實作指南

AWS 上的虛擬等候室

AWS 上的虛擬等候室: 實作指南

Table of Contents

使用 上的虛擬等待室，吸收您網站的大型流量暴增 AWS

發佈日期：2021 年 11 月

解決方案上的虛擬等待室 AWS 有助於控制流量暴增期間傳入網站的使用者請求。它建立雲端基礎設施，旨在暫時將傳入流量卸載至您的網站，並提供自訂和整合虛擬等待室的選項。此解決方案可以與新的或現有的網站整合，以無縫擴展以處理流量突然激增的情況。

可能造成網站流量激增的大規模事件範例包括：

- 開始銷售音樂會或體育賽事門票
- 火力銷售或其他大型零售銷售，例如黑色星期五
- 推出新產品並發佈廣泛的行銷公告
- 檢查線上測試和課程的存取和入學
- 發佈醫療預約時段
- 推出需要建立帳戶和付款的新direct-to-customer服務

解決方案可做為您網站訪客的保留區域，並允許流量在有足夠的容量時通過。訪客使用的用戶端軟體可設定為透明地允許流量通過等待室，直到網站達到最大容量；此時等待室會保留訪客。當您的網站具有更多流量的容量時，解決方案會產生 JSON Web Token (JWT)，允許使用者存取網站。例如，如果您的事件持續兩個小時，而您的網站每秒可以處理 50 個使用者，但您預期每秒 250 個使用者，則您可以使用此解決方案來調節流量，同時允許使用者在佇列中保持位置。

此解決方案提供下列主要功能：

- 將使用者結構化佇列排入您的網站
- 控制非常大型事件大小流量的可擴展性
- 產生 JSON Web 字符以允許進入目標網站
- 所有功能都是透過 REST APIs控制
- 用戶端解決方案的 Turnkey API Gateway 授權方
- 獨立整合或搭配 OpenID 使用

此實作指南說明在 Amazon Web Services (AWS) 雲端 AWS 中部署虛擬等待室的架構考量和組態步驟。它包含 範本的連結，這些AWS CloudFormation範本會使用安全性和可用性的 AWS 最佳實務來啟動和設定部署此解決方案所需的 AWS 服務。

本指南適用於 IT 架構師、開發人員、DevOps 員工、資料分析師，以及具備 AWS 雲端架構實務經驗的行銷技術專業人員。

成本

您需負責執行此解決方案時使用 AWS 的服務成本。自此修訂起，在美國東部（維吉尼亞北部）區域中使用預設設定執行此解決方案的成本約為每堆疊每天 10.00 USD，加上相對於事件大小的 API 請求和資料流量費用。

維護解決方案而沒有任何事件的每日成本

AWS 服務	請求/時間	成本 【美元】
Amazon API Gateway	0	0.00 美元
Amazon CloudFront	0	0.00 美元
Amazon CloudWatch	0	0.00 美元
Amazon DynamoDB	0	0.00 美元
Amazon ElastiCache	運算節點小時數 (Redis)	~$6.00
AWS Lambda	免費方案*	0.00 美元
AWS Secrets Manager	免費方案*	0.00 美元
Amazon Simple Storage Service (Amazon S3)	免費方案*	0.00 美元
Amazon Virtual Private Cloud (Amazon VPC)	VPC 端點時數 NAT 閘道時數	~5.00 美元
總計：		~11.00 美元

*成本估算是根據乾淨的環境。如果您在此解決方案之外使用此 AWS 服務，可能會超過免費方案配額。

下表顯示 50，000 位使用者和 100，000 位使用者等待室的預估成本，其事件持續時間範圍為 2-4 小時，其中有 500 位使用者/秒傳入和 1，000 位使用者/分鐘傳出。價格可能變動。如需完整詳細資訊，請參閱此解決方案中使用的每個 AWS 服務的定價網頁。

2 小時事件期間 50，000 位等待室使用者的預估成本

AWS 服務	Dimensions (尺寸)	成本 【美元】
Amazon API Gateway	請求	2.00 美元
CloudFront	請求、頻寬	75.00 美元
CloudWatch	指標、警示、儲存	1.00 美元
Amazon CloudWatch Events	事件	1.00 美元
DynamoDB	讀取/寫入單位、儲存	1.00 美元
ElastiCache	節點小時數	8.00 美元
Lambda	請求、運算時間	1.00 美元
AWS Secrets Manager	秘密、請求	1.00 美元
Amazon S3	請求、儲存	1.00 美元
Amazon VPC	資料傳輸、端點時間	2.00 美元
總計		94.00 美元

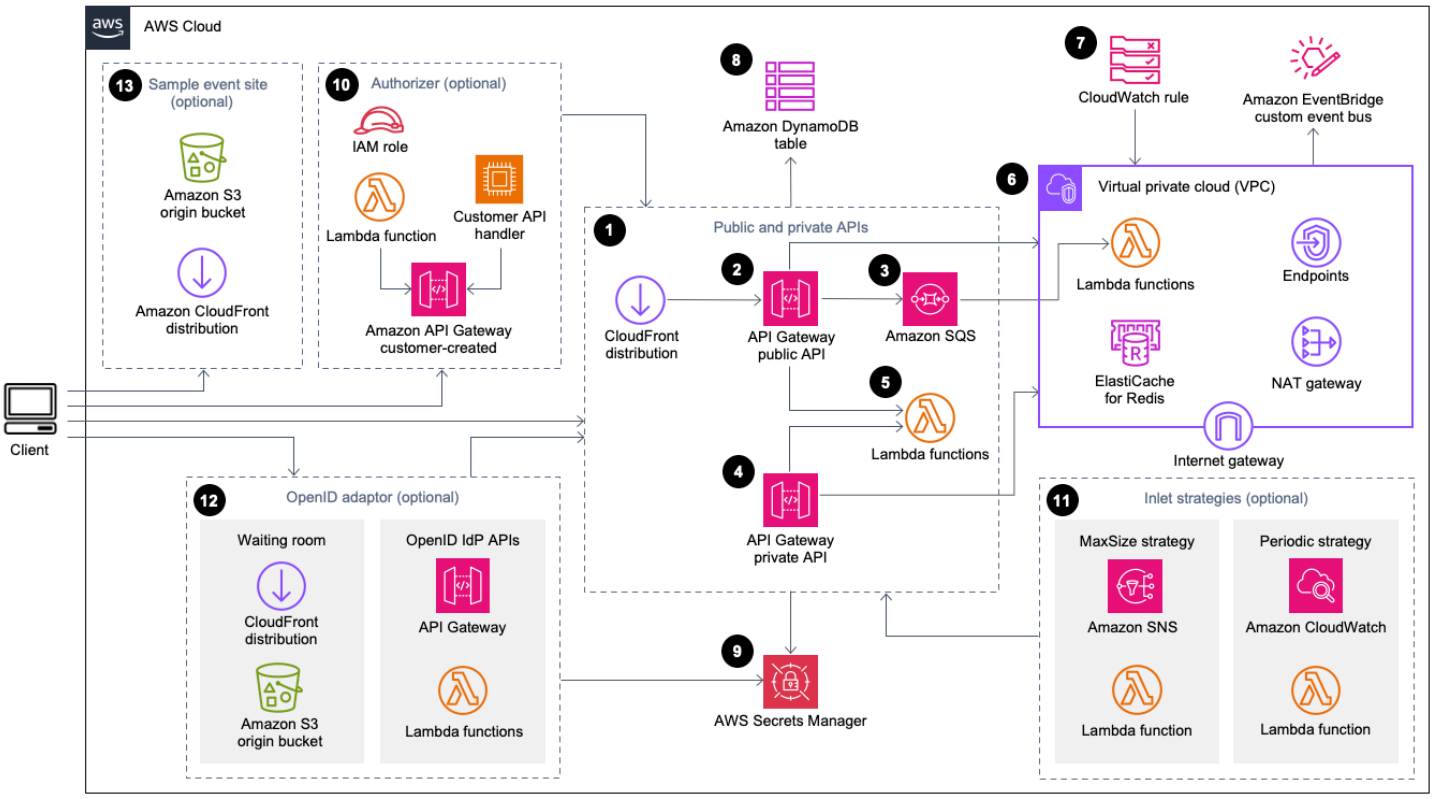
2 小時事件期間 100，000 個等待室使用者的預估成本

AWS 服務	Dimensions (尺寸)	成本 【美元】
Amazon API Gateway	請求	4.00 美元
CloudFront	請求、頻寬	296.00 美元
CloudWatch	指標、警示、儲存	1.00 美元
CloudWatch Events	事件	1.00 美元
DynamoDB	讀取/寫入單位、儲存	4.00 美元

ElastiCache	節點小時數	32.00 美元
Lambda	請求、運算時間	1.00 美元
AWS Secrets Manager	秘密、請求	1.00 美元
Amazon Simple Queue Service (Amazon SQS)	請求	1.00 美元
Amazon S3	請求、儲存	1.00 美元
Amazon VPC	資料傳輸、端點時間	6.00 美元
總計		348.00 美元

架構概觀

使用預設參數，以必要和選用的範本部署此解決方案，可在 AWS 雲端中建置下列環境。



AWS 架構上的虛擬等待室

AWS CloudFormation 範本部署下列基礎設施：

1. Amazon CloudFront 分佈，可為用戶端提供公有 API 呼叫。
2. Amazon API Gateway 公有 API 資源可處理來自虛擬等待室的佇列請求、追蹤佇列位置，並支援驗證允許存取目標網站的字符。
3. Amazon Simple Queue Service (Amazon SQS) 佇列，可調節處理佇列訊息的 AWS Lambda函數流量。SQS 佇列不會為每個請求叫用 Lambda 函數，而是將傳入的請求爆量批次處理。
4. API Gateway 私有 API 資源，以支援管理功能。
5. Lambda 函數可驗證和處理公有和私有 API 請求，並傳回適當的回應。
6. Amazon Virtual Private Cloud (VPC) 託管直接與 Elasticache (Redis OSS) 叢集互動的 Lambda 函數。VPC 端點可讓 VPC 中的 Lambda 函數與解決方案中的服務通訊。此外，NAT 閘道允許 VPC 中的 Lambda 函數連接 CloudFront 端點，並視需要使快取失效。

