實作指南

上的虛擬等待室 AWS

上的虛擬等待室 AWS: 實作指南

Table of Contents

在 上的虛擬等待室中吸收大量流量至您的網站 AWS

發佈日期：2021 年 11 月（上次更新：2024 年 9 月）

Virtual Waiting Room on AWS 解決方案有助於控制大量流量時傳入網站的使用者請求。它建立了雲端基礎設施，旨在暫時卸載傳入的流量至您的網站，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
- 火警銷售或其他大型零售銷售，例如 Black Friday
- 推出新產品並發佈廣泛的行銷公告
- 線上測試和課程的測驗存取和課程出席
- 醫療約診時段的發行
- 啟動需要建立帳戶和付款的新 direct-to-customer 服務

此解決方案可做為網站訪客的保留區域，並允許流量在容量足夠時通過。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 權杖（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 個磁碟區，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其位置。

此解決方案提供下列主要功能：

- 網站中使用者的結構式佇列
- 控制非常大型事件大小的流量的可擴展性
- JSON 產生 Web 權杖以允許進入目標網站
- 所有功能都透過 控制 REST APIs
- 用戶端解決方案的 Turnkey API Gateway 授權方
- 獨立整合或與 OpenID 搭配使用

本實作指南說明在 Amazon Web Services （AWS） Cloud AWS 中在 上部署虛擬等待室的架構考量和組態步驟。其中包含範本的連結，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。

本指南適用於在 AWS Cloud 中具有實際架構經驗的 IT 架構師、開發人員、 DevOps 工作人員、資料分析師和行銷技術專業人員。

費用

您必須負責執行此解決方案時所使用之 AWS 服務的成本。在此修訂版本中，以美國東部 (維吉尼亞北部) 區域的預設設定執行此解決方案的成本約為每個堆疊 10.00 USD，再加上相對於事件大小的 API 要求和資料流量的費用。

維護解決方案的每日成本，沒有任何事件

AWS 服務	請求/時間	費用 [美元]
Amazon API Gateway	0	$0.00
Amazon CloudFront	0	$0.00
Amazon CloudWatch	0	$0.00
Amazon DynamoDB	0	$0.00
Amazon ElastiCache	計算節點小時數 (Redis)	約 6 美元
AWS Lambda	免費方案 *	$0.00
AWS Secrets Manager	免費方案 *	$0.00
Amazon Simple Storage Service (Amazon S3)	免費方案 *	$0.00
Amazon Virtual Private Cloud (Amazon VPC)	VPC 端點小時 NAT 閘道時數	約 5 美元
總計:		約 11.00 美元

* 費用估算基於乾淨的環境。如果您在此解決方案以外使用此 AWS 服務，則可能會超過免費方案配額。

下表顯示 50,000 位使用者和 10 萬使用者等候室的估計成本，事件持續時間範圍為 2-4 小時，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之每項 AWS 服務的定價網頁。

50,000 名等候室用戶在 2 小時活動期間的估計費用

AWS 服務	Dimensions (尺寸)	費用 [美元]
Amazon API Gateway	請求	2.00 美元
CloudFront	請求，帶寬	$75.00
CloudWatch	指標、警報、儲存	$1.00
Amazon CloudWatch 活動	事件	$1.00
DynamoDB	讀/寫單元、儲存	$1.00
ElastiCache	節點小時數	8.00 美元
Lambda	請求, 計算時間	$1.00
AWS Secrets Manager	秘密，請求	$1.00
Amazon S3	請求，存儲	$1.00
Amazon VPC	資料傳輸、端點時間	2.00 美元
總計		$94.00

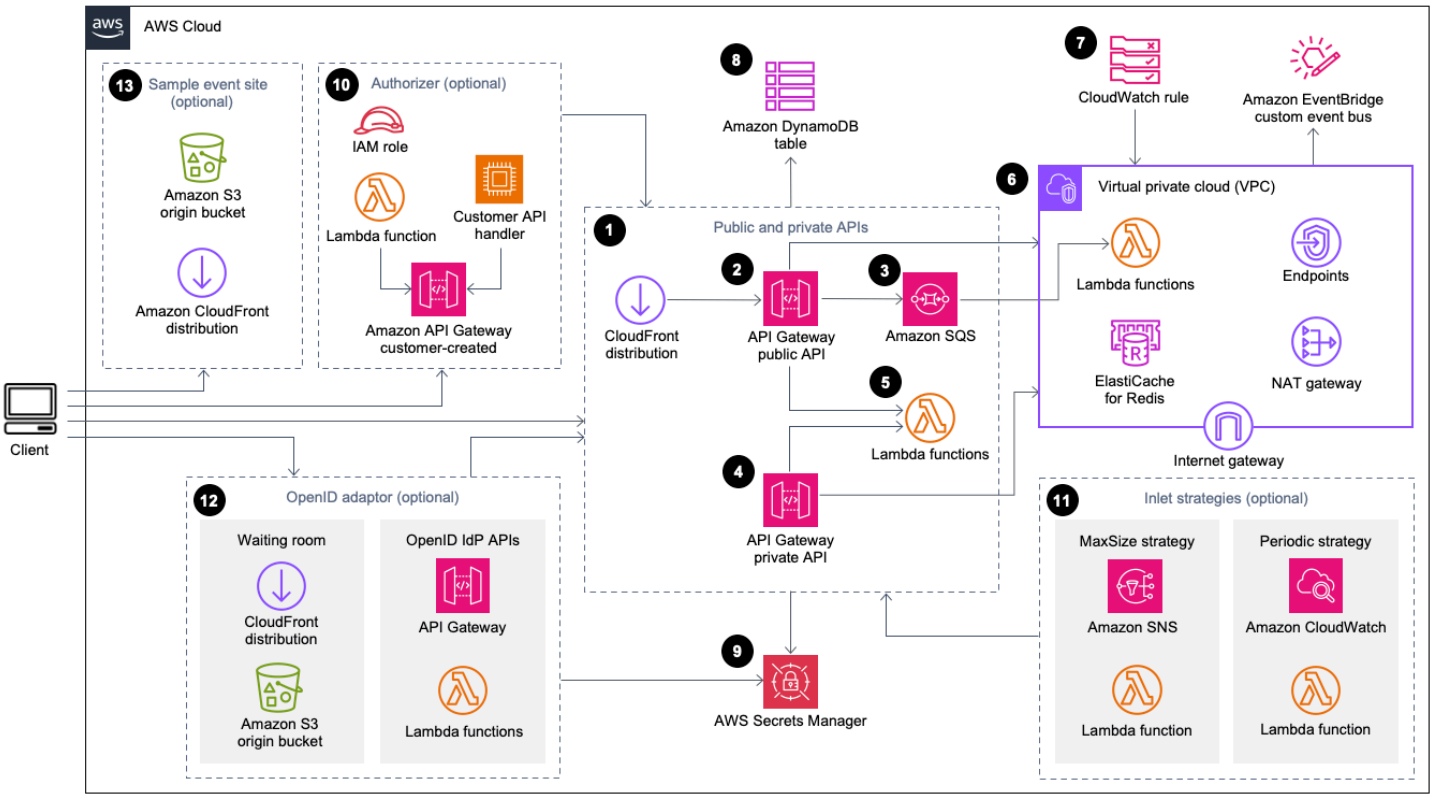
10 萬名等候室用戶在 2 小時活動期間的估計費用

AWS 服務	Dimensions (尺寸)	費用 [美元]
Amazon API Gateway	請求	4.00 美元
CloudFront	請求，帶寬	296.00 美元
CloudWatch	指標、警報、儲存	$1.00
CloudWatch 活動	事件	$1.00
DynamoDB	讀/寫單元、儲存	4.00 美元

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

架構概觀

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



虛擬等候 AWS 室

AWS CloudFormation 範本會部署下列基礎結構：

1. 用於為客戶提供公共API呼叫的 Amazon CloudFront 分發。
2. Amazon API Gateway 公有API資源可處理虛擬等候室的佇列請求、追蹤佇列位置，並支援驗證允許存取目標網站的權杖。
3. Amazon 簡單佇列服務 (AmazonSQS) 佇列，用於管理處理佇列訊息之AWS Lambda函數的流量。SQS佇列不會為每個要求叫用 Lambda 函數，而是批次處理傳入的請求突發。
4. API閘道私有API資源，以支援管理功能。
5. Lambda 函數可驗證和處理公開和私有API請求，並傳回適當的回應。
6. Amazon Virtual Private Cloud (VPC) 可託管 Lambda 函數，這些函數可直接與彈性護理 (RedisOSS) 叢集互動。VPC端點可讓中的 Lambda 函數與VPC解決方案內的服務進行通訊。此外，NAT閘道允許中的 Lambda 函數連VPC接 CloudFront 端點，並視需要使快取失效。

