

通過Amazon S3服務瞭解面向MSP、MSSP和多組織客戶的集中式保護傘日誌管理

目錄

[簡介](#)

[概觀](#)

[兩種型別的Umbrella日誌管理](#)

[快速入門](#)

[配置自我管理的S3儲存桶](#)

[必要條件](#)

[設定Amazon S3儲存桶](#)

[驗證您的Amazon S3儲存桶](#)

[管理日誌生命週期](#)

[配置Cisco管理的S3儲存桶](#)

[配置後選項](#)

[日誌上傳失敗](#)

[檢查上傳的日誌和格式](#)

[啟用基於每個客戶的記錄](#)

[下載日誌、瞭解格式和Splunk/QRadar整合](#)

[S3日誌有多大？](#)

簡介

本文檔介紹使用Amazon S3服務對MSP、MSSP和多組織客戶進行集中化的Umbrella日誌管理。

概觀

MSP、MSSP和多組織控制檯能夠在雲端儲存中儲存您的離線客戶的DNS、URL和IP日誌。儲存位於Amazon S3中，日誌上傳後，可以出於合規性原因或安全分析原因下載並儲存它們。

此文檔可幫助您瞭解此功能，在您的Umbrella控制面板和Amazon S3控制檯中對其進行設定，並運行多個配置選項，包括您希望將日誌保留在S3中的持續時間。

Umbrella for MSP、MSSP和Multi-Org都能夠上傳來自控制檯子組織的流量活動日誌，並將這些日誌儲存在雲中。Amazon的AWS S3(Simple Storage Service)是存檔日誌的服務，有時也稱為is offline storage it is or it islog retention。它是

歸檔日誌可能有用，原因有多種，具體取決於您的需要。對於某些人，可以將匯出和歸檔的日誌匯入到資料分析或安全取證工具（如SIEM）中。對於其他人來說，活動日誌歸檔對於安全事件或人力資源記錄下的資料取證非常有用。

AWS S3以CSV格式將日誌儲存在壓縮(gzip)存檔中。由於日誌每10分鐘上載一次，因此來自您的網路的網路流量之間至少存在10分鐘的延遲，這些流量由Umbrella記錄，然後可供從S3下載。

控制檯中的orgID號

每個客戶組織使用控制檯中的orgID號單獨上載其日誌，以將每個客戶對映到資料夾。也可以按每個客戶/每個組織啟用或禁用此功能。

兩種型別的Umbrella日誌管理

日誌管理是通過將日誌上傳到所謂的it isbucketit is (基本上是AWSit is S3環境中的資料夾)來執行的。有兩種方法可以為Umbrella日誌託管儲存桶：

- 你們公司管理者管理和支付的。
- 由Cisco Umbrella管理、管理和支付。

讓思科管理您的S3儲存桶有優缺點。

思科管理儲存桶的優勢：

- 安裝非常簡單。只需幾分鐘，之後便極易管理。
- Umbrella的許可證成本中包含思科儲存桶管理，有效實現了服務的免費。儘管擁有自己的儲存桶成本高昂，但管理另一張帳單的開銷成本卻高得令人望而卻步。

自己管理S3例項的優點：

- 對離線儲存資料的時間沒有限制。思科將離線儲存限制為最多30天。
- 您可以向儲存桶中新增任何內容，包括Umbrella中的日誌檔案，因此儲存桶也可供其他應用程式使用。
- 您可以直接從Amazon獲得高級配置支援，例如自動化或命令列幫助。