7. 用來叫用 Lambda 函數的 Amazon CloudWatch 規則，該函數可與自訂 Amazon EventBridge 匯流排搭配使用，以定期廣播狀態更新。
8. Amazon DynamoDB 資料表，用於存放字符、佇列位置和提供計數器資料。
9. AWS Secrets Manager 存放字符操作和其他敏感資料的金鑰。
10. （選用）授權方元件，包含 AWS Identity and Access Management(IAM) 角色和 Lambda 授權方函數，可用於 API Gateway。
11. （選用）Amazon Simple Notification Service (Amazon SNS)、CloudWatch 和 Lambda 函數，以支援兩種輸入策略。
12. （選用）OpenID 具有 API Gateway 和 Lambda 函數的 OpenID 轉接器元件，以允許 OpenID 提供者驗證網站的使用者。具有 Amazon Simple Storage Service (Amazon S3) 儲存貯體的 CloudFront 分佈，用於此元件的等待室頁面。
13. （選用）Amazon S3 原始伺服器儲存貯體的 CloudFront 分佈，用於範例等待室 Web 應用程式。

解決方案的運作方式

本節說明 AWS 虛擬等待室工作流程中高階的步驟。請參閱 GitHub 上的 開發人員指南，以取得建置、自訂和整合網站等候室的詳細資訊。

等待室的公有 API 可以位於網站周邊安全後方，或者無需任何授權即可使用。根據您使用哪種方法來整合等待室與網站，使用者可能需要先驗證網站，才能導覽至等待室並取得佇列中的位置。

用戶端軟體必須具有事件 ID，才能進入等候室並提出其他請求。事件 ID 是針對公有和私有 APIs 的大多數請求所需的唯一 ID。事件 ID 是在核心 API 堆疊的安裝期間設定。在操作期間，事件 ID 可透過等待室頁面以 URL 參數或 Cookie 的形式提供；它可以作為身分驗證字符宣告的一部分提供，也可以透過不同的資料路徑分發給用戶端。

在某些情況下，用戶端需要事件 ID 和請求 ID 才能進行特定 API 呼叫。請求 ID 是從等待室發出的唯一 ID，代表特定用戶端上線。

下列步驟說明佇列項目的 API 請求流程、等待佇列進行，以及使用網站的存取權杖離開等待室。

使用者進入等待室：

1. 使用者會看到代表等候室進入點的畫面或頁面。他們選擇輸入佇列，用戶端軟體（瀏覽器、行動裝置、裝置）會呼叫`assign_queue_num`公有 API 來請求佇列位置。
2. API Gateway 會立即將 API 請求交付至 Amazon SQS 佇列。
3. `assign_queue_num` API 呼叫會在請求放入佇列時傳回 。用戶端會收到唯一的請求 ID，稍後可用來擷取佇列位置、請求的時間和存取字符。
4. `AssignQueueNum` Lambda 函數會從 SQS 佇列接收最多十個請求的批次。Lambda 服務風扇會發出呼叫，以處理多個批次的請求。
5. `AssignQueueNum` Lambda 函數會驗證其批次中的每個訊息、將佇列計數器增加至 Elasticache (Redis OSS)，並將每個請求與其相關聯的佇列位置存放在 Elasticache (Redis OSS) 中。
6. 每個訊息都會在成功處理時刪除。涉及錯誤條件的訊息會在稍後的批次中重新處理一次。在第二次失敗後，它們會傳送至連線至 CloudWatch 警示的dead-letter-queue。
7. 用戶端在收到`assign_queue_num`來自呼叫的請求 ID 後，可以開始輪詢 `queue_num` API。用戶端會將事件 ID 和請求 ID 傳送至 `queue_num` API，並接收數值佇列位置或回應，指出請求尚未處理。在大型事件期間，用戶端可能需要進行此呼叫多次。API Gateway 會叫用 `GetQueueNum` Lambda 函數，並從 DynamoDB 傳回佇列中的用戶端數值位置。

使用者在等待室等待：

8. 在用戶端在佇列中的位置之後，可以定期開始輪詢 serving_num API。serving_num API 會以事件 ID 呼叫，並傳回佇列目前的服務位置。serving_num API 的回應會告知用戶端何時可以從等待室移至最終交易的實際目標網站。GetServingNum Lambda 函數會傳回等待室目前的服務位置。
9. 當服務位置等於或大於用戶端的佇列（請求）位置時，用戶端可以從公有 API 請求 JSON Web Token (JWT)。權杖可與目標網站搭配使用，以完成交易。generate_token API 會以事件 ID 和請求 ID 呼叫。API Gateway 會使用 參數叫用 GenerateToken Lambda 函數。
10. GenerateToken Lambda 函數會驗證請求，並檢查先前是否已產生此字符。Lambda 函數會查詢 DynamoDB 資料表，以取得相符的字符。如果找到，該字符會傳回給發起人，而且不會重新產生。此程序可防止單一請求 ID 用於產生具有新過期時間的多個不同字符。
11. 如果在 DynamoDB 中找不到字符，Lambda 函數會擷取金鑰以建立字符，並使用事件 ID 和用戶端的請求 ID 將字符儲存在 DynamoDB 中。Lambda 函數會將事件寫入 EventBridge，以表示已產生新的字符。Lambda 函數會遞增 Elasticache (Redis OSS) 計數器，以追蹤為事件產生的字符數量。
12. 如果 queue_pos_expiry已開啟，用戶端可以透過呼叫叫用 GetQueuePositionExpiryTime Lambda 函數的 queue_pos_expiry API 來查詢其到期前的剩餘時間。

使用者離開等候室：

13. 當用戶端收到其字符時，它會進入目標網站以開始其交易。根據您的基礎設施支援與 JWT 整合的方式，用戶端可能需要在請求標頭、Cookie 或其他方式中呈現字符。API Gateway 的授權方可用來驗證用戶端請求中包含的字符。用於驗證和管理 JWTs的任何商業或開放原始碼程式庫，都可以與 AWS 字符上的虛擬等待室搭配使用。如果字符有效，則允許用戶端繼續其交易。
14. 用戶端完成交易後，會呼叫私有 API 來更新用戶端字符的狀態，並在 DynamoDB 中完成。

佇列位置過期：

15. 啟用此功能時，對應至特定佇列位置的請求 ID 才有資格在指定的時間間隔內產生字符。

佇列位置過期時遞增服務計數器：

16. 啟用此功能時，服務計數器會根據無法產生字符的過期佇列位置自動遞增。

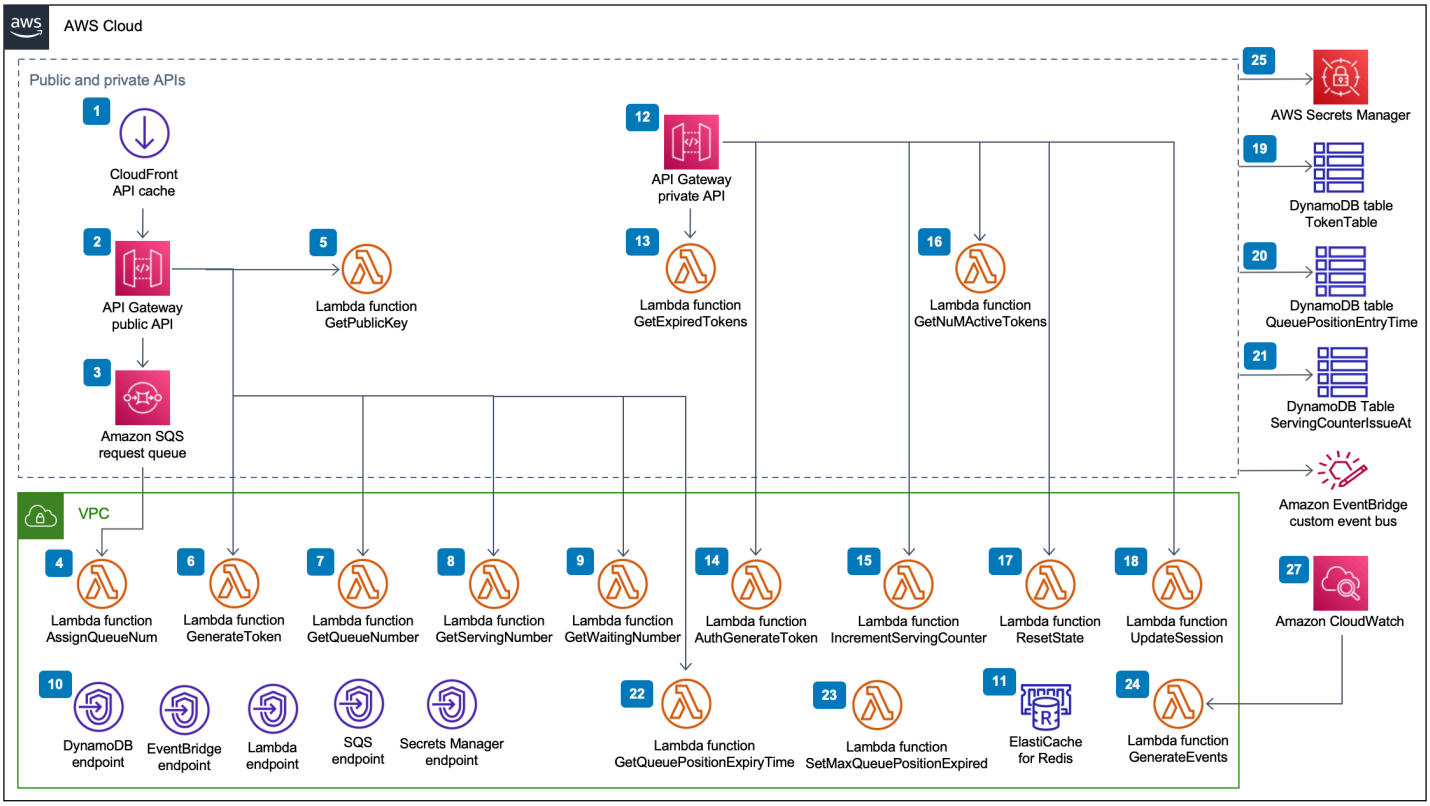
解決方案元件

等候室公有和私有 APIs

AWS 解決方案主要用途的虛擬等待室是以受控方式控制用戶端的 JSON Web 權杖 (JWT) 產生，以避免可能超過目的地網站的新使用者爆增。JWTs 可用於網站保護、防止存取網頁，直到取得等待室字符，以及 API 存取授權。

