AWS 白皮書

AWS 上的即時通訊

AWS 上的即時通訊: AWS 白皮書

Table of Contents

AWS 上的即時通訊

在 AWS 上設計高度可用和可擴展即時通訊 (RTC) 工作負載的最佳實務

出版日期：2020 年 2 月 13 日 (文件修訂)

摘要

如今，許多組織都希望降低成本並實現即時語音、訊息傳遞和多媒體工作負載的可擴展性。本白皮書概述了在 AWS 上管理即時通訊工作負載的最佳實務，並包括滿足這些要求的參考架構。本白皮書為熟悉即時通訊的個人提供了指南，瞭解如何實現這些工作負載的高可用性和可擴展性。

簡介

使用語音、視訊和訊息傳遞做為管道的通訊應用程式是許多組織及其最終使用者的關鍵要求。這些即時通訊 (RTC) 工作負載具有特定的延遲和可用性要求，可透過遵循相關的設計最佳實務來滿足這些要求。過去，RTC 工作負載已經部署到傳統的內部部署資料中心，並使用專用資源。

但是，由於一組成熟且不斷增長的功能，儘管存在嚴格的服務層級要求，仍可以在 Amazon Web Services (AWS) 上部署 RTC 工作負載，同時也可以受益於可擴展性、彈性和高可用性。如今，一些客戶正在使用 AWS、合作夥伴和開放原始碼解決方案來執行 RTC 工作負載，以降低成本、提高敏捷性、能夠在幾分鐘內實現全球化，並且獲得 AWS 服務的豐富功能。

客戶利用 AWS 的功能，例如使用彈性網路轉接器 (ENA) 的增強型聯網和最新一代 Amazon Elastic Compute Cloud (EC2) 執行個體，從資料平面開發套件 (DPDK)、單根 I/O 虛擬化 (SR-IOV)、巨型分頁、NVM Express (NVMe)、非統一記憶體存取 (NUMA) 支援以及裸機執行個體，以滿足 RTC 工作負載要求。這些執行個體提供高達 100 Gbps 的網路頻寬和每秒相應封包，從而為網路密集型應用程式提供更高的效能。對於擴展，Elastic Load Balancing 提供 Application Load Balancer，它提供 WebSocket 支援和 Network Load Balancer，每秒可以處理數百萬個請求。對於網路加速，AWS Global Accelerator 提供靜態 IP 地址，用作 AWS 中應用程式端點的固定入口點。這支援將靜態 IP 地址用於負載平衡器。為了減少延遲、降低成本並提高頻寬輸送量，AWS Direct Connect 建立從內部部署到 AWS 的專用網路連線。高可用性的受管 SIP 幹線由 Amazon Chime Voice Connector 提供。Amazon Kinesis Video Streams 與 WebRTC 輕鬆串流傳輸即時雙向媒體，具有高可用性。

本白皮書包括一些參考架構，展示如何在 AWS 上設定 RTC 工作負載，並優化解決方案以滿足最終使用者要求的最佳實務，同時針對雲端進行優化。演進的封包核心 (EPC) 已超出本白皮書的範圍，但詳細介紹的最佳實務可套用於虛擬網路功能 (VNF)。

RTC 架構的基本元件

在電信行業，即時通訊 (RTC) 通常是指兩個端點之間最小延遲的直播媒體工作階段。這些工作階段可以與以下內容相關：

- 雙方之間的語音工作階段 (例如電話系統、手機、VoIP)
- 即時訊息 (例如聊天、IRC)
- 即時視訊工作階段 (例如，視訊會議、遠端監控)

前面的每個解決方案都有一些共同的元件 (例如，提供身分驗證、授權和存取控制、轉碼、緩衝和中繼等的元件)和一些傳輸媒體類型獨有的元件 (例如，廣播服務、訊息伺服器和佇列等)。本節重點介紹定義基於語音和視訊的 RTC 系統以及圖 1 所示的所有相關元件。

圖 1：RTC 的基本架構元件

主題

軟交換/PBX

軟交換或 PBX 是語音電話系統的核心，透過使用不同元件在企業內外建立、維護和路由語音通話提供智慧功能。企業的所有使用者都必須在軟交換註冊才能接聽或撥打電話。軟交換的一個重要功能是追蹤每個使用者，以及如何透過使用語音網路中的其他元件聯絡使用者。