對於大多數客戶來說，維護儲存桶的成本非常低廉，但事實證明這非常麻煩。

快速入門

在Console的設定>日誌管理下可以找到日誌管理功能 (您可以點選下拉箭頭)。

Search for a customer or organization

Settings

< Keys

PSA Integration Details

More ▾

Support Contact

Log Management

115012963103

配置自我管理的S3儲存桶

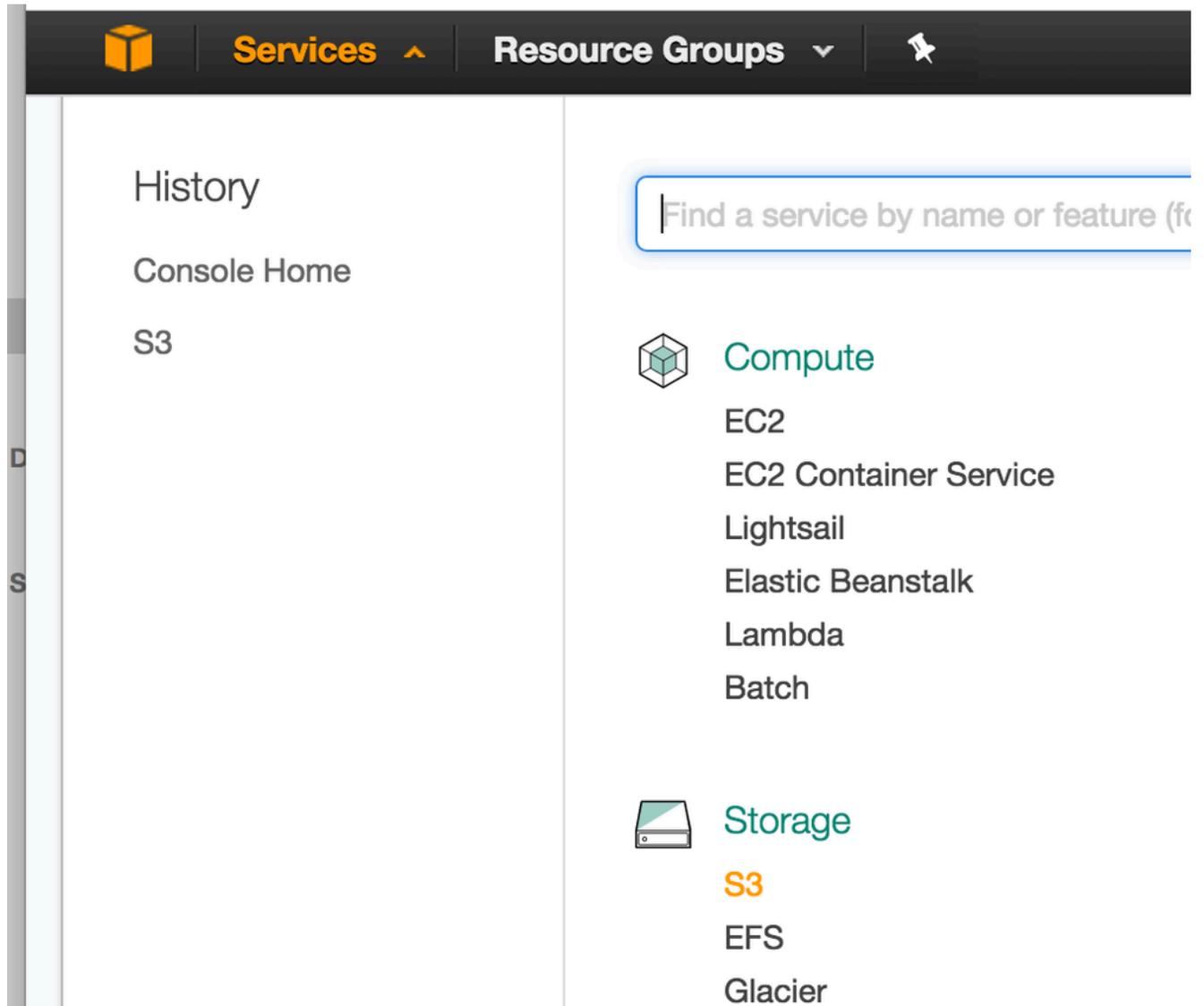
必要條件

要歸檔日誌，必須滿足以下要求：

- 對Cisco Umbrella MSP、MSSP或多組織控制檯的完全管理訪問許可權。
- 登入Amazon AWS服務(<https://aws.amazon.com/console/>)。如果您擁有帳戶，Amazon會為您提供S3的免費註冊。但是，如果您的使用率超過免費計畫的使用率，則需要使用信用卡。
- 在Amazon S3中為日誌儲存配置的儲存桶。有關配置和設定Amazon S3儲存段的說明，請參見下一節。

