使用自行管理的S3儲存桶配置Splunk

目錄

簡介

本文檔介紹如何使用自管理的S3儲存桶配置Splunk。

概觀

Splunk是日誌分析的常用工具。它提供強大的介面來分析大量資料，例如Cisco Umbrella為您的組織的DNS流量提供的日誌。

這篇文章概括介紹了如何設定Splunk並運行，以便它能夠從S3儲存桶提取日誌並使用它們。有兩個主要階段，一個是配置AWS S3安全憑證，以允許Splunk訪問日誌，另一個是將Splunk本身配置為指向您的儲存桶。

此處提供了AWS S3的Splunk附加模組的文檔，其中有些文檔已逐字複製到本文檔中。有關Splunk設定的具體問題，請參閱
http://docs.splunk.com/Documentation/AddOns/latest/AWS/Description

本文包含以下部分：

- 必要條件
- 階段1:在AWS中配置您的安全憑證（僅限自管理儲存桶）
- 階段2: 設定Splunk以從S3儲存桶提取DNS日誌資料
    - 步驟 1:設定Splunk以從自我管理的S3儲存桶提取DNS日誌資料
- 階段3:為Splunk配置資料輸入

必要條件

Splunk Add-on for Amazon Web Services支援這些平台。

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

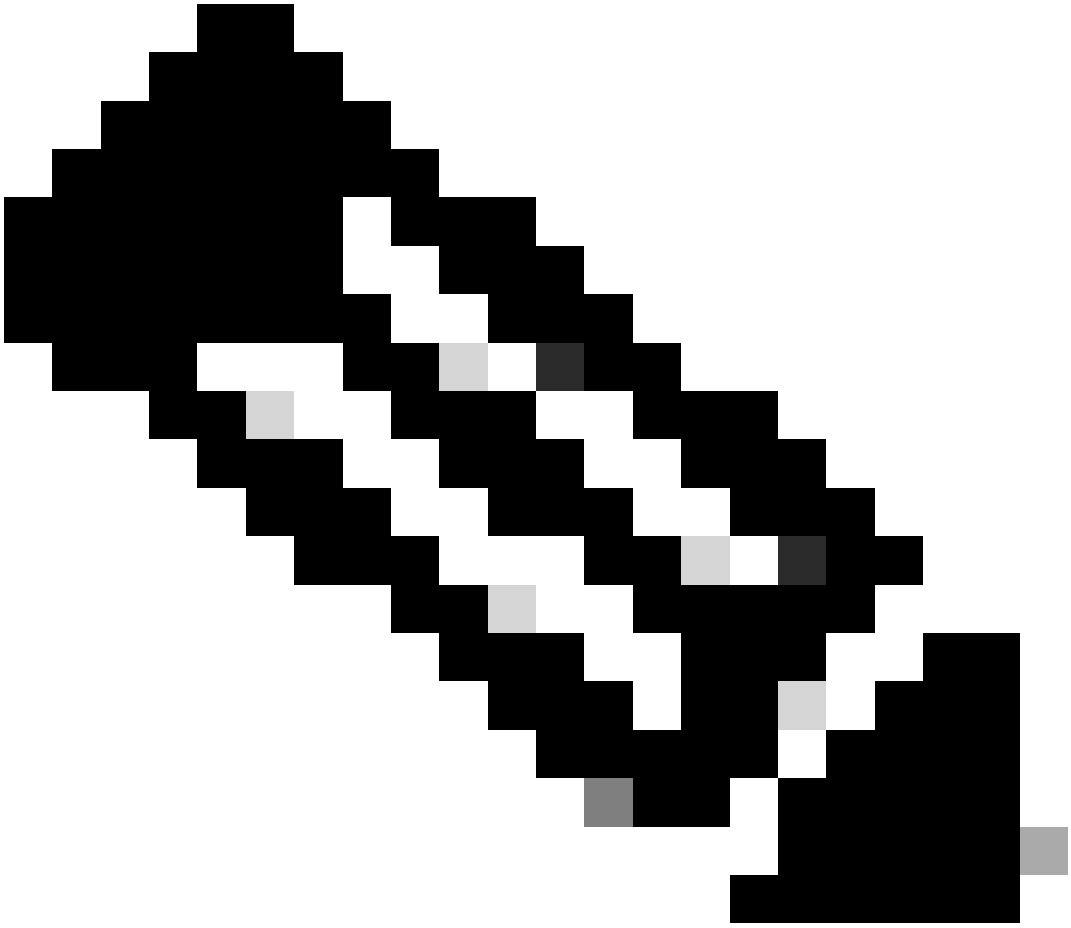
Splunk企業系統要求

由於此附加模組在Splunk Enterprise上運行，因此所有Splunk Enterprise系統要求都適用。請參閱Splunk Enterprise文檔中的「系統要求」安裝手冊。這些說明適用於Splunk Enterprise版本6.2.1。