工作階段邊界控制器 (SBC)

工作階段邊界控制器 (SBC) 位於語音網路的邊緣，並追蹤所有傳入和傳出流量 (包括控制和資料平面)。SBC 的主要職責之一是保護語音系統免受惡意使用。SBC 可用於與工作階段啟動通訊協定 (SIP) 中繼互連，以實現外部連接。一些 SBC 也提供轉碼功能，用於將編解碼器從一種格式轉換為另一種

格式。最後，大多數 SBC 也提供 NAT 周遊功能，這有助於確保建立通話，甚至跨防火牆網路建立通話。

PSTN 連線能力

IP 語音 (VoIP) 解決方案使用 PSTN 閘道和 SIP 幹線連接舊式的 PSTN 網路。

PSTN 閘道

公共交換電話網路 (PSTN) 閘道轉換傳送訊號 (SIP 和 SS7 之間) 和媒體 (使用編解碼器轉碼在 RTP 和時間分隔多工處理 [TDM] 之間)。 PSTN 閘道始終位於靠近 PSTN 網路的邊緣。

SIP 幹線

在 SIP 幹線中，企業不會終止對 TDM (基於 SS7) 網路的通話，不過企業與電信之間的流量保持在 IP 上。大多數 SIP 幹線都是使用 SBC 建立而成。企業必須就來自電信的預先定義安全規則達成一致，例如允許一定範圍的 IP 地址、連接埠等。

媒體閘道 (轉換編碼器)

一般的語音解決方案允許各種類型的轉碼器。一些常見的編解碼器是北美的 G.711 μ-law，以及北美以外的 G.711 A-law、G.729 和 G.722。當使用兩個不同轉碼器的兩台裝置相互通訊時，媒體伺服器會轉換裝置之間的轉碼器流量。換句話說，媒體閘道處理媒體並確保終端裝置能夠相互通訊。

WebRTC 和 WebRTC 閘道

Web 即時通訊 (WebRTC) 允許您從 Web 瀏覽器建立通話或使用 API 從後端伺服器請求資源。該技術在設計時考慮到雲端技術，因此提供了各種可用於建立通話的 API。由於並非所有語音解決方案 (包括 SIP) 都支援這些 API，因此 WebRTC 閘道需要將 API 呼叫轉換為 SIP 訊息，反之亦然。

圖 2 顯示了高可用性 WebRTC 架構的設計模式。來自 WebRTC 用戶端的傳入流量由 Amazon Application Load Balancer 進行平衡，而 WebRTC 在屬於 Auto Scaling 群組的 EC2 執行個體上執行 WebRTC。

