使用者指南

# AWS 終端使用者訊息推送

# AWS 終端使用者訊息推送: 使用者指南

# Table of Contents

# 什麼是一 AWS 般使用者訊息推送？

> **Note**
>
> Amazon Pinpoint 的推播通知功能現在稱為 AWS 終端使用者簡訊。

透過使用 AWS 者訊息推送，您可以透過推播通知通道傳送推播通知，以吸引應用程式的使用者。我們支持蘋果推送通知服務（APNs），Firebase 雲消息傳遞（FCM），Amazon 設備消息傳遞（ADM）和百度推送。

主題



## 您是第一次使用 AWS 者訊息推送使用者嗎？

如果您是第一次使用 AWS 者訊息推送的使用者，建議您先閱讀下列章節：

- 設置一個 AWS 帳戶
- 開始使用一 AWS 般使用者訊息推送
- 建立應用程式並啟用推播通道

## AWS 終端使用者訊息推送的功能

您可以針對以下推播通知服務使用單獨的管道，將推播通知傳送到應用程式：

- 火力地堡雲消息傳遞（FCM）
- 蘋果推送通知服務（APNs）

> **Note**
>
> 您可以使用APNs將消息發送到 iOS 設備（例如 iPhones 和iPads）以及 macOS 設備（例如 Mac 筆記本電腦和台式機）上的 Safari 瀏覽器。

- 百度雲推送
- Amazon 設備消息（ADM）

# 存取一 AWS 般使用者訊息推送

簡要說明取得服務存取權的不同方式，無論是透過主控台CLI、或API。

您可以使用下列介面來管理「一 AWS 般使用者訊息推送」：

AWS 使用者訊息推送主控台

您可以在其中建立及管理「使用 AWS 者訊息推送」資源的 Web 介面。如果您已註冊 AWS 帳戶，則可以從存取一 AWS 般使用者訊息推送主控台 AWS Management Console。

AWS Command Line Interface

使用命令列殼層中的命令與 AWS 服務互動。在視窗、macOS 和 Linux 上支援 AWS Command Line Interface 此功能。若要取得有關的更多資訊 AWS CLI，請參閱AWS Command Line Interface 使用者指南。您可以在《命令參考》中找到「一 AWS 般使用者訊息推送」AWS CLI 命令。

AWS SDKs

如果您是喜歡使用特定語言來構建應用程序的軟件開發人員，APIs而不是通過HTTP或提交請求，則 AWS 提供庫HTTPS，示例代碼，教程和其他資源。這些程式庫提供可自動化工作的基本功能，例如加密簽署要求、重試要求，以及處理錯誤回應。這些功能有助於讓您更有效率地開始使用。如需詳細資訊，請參閱在 AWS上建置的工具。

# 區域可用性

AWS 一般使用者訊息推送服務 AWS 區域 於北美、歐洲、亞洲和大洋洲提供數個服務。在每個區域中， AWS 維護多個可用區域。這些可用區域各自實體隔離，但以私有、低延遲、高輸送量、高度冗餘的網路連線加以整合。這些可用區域可用於提供非常高層級的可用性和備援，同時也將延遲降至最低。

若要深入瞭解 AWS 區域，請參閱在中指定 AWS 區域 您的帳戶可以使用的Amazon Web Services 一般參考。如需目前提供使用者簡訊推送的 AWS 所有區域清單，以及每個區域的端點，請參閱中的 Amazon Pinpoint 和AWS 服務端點的端點API和配額。Amazon Web Services 一般參考如需進一步了解各區域之可用區域數量的資訊，請參閱 AWS 全球基礎設施。

# 設置一個 AWS 帳戶

您必須先取得 AWS 帳戶 具有足夠IAM權限的「使用 AWS 者訊息推送」，才能將推播通知傳送至您的應用程式。這也 AWS 帳戶 可以用於 AWS 生態系統中的其他服務。

主題



## 註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

1. 打開https://portal.aws.amazon.com/billing/註冊。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

## 建立具有管理存取權的使用者

註冊後，請保護 AWS 帳戶 AWS 帳戶根使用者、啟用和建立系統管理使用者 AWS IAM Identity Center，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。AWS Management Console在下一頁中，輸入您的密碼。

如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。

2. 為您的 root 使用者開啟多因素驗證 (MFA)。

   如需指示，請參閱《使用指南》中的「IAM為 AWS 帳戶 root 使用者啟用虛擬MFA裝置 (主控台)」。

建立具有管理存取權的使用者

1. 啟用IAM身分識別中心。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。

2. 在IAM身分識別中心中，將管理存取權授與使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以具有管理存取權的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者登入URL，請使用建立IAM身分識別中心使用者時傳送至您電子郵件地址的登入資訊。

  如需使用IAM身分識別中心使用者登入的說明，請參閱使用指南中的登入 AWS 存取入口網站。AWS 登入

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立遵循套用最低權限權限的最佳作法的權限集。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的新增群組。

# 開始使用一 AWS 般使用者訊息推送

若要設定「一 AWS 般使用者訊息推送」，讓它能夠傳送推播通知給您的應用程式，您必須先提供授權「使用 AWS 者訊息推送」將訊息傳送至您的應用程式的認證。您提供的登入資料取決於您使用的推送通知系統：

- 如需 Apple 推播通知服務 (APN) 憑證，請參閱 Apple 開發人員說明文件中的從 Apple 取得加密金鑰和金鑰 ID 和從 Apple 取得供應商憑證。
- 有關 Firebase 雲消息傳遞（FCM）憑據，可以通過 Firebase 控制台獲取它們，請參閱 Firebase 雲消息傳遞。
- 有關百度憑據，請參閱百度。
- 有關 Amazon 裝置簡訊 (ADM) 登入資料，請參閱取得登入資料。

# 建立應用程式並啟用推播通道

您必須先建立應 AWS 用程式並啟用推播通知通道，才能使用「一般使用者訊息推送」來傳送推播通知。

## 上下文

Application (應用程式)

應用程式是所有「一 AWS 般使用者訊息推送」設定的儲存容器。該應用程序還存儲您的 Amazon Pinpoint 渠道，營銷活動和旅程設置。

索引鍵

一 AWS 般使用者訊息推送所使用的私密簽署金鑰，以加密簽署APNs驗證 Token。您可以透過您的 Apple 開發人員帳戶取得簽署金鑰。

如果您提供簽署金鑰，「一AWS 般使用者訊息推送」會APNs針對您傳送的每個推播通知使用 Token 進行驗證。使用簽署金鑰，您可以將推播通知傳送至APNs生產環境和沙箱環境。

與憑證不同，您的簽署金鑰不會過期。您只需提供您的簽署金鑰一次，而且之後不需要更新它。您可以將相同的簽署金鑰用於多個應用程式。有關更多信息，請參閱 Xcode 幫助中的APNs使用身份驗證令牌進行通信。

憑證

一般使用 AWS 者訊息推送在您傳送推播通知APNs時用來驗證的TLS憑證。APNs憑證可同時支援生產環境和沙箱環境，也可以只支援沙箱環境。您可以透過您的 Apple 開發人員帳戶取得憑證。

憑證會在一年後過期。發生這種情況時，您必須建立新憑證，然後將憑證提供給「使用 AWS 者訊息推送」，以更新推播通知傳送。有關更多信息，請參閱 Xcode 幫助中的APNs使用TLS證書進行通信。

## 必要條件

在您可以使用任何推送通道之前，您需要有效的推送服務認證。如需取得認證的詳細資訊，請參閱開始使用一 AWS 般使用者訊息推送。

# 程序

依照下列指示建立應用程式並啟用任何推播通道。若要完成此程序，您只需要輸入應用程式名稱。您可以稍後啟用或停用任何推送通道。

1. 在開啟「一 AWS 般使用者訊息推送主控台」https://console.aws.amazon.com/push-notifications/。
2. 選擇建立應用程式。
3. 針對應用程式名稱，輸入您應用程式的名稱。
4. (選擇性) 依照此選擇性步驟啟用 Apple 推播通知服務 (APNs)。
   a. 對於 Apple 推播通知服務（APNs），請選擇啟用。
   b. 對於「預設驗證類型」，請選擇：
      i. 如果您選擇「金鑰認證」，請提供 Apple 開發人員帳戶中的下列資訊。 AWS 一般使用者訊息推送需要此資訊才能建構驗證 Token。
         - 金鑰 ID – 指派給簽署金鑰的 ID。
         - 封包識別符 – 指派給 iOS 應用程式的 ID。
         - 團隊識別符 – 指派給 Apple 開發人員帳戶團隊的 ID。
         - 驗證金鑰 – 您在建立驗證金鑰時，從 Apple 開發人員帳戶下載的 .p8 檔案。
      ii. 如果您選擇憑證登入資料，請提供下列資訊：
         - SSL憑證 — 憑證的 .p12 檔案TLS。
         - 憑證密碼 – 如果您已為憑證指派密碼，請在此處輸入。
         - 憑證類型 – 選取要使用的憑證類型。
5. （可選）請按照此可選步驟啟用 Firebase 雲消息傳遞（FCM）。
   a. 對於 Firebase 雲消息傳遞（FCM），請選擇啟用。
   b. 對於「預設驗證類型」，請選擇：
      i. 對於令牌憑據（推薦），請選擇「選擇文件」，然後選擇您的服務JSON文件。
      ii. 對於密鑰憑據，請輸入API密鑰。
6. (選擇性) 請依照此選擇性步驟啟用百度雲推送。
   a. 對於百度雲推送，請選擇啟用。

