配置与Umbrella日志管理和S3的QRadar集成

目录

简介

本文档介绍如何将QRadar配置为从AWS S3存储桶中接收日志以进行Umbrella日志管理。

先决条件

要求

Cisco 建议您了解以下主题：

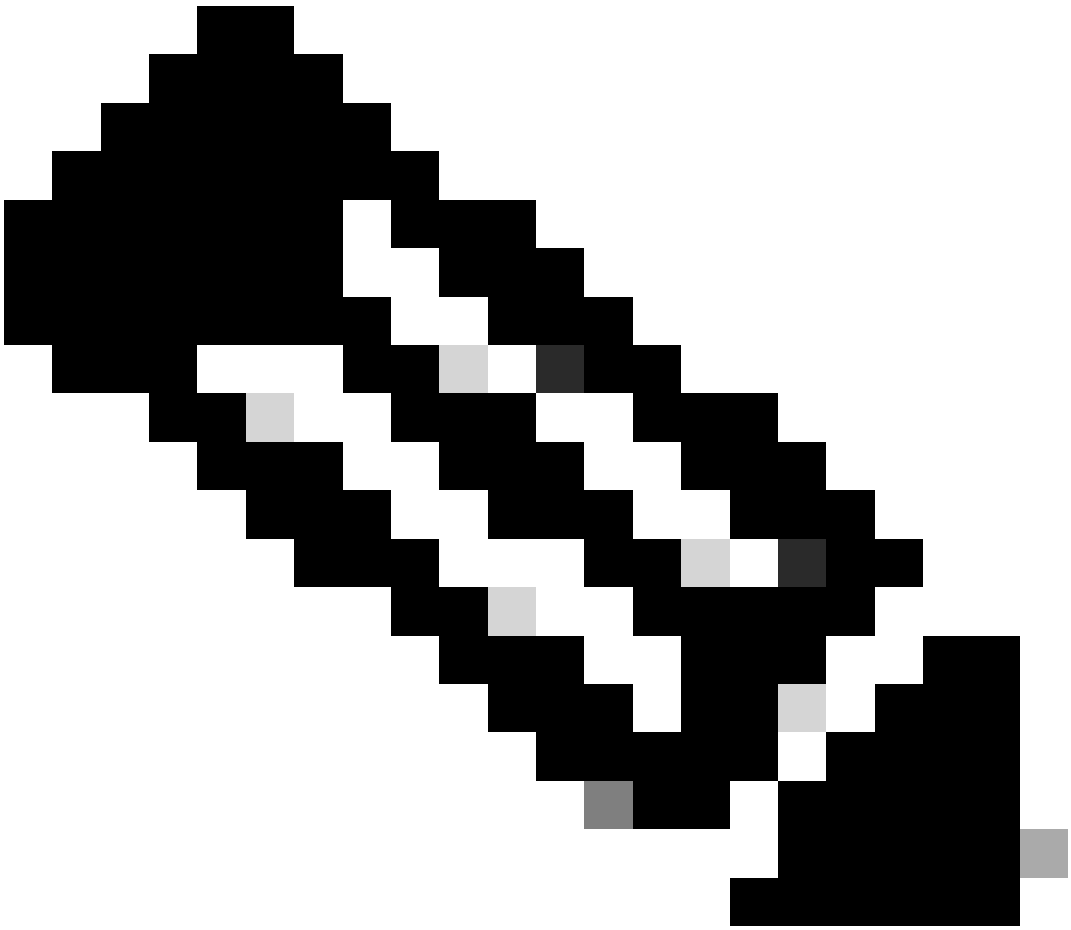
- 本文档假设您的Amazon AWS S3存储桶已在Umbrella(Settings > Log Management)中配置，并且显示绿色且最近日志已上传。有关如何配置此功能的详细信息，请阅读以下文章：从AWS S3中的Umbrella Log Management下载日志
- 除了对QRadar设备、Amazon S3配置和Umbrella控制面板的管理权限之外，这些说明假设QRadar管理员熟悉创建LSX（日志源扩展）文件。