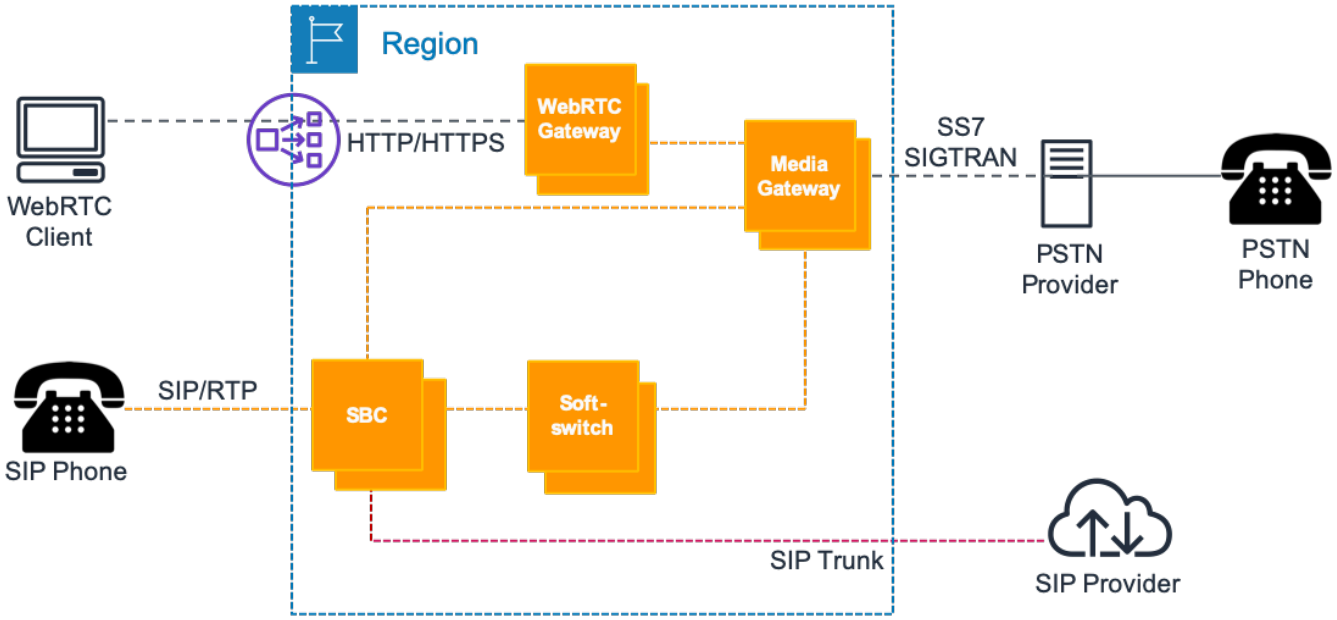

圖 2：語音 RTC 系統的基本拓撲

SIP 和 RTP 流量的另一種設計模式是跨可用區域以主動被動模式使用 Amazon EC2 上的 SBC 對（圖 3）。在其中，彈性 IP 地址可以在發生故障時在無法使用 DNS 的執行個體之間動態移動。