7. 用於叫用 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. 用於存放令牌、佇列位置和服務計數器資料的 Amazon DynamoDB 表格。
9. AWS Secrets Manager 存儲令牌操作和其他敏感數據的密鑰。
10. (選用) 授權者元件，由 AWS Identity and Access Management(IAM) 角色和 Lambda 授權者函數組成，可與閘道搭配API使用。
11. (選用) Amazon 簡易通知服務 (AmazonSNS) 和 Lambda 函數 CloudWatch，可支援兩種輸入策略。
12. (可選) 具有API閘道和 Lambda 函數的 OpenID 適配器組件，可讓 OpenID 提供程序對您網站的用戶進行身份驗證。 CloudFront 使用此元件的等候室頁面的 Amazon 簡易儲存服務 (Amazon S3) 儲存貯體散發。
13. (選擇性) 在等候室 Web 應用程式範例使用 Amazon S3 原始儲存貯體 CloudFront 散發。

解決方案的運作方式

本節說明高階「 AWS 虛擬等候室」工作流程中的步驟。有關 GitHub為您的網站構建，自定義和集成等候室的詳細信息，請參閱《開發人員指南》。

等候室的公眾API可以位於您站點周邊安全的後面，也可以在未經授權的情況下使用。根據您用於將等候室與網站整合的方法而定，使用者可能需要先對網站進行驗證，才能導覽至等候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要求。事件 ID 是針對公用和私人請求的大多數要求所需的唯一 ID APIs。事件 ID 是在安裝核心API堆疊期間設定的。在作業期間，事件 ID 可以透過等候室頁面以URL參數或 Cookie 的形式提供；它可以做為驗證 Token 宣告的一部分提供，也可以透過不同的資料路徑將事件 ID 散發給用戶端。

有些情況下，客戶端需要事件 ID 和請求 ID 來進行某些API調用。請求 ID 是從等候室發出的唯一 ID，代表排隊的特定用戶端。

下列步驟說明佇列項目、等待佇列進度，以及使用網站存取權杖離開等候室的API要求流程。

用戶進入等候室：

1. 使用者會看到代表等候室進入點的畫面或頁面。他們選擇進入隊列，客戶端軟件（瀏覽器，移動設備，設備）打電話API給`assign_queue_num`公眾請求隊列位置。
2. API閘道會立即將API請求傳送至 Amazon SQS 佇列。
3. 當請求被放置到隊列中的`assign_queue_num`API調用返回。客戶端收到一個唯一的請求 ID，以後可用於檢索隊列位置，請求的時間和訪問令牌。
4. L `AssignQueueNum` ambda 函數會從SQS佇列接收最多十個要求的批次。Lambda 服務風扇會呼叫以處理多個批次的請求。
5. `AssignQueueNumLambda` 函數會驗證其批次中的每個訊息，在 Elasticache (Redis) 中遞增佇列計數器，並將每個要求儲存在 Elasticache (RedisOSS) 中，並將其相關聯的佇列位置儲存在 Elasticache (RedisOSS) 中。
6. 成功處理每封郵件時都會刪除。涉及錯誤狀況的訊息會在稍後的批次中重新處理一次。第二次故障後，它們被發送到 dead-letter-queue 連接到CloudWatch警報。
7. 用戶端可以在收到來自`assign_queue_num`呼叫的要求 ID `queue_num` API 之後開始輪詢。客戶端將事件 ID 和請求 ID 發送到`queue_num`API並接收數字隊列位置或表示尚未處理請求的響應。在大型事件期間，用戶端可能需要多次撥打此呼叫。`GetQueueNumLambda` 函數是由API閘道器叫用，並從 DynamoDB 傳回用戶端在佇列中的數字位置。

用戶在等候室等待：

8. 用戶端在佇列中的位置之後，就可以定期開始輪詢。serving_num API會serving_numAPI以事件 ID 呼叫，並傳回佇列目前的服務位置。來自的響應serving_numAPI告訴客戶端何時他們可以從等待室移動到實際的目標站點，其中最終的事務可以發生。L GetServingNum ambda 函數返回等待室的當前服務位置。
9. 當服務位置等於或大於客戶端的隊列（請求）位置時，客戶端可以向公眾請求 JSON Web 令牌（JWT）API。該令牌可與目標站點一起使用以完成交易。會generate_tokenAPI以事件識別碼和要求識別碼呼叫。API閘道會叫用含有參數的 GenerateToken Lambda 函數。
10. L GenerateToken ambda 函數會驗證要求，並檢查先前是否已產生此權杖。Lambda 函數會查詢 DynamoDB 資料表是否有相符的權杖。如果找到，該令牌將返回給調用者，並且不會再生。此程序可防止使用單一要求 ID 來產生具有新到期時間的多個不同權杖。
11. 如果在 DynamoDB 中找不到權杖，Lambda 函數會擷取金鑰以建立權杖，並使用事件識別碼和用戶端的請求識別碼將權杖儲存在 DynamoDB 中。Lambda 函數會寫入事件， EventBridge 以表示已產生新的權杖。Lambda 函數會遞增一個 Elasticache (RedisOSS) 計數器，該計數器會追蹤為事件產生的記號數目。
12. 如果queue_pos_expiry開啟，用戶端可以呼叫叫用 GetQueuePositionExpiryTime Lambda 函數來查詢到期前queue_pos_expiryAPI的剩餘時間。

使用者離開等候室：

13. 當客戶端收到其令牌時，它會進入目標站點以開始其交易。視您的基礎結構支援與整合的方式而定 JWT，用戶端可能需要以要求標頭、Cookie 或其他方式呈現權杖。APIGateway 的授權者可用於驗證客戶端請求中包含的令牌。任何用於驗證和管理的商業或開源庫都JWTs可以與 AWS 令牌上的虛擬等候室一起使用。如果令牌有效，則允許客戶繼續其交易。
14. 用戶端完成交易後，會呼APIAPI叫 private 來更新用戶端權杖的狀態，並在 DynamoDB 中完成。