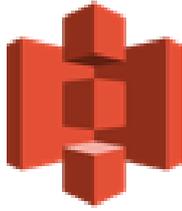
設定Amazon S3儲存桶

1. 首先登入[AWS控制檯](#)，然後從「儲存」下的選項清單中選擇「S3」。



115012842106

2. 您會看到歡迎您加入Amazon Simple Storage System的簡介螢幕
3. 接下來，如果您還沒有儲存桶，則希望建立一個儲存桶。按一下 [建立儲存桶](#)



Amazon S3



Search for buckets

+ Create bucket

Dele

115012842326

4. 首先輸入時段名稱

儲存段名稱必須是通用唯一的，不僅對您的AWS或Umbrella是如此，對所有Amazon AWS都是如此。使用個人資料(如「my-organization-name-log-bucket」)可以幫助您繞過通用唯一時段名稱的要求。桶名稱只能使用小寫字母，不能包含空格或句點，並且必須符合DNS命名慣例。有關名稱限制的詳細資訊，請閱讀[此處](#)。有關桶建立的詳細資訊，包括命名，請閱讀[此處](#)。

Create bucket

1 Name and region 2 Set properties 3 Set permissions 4 Review

Name and region

Bucket name ⓘ

my-msp-organization-name-log-bucket

Region

US West (N. California) ▾

Copy settings from an existing bucket

Select bucket (optional) 2 Buckets ▾

Create Cancel Next

115013010503

5. 選擇最適合您所在位置的區域，然後按一下Create。請勿從另一個儲存桶複製設定
6. 在「設定屬性」步驟中，按一下下一步。這些可在以後調整
7. 在「設定許可權」步驟中，只需按一下下一步。我們稍後將重新訪問許可權，以設定用於上傳的儲存段
8. 完成稽核過程並按一下 建立儲存桶

Create bucket ✕

✓ Name and region
✓ Set properties
✓ Set permissions
④ Review

Name and region Edit

Bucket name my-msp-organization-name-log-bucket-2 **Region** US West (N. California)

Properties Edit

Versioning	Disabled
Logging	Disabled
Tagging	0 Tags

Permissions Edit

Users	1
Public permissions	Disabled
System permissions	Disabled

Previous
Create bucket

115012842686

9. 接下來，您需要將儲存桶配置為接受來自Umbrella服務的上傳。在S3中，這稱為時段策略。按一下新配置的儲存桶的名稱，然後選擇介面頂部的Permissions頁籤

Amazon S3 > my-msp-organization-name-log-bucket

Overview

Properties

Permissions

Management

🔍 Type a prefix and press Enter to search. Press ESC to clear.

115012842906

10. 選擇Bucket Policy，然後提示您貼上到桶中

Access Control List

Bucket Policy

CORS configuration

Bucket policy editor ARN: arn:aws:s3:::my-msp-organization-name-log-bucket

Type to add a new policy or edit an existing policy in the text area below.

```
1 {
2   "Version": "2008-10-17",
3   "Statement": [
4     {
5       "Sid": "",
6       "Effect": "Allow",
7       "Principal": {
8         "AWS": "arn:aws:iam::568526795995:user/logs"
9     },
10    "Action": "s3:PutObject"
11  }
12  ]
13 }
```

115012843006

11. 將下麵包含桶策略的JSON字串複製並貼上到文本編輯器中，或者直接貼上到視窗中。在下面指定bucketname的位置替換準確的bucketname。如果未能執行此操作，則會出現錯誤消息

```
{
"版本":"2008-10-17",
"宣告":[
{
"Sid":"",
"效果":"允許",
"主體":{"
「AWS」 : "arn:aws:iam::568526795995:user/logs"
}},
"操作":"s3:PutObject",
"資源":"arn:aws:s3:::bucketname/*"
},
{
"Sid":"",
"效果":"拒絕",
"主體":{"
「AWS」 : "arn:aws:iam::568526795995:user/logs"
}},
"操作":"s3:GetObject",
"資源":"arn:aws:s3:::bucketname/*"
},
{
"Sid":"",
"效果":"允許",
"主體":
{
「AWS」 : "arn:aws:iam::568526795995:user/logs"
}
}
```

