配置與Umbrella日誌管理和S3的QRadar整合

目錄

簡介

本文檔介紹如何配置QRadar以從AWS S3儲存桶中接收日誌以進行Umbrella日誌管理。

必要條件

需求

思科建議您瞭解以下主題：

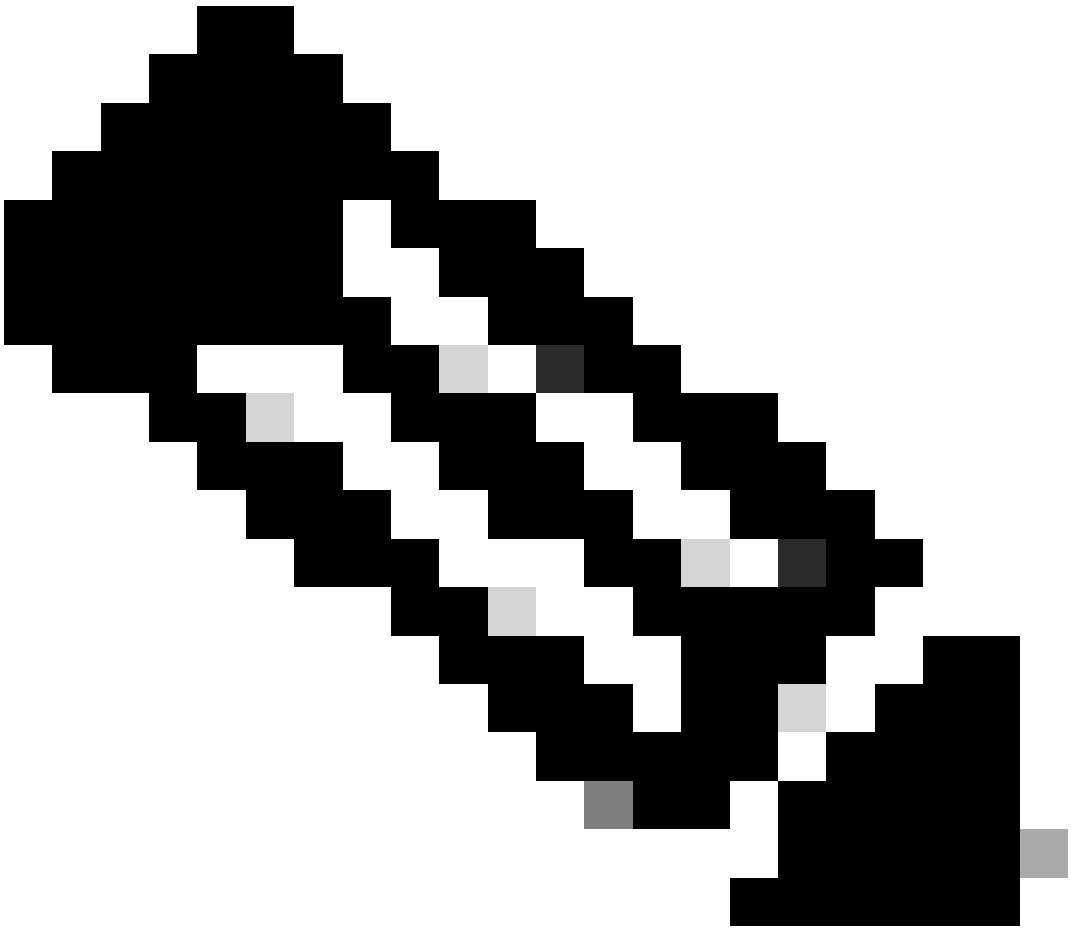
- 本文檔假設您的Amazon AWS S3儲存桶已在Umbrella(Settings > Log Management)中配置，並且顯示綠色且最近已上傳日誌。有關如何配置此功能的詳細資訊，請閱讀以下文章：Download Logs from Umbrella Log Management in AWS S3
- 除了對QRadar裝置、Amazon S3配置和Umbrella控制面板的管理許可權之外，這些說明假設QRadar管理員熟悉建立LSX（日誌源擴展）檔案。