b. 對於API密鑰，輸入您的API密鑰。

c. 對於秘密密鑰，請輸入您的密鑰。

7. (選擇性) 按照此選用步驟啟用 Amazon 裝置簡訊。

a. 對於 Amazon 裝置簡訊，請選取啟用。

b. 對於客戶 ID，請輸入您的客戶 ID。

c. 對於客戶密碼，請輸入您的客戶密碼。

8. 選擇建立應用程式。

# 停用推送通道

請遵循以下指示停用任何推送通道。

1. 在開啟一 AWS 般使用者訊息推送主控台https://console.aws.amazon.com/push-notifications/。
2. 選擇包含您的推送認證的應用程式。
3. (選擇性) 若為 Apple 推播通知服務 (APNs)，請清除啟用。
4. （可選）對於 Firebase 雲消息傳遞（FCM），請清除啟用。
5. （可選）對於百度雲推送清除啟用。
6. (選擇性) 若為 Amazon 裝置簡訊，請清除啟用。
7. 選擇儲存變更。

# 傳送訊息

「一 AWS 般使用者訊息推送」API 可以傳送交易推播通知給特定裝置識別碼。本節包含完整的程式碼範例，您可以使用這些範例，透API過使用 AWS SDK. AWS

您可以使用這些範例，透過「一 AWS 般使用者訊息推送」支援的任何推播通知服務傳送推播通知。目前， AWS 最終用戶消息推送支持以下渠道：Firebase 雲消息傳遞（FCM），蘋果推送通知服務（APNs），百度雲推送和 Amazon 設備消息傳遞（ADM）。

如需有關端點、區段和通道的更多程式碼範例，請參閱程式碼範例。

> **Note**
>
> 當您通過 Firebase 雲消息傳遞（FCM）服務發送推送通知時，請GCM在呼叫 AWS 最終用戶消息傳遞推送時使用該服務名稱API。谷歌雲消息傳遞（GCM）服務已於 2018 年 4 月 10 日由谷歌停產。不過，「一 AWS 般API使用者訊息推送」會針對透過GCM服務傳送的訊息使用FCM服務名稱，以維持與停止服GCM務之前撰寫之API程式碼的相容性。

GCM (AWS CLI)

下列範例會使用傳送訊息來傳送GCM推播通知。 AWS CLI Replace (取代) *token* 具有設備的唯一令牌 *611e3e3cdd47474c9c1399a50example* 與您的應用程序標識符。

```
aws pinpoint send-messages \
--application-id 611e3e3cdd47474c9c1399a50example \
--message-request file://myfile.json \
--region us-west-2

Contents of myfile.json:
{
  "Addresses": {
    "token": {
      "ChannelType" : 'GCM'
    }
  },
  "MessageConfiguration": {
    "GCMMessage": {
      "Action": "URL",
      "Body": "This is a sample message",
      "Priority": "normal",
```

```
      "SilentPush": True,
      "Title": "My sample message",
      "TimeToLive": 30,
      "Url": "https://www.example.com"
      }
  }
}
```

下列範例會使用傳送訊息來傳送GCM推播通知，並使用所有舊金鑰與. AWS CLI Replace (取代) *token* 具有設備的唯一令牌 *611e3e3cdd47474c9c1399a50example* 與您的應用程序標識符。

```
aws pinpoint send-messages \
--application-id 611e3e3cdd47474c9c1399a50example \
--message-request
'{
  "MessageConfiguration": {
    "GCMMessage":{
      "RawContent": "{\"notification\": {\n \"title\": \"string\",\n \"body\":
 \"string\",\n \"android_channel_id\": \"string\",\n \"body_loc_args\": [\n \"string
\"\n ],\n \"body_loc_key\": \"string\",\n \"click_action\": \"string\",\n \"color\":
 \"string\",\n \"icon\": \"string\",\n \"sound\": \"string\",\n \"tag\": \"string
\",\n \"title_loc_args\": [\n \"string\"\n ],\n \"title_loc_key\": \"string\"\n },
\"data\":{\"message\":\"hello in data\"} }",
      "TimeToLive" : 309744
     }
   },
  "Addresses": {
    "token": {
      "ChannelType":"GCM"
      }
   }
}'
\ --region us-east-1
```

下列範例會使用傳送訊息，使用傳送訊息來傳送包含FCMv1訊息承載的GCM推播通知。 AWS CLI Replace (取代) *token* 具有設備的唯一令牌 *611e3e3cdd47474c9c1399a50example* 與您的應用程序標識符。

```
aws pinpoint send-messages \
--application-id 6a2dafd84bec449ea75fb773f4c41fa1 \
--message-request
'{
```

```
  "MessageConfiguration": {
    "GCMMessage":{
      "RawContent": "{\n \"fcmV1Message\": \n {\n \"message\" :{\n  \"notification
\": {\n \"title\": \"string\",\n \"body\": \"string\"\n },\n \"android\": {\n
 \"priority\": \"high\",\n \"notification\": {\n \"title\": \"string\",\n \"body
\": \"string\",\n \"icon\": \"string\",\n \"color\": \"string\",\n \"sound\":
 \"string\",\n \"tag\": \"string\",\n \"click_action\": \"string\",\n \"body_loc_key
\": \"string\",\n \"body_loc_args\": [\n \"string\"\n ],\n \"title_loc_key
\": \"string\",\n \"title_loc_args\": [\n \"string\"\n ],\n \"channel_id\":
 \"string\",\n \"ticker\": \"string\",\n \"sticky\": true,\n \"event_time\":
 \"2024-02-06T22:11:55Z\",\n \"local_only\": true,\n \"notification_priority\":
 \"PRIORITY_UNSPECIFIED\",\n \"default_sound\": false,\n \"default_vibrate_timings
\": true,\n \"default_light_settings\": false,\n \"vibrate_timings\": [\n \"22s
\"\n ],\n \"visibility\": \"VISIBILITY_UNSPECIFIED\",\n \"notification_count\": 5,
\n \"light_settings\": {\n \"color\": {\n \"red\": 1,\n \"green\": 2,\n \"blue\":
 3,\n \"alpha\": 6\n },\n \"light_on_duration\": \"112s\",\n \"light_off_duration
\": \"1123s\"\n },\n \"image\": \"string\"\n },\n \"data\": {\n \"dataKey1\":
 \"priority message\",\n \"data_key_3\": \"priority message\",\n \"dataKey2\":
 \"priority message\",\n \"data_key_5\": \"priority message\"\n },\n \"ttl\":
 \"10023.32s\"\n },\n \"apns\": {\n \"payload\": {\n \"aps\": {\n \"alert\": {\n
 \"subtitle\": \"string\",\n \"title-loc-args\": [\n \"string\"\n ],\n \"title-loc-
key\": \"string\",\n \"launch-image\": \"string\",\n \"subtitle-loc-key\": \"string
\",\n \"subtitle-loc-args\": [\n \"string\"\n ],\n \"loc-args\": [\n \"string
\"\n ],\n \"loc-key\": \"string\",\n \"title\": \"string\",\n \"body\": \"string
\"\n },\n \"thread-id\": \"string\",\n \"category\": \"string\",\n \"content-
available\": 1,\n \"mutable-content\": 1,\n \"target-content-id\": \"string\",\n
 \"interruption-level\": \"string\",\n \"relevance-score\": 25,\n \"filter-criteria
\": \"string\",\n \"stale-date\": 6483,\n \"content-state\": {},\n \"timestamp\":
 673634,\n \"dismissal-date\": 4,\n \"attributes-type\": \"string\",\n \"attributes
\": {},\n \"sound\": \"string\",\n \"badge\": 5\n }\n }\n },\n \"webpush\": {\n
 \"notification\": {\n \"permission\": \"granted\",\n \"maxActions\": 2,\n \"actions
\": [\n \"title\"\n ],\n \"badge\": \"URL\",\n \"body\": \"Hello\",\n \"data\": {\n
 \"hello\": \"hey\"\n },\n \"dir\": \"auto\",\n \"icon\": \"icon\",\n \"image\":
 \"image\",\n \"lang\": \"string\",\n \"renotify\": false,\n \"requireInteraction\":
 true,\n \"silent\": false,\n \"tag\": \"tag\",\n \"timestamp\": 1707259524964,\n
 \"title\": \"hello\",\n \"vibrate\": [\n 100,\n 200,\n 300\n ]\n },\n \"data\": {\n
 \"data1\": \"priority message\",\n \"data2\": \"priority message\",\n \"data12\":
 \"priority message\",\n \"data3\": \"priority message\"\n }\n },\n \"data\": {\n
 \"data7\": \"priority message\",\n \"data5\": \"priority message\",\n \"data8\":
 \"priority message\",\n \"data9\": \"priority message\"\n }\n }\n \n}\n}",
      "TimeToLive" : 309744
    }
  },
  "Addresses": {
```

```
    token: {
      "ChannelType":"GCM"
    }
   }
}'
\ --region us-east-1
```