使用的组件

本文档中的信息基于Cisco Umbrella。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述



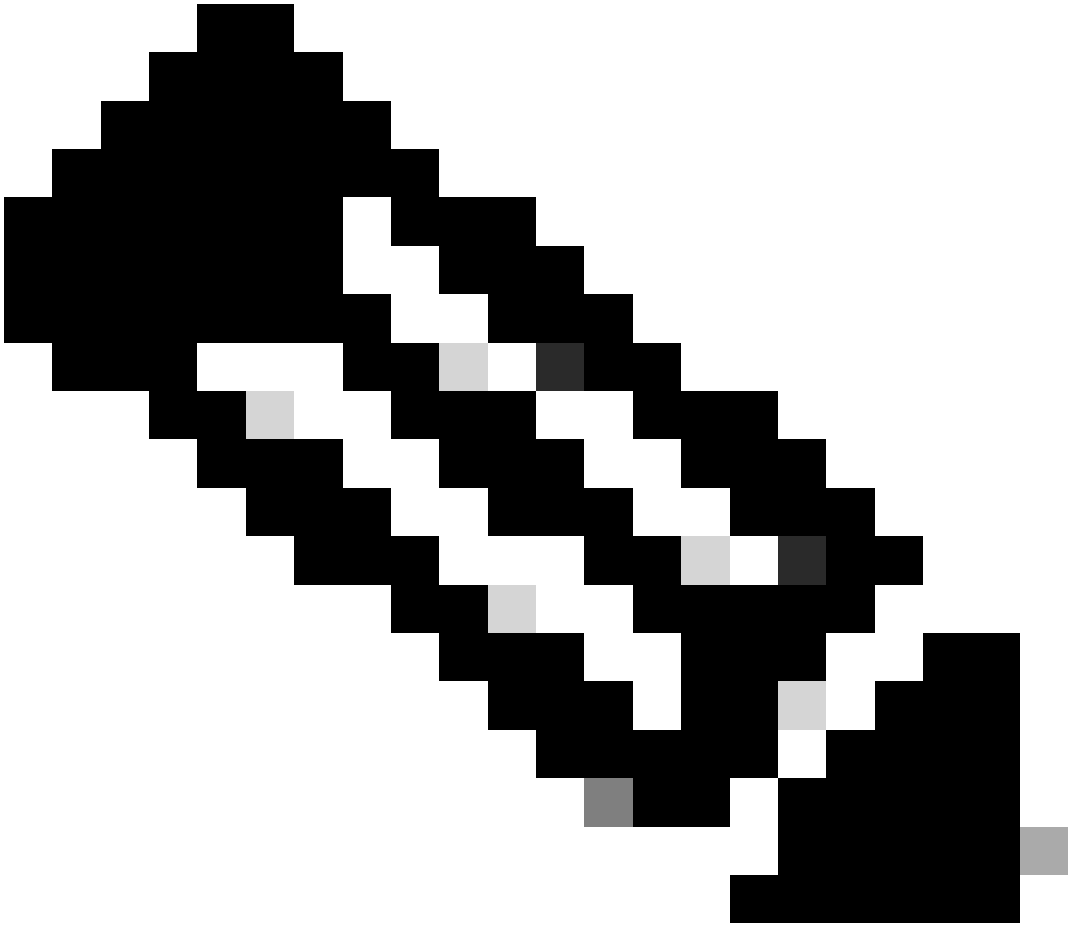
> 注意：配置QRadar以与Cisco Umbrella配合使用的最佳方法是通过思科云安全应用。只有在无法配置应用时才能继续使用此方法。