佇列位置到期時間：

15. 啟動此功能後，與特定佇列位置對應的「要求 ID」只能在指定的時間間隔內產生權杖。

增加隊列位置到期的服務計數器：

16. 啟動此功能時，服務計數器會根據無法產生權杖的過期佇列位置自動遞增。

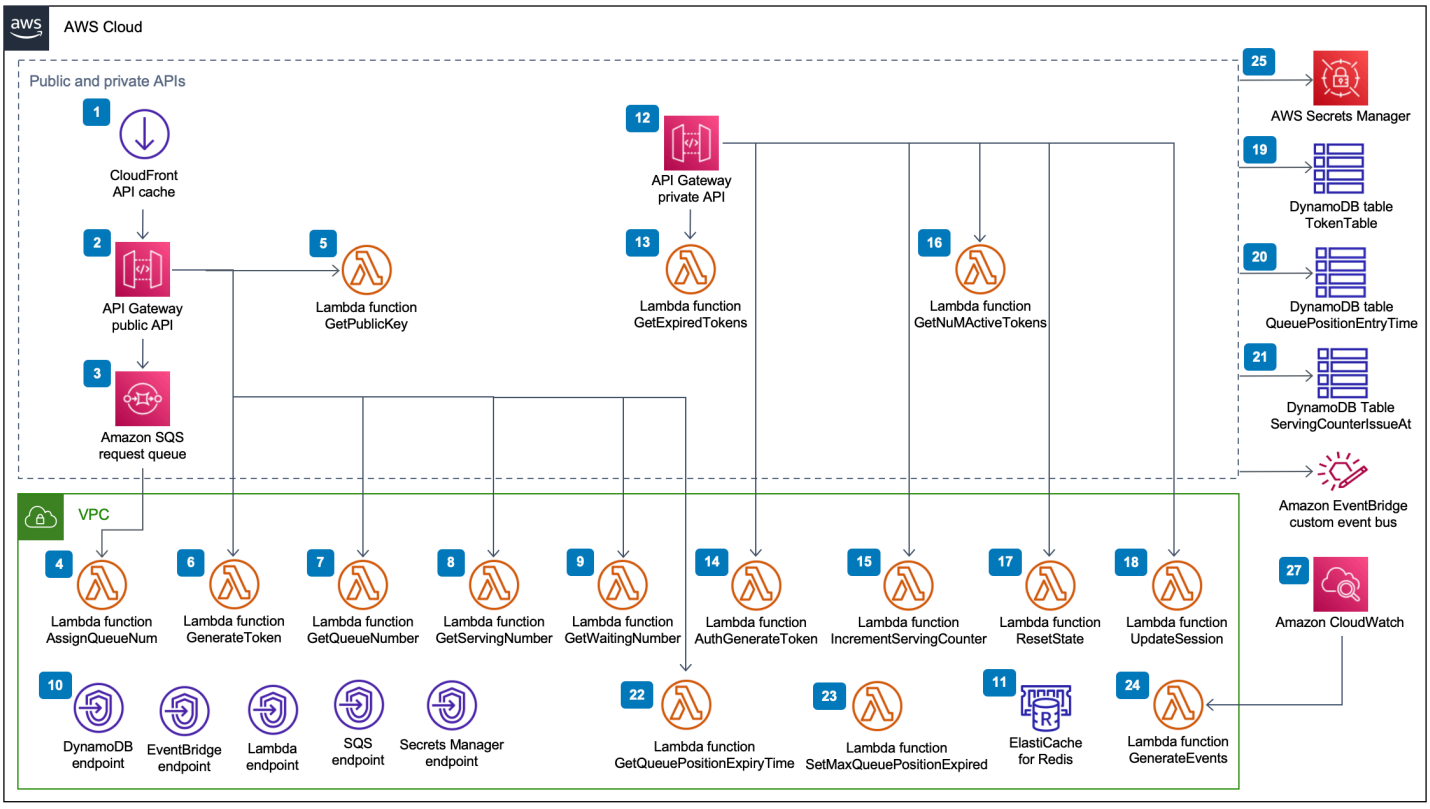
方案元件

公共和私人等候室 APIs

關於 AWS 解決方案的主要目的的虛擬等待室是以受控的方式控制客戶端的 JSON Web Token（JWT）的生成，以避免可能使目標網站不堪重負的新用戶爆發。JWTs可用於網站保護，在獲得等候室令牌之前防止訪問網頁，以及用於API訪問授權。

核心模板安裝API用於大多數虛擬等候室的公共API和私有（IAM-授權）的 AWS 操作。公API用會根據API路徑設定具有多個快取原則的 CloudFront散佈。隨即建立 DynamoDB 資料表和 EventBridge事件匯流排。該範本會新增一個VPC包含兩個可用區域 (AZs)、兩者中的彈性疼 (RedisOSS) 叢集AZs，以及多個 Lambda 函數的新功能。與 Elasticache (RedisOSS) 互動的 Lambda 函數在其中具有網路介面，VPC而所有其他 Lambda 函數均具有預設網路連線能力。核心APIs是與解決方案的交互的最低層。其他 Lambda 函數、Amazon 彈性運算雲端 (AmazonEC2) 執行個體和容器都可以充當擴充功能，並呼叫核心APIs以建立等候室、控制入口流量，以及對解決方案產生的事件做出反應。

此外，核心堆疊會針對其所有 Lambda 函數錯誤和節流狀況建立警示，以及針對 4XX 和 5XX 狀態碼的每個API閘道部署建立警示。



AWS公共和私有APIs組件上的虛擬等候室

1. CloudFront 分佈為客戶端提供公共API呼叫，並在適當的情況下緩存結果。
2. Amazon API Gateway 來自虛擬等候室的公有API程序佇列請求、追蹤佇列位置，並支援驗證允許存取目標網站的權杖。
3. SQSqueue 可調節處理佇列訊息之 AWS Lambda 函數的流量。
4. AssignQueueNumLambda 函數會驗證其批次接收的每則訊息、在 Elasticache (Redis) 中遞增佇列計數器，並將每個要求儲存在 Elasticache (RedisOSS) 中，並將每個要求及其相關聯的佇列位置儲存在 Elasticache (RedisOSS) 中。
5. L GetPublicKey ambda 函數會從 Secrets Manager 擷取公開金鑰值。
6. L GenerateToken ambda 函數會針JWT對已允許在目標網站完成交易的有效請求產生一個。它將事件寫入等候室的自定義事件總線，該事件已生成令牌。如果先前已為此請求生成令牌，則不會生成新令牌。
7. GetQueueNumberLambda 函數檢索並返回從彈性（Redis OSS 的）隊列中的客戶端的數字位置。
8. 該 GetServingNumber Lambda 函數檢索並返回當前由等待室從彈性（RedisOSS）提供服務的號碼。
9. L GetWaitingNum ambda 函數返回當前在等待室中排隊並尚未發出令牌的數字。
10. VPC端點可讓中的 Lambda 函數與VPC解決方案內的服務進行通訊。
11. Elasticache (RedisOSS) 叢集會儲存所有使用有效事件識別碼進入等候室的要求。它還存儲了幾個計數器，例如排入隊的請求數量，當前服務的數量，生成的令牌數量，完成的會話數以及放棄的會話數量。
12. API閘道私有API資源，以支援管理功能。私APIs有已 AWS IAM驗證。
13. L GetExpiredTokens ambda 函數返回帶IDs有過期令牌的請求列表。
14. L AuthGenerateToken ambda 函數會為已允許在目標網站完成交易的有效請求產生權杖。核心堆疊部署期間最初設定的權杖的發行者和有效期間可以覆寫。它將事件寫入等候室的自定義事件總線，該事件已生成令牌。如果先前已為此請求生成令牌，則不會生成新令牌。
15. IncrementServingCounterLambda 函數增加存儲在彈性（RedisOSS）中的等待室的服務計數器，給定的增量按值。
16. GetNumActiveTokensLambda 函數會查詢 DynamoDB 中尚未過期、尚未用來完成其交易且尚未標示為放棄的權杖數目。
17. ResetStateLambda 函數會重設儲存在彈性痛 (RedisOSS) 中的所有計數器。它也會刪除和重新建立TokenTableQueuePositionEntryTime、和 ServingCounterIssuedAt DynamoDB 表格。此外，它執行 CloudFront 緩存失效。

18UpdateSessionLambda 函數會更新儲存在 TokenTable DynamoDB 表中的工作階段 (權杖) 的狀態。會話狀態由一個整數表示。工作階段設定為的狀態1表示已完成，並-1表示已放棄。它會將事件寫入等候室的自訂事件匯流排，表示工作階段已更新。

19動TokenTable態資料表會儲存權杖資料。

20QueuePositionEntryTimeDynamoDB 表格會儲存佇列位置和輸入時間資料。

21ServingCounterIssuedAtDynamoDB 資料表會將更新儲存至服務計數器。

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

23L SetMaxQueuePositionExpired ambda 函數設置已過期對應於ServingCounterIssuedAt表值的最大隊列位置。如果true在核心堆疊部署期間將IncrSvcOnQueuePositionExpiry參數設定為，它會每分鐘執行一次。

24GenerateEventsLambda 函數會將各種等候室指標寫入等候室的自訂事件匯流排。如果true在核心堆疊部署期間將啟用事件產生參數設定為，它會每分鐘執行一次。

25AWS Secrets Manager 存儲令牌操作和其他敏感數據的密鑰。

26每次產生權杖並在 TokenTable DynamoDB 表中更新工作階段時，Amazon EventBridge 自訂事件匯流排都會收到事件。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，則會使用各種等候室指標寫入。

27如果在核心堆疊部署期間將啟用 CloudWatch 事件產生參數設定為 true，則會建立 Amazon 事件規則。此事件規則會每分鐘啟動 GenerateEvents Lambda 函數。