採用元件

本檔案中的資訊是根據Cisco Umbrella。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀



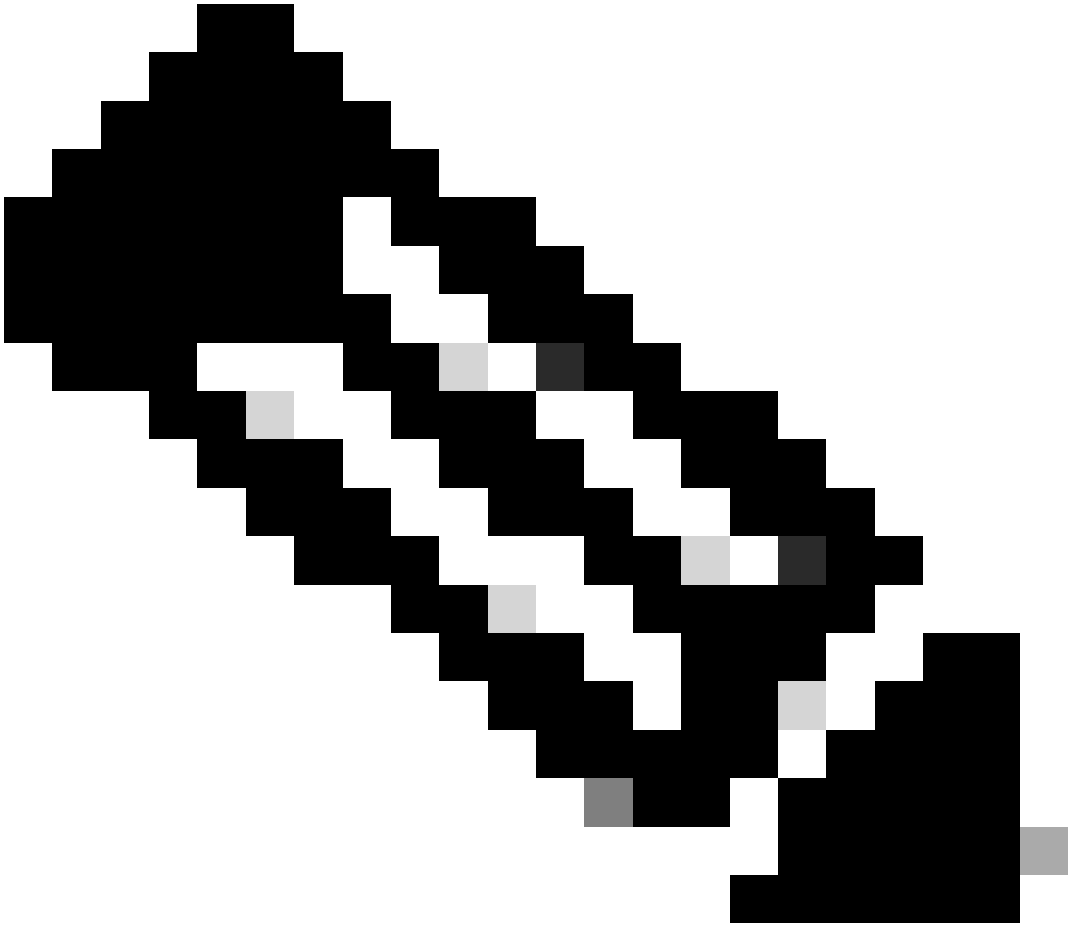
附註：配置QRadar以與Cisco Umbrella配合使用的最佳方法是通過思科雲安全應用。僅當無法配置應用時才繼續使用此方法。

來自IBM的QRadar是日誌分析的常用的SIEM。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QRadar並使其運行，以便它能夠從S3儲存桶提取日誌並使用這些日誌。主要分為兩個階段：