IBM的QRadar是常用的日志分析SIEM。它提供强大的接口来分析大数据块，例如Cisco Umbrella为您的组织的DNS流量提供的日志。

这篇文章概括介绍了如何设置QRadar并运行QRadar，以便它能够从S3存储桶提取日志并使用这些日志。主要分为两个阶段：

- 配置AWS S3安全凭证，以允许QRadar访问日志。
- 将QRadar本身配置为指向您的存储桶。

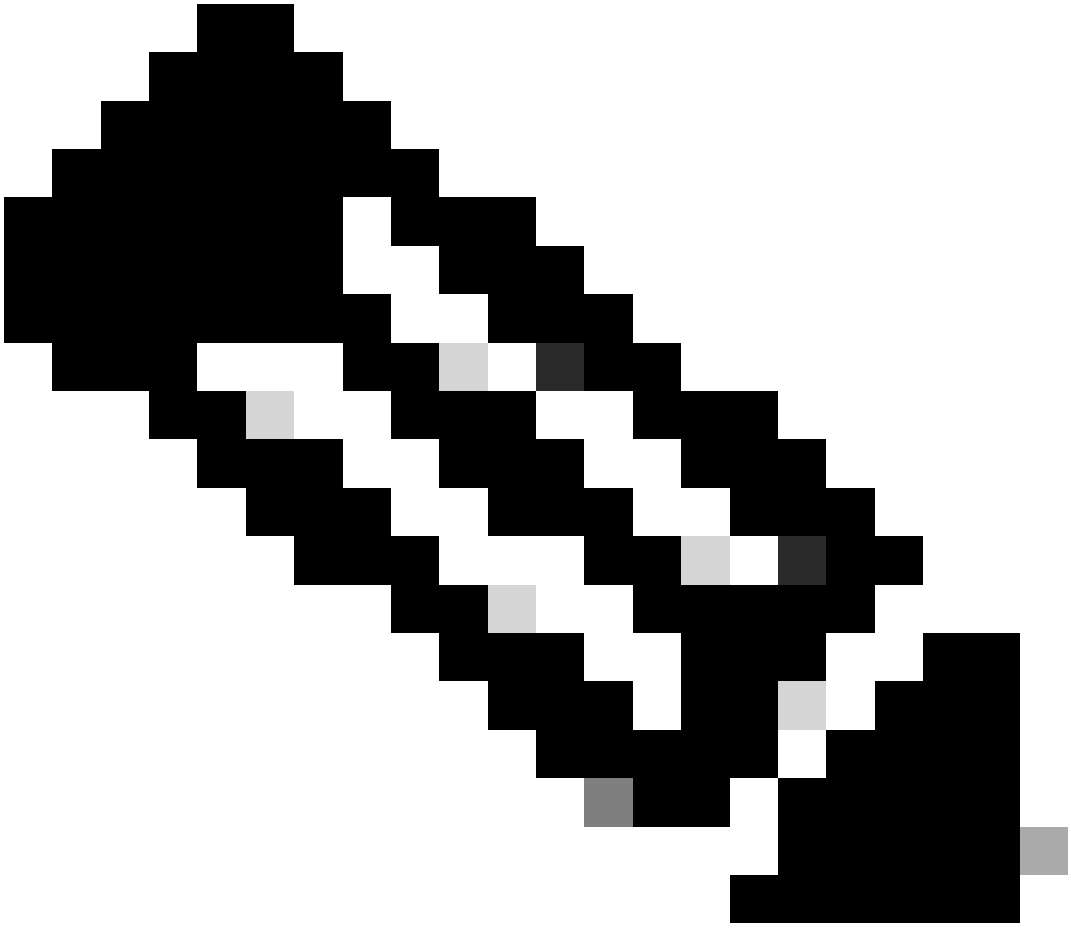
如果您使用的是思科托管的S3存储桶，请使用使用AWS CLI从Umbrella日志管理下载日志文章中的这些说明。



注意：此集成已经过客户管理的S3存储桶和思科管理的S3存储桶的测试。本文讨论的信息自撰写本文时起（2019年10月），可以根据QRadar和AWS Services接口的方式进行更改。本文档为活文档。如果您有反馈或找到了可以帮助其他客户的技巧或提示，请联系Cisco Umbrella支持。

对QRadar的支持必须来自IBM，因为思科无法直接支持第三方硬件或软件。对于将Umbrella控制面板连接到S3存储桶的任何问题，Cisco Umbrella都可以提供支持。本文中的许多信息也可在IBM网站上找到。

第 1 阶段：在AWS中配置安全凭证



注意：这些步骤与介绍如何配置工具从存储桶下载日志的文章中概述的步骤相同(从AWS S3中的Umbrella日志管理下载日志)。如果您已经执行这些步骤，则可以跳到阶段2，尽管以后需要来自IAM用户的安全凭证来将QRadar验证到存储桶。