如果使用 ImageUrl field forGCM，則精確定位將字段作為數據通知發送，密鑰為pinpoint.notification.imageUrl，這可以防止圖像被渲染開箱即用。請使用 RawContent 或添加對數據鍵的處理，例如將您的應用程序與之集成 AWS Amplify。

Safari (AWS CLI)

您可以使用「一 AWS 般使用者訊息推送」，將訊息傳送至使用 Apple Safari 網頁瀏覽器的 macOS 電腦。若要傳訊到 Safari 瀏覽器，必須指定原始訊息內容，且須在訊息承載中包含特定屬性。您可以透過建立具有原始訊息承載的推播通知範本，或在 Amazon Pinpoint 使用者指南中直接在行銷活動訊息中指定原始訊息內容，以達到此目的。

> **Note**
>
> 傳送到使用 Safari 網頁瀏覽器的 macOS 筆記型電腦和桌上型電腦，需要此特殊屬性。發送到 iOS 設備（例如 iPhones 和 ）不需要它iPads。

若要傳訊到 Safari 網頁瀏覽器，必須指定原始訊息承載。原始訊息承載必須在 aps 物件中包含一個 url-args 陣列。需要 url-args 陣列才能將推播通知傳送到 Safari 網頁瀏覽器。但可以接受陣列包含單一空白元素。

下列範例會使用傳送訊息，將通知傳送至 Safari 網頁瀏覽器。 AWS CLI Replace (取代) *token* 具有設備的唯一令牌 *611e3e3cdd47474c9c1399a50example* 與您的應用程序標識符。

```
aws pinpoint send-messages \
--application-id 611e3e3cdd47474c9c1399a50example \
--message-request
'{
  "Addresses": {
    "token":
    {
      "ChannelType":"APNS"
    }
  },
```

```
  "MessageConfiguration": {
    "APNSMessage": {
        "RawContent":
          "{\"aps\": {\"alert\": { \"title\": \"Title of my message\", \"body\":
 \"This is a push notification for the Safari web browser.\"},\"content-available\":
 1,\"url-args\": [\"\"]}}"
     }
  }
}'
\ --region us-east-1
```

如需 Safari 推播通知的詳細資訊，請參閱 Apple 開發人員網站上的設定 Safari 推播通知。

APNS (AWS CLI)

下列範例會使用傳送訊息來傳送APNS推播通知。 AWS CLI Replace (取代) *token* 使用設備的唯一令牌，*611e3e3cdd47474c9c1399a50example* 與您的應用程序標識符，以及 *GAME_INVITATION* 具有唯一標識符。

```
aws pinpoint send-messages \
--application-id 611e3e3cdd47474c9c1399a50example \
--message-request
'{
    "Addresses": {
     "token":
    {
      "ChannelType":"APNS"
    }
  },
  "MessageConfiguration": {
    "APNSMessage": {
      "RawContent": "{\"aps\" : {\"alert\" : {\"title\" : \"Game Request\",
\"subtitle\" : \"Five Card Draw\",\"body\" : \"Bob wants to play poker\"},\"category
\" : \"GAME_INVITATION\"},\"gameID\" : \"12345678\"}"
      }
    }
}'
\ --region us-east-1
```

JavaScript (Node.js)

使用此範例可 JavaScript 在 Node.js 中使用的 AWS SDK傳送推播通知。此範例假設您已經 JavaScript 在 Node.js 中安裝並設定了。SDK

此範例也會假設您使用共用的登入資料檔案，指定現有 使用者的存取金鑰和私密存取金鑰。如需詳細資訊，請參閱 Node.js 開發人員指南 JavaScript 中AWS SDK的中的設定認證。

```
'use strict';

const AWS = require('aws-sdk');

// The AWS Region that you want to use to send the message. For a list of
// AWS Regions where the API is available
const region = 'us-east-1';

// The title that appears at the top of the push notification.
var title = 'Test message sent from End User Messaging Push.';

// The content of the push notification.
var message = 'This is a sample message sent from End User Messaging Push by using
 the '
            + 'AWS SDK for JavaScript in Node.js';

// The application ID that you want to use when you send this
// message. Make sure that the push channel is enabled for the project that
// you choose.
var applicationId = 'ce796be37f32f178af652b26eexample';

// An object that contains the unique token of the device that you want to send
// the message to, and the push service that you want to use to send the message.
var recipient = {
  'token': 'a0b1c2d3e4f5g6h7i8j9k0l1m2n3o4p5q6r7s8t9u0v1w2x3y4z5a6b7c8d8e9f0',
  'service': 'GCM'
  };

// The action that should occur when the recipient taps the message. Possible
// values are OPEN_APP (opens the app or brings it to the foreground),
// DEEP_LINK (opens the app to a specific page or interface), or URL (opens a
// specific URL in the device's web browser.)
var action = 'URL';

// This value is only required if you use the URL action. This variable contains
// the URL that opens in the recipient's web browser.
var url = 'https://www.example.com';

// The priority of the push notification. If the value is 'normal', then the
// delivery of the message is optimized for battery usage on the recipient's
```

```
// device, and could be delayed. If the value is 'high', then the notification is
// sent immediately, and might wake a sleeping device.
var priority = 'normal';

// The amount of time, in seconds, that the push notification service provider
// (such as FCM or APNS) should attempt to deliver the message before dropping
// it. Not all providers allow you specify a TTL value.
var ttl = 30;

// Boolean that specifies whether the notification is sent as a silent
// notification (a notification that doesn't display on the recipient's device).
var silent = false;

function CreateMessageRequest() {
  var token = recipient['token'];
  var service = recipient['service'];
  if (service == 'GCM') {
    var messageRequest = {
      'Addresses': {
        [token]: {
          'ChannelType' : 'GCM'
        }
      },
      'MessageConfiguration': {
        'GCMMessage': {
          'Action': action,
          'Body': message,
          'Priority': priority,
          'SilentPush': silent,
          'Title': title,
          'TimeToLive': ttl,
          'Url': url
        }
      }
    };
  } else if (service == 'APNS') {
    var messageRequest = {
      'Addresses': {
        [token]: {
          'ChannelType' : 'APNS'
        }
      },
      'MessageConfiguration': {
        'APNSMessage': {
```

```
          'Action': action,
          'Body': message,
          'Priority': priority,
          'SilentPush': silent,
          'Title': title,
          'TimeToLive': ttl,
          'Url': url
        }
      }
    };
  } else if (service == 'BAIDU') {
    var messageRequest = {
      'Addresses': {
        [token]: {
          'ChannelType' : 'BAIDU'
        }
      },
      'MessageConfiguration': {
        'BaiduMessage': {
          'Action': action,
          'Body': message,
          'SilentPush': silent,
          'Title': title,
          'TimeToLive': ttl,
          'Url': url
        }
      }
    };
  } else if (service == 'ADM') {
    var messageRequest = {
      'Addresses': {
        [token]: {
          'ChannelType' : 'ADM'
        }
      },
      'MessageConfiguration': {
        'ADMMessage': {
          'Action': action,
          'Body': message,
          'SilentPush': silent,
          'Title': title,
          'Url': url
        }
      }
```

```
    };
  }

  return messageRequest
}

function ShowOutput(data){
  if (data["MessageResponse"]["Result"][recipient["token"]]["DeliveryStatus"]
      == "SUCCESSFUL") {
    var status = "Message sent! Response information: ";
  } else {
    var status = "The message wasn't sent. Response information: ";
  }
  console.log(status);
  console.dir(data, { depth: null });
}

function SendMessage() {
  var token = recipient['token'];
  var service = recipient['service'];
  var messageRequest = CreateMessageRequest();

  // Specify that you're using a shared credentials file, and specify the
  // IAM profile to use.
  var credentials = new AWS.SharedIniFileCredentials({ profile: 'default' });
  AWS.config.credentials = credentials;

  // Specify the AWS Region to use.
  AWS.config.update({ region: region });

  //Create a new Pinpoint object.
  var pinpoint = new AWS.Pinpoint();
  var params = {
    "ApplicationId": applicationId,
    "MessageRequest": messageRequest
  };

  // Try to send the message.
  pinpoint.sendMessages(params, function(err, data) {
    if (err) console.log(err);
    else     ShowOutput(data);
  });
}
```

```
SendMessage()
```