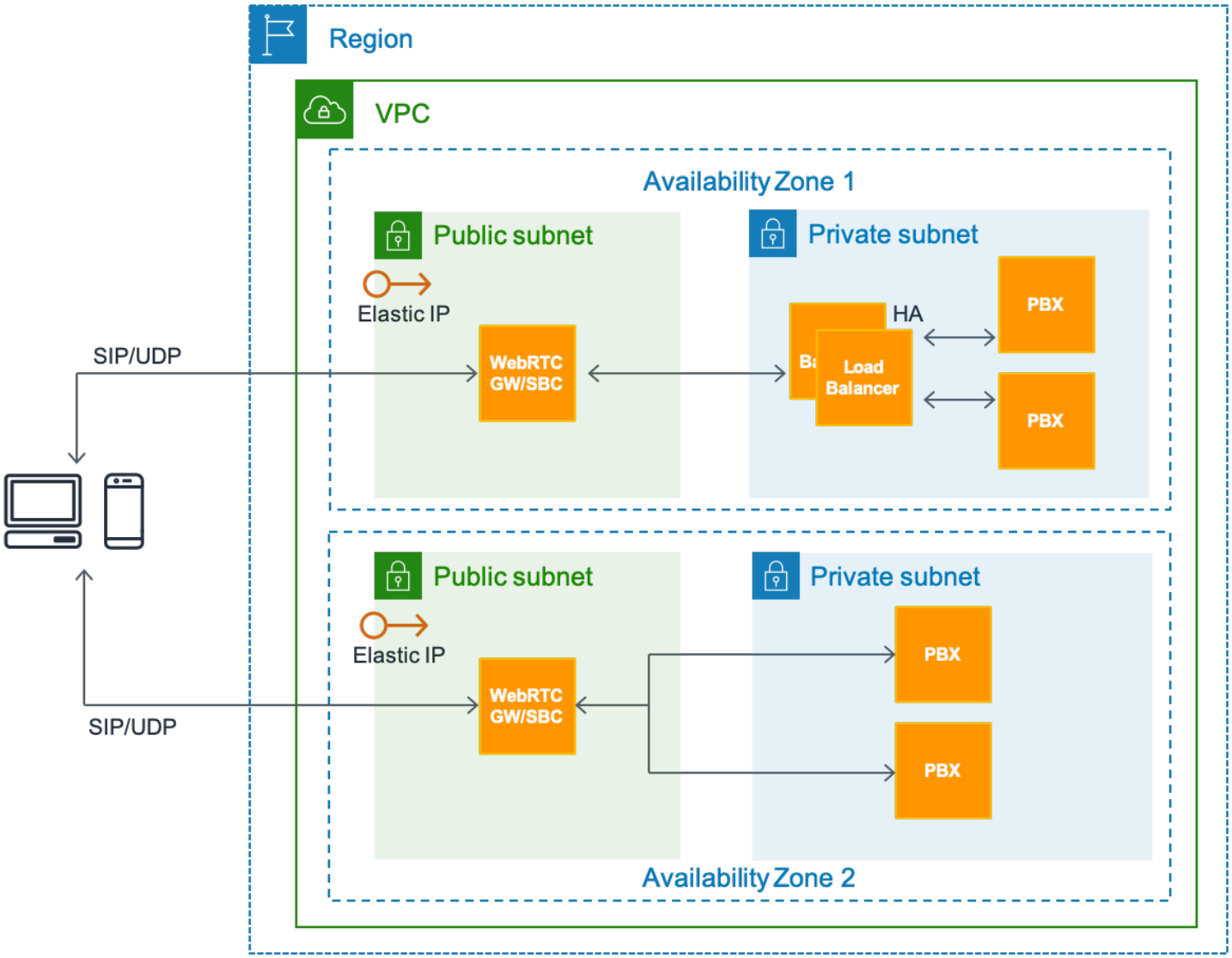

圖 3：在 VPC 中使用 Amazon EC2 的 RTC 架構

AWS 的高可用性和可擴展性

大多數即時通訊服務供應商都與服務層級保持一致，可用性介於 99.9% 到 99.999% 之間。根據所需的高可用性 (HA) 程度，您必須在應用程式的整個生命週期中採取日益複雜的措施。我們建議遵循以下準則，以實現強大的高可用性：

- 將系統設計為沒有單一故障點。對無狀態元件和狀態元件使用自動監控、故障偵測和容錯移轉機制
- 通常使用 N+1 或 2N 備援配置消除單一故障點 (SPOF)，其中 N+1 透過進行中–進行中節點之間的負載平衡實現，2N 透過進行中–備用組態中的一對節點實現。
- AWS 有多種方法可透過這兩種做法實現高可用性，例如透過可擴展的負載平衡叢集或使用進行中–備用對。
- 正確測試系統的可用性。
- 為手動機制準備操作程序，以回應故障、緩解故障並從故障中恢復。

本節重點介紹如何使用 AWS 上提供的功能實現無單一故障點。具體而言，本節介紹了 AWS 核心功能和設計模式的一部分，這些功能和設計模式允許您在平台上建置高可用性的即時通訊應用程式。

主題

進行中-備用狀態伺服器之間 HA 的浮動 IP 模式

浮動 IP 設計模式是一種眾所周知的機制，用於在進行中和備用硬體節點 (媒體伺服器) 對之間實現自動容錯移轉。將靜態輔助虛擬 IP 地址指派給進行中節點。進行中節點和備用節點之間的連續監控可偵測

到故障。如果進行中節點出現故障，監控指令碼會將虛擬 IP 指派給就緒備用節點，並由備用節點接管主要進行中功能。透過這種方式，虛擬 IP 在進行中節點和備用節點之間浮動。

主題

RTC 解決方案的適用性

並不總是可以在服務中使用同一個元件的多個進行中執行個體，例如 N 個節點的進行中-進行中叢集。進行中-備用配置為 HA 提供了最佳機制。例如，RTC 解決方案中的狀態元件 (例如媒體伺服器或會議伺服器，甚至 SBC 或資料庫伺服器) 非常適合用於進行中-備用設定。SBC 或媒體伺服器在指定時間有幾個長時間執行的工作階段或通道進行中，如果 SBC 進行中執行個體出現故障，端點可以重新連接到備用節點，完全不會因為浮動 IP 而造成任何用戶端組態。