中，

```

"操作": "s3:GetBucketLocation",
"資源": "arn:aws:s3:::bucketname"
},
{
  "Sid": "",
  "效果": "允許",
  "主體": {
    「AWS」: "arn:aws:iam::568526795995:user/logs"
  },
  "操作": "s3:ListBucket",
  "資源": "arn:aws:s3:::bucketname"
}
]
}

```

12. 按一下Save以確認此更改

驗證您的Amazon S3儲存桶

步驟 1:

1. 返回到Umbrella控制檯並導航到設定>日誌管理
2. 點選「Amazon S3」以展開視窗
3. 在Bucket Name欄位中，鍵入或貼上您在S3中建立的確切儲存桶名稱，然後按一下Verify
您會在控制面板中收到一條確認消息，指示已成功驗證儲存桶。

The screenshot shows the 'Log Management' interface for 'Amazon S3'. At the top right, there are two columns: 'STATUS' with a radio button selected for 'Not Configured', and 'LAST SYNC' with the value 'Never'. Below this, the 'AWS S3 Bucket' section contains a text input field with the value 'my-msp-organization-name-log-bucket' and a blue 'VERIFY' button. A green checkmark icon is followed by the text 'Verification Successful'. Below this, a message states: 'For security, we need to confirm that we're sending logs to your bucket. Navigate to your AWS account, copy your unique token from the README file from your bucket, paste it below, and click save.' Underneath is a 'Unique Token' label and an empty text input field. At the bottom right, there are two buttons: 'CANCEL' and 'SAVE'.

115012847146

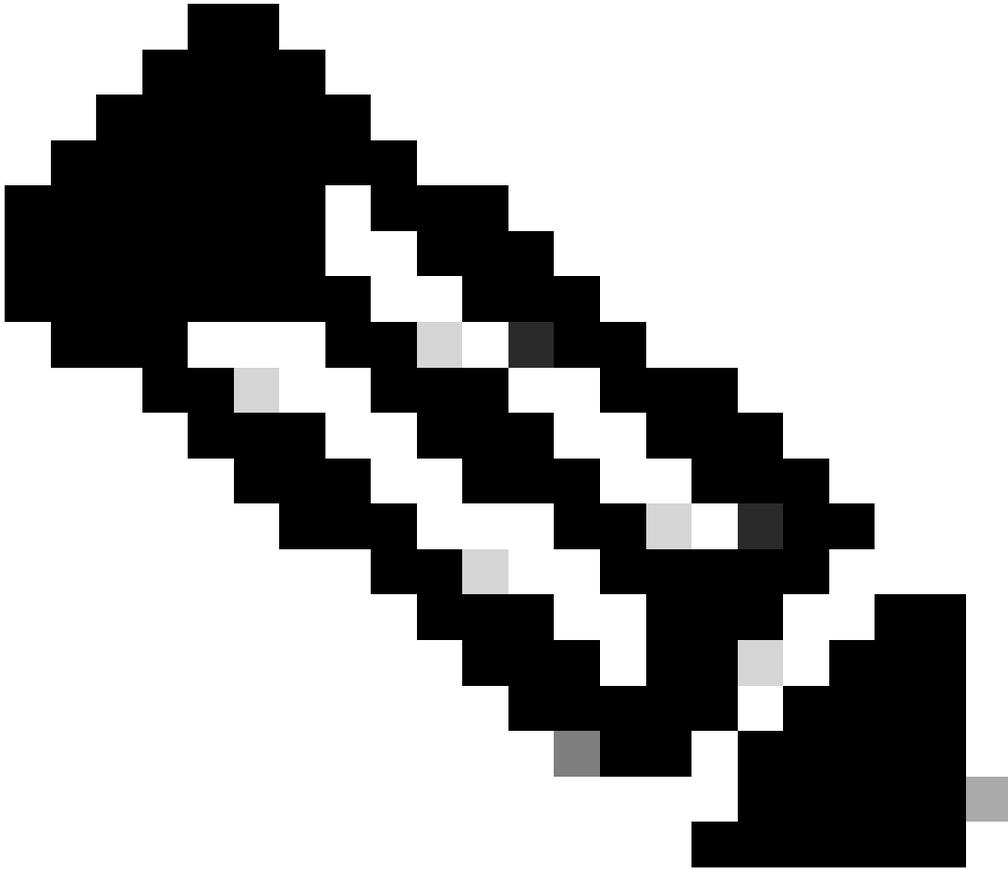
如果您收到錯誤資訊，指出無法驗證儲存桶，請重新檢查儲存桶名稱的語法，並檢查配置。如果問題仍然存在，請與我們的支援部門聯絡