Python

使用 AWS SDK for Python (Boto3)藉此範例傳送推送通知。這個範例假設您已經安裝並設定SDK了Python (Boto3)。

此範例也會假設您使用共用的登入資料檔案，指定現有 使用者的存取金鑰和私密存取金鑰。如需詳細資訊，請參閱AWS SDK針對 Python (Boto3) API 參考資料中的認證。

```
import json
import boto3
from botocore.exceptions import ClientError

# The AWS Region that you want to use to send the message. For a list of
# AWS Regions where the API is available
region = "us-east-1"

# The title that appears at the top of the push notification.
title = "Test message sent from End User Messaging Push."

# The content of the push notification.
message = ("This is a sample message sent from End User Messaging Push by using the
 "
           "AWS SDK for Python (Boto3).")

# The application ID to use when you send this message.
# Make sure that the push channel is enabled for the project or application
# that you choose.
application_id = "ce796be37f32f178af652b26eexample"

# A dictionary that contains the unique token of the device that you want to send
 the
# message to, and the push service that you want to use to send the message.
recipient = {
    "token": "a0b1c2d3e4f5g6h7i8j9k0l1m2n3o4p5q6r7s8t9u0v1w2x3y4z5a6b7c8d8e9f0",
    "service": "GCM"
    }

# The action that should occur when the recipient taps the message. Possible
# values are OPEN_APP (opens the app or brings it to the foreground),
# DEEP_LINK (opens the app to a specific page or interface), or URL (opens a
# specific URL in the device's web browser.)
```

```
action = "URL"

# This value is only required if you use the URL action. This variable contains
# the URL that opens in the recipient's web browser.
url = "https://www.example.com"

# The priority of the push notification. If the value is 'normal', then the
# delivery of the message is optimized for battery usage on the recipient's
# device, and could be delayed. If the value is 'high', then the notification is
# sent immediately, and might wake a sleeping device.
priority = "normal"

# The amount of time, in seconds, that the push notification service provider
# (such as FCM or APNS) should attempt to deliver the message before dropping
# it. Not all providers allow you specify a TTL value.
ttl = 30

# Boolean that specifies whether the notification is sent as a silent
# notification (a notification that doesn't display on the recipient's device).
silent = False

# Set the MessageType based on the values in the recipient variable.
def create_message_request():

    token = recipient["token"]
    service = recipient["service"]

    if service == "GCM":
        message_request = {
            'Addresses': {
                token: {
                    'ChannelType': 'GCM'
                }
            },
            'MessageConfiguration': {
                'GCMMessage': {
                    'Action': action,
                    'Body': message,
                    'Priority' : priority,
                    'SilentPush': silent,
                    'Title': title,
                    'TimeToLive': ttl,
                    'Url': url
                }
```

```
            }
        }
    elif service == "APNS":
        message_request = {
            'Addresses': {
                token: {
                    'ChannelType': 'APNS'
                }
            },
            'MessageConfiguration': {
                'APNSMessage': {
                    'Action': action,
                    'Body': message,
                    'Priority' : priority,
                    'SilentPush': silent,
                    'Title': title,
                    'TimeToLive': ttl,
                    'Url': url
                }
            }
        }
    elif service == "BAIDU":
        message_request = {
            'Addresses': {
                token: {
                    'ChannelType': 'BAIDU'
                }
            },
            'MessageConfiguration': {
                'BaiduMessage': {
                    'Action': action,
                    'Body': message,
                    'SilentPush': silent,
                    'Title': title,
                    'TimeToLive': ttl,
                'Url': url
                }
            }
        }
    elif service == "ADM":
        message_request = {
            'Addresses': {
                token: {
                    'ChannelType': 'ADM'
```

```
                }
            },
            'MessageConfiguration': {
                'ADMMessage': {
                    'Action': action,
                    'Body': message,
                    'SilentPush': silent,
                    'Title': title,
                    'Url': url
                }
            }
        }
    else:
        message_request = None

    return message_request

# Show a success or failure message, and provide the response from the API.
def show_output(response):
    if response['MessageResponse']['Result'][recipient["token"]]['DeliveryStatus']
 == "SUCCESSFUL":
        status = "Message sent! Response information:\n"
    else:
        status = "The message wasn't sent. Response information:\n"
    print(status, json.dumps(response,indent=4))

# Send the message through the appropriate channel.
def send_message():

    token = recipient["token"]
    service = recipient["service"]
    message_request = create_message_request()

    client = boto3.client('pinpoint',region_name=region)

    try:
        response = client.send_messages(
            ApplicationId=application_id,
            MessageRequest=message_request
        )
    except ClientError as e:
        print(e.response['Error']['Message'])
    else:
        show_output(response)
```

```
send_message()
```

# 其他資源

- 如需有關推播通道範本的詳細資訊，請參閱 Amazon Pinpoint 使用者指南中的建立推播通知範本。

# 在應用程式中接收推送通知

下列主題說明如何修改 Swift、Android、反應原生或 Flutter 應用程式，以便接收推送通知。

主題



## 設定快速推播通知

iOS 應用程式的推播通知會使用 Apple 推播通知服務 (APNs) 傳送。在您可以傳送推送通知至 iOS 裝置之前，您必須在 Apple 開發人員入口網站上建立一個應用程式 ID，並且必須建立必要的憑證。您可以在 AWS Amplify 文件中的設定推播通知服務中找到有關完成這些步驟的詳細資訊。

### 使用APNs令牌

根據最佳實務，您應該開發應用程式，以便在重新安裝應用程式時重新產生客戶的裝置字符。

如果收件人將其裝置升級到新的 iOS 主要版本 (例如，從 iOS 12 升級到 iOS 13)，並在稍後重新安裝您的應用程式，則應用程式會產生新的字符。如果您的應用程式未重新整理字符，則會使用較舊的字符來傳送通知。因此，Apple 推送通知服務（APNs）拒絕通知，因為令牌現在無效。當您嘗試傳送通知時，您會收到來自的訊息失敗通知APNs。

## 設定 Android 推送通知

Android 應用程序的推送通知使用 Firebase 雲消息傳遞（FCM）發送，該消息傳遞（ ）取代谷歌雲消息傳遞（GCM）。您必須先取得FCM認證，才能傳送推播通知至 Android 裝置。接著您可以使用那些登入資料來建立 Android 專案，並啟動可接收推送通知的範例應用程式。您可以在 AWS Amplify 文件的「推送通知」一節中找到有關完成這些步驟的詳細資訊。

# 設定 Flutter 推播通知

Flutter 應用程序的推送通知使用火力地堡雲消息傳遞（FCM）安卓系統和 iOS APNs 發送。您可以在 AWS Amplify Flutter 文件的推播通知區段中，找到完成相關步驟的詳細資訊。

# 設定 React Native 推播通知

反應本機應用程序的推送通知使用火力地堡雲消息傳遞（FCM）APNs為 Android 和 iOS 發送。您可以在 AWS Amplify JavaScript 文件的「推送通知」一節中找到有關完成這些步驟的詳細資訊。

# 在一 AWS 般使用者訊息推送中建立應用程式

若要在「一 AWS 般使用者訊息推送」中開始傳送推播通知，您必須建立應用程式。接著，您必須提供適當的登入資料，以啟用您想要使用的推送通知管道。

您可以使用「一般使用者訊息推送」主控台來建立新應 AWS 用程式並設定推播通道。如需詳細資訊，請參閱 建立應用程式並啟用推播通道。

您也可以使用API、a 或 AWS Command Line Interface(AWS CLI) 來建立和設定應用程式。AWS SDK若要建立應用程式，請使用Apps資源。若要設定推送通知管道，請使用下列資源：

- APNs通道使用 Apple 推送通知服務將消息發送給 iOS 設備的用戶。
- ADM通道將消息發送到 Amazon Kindle 消防設備的用戶。
- 百度管道，以傳送訊息給百度使用者。
- GCM使用火力地堡雲消息傳遞（FCM）將消息發送到 Android 設備的渠道，該消息取代了谷歌雲消息傳遞（GCM）。

# 處理推送通知

取得傳送推播通知所需的認證後，您可以更新應用程式，以便他們能夠接收推播通知。如需詳細資訊，請參閱文件中的推播通知 — 入門。 AWS Amplify

# 刪除應用程式

此程序會從您的帳戶和應用程式中的所有資源中移除應用程式。

## 上下文

Application (應用程式)

應用程式是所有「一 AWS 般使用者訊息推送」設定的儲存容器。該應用程序還存儲您的 Amazon Pinpoint 渠道，營銷活動和旅程設置。

## 程序

1. 在開啟一 AWS 般使用者訊息推送主控台https://console.aws.amazon.com/push-notifications/。
2. 選擇應用程式，然後選擇 [刪除]。
3. 在刪除應用程式視窗中輸入，**`delete`**然後選擇刪除。

> **Important**
>
> 任何 Amazon Pinpoint 通道、行銷活動、旅程或細分也會一併刪除。

# 最佳實務

即使您已將客戶的最佳利益列入考量，仍會遇到可能影響您的訊息可交付性的情況。下節提供的建議，有助推播通訊觸及目標受眾。

## 傳送大量推播通知

傳送大量推播通知之前，請確定您的帳戶已設定為支援您的輸送量需求。根據預設，所有帳戶都設定為每秒傳送 25,000 封郵件。若需要在一秒鐘內傳送超過 25,000 封郵件，可以請求增加配額。如需詳細資訊，請參閱 使用 AWS 者訊息推送的配額。