在 AWS 上實作

對於使用 Amazon Elastic Compute Cloud (Amazon EC2) 核心功能的 AWS、Amazon EC2 API、彈性 IP 地址以及對輔助私有 IP 地址的 Amazon EC2 支援，您可以實施此模式。

1. 啟動兩個 EC2 執行個體以使用主節點和次節點的角色，主節點預設被假定為處於進行中狀態。
2. 為主 EC2 執行個體指派額外的輔助私有 IP 地址。
3. 彈性 IP 地址與虛擬 IP (VIP) 類似，與輔助私有位址相關聯。此輔助私有位址是外部端點用於存取應用程式的位址。
4. 要將輔助 IP 地址作為別名加入到主網路介面，需要進行某些作業系統組態。
5. 應用程式必須綁定到此彈性 IP 地址。對於星號軟體，您可以透過進階星號 SIP 設定來設定綁定。
6. 在每個節點上執行監控指令碼 (自訂指令碼、KeepAlive on Linux、Corosync 等) 以監控對等節點的狀態。如果目前進行中節點出現故障，對等節點將偵測到此故障，並叫用 Amazon EC2 API 將輔助私有 IP 地址重新指派給自身。
7. 因此，正在偵聽輔助私有 IP 地址相關聯 VIP 的應用程式將透過備用節點可供端點使用。

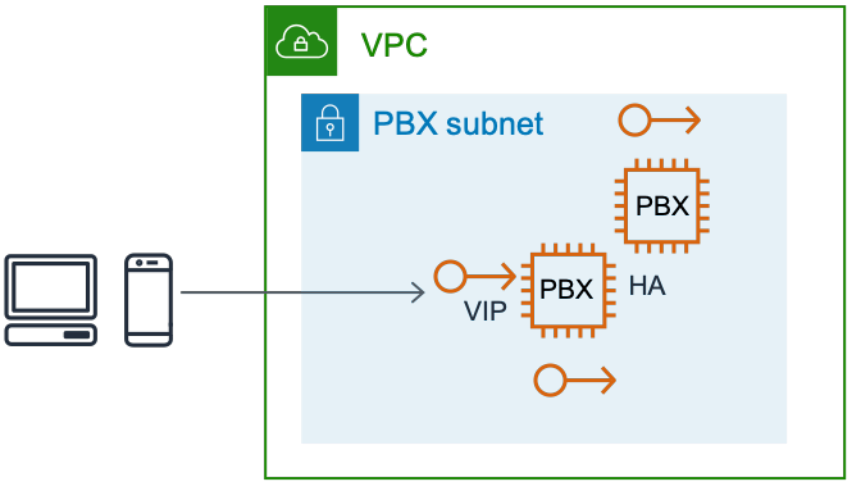

圖 4：使用彈性 IP 地址在狀態 EC2 執行個體之間進行容錯移轉

優勢

此方法是可靠的低預算解決方案，可防止 EC2 執行個體、基礎設施或應用程式層級的故障發生。

限制和可擴展性

此設計模式通常僅限於單個可用區域內。它可以跨兩個可用區域實施，但有變化。在這種情況下，浮動彈性 IP 地址將透過可用的重新關聯彈性 IP 地址 API 在不同可用區域的進行中節點和備用節點之間重新關聯。在圖 4 所示的容錯移轉實施中，正在進行的通話將被刪除，端點必須重新連接。可以透過複寫基礎工作階段資料來擴展此實施，以提供工作階段的無縫容錯移轉或媒體連續性。

透過 WebRTC 和 SIP 實現可擴展性和高可用性的負載平衡

基於預先定義的規則 (例如循環、關聯性或延遲等) 對進行中執行個體叢集進行負載平衡，是 HTTP 請求的無狀態性質廣泛普及的設計模式。事實上，在許多 RTC 應用程式元件的情況下，負載平衡是可行的選擇。

負載平衡器充當對所需應用程式的請求的反向代理或入口點，該應用程式本身被設定為同時在多個進行中節點執行。在任何指定時間點，負載平衡器會將使用者請求導向到定義的叢集之中的一個進行中節點。負載平衡器對其目標叢集中的節點運作狀態檢查，不會向未通過運作狀態檢查的節點發送傳入請求。因此，透過負載平衡實現了一定程度的高可用性。此外，由於負載平衡器以不到 1 秒的間隔對所有叢集節點執行主動和被動運作狀態檢查，因此容錯移轉時間接近瞬間。