步驟 2:

為確保指定了正確的儲存桶，Umbrella會要求您輸入唯一的啟用令牌。可以通過重新訪問S3儲存桶

來獲取啟用令牌。作為驗證過程的一部分，一個名為README_FROM_UMBRELLA.txt的檔案已從Umbrella上傳到您的Amazon S3儲存桶並出現在此處。

1. 按兩下自述檔案，然後在文本編輯器中將其開啟，從而下載自述檔案。在檔案中，有一個唯一的令牌將您的S3儲存桶繫結到您的Umbrella控制面板
-



附註：您可能需要在瀏覽器中刷新S3儲存桶，以便在上載後檢視README檔案。

2. 返回到Umbrella儀表板並將令牌貼上到標籤為「Unique token」的欄位中，然後按一下Save。此時，配置為完成。要檢視您的配置，只需點選Log Management部分中的Amazon S3名稱

Log Management

Amazon S3

STATUS

LAST SYNC

● Configured August 2nd 2017, 11:43:21 am

AWS S3 Bucket: my-msp-organization-name-log-bucket
Last Sync: August 2nd 2017, 11:43:21 am

i By default all customers are logged to this Amazon S3 Bucket. Logging can be manually turned off for customers individually from the [Customer Management](#) page.

STOP LOGGING

CLOSE

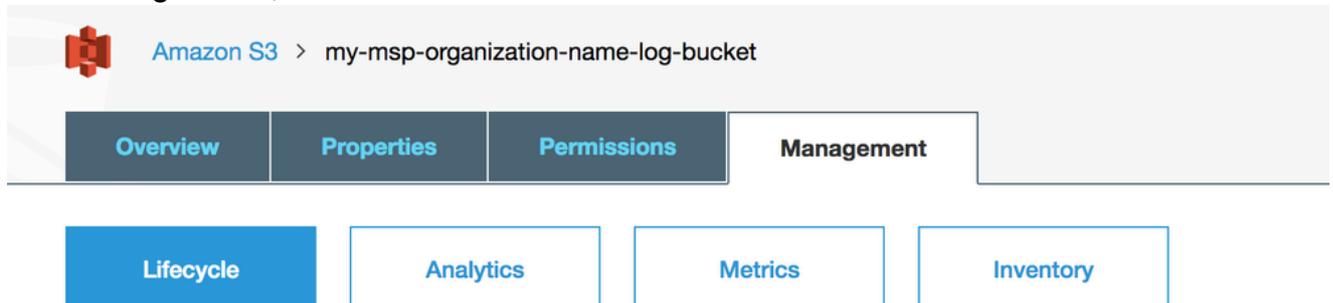
115012848126

管理日誌生命週期

使用S3時，您可以在儲存桶中管理資料的生命週期，以延長您要為其保留日誌的持續時間。根據您使用外部日誌管理的原因，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，然後將其離線儲存，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維護的成本。有關S3生命週期的詳細資訊，請在此處閱讀。

要配置儲存段的生命週期，請執行以下操作：

1. 選擇Management，然後按一下 生命週期



115012848246

2. 按一下Add a Rule，然後按一下Apply the Rule to the whole bucket（或子資料夾，如果您已進行了相應配置）。
3. 選擇對對象執行的操作（例如Delete或Archive），然後選擇時間段以及是否希望使用Glacier儲存來幫助降低Amazon成本。（Glacier是iscoldit是離線儲存，雖然訪問速度較慢，但成本較低。）
4. 如果您偏好使用其他方法（如您的內部備份解決方案）管理日誌，只需從S3下載日誌並以其他方式保留它們，然後將保留時間設定為幾天。