請確定您的帳戶已正確設定使用您計劃使用的每個推播通知提供者的認證，例如FCM或APNs。

最後想出處理例外訊息的方法。每個推播通知服務提供的例外訊息都不同。對於交易式傳送，如果對應的平台 Token (例如FCM) 或憑證 (例如) 在訊息傳送期間判定為無效，則每個端點狀態碼為 400 永久失敗，APN則API呼叫的主要狀態碼為 200。

# 使用 AWS 者訊息推送中的安全性

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端安全性 — AWS 負責保護中執行 AWS 服務的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。若要瞭解適用於「一 AWS 般使用者訊息推送」的規範計劃，請參閱AWS 符合性計劃的規範AWS)。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您瞭解如何在使用「一般使用者訊息推送」時套 AWS 用共用責任模型。下列主題說明如何設定「一 AWS 般使用者訊息推送」，以符合您的安全性與合規性目標。您也會學到如何使用其他可 AWS 協助您監視和保護使用 AWS 者訊息推送資源的服務。

主題

- AWS 終端使用者訊息推送中的資料保護
- 使用者訊息推送的 AWS 身分識別與存取管理
- 一 AWS 般使用者訊息推送的符合性驗證
- AWS 終端使用者訊息推送中的彈性
- 使用者訊息推送中的基礎 AWS 結構安全
- 組態與漏洞分析
- 安全最佳實務

## AWS 終端使用者訊息推送中的資料保護

AWS 共用責任模型適用於「一 AWS 般使用者訊息推送」中的資料保護。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需有關資料隱私權的詳細資訊，請參閱資料隱私權FAQ。 如需歐洲資料保護的相關資訊，請參閱AWS 安全性GDPR部落格上的AWS 共同責任模型和部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 認證並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 對每個帳戶使用多重要素驗證 (MFA)。
- 使用SSL/TLS與 AWS 資源溝通。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 使用設定API和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果 AWS 透過命令列介面或存取時需要 FIPS 140-2 驗證的密碼編譯模組API，請使用端點。FIPS 如需有關可用FIPS端點的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用一 AWS 般使用者訊息推送或其他 AWS 服務 使用主控台API AWS CLI、、或 AWS SDKs。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供URL給外部伺服器，我們強烈建議您不要在中包含認證資訊，URL以驗證您對該伺服器的要求。

## 資料加密

AWS 一般使用者訊息推送資料在傳輸和靜態時都會加密。當您將資料提交至「一 AWS 般使用者訊息推送」時，它會在接收和儲存資料時加密資料。當您從「一般使用 AWS 者訊息推送」擷取資料時，它會使用目前的安全性通訊協定將資料傳送給您。

### 靜態加密

AWS 「一般使用者訊息推送」會加密其為您儲存的所有資料。這包括設定資料、使用者和端點資料、分析資料，以及您新增或匯入至一 AWS 般使用者訊息推送的任何資料。為了加密您的資料，一 AWS 般使用者訊息推送會使用服務所擁有並代表您維護的內部 AWS Key Management Service (AWS KMS) 金鑰。我們會定期輪換這些金鑰。如需相關資訊 AWS KMS，請參閱開AWS Key Management Service 發人員指南。

## 傳輸中加密

AWS 一般使用者訊息推送會使用HTTPS和傳輸層安全性 (TLS) 1.2 或更新版本與用戶端和應用程式進行通訊。若要與其他 AWS 服務通訊，「一 AWS 般使用者訊息推送」會使用HTTPS和 TLS 1.2。

此外，當您使用主控台、或建立和管理一 AWS 般使用者訊息推送資源時 AWS SDK AWS Command Line Interface，所有通訊都會使用HTTPS和 TLS 1.2 來保護。

## 金鑰管理

為了加密「一 AWS 般使用者訊息推送」資料，「一 AWS 般使用者訊息推送」會使用服務所擁有並代表您維護的內部 AWS KMS 金鑰。我們會定期輪換這些金鑰。您無法佈建及使用自己 AWS KMS 或其他金鑰來加密儲存在「一般使用 AWS 者訊息推送」中的資料。

## 網際網路流量隱私權

網路間流量隱私權是指保護一 AWS 般使用者訊息推送與內部部署用戶端和應用程式之間，以及使用者訊息推送與相同 AWS 區域中其他 AWS 資源之間 AWS 的連線和流量的安全。下列功能和做法可協助您確保「一 AWS 般使用者訊息推送」的網路間流量隱私權。

### 使用者訊息推送與內部部署用戶端與應用程式之 AWS 間的

若要在使用者訊息推送與內部部署網路上的用戶端與應用程式之 AWS 間建立私人連線，您可以使用 AWS Direct Connect。這可讓您使用標準光纖乙太網路纜線將網路連結至某個 AWS Direct Connect 位置。纜線的一端連接到路由器。另一端連接到 AWS Direct Connect 路由器。如需詳細資訊，請參閱《 AWS Direct Connect使用者指南》中的什麼是AWS Direct Connect ？。

為了協助透過已發佈的「一 AWS 般使用者訊息推送」安全存取APIs，建議您遵守通API話的「使用 AWS 者訊息推送」需求。 AWS 使用者訊息推送要求用戶端使用傳輸層安全性 (TLS) 1.2 或更新版本。客戶還必須支持具有完美正向保密（ ）的密碼套件，例如短暫的迪菲-赫爾曼（PFS）或橢圓曲線迪菲-赫爾曼短暫（ ）。DHE ECDHE現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與您 AWS 帳戶 AWS Identity and Access Management (IAM) 主體相關聯的秘密存取金鑰來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 來產生暫時安全登入資料來簽署請求。

### 一 AWS 般使用者訊息推送與其他 AWS 資源之間的流量

為了保護一般使用 AWS 者訊息推送與相同 AWS 區域中其他 AWS 資源之間的通訊安全，一 AWS 般使用者訊息推送預設會使用HTTPS和 TLS 1.2。

# 使用者訊息推送的 AWS 身分識別與存取管理

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM系統管理員控制誰可以驗證 (登入) 和授權 (具有權限) 使用一 AWS 般使用者訊息推送資源。IAM是一種您 AWS 服務 可以使用，無需額外費用。

主題



## 物件

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，視您在「使用 AWS 者訊息推送」中所做的工作而定。

服務使用者 — 如果您使用「一 AWS 般使用者訊息推送」服務執行工作，則系統管理員會為您提供所需的認證和權限。當您使用更多使用 AWS 者訊息推送功能來完成工作時，您可能需要其他權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取「一 AWS 般使用者訊息推送」中的功能，請參閱疑難排 AWS 解使用者訊息推播身分和存取。

服務管理員 — 如果您負責公司的「一 AWS 般使用者訊息推送」資源，您可能擁有「一 AWS 般使用者訊息推送」的完整存取權。判斷服務使用者應存取哪些使用 AWS 者訊息推送功能和資源是您的工作。然後，您必須向IAM管理員提交請求，才能變更服務使用者的權限。檢閱此頁面上的資訊，以瞭解的基本概念IAM。若要深入瞭解貴公司如何IAM搭配使用 AWS 者訊息推送使用，請參閱一 AWS 般使用者訊息推送如何搭配使用 IAM。

IAM系統管理員 — 如果您是IAM系統管理員，您可能想要瞭解如何撰寫原則以管理使用 AWS 者訊息推送存取權的詳細資料。若要檢視可在中使用的一 AWS 般使用者訊息推送身分型原則範例IAM，請參閱。一 AWS 般使用者訊息推送的身分識別型原則範例

# 使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以IAM使用者身分或假設IAM角色來驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM身分識別中心) 使用者、貴公司的單一登入驗證，以及您的 Google 或 Facebook 認證都是聯合身分識別的範例。當您以同盟身分登入時，您的管理員先前會使用IAM角色設定聯合身分識別。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以密碼編譯方式簽署您的要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署要求的詳細資訊，請參閱使用IAM者指南中的簽署 AWS API要求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。若要深入瞭解，請參閱使用AWS IAM Identity Center 者指南中的多重要素驗證和使用多重要素驗證 (MFA) AWS的使用IAM者指南。

## AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以 root 使用者身分登入的完整工作清單，請參閱《使用指南》中的〈需要 root 使用者認證的IAM工作〉。

## 聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步至您自己身分識別來源中的一組使用者和群組，以便在所有應用

程式 AWS 帳戶 和應用程式中使用。如需IAM身分識別中心的相關資訊，請參閱IAM識別中心是什麼？在《AWS IAM Identity Center 使用者指南》中。

## IAM 使用者和群組

IAM使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定權限。在可能的情況下，我們建議您仰賴臨時登入資料，而不要建立具有長期認證 (例如密碼和存取金鑰) 的IAM使用者。不過，如果您的特定使用案例需要使用IAM者的長期認證，建議您輪換存取金鑰。如需詳細資訊，請參閱《使用指南》中的「IAM定期輪換存取金鑰」以瞭解需要長期認證的使用案例。

IAM群組是指定IAM使用者集合的身分識別。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為的群組，IAMAdmins並授與該群組管理IAM資源的權限。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。要了解更多信息，請參閱《IAM用戶指南》中的創建用戶（而不是角色）的IAM時間。