- 配置AWS S3安全憑證，以允許QRadar訪問日誌。
- 將QRadar本身設定為指向您的儲存桶。

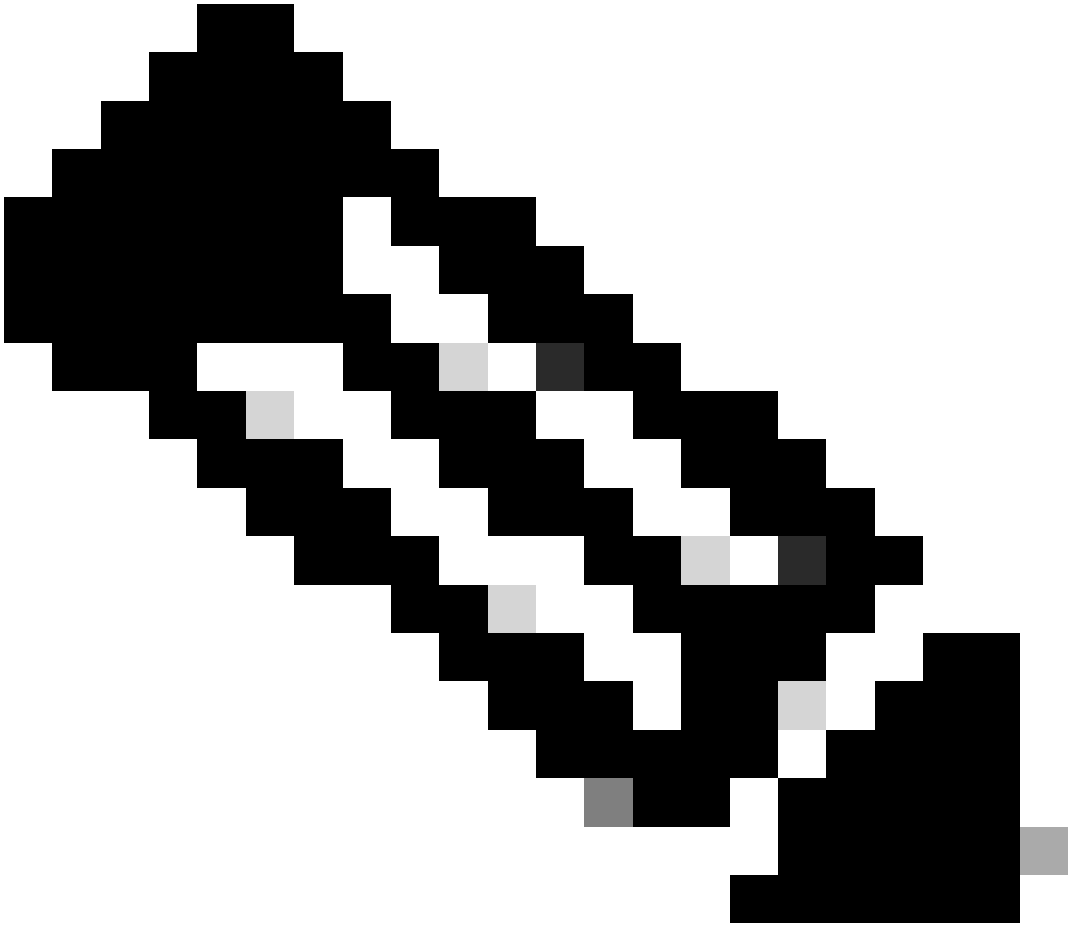
如果您使用的是思科管理的S3儲存桶，請使用使用AWS CLI從Umbrella日誌管理下載日誌文章中的這些說明。



附註：此整合已經過客戶管理的S3儲存桶和思科管理的S3儲存桶的測試。本文討論的資訊自本文撰寫之日起（2019年10月）已更新，可以根據QRadar和AWS Services介面的方式進行更改。本文檔為活文檔。如果您有意見回饋或找到了可以幫助其他客戶的技巧或提示，請與Cisco Umbrella支援聯絡。

對QRadar的支援必須來自IBM，因為思科無法直接支援第三方硬體或軟體。對於將您的Umbrella控制面板連線到S3儲存桶的任何問題，思科Umbrella可提供支援。本文中的許多資訊也可在IBM網站上找到。

階段1:在AWS中配置您的安全憑證



附註：這些步驟與介紹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(從AWS S3中的Umbrella Log Management下載日誌)。如果您已經執行這些步驟，則可以跳到第2階段，儘管您以後需要來自IAM使用者的安全憑證來驗證儲存桶中的QRadar。