核心範本會安裝用於大多數虛擬等待室 AWS 操作的公有 API 和私有 (IAM 授權） API。公有 API 是以具有多個快取政策的 CloudFront 分佈設定，以 API 路徑為基礎。建立 DynamoDB 資料表和 EventBridge 事件匯流排。範本新增了具有兩個可用區域 (AZs) 的新 VPC、兩個AZs區域中的 Elasticache (Redis OSS) 叢集，以及數個 Lambda 函數。與 Elasticache (Redis OSS) 互動的 Lambda 函數在 VPC 中具有網路介面，而所有其他 Lambda 函數都具有預設網路連線能力。核心 APIs 是與解決方案互動的最低層。其他 Lambda 函數、Amazon Elastic Compute Cloud (Amazon EC2) 執行個體和容器可以充當延伸模組，並呼叫核心 APIs來建置等待室、控制入口流量，以及對解決方案產生的事件做出反應。

此外，核心堆疊會為其所有 Lambda 函數錯誤和調節條件建立警示，以及針對 4XX 和 5XX 狀態碼的每個 API Gateway 部署建立警示。



AWS 公有和私有 APIs元件上的虛擬等待室

1. CloudFront 分佈會為用戶端提供公有 API 呼叫，並在適當時快取結果。
2. Amazon API Gateway 公有 API 程序佇列請求來自虛擬等待室、追蹤佇列位置，並支援驗證允許存取目標網站的字符。
3. SQS 佇列會將流量調節至處理佇列訊息的 AWS Lambda 函數。
4. `AssignQueueNum` Lambda 函數會驗證其批次中接收的每個訊息、將佇列計數器增加至 Elasticache (Redis OSS)，並將每個請求與其相關聯的佇列位置存放在 Elasticache (Redis OSS) 中。
5. `GetPublicKey` Lambda 函數會從 Secrets Manager 擷取公有金鑰值。
6. `GenerateToken` Lambda 函數會為允許在目標網站完成其交易的有效請求產生 JWT。它會將已產生字符的事件寫入等待室的自訂事件匯流排。如果先前已為此請求產生字符，則不會產生新的字符。
7. `GetQueueNumber` Lambda 函數會從 Elasticache (Redis OSS) 擷取並傳回佇列中的用戶端數字位置。
8. `GetServingNumber` Lambda 函數會從 Elasticache (Redis OSS) 擷取並傳回等待室目前正在提供的號碼。
9. `GetWaitingNum` Lambda 函數會傳回目前排入等候室佇列且尚未核發字符的號碼。
10. VPC 端點可讓 VPC 中的 Lambda 函數與解決方案中的服務通訊。
11. Elasticache (Redis OSS) 叢集會存放所有請求，以使用有效的事件 ID 進入等待室。它也會存放數個計數器，例如已排入佇列的請求數、目前正在服務的請求數、產生的字符數、完成的工作階段數，以及已捨棄的工作階段數。
12. API Gateway 私有 API 資源，以支援管理功能。私有 APIs 經過 AWS IAM 驗證。
13. `GetExpiredTokens` Lambda 函數會傳回具有過期字符的請求 IDs 清單。
14. `AuthGenerateToken` Lambda 函數會為允許在目標網站完成其交易的有效請求產生字符。可以覆寫在核心堆疊部署期間最初設定的字符發行者和有效期間。它會將已產生字符的事件寫入等待室的自訂事件匯流排。如果先前已為此請求產生字符，則不會產生新的字符。
15. `IncrementServingCounter` Lambda 函數會遞增存放在 Elasticache (Redis OSS) 中的等待室服務計數器，並依值遞增。
16. `GetNumActiveTokens` Lambda 函數會查詢 DynamoDB 中尚未過期、尚未用於完成其交易，且尚未標示為已捨棄的字符數量。

17.ResetState Lambda 函數會重設存放在 Elasticache (Redis OSS) 中的所有計數器。它也會刪除並重新建立 TokenTable、 QueuePositionEntryTime和 ServingCounterIssuedAt DynamoDB 資料表。此外，它會執行 CloudFront 快取失效。

18.UpdateSession Lambda 函數會更新存放在 TokenTable DynamoDB 資料表中的工作階段 （權杖） 狀態。工作階段狀態以整數表示。工作階段設定為 狀態1表示已完成，且-1表示已捨棄。它會將事件寫入等待室的自訂事件匯流排，表示工作階段已更新。

19.TokenTable DynamoDB 資料表存放字符資料。

20.QueuePositionEntryTime DynamoDB 資料表存放佇列位置和進入時間資料。

21.ServingCounterIssuedAt DynamoDB 資料表會儲存服務計數器的更新。

22.當用戶端請求剩餘的佇列位置到期時間時，會叫用 GetQueuePositionExpireTime Lambda 函數。

23.SetMaxQueuePositionExpired Lambda 函數會設定與ServingCounterIssuedAt資料表值對應的已過期佇列位置上限。如果 IncrSvcOnQueuePositionExpiry 參數在核心堆疊部署true期間設定為 ，它會每分鐘執行一次。

24.GenerateEvents Lambda 函數會將各種等待室指標寫入等待室的自訂事件匯流排。如果啟用事件產生參數在核心堆疊部署true期間設定為 ，它會每分鐘執行一次。

25.AWS Secrets Manager 會存放字符操作和其他敏感資料的金鑰。

26.Amazon EventBridge 自訂事件匯流排會在每次產生字符時接收事件，並在 TokenTable DynamoDB 資料表中更新工作階段。當服務計數器在 SetMaxQueuePositionExpired Lambda 中移動時，它也會接收事件。如果在核心堆疊部署期間啟用，它會使用各種等待室指標寫入 。

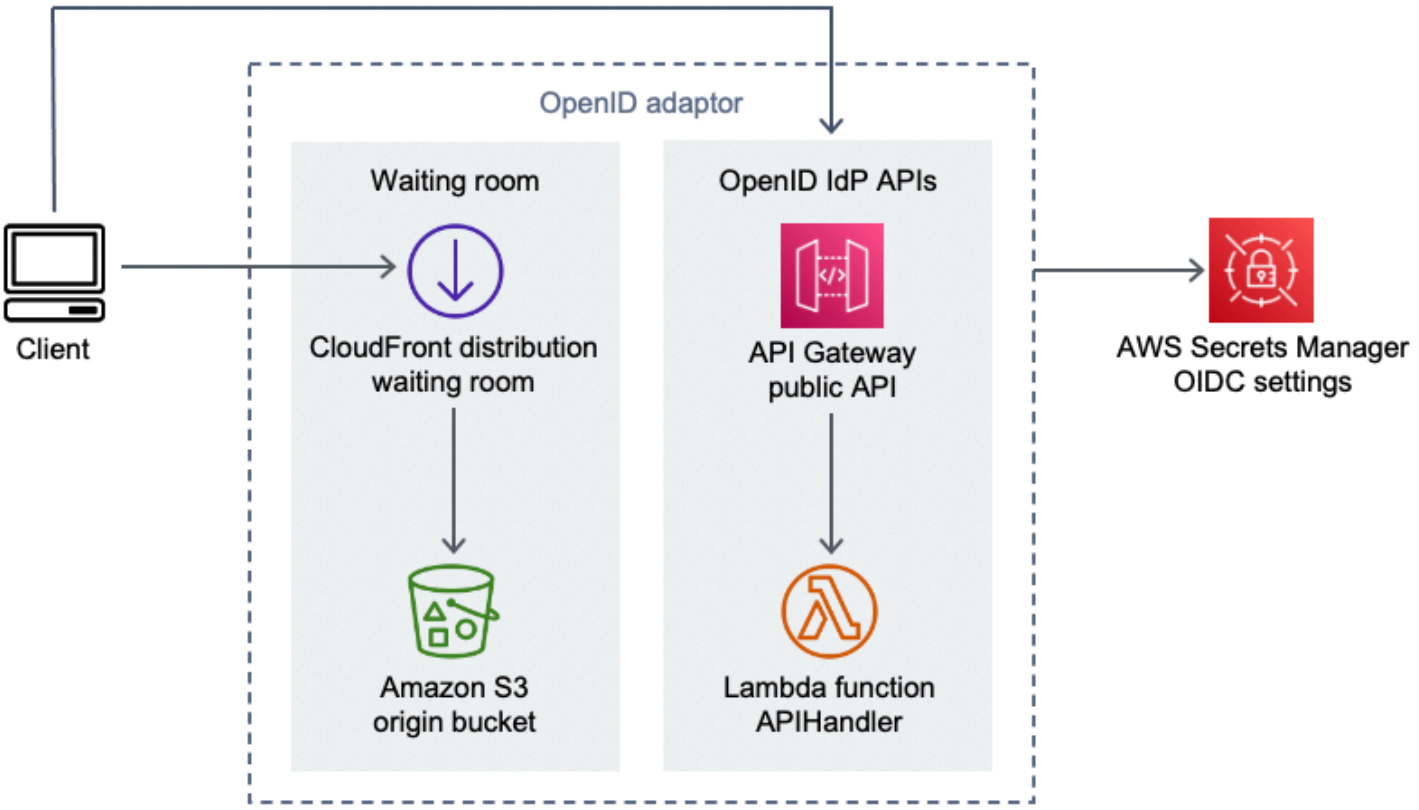
27.如果啟用事件產生參數在核心堆疊部署期間設定為 true，則會建立 Amazon CloudWatch 事件規則。此事件規則每分鐘啟動 GenerateEvents Lambda 函數。