## IAM 角色

IAM角色是您 AWS 帳戶 中具有特定權限的身份。它類似於用IAM戶，但不與特定人員相關聯。您可以 AWS Management Console 透過切換角色來暫時擔任中的角色。IAM您可以透過呼叫 AWS CLI 或 AWS API作業或使用自訂來擔任角色URL。如需有關使用角色方法的詳細資訊，請參閱《使用指南》中的IAM〈使用IAM角色〉。

IAM具有臨時認證的角色在下列情況下很有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱《使用指南》中的〈建立第三方身分識別提供IAM者的角色〉。如果您使用IAM身分識別中心，則需要設定權限集。為了控制身分驗證後可以存取的內IAM容，IAMIdentity Center 會將權限集與中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時IAM使用者權限 — IAM 使用者或角色可以假定某個IAM角色，暫時取得特定工作的不同權限。
- 跨帳戶存取 — 您可以使用IAM角色允許不同帳戶中的某個人 (受信任的主體) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要瞭解跨帳戶存取角色與以資源為基礎的政策之間的差異，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。

- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或將物件存放在 Amazon S3 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用使用IAM者或角色執行中的動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。
  - 服務角色 — 服務角色是指服務代表您執行動作所代表的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。
- 在 Amazon 上執行的應用程式 EC2 — 您可以使用IAM角色來管理在執行個體上EC2執行的應用程式以及發出 AWS CLI 或 AWS API請求的臨時登入資料。這比在EC2實例中存儲訪問密鑰更好。若要將 AWS 角色指派給EC2執行個體並讓其所有應用程式都能使用，請建立附加至執行個體的執行個體設定檔。執行個體設定檔包含角色，可讓執行個體上EC2執行的程式取得臨時登入資料。如需詳細資訊，請參閱使用者指南中的使用IAM角色將許可授與在 Amazon EC2 執行個體上執行的應IAM用程式。

要了解是否使用IAM角色還是用IAM戶，請參閱《用戶指南》中的「IAM創建IAM角色的時機（而不是用戶）」。

## 使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以JSON文件的形式儲存在中。如需有關JSON原則文件結構和內容的詳細資訊，請參閱《IAM使用指南》中的策略概觀。JSON

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

IAM原則會定義動作的權限，不論您用來執行作業的方法為何。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或取得角色資訊 AWS API。

### 身分型政策

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管策略或內嵌策略之間進行選擇，請參閱《IAM使用手冊》中的「在受管策略和內嵌策略之間進行選擇」。

### 資源型政策

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的策略IAM中使用 AWS 受管政策。

### 存取控制清單 (ACLs)

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

Amazon S3 和 Amazon VPC 是支持服務的示例ACLs。 AWS WAF若要進一步了解ACLs，請參閱 Amazon 簡單儲存服務開發人員指南中的存取控制清單 (ACL) 概觀。

### 其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 權限界限 — 權限界限是一項進階功能，您可以在其中設定以身分識別為基礎的原則可授與給IAM實體 (IAM使用者或角色) 的最大權限。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界

限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需有關權限界限的詳細資訊，請參閱《IAM使用指南》中的IAM實體的權限界限。

- 服務控制策略 (SCPs) — SCPs 是指定中組織或組織單位 (OU) 最大權限的JSON策略 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。如果您啟用組織中的所有功能，則可以將服務控制策略 (SCPs) 套用至您的任何或所有帳戶。SCP限制成員帳戶中實體的權限，包括每個帳戶 AWS 帳戶根使用者。若要取得有關 Organizations 的更多資訊SCPs，請參閱《AWS Organizations 使用指南》中的〈SCPs運作方式〉
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱《IAM使用指南》中的工作階段原則。

### 多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要瞭解如何在涉及多個原則類型時 AWS 決定是否允許要求，請參閱IAM使用指南中的原則評估邏輯。

## 一 AWS 般使用者訊息推送如何搭配使用 IAM

在您用IAM來管理一般使用 AWS 者訊息推送的存取權之前，請先了解哪些IAM功能可與使用 AWS 者訊息推送搭配使用。

IAM您可以搭配使用 AWS 者訊息推送使用的功能

| IAM 功能 | AWS 終端使用者訊息推送支援 |
| --- | --- |
| 身分型政策 | 是 |
| 資源型政策 | 是 |
| 政策動作 | 是 |
| 政策資源 | 是 |
| 政策條件索引鍵 | 是 |
| ACLs | 否 |

| IAM 功能 | AWS 終端使用者訊息推送支援 |
| --- | --- |
| ABAC(策略中的標籤) | 部分 |
| 臨時憑證 | 是 |
| 主體許可 | 是 |
| 服務角色 | 是 |
| 服務連結角色 | 否 |

若要取得使用 AWS 者訊息推送和其他 AWS 服務如何與大部分IAM功能搭配運作的高階檢視，請參閱《IAM使用者指南》IAM中的適用AWS 服務。

## 一般使用者訊 AWS 息推送的身分識別型原則

支援以身分識別為基礎的原則：是

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

使用以IAM身分識別為基礎的策略，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要瞭解可在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的IAMJSON策略元素參考資料。

一 AWS 般使用者訊息推送的身分識別型原則範例

若要檢視一般使用 AWS 者訊息推送身分型原則的範例，請參閱。一 AWS 般使用者訊息推送的身分識別型原則範例

## 一般使用者訊息推送中 AWS 的資源型政策

支援以資源為基礎的政策：是

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條

件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

若要啟用跨帳戶存取，您可以在以資源為基礎的策略中指定一個或多個帳戶中的一個或多個帳戶中的IAM實體作為主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主參與者和資源不同時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授與主參與者實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。

## 一 AWS 般使用者訊息推送的原則動作

支援原則動作：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON策略Action元素描述了您可以用來允許或拒絕策略中存取的動作。策略動作通常與關聯的 AWS API操作具有相同的名稱。有一些例外情況，例如沒有匹配API操作的僅限權限的操作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看一 AWS 般使用者訊息推送動作清單，請參閱服務授權參考中的使用 AWS 者訊息推送定義的動作。

「一般使用 AWS 者訊息推送」中的原則動作會在動作之前使用下列前置詞：

```
mobiletargeting
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "mobiletargeting:action1",
      "mobiletargeting:action2"
         ]
```

若要檢視一般使用 AWS 者訊息推送身分型原則的範例，請參閱。一 AWS 般使用者訊息推送的身分識別型原則範例

## 一 AWS 般使用者訊息推送的原則資源

支援原則資源：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

ResourceJSON原則元素會指定要套用動作的一個或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 Amazon 資源名稱 (ARN) 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看一 AWS 般使用者訊息推送資源類型及其清單ARNs，請參閱服務授權參考中的一AWS 般使用者訊息推送定義的資源。若要瞭解您可以針對每個資源指定哪些動作，請參閱使用 AWS 者訊息推送定義ARN的動作。

若要檢視一般使用 AWS 者訊息推送身分型原則的範例，請參閱。一 AWS 般使用者訊息推送的身分識別型原則範例

## 一 AWS 般使用者訊息推送的原則條件金鑰

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，只有在IAM使用者名稱標記資源時，您才可以授與IAM使用者存取資源的權限。如需詳細資訊，請參閱《IAM使用指南》中的IAM政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《使用指南》中的AWS 全域條件內IAM容索引鍵。

若要查看一 AWS 般使用者訊息推送條件金鑰清單，請參閱服務授權參考中的一AWS 般使用者訊息推送的條件金鑰。若要瞭解您可以使用條件索引鍵的動作和資源，請參閱使用AWS 者訊息推送所定義的動作。

若要檢視一般使用 AWS 者訊息推送身分型原則的範例，請參閱。一 AWS 般使用者訊息推送的身分識別型原則範例

## ACLs在 AWS 最終用戶消息推送

支持ACLs：無

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

## ABAC使用 AWS 終端使用者訊息推送

支援 ABAC (策略中的標籤): 部分

以屬性為基礎的存取控制 (ABAC) 是一種授權策略，可根據屬性定義權限。在中 AWS，這些屬性稱為標籤。您可以將標籤附加至IAM實體 (使用者或角色) 和許多 AWS 資源。標記實體和資源是的第一步ABAC。然後，您可以設計ABAC策略，以便在主參與者的標籤與他們嘗試存取的資源上的標籤相符時允許作業。

ABAC在快速成長的環境中很有幫助，並且有助於原則管理變得繁瑣的情況。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需有關的詳細資訊ABAC，請參閱什麼是ABAC？ 在《IAM使用者指南》中。若要檢視包含設定步驟的自學課程ABAC，請參閱《使用指南》中的〈使用以屬性為基礎的存取控制 (ABAC) IAM 〉。

## 搭配一般使用 AWS 者訊息推送使用臨時認證

支持臨時憑據：是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配使用 AWS 服務 ，請參閱《IAM使用指南》IAM中的使用方式。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立臨時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需有關切換角色的詳細資訊，請參閱《IAM使用者指南》中的〈切換到角色 (主控台)〉。

您可以使用 AWS CLI 或手動建立臨時認證 AWS API。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱IAM。