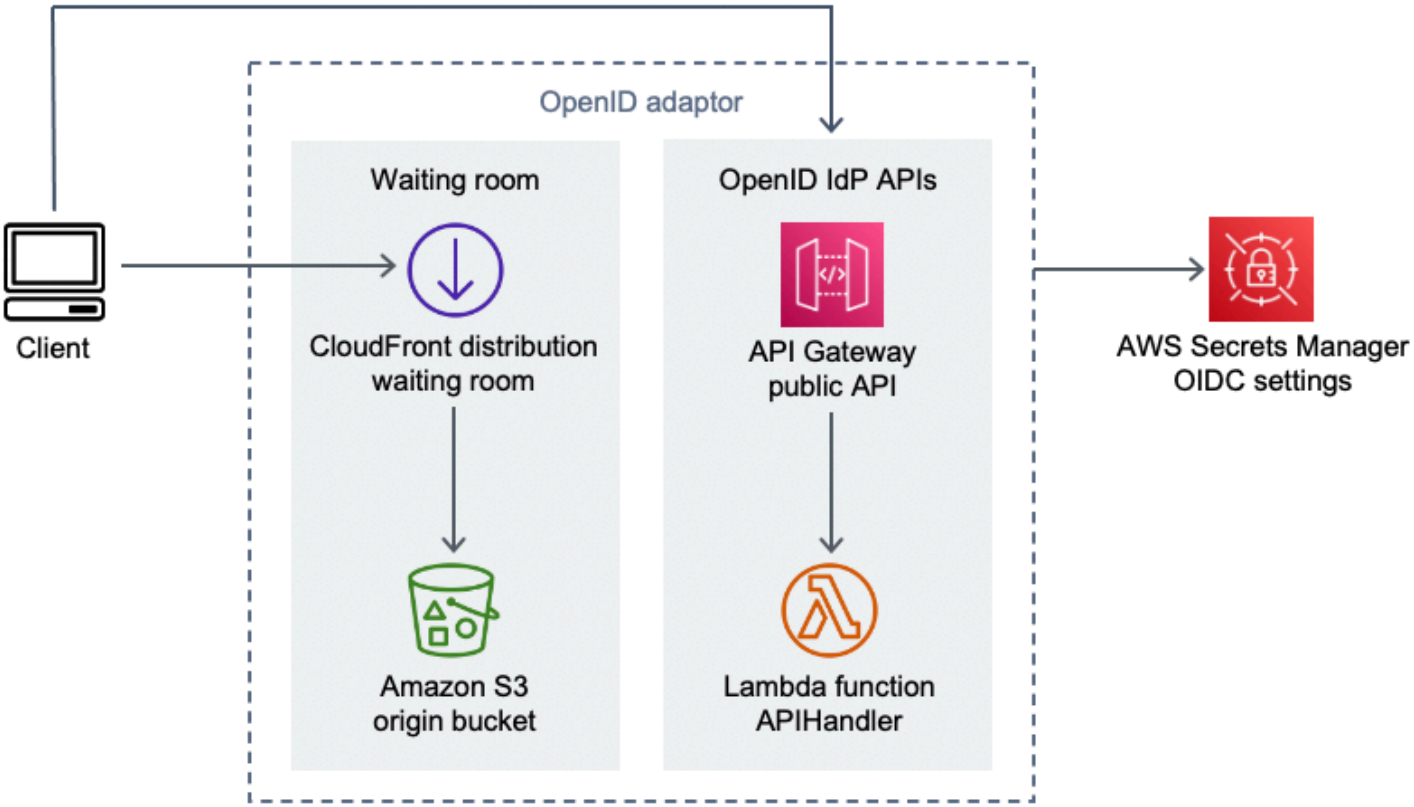
Authorizers

此解決方案包括API閘道 Lambda 授權者堆疊。該堆棧由一個IAM角色和一個 Lambda 函數組成。L APIGatewayAuthorizer ambda 函數是API閘道的授權者，可驗證虛擬等候室所發行權杖的簽章和宣告。 AWS API堆疊隨附的 Lambda 函數可用於保護雲端，APIs直到使用者在等候室中進展並收到存取權杖為止。授權者會自動從核心檢索並緩存公鑰和配置以API進行令牌驗證。它可以在沒有修改的情況下使用，並且可以安裝在任何支持的 AWS 區域 AWS Lambda。

OpenID 適配器

OpenID 介面卡堆疊會部署API閘道和 Lambda 函數，以做為 OpenID 身分識別提供者。OpenID 介面卡提供了一組 OIDC-相容，APIs可與支援OIDC身分提供者 (例如 AWS 彈性負載平衡器) 的現有 Web 託管軟體搭配使用 WordPress，或作為 Amazon Cognito 或類似服務的聯合身分提供者使用。該適配器允許客戶在使用具有有限集成選項的 off-the-shelf Web 託管軟件時使用 Authn/Authz 流程中的等候

室。此堆疊也會安裝 CloudFront 分發，其中包含一個 Amazon S3 儲存貯體做為來源，另一個用於記錄請求的 S3 儲存貯體。OpenID 適配器提供一個示例等待室頁面，類似於示例等待室堆棧中提供的頁面，但是為 OpenID 身份驗證流程而設計。通過身份驗證的過程涉及獲取等待室隊列中的位置，並等待服務位置等於或大於客戶端的隊列位置。OpenID 等候室頁面會重新導向回目標網站，該網站使用 OpenID 完API成用戶端的權杖擷取和工作階段設定。該解決方案的API端點直接映射到官方 OpenID Connect 1.0 流程規範， name-for-name. 有關詳細信息，請參閱 OpenID Connect 核心 1.0 認證。



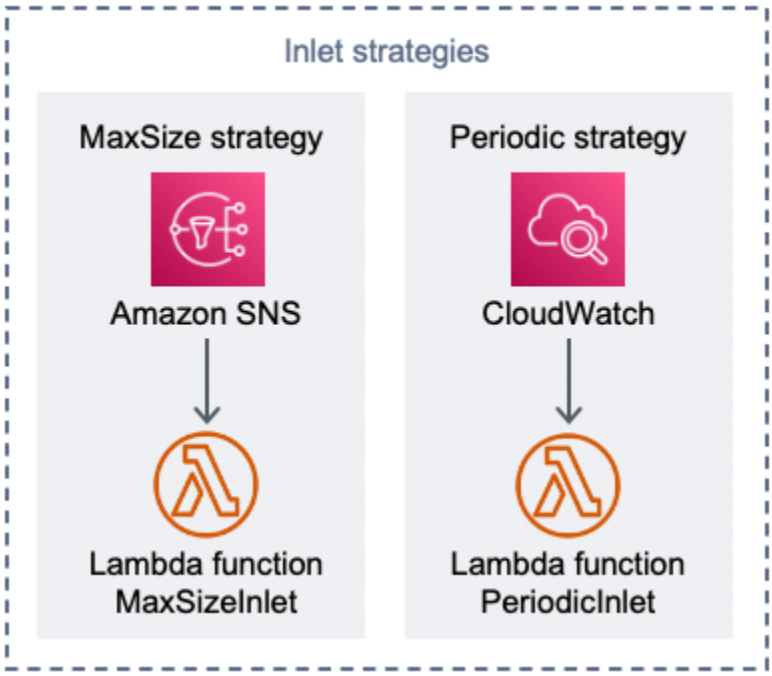
AWS OpenID 適配器組件上的虛擬等候室

1. CloudFront 散發將 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候室頁面。
3. Amazon API Gateway API 提供一組與現有的OIDC網路託管軟體搭配使用，這些軟體可支援OIDC身分供應商的 Lambda 授權功能。APIs
4. `APIHandler`Lambda 函數會處理所有API閘道資源路徑的要求。同一模塊中的不同 Python 函數映射到每個API路徑。例如，API閘道中的`/authorize`資源路徑會在 Lambda 函數`authorize()`內叫用。
5. OIDC設定會儲存在 Secrets Manager 中。

進水策略範例

入口策略決定解決方案的服務計數器何時應向前移動，以容納更多目標場地的使用者。若要取得有關等候室進水策略的更多概念資訊，請參閱設計考量。

解決方案提供了兩種取樣入口策略：MaxSize和「週期性」。



AWS 進水口的虛擬等候室策略元件

最大尺寸入口策略選項：

1. 用戶端會發出 Amazon SNS 通知，呼叫 `MaxSizeInlet` Lambda 函數，以根據訊息承載增加服務計數器。
2. `MaxSizeInlet`Lambda 函數會預期收到一則訊息，說明它使用它決定要增加多少服務計數器。

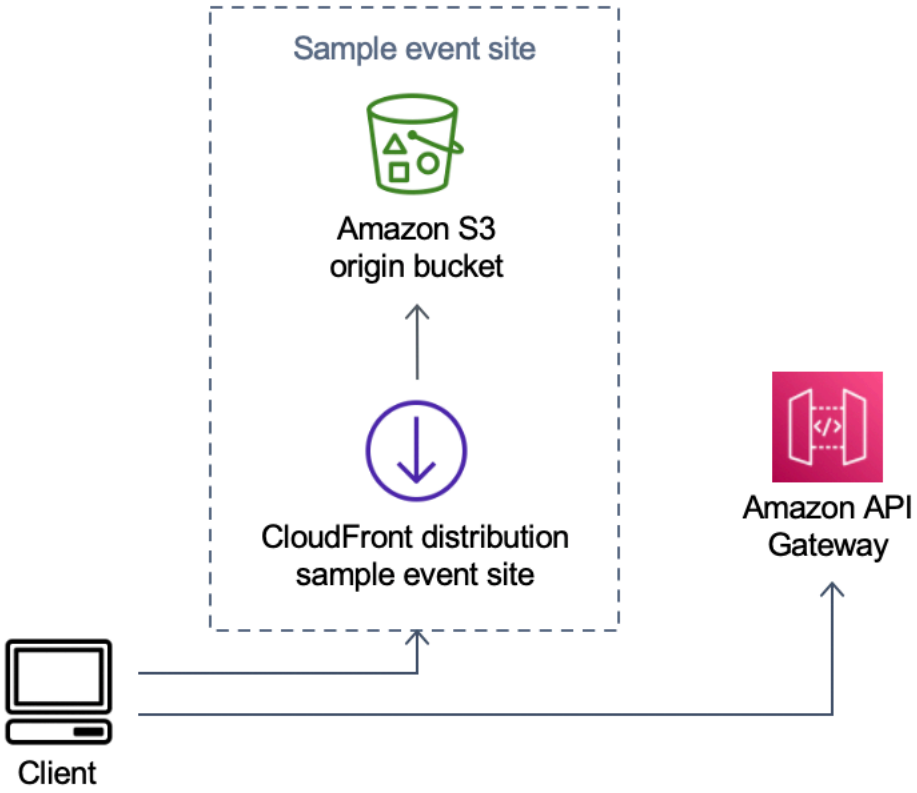
週期性入口策略選項：

3. CloudWatch 規則會每分鐘叫用 Lambda 函數，將服務計數器增加固定數量。
4. 如果時間在提供的開始和結束時間之間，則 `PeriodicInlet` Lambda 函數會按給定大小遞增服務計數器。或者，它會檢查 CloudWatch 警示，如果警示OK處於狀態，則執行增量，否則會略過它。