根據負載平衡器中定義的系統規則來決定要導向哪個節點，其中包括：

- 輪詢均衡
- 工作階段或 IP 關聯性，確保工作階段內或來自同一個 IP 的多個請求發送到叢集中的同一節點
- 基於延遲
- 基於負載

主題

RTC 架構中的適用性

WebRTC 通訊協定使 WebRTC 閘道可以透過基於 HTTP 的負載平衡器 (例如 Elastic Load Balancing、Application Load Balancer 或 Network Load Balancer) 輕鬆實現負載平衡。由於大多數 SIP 實現都依賴於透過 TCP 和 UDP 傳輸，因此需要網路或連接層級負載平衡，同時支援基於 TCP 和 UDP 的流量。

使用 Application Load Balancer 和 Auto Scaling 在適用於 WebRTC 的 AWS 上進行負載平衡

對於基於 WebRTC 的通訊，Elastic Load Balancing 提供完全受管、高可用性和可擴展的負載平衡器，以作為請求的入口點，然後將請求導向到彈性負載平衡相關聯 EC2 執行個體的目標叢集。此外，由於 WebRTC 請求是無狀態的，因此您可以使用 Amazon EC2 Auto Scaling 提供完全自動化和可控制的可擴展性、彈性和高可用性。

Application Load Balancer 提供全受管的負載平衡服務，該服務使用多個可用區域而達到高可用性，而且可擴展。這支援 WebSocket 請求的負載平衡，這些請求處理 WebRTC 應用程式的傳送訊號，以及用戶端與伺服器之間使用長時間執行的 TCP 連接進行的雙向通訊。Application Load Balancer 也支援基於內容的路由和黏性工作階段，使用負載平衡器產生的 Cookie 將同一個用戶端的請求路由傳輸到同一個目標。如果您啟用黏性工作階段，相同的目標會收到請求，並可使用 Cookie 復原工作階段內容。

