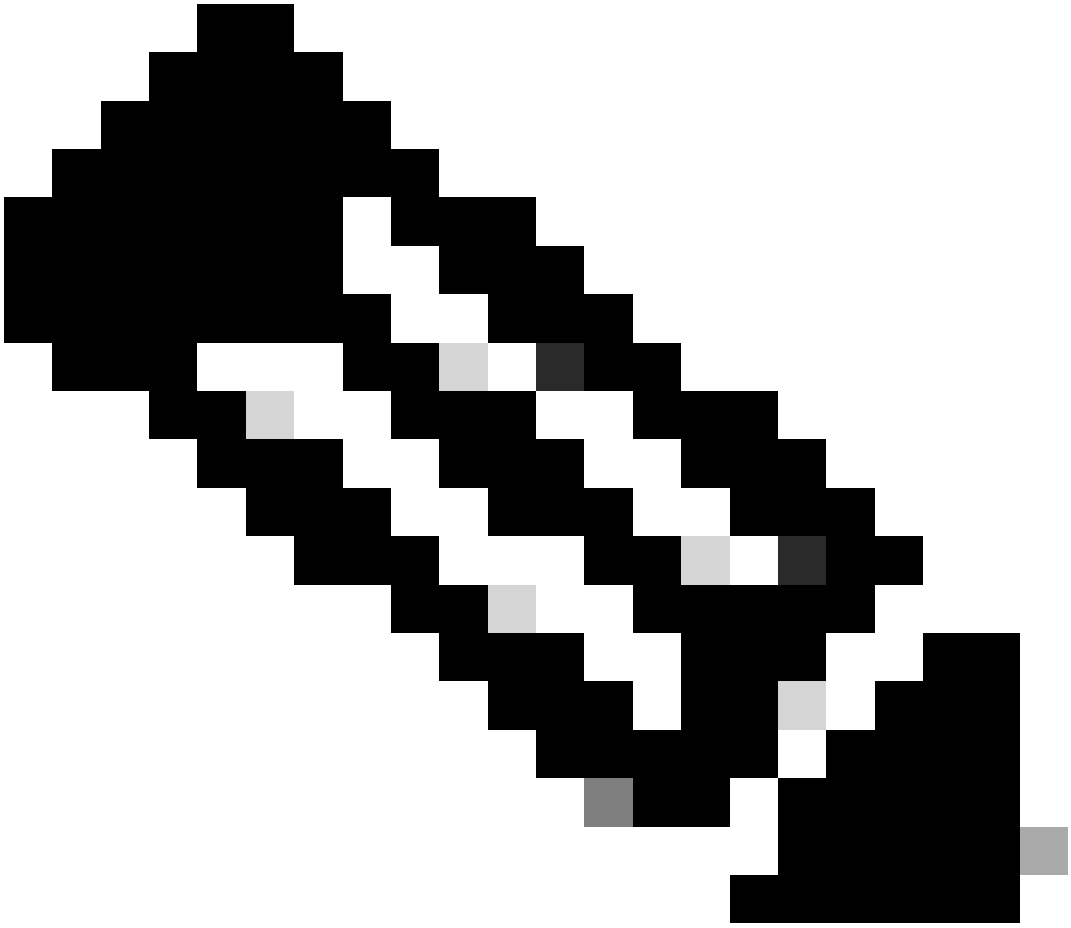
2. أستخدم Firefox لتصدير شهادة SSL من AWS كشهادة (.DER). باستطاعة Firefox إنشاء الشهادة المطلوبة باستخدام المرحق .DER:

   1. حدد رمز هوية الموقع (رمز القفل في شريط العناوين).
   2. حدد المزيد من المعلومات > عرض الشهادة وحدد عالمة التبويب تفاصيل.
   3. حدد تصدير للتصدير بتنسيق .DER للشهادة.



ملاحظة: ملحق DER حساس لحالة الأحرف ويجب أن يكون حروف كبيرة.

3. انسخ شهادة .DER إلى دليل /opt/qrAdar/conf/trusted_certificates الخاص بجهاز QRadar الذي يدير مصدر سجل Amazon AWS CloudTrack. يمكنك إستخدام WinSCP لنسخه.



ملاحظة: يتم تحديد جهاز QRadar الذي يدير مصدر السجل بواسطة حقل تجميع الأحداث الهدف في مصدر سجل CloudTrack ل Amazon AWS. يجب أن يكون لدى جهاز QRadar الذي يدير مصدر سجل Amazon AWS CloudTrail نسخة من شهادة .DER في /opt/QRadar/conf/trusted_certificates.

