使用自我管理的S3存储桶配置Splunk

目录

简介

本文档介绍如何使用自我管理的S3存储桶配置Splunk。

概述

Splunk是日志分析的常用工具。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Splunk并运行Splunk，以便从S3存储桶中提取日志并使用它们。有两个主要阶段，一个是配置您的AWS S3安全凭证，以允许Splunk访问日志，另一个是配置Splunk自身以指向您的存储桶。

此处提供了AWS S3的Splunk加载项的文档，其中一些已逐字复制到本文档中。有关Splunk设置的具体问题，请参阅http://docs.splunk.com/Documentation/AddOns/latest/AWS/Description

本文包含以下部分：

- 先决条件
- 第 1 阶段：在AWS中配置您的安全凭证（仅限自管理存储桶）
- 第 2 阶段: 设置Splunk以从S3存储桶中提取DNS日志数据
  - 步骤 1：设置Splunk以从自我管理的S3存储桶提取DNS日志数据
- 第 3 阶段:配置Splunk的数据输入

先决条件

Splunk Add-on for Amazon Web Services支持这些平台。

- AWS Linux
- RedHat
- Windows 2008R2、2012R2

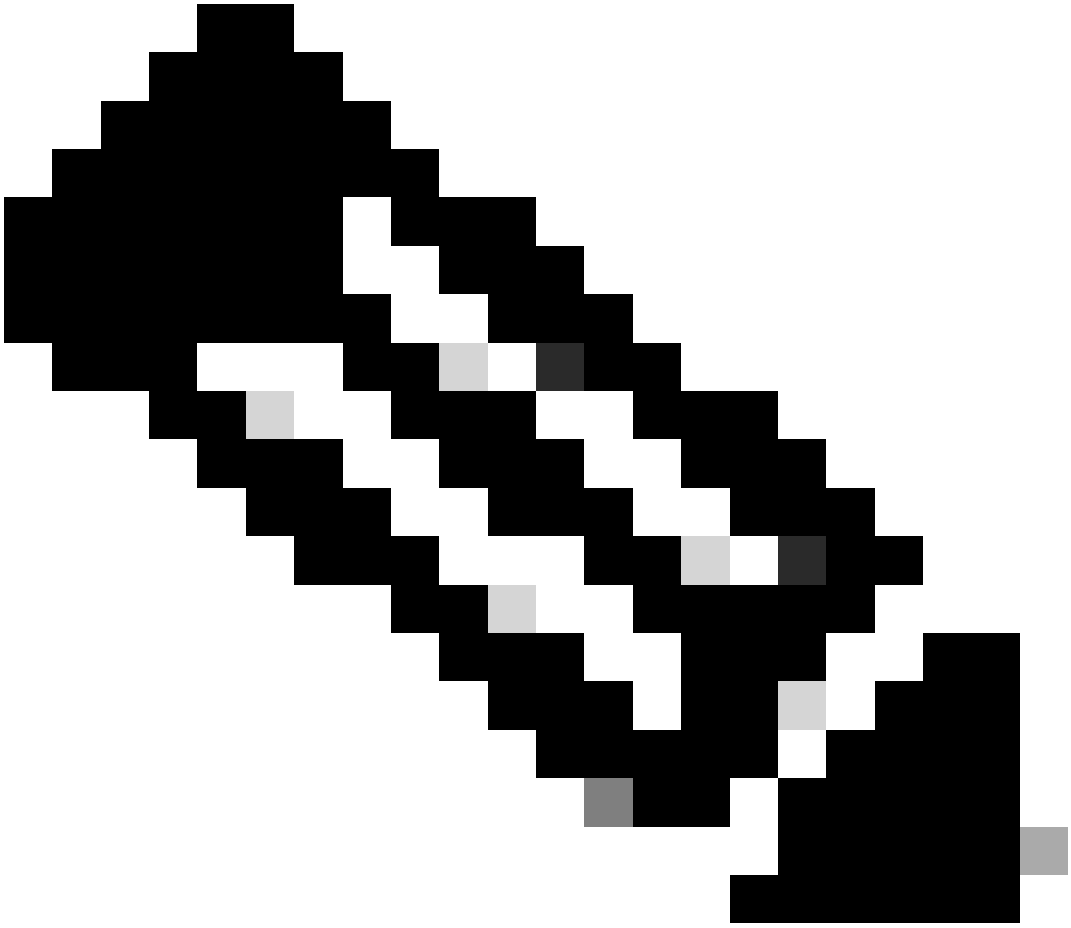
Splunk企业系统要求

由于此附加组件在Splunk Enterprise上运行，所有Splunk Enterprise系统要求都适用。请参阅Splunk Enterprise文档中的“系统要求”安装手册。这些说明适用于Splunk Enterprise版本6.2.1。