圖 5 顯示目標拓撲。

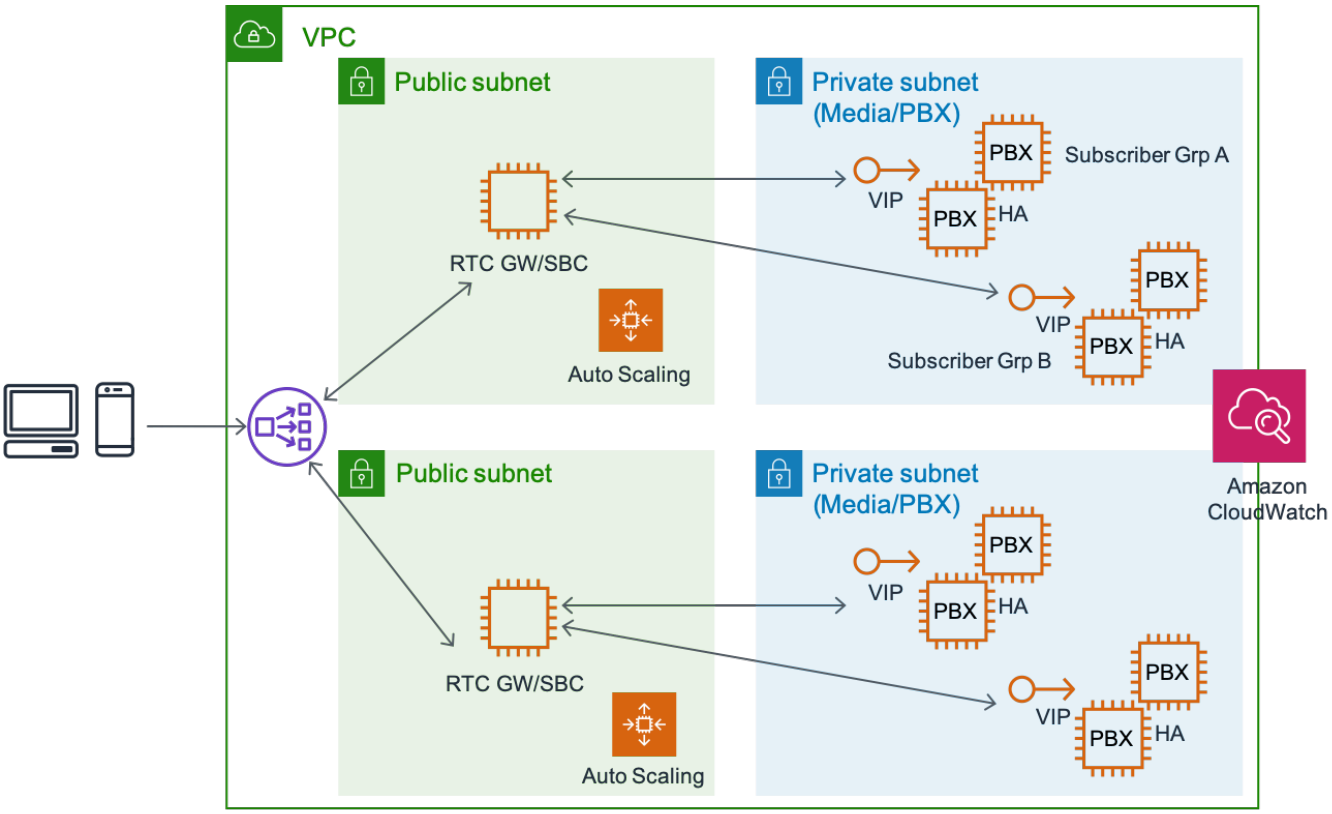

圖 5：WebRTC 可擴展性和高可用性架構

使用 Network Load Balancer 或 AWS Marketplace 產品實施 SIP

對於基於 SIP 的通訊，透過 TCP 或 UDP 建立連接，大多數 RTC 應用程式都使用 UDP。如果 SIP/TCP 是首選的訊號通訊協定，則可以使用 Network Load Balancer 實現完全受管、高可用性、可擴展性和效能負載平衡。

Network Load Balancer 也可在連線層 (Layer 4) 運作，根據 IP 協定資料將連線路由傳輸至目標，例如 Amazon EC2 執行個體、容器及 IP 地址。網路負載平衡適合用於 TCP 或 UDP 流量的負載平衡，每秒能夠處理數百萬個請求，同時保持超低延遲。這與其他流行的 AWS 服務整合，例如 AWS Auto Scaling)、Amazon Elastic Container Service (Amazon ECS)、Amazon Elastic Kubernetes Service (Amazon EKS) 和 AWS CloudFormation。

如果啟動了 SIP 連接，則另一種選擇是使用現成的 AWS Marketplace 商用軟體 (COTS)。AWS Marketplace 提供許多可以處理 UDP 和其他類型第 4 層連接負載平衡的產品。這些 COTS 通常包括對高可用性的支援，並且通常與諸如 AWS Auto Scaling 等功能整合，以進一步增強可用性和可擴展性。圖 6 顯示目標拓撲：