## 一 AWS 般使用者訊息推送的跨服務主體權限

支援轉寄存取工作階段 (FAS)：是

當您使用使用IAM者或角色在中執行動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。

## 一 AWS 般使用者訊息推送的服務角色

支援服務角色：是

服務角色是服務假定代表您執行動作的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色 IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給

> **Warning**
>
> 變更服務角色的權限可能會中斷使用 AWS 者訊息推送功能。只有在「一 AWS 般使用者訊息推送」提供指引時，才編輯服務角色。

## AWS 終端使用者訊息推送的服務連結角色

支援服務連結角色：否

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

如需有關建立或管理服務連結角色的詳細資訊，請參閱使用IAM的AWS 服務。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

# 一 AWS 般使用者訊息推送的身分識別型原則範例

根據預設，使用者和角色沒有建立或修改一 AWS 般使用者訊息推送資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或執行工作 AWS API。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

若要瞭解如何使用這些範例原則文件來建立以IAM身分識別為基礎的JSON策略，請參閱使用指南中的IAM建立IAM策略。

如需有關「一 AWS 般使用者訊息推送」所定義之動作和資源類型的詳細資訊，包括每個資源類型的格式，請參閱服務授權參考中的 AWS 終端使用者訊息推送的動作、資源和條件索引鍵。ARNs

主題

- 政策最佳實務
- 使用一 AWS 般使用者訊息推送主控台
- 允許使用者檢視他們自己的許可

## 政策最佳實務

以身分識別為基礎的原則會決定某人是否可以在您帳戶中建立、存取或刪除「一 AWS 般使用者訊息推送」資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需詳細資訊，請參閱AWS 《IAM使用指南》中針對工作職能的AWS 受管理策略或受管理的策略。
- 套用最低權限權限 — 當您使用原則設定權限時，IAM只授與執行工作所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需有關使用套用權限IAM的詳細資訊，請參閱《使用指南》IAM中的IAM《策略與權限》。
- 使用IAM策略中的條件進一步限制存取 — 您可以在策略中新增條件，以限制對動作和資源的存取。例如，您可以撰寫政策條件，以指定必須使用傳送所有要求SSL。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱《IAM使用指南》中的IAMJSON策略元素：條件。
- 使用 IAM Access Analyzer 驗證您的原IAM則，以確保安全和功能性的權限 — IAM Access Analyzer會驗證新的和現有的原則，以便原則遵循IAM原則語言 (JSON) 和IAM最佳做法。IAMAccess

Analyzer 提供超過 100 項原則檢查和可行的建議，協助您撰寫安全且功能正常的原則。如需詳細資訊，請參閱IAM使IAM用指南中的存取分析器原則驗證。

- 需要多因素驗證 (MFA) — 如果您的案例需要使IAM用者或 root 使用者 AWS 帳戶，請開啟以取得額外MFA的安全性。若要在呼叫API作業MFA時需要，請在原則中新增MFA條件。如需詳細資訊，請參閱《IAM使用指南》中的 < 設定MFA受保護的API存取 > 。

如需中最佳作法的詳細資訊IAM，請參閱《IAM使用指南》IAM中的「安全性最佳作法」。

## 使用一 AWS 般使用者訊息推送主控台

若要存取一 AWS 般使用者訊息推送主控台，您必須擁有最少一組權限。這些權限必須允許您列 AWS 出及檢視有關 AWS 帳戶. 如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

您不需要為只對 AWS CLI 或撥打電話的使用者允許最低主控台權限 AWS API。相反地，只允許存取符合他們嘗試執行之API作業的動作。

若要確保使用者和角色仍可使用一般使用 AWS 者訊息推送主控台，請同時將AWSEndUserMessaging AWS 受管理的原則附加至實體。如需詳細資訊，請參閱《使用指南》中的〈將權限新增至IAM使用者〉。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSEndUserMessaging",
   "Effect": "Allow",
   "Action": [
    "mobiletargeting:CreateApp",
                "mobiletargeting:GetApp",
                "mobiletargeting:GetApps",
                            "mobiletargeting:DeleteApp",
                            "mobiletargeting:GetChannels",
                            "mobiletargeting:GetApnsChannel",
                            "mobiletargeting:GetApnsVoipChannel",
                            "mobiletargeting:GetApnsVoipSandboxChannel",
                            "mobiletargeting:GetApnsSandboxChannel",
                "mobiletargeting:GetAdmChannel",
                "mobiletargeting:GetBaiduChannel",
                "mobiletargeting:GetGcmChannel",
                "mobiletargeting:UpdateApnsChannel",
```