步驟 1

1.向您的Amazon Web Services帳戶新增訪問金鑰，以允許遠端訪問您的本地工具，並允許上傳、下載和修改S3中的檔案：

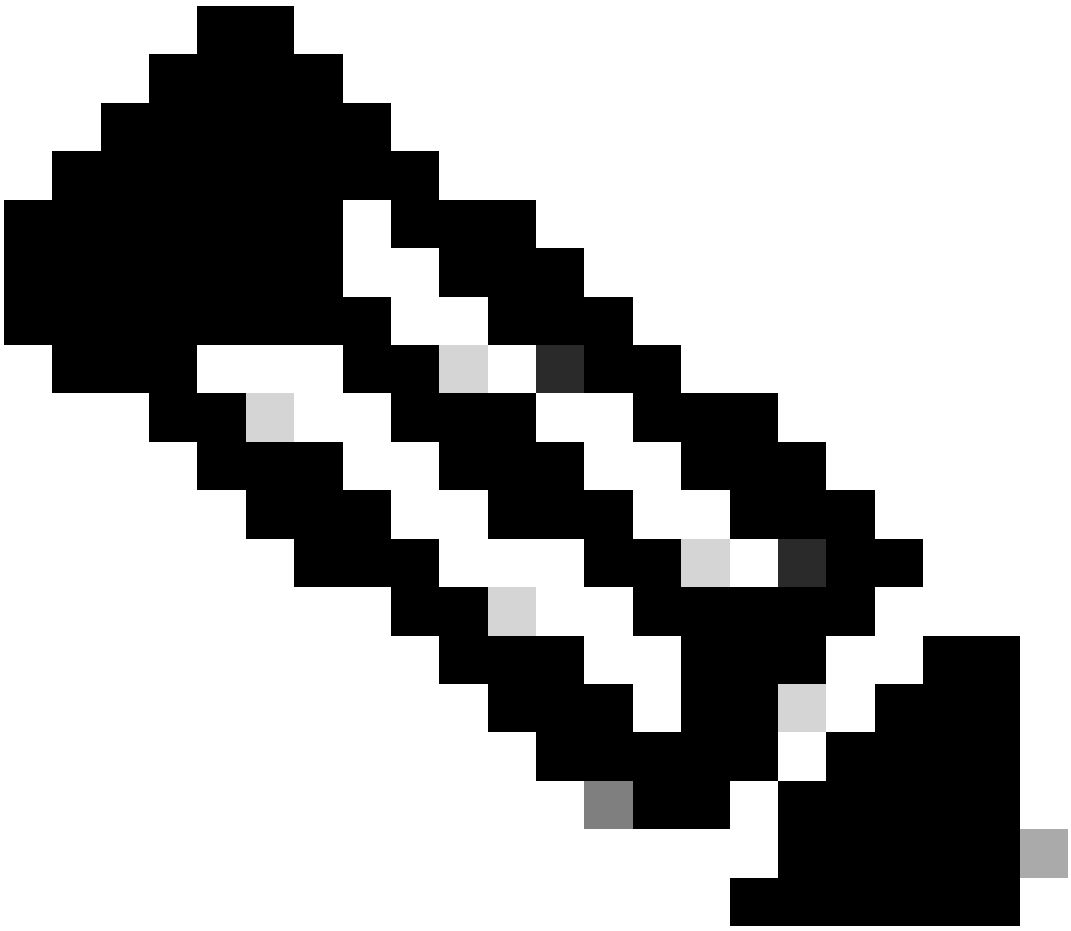
1. 登入AWS。
2. 在右上角選擇您的帳戶名稱。
3. 在下拉選單中，選擇Security Credentials。

2.然後，系統將提示您使用Amazon最佳實踐並建立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，請參閱AWS文檔。

步驟 2

1.選擇開始使用IAM使用者以建立一個IAM使用者以訪問您的S3儲存桶。然後，您將進入一個螢幕，您可以在其中建立IAM使用者。
2.選擇New Users，然後填寫欄位。



附註：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 User Security Credentials的兩個重要資訊。Umbrella強烈建議您使用右下方的按鈕下載這些資訊，以便進行備份。在設定中的此階段之後，它們將不可用。請確保您記下您的訪問金鑰ID和秘密訪問金鑰，因為稍後需要它們。