配置Cisco管理的S3儲存桶

在Umbrella控制面板中導航到Settings > Log Management。

有兩種選擇：

- 使用您公司管理的Amazon S3儲存桶
- 使用Cisco管理的Amazon S3儲存桶

Settings

 Log Management

Amazon S3

Use your company-managed Amazon S3 bucket

Amazon S3 bucket

[VERIFY](#)

[Learn more about Amazon S3 bucket verification »](#)

Use a Cisco-managed Amazon S3 bucket

25231151138964

選擇「使用思科託管的Amazon S3儲存桶」，您將獲得兩個新選項："Select a Region"和"Select a Retention Duration"。



Amazon S3

- Use your company-managed Amazon S3 bucket
- Use a Cisco-managed Amazon S3 bucket

Cisco will manage your logs in Amazon S3 for you. To learn more [view our guide](#).

Select a Region

US West (N. California) ▼

Select a Retention Duration

Data older than the selected time period will be automatically deleted and cannot be recovered.

30 days ▼

25231151158036

選擇區域

在將日誌下載到您的伺服器時，區域終端對於最大限度地減少延遲非常重要。列出的區域與 Amazon S3 中可用的區域相匹配，但並非所有區域都可用。例如，中國並未被列出。

從下拉選單中選擇離您最近的區域。如果您希望將來更改您的區域，您需要刪除當前設定並重新開始。

選擇保留期限

保留期僅為 7、14 或 30 天。在選定的時間段之後，所有資料都會被清除，而且無論什麼資料都不能檢索。如果你的攝取週期是正常的，我們建議你縮短一點時間。保留期可以稍後更改。

做出選擇後，按一下下一步，系統將提示您確認地區和持續時間

Do these settings look ok?

If you wish to change your region in the future, you will need to delete your current bucket and start over. Retention duration can be changed at any time.

Storage Region Asia Pacific (Seoul)
Retention Duration 30 Days

CANCEL

CONTINUE

25231181211796

一旦您同意繼續，您將收到啟用通知。

We're activating AWS S3 export now...



We're still working to create your AWS S3 bucket...

Once activation is complete, we'll provide you with keys to access your new bucket.

25231181218708

然後您會收到訪問金鑰和金鑰。您必須接受(單擊「獲得！」)，因為這是您唯一一次能夠看到任何金鑰的時間。訪問金鑰和金鑰是訪問儲存桶和下載日誌所必需的。

最後，您會看到顯示配置的摘要螢幕，最重要的是，您的儲存段名稱。

Amazon S3

Status

● Active (Managed)

Last Sync

Sep 28, 2017 at 10:19 AM



We're sending data to your managed S3 bucket

Storage Region us-west-1

Retention Duration 30 days [EDIT](#)

Bucket Name s3://umbrella-managed-

Last Sync Sep 28, 2017 at 10:19 AM



Forget your keys?

