從AWS S3的Umbrella Log Management下載日誌

目錄

簡介

本文檔介紹如何從AWS S3中的Umbrella Log Management下載日誌。

概觀

一旦您設定並測試了Amazon S3中的日誌管理是否正常運行，您可能希望開始自動下載日誌並將其儲存在您的網路基礎設施中，以保留或使用（或同時使用）。

為此，我們概述了使用http://s3tools.org中的s3tools的方法。s3tools使用用於Linux或OS/X的s3cmd命令列實用程式。還有其他一些工具可以為Windows使用者實現類似的功能：

- 對於命令列工具，您可以在此處下載小型命令列可執行檔案。
- 如果您偏好圖形介面，請檢視S3瀏覽器(https://s3browser.com/)，不過由於圖形介面不可編寫指令碼以自動執行流程，因此我們並不介紹如何使用它。本文提供設定這兩個命令列工具的步驟。如果您願意，可以使用階段1中的資訊來配置s3browser應用程式。

首先為您打算使用的作業系統下載該工具。目前，我們只介紹用於OS/X和Linux的s3cmd ，儘管訪問儲存桶和下載資料的步驟對於Windows而言實際上是一樣的。

從此處的s3tools獲取安裝程式。

安裝程式不需要您安裝該程式即可運行命令列，因此只需解壓已下載的程式包即可。

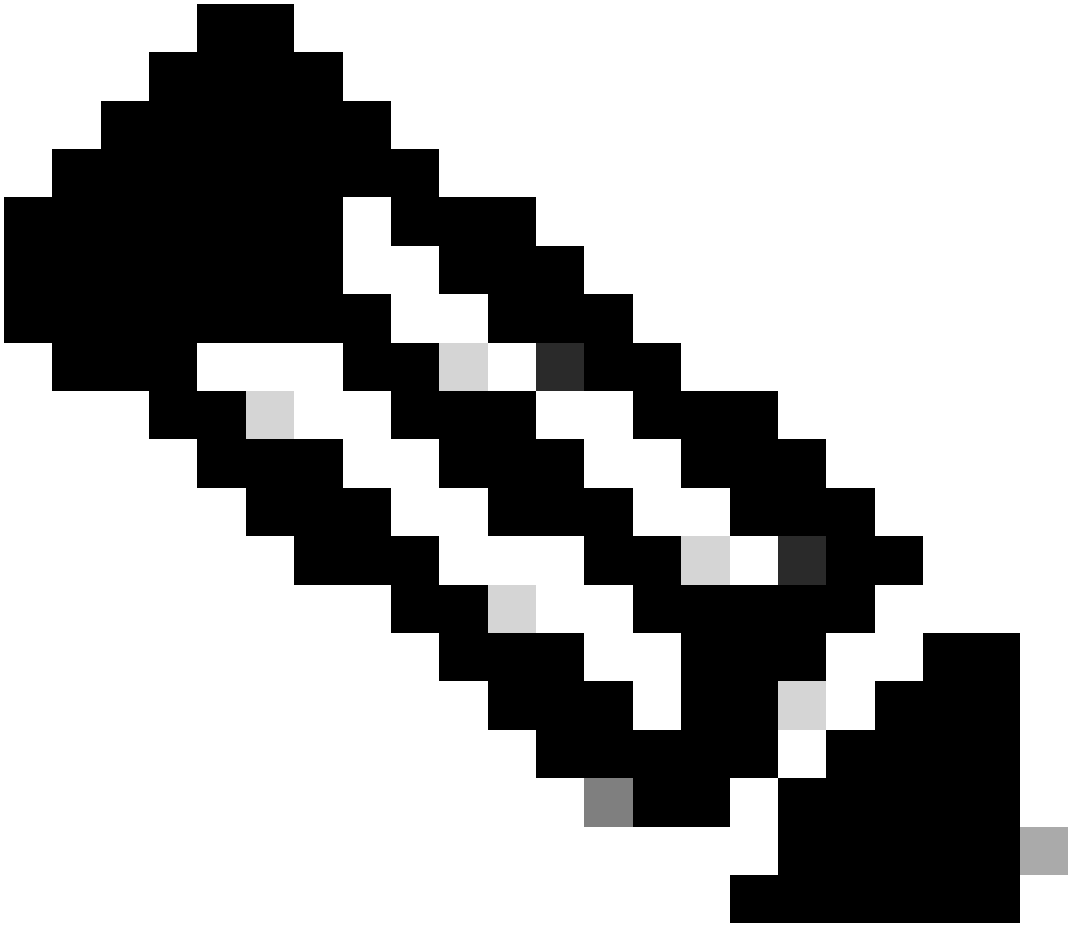
階段1:在AWS中配置您的安全憑證

步驟 1

1. 向Amazon Web Services帳戶新增訪問金鑰，以便遠端訪問您的本地工具，並能夠上傳、下載和修改S3中的檔案。登入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. 提示會指示您使用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。