```
                "mobiletargeting:UpdateApnsVoipChannel",
                "mobiletargeting:UpdateApnsVoipSandboxChannel",
                "mobiletargeting:UpdateBaiduChannel",
                "mobiletargeting:UpdateGcmChannel",
                "mobiletargeting:UpdateAdmChannel"
            ],
   "Resource": [
    "*"
   ]
  }
 ]
}
```

## 允許使用者檢視他們自己的許可

此範例顯示如何建立原則，讓使IAM用者檢視附加至其使用者身分識別的內嵌和受管理原則。此原則包含在主控台上或以程式設計方式使用或完成此動作的 AWS CLI 權限 AWS API。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
```

```
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

# 疑難排 AWS 解使用者訊息推播身分和存取

使用下列資訊可協助您診斷及修正使用者訊息推送和時可能會遇到的常見問題IAM。 AWS

主題

- 我沒有在「一 AWS 般使用者訊息推送」中執行動作的授權
- 我沒有授權執行 iam：PassRole
- 我想要允許我以外的人員存 AWS 帳戶 取我的使用 AWS 者訊息推送資源

## 我沒有在「一 AWS 般使用者訊息推送」中執行動作的授權

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

當使用mateojacksonIAM者嘗試使用主控台來檢視虛構*my-example-widget*資源的詳細資料，但沒有虛構的mobiletargeting:*GetWidget*權限時，就會發生下列範例錯誤。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 mobiletargeting:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 mobiletargeting:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

## 我沒有授權執行 iam：PassRole

如果您收到未獲授權執行iam:PassRole動作的錯誤訊息，則必須更新您的原則，才能讓您將角色傳遞給使用 AWS 者訊息推送。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為的使用者marymajor嘗試使用主控台在「一 AWS 般使用IAM者訊息推送」中執行動作時，就會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

### 我想要允許我以外的人員存 AWS 帳戶 取我的使用 AWS 者訊息推送資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。對於支援以資源為基礎的政策或存取控制清單 (ACLs) 的服務，您可以使用這些政策授與人員存取您的資源。

如需進一步了解，請參閱以下內容：

- 若要瞭解一 AWS 般使用者訊息推送是否支援這些功能，請參閱一 AWS 般使用者訊息推送如何搭配使用 IAM。
- 若要瞭解如何提供您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM使用者指南》中 AWS 帳戶 的〈提供存取權給其他IAM使用者〉。
- 若要瞭解如何將資源存取權提供給第三方 AWS 帳戶，請參閱《IAM使用指南》中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要瞭解如何透過身分聯盟提供存取權，請參閱使用指南中的提供對外部驗證使用IAM者的存取權 (身分聯合)。
- 若要瞭解針對跨帳號存取使用角色與以資源為基礎的政策之間的差異，請參閱《使用IAM者指南》IAM中的〈跨帳號資源存取〉。

## 一 AWS 般使用者訊息推送的符合性驗證

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上進行HIPAA安全與合規架構 — 本白皮書說明公司如何使用建立符合資格的應 AWS 用程HIPAA式。

> **Note**
>
> 並非所有 AWS 服務 人都HIPAA符合資格。如需詳細資訊，請參閱合HIPAA格服務參考資料。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準 AWS 服務 與技術研究所 (NIST)、支付卡產業安全標準委員會 () 和國際標準化組織 ()PCI) 中保護安全控制指引的最佳做法，並將其對應至安全性控制。ISO
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求 PCIDSS，例如符合特定合規性架構所要求的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

# AWS 終端使用者訊息推送中的彈性

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域與低延遲、高輸送量和高冗餘網路相連。透過可用區域，您可以設計與操作的應用程式

和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱AWS 全域基礎結構。

除了 AWS 全球基礎結構之外，一 AWS 般使用者訊息推送還提供多種功能，協助支援您的資料恢復能力和備份需求。

# 使用者訊息推送中的基礎 AWS 結構安全

作為受管服務，一 AWS 般使用者簡訊推送受 Amazon Web Services：安 AWS 全程序概觀白皮書中所述的全球網路安全程序保護。

您可以使用 AWS 已發佈的API呼叫，透過網路存取一 AWS 般使用者訊息推送。用戶端必須支援「傳輸層安全性」(TLS) 1.2 或更新版本。客戶還必須支持具有完美前向保密（ ）的密碼套件，例如（短暫的迪菲-赫爾曼PFS）或DHE（橢圓曲線短暫迪菲-赫爾曼）。ECDHE現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與IAM主體相關聯的秘密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

# 組態與漏洞分析

作為受管服務，一 AWS 般使用者簡訊推送受 Amazon Web Services：安 AWS 全程序概觀白皮書中所述的全球網路安全程序保護。這表示 AWS 管理和執行基本的安全性工作和程序，以強化、修補、更新和以其他方式維護您帳戶和資源的基礎結構。這些程序已由適當的第三方進行檢閱並認證。

# 安全最佳實務

使用 AWS Identity and Access Management (IAM) 帳戶來控制API作業的存取，尤其是建立、修改或刪除資源的作業。對於API, 這樣的資源包括項目, 活動和旅程.

- 為管理 資源的每個人 (包括您自己)，建立個人使用者。請勿使用 AWS 根憑證來管理資源。
- 授予每個使用者執行其職責所需最低程度的許可。
- 使用IAM群組有效管理多個使用者的權限。
- 定期輪換您的 IAM 登入資料。

如需詳細資訊，請參閱 使用 AWS 者訊息推送中的安全性。如需相關資訊IAM，請參閱 AWS Identity and Access Management。如需有關IAM最佳做法的資訊，請參閱IAM最佳做法。

# 監督一 AWS 般使用者訊息推送

監控是維護「一 AWS 般使用者訊息推送」及其他AWS解決方案之可靠性、可用性和效能的重要組成部分。AWS提供下列監控工具，以監視「使用 AWS 者訊息推送」、在發生錯誤時回報，並在適當時採取自動動作：

- Amazon 會即時 CloudWatch監控您的 AWS 資源和執行 AWS 的應用程式。您可以收集和追蹤指標、建立自訂儀板表，以及設定警示，在特定指標達到您指定的閾值時通知您或採取動作。例如，您可以 CloudWatch 追蹤 Amazon EC2 執行個體的CPU使用情況或其他指標，並在需要時自動啟動新執行個體。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。
- Amazon CloudWatch 日誌可讓您從 Amazon EC2 執行個體和其他來源監控 CloudTrail、存放和存取日誌檔。 CloudWatch 記錄檔可以監控記錄檔中的資訊，並在符合特定臨界值時通知您。您也可以將日誌資料存檔在高耐用性的儲存空間。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南。
- Amazon EventBridge 可用於自動化 AWS 服務並自動回應系統事件，例如應用程式可用性問題或資源變更。來自 AWS 服務的事件會以近乎即時 EventBridge 的方式傳送到。您可編寫簡單的規則，來指示您在意的事件，以及當事件符合規則時所要自動執行的動作。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南。
- AWS CloudTrail擷取您帳戶或代表您的 AWS 帳戶發出的API呼叫和相關事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。

## 使用 Amazon 監控 AWS 終端使用者簡訊推送 CloudWatch

您可以使用來監視「一 AWS 般使用者訊息推送」 CloudWatch，以收集原始資料，並將其處理為可讀且接近即時的量度。這些統計資料會保留 15 個月，以便您存取歷史資訊，並更清楚 Web 應用程式或服務的執行效能。您也可以設定留意特定閾值的警示，當滿足這些閾值時傳送通知或採取動作。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

如需指標和維度的清單，請參閱 Amazon Pinpoint 位使用者指南 CloudWatch中的使用監控 Amazon 精確定位。

## 記錄 AWS 使用者訊息推送API呼叫 AWS CloudTrail

AWS 「一般使用者訊息推送」是與服務整合的服務 AWS CloudTrail，可提供使用者、角色或 AWS 服務在「一般使用 AWS 者訊息推送」中所採取之動作的記錄。 CloudTrail 將「一 AWS 般使用者

訊息推送」的所有API呼叫擷取為事件。擷取的呼叫包括來自一 AWS 般使用者訊息推送主控台的呼叫，以及對一 AWS 般使用者訊息推送API作業的程式碼呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括使用 AWS 者簡訊推送的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷向一般使用 AWS 者訊息推送提出的要求、提出要求的 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

## AWS 終端使用者訊息推送資訊 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當一 AWS 般使用者訊息推送中發生活動時，該活動會與 CloudTrail 事件歷史記錄中的其他 AWS 服務事件一起記錄在事件中。您可以查看，搜索和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

如需您 AWS 帳戶的事件持續記錄 (包括「一 AWS 般使用者訊息推送」的事件)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件並從多個帳戶接收 CloudTrail 日誌文件

所有「一 AWS 般使用者訊息推送」動作都會記錄下來， CloudTrail 並記錄在「一AWS 般使用者訊息推送API參考」中。例如，呼叫`UpdateApnsChannel`和`GetApnsVoipChannel`動作會`GetAdmChannel`在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 要求是使用 root 或 AWS Identity and Access Management (IAM) 使用者認證提出的。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱CloudTrail userIdentity元素。

# 了解一 AWS 般使用者訊息推送記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共API調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

# 使用介面端點存取一 AWS 般使用者訊息推送 (AWS PrivateLink)

您可以使用 AWS PrivateLink 在您VPC和「一 AWS 般使用者訊息推送」之間建立私人連線。您可以在不使用網際網路閘道、NAT裝置、連線或VPN AWS Direct Connect 連線的情況下VPC，就像存取一AWS 般使用者訊息推送一般使用者訊息推送一樣。您中的執行個體VPC不需要公用 IP 位址即可存取一 AWS 般使用者訊息推送。

您可以建立由 AWS PrivateLink提供支援的介面端點來建立此私有連線。我們會在您為介面端點啟用的每個子網中建立端點網路介面。這些是由要求者管理的網路介面，可做為傳送至「一 AWS 般使用者訊息推送」之流量的進入點。

如需詳細資訊，請參閱AWS PrivateLink 指南 AWS PrivateLink中的 AWS 服務 透過存取。

## 一 AWS 般使用者訊息推播的考量

在為 AWS 使用者訊息推送設定介面端點之前，請先檢閱AWS PrivateLink 手冊中的考量事項。

AWS 一般使用者訊息推送支援透過介面端點呼叫其所有API動作。

VPC AWS 終端使用者訊息推送不支援端點原則。依預設，允許透過介面端點對一 AWS 般使用者訊息推送的完整存取權。或者，您可以將安全群組與端點網路介面建立關聯，以控制透過介面端點傳送至「一 AWS 般使用者訊息推送」的流量。

## 建立一 AWS 般使用者訊息推送的介面端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface (AWS CLI) 為 AWS 終端使用者簡訊推送建立介面端點。如需詳細資訊，請參閱《AWS PrivateLink 指南》中的建立介面端點。

使用下列服務名稱為「一 AWS 般使用者訊息推送」建立介面端點：

```
com.amazonaws.region.pinpoint
```

如果您DNS為介面端點啟用 private，則可以使用其預設地區DNS名稱向一 AWS 般使用者訊息推送提出API要求。例如 `com.amazonaws.us-east-1.pinpoint`。

# 為您的介面端點建立端點政策

端點策略是您可以附加到介面端點的IAM資源。預設端點策略允許透過介面端點完整存取「一 AWS 般使用者訊息推送」。若要控制允許從您的使用 AWS 者訊息推送存取VPC，請將自訂端點原則附加到介面端點。

端點政策會指定以下資訊：

- 可以執行動作 (AWS 帳戶、IAM使用者和IAM角色) 的主參與者。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱《AWS PrivateLink 指南》中的使用端點政策控制對服務的存取。

範例： AWS 終VPC端使用者訊息推送動作的端點原則

以下是自訂端點政策的範例。當您將此原則附加至介面端點時，它會授與所有資源上所有主體列出之「一 AWS 般使用者訊息推送」動作的存取權。

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
             "mobiletargeting:CreateApp",
             "mobiletargeting:DeleteApp"
         ],
         "Resource":"*"
      }
   ]
}
```

# 使用 AWS 者訊息推送的配額

您的每項 AWS 服務都 AWS 帳戶 有預設配額 (先前稱為限制)。除非另有說明，否則每個配額都是區域特定規定。您可以請求提高某些配額，而其他配額無法提高。

若要檢視「一 AWS 般使用者訊息推送」的配額，請開啟「Service Quotas」主控台。在導覽窗格中，選擇「AWS服務」，然後選取「Amazon Pinpoint」。

您的AWS帳戶具有下列與「使用 AWS 者訊息推送」相關的配額。

| 資源 | 預設配額 | 是否可增加？ |
| --- | --- | --- |
| 行銷活動中每秒可傳送的推播通知數目上限 | 每秒 25,000 個通知 | 是，請使用 Service Quotas 主控台 |
| Amazon 設備消息（ADM）消息有效負載大小 | 每則訊息 6 KB | 否 |
| 蘋果推送通知服務（APNs）消息有效負載大小 | 每則訊息 4 KB | 否 |
| APNs 沙盒訊息承載大小 | 每則訊息 4 KB | 否 |
| 百度雲推送訊息承載大小 | 每則訊息 4 KB | 否 |
| 火力地堡雲消息傳遞（FCM）消息負載大小 | 每則訊息 4 KB | 否 |

# 一 AWS 般使用者訊息推送使用者指南的文件歷史記錄

下表說明「一 AWS 般使用者訊息推送」的文件版本。

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| 初始版本 | AWS 終端使用者訊息推送使用者指南的初始版本 | 2024年7月24日 |

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。