Umbrella要求

本文檔假設您的Amazon AWS S3儲存桶已在Umbrella控制面板（管理>日誌管理）中配置，並且顯示綠色且已上傳最近的日誌。有關日誌管理的詳細資訊，請參閱Amazon S3中的Cisco Umbrella Log Management。

階段1:在AWS中配置您的安全憑證



附註：這些步驟與描述如何配置工具從儲存桶下載日誌的文章中概述的步驟相同(如何：從AWS S3)中的Cisco Umbrella Log Management下載日誌。 如果您已經執行這些步驟，則可以直接跳到步驟2，儘管您需要來自IAM使用者的安全憑證來驗證儲存桶的Splunk外掛。

步驟 1

1. 為您的Amazon Web Services帳戶新增訪問金鑰，以允許遠端訪問您的本地工具，並讓您能夠上傳、下載和修改S3中的檔案。登入到AWS，然後按一下右上角的帳戶名稱。在下拉選單中，選擇Security Credentials。
2. 系統將提示您使用Amazon Best Practices並建立AWS Identity and Access Management(IAM)使用者。實質上，IAM使用者會確保s3cmd用於訪問儲存桶的帳戶不是整個S3配置的主帳戶（例如，您的帳戶）。通過為訪問您帳戶的人員建立單個IAM使用者，您可以為每個IAM使用者提供一組唯一的安全憑據。您還可以向每個IAM使用者授予不同的許可權。如有必要，您可以隨時更改或撤消IAM使用者的許可權。
   有關IAM使用者和AWS最佳實踐的更多資訊，請閱讀此處：https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

步驟 2

1. 通過按一下IAM使用者入門，建立一個IAM使用者以訪問您的S3儲存桶。 您將進入一個螢幕，您可以在其中建立IAM使用者。
2. 按一下Create New Users，然後填寫欄位。請注意，使用者帳戶不能包含空格。
3. 建立使用者帳戶後，您只有一次機會獲取包含您的Amazon使用者安全憑據的兩個重要資訊。我們強烈建議您使用右下角的按鈕下載這些信息，以備份它們。在設定中的此階段之後，它們將不可用。 確保您在設定Splunk時記下訪問金鑰ID和秘密訪問金鑰，因為稍後我們會需要它們。