樣品等候室

樣品等候室除了定制授權者之外，還與公共和私人APIs集成，以展示最小的 end-to-end 等候室解決方案。主網頁存放在 S3 儲存貯體中，並作為的來源使用 CloudFront。它需要用戶完成以下步驟：

1. 在等候室排隊進入現場。
2. 獲得客戶在線的位置。
3. 獲得等候室的服務位置。
4. 當服務位置等於或大於客戶的位置時，獲取令牌集。
5. 使用權杖呼叫受 Lambda 授權者API保護的權限。



AWS 範例事件網站元件上的虛擬等候室

1. S3 儲存貯體託管等候室和控制台的範例內容。
2. CloudFront 散發將 S3 儲存貯體內容提供給使用者。

3. 使用類似購物的資源路徑 (如和) 的API閘道部署範例。/search /checkoutAPI它由堆棧安裝並使用令牌授權者配置。它旨在作為一個簡單的方法來保護候車室API的例子。顯示有效權杖的要求會轉送至 Lambda，否則會傳回錯誤。除了附加的 Lambda 函數的回應之外，沒有API其他功能。

安全

當您在 AWS 基礎架構上建置系統時，安全性責任會由您和 AWS. 由於操作、管理和控制元件，包括主機作業系統、虛擬化層，以及服務 AWS 運作所在設施的實體安全性，因此此共用模型可減輕您的營運負擔。如需有關 AWS 安全性的詳細資訊，請造訪AWS 雲端安全。

彈性痛（RedisOSS）被分配了私有內部的網絡接口。VPC與 Elasticache (RedisOSS) 互動的 Lambda 函數也會在. VPC 所有其他資源都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端點連線到這些服務。

用於建立和驗證JSON網頁權杖的公開金鑰和私密金鑰會在部署階段產生，並儲存在 Secrets Manager 中。用來連線至 Elasticache (RedisOSS) 的密碼也會在部署時產生，並儲存在 Secrets Manager 中。私鑰和彈性密碼（RedisOSS）無法通過任何解決方案訪問。API

公眾API必須通過訪問 CloudFront。解決方案會產生 API Gateway 的API金鑰，此金鑰用作自訂標頭的值`x-api-key`，在中 CloudFront。 CloudFront 在提出原始請求時包含此標頭。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請求。

private APIs 被配置為需要 AWS IAM授權進行調用。解決方案會建立具有適當權限的`ProtectedAPIGroup`IAM使用者群組，以呼叫 private APIs。新增至此群組的IAM使用者會被授權叫用私用APIs。

IAM在角色中使用的原則和附加至解決方案所建立之各種資源的權限，只會授與執行必要工作所需的權限。

對於 S3 儲存貯體、SQS佇列和解決方案產生的SNS主題等資源，靜態和傳輸期間的加密會盡可能啟動。

監控

核心API堆疊包含數個 CloudWatch 警示，可在解決方案運作時進行監控，以偵測問題。堆疊會針對 Lambda 函數錯誤和節流狀況建立警示，並`OK`將`ALARM`警示狀態從一分鐘內發生錯誤或節流狀態時變更為。

此堆疊也會針對 4XX 和 5XX 狀態碼的每個API閘道部署建立警示。`ALARM`如果API在一分鐘內傳回 4XX 或 5XX 狀態碼，警示會`OK`將狀態從變更為。

這些警報會在沒有錯誤或節流一分鐘後返回到`OK`狀態。

IAM角色

AWS Identity and Access Management (IAM) 角色可讓客戶將精細的存取原則和權限指派給 AWS 雲端上的服務和使用者。此解決方案會建立IAM角色，授與解決方案的 AWS Lambda 功能存取權，以建立區域資源。

Amazon CloudFront

建立等候室核心公用和私有APIs的`virtual-waiting-room-on-aws.template` CloudFormation範本，也會為公API用部署 CloudFront 發行版。 CloudFront 緩存來自公眾的響應API，從而減少API網關和執行工作的 Lambda 函數的負載。

此解決方案還具有選用的範例等候室範本，可部署託管在 Amazon 簡單儲存服務 (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 分發部署時使用來源存取身分識別，該身分是提供公開存取解決方案網站儲存貯體內容的 CloudFront 使用者。如需詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的使用來源存取身分限制 Amazon S3 內容的存取。

安全群組

在此解決方案中建立的VPC安全性群組是設計來控制和隔離 Elasticache (RedisOSS) 的網路流量。需要與彈性（RedisOSS）進行通信的 Lambda 被放置在相同的安全組作為彈性（Redis）。OSS我們建議您檢閱安全性群組，並在部署啟動並執行之後，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內容，請部署`virtual-waiting-room-on-aws-getting-started.template`巢狀樣 CloudFormation板，以安裝核心、授權者和範例等候室範本。這為您提供了一個簡單的流程最小的候車室。

支援的通訊協定

AWS 解決方案的虛擬等候室可以與以下內容集成：

- JSON網絡令牌驗證庫和工具
- 現有API閘道部署
- RESTAPI客戶
- OpenID 客戶端和供應商

等候室進氣策略

入口策略封裝了將客戶從等候室轉移到網站所需的邏輯和數據。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。它不需要是一個雲資源，只要它可以調用等候室公共和私人APIs。入口策略接收有關等候室，網站或其他外部指標的事件，這些指標可以幫助其決定何時更多的客戶可以發行令牌並進入站點。入口策略有數種方法。您採用哪一種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呼叫 `increment_serving_num` Amazon API Gateway 私API有的相對值，該值指出有多少用戶端可以進入網站。本節介紹兩種取樣入口策略。這些可以按原樣使用，定制，或者您可以採用完全不同的方法。

MaxSize

使用該 MaxSize 策略，`MaxSizeInletLambda` 函數設定為可同時使用網站的用戶端數目上限。這是一個固定值。用戶端會發出 Amazon SNS 通知，呼叫 `MaxSizeInlet` Lambda 函數，以根據訊息承載增加服務計數器。SNS消息的來源可以來自任何地方，包括網站上的代碼或監視網站使用率水平的監視工具。

L `MaxSizeInlet` ambda 函數預期會收到一則訊息，其中包括：

- `exited` :已完成的交易數
- 要標示為已完成的要求IDs清單
- 要標記為放棄的IDs要求清單

此數據用於確定多少增加服務計數器。在某些情況下，根據用戶端目前的數量，可能沒有額外的容量來增加計數器。

定期

使用週期性策略時， CloudWatch 規則會每分鐘叫用 `PeriodicInlet` Lambda 函數，將服務計數器增加固定數量。週期性入口會以事件開始時間、結束時間和增量來參數化。或者，此策略也會檢查 CloudWatch 警示，如果警示0K處於狀態，則會執行增量，否則會略過警示。場地整合商可以將使用率指標連接到警報，並使用該警報來暫停定期進氣口。此策略只會在目前時間介於開始和結束時間之間時變更服務位置，並且可選擇性地變更指定的警示處於0K狀態。

自訂和延伸解決方案

您組織的場地管理員必須決定要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閘道授權者進行基本整合。
2. 通過身份提供商進行 OpenID 集成。

除了上述整合之外，您可能還需要設定網域名稱重新導向。您也必須負責部署自訂等候室網站頁面。

虛擬等候室 AWS 解決方案專為通過兩種機制進行擴展而設計： EventBridge 用於單向事件通知和 RESTAPIs雙向通信。

配額

虛擬等候室的主要規模限制 AWS 是已安裝 AWS 區域的 Lambda 節流限制。安裝到具有預設 Lambda 並行執行配額的 AWS 帳戶時，虛擬等候室 AWS 解決方案每秒最多可處理 500 個用戶端要求佇列中的位置。每秒 500 個用戶端費率是以具有專門提供所有 Lambda 函數並行配額限制的解決方案為基礎。如果帳戶中的區域與其他叫用 Lambda 函數的解決方案共用，則 AWS 解決方案上的虛擬等候室應至少有 1,000 個並行叫用可用。您可以使用 CloudWatch 指標來繪製帳戶中一段時間內 Lambda 並行呼叫