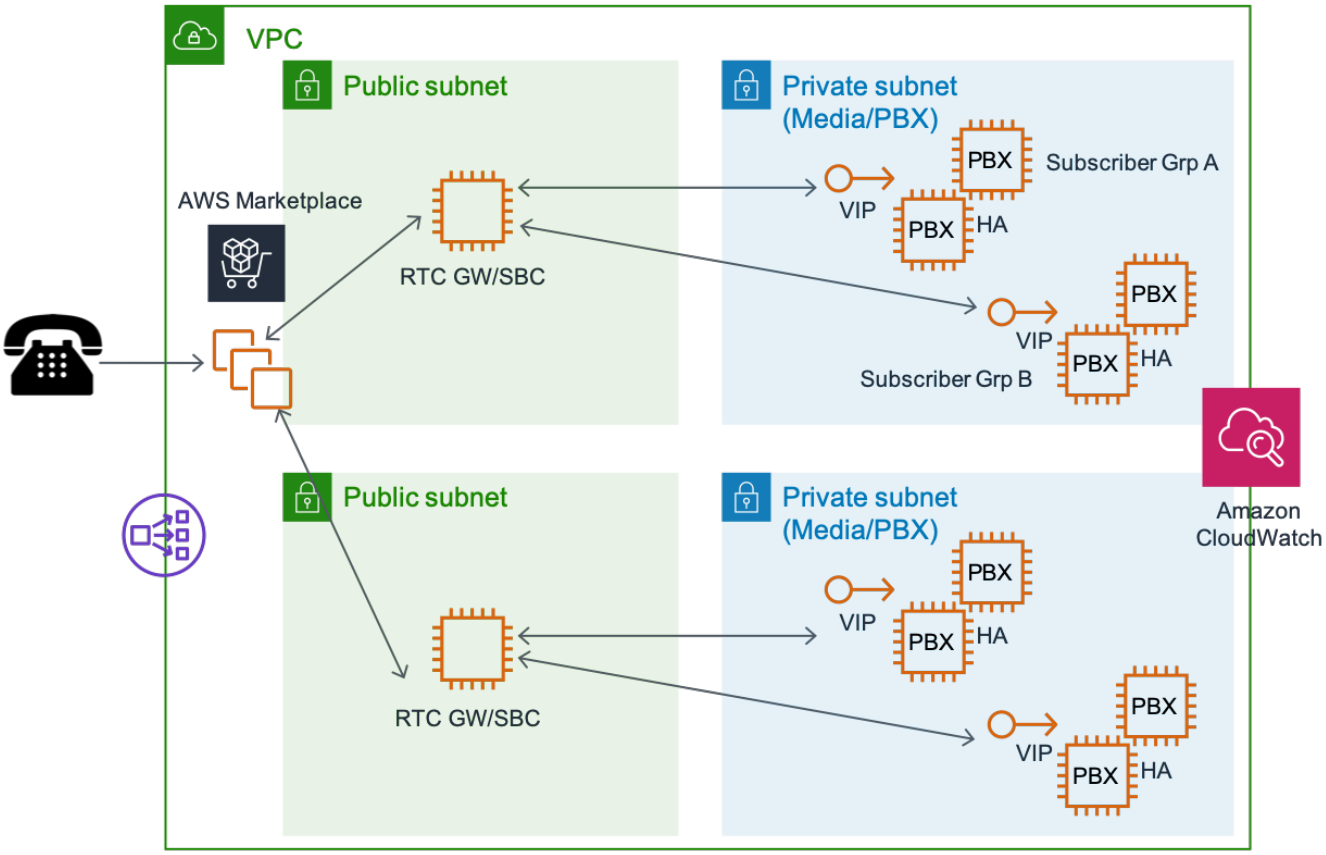

圖 6：基於 SIP 的 RTC 可擴展性與 AWS Marketplace 產品

跨區域基於 DNS 的負載平衡和容錯移轉

Amazon Route 53 提供全球 DNS 服務，可用作公有或私有端點，供 RTC 用戶端註冊和連接媒體應用程式。使用 Amazon Route 53，可以將 DNS 運作狀態檢查設定為將流量路由傳輸到狀況良好的端點，或獨立監控應用程式的運作狀態。Amazon Route 53 Traffic Flow 功能讓您可以輕鬆透過多種路由類型 (包括 Latency Based Routing、Geo DNS、Geoproximity 和加權輪詢均衡) 來管理全球流量，所有的路由類型都可以與 DNS 備援進行組合，以實現各種低延遲容錯架構。無論最終使用者是在單一 AWS 區域或分佈於世界各地，Amazon Route 53 Traffic Flow 簡單視覺化編輯器可以輕鬆管理他們路由到應用程式端點的方式。

在全球部署的情況下，Route 53 中基於延遲的路由政策特別有助於將客戶導向到媒體伺服器的最近連接點，以提高與直播媒體交換相關的服務品質。

請注意，若要強制執行容錯移轉到新 DNS 位址，必須排新用戶端快取。此外，DNS 變更可能會有延遲，因為它們在全球 DNS 伺服器上傳播。您可以使用「存留時間」屬性管理 DNS 查詢的重新整理間隔。此屬性可在設定