总括要求

本文档假设您的Amazon AWS S3存储桶已在Umbrella控制面板（管理>日志管理）中配置，并且显示绿色且已上传最近的日志。有关日志管理的详细信息，请参阅Amazon S3中的Cisco Umbrella日志管理。

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(如何：从Cisco Umbrella Log Management(AWS S3)下载日志。 如果您已经执行这些步骤，则可以直接跳到步骤2，尽管您需要来自IAM用户的安全凭证来验证存储桶的Splunk插件。

第 1 步

1. 向Amazon Web Services帐户添加访问密钥，以允许远程访问您的本地工具，并能够上传、下载和修改S3中的文件。登录AWS，点击右上角的帐户名称。在下拉列表中，选择Security Credentials。
2. 系统将提示您使用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，请阅读此处
   ：https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

第 2 步

1. 通过点击IAM Users入门创建一个IAM用户以访问您的S3存储桶。 您将进入一个屏幕，您可以在其中创建IAM用户。
2. 单击Create New Users，然后填写字段。请注意，用户帐户不能包含空格。
3. 创建用户帐户后，您仅有机会获取包含Amazon用户安全凭据的两个重要信息。我们强烈建议您使用右下方的按钮下载这些信息，以对其进行备份。在设置中的此阶段之后，它们不可用。确保您记下访问密钥ID和秘密访问密钥，因为稍后设置Splunk时需要它们。