的圖表，以便做出決定。您可以使用 Ser vice Quotas 控制台來請求增加。如果實際發生額外呼叫，增加 Lambda 節流限制只會增加每月帳戶費用。

每秒額外每 500 個用戶端，將您的節流限制提高 1,000 個。

預期每秒傳入使用者數	建議的並行執行配額
0-500	一千 (預設值)
501-1,000	2,000
1,001-1,500	3,000

Lambda 具有 3,000 次並發呼叫的固定突發限制。如需詳細資訊，請參閱 Lambda 函數調整。如果傳回指出暫時節流狀況的錯誤碼，用戶端程式碼應該預期並重試某些API呼叫。等候室用戶端範例包含此程式碼，作為如何設計用於高容量和高突發事件的用戶端的範例。

此解決方案也與 Lambda 保留和佈建並行處理相容，以及自訂組態步驟。如需詳細資訊，請參閱管理 Lambda 保留並行。

可以進入等候室、接收權杖並繼續進行交易的使用者上限受 Elasticache (RedisOSS) 計數器的上限限制。計數器用於等候室服務位置和解決方案的追蹤摘要狀態。在彈性痛（雷迪斯OSS）中使用的計數器的上限為 9,223,372,036,854,775,807。DynamoDB 表用於儲存發行給等候室使用者的每個權杖的副本。DynamoDB 對於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使用的服務。如需按區域提供的最新 AWS 服務，請參閱區AWS 域服務清單。

AWS CloudFormation 模板

若要自動化部署，此解決方案會使用下列 AWS CloudFormation 範本，您可以在部署前下載這些範本。

如果這是第一次安裝，或者您不確定要安裝什麼內容，請部署範本，該`virtual-waiting-room-on-aws-getting-started.template` AWS CloudFormation 範本會安裝核心、授權者和範例等候室程式碼範本。這使您可以通過簡單的流程測試工作等候室。

View template

virtual-waiting-room-on-aws-api-gateway-cw-logs-role.template：使用此範本可將預設角色新增至帳戶層級的API閘道，ARN以供記錄使用權限。 CloudWatch 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、授權者和範例等候室堆疊。

View template

virtual-waiting-room-on-aws.template：使用此核心模板安裝用於創建等候室事件的核心公共RESTAPIs和私有和雲服務。在您需要等候室RESTAPIs、彈性疼 (RedisOSS) 和 DynamoDB 表格的帳戶和區域中安裝此範本。

View template

virtual-waiting-room-on-aws-Authorizers.template：使用此範本可安裝 Lambda 授權器，專為驗證等候室發出的權杖而設計，以保護最終使用者。APIs需要核心堆疊。核心堆疊的某些輸出需要做為部署此堆疊的參數。這是一個可選的模板。

View template

virtual-waiting-room-on-aws-openid.template：使用此模板安裝 OpenID 身份提供程序，用於等待室與授權接口集成。需要核心堆疊。部署此堆疊需要核心堆疊的某些輸出。這是一個可選的模板。

View template

virtual-waiting-room-on-aws-sample-inlet-strategy .template：使用此範本安裝用於目標站點和等候室之間的樣本入口策略。入口策略有助於封裝邏輯，以確定何時允許更多使用者進入目標場地。需要核心堆疊。部署此堆疊需要核心堆疊的輸出。這是一個可選的模板。

View template

virtual-waiting-room-on-aws-sample.template：使用此範本為等候室和目標網站安裝範例最小網頁和API閘道組態。需要核心和授權者堆疊。核心和授權者堆疊的輸出需要做為部署此堆疊的參數。這是一個可選的模板。

自動化部署

在您啟動解決方案之前，請先檢閱本指南中討論的成本、架構、網路安全性及其他考量。遵循本節中的 step-by-step 指示，設定解決方案並將其部署到您的帳戶中。

部署時間：約 30 分鐘 (僅限取得啟動堆疊)

必要條件

- AWS 帳號主控台權限等同於管理員存取權。
- 從API閘道啟動 CloudWatch 記錄：
  - 登入API閘道主控台，然後選取您計劃安裝堆疊的區域。

    如果您已在此區域中APIs定義現有：

    1. 選取任何API。
    2. 在左側導覽列中，選取 [設定]。
    3. 檢查記CloudWatch 錄角色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，請從啟動獲取啟動堆棧開始。

    如果此區域中沒有APIs定義任何現有的，請安裝virtual-waiting-room-on-aws-api-gateway-cw-logs-role.template.
- 要保護的目標站點的體系結構和實施細節的知識。

部署概觀

請使用下列步驟在上部署此解決方案 AWS。如需詳細說明，請點選各項步驟連結。

步驟 1. 啟動獲取啟動的堆棧

- 將 AWS CloudFormation 範本啟動至您的 AWS 帳戶。
- 檢閱樣板參數，並視需要輸入或調整預設值。

步驟 2.（可選）測試等候室

- 生成 AWS 密鑰以調用IAM安全APIs。
- 打開樣品等候室的控制面板。
- 測試樣品等候室。

步驟 1. 啟動獲取啟動的堆棧

此自動化 AWS CloudFormation 範本會部署核心、授權者和範例等候室範本，讓您檢視和測試工作等候室。在啟動堆疊之前，您必須閱讀並瞭解先決條件。

> **Note**
>
> 您必須負責執行此解決方案時所使用之 AWS 服務的成本。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所使用之每項 AWS 服務的定價網頁。

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

   Launch solution

   或者，您也可以下載範本作為自己實作的起點。
2. 依預設，範本會在美國東部 (維吉尼亞北部) 區域啟動。若要在不同的 AWS 區域中啟動解決方案，請使用主控台導覽列中的 [地區] 選取器。
3. 在 [建立堆疊] 頁面上，確認 Amazon S3 URL 文字方塊中URL是否有正確的範本，然後選擇 [下一步]。
4. 在 [指定堆疊詳細資料] 頁面上，為您的解決方案堆疊指派名稱。若要取得有關命名字元限制的資訊，請參閱《AWS Identity and Access Management 使用指南》中的〈IAM和STS限制〉。
5. 在參數之下，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
事件識別碼	`Sample`	此等候室執行個體的唯一 ID，建議使用GUID格式。
有效期	`3600`	權杖有效期 (以秒為單位)。

參數	預設	描述
啟用事件產生	`false`	如果設為`true`，則與等候室相關的度量會每分鐘寫入其事件匯流排
彈性疼（紅色OSS）端口	`1785`	用於連接至 Elasticache (RedisOSS) 伺服器的連接埠號碼。建議不要使用的預設彈性 (RedisOSS) 連接埠。6379
EnableQueuePositionExpiry	`true`	如果設定為`false`，則不會套用佇列位置到期時間。
QueuePositionExpiryPeriod	`900`	它是以秒為單位的時間間隔，超過該隊列位置不符合產生令牌的資格。
IncrSvcOnQueuePosi tionExpiry	`false`	如果設定為`true`，則會根據未成功產生 Token 的過期佇列位置自動升級服務計數器。

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。核取確認範本建立 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 [AWS CloudFormation 主控台] 的 [狀態] 欄中檢視堆疊的狀態。您應該會在大約 30 分鐘內收到 CREATE _ COMPLETE 狀態。

步驟 2.（可選）測試等候室

如果您部署了取得啟動的堆疊，下列步驟可協助您測試等候室的功能。要完成測試，您需要具有權限的 AWS 密鑰才能調用核心堆棧APIs中的IAM安全密鑰。

生成 AWS 密鑰以調用IAM安全 APIs

1. 在部署`aws-virtual-waiting-room-getting-started.template` CloudFormation 範本的 AWS 帳IAM戶中建立或使用使用者。
2. 授與IAM使用者程式設計存取權限。為IAM使用者建立一組新的存取金鑰時，請在出現時下載金鑰檔案。您需要IAM使用者的存取金鑰 ID 和秘密存取金鑰，才能測試等候室。
3. 將IAM使用者新增至範本所建立的 P rotectedAPIGroup IAM 使用者群組。

打開樣品等候室的控制面板

1. 登入AWS CloudFormation 主控台，然後選取解決方案的開始堆疊。
2. 選擇 Output (輸出) 索引標籤。
3. 在「主鍵」欄下 ControlPanelURL，找到並選取對應的值。
4. 在新標籤頁或瀏覽器視窗中開啟控制台。
5. 在控制台中，展開「組態」區段。
6. 輸入您在產生金鑰中擷取的存取金鑰 ID 和秘密存取AWS 金鑰，以呼叫IAM受保護的金鑰APIs。端點和事件 ID 會從URL參數中填入。
7. 選擇「使用」。提供認證後，按鈕會啟動。

測試樣品等候室

1. 在AWS CloudFormation 主控台中，選取解決方案的啟動堆疊。
2. 選擇 Output (輸出) 索引標籤。
3. 在「主鍵」欄下 WaitingRoomURL，找到並選取對應的值。
4. 打開等候室，然後選擇「預約」進入候車室。
5. 導航回到具有控制面板的瀏覽器選項卡。
6. 在「增加服務計數器」下選擇「變更」 這允許 100 個用戶從等候室移動到目標站點。
7. 返回等候室並選擇立即退房！現在，您將被重定向到目標站點。
8. 選擇「立即購買」以在目標站點完成交易。