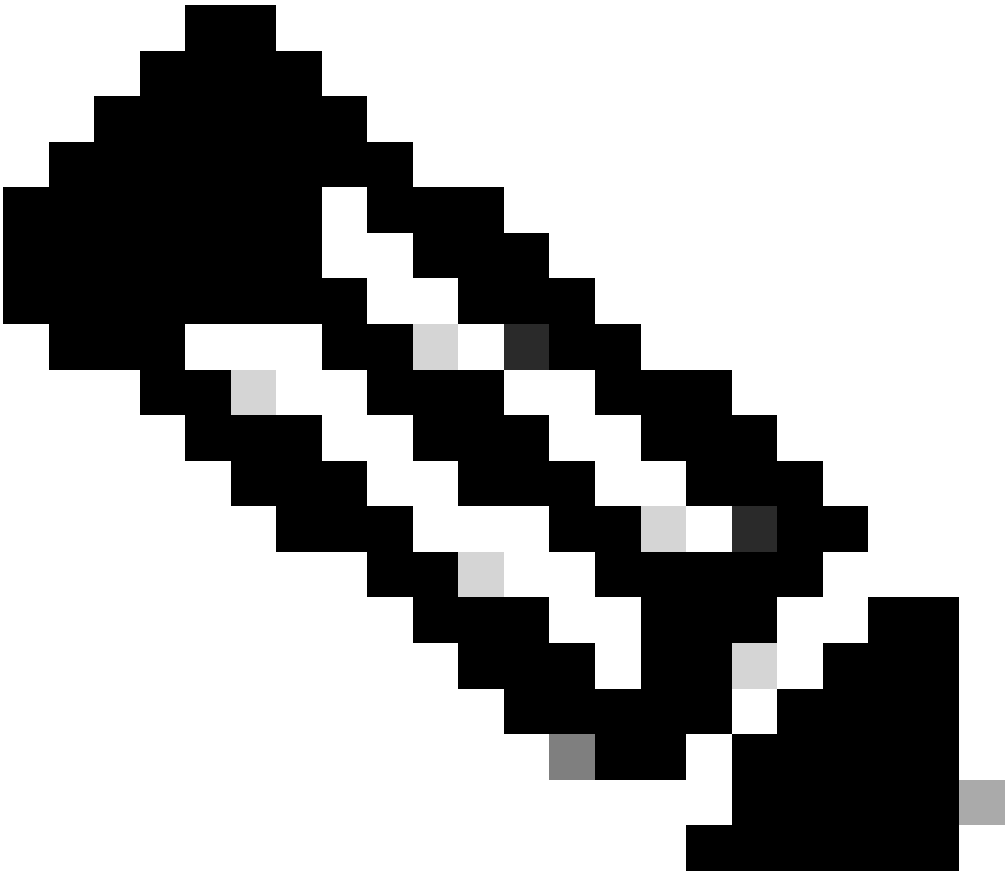
步驟 3

1. 接下來，您要為IAM使用者新增策略，以便他們能夠訪問您的S3儲存桶。按一下剛建立的使用者，然後向下滾動瀏覽使用者屬性，直到看到「Attach Policy（附加策略）」按鈕。
2. 按一下Attach Policy，然後在策略型別篩選器中輸入「s3」。這顯示了兩個結果：「AmazonS3FullAccess」和「AmazonS3ReadOnlyAccess」。
3. 選擇AmazonS3FullAccess，然後按一下Attach Policy。

階段2:設定Splunk以從S3儲存桶提取DNS日誌資料

第1步：設定Splunk以從自我管理的S3儲存桶提取DNS日誌資料

1. 首先將「Splunk Add-on for Amazon Web Services」安裝到您的Splunk例項。開啟你的Splunk儀表板，然後按一下Apps，如果儀表板上顯示，請按一下Splunk Apps。進入Apps部分後，在搜尋視窗中鍵入「s3」以查詢「Splunk Add-on for Amazon Web Services」，然後安裝該應用。



附註：安裝過程中可能需要重新啟動Splunk。
安裝後，您會看到Splunk Add-on for AWS，其資料夾名稱為「Splunk_TA_aws」，現在列在Apps下。

2. 按一下Set up以配置應用。這就是您需要從本文檔的第1階段獲得安全憑據的地方。
安裝程式要求輸入以下欄位：

- 友好名稱 — 用於引用此整合的名稱
- 您的AWS賬戶金鑰ID（來自階段1）
- 您的密碼（您的AWS賬戶金鑰，也來自階段1）

如果Splunk需要訪問AWS，您還可以設定任何本地代理資訊，以及調整日誌記錄。設定螢幕如下所示：
3.新增相關資訊後，按一下Save，即可完全配置Splunk Add-on for Amazon Web Services。

階段3:為Splunk配置資料輸入

1. 接下來，您要配置Amazon Web Services S3的資料輸入。導航到Settings > Data > Data Inputs，然後在Local Inputs下看到各種Amazon輸入清單，包括清單底部的S3。

2. 按一下AWS S3配置輸入。
3. 按一下New。
4. 您需要提供以下幾項資訊：

    - 輸入您的S3整合的友好名稱。
    - 選擇您的 下拉選單中的AWS賬戶。這是您在步驟1中提供的友好名稱。
    - 從下拉選單中選擇您的S3儲存桶。這是在Umbrella控制面板（「設定」>「日誌管理」）中指定的儲存段名稱。
    - 從下拉選單中選擇S3金鑰名稱。列出儲存桶中的每個專案，我們建議選擇頂級目錄\dns-logs\（包含其下的所有檔案和目錄）。
    - 在「消息系統配置」下有幾個選項，我們建議保留這些設定不變 — 預設設定。
    - 「More settings」下還有其他選項。 值得注意的是「Source type」，預設情況下為aws:s3。我們建議保持原樣，但是如果確實進行了更改，則搜尋中日誌的篩選器將從這些說明的第3步所述內容更改。

填寫詳細資訊，您的資料輸入看起來與以下內容類似：

4.按一下下一步完成您的詳細資訊。
系統將顯示一個螢幕，顯示輸入已成功建立

步驟 3

執行快速搜尋，檢視您的資料是否正被正確匯入。只需將sourcetype="aws:s3" 貼上到右上角的「搜尋」視窗中，然後在搜尋中選擇「Open sourcetype="aws:s3」

這將帶您進入一個類似於從中檢視組織DNS日誌中的事件的螢幕。在這裡，Cisco Umbrella移動服務正在阻止iPhone上的社群媒體。您還可以使用檔名的源根據特定日誌批進行過濾。

在此之後，後台的cron作業將繼續運行，並從儲存桶中的日誌資訊提取最新集合。

除了Splunk的簡要說明之外，您還有很多其他功能可以做。如果您有機會在自己的安全響應程式中嘗試使用這些資料，我們將非常期待您的反饋。請將任何反饋、問題或問題傳送至umbrella-support@cisco.com，並參考本文。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。