Authorizers

解決方案包含 API Gateway Lambda 授權方堆疊。堆疊包含一個 IAM 角色和一個 Lambda 函數。APIGatewayAuthorizer Lambda 函數是 API Gateway 的授權方，可驗證 AWS API 上的虛擬等待室所發行字符的簽章和宣告。堆疊隨附的 Lambda 函數可用來保護雲端 APIs，直到使用者經過等待室並收到存取權杖為止。授權方會自動從核心 API 擷取和快取公有金鑰和組態，以進行權杖驗證。它可以在不修改的情況下使用，並且可以安裝在 支援的任何 AWS 區域中 AWS Lambda。

OpenID 轉接器

OpenID 轉接器堆疊會部署 API Gateway 和 Lambda 函數，做為 OpenID 身分提供者。OpenID 轉接器提供一組與 OIDC 相容的 APIs，可與支援 OIDC 身分提供者的現有 Web 託管軟體搭配使用，例如 AWS Elastic Load Balancer、WordPress 或 Amazon Cognito 或類似服務的聯合身分提供者。轉接器可讓客戶在使用具有有限整合選項的off-the-shelf Web 託管軟體時，在 AuthN/AuthZ 流程中使用等候室。堆疊也會安裝 CloudFront 分佈，其中有一個 Amazon S3 儲存貯體做為原始伺服器，另一個 S3 儲存貯體用於記錄請求。OpenID 轉接器提供範例等待室頁面，類似於範例等待室堆疊中提供的頁面，但專為 OpenID 身分驗證流程而設計。驗證的程序包括在等待室佇列中取得位置，並等待服務位置等於或大於用戶端的佇列位置。OpenID 等待室頁面會重新導向回目標網站，該網站使用 OpenID API 完成用戶端的字符取得和工作階段組態。此解決方案的 API 端點會直接對應至官方 OpenID Connect 1.0 流程規格，即 name-for-name。如需詳細資訊，請參閱 OpenID Connect Core 1.0 身分驗證。



AWS OpenID 轉接器元件上的虛擬等待室

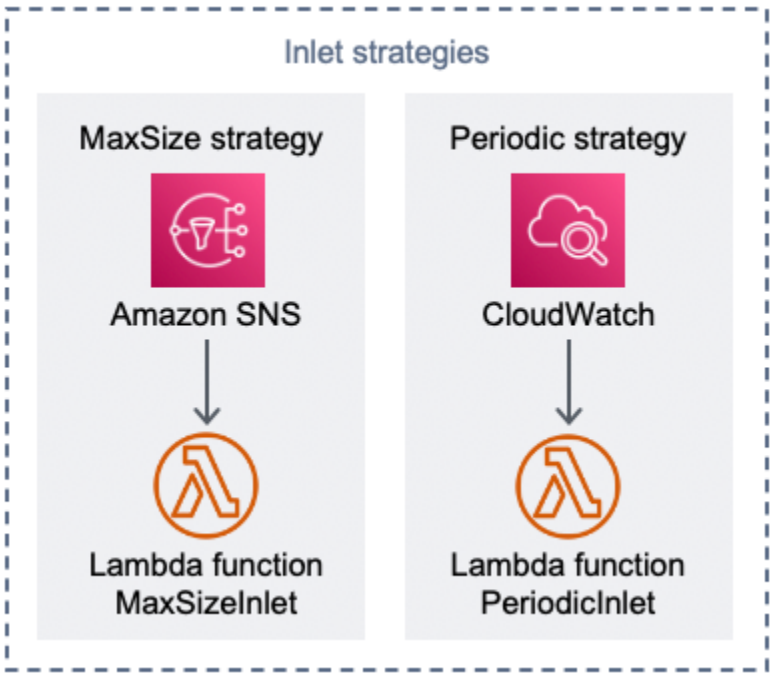
1. CloudFront 分佈會將 S3 儲存貯體的內容提供給使用者。
2. S3 儲存貯體託管範例等待室頁面。
3. Amazon API Gateway API 提供一組與 OIDC 相容的 APIs，可與支援 OIDC 身分提供者 Lambda 授權函數的現有 Web 託管軟體搭配使用。

4. APIHandler Lambda 函數會處理所有 API Gateway 資源路徑的請求。相同模組中的不同 Python 函數會映射到每個 API 路徑。例如，API Gateway 中的/authorize資源路徑會在 Lambda 函數authorize()內叫用 。
5. OIDC 設定存放在 Secrets Manager 中。

範例入口策略

入口策略會決定解決方案的服務計數器何時應向前移動，以容納目標站點中的更多使用者。如需等待房間入口策略的概念性資訊，請參閱設計考量。

解決方案提供兩種範例入口策略：MaxSize 和 Periodic。



AWS Inlet 策略元件上的虛擬等待室

最大大小入口策略選項：

1. 用戶端發出 Amazon SNS 通知，該通知會叫用 MaxSizeInlet Lambda 函數，根據訊息承載增加服務計數器。
2. MaxSizeInlet Lambda 函數預期會收到一則訊息，其會使用此訊息來決定增加服務計數器的數量。

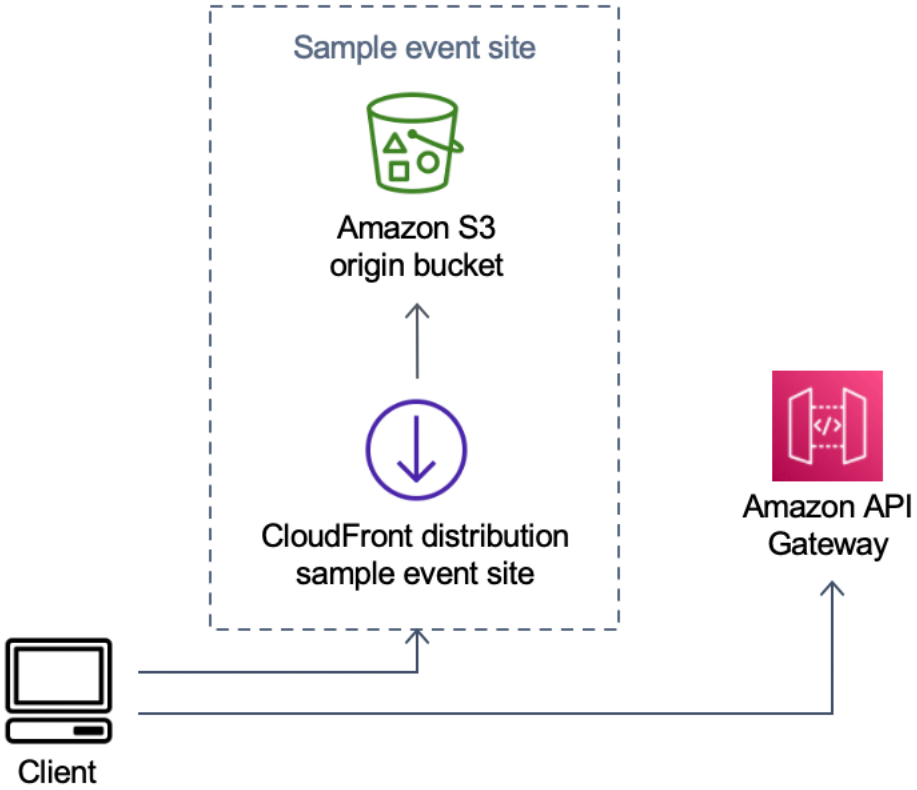
定期入口策略選項：

3. CloudWatch 規則每分鐘會叫用 Lambda 函數，將服務計數器增加固定數量。
4. 如果時間介於提供的開始和結束時間之間，PeriodicInletLambda 函數會將服務計數器增加給定的大小。或者，它會檢查 CloudWatch 警示，如果警示處於 OK 狀態，則執行增量，否則會略過該警示。

等待室範例

除了自訂授權方之外，範例等待室還與公有和私有 APIs 整合，以示範最小end-to-end等待室解決方案。主要網頁存放在 S3 儲存貯體中，並做為 CloudFront 的原始伺服器。它會引導使用者完成下列步驟：

1. 在等待室排隊進入網站。
2. 取得用戶端排成一行的位置。
3. 取得等待室的提供服務位置。
4. 服務位置等於或大於用戶端位置時，取得權杖集。
5. 使用權杖呼叫受 Lambda 授權方保護的 API。



AWS 範例事件網站元件上的虛擬等待室

1. S3 儲存貯體託管等待室和控制面板的範例內容。
2. CloudFront 分佈會將 S3 儲存貯體內容提供給使用者。
3. 範例 API Gateway 部署，搭配類似購物的資源路徑，例如 `/search`和 `/checkout`。此 API 由堆疊安裝，並使用權杖授權方設定。它旨在作為使用等待室保護 API 的簡單方法範例。呈現有效字符的請求會轉送至 Lambda，否則會傳回錯誤。除了連接的 Lambda 函數回應之外，API 沒有其他功能。