步驟 3

接下來，為您的IAM使用者新增策略，以便他們能夠訪問您的S3儲存桶：

1.選擇剛建立的使用者，然後向下滾動瀏覽使用者的屬性，直到看到Attach Policy按鈕。

2.選擇Attach Policy，然後在策略型別篩選器中輸入「s3」。這顯示了兩個結果：

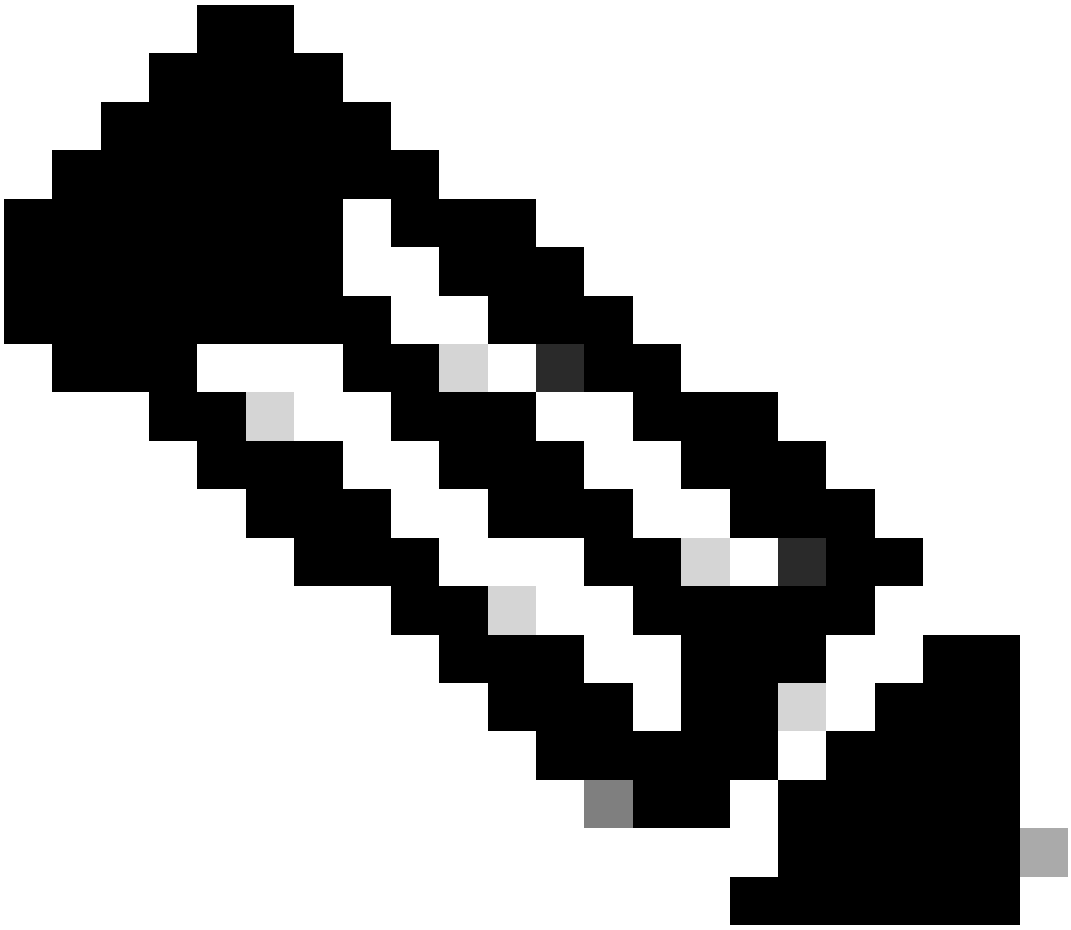
- AmazonS3FullAccess
- AmazonS3隻讀訪問

3.選擇AmazonS3FullAccess，然後在右下角選擇Attach Policy。

階段2:設定QRadar以從S3儲存桶提取DNS日誌資料

QRadar使用AWS CloudTrail服務，該服務是一種Web服務，記錄您賬戶的AWS API呼叫並向您傳送日誌檔案。

在QRadar訪問Amazon S3之前，請從IBM完成此過程以獲取Amazon伺服器證書。這部分是困難的，所以請確保您正確完成說明。



附註：在測試中，必須使用Firefox瀏覽器才能使此操作按預期工作。

要獲取Amazon伺服器證書，您必須將DER格式的證書移動到正確的QRadar裝置。需要證書的QRadar裝置是在Amazon AWS CloudTrail日誌源的Target Event Collector欄位中分配的裝置。