部署個別的堆疊

核心堆疊是取得等候室主要功能的唯一必要堆疊。所有其他堆棧都是可選的。如果您還沒有驗證等候室發行的令牌或保護您可能已經擁有的令牌的方法，請啟動授權者堆棧。APIs如果您需要 OpenID 身份提供程序來等待與授權接口的房間集成，請啟動 OpenID 堆棧。範例入口策略堆疊提供了幾個範例，說明如何以及何時允許更多使用者進入您想要保護的網站。

1. 啟動核心堆疊

部署時間：約 20 分鐘

此自動化 AWS CloudFormation 範本可 AWS 在 AWS 雲端上部署虛擬等候室。您必須先完成先決條件，然後才能啟動堆疊。

> **Note**
>
> 您必須自行負責執行此解決方案時所使用之 AWS 服務的成本。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所使用之每項 AWS 服務的定價網頁。

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

   Launch solution

   或者，您也可以下載範本作為自己實作的起點。
2. 依預設，範本會在美國東部 (維吉尼亞北部) 區域啟動。若要在不同的 AWS 區域中啟動解決方案，請使用主控台導覽列中的 [地區] 選取器。
3. 在 [建立堆疊] 頁面上，確認 Amazon S3 URL 文字方塊中URL是否有正確的範本，然後選擇 [下一步]。
4. 在 [指定堆疊詳細資料] 頁面上，為您的解決方案堆疊指派名稱。若要取得有關命名字元限制的資訊，請參閱《AWS Identity and Access Management 使用指南》中的〈IAM和STS限制〉。
5. 在參數之下，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
事件識別碼	Sample	此等候室執行個體的唯一 ID，建議使用GUID格式。
有效期	3600	權杖有效期 (以秒為單位)。
啟用事件產生	false	如果設定為true，則會每分鐘將與等候室相關的指標寫入其事件匯流排。
彈性疼（紅色OSS）端口	1785	用於連接至 Elasticache (RedisOSS) 伺服器的連接埠號碼。建議不要使用的預設彈性 (RedisOSS) 連接埠。6379
EnableQueuePositionExpiry	true	如果設定為false，則不會套用佇列位置到期時間。
QueuePositionExpiryPeriod	900	它是以秒為單位的時間間隔，超過該隊列位置不符合產生令牌的資格。
IncrSvcOnQueuePosi tionExpiry	false	如果設定為true，則會根據未成功產生 Token 的過期佇列位置自動升級服務計數器。

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。核取確認範本建立 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 [AWS CloudFormation 主控台] 的 [狀態] 欄中檢視堆疊的狀態。您應該會在大約 20 分鐘內收到 CREATE _ COMPLETE 狀態。

2. (選擇性) 啟動授權者堆疊

部署時間：大約 5 分鐘

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

   Launch solution

   或者，您也可以下載範本作為自己實作的起點。
2. 依預設，範本會在美國東部 (維吉尼亞北部) 區域啟動。若要在不同的 AWS 區域中啟動解決方案，請使用主控台導覽列中的 [地區] 選取器。
3. 在 [建立堆疊] 頁面上，確認 Amazon S3 URL 文字方塊中URL是否有正確的範本，然後選擇 [下一步]。
4. 在 [指定堆疊詳細資料] 頁面上，為您的解決方案堆疊指派名稱。若要取得有關命名字元限制的資訊，請參閱《AWS Identity and Access Management 使用指南》中的〈IAM和STS限制〉。
5. 在參數之下，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
公用API端點	*<Requires input>*	虛擬等候室的公用端點APIs。
等候室事件 ID	`Sample`	等候室的事件 ID。
發行人 URI	*<Requires input>*	公鑰和令牌URI的發行者。

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。核取確認範本建立 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 [AWS CloudFormation 主控台] 的 [狀態] 欄中檢視堆疊的狀態。您應該會在大約五分鐘內收到 CREATE _ COMPLETE 狀態。

3. （可選）啟動 OpenID 堆棧

部署時間：大約 5 分鐘

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

   Launch solution

   或者，您也可以下載範本作為自己實作的起點。
2. 依預設，範本會在美國東部 (維吉尼亞北部) 區域啟動。若要在不同的 AWS 區域中啟動解決方案，請使用主控台導覽列中的 [地區] 選取器。
3. 在 [建立堆疊] 頁面上，確認 Amazon S3 URL 文字方塊中URL是否有正確的範本，然後選擇 [下一步]。
4. 在 [指定堆疊詳細資料] 頁面上，為您的解決方案堆疊指派名稱。若要取得有關命名字元限制的資訊，請參閱《AWS Identity and Access Management 使用指南》中的〈IAM和STS限制〉。
5. 在參數之下，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
公用API端點	*<Requires input>*	虛擬等候室的公URL用端點APIs。
私有API端點	*<Requires input>*	虛擬等候室的私人端點URLAPIs。
API地區	*<Requires input>*	AWS 公共和私人等候室的區域名稱APIs。
事件識別碼	`Sample`	等候室的事件 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。核取確認範本建立 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 [AWS CloudFormation 主控台] 的 [狀態] 欄中檢視堆疊的狀態。您應該會在大約五分鐘內收到 CREATE _ COMPLETE 狀態。

4. (選擇性) 啟動樣本入口策略堆疊

部署時間：約 2 分鐘

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

   或者，您也可以下載範本作為自己實作的起點。
2. 依預設，範本會在美國東部 (維吉尼亞北部) 區域啟動。若要在不同的 AWS 區域中啟動解決方案，請使用主控台導覽列中的 [地區] 選取器。
3. 在 [建立堆疊] 頁面上，確認 Amazon S3 URL 文字方塊中URL是否有正確的範本，然後選擇 [下一步]。
4. 在 [指定堆疊詳細資料] 頁面上，為您的解決方案堆疊指派名稱。若要取得有關命名字元限制的資訊，請參閱《AWS Identity and Access Management 使用指南》中的〈IAM和STS限制〉。
5. 在參數之下，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
事件識別碼	`Sample`	等候室的事件 ID。
私有核心API端點	*`<Requires input>`*	虛擬等候室的私人端點URLAPIs。
核心API區域	*`<Requires input>`*	AWS 核心安裝API的區域。
進水策略	`Periodic`	要部署的入口策略。`Periodic`每分鐘遞增服務數量。 `MaxSize`根據下游目標網站在指定時間可處理的最大交易數，遞增服務數目。

參數	預設	描述
增量依據	*<Requires input>*	每分鐘應增加多少服務計數器。如果選取週期性入口策略，則需要
開始時間	*<Requires input>*	開始遞增服務數目的時間戳記 (紀元時間 (以秒為單位)。如果選取週期性入口策略，則需要
End Time (結束時間)	*<Requires input>*	停止遞增服務數目的時間戳記 (紀元時間 (以秒為單位)。如果離開 0，則服務數量會無限期地增加。如果選取週期性入口策略，則需要
CloudWatch 警報名稱	*<Requires input>*	與週期性進氣策略相關聯的可選 CloudWatch 報警名稱。如果提供且處於警告狀態，則服務數量不會增加。僅適用於週期性入口策略。
最大尺寸	*<Requires input>*	下游目標網站一次可以處理的最大交易數 (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。核取確認範本建立 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 [AWS CloudFormation 主控台] 的 [狀態] 欄中檢視堆疊的狀態。您應該會在大約兩分鐘內收到 CREATE _ COMPLETE 狀態。

5. (選擇性) 啟動等候室堆疊範例

部署時間：大約 5 分鐘

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

   Launch solution或者，您也可以下載範本作為自己實作的起點。
2. 依預設，範本會在美國東部 (維吉尼亞北部) 區域啟動。若要在不同的 AWS 區域中啟動解決方案，請使用主控台導覽列中的 [地區] 選取器。
3. 在 [建立堆疊] 頁面上，確認 Amazon S3 URL 文字方塊中URL是否有正確的範本，然後選擇 [下一步]。
4. 在 [指定堆疊詳細資料] 頁面上，為您的解決方案堆疊指派名稱。若要取得有關命名字元限制的資訊，請參閱《AWS Identity and Access Management 使用指南》中的〈IAM和STS限制〉。
5. 在參數之下，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
API閘道區域	*<Requires input>*	AWS API閘道的區域名稱。
授權者 ARN	*<Requires input>*	ARNAPI閘道 Lambda 授權者的。
事件識別碼	`Sample`	等候室的事件識別碼。
私有API端點	*<Requires input>*	虛擬等候室的私人端點URLAPIs。
公用API端點	*<Requires input>*	虛擬等候室的公URL用端點APIs。