安全

當您在 AWS 基礎設施上建置系統時，安全責任會由您和 共同承擔 AWS。此共用模型可減少您的操作負擔，因為 會 AWS 操作、管理和控制元件，包括主機作業系統、虛擬化層，以及服務操作所在設施的實體安全性。如需 AWS 安全性的詳細資訊，請造訪 AWS Cloud Security。

Elasticache (Redis OSS) 會在私有 VPC 內指派網路介面。與 Elasticache (Redis OSS) 互動的 Lambda 函數也會在 VPC 中指派網路介面。所有其他資源在共用網路空間中具有 AWS 網路連線能力。具有與其他 AWS 服務互動之 VPC 介面的 Lambda 函數會使用 VPC 端點來連線至這些服務。

用於建立和驗證 JSON Web 權杖的公有和私有金鑰會在部署時間產生，並存放在 Secrets Manager 中。用於連線至 Elasticache (Redis OSS) 的密碼也會在部署時間產生並存放在 Secrets Manager 中。私有金鑰和 Elasticache (Redis OSS) 密碼無法透過任何解決方案 API 存取。

公有 API 必須透過 CloudFront 存取。解決方案會產生 API Gateway 的 API 金鑰，做為 CloudFront `x-api-key`中自訂標頭 的值。CloudFront 會在發出原始伺服器請求時包含此標頭。如需其他詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的將自訂標頭新增至原始伺服器請求。

私有 APIs 設定為需要 IAM AWS 授權才能叫用。解決方案會建立具有適當許可的 `ProtectedAPIGroup` IAM 使用者群組，以叫用私有 APIs。新增至此群組的 IAM 使用者有權叫用私有 APIs。

用於角色和許可的 IAM 政策，連接到解決方案建立的各種資源，僅授予執行必要任務所需的許可。

對於解決方案產生的 S3 儲存貯體、SQS 佇列和 SNS 主題等資源，會盡可能啟用靜態加密和傳輸期間加密。

監控

核心 API 堆疊包含數個 CloudWatch 警示，可在解決方案運作時監控這些警示以偵測問題。堆疊會建立 Lambda 函數錯誤和調節條件的警示，如果錯誤或調節條件在一分鐘期間內發生`ALARM`，則會將警示的狀態`OK`從 變更為 。

堆疊也會為每個 API Gateway 部署建立 4XX 和 5XX 狀態碼的警示。`OK` `ALARM` 如果在一分鐘內從 API 傳回 4XX 或 5XX 狀態碼，警示會從 變更為 狀態。

這些警示會在一分鐘沒有錯誤或調節後返回 `OK` 狀態。

IAM 角色

AWS Identity and Access Management (IAM) 角色可讓客戶將精細存取政策和許可指派給 AWS 雲端上的服務和使用者。此解決方案會建立 IAM 角色，授予解決方案的 AWS Lambda 函數建立區域資源的存取權。

Amazon CloudFront

`virtual-waiting-room-on-aws.template` CloudFormation 範本會建立等待室的核心公有和私有 APIs，也會部署公有 API 的 CloudFront 分佈。CloudFront 會快取來自公有 API 的回應，從而減少 API Gateway 和 Lambda 函數執行工作的負載。

此解決方案也有選用的範例等待室範本，可部署託管在 Amazon Simple Storage Service (Amazon S3) 儲存貯體中的簡單 Web 應用程式。為了協助減少延遲並改善安全性，Amazon CloudFront 分佈會部署原始存取身分，這是 CloudFront 使用者，提供對解決方案網站儲存貯體內容的公開存取。如需詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的使用原始存取身分限制對 Amazon S3 內容的存取。 Amazon CloudFront

安全群組

在此解決方案中建立的 VPC 安全群組旨在控制和隔離 Elasticache (Redis OSS) 的網路流量。需要與 Elasticache (Redis OSS) 通訊的 Lambda 會放置在與 Elasticache (Redis OSS) 相同的安全群組中。我們建議您檢閱安全群組，並在部署啟動並執行後視需要進一步限制存取。

設計考量

部署選項

如果這是第一次安裝，或者您不確定要安裝什麼，請部署`virtual-waiting-room-on-aws-getting-started.template`巢狀 CloudFormation 範本，這會安裝核心、授權方和範例等待室範本。這為您提供一個最小的等待室，具有簡單的流程。

支援的通訊協定

AWS 解決方案上的虛擬等待室可以與下列項目整合：

- JSON Web Token 驗證程式庫和工具
- 現有的 API Gateway 部署
- REST API 用戶端
- OpenID 用戶端和提供者

等待室入口策略

入口策略會封裝將用戶端從等待室移至網站所需的邏輯和資料。入口策略可以實作為 Lambda 函數、容器、Amazon EC2 執行個體或任何其他運算資源。只要它可以呼叫等待室公有和私有 APIs，就不需要是雲端資源。入口策略會接收等待室、網站或其他外部指標的事件，以協助其決定何時可以發行更多用戶端並進入網站。有幾種方法可以導入策略。您採用哪個資源取決於您可用的資源，以及受保護網站設計的限制。

入口策略採取的主要動作是使用相對值呼叫 `increment_serving_num` Amazon API Gateway 私有 API，指出有多少用戶端可以進入網站。本節說明兩個範例入口策略。這些可以依原狀使用、自訂，或者您可以採用完全不同的方法。

MaxSize

使用 MaxSize 策略，`MaxSizeInletLambda` 函數會設定為可同時使用網站的用戶端數量上限。這是固定值。用戶端發出 Amazon SNS 通知，該通知會叫用 `MaxSizeInlet` Lambda 函數，根據訊息承載增加服務計數器。SNS 訊息的來源可以來自任何地方，包括網站上的程式碼或觀察網站使用率層級的監控工具。

MaxSizeInlet Lambda 函數預期會收到訊息，其中包含：

- exited ：已完成的交易數量
- 要標記為完成的請求 IDs清單
- 要標示為已捨棄的請求 IDs 清單

此資料用於判斷服務計數器的增量。在某些情況下，根據目前的用戶端數量，計數器可能沒有額外的容量增加。

定期

使用週期性策略時，CloudWatch 規則每分鐘會叫用 PeriodicInlet Lambda 函數，將服務計數器增加固定數量。週期性入口會參數化為事件開始時間、結束時間和增量量。或者，此策略也會檢查 CloudWatch 警示，如果警示處於 OK 狀態，則會執行增量，否則會略過警示。網站整合商可以將使用率指標連接到警示，並使用該警示來暫停定期入口。此策略只會在目前時間介於開始和結束時間之間，以及選擇性地變更指定的警示處於 OK 狀態時，變更服務位置。

自訂和擴展解決方案

您組織的網站管理員必須決定與等候室搭配使用的整合方法。有兩個選項：

1. 直接使用 APIs和 API Gateway 授權方的基本整合。
2. 透過身分提供者進行 OpenID 整合。

除了上述整合之外，您可能需要設定網域名稱重新導向。您也必須負責部署自訂的等待室網站頁面。

Virtual Waiting Room on AWS 解決方案旨在透過兩種機制進行延伸：EventBridge 用於單向事件通知，而 REST APIs 用於雙向通訊。

配額

虛擬等待室的主要規模限制 AWS 是已安裝 AWS 區域的 Lambda 限流限制。將 安裝在具有預設 Lambda 並行執行配額 AWS 的帳戶中時，虛擬等待室 AWS 解決方案每秒最多可以處理 500 個用戶端，請求佇列中的位置。每秒 500 個用戶端的速率是根據解決方案，該解決方案具有所有 Lambda 函數並行配額限制，僅供使用。如果帳戶中的區域與其他叫用 Lambda 函數的解決方案共用，則虛擬等待室解決方案 AWS 應至少有 1，000 個可用的並行叫用。您可以使用 CloudWatch 指標來繪製您帳

戶中 Lambda 並行調用的圖表，以做出決定。您可以使用 Service Quotas 主控台來請求增加。提高 Lambda 限流限制只會在實際發生其他調用時，才會提高每月帳戶費用。

對於每秒每多 500 個用戶端，將限流限制增加 1，000。

預期每秒傳入使用者數	建議的並行執行配額
0-500	1，000（預設）
501-1，000	2,000
1，001-1，500	3,000

Lambda 的固定爆量限制為 3，000 個並行調用。如需詳細資訊，請參閱 Lambda 函數擴展。如果傳回錯誤碼表示暫時調節情況，用戶端程式碼應該預期並重試一些 API 呼叫。範例等待室用戶端包含此程式碼，做為如何設計用於高容量和高爆量事件之用戶端的範例。

此解決方案也與具有自訂組態步驟的 Lambda 預留和佈建並行相容。如需詳細資訊，請參閱管理 Lambda 預留並行。

可進入等候室、接收字符並繼續交易的使用者上限，受限於 Elasticache (Redis OSS) 計數器的上限。計數器用於等待室服務位置和追蹤解決方案的摘要狀態。Elasticache (Redis OSS) 中使用的計數器上限為 9，223，372，036，854，775，807。DynamoDB 資料表用於存放發給等待室使用者的每個字符的副本。DynamoDB 對資料表的大小沒有實際限制。

區域部署

所有 AWS 區域都支援此解決方案所使用的服務。如需 AWS 依區域提供服務的最新可用性，請參閱AWS 區域服務清單。

AWS CloudFormation 範本

為了自動化部署，此解決方案使用以下範本，您可以在部署之前下載這些 AWS CloudFormation 範本。

如果這是第一次安裝，或者您不確定要安裝什麼，請部署 `virtual-waiting-room-on-aws-getting-started.template` AWS CloudFormation 範本，這會安裝核心、授權方和範例等待室程式碼範本。這可讓您使用簡單的流程來測試工作等待室。