開始之前

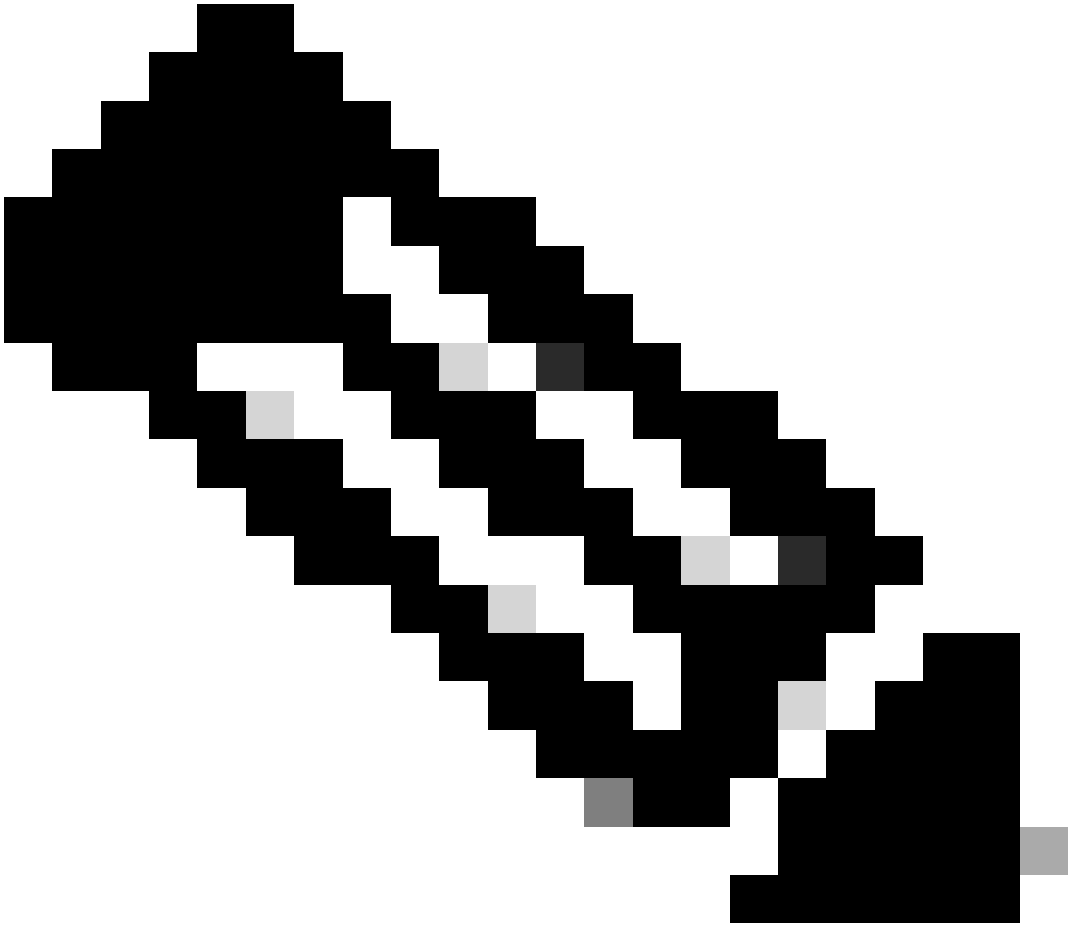
- 證書必須採用.DER格式。
- 副檔名.DER區分大小寫，並且必須是大寫。
- 如果證書以小寫形式匯出，則日誌源可能會遇到事件收集問題。

初始步驟

1.訪問您的AWS CloudTrail S3儲存桶:`https://<bucketname>.s3.amazonaws.com`

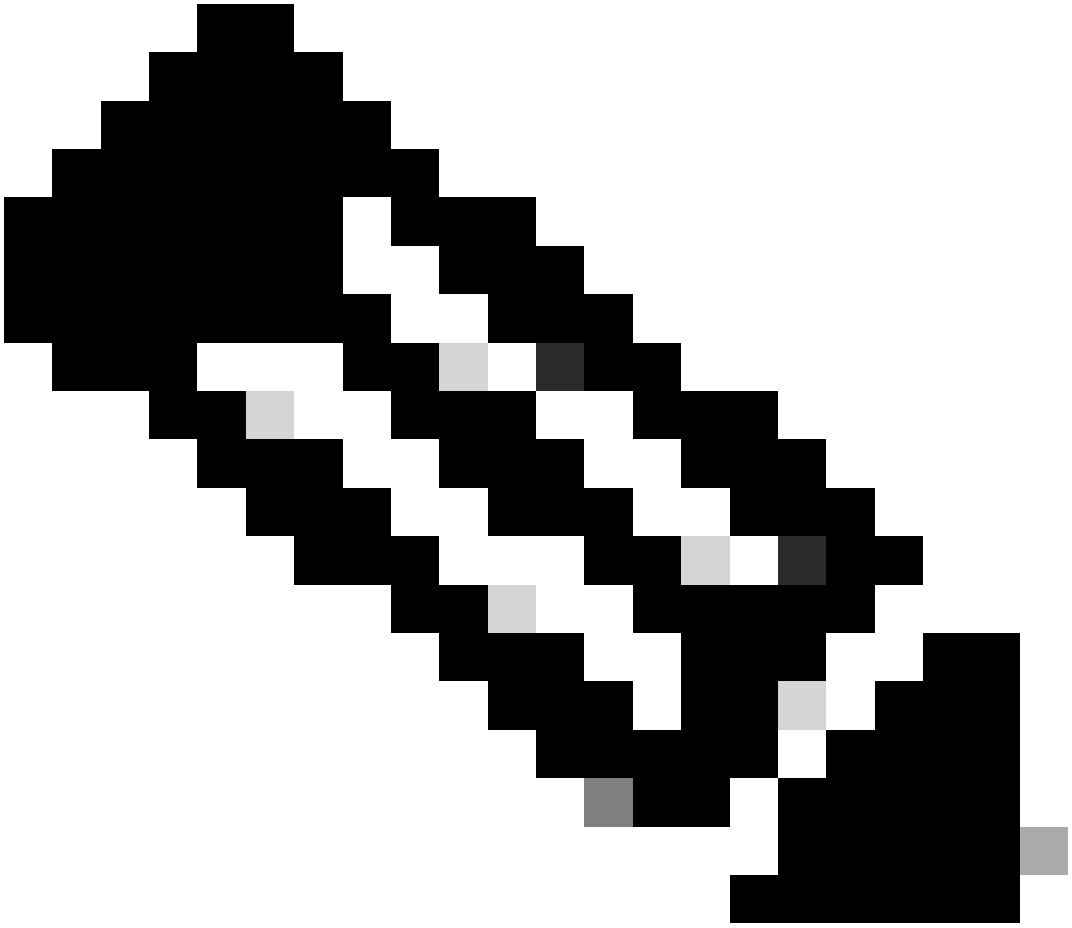
2.使用Firefox從AWS將SSL證書匯出為(.DER)證書。Firefox可以使用.DER副檔名建立所需的證書：