第 1 步

1.向您的Amazon Web Services帐户添加访问密钥，以允许远程访问您的本地工具，并允许上传、下载和修改S3中的文件：

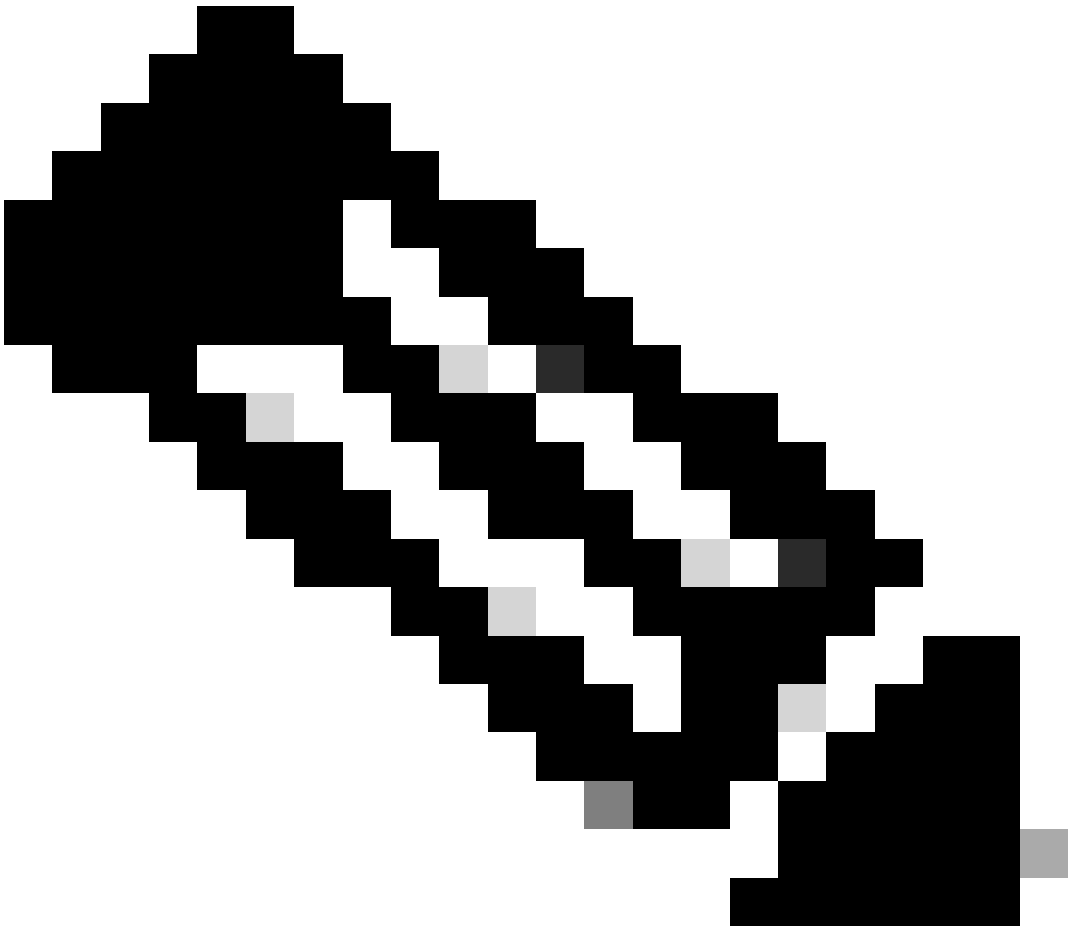
1. 登录AWS。
2. 在右上角选择您的帐户名称。
3. 在下拉列表中，选择Security Credentials。

2.然后系统会提示您使用Amazon最佳实践并创建AWS Identity and Access Management(IAM)用户。实质上，IAM用户会确保s3cmd用于访问存储桶的帐户不是整个S3配置的主帐户（例如，您的帐户）。通过为访问您帐户的用户创建单个IAM用户，您可以为每个IAM用户提供一组唯一的安全凭据。您也可以向每个IAM用户授予不同的权限。如有必要，您可以随时更改或撤消IAM用户的权限。有

关IAM用户和AWS最佳实践的更多信息，请参阅AWS文档。

第 2 步

1.选择IAM用户入门以创建一个IAM用户以访问您的S3存储桶。然后，您将进入一个屏幕，您可以在其中创建IAM用户。
2.选择新用户，然后填写字段。



注意：用户帐户不能包含空格。

3.创建用户帐户后，您只有一次机会获取包含Amazon User Security Credentials的两个重要信息。Umbrella强烈建议您使用右下方的按钮下载这些信息，以便进行备份。在设置中的此阶段之后，它们不可用。请确保记录您的访问密钥ID和秘密访问密钥，因为在后面的步骤中需要它们。