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。核取確認範本建立 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 [AWS CloudFormation 主控台] 的 [狀態] 欄中檢視堆疊的狀態。您應該會在大約五分鐘內收到 CREATE _ COMPLETE 狀態。

從以前的版本更新堆棧

我們建議您刪除堆疊並為新版本建立新堆疊。目前，不支援使用 CloudFormation 堆疊更新移轉至較新版本。卸載解決方案然後請參閱啟動獲取啟動的堆棧。

> **Note**
>
> 如果您沒有主動使用解決方案來支援持續的事件，我們建議您移轉至較新版本。

效能資料

虛擬等候室 AWS 已使用名為蝗蟲的工具進行負載測試。模擬事件大小從 10,000 到 10 萬個用戶端不等。負載測試環境包括以下配置：

- 蝗蟲 2.x 與雲部署的 AWS 自定義
- 四個 AWS 區域 (us-west-1us-west-2、us-east-1、us-east-2)
- 每個區域 10 c5.4xlarge Amazon EC2 主機 (總共 40 個)
- 每個主機 32 個蝗蟲處理
- 模擬用戶在 1,280 個進程中均勻分佈

每個使用者程序的 end-to-end API 測試步驟：

1. 呼叫assign_queue_num並接收請求 ID。
2. 循環queue_num請求 ID，直到它返回用戶的隊列位置（短時間）。
3. 循環serving_num直到返回值 >= 用戶的隊列位置（長時間）。
4. 很少打電話waiting_room_size來檢索等待用戶的數量。
5. 呼叫generate_token並接收 JWT 以在目標站點中使用。

問題清單

可以通過候診室處理的客戶數量沒有實際上限。

使用者進入等候室的速率會影響 Lambda 函數部署所在區域的並行執行配額。

透過搭配使用的快取政策，負載測試無法超過每秒 10,000 個要求的預設 API Gateway 要求限制 CloudFront。

L get_queue_num ambda 函數的叫用率接近 1:1，接近等候室的傳入使用者。由於並行限制或突發限制，在傳入使用者的高速率期間，此 Lambda 函數可能會受到限制。大量 get_queue_num Lambda 函數叫用所造成的節流可能會影響其他 Lambda 函數的副作用。如果用戶端軟體可以透過重試/退回邏輯適當地回應此類暫時縮放錯誤，整個系統會繼續運作。

核心堆疊在預設配額組態中設定的 CloudFront 散佈可以處理容納 250,000 名使用者的等候室，每位使用者至少每秒輪詢 serving_num API 一次。

疑難排解

本節提供此解決方案的疑難排解資訊。

如果本節無法解決您的問題，請聯絡 AWS Support 提供針對此解決方案開啟 AWS Support 案例的說明。

來自 API 的 4xx 回應狀態

- 這可能是由於不正確的事件 ID 或請求 ID 或兩者都引起的。這會發生在相關 Lambda 函數的 CloudWatch 記錄中。
- 私有 API 通過 IAM 身份驗證，客戶端需要有權調用私有 API 的 AWS 密鑰。這會發生在 API Gateway 的 CloudWatch 記錄檔中。

來自 API 的 5xx 回應狀態

- 來自節流 Lambda 或 API Gateway 的回應，檢查*<LambdaFunctionName>*ThrottlesAlarm CloudWatch警示。
- 後端配置錯誤，請檢查*<LambdaFunctionName>*ErrorsAlarm CloudWatch 警報和 CloudWatch 日誌以獲取詳細信息。

5XX/ErrorPublicPrivateApiAlarm

- 此警報狀態是指 API ALARM 在 60 秒內將 5XX 狀態傳回給呼叫者的時間。
- 此警報OK會在 60 秒內未傳回 5xx 狀態時返回。
- 此警示可透過 Lambda 函數或 Lambda 執行階段將錯誤傳回給 API Gateway 啟動。

4XX/ErrorPublicPrivateApiAlarm

- 此警報狀態是指 API ALARM 在 60 秒內將 4XX 狀態傳回給呼叫者的時間。
- 此警報返回OK到 4XX 狀態返回 60 秒的時間。
- 此警示可由不正確的 API URL 啟動。

*<LambdaFunctionName>*ThrottlesAlarm

- 當具名的 Lambda 在 60 秒內遇到並行執行限制時，此警示狀態為「警示」。

- OK如果 60 秒內沒有遇到節流，則此警報會返回。
- 您可能需要提高帳戶所在地區的並行限制。
- 您可能遇到 Lambda 的突發限制，這需要在用戶端上進行一些重試邏輯。

*<LambdaFunctionName>*ErrorsAlarm

- 此警示狀態是指名為 Lambda ALARM 在 60 秒期間內遇到執行階段執行錯誤的情況。
- OK如果 60 秒內沒有發生任何錯誤，則此警報會返回到。
- 這可能是由於後端配置錯誤引起的。
- 這可能是由 Lambda 程式碼中的錯誤所造成。

。聯繫 AWS Support

如果您有 AWS 開發人員 Support、AWS 商業 S upport 或 AWS 企業 Support，您可以使用 Support 中心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 Sup port 中心。
2. 選擇建立案例。

我們可以如何提供協助？

1. 選擇 [技術]。
2. 對於服務，請選取解決方案。
3. 選取「其他解法」做為「類別」。
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，介面會填入常見疑難排解問題的連結。如果您無法透過這些連結解決問題，請選擇 [下一步：其他資訊]。

其他資訊

1. 在「主旨」中，輸入問題或問題摘要的文字。
2. 對於「說明」，請詳細描述問題。

3. 選擇「附加檔案」。
4. 附加處理請求所 AWS Support 需的資訊。

幫助我們更快地解決您的案件

1. 輸入要求的資訊。
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]，輸入要求的資訊，然後選擇 [提交]。

其他資源

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

卸載解決方案

您可以從 AWS Management Console 或使用 AWS 解決方案解除安裝虛擬等候室 AWS Command Line Interface。您必須依據此解決方案建立的各種資源手動刪除用於存放日誌的 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，因此您仍然可以在解決方案刪除後檢閱記錄事件。

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 使用者群組中移除 IAM 使用者，然後再解除安裝解決方案。否則，IAM 使用者群組和相關聯的 IAM 政策將無法刪除。

對於每個部署的堆棧，請按照以下說明進行操作。

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) 是否可在您的環境中使用。如需安裝指示，請參閱「什麼是 AWS Command Line Interface？ 在《AWS CLI 使用者指南》中。確認可用之後，執行下列命令。 AWS CLI

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

刪除 Amazon S3 存儲桶

如果您決定刪除 AWS CloudFormation 堆疊以防止意外資料遺失，則此解決方案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. 從左側導覽窗格中選擇「值區」。
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儲存庫以下載此解決方案的原始碼檔案，並與其他人共用您的自訂項目。

貢獻者

- 吉姆·塔里奧
- 蒂亚格·拉马干德兰
- 瓊·摩根
- 賈斯汀·皮特爾
- 艾倫·莫海馬尼
- 加維特·辛格
- 巴塞姆瓦尼斯

修訂

日期	變更
2021 年 11 月	初始版本
2022 年 9 月	1.1 版：根據過期佇列位置自動增加服務計數器。將部分 Elasticache （RedisOSS） 用量重新定位至 DynamoDB 。取得剩餘佇列位置到期時間的公有API端點。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2023 年 4 月	1.1.1 版：已緩解所有新 S3 儲存貯體因 S3 物件擁有權 （ACLs 已停用） S3新預設設定所造成的影響。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2023 年 11 月	1.1.2 版：更新套件版本以解決安全漏洞。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2024 年 3 月	1.1.3 版：已解決三個問題：等待室大小中持續存在的過期佇列位置、即使重設後仍queue_num API傳回舊結果，以及 OpenID 轉接器 /userInfo 中的間歇性失敗API。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2024 年 4 月	1.1.4 版：更新套件版本以解決安全漏洞。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2024 年 6 月	1.1.5 版：更新套件版本以解決安全漏洞。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。

日期	變更
2024 年 8 月	1.1.6 版：更新套件版本以解決安全漏洞。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2024 年 8 月	1.1.7 版：更新套件版本以解決安全漏洞。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。
2024 年 9 月	1.1.8 版：更新套件版本以解決安全漏洞。如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。

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 目前的產品供應項目和做法，如有變更，恕不另行通知，且 (c) 不會向其關聯公司、供應商或授權人建立任何承諾或保證。 AWS AWS 產品或服務係依「原狀」提供，不含任何明示或暗示之擔保、陳述或條件。 AWS 客戶的責任和責任由 AWS 協議控制，本文件不屬於與客戶之間 AWS 的任何協議的一部分，也不會修改。

上 AWS 的虛擬等候室根據 Apache 授權 2.0 版的條款授權。

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。