1. 選擇Site Identity圖示（位址列中的鎖定圖示）。
2. 選擇More Information > View Certificate，然後選擇Details頁籤。
3. 選擇Export以證書.DER格式匯出。



附註：.DER副檔名區分大小寫，並且必須是大寫。

3.將.DER證書複製到管理Amazon AWS CloudTrail日誌源的QRadar裝置的/opt/QRadar/conf/trusted_certificates目錄。您可以使用WinSCP複製它。



附註：管理日誌源的QRadar裝置由Amazon AWS CloudTrail日誌源中的Target Event Collect欄位標識。管理Amazon AWS CloudTrail日誌源的QRadar裝置必須具有/opt/QRadar/conf/trusted_certificates中的.DER證書副本。

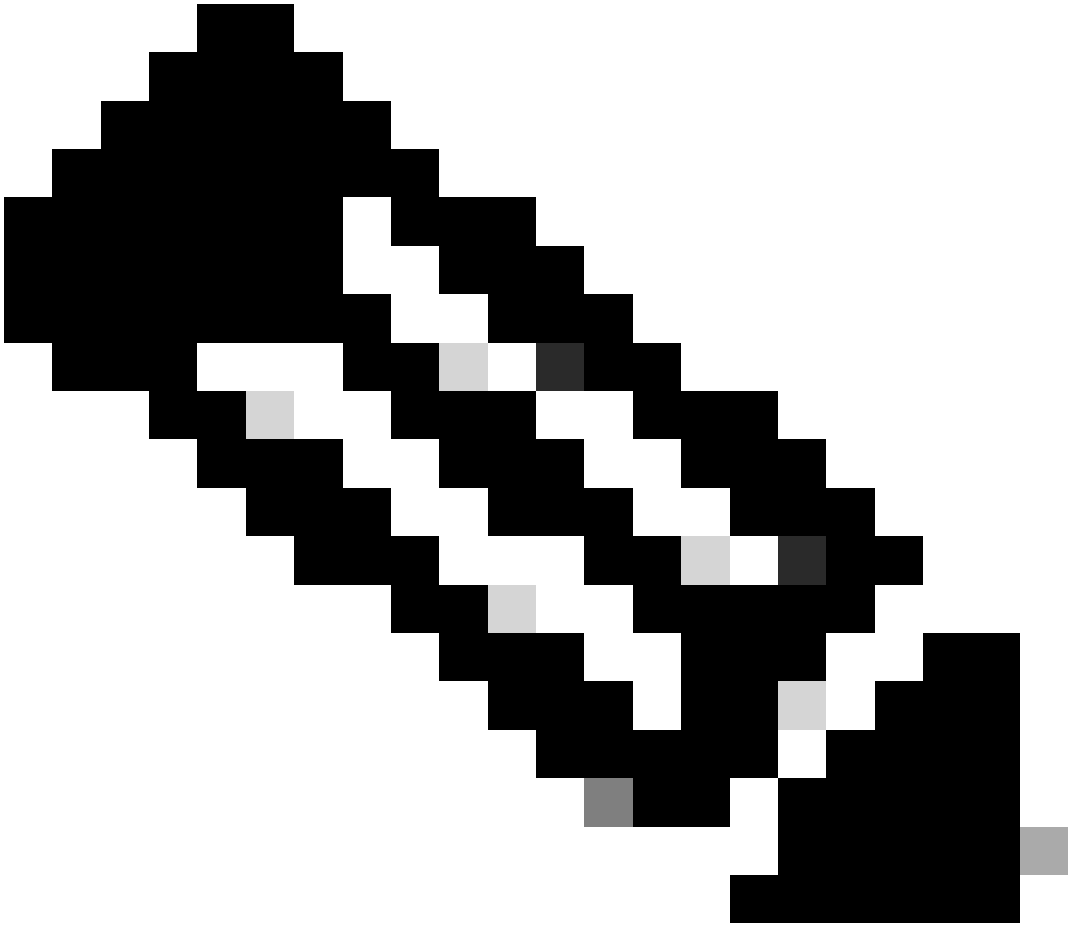
4.以管理使用者身份登入QRadar使用者介面。

5.選擇Admin頁籤。

6.選擇「日志源」圖示。

7.選擇Amazon AWS CloudTrail日志源。

8.在導航選單中，選擇Enable/Disable以禁用，然後重新啟用Amazon AWS CloudTrail日誌源。



附註：當管理員將日誌源從禁用強製為啟用時，該協定允許連線到日誌源中定義的Amazon AWS儲存桶。然後，作為第一次通訊的一部分，將進行證書檢查。

9.如果您仍然有問題，請驗證「日誌源識別符號」欄位是否包含正確的Amazon AWS儲存段名稱，以及日誌源配置中的遠端目錄路徑是否正確。

完成QRadar配置

1.在QRadar中，確保所有協定、DSM和其他資訊都是最新的。使用這些配置選擇LogFileProtocol（您的頻率、開始時間、重複週期和其他資訊可以不同）。

2.在日誌源標籤中，輸入日誌源名稱和日誌源說明。你可以隨便吃。

3.輸入您的S3儲存桶名稱、AWS訪問金鑰、您的AWS金鑰和Remote Directory（可能為下載，但取決於您的設定）。 新增日誌源識別符號（如年份）可幫助篩選，以便僅提取其中包含「2019」的日誌。