第 3 步

接下来，为IAM用户添加策略，以便他们能够访问您的S3存储桶：

1.选择刚创建的用户，然后向下滚动浏览用户的属性，直到您看到Attach Policy按钮。

2.选择Attach Policy，然后在策略类型过滤器中输入“s3”。这显示了两个结果：

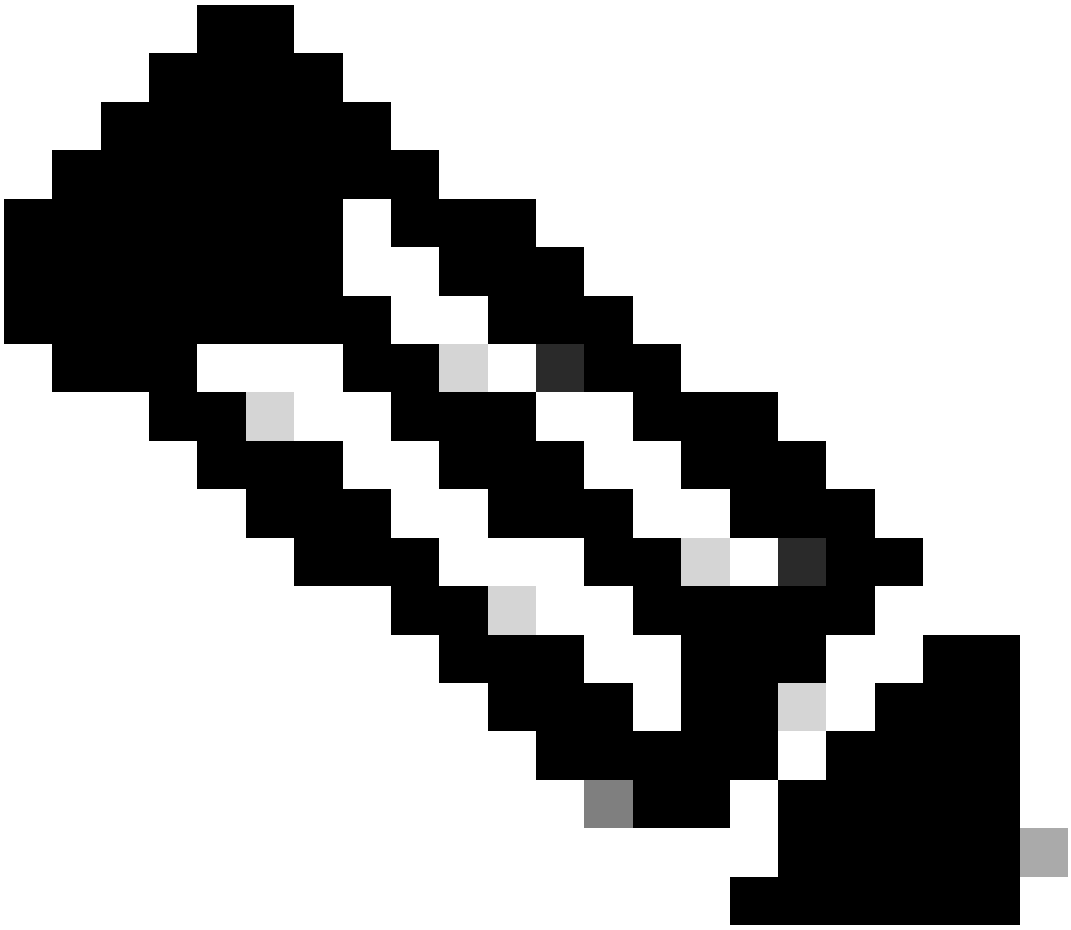
- AmazonS3FullAccess
- AmazonS3只读访问

3.选择AmazonS3FullAccess，然后选择右下角的Attach Policy。

第 2 阶段:设置QRadar以从S3存储桶中提取DNS日志数据

QRadar使用AWS CloudTrail服务，该服务是一种Web服务，可记录您账户的AWS API调用并向您传送日志文件。

在QRadar访问Amazon S3之前，请从IBM完成此过程以获取Amazon服务器证书。此部分比较困难，因此请确保您正确完成说明。



注意：在测试中，必须使用Firefox浏览器才能使此操作按预期工作。

要获取Amazon服务器证书，您必须将DER格式的证书移动到正确的QRadar设备。需要证书的QRadar设备是在Amazon AWS CloudTrail日志源的Target Event Collector字段中分配的设备。