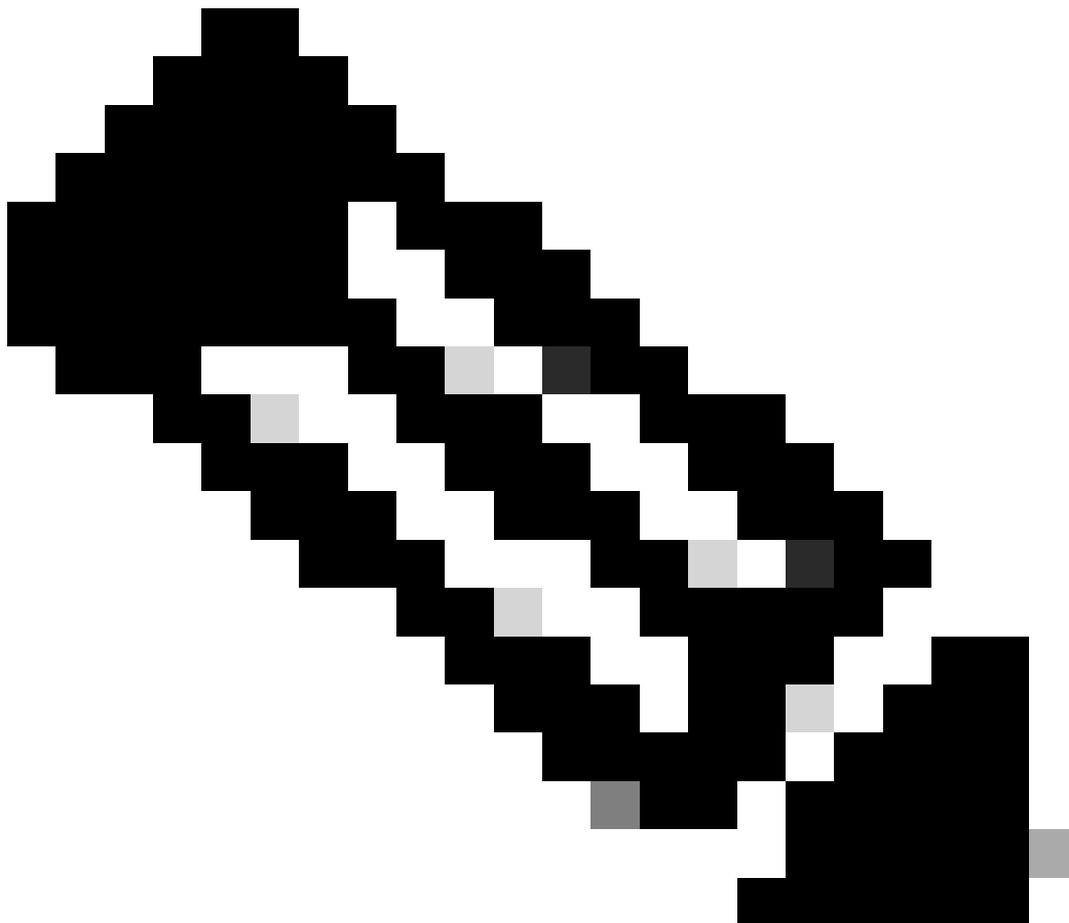
You can regenerate them below. Note that this will invalidate any existing keys.

[STOP LOGGING](#)

[REGENERATE KEYS](#)

25231181228180

您可以在方便時開啟或關閉登入。



附註：即使已關閉日誌記錄，思科仍會根據選定的保留持續時間繼續清除日誌。

配置後選項

日誌上傳失敗

如果無法將日誌從Cisco Umbrella上傳到S3儲存桶，則有4小時的寬限期，在此期間，服務每20分鐘重試一次。四個小時後，我們的支援團隊會開啟一個案例，他們會開始調查問題的原因，並主動聯絡您，以便您知道問題。

檢查上傳的日誌和格式

日誌會以十分鐘間隔從Umbrella日誌隊列上傳到S3儲存桶。完成配置後，第一個日誌將在兩小時內上傳到S3儲存桶，不過此過程通常是立即或接近立即的。但是，上傳任何內容都需要存在新生成的日誌資料，因此，如果您在測試環境中嘗試此操作，請確保將網路資料記錄在「活動搜尋」中。

要驗證是否一切正常，Umbrella控制面板中的上次同步時間更新和日誌開始顯示在S3儲存桶中。

在時段內，每個客戶或組織都標有組織ID，因此資料夾結構為：

Amazon S3/<bucket-name>/<orgID>/<subfolder>

<bucket-name>是您的儲存桶名稱，<orgID>是您的組織ID，<subfolder>是dnslogs、proxylogs或iplogs，具體取決於中的日誌型別。

對於MSP和MSSP客戶，orgID與「部署引數」部分中每個客戶詳細資訊下的「客戶設定」中的orgID匹配。多組織客戶可以通過登入到每個單獨的子組織並在瀏覽器url中註明orgID來收集orgID:(<https://dashboard.umbrella.com/o/#####/>)。

S3 LOGS

Centralized Log Management
To enable centralized log management, a centralized bucket needs to be set up in the [Log Management](#) page.

Individual Log Management
[Configure individual log management](#)
This enables logging dedicated to this customer.