---

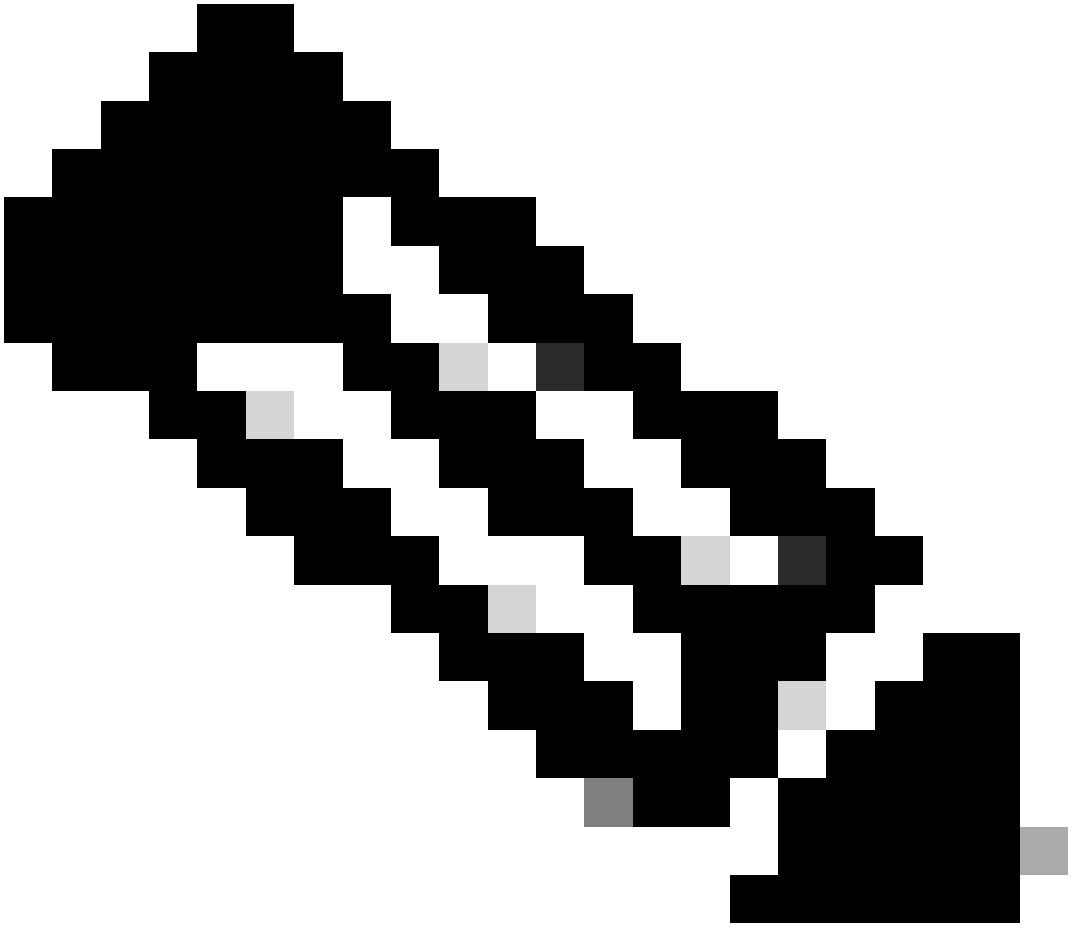
4. سجل الدخول إلى واجهة مستخدم QRadar كمسؤول إداري.

5. حدد علامة التبويب مسؤول.

6. حدد أيقونة مصادر السجل.

7. حدد مصدر سجل Amazon AWS CloudTrail.

8. من قائمة التنقل، حدد enable/disable لتعطيله ثم أعد تمكين مصدر سجل Amazon AWS CloudTrack.



ملاحظة: عندما يقوم المسؤول بفرض مصدر السجل من "معطل" إلى "ممكن"، يسمح Amazon AWS كما هو محدد في مصدر السجل. لذلك للبروتوكول بالاتصال بسطل. ويتم التحقق من الشهادة بعد ذلك كجزء من الاتصال الأول.

9. إذا إستمرت المشكلات في الظهور، فتحقق من أن حقل "معرف مصدر السجل" يحتوي على اسم مستودع AWS الصحيح في Amazon ومن صحة مسار "الدليل البعيد" في تكوين مصدر السجل.