开始使用前

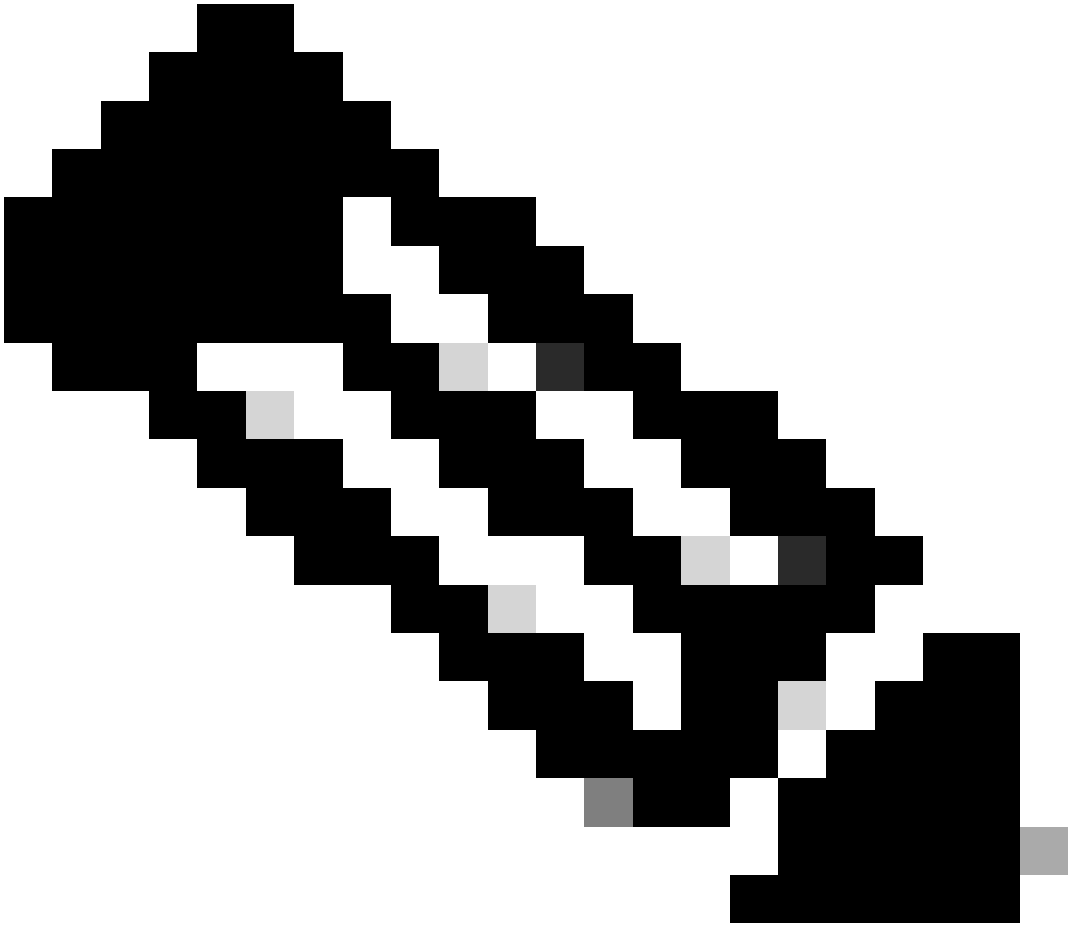
- 证书必须是.DER格式。
- 扩展名.DER区分大小写，并且必须是大写。
- 如果证书以小写形式导出，则日志源可能会遇到事件收集问题。

初始步骤

1.访问您的AWS CloudTrail S3存储桶:`https://<bucketname>.s3.amazonaws.com`

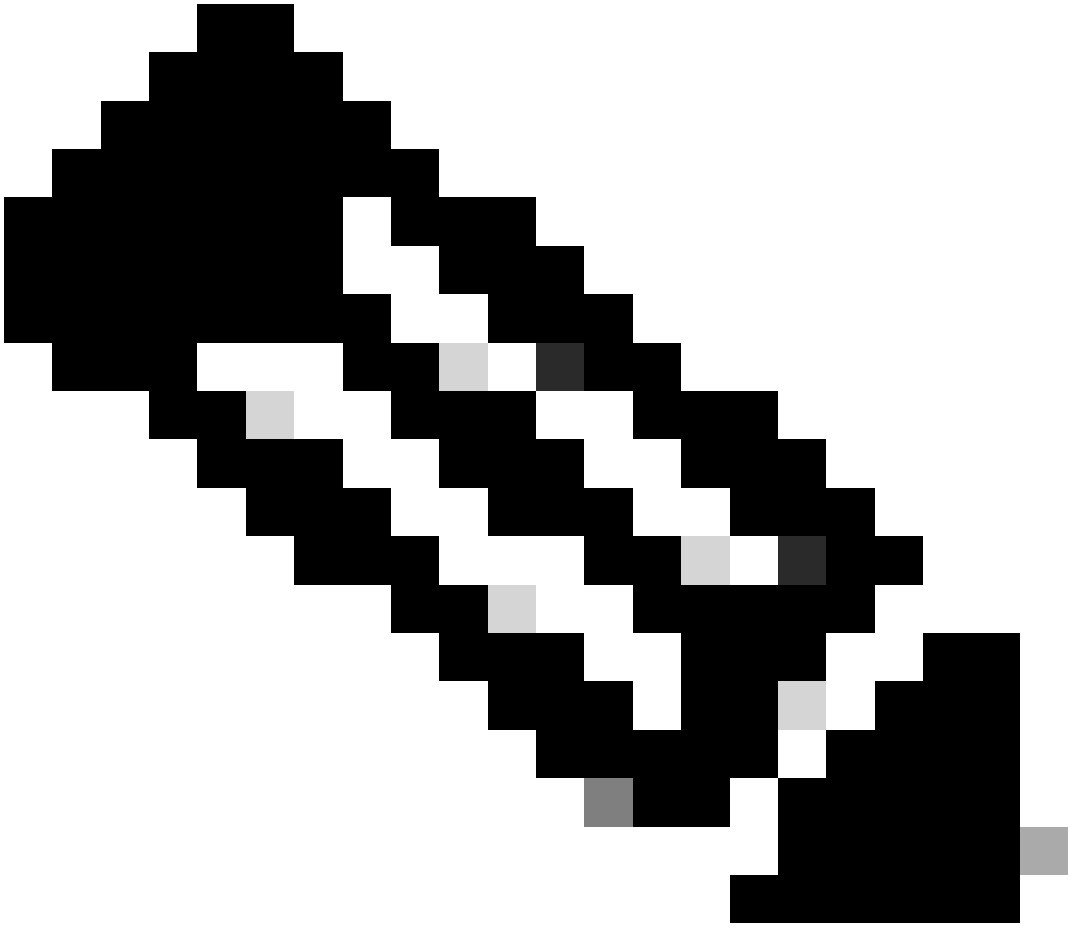
2.使用Firefox从AWS导出SSL证书作为(.DER)证书。Firefox可以创建带有.DER扩展名的所需证书：