步驟 2

1. 按一下IAM使用者入門，建立有權訪問S3儲存桶的IAM使用者。導航到可以建立IAM使用者的螢幕。
2. 按一下Create New Users並填寫欄位。
3. 建立使用者帳戶後，您只有一次機會獲取包含您的Amazon使用者安全憑證的兩個關鍵資訊。我們強烈建議您使用右下角的按鈕下載這些檔案，以便進行備份。在設定中的此階段之後，它們將不可用。請確保您記下訪問金鑰ID和秘密訪問密鑰，因為我們在後續步驟中需要它們。



附註：使用者帳戶不能包含空格。

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」。這應顯示兩個結果「AmazonS3FullAccess」和「AmazonS3ReadOnlyAccess」。
3. 選擇AmazonS3FullAccess，然後按一下Attach Policy。

階段2:配置工具從儲存桶下載DNS日誌

適用於MacOS和Linux的s3cmd

1. 轉至在上一個階段提取了s3cmd的路徑，然後在「終端」中鍵入：

```
./s3cmd --configure
```

這應該會提示您提供安全認證：

輸入新值或接受括弧中的預設值，然後輸入。

有關所有選項的詳細說明，請參閱使用者手冊。

訪問金鑰和金鑰是您的Amazon S3識別符號。留空它們以使用env變數。

Access Key [YOUR ACCESS KEY]:

金鑰[您的金鑰]:

2.接下來，您將被問到一系列有關如何配置對儲存桶的訪問許可權的問題。在這種情況下，我們不設定加密密碼(GPG)，也不使用HTTPS或代理伺服器。如果您的網路或首選項不同，請填寫必填欄位：

預設區域[US]:

加密密碼用於保護您的檔案在傳輸到S3時不被未經授權的人讀取

加密密碼：

GPG計畫的路徑[無]:

使用安全HTTPS協定時，與Amazon S3伺服器的所有通訊都受到保護，不會受到第三方竊聽。此方法是

比普通HTTP慢，且只能用Python 2.7或更新版本代理

使用HTTPS協定[否]:

在某些網路中，所有Internet訪問都必須通過HTTP代理。

如果無法直接連線到S3，請嘗試在此處進行設定

HTTP Proxy伺服器名稱：

輸入任何網路特定設定或任何加密後，您有機會檢查：

新設定：

訪問金鑰：您的金鑰

金鑰：您的金鑰

預設區域：美國

加密密碼：

GPG計畫的路徑：無

使用HTTPS協定：假

HTTP Proxy伺服器名稱：

HTTP代理伺服器埠：0

最後，您需要進行測試，如果成功，請儲存設定：

是否使用提供的憑據測試訪問許可權？[Y/n] y

請稍候，正在嘗試列出所有儲存桶……

成功。您的訪問金鑰和金鑰工作正常��

正在驗證加密是否有效……

未配置。算了。

儲存設定？[y/N]

Windows命令列執行檔(s3.exe)

下載工具(https://s3.codeplex.com/releases/view/47595)後，將.exe複製到您首選的工作資料夾，然後在命令提示符下鍵入以下內容，替換您的訪問金鑰和密碼：

<#root>

```
s3 auth [


        ]
```

有關驗證語法的詳細資訊，請閱讀此處。

階段3:測試從儲存桶下載檔案

步驟 1:測試下載

s3cmd for OS/X and Linux

從終端運行此命令，其中「my-organization-name-log-bucket」是已在Umbrella控制面板的「日誌管理」部分中配置的儲存桶的名稱。在本例中，此操作從包含s3cmd執行檔的資料夾中運行，並且檔案被傳送到相同的路徑，但是可以更改這些路徑：

<#root>

```
./s3cmd sync s3://my-organization-name-log-bucket ./
```

如果儲存桶中的檔案與磁碟上目標路徑中的檔案存在差異，則同步應下載缺失或更新的檔案。檢索到的第一個檔案應為通常上傳的自述檔案：

./s3cmd sync s3://my-organization-name-log-bucket./

s3://my-organization-name-log-bucket/README_FROM_UMBRELLA.txt -> <fdopen> [1/1]

1800的1800個100%在0s 15.00 kB/s完成

完成。1.0秒內下載了1800位元組，1800.00 B/s

同時會下載存在的所有日誌檔案。如果您想設定cron作業以定期計畫此功能，則由您自己決定，但是您現在應該能夠將儲存桶中任何新的或更改的日誌檔案自動下載到本地路徑中以進行長期保留。

Windows命令列執行檔(s3.exe)

在命令提示符下，運行此命令，其中「my-organization-name-log-bucket」是已在Umbrella控制面板的「日誌管理」部分中配置的儲存桶名稱。在此示例中，儲存桶（用星號萬用字元定義）中的所有檔案都將下載到\dnslogbackups\資料夾。

<#root>

```
s3 get my-organization-name-log-bucket/* c:\dnslogbackups\
```

有關此指令語法的詳細資訊，請閱讀這裡。

步驟 2:自動下載

在測試語法並按預期工作後，將指令複製到指令碼設定、cron作業(OS X / Linux)或計畫任務

(Windows)中，或使用您可能擁有的任何其他任務自動化工具。下載檔案以釋放S3例項中的空間後，也可以使用這些工具從儲存桶中移除檔案。我們建議您檢視所用工具的文檔，瞭解哪些內容最適合您的資料保留策略。

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）。