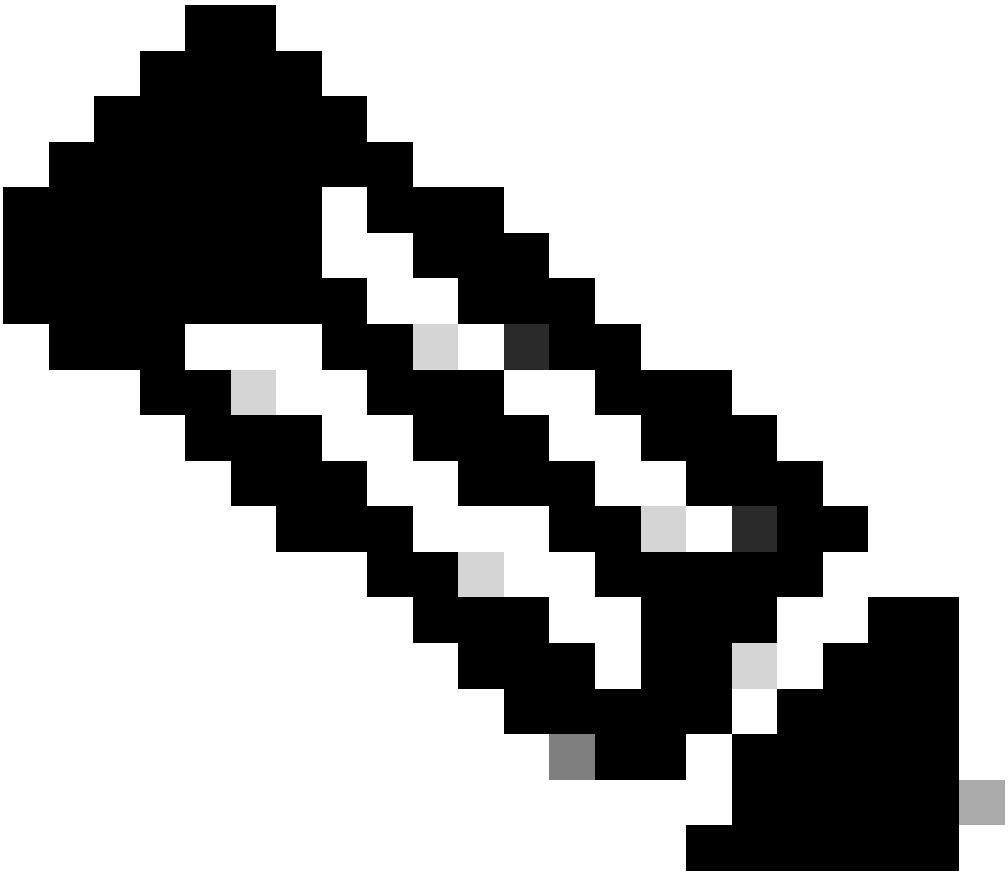
第 3 步

1. 接下来，您要为IAM用户添加策略，以便他们能够访问您的S3存储桶。点击您刚刚创建的用户，然后向下滚动浏览用户的属性，直到您看到Attach Policy（附加策略）按钮。
2. 单击Attach Policy，然后在策略类型过滤器中输入“s3”。这显示了两个结果：“Amazon S3FullAccess”和“Amazon S3ReadOnlyAccess”。
3. 选择AmazonS3FullAccess，然后单击Attach Policy。

第 2 阶段:设置Splunk以从S3存储桶中提取DNS日志数据

第1步：设置Splunk以从自我管理的S3存储桶提取DNS日志数据

1. 首先将“Splunk Add-on for Amazon Web Services”安装到您的Splunk实例中。打开您的Splunk控制面板并单击Apps，或者单击Splunk Apps（如果它出现在控制面板上）。进入Apps部分后，在搜索窗口中键入“s3”以查找“Splunk Add-on for Amazon Web Services”，然后安装应用。



注意：您可能需要在安装期间重新启动Splunk。
安装后，您会看到Splunk Add-on for AWS，文件夹名称为“Splunk_TA_aws”，现在列在Apps下。

2. 单击Set up配置应用。此时需要本文档第1阶段的安全凭证。
设置要求输入以下字段：

- 友好名称 — 用于引用此集成的名称
- 您的AWS账户密钥ID（来自阶段1）
- 您的密码（您的AWS账户密钥，也来自阶段1）

如果Splunk需要访问AWS，您还可以设置任何本地代理信息，以及调整日志记录。设置屏幕如下所示：
3.添加相关信息后，单击Save，即可完全配置用于Amazon Web Services的Splunk Add-on。

第 3 阶段:配置Splunk的数据输入

1. 接下来，您要配置Amazon Web Services S3的数据输入。导航到设置>数据>数据输入，在Local Inputs下，您现在会看到各种Amazon输入的列表，包括列表底部的S3。

2. 单击AWS S3配置输入。
3. 点击 New（新建）。
4. 您需要提供以下信息：

   - 输入您的S3集成的友好名称。
   - 选择您的 下拉菜单中的AWS账户。这是您在步骤1中提供的友好名称。
   - 从下拉列表中选择您的S3存储桶。这是在Umbrella控制面板（“设置”>“日志管理”）中指定的桶名称。
   - 从下拉列表中选择S3密钥名称。您存储桶中的每个项目都会列出，我们建议选择顶级目录\dns-logs\ ，其中包括其下的所有文件和目录。
   - “消息系统配置”下有几个选项，我们建议保留这些设置 — 默认设置。
   - “More settings”下还有其他选项。 请注意，“源类型”默认为aws:s3。我们建议保持原样，但是如果您进行了更改，则“搜索”中您日志的过滤器将从这些说明的第3步所述内容更改。

填写详细信息，您的数据输入看起来与以下内容类似：

4.单击下一步完成您的详细信息。
系统将显示一个屏幕，显示输入已成功创建

第 3 步

执行快速搜索，查看您的数据是否正确导入。只需将sourcetype="aws:s3" 粘贴到右上角的“搜索”窗口中，然后在搜索中选择“Open sourcetype="aws:s3”

这会将您引导至类似于您从组织的DNS日志中查看事件的屏幕。在这里，Cisco Umbrella移动服务正在阻止iPhone上的社交媒体。您还可以使用文件名的源文件过滤特定批日志。

此后，后台的cron作业将继续运行，并从存储桶中的日志信息提取最新集。

除了本文中介绍的内容，您还可以对Splunk执行更多操作。如果您有机会在自己的安全响应程序中使用这些数据，我们很想收到您的反馈。请将任何反馈、问题或疑问发送到umbrella-support@cisco.com，并参考本文档。

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）。