View template

virtual-waiting-room-on-aws-api-gateway-cw-logs-role.template：使用此範本在 CloudWatch 記錄許可的帳戶層級將預設角色 ARN 新增至 API Gateway。如需您的帳戶是否需要部署此範本的詳細資訊，請參閱先決條件。

View template

virtual-waiting-room-on-aws-getting-started.template：使用此巢狀範本來安裝核心、授權方和範例等待室堆疊。

View template

virtual-waiting-room-on-aws.template：使用此核心範本安裝核心公有和私有 REST APIs和雲端服務，以建立等待室事件。在您需要等候室 REST APIs、Elasticache (Redis OSS) 和 DynamoDB 資料表的帳戶和區域中安裝此範本。

View template

virtual-waiting-room-on-aws-authorizers.template：使用此範本安裝 Lambda 授權方，其設計用於驗證等待室發行的權杖，並用於保護最終使用者的 APIs。需要核心堆疊。需要來自核心堆疊的某些輸出做為參數，才能部署此堆疊。這是選用範本。

View template

virtual-waiting-room-on-aws-openid.template：使用此範本安裝 OpenID 身分提供者，以等待與授權介面的會議室整合。需要核心堆疊。部署此堆疊需要核心堆疊的一些輸出。這是選用範本。

View template

virtual-waiting-room-on-aws-sample-inlet-strategy.template：使用此範本安裝範例入口策略，用於目標網站和等待室之間。入口策略有助於封裝邏輯，以判斷何時允許更多使用者進入目標網站。需要核心堆疊。部署此堆疊需要核心堆疊的輸出。這是選用範本。

View template

virtual-waiting-room-on-aws-sample.template：使用此範本為等待室和目標網站安裝範例最小 Web 和 API Gateway 組態。需要核心和授權方堆疊。核心和授權方堆疊的輸出需要參數才能部署此堆疊。這是選用範本。

自動化部署

啟動解決方案之前，請檢閱本指南中討論的成本、架構、網路安全和其他考量事項。遵循本節中的step-by-step說明，設定解決方案並將其部署至您的帳戶。

部署時間：約 30 分鐘 （僅限入門堆疊）

先決條件

- AWS 帳戶主控台許可等同於管理員存取。
- 從 API Gateway 啟用 CloudWatch 記錄：
  - 登入 API Gateway 主控台，然後選取您計劃安裝堆疊的區域。

    如果您在此區域中定義了現有的 APIs：

    1. 選取任何 API。
    2. 從左側導覽中，選取設定。
    3. 檢查 CloudWatch 日誌角色 ARN 欄位中的值。
    - 如果沒有 ARN，請安裝 `virtual-waiting-room-on-aws-api-gateway-cw-logs-role.template`。
    - 如果有 ARN，請從啟動入門堆疊開始。

    如果此區域未定義現有的 APIs，請安裝 `virtual-waiting-room-on-aws-api-gateway-cw-logs-role.template`。
- 了解要保護之目標網站的架構和實作詳細資訊。

部署概觀

使用下列步驟來部署此解決方案 AWS。如需詳細說明，請點選各項步驟連結。

步驟 1. 啟動入門堆疊

- 在 AWS 您的帳戶中啟動 AWS CloudFormation 範本。
- 檢閱範本參數，並視需要輸入或調整預設值。

步驟 2. （選用）測試等候室

- 產生 AWS 金鑰以呼叫 IAM 安全 APIs。
- 開啟範例等待室的控制面板。
- 測試範例等待室。

步驟 1. 啟動入門堆疊

此自動化 AWS CloudFormation 範本會部署核心、授權方和範例等待室範本，可讓您檢視和測試工作等待室。您必須先閱讀並了解先決條件，才能啟動堆疊。

> **Note**
>
> 您需負責支付執行此解決方案時使用 AWS 的服務成本。如需詳細資訊，請參閱本指南中的成本區段，並參閱此解決方案中使用的每個 AWS 服務的定價網頁。

1. 登入 AWS Management Console，然後選取按鈕以啟動 `virtual-waiting-room-on-aws-getting-started.template` AWS CloudFormation 範本。

   或者，您可以下載範本做為自有實作的起點。
2. 根據預設，範本會在美國東部（維吉尼亞北部）區域啟動。若要在不同區域中啟動解決方案 AWS ，請使用主控台導覽列中的區域選擇器。
3. 在建立堆疊頁面上，確認正確的範本 URL 位於 Amazon S3 URL 文字方塊中，然後選擇下一步。
4. 在指定堆疊詳細資訊頁面上，為您的解決方案堆疊指派名稱。如需有關命名字元限制的資訊，請參閱AWS Identity and Access Management 《 使用者指南》中的 IAM 和 STS 限制。
5. 在參數下，檢閱此解決方案範本的參數，並視需要修改。此解決方案使用下列預設值。

參數	預設	描述
事件 ID	`Sample`	此等待室執行個體的唯一 ID，建議使用 GUID 格式。
有效期間	`3600`	字符有效期間，以秒為單位。

參數	預設	描述
啟用事件產生	`false`	如果設為 `true`，則每分鐘會將與等待室相關的指標寫入其事件匯流排
Elasticache (Redis OSS) 連接埠	`1785`	用於連線至 Elasticache (Redis OSS) 伺服器的連接埠號碼。建議不要使用 的預設 Elasticache (Redis OSS) 連接埠6379。
EnableQueuePositionExpiry	`true`	如果設定為 `false`，則不會套用佇列位置過期期間。
QueuePositionExpiryPeriod	`900`	這是佇列位置不符合產生字符資格的時間間隔，以秒為單位。
IncrSvcOnQueuePositionExpiry	`false`	如果設定為 `true`，則服務計數器會根據未成功產生字符的過期佇列位置自動進階。

6. 選擇 Next (下一步)。
7. 在 Configure stack options (設定堆疊選項) 頁面，選擇 Next (下一步)。
8. 在檢視 頁面上，檢視和確認的設定。勾選確認範本建立 AWS Identity and Access Management (IAM) 資源的方塊。
9. 選擇 Create stack (建立堆疊) 以部署堆疊。

   您可以在狀態欄的 AWS CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約 30 分鐘內收到 CREATE_COMPLETE 狀態。

步驟 2.（選用）測試等候室

如果您已部署入門堆疊，下列步驟可協助您測試等待室的功能。若要完成測試，您需要具有許可的 AWS 金鑰，才能呼叫核心堆疊中的 IAM APIs。

產生 AWS 金鑰以呼叫 IAM 安全 APIs

1. 在部署 `aws-virtual-waiting-room-getting-started.template` CloudFormation 範本的 AWS 帳戶中建立或使用 IAM 使用者。
2. 授予 IAM 使用者程式設計存取權。為 IAM 使用者建立新的一組存取金鑰時，請在出現時下載金鑰檔案。您需要 IAM 使用者的存取金鑰 ID 和私密存取金鑰，才能測試等候室。
3. 將 IAM 使用者新增至範本建立的 ProtectedAPIGroup IAM 使用者群組。

開啟範例等待室的控制面板

1. 登入 AWS CloudFormation 主控台，然後選取解決方案的入門堆疊。
2. 選擇 Output (輸出) 索引標籤。
3. 在金鑰欄下，找到 ControlPanelURL，然後選取對應的值。
4. 在新的索引標籤或瀏覽器視窗中開啟控制面板。
5. 在控制面板中，展開組態區段。
6. 輸入您在產生金鑰中擷取的存取金鑰 ID 和私密存取 AWS 金鑰，以呼叫 IAM 安全 APIs。端點和事件 ID 會從 URL 參數填入。
7. 選擇使用。在您提供登入資料後，按鈕會啟用。

測試範例等待室

1. 在 AWS CloudFormation 主控台中，選取解決方案的入門堆疊。
2. 選擇 Output (輸出) 索引標籤。
3. 在金鑰欄下，找到 WaitingRoomURL，然後選取對應的值。
4. 開啟等候室，然後選擇預留以進入等候室。
5. 導覽回具有控制面板的瀏覽器索引標籤。
6. 在增量服務計數器下，選擇變更。這可讓 100 個使用者從等待室移至目標站點。
7. 導覽回等候室，然後選擇立即查看！您現在將重新導向至目標網站。
8. 選擇立即購買，以在目標網站上完成交易。

部署個別堆疊

核心堆疊是取得等待室主要功能的唯一必要堆疊。所有其他堆疊都是選用的。如果您還沒有方法來驗證等待室發行的字符或保護您可能已經擁有的任何 APIs，請啟動授權方堆疊。如果您需要 OpenID 身分提供者來等待與授權介面的聊天室整合，請啟動 OpenID 堆疊。範例入口策略堆疊提供幾個範例，說明如何和何時允許更多使用者進入您嘗試保護的網站。

1. 啟動核心堆疊

部署時間：約 20 分鐘

此自動化 AWS CloudFormation 範本會在 AWS 雲端 AWS 的 上部署虛擬等待室。您必須先完成先決條件，才能啟動堆疊。

> **Note**
>
> 您需負責執行此解決方案時使用 AWS 的服務成本。如需詳細資訊，請參閱本指南中的成本區段，並參閱此解決方案中使用的每個 AWS 服務的定價網頁。

1. 登入 AWS Management Console，然後選取按鈕以啟動`aws-virtual-waiting-room-on-aws.template` AWS CloudFormation 範本。