1. 选择Site Identity图标（地址栏中的锁定图标）。
2. 选择More Information > View Certificate，然后选择Details选项卡。
3. 选择Export以证书.DER格式导出。



注意：.DER扩展名区分大小写，并且必须是大写。

3.将.DER证书复制到管理Amazon AWS CloudTrail日志源的QRadar设备的/opt/QRadar/conf/trusted_certificates目录。您可以使用WinSCP复制它。



注意：管理日志源的QRadar设备由Amazon AWS CloudTrail日志源中的Target Event Collect字段标识。管理Amazon AWS CloudTrail日志源的QRadar设备必须具有/opt/QRadar/conf/trusted_certificates中的.DER证书副本。

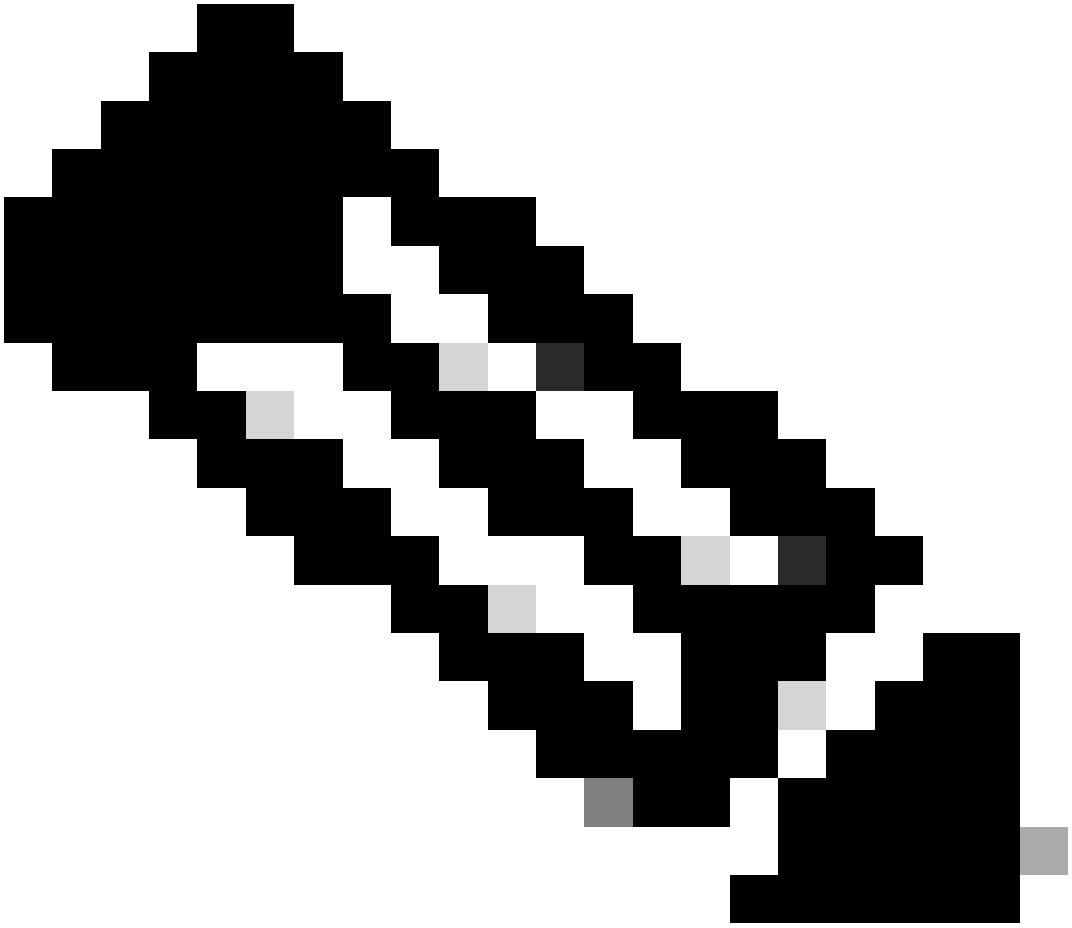
4.以管理用户身份登录QRadar用户界面。

5.选择Admin选项卡。

6.选择“日志源”图标。

7.选择Amazon AWS CloudTrail日志源。

8.在导航菜单中，选择Enable/Disable以禁用，然后重新启用Amazon AWS CloudTrail日志源。



注意：当管理员强制将日志源从禁用转为启用时，该协议允许协议连接到日志源中定义的Amazon AWS存储桶。然后，在第一次通信过程中进行证书检查。

9.如果您继续遇到问题，请验证“日志源标识符”(Log Source Identifier)字段是否包含正确的Amazon AWS存储桶名称，以及日志源配置中的远程目录路径是否正确。

完成QRadar配置

1.在QRadar中，确保所有协议、DSM和其他信息都是最新的。选择带有这些配置的LogFileProtocol（频率、开始时间、重复周期和其他信息可以不同）。

2.在日志源标签中，输入日志源名称和日志源说明。你可以随便吃。

3.输入您的S3 Bucket Name、您的AWS Access Key、您的AWS Secret Key和Remote Directory（可能为dnslogs，但取决于您的设置）。 添加日志源标识符（如年份）可帮助过滤，因此仅提取其中包含“2019”的日志。