DEPLOYMENT PARAMETERS

Org ID	Fingerprint	User ID	Show install command	Resource
1918	1300a53676a576151b1c37	8955		How to set up RMM scripts

[DELETE THIS ORGANIZATION](#) [CANCEL](#) [SAVE](#)

目前，MSP、MSSP和多組織客戶的日誌格式版本是1.1版。日誌以GZIP格式顯示，並上載到相應子資料夾中的S3儲存段，其命名格式為：

```
<subfolder>/<YYYY>-<MM>-<DD>/<YYYY>-<MM>-<DD>-<hh>-<mm>-<xxxx>.csv.gz
```

<subfolder>是dnslogs、proxylogs或iplogs，具體取決於中的日誌型別。<xxxx>是由四個字母數字字元組成的隨機字串，可防止覆蓋重複的檔名。

舉例來說：

```
dnslogs/2019-01-01/2019-01-01-00-00-e4e1.csv.gz
```

如果您在10分鐘內未看到儲存桶中的日誌，請與支援部門聯絡，概述您目前採取的步驟。

一旦日誌確實出現，我們建議通過解壓收到的前幾個日誌上載的內容來檢視資料，以確保可以在文本編輯器（甚至Microsoft Excel，通常是CSV的預設格式）中檢視資料。有關日誌中每個欄位代表的資訊，請在此處閱讀。

如果從Cisco Umbrella到S3儲存桶的日誌上傳失敗，服務會有4小時的寬限期，每隔二十分鐘重試一次。四個小時後，我們的支援團隊會開啟一個案例，支援團隊會開始調查問題的原因，並主動聯絡您，以便您瞭解問題。

啟用基於每個客戶的記錄

除非另有說明，否則此功能將針對所有客戶啟用。您可以為個別客戶關閉此功能，如果您為擁有此功能的客戶提供了不同的服務級別，此功能會很有幫助。這是在Console中的每個自定義設定下。上一節中的螢幕截圖顯示了關閉此功能的切換功能。

還可以在Amazon中建立IAM使用者，並將這些IAM使用者分配給作為儲存桶子資料夾的各個組織。這樣，您就可以允許終端使用者訪問其日誌，但只能訪問其日誌。

下載日誌、瞭解格式和Splunk/QRadar整合

為了下載用於保留或使用的日誌，有幾種方法可以從S3下載DNS日誌。Weit建立了一篇文章，概述了解決此問題的幾種方法。

您還可能遇到一些有關日誌格式的問題，以及它與Umbrella控制面板中顯示的日誌有何細微區別。有關匯出的日誌格式的更多資訊，請閱讀本文內容。

最後，匯出DNS日誌的主要用途之一是與SIEM工具整合。雖然處理此類日誌時的SIEM配置通常可歸結為管理員個人偏好，但我們仍對最常見的SIEM提供一些指導。

有關為Amazon AWS S3和Umbrella設定Splunk外掛的更多資訊，請閱讀此處。

有關配置IBM QRadar以從Amazon S3中提取日誌並對其進行摘要的資訊，請閱讀此處。

S3日誌有多大？

S3日誌的大小取決於發生的事件數，具體取決於DNS流量的大小。

您可以在此處找到S3日誌記錄的日誌格式。

示例條目為220位元組，但每條日誌行的大小取決於條目的數量（域名長度、類別數量等）。假設每個日誌行為220位元組，則一百萬個請求將為220 MB。

要估計每天可見的DNS查詢數量，請執行以下操作：

1. 在Umbrella控制面板中，導航到Reporting > Activity Search。
2. 在Filters下，運行過去24小時的報告，然後按一下Export CSV圖示。
3. 開啟下載的.csv檔案。行數（頭數減一）是每天的DNS查詢數；乘以220位元組，得出某天的估計值。

在成本方面，儘管成本是可變的，但我們發現，即使我們流量最大的客戶每月也只花幾美元用於這項服務。一個成本與儲存時間有關，另一個成本與從S3下載到您的環境的資料有關。有關更多詳細資訊，請與Amazon聯絡。

與我們的任何功能一樣，Weit非常想知道您的想法，特別是關於SIEM整合或本文檔中列出的任何其他問題。如果您有任何反饋，請通知我們！

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）。