   Launch solution

   或者，您可以下載範本做為自有實作的起點。
2. 根據預設，範本會在美國東部（維吉尼亞北部）區域啟動。若要在不同區域中啟動解決方案 AWS ，請使用主控台導覽列中的區域選擇器。
3. 在建立堆疊頁面上，確認 Amazon S3 URL 文字方塊中的範本 URL 是否正確，然後選擇下一步。
4. 在指定堆疊詳細資訊頁面上，為您的解決方案堆疊指派名稱。如需有關命名字元限制的資訊，請參閱AWS Identity and Access Management 《使用者指南》中的 IAM 和 STS 限制。
5. 在參數下，檢閱此解決方案範本的參數，並視需要修改。此解決方案使用下列預設值。

參數	預設	描述
事件 ID	`Sample`	此執行個體的唯一 ID，建議使用 GUID 格式。
有效期間	`3600`	字符有效期間，以秒為單位。
啟用事件產生	`false`	如果設定為 `true`，則每分鐘會將與等待室相關的指標寫入其事件匯流排。
Elasticache (Redis OSS) 連接埠	`1785`	用於連線至 Elasticache (Redis OSS) 伺服器的連接埠號碼。建議不要使用 的預設 Elasticache (Redis OSS) 連接埠6379。
EnableQueuePositionExpiry	`true`	如果設為 `false`，則不會套用佇列位置過期期間。
QueuePositionExpiryPeriod	`900`	這是佇列位置不符合產生字符資格的時間間隔，以秒為單位。
IncrSvcOnQueuePositionExpiry	`false`	如果設定為 `true`，則服務計數器會根據未成功產生字符的過期佇列位置自動進階。

6. 選擇 Next (下一步)。
7. 在 Configure stack options (設定堆疊選項) 頁面，選擇 Next (下一步)。
8. 在檢視 頁面上，檢視和確認的設定。勾選確認範本建立 AWS Identity and Access Management (IAM) 資源的方塊。
9. 選擇 Create stack (建立堆疊) 以部署堆疊。

   您可以在狀態欄的 AWS CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約 20 分鐘內收到 CREATE_COMPLETE 狀態。

2.（選用）啟動授權方堆疊

部署時間：大約 5 分鐘

1. 登入 AWS Management Console，然後選取按鈕以啟動 `aws-virtual-waiting-room-on-aws-authorizers.template` AWS CloudFormation 範本。

   Launch solution

   或者，您可以下載範本做為自有實作的起點。
2. 根據預設，範本會在美國東部（維吉尼亞北部）區域啟動。若要在不同區域中啟動解決方案 AWS ，請使用主控台導覽列中的區域選擇器。
3. 在建立堆疊頁面上，確認正確的範本 URL 位於 Amazon S3 URL 文字方塊中，然後選擇下一步。
4. 在指定堆疊詳細資訊頁面上，為您的解決方案堆疊指派名稱。如需有關命名字元限制的資訊，請參閱《 AWS Identity and Access Management 使用者指南》中的 IAM 和 STS 限制。
5. 在參數下，檢閱此解決方案範本的參數，並視需要修改。此解決方案使用下列預設值。

參數	預設	描述
公有 API 端點	`####`	虛擬等待室 APIs公有端點。
等候室事件 ID	`Sample`	等待室的事件 ID。
發行者 URI	`####`	公有金鑰和字符的發行者 URI。

6. 選擇 Next (下一步)。
7. 在 Configure stack options (設定堆疊選項) 頁面，選擇 Next (下一步)。
8. 在檢視 頁面上，檢視和確認的設定。勾選確認範本建立 AWS Identity and Access Management (IAM) 資源的方塊。
9. 選擇 Create stack (建立堆疊) 以部署堆疊。

   您可以在狀態欄的 AWS CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約五分鐘內收到 CREATE_COMPLETE 狀態。

3.（選用）啟動 OpenID 堆疊

部署時間：大約 5 分鐘

1. 登入 AWS Management Console，然後選取按鈕以啟動 `aws-virtual-waiting-room-on-aws-openid.template` AWS CloudFormation 範本。

   或者，您可以下載範本做為自有實作的起點。

2. 根據預設，範本會在美國東部（維吉尼亞北部）區域啟動。若要在不同區域中啟動解決方案 AWS ，請使用主控台導覽列中的區域選擇器。
3. 在建立堆疊頁面上，確認正確的範本 URL 位於 Amazon S3 URL 文字方塊中，然後選擇下一步。
4. 在指定堆疊詳細資訊頁面上，為您的解決方案堆疊指派名稱。如需有關命名字元限制的資訊，請參閱《 AWS Identity and Access Management 使用者指南》中的 IAM 和 STS 限制。
5. 在參數下，檢閱此解決方案範本的參數，並視需要修改。此解決方案使用下列預設值。

參數	預設	描述
公有 API 端點	`####`	虛擬等待室 APIs公有端點 URL。
私有 API 端點	`####`	虛擬等待室 APIs的私有端點 URL。
API 區域	`####`	AWS 公有和私有等待室 APIs 的區域名稱。
事件 ID	`Sample`	等待室的事件 ID。

6. 選擇 Next (下一步)。
7. 在 Configure stack options (設定堆疊選項) 頁面，選擇 Next (下一步)。
8. 在檢視 頁面上，檢視和確認的設定。勾選確認範本建立 AWS Identity and Access Management (IAM) 資源的方塊。
9. 選擇 Create stack (建立堆疊) 以部署堆疊。

您可以在狀態欄的 AWS CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約五分鐘內收到 CREATE_COMPLETE 狀態。

4.（選用）啟動範例入口策略堆疊

部署時間：大約兩分鐘

1. 登入 AWS Management Console，然後選取按鈕以啟動`aws-virtual-waiting-room-sample-inlet-strategy.template` AWS CloudFormation 範本。

   Launch solution

   或者，您可以下載範本做為自有實作的起點。
2. 根據預設，範本會在美國東部（維吉尼亞北部）區域啟動。若要在不同區域中啟動解決方案 AWS ，請使用主控台導覽列中的區域選擇器。
3. 在建立堆疊頁面上，確認 Amazon S3 URL 文字方塊中的範本 URL 是否正確，然後選擇下一步。
4. 在指定堆疊詳細資訊頁面上，為您的解決方案堆疊指派名稱。如需有關命名字元限制的資訊，請參閱《 AWS Identity and Access Management 使用者指南》中的 IAM 和 STS 限制。
5. 在參數下，檢閱此解決方案範本的參數，並視需要修改它們。此解決方案使用下列預設值。

參數	預設	描述
事件 ID	`Sample`	等待室的事件 ID。
私有核心 API 端點	`####`	虛擬等待室 APIs的私有端點 URL。
核心 API 區域	`####`	AWS 安裝核心 API 的區域。
入口策略	`Periodic`	要部署的入口策略。 每分鐘`Periodic`遞增服務數量。會根據下游目標網站在特定時間可處理的最大交易數量`MaxSize`遞增服務數量。

參數	預設	描述
增量依據	####	每分鐘應增加多少服務計數器。如果選取定期輸入策略，則為必要。
開始時間	####	開始遞增服務號碼的時間戳記 (epoch 時間，以秒為單位）。如果選取定期輸入策略，則為必要。
End Time (結束時間)	####	停止遞增服務號碼的時間戳記 (epoch 時間，以秒為單位）。如果保留 0，則服務數量會無限期增加。如果選取定期輸入策略，則為必要。
CloudWatch 警示名稱	####	要與定期輸入策略相關聯的選用 CloudWatch 警示名稱。如果提供 且處於警示狀態，則服務號碼不會遞增。僅適用於週期性入口策略。
大小上限	####	下游目標網站一次可處理的最大交易數 (MaxSize 策略）。

6. 選擇 Next (下一步)。
7. 在 Configure stack options (設定堆疊選項) 頁面，選擇 Next (下一步)。
8. 在檢視 頁面上，檢視和確認的設定。勾選確認範本建立 AWS Identity and Access Management (IAM) 資源的方塊。
9. 選擇 Create stack (建立堆疊) 以部署堆疊。

   您可以在狀態欄的 AWS CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約兩分鐘內收到 CREATE_COMPLETE 狀態。

5.（選用）啟動範例等待室堆疊

部署時間：大約 5 分鐘

1. 登入 AWS Management Console，然後選取按鈕以啟動`aws-virtual-waiting-room-sample.template` AWS CloudFormation 範本。

   Launch solution

   或者，您可以下載範本做為自有實作的起點。
2. 根據預設，範本會在美國東部（維吉尼亞北部）區域啟動。若要在不同區域中啟動解決方案 AWS ，請使用主控台導覽列中的區域選擇器。
3. 在建立堆疊頁面上，確認正確的範本 URL 位於 Amazon S3 URL 文字方塊中，然後選擇下一步。
4. 在指定堆疊詳細資訊頁面上，為您的解決方案堆疊指派名稱。如需有關命名字元限制的資訊，請參閱AWS Identity and Access Management 《使用者指南》中的 IAM 和 STS 限制。
5. 在參數下，檢閱此解決方案範本的參數，並視需要修改。此解決方案使用下列預設值。

參數	預設	描述
API Gateway 區域	`####`	AWS API Gateway 的區域名稱。
授權方 ARN	`####`	API Gateway Lambda 授權方的 ARN。
事件 ID	`Sample`	等待室的事件 ID。
私有 API 端點	`####`	虛擬等待室 APIs的私有端點 URL。
公有 API 端點	`####`	虛擬等待室 APIs公有端點 URL。

6. 選擇 Next (下一步)。
7. 在 Configure stack options (設定堆疊選項) 頁面，選擇 Next (下一步)。
8. 在檢視 頁面上，檢視和確認的設定。勾選確認範本建立 AWS Identity and Access Management (IAM) 資源的方塊。

9. 選擇 Create stack (建立堆疊) 以部署堆疊。

   您可以在狀態欄的 AWS CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約五分鐘內收到 CREATE_COMPLETE 狀態。

從舊版更新堆疊

建議您刪除堆疊，並為新版本建立新的堆疊。目前不支援使用 CloudFormation 堆疊更新遷移至較新版本。請參閱 ，解除安裝解決方案然後啟動入門堆疊。 ???