إنهاء تكوين QRadar

1. في QRadar، تأكد من أن جميع بروتوكولات DSMs ومعلومات أخرى محدثة. حدد بروتوكول LogFileProtocol باستخدام هذه التكوينات (يمكن أن يكون التكرار ووقت البدء والتكرار ومعلومات أخرى مختلفة).

2. في علامة التبويب مصادر السجل، أدخل اسم مصدر السجل ووصف مصدر السجل. هذه يمكن أن تكون ما تريد.

3. أدخل اسم مستودع S3، ومفاتيح الوصول إلى AWS الخاص بك، ومفاتيح AWS السري الخاص بك، والدليل البعيد (على الأرجح DNSLOG ولكن يعتمد على الإعداد الخاص بك). يمكن أن تساعد إضافة معرف مصدر السجل مثل السنة في تصفية السجلات بحيث يتم سحب السجلات التي تحتوي على "2019" فقط.

4. قم بإنشاء LSX (سجل مصدر eXtension) الذي يمكن أن يعرب أحداث Cisco Umbrella. (هذا مدبدب عليه بعد الاستيراد إلى QRadar.) يمكن العثور على مزيد من المعلومات حول كيفية إنشاء LSX بالضبط على موقع IBM على الويب. هذا مجرد مثال. تختلف البيانات التي تريد سحبها من السجلات حسب حالة الاستخدام.

5. تحقق مرتين من نسخ مفاتيح الوصول إلى AWS ومفاتيح AWS السري بنجاح ولصقها في تكوين مصدر السجل.

6. حدد معالج GZIP ومودل حدث للخط المتعدد القائم على RegEx. أسهل طريقة للحصول على حدث واحد لكل خط هي باستخدام نمط بدء RegEx ل:

```
("\d{4}-\d{2}-\d{2}\s\d{2}:\d{2}:\d{2}:\d{2}"،)
```

تأكد من تحديد امتداد مصدر السجل وشرط الاستخدام، ثم احفظ مصدر السجل.

7. إجراء عملية نشر كاملة في QRadar.

ثم أستخدم مصدر السجل الخاص بك RestAPI للاتصال بالدلو الخاص بك باستخدام بيانات الاعتماد والمفاتيح التي قمت بتوفيرها وبدء تشغيل الأحداث.

معلومات إضافية

تمكين تسجيل الدلو

لتمكين تسجيل الدلو، اقرأ وثائق AWS أو كمل الإجراءات المحددة. بشكل افتراضي، يتم تعطيل التسجيل. بمجرد تمكينها، يوجد مجلد جديد يسمى /log في جذر الدلو الخاص بك لإظهار معلومات GET و PUT و DELETES لك.

إدارة دورة السجل

عند إستخدام S3، يمكنك إدارة دورة حياة البيانات داخل المستودع لتمديد الفترة الزمنية التي تريد الاحتفاظ بالسجلات الخاصة بها. اعتمادا على الغرض من إستخدام إدارة السجل الخارجي له، يمكن أن تكون المدة قصيرة جدا أو طويلة جدا. على سبيل المثال، يمكنك ببساطة تنزيل السجلات من دلو S3 بعد 24 ساعة وتخزينها دون اتصال، أو الاحتفاظ بالسجلات إلى أجل غير مسمى في السحابة.

وبشكل افتراضي، تخزن شركة Amazon البيانات في دلو إلى أجل غير مسمى، ولكن التخزين غير المحدود يؤدي إلى رفع تكلفة صيانة الدلو. لمزيد من المعلومات حول دورات حياة S3، الرجاء قراءة وثائق AWS.

لتهيئة دورة حياة دلو الخاص بك:

1. حدد خصائص > دورة الحياة.

2. حدد إضافة قاعدة، ثم قم بتطبيق القاعدة على الدلو بأكمله (أو مجلد فرعي إذا قمت بتكوينه على هذا النحو).

3. حدد إجراء على الكائنات، مثل حذف أو أرشفة، ثم حدد الفترة الزمنية وما إذا كنت تريد إستخدام تخزين النهر الجليدي للمساعدة في تقليل تكاليف Amazon. (الأنهار الجليدية هي وحدات تخزين "بارد" غير متصلة بالإنترنت، والتي، رغم كونها أبطأ من حيث الوصول إليها، إلا أنها أقل تكلفة).

إذا كنت تفضل إدارة السجلات بطريقة أخرى (على سبيل المثال، على حل النسخ الاحتياطي الداخلي الخاص بك)، يمكنك ببساطة تنزيل السجلات من S3 والاحتفاظ بها بطريقة أخرى.

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).