4.创建可以分析Cisco Umbrella事件的LSX（日志源扩展）。（这是导入QRadar后显示的内容。

）有关如何创建LSX的详细信息，请访问IBM网站。这只是一个例子。要从日志提取的数据因使用案例而异。

5.仔细检查您的AWS访问密钥和AWS密钥是否已成功复制并粘贴到日志源配置中。

6.选择基于RegEx的多线路的GZIP处理器和事件生成器。每行获取一个事件的最简单方法是使用以下启动模式RegEx:

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

确保选择“日志源扩展”和“使用条件”，然后保存日志源。

7.在QRadar中执行完全部署。

然后，您的日志源使用RestAPI使用您提供的凭证和密钥连接到存储桶，并开始提取事件。

Additional Information

启用桶记录

要启用桶记录，请阅读AWS文档并完成概述的程序。默认情况下，日志记录处于禁用状态。启用后，一个名为/logs的新文件夹将驻留在存储桶根中，以显示GETS、PUTS和DELETES的信息。

管理日志周期

使用S3时，您可以管理存储桶中数据的生命周期，从而延长希望保留日志的时间。根据您使用外部日志管理的目的，持续时间可能非常短或非常长。例如，您可以在24小时后从S3存储桶下载日志并脱机存储，或者无限期地在云中保留日志。

默认情况下，Amazon将数据无限期存储在存储桶中，但无限存储确实提高了存储桶维护成本。有关S3生命周期的更多信息，请阅读AWS文档。

要配置存储桶的生命周期，请执行以下操作：

1.选择“属性”>“生命周期”。

2.选择Add a Rule，然后选择Apply the Rule至整个存储桶（或子文件夹，如果进行了相应配置）。

3.选择对对象执行的操作，如Delete或Archive，然后选择时间段，以及是否要使用Glacier存储来帮助降低Amazon成本。（Glacier是“冷”离线存储，虽然访问速度较慢，但成本要低得多。）

如果您喜欢使用其他方法（例如，在您的内部备份解决方案上）管理日志，则只需从S3下载日志并以其他方式保留它们即可。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。