4.建立可以分析Cisco Umbrella事件的LSX（日誌源擴展）。（這是匯入QRadar後的外觀。）有關

如何建立LSX的更多資訊，請訪問IBM網站。這只是一個例子。要從日誌中提取的資料因使用案例而異。

5.仔細檢查您的AWS訪問金鑰和AWS金鑰是否已成功複製並貼上到日誌源配置中。

6.選擇基於RegEx的多線路的GZIP處理器和事件生成器。每行獲取一個事件的最簡單方法是使用以下專案的開始模式RegEx:

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

確保選擇日誌源擴展和使用條件，然後儲存日誌源。

7.在QRadar中執行完全部署。

然後，您的日誌源使用RestAPI使用您提供的憑據和金鑰連線到儲存桶，並開始提取事件。

其他資訊

啟用儲存段日誌記錄

要啟用儲存桶記錄，請閱讀AWS文檔並完成概述的程式。預設情況下，日誌記錄處於禁用狀態。啟用後，一個名為/logs的新資料夾將駐留在儲存桶根中，以顯示GETS、PUTS和DELETES的資訊。

管理日誌週期

使用S3時，您可以管理儲存桶中資料的生命週期，以延長要為其保留日誌的持續時間。根據所使用的外部日誌管理的用途，持續時間可能很短或很長。例如，您只需在24小時後從S3儲存桶下載日誌並離線儲存，或者將日誌無限期保留在雲中。

預設情況下，Amazon將資料無限期儲存在儲存桶中，但無限的儲存確實提高了儲存桶的維護成本。有關S3生命週期的更多資訊，請閱讀AWS文檔。

要配置儲存段的生命週期，請執行以下操作：

1.選擇「屬性」>「生命週期」。

2.選擇新增規則，然後選擇將規則應用於整個儲存桶（或子資料夾，如果進行了相應配置）。

3.選擇對對象執行的操作，如Delete或Archive，然後選擇時間段以及是否要使用Glacier儲存來幫助降低Amazon成本。（Glacier是「冷」離線儲存，雖然訪問速度較慢，但成本要低得多。）

如果您更喜歡使用其他方法（例如，在您的內部備份解決方案上）管理日誌，只需從S3下載日誌並以其他方式保留它們即可。

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）。