> **Note**
>
> 當您未主動使用解決方案來支援進行中的事件時，建議您遷移至較新的版本。

效能資料

上的虛擬等待室 AWS 已使用名為 Locust 的工具進行負載測試。模擬事件大小的範圍從 10，000 到 100，000 個用戶端。負載測試環境包含下列組態：

- Locust 2.x 搭配 AWS 雲端部署的自訂功能
- 四個 AWS 區域 (us-west-1、us-west-2、us-east-1、us-east-2)
- 每個區域 10 個 c5.4xlarge Amazon EC2 主機 （總計 40 個）
- 每個主機 32 個 Locust 程序
- 模擬使用者平均分散在 1，280 個程序中

每個使用者程序的end-to-end測試步驟：

1. 呼叫 assign_queue_num並接收請求 ID。
2. queue_num 使用請求 ID 進行迴圈，直到傳回使用者的佇列位置 （短時間）。
3. 循環serving_num直到傳回的值 >= 使用者的佇列位置 （長時間）。
4. 不常呼叫 waiting_room_size來擷取等待中的使用者數量。
5. 呼叫 generate_token並接收 JWT 以在目標網站中使用。

問題清單

可透過等候室處理的用戶端數量沒有實際上限。

使用者進入等待室的速率會影響部署所在區域的 Lambda 函數並行執行配額。

負載測試無法超過每秒 10，000 個請求的預設 API Gateway 請求限制，且快取政策會與 CloudFront 搭配使用。

get_queue_num Lambda 函數的調用率接近 1：1，接近對等待室的傳入使用者率。由於並行限制或爆量限制，此 Lambda 函數可能會在高速率的傳入使用者期間受到調節。大量 get_queue_num Lambda 函數調用所造成的調節，可能會影響其他 Lambda 函數，進而產生副作用。如果用戶端軟體可以使用重試/退避邏輯適當回應這種暫時擴展錯誤，整體系統會繼續運作。

預設配額組態中核心堆疊設定的 CloudFront 分佈可以處理擁有 250，000 名使用者的等待室，每個使用者至少每秒輪詢一次 serving_num API。

疑難排解

本節提供此解決方案的疑難排解資訊。

如果本節未解決您的問題，請聯絡 AWS Support 提供為此解決方案開啟 AWS Support 案例的說明。

來自 APIs 4xx 回應狀態

- 這可能是由於不正確的事件 ID 或請求 ID 或兩者所致。這發生在相關 Lambda 函數的 CloudWatch Logs 中。
- 私有 APIs 經過 IAM 驗證，用戶端需要有權叫用私有 APIs AWS 金鑰。這發生在 API Gateway 的 CloudWatch Logs 中。

來自 APIs 5xx 回應狀態

- 來自限流 Lambda 或 API Gateway 的回應，請檢查 *<LambdaFunctionName>*ThrottlesAlarm CloudWatch 警示。
- 後端設定錯誤，請檢查 *<LambdaFunctionName>*ErrorsAlarm CloudWatch 警示和 CloudWatch Logs 以取得詳細資訊。

5XXErrorPublic/PrivateApiAlarm

- 此警示狀態是 API 在 60 秒內將 5XX 狀態傳回給發起人ALARM時。
- 當 60 秒內沒有傳回 5xx 狀態OK時，此警示會傳回 。
- 此警示可由 Lambda 函數或 Lambda 執行時間啟動，將錯誤傳回 API Gateway。

4XXErrorPublic/PrivateApiAlarm

- 此警示狀態是 API 在 60 秒內將 4XX 狀態傳回給發起人ALARM時。
- 此警示會在 60 秒內傳回 至 4XX 狀態OK時傳回 。
- 此警示可由不正確的 API URL 啟動。

*<LambdaFunctionName>*ThrottlesAlarm

- 當具名 Lambda 在 60 秒期間內遇到並行執行限制時，此警示狀態為 ALARM。

- OK 如果 60 秒內沒有遇到任何調節，此警示會傳回 。
- 您可能需要提高帳戶區域的並行限制。
- 您可能會遇到 Lambda 的爆量限制，這需要在用戶端上重試邏輯。

*<LambdaFunctionName>*ErrorsAlarm

- 當名為 的 Lambda 在 60 秒期間內遇到執行時間執行錯誤ALARM時，此警示狀態即為 。
- OK 如果 60 秒內沒有發生錯誤，此警示會傳回 。
- 這可能是因為後端組態錯誤所造成。
- 這可能是因為 Lambda 程式碼中的錯誤所造成。

聯絡人 支援

如果您有 AWS 開發人員支援、AWS Business Support 或 AWS Enterprise Support，您可以使用 支援中心來取得此解決方案的專家協助。以下章節將提供說明。

建立案例

1. 登入支援中心。
2. 選擇建立案例。

如何提供協助？

1. 選擇技術。
2. 針對服務，選取解決方案。
3. 針對類別，選取其他解決方案。
4. 針對嚴重性，選取最符合您使用案例的選項。
5. 當您輸入服務、類別和嚴重性時，界面會填入常見故障診斷問題的連結。如果您無法使用這些連結來解決問題，請選擇下一步：其他資訊。

其他資訊

1. 針對主旨，輸入摘要您的問題的文字。
2. 針對描述，詳細說明問題。

3. 選擇連接檔案。
4. 連接處理請求 支援 所需的資訊。

協助我們更快解決您的案例

1. 輸入請求的資訊。
2. 選擇下一步驟：立即解決或聯絡我們。

立即解決或聯絡我們

1. 檢閱立即解決解決方案。
2. 如果您無法解決這些解決方案的問題，請選擇聯絡我們，輸入請求的資訊，然後選擇提交。

其他資源

AWS 服務	
• AWS CloudFormation	• Amazon DynamoDB
• Amazon Simple Storage Service	• Amazon API Gateway
• AWS Lambda	• AWS Secrets Manager
• Amazon CloudFront	• Amazon Simple Queue Service
• Amazon EventBridge	• Amazon CloudWatch
• Elasticache (Redis OSS)	• Amazon Comprehend
• Amazon Virtual Private Cloud	• AWS Identity and Access Management

解除安裝解決方案

您可以從 AWS Management Console 或使用 解除安裝 AWS 解決方案上的虛擬等待室 AWS Command Line Interface。您必須手動刪除由此解決方案建立的各種資源用來存放日誌的 S3 儲存貯體。 AWS 解決方案實作不會自動刪除這些 S3 儲存貯體，因此在解決方案刪除之後，您仍然可以檢閱日誌事件。

如果您已手動將 IAM 使用者新增至解決方案建立的 `ProtectedAPIGroup` IAM 使用者群組，請先從 IAM 使用者群組移除 IAM 使用者，再解除安裝解決方案。否則，IAM 使用者群組和相關聯的 IAM 政策無法刪除。

對於每個部署的堆疊，請遵循下列指示。

使用 AWS Management Console

1. 登入 AWS CloudFormation 主控台。
2. 在堆疊頁面上，選取此解決方案的安裝堆疊。
3. 選擇 刪除 。

使用 AWS Command Line Interface

判斷 AWS Command Line Interface (AWS CLI) 是否在您的環境中可用。如需安裝說明，請參閱AWS CLI 《 使用者指南》中的什麼是 AWS Command Line Interface？。確認 AWS CLI 可供使用之後，請執行下列命令。

```
$ aws cloudformation delete-stack --stack-name <installation-stack-name>
```

刪除 Amazon S3 儲存貯體

如果您決定刪除 AWS CloudFormation 堆疊以防止意外資料遺失，此解決方案會設定為保留解決方案建立的 Amazon S3 儲存貯體 （用於在選擇加入區域中部署）。解除安裝解決方案之後，如果您不需要保留資料，可以手動刪除此 S3 儲存貯體。請依照下列步驟刪除 Amazon S3 儲存貯體。

1. 登入 Amazon S3 主控台。
2. 從左側導覽窗格選擇儲存貯體。

3. 找到 *<stack-name>*S3 儲存貯體。
4. 選取 S3 儲存貯體，然後選擇刪除。

若要使用 刪除 S3 儲存貯體 AWS CLI，請執行下列命令：

```
$ aws s3 rb s3://<bucket-name> --force
```

來源碼

請造訪我們的 GitHub 儲存庫，下載此解決方案的來源檔案，並與他人共用您的自訂項目。

貢獻者

- Jim Thario
- Thyag Ramachandran
- 約安摩根
- 賈斯汀水泥
- 阿蘭莫海默尼
- Garvit Singh
- Bassem Wanis

修訂

檢查 GitHub 儲存庫中的 CHANGELOG.md 檔案，以查看軟體的所有顯著變更和更新。變更日誌提供每個版本的改善和修正的清楚記錄。

注意

客戶有責任對本文件中的資訊進行自己的獨立評定。本文件： (a) 僅供參考， (b) 代表 AWS 目前的產品產品和實務， 可能隨時變更，恕不另行通知。 和 (c) 不會從 AWS 及其附屬公司建立任何承諾或保證， 供應商或 licensors. AWS products 或服務「原樣」提供，不做任何保證， 表示法、 或任何類型的條件， 無論明示或暗示。 AWS 對客戶的責任和責任受 AWS 協議、 本文件不屬於 也不會修改 AWS 與其客戶之間的任何協議。

上的虛擬等待室 AWS 是根據 Apache 授權 2.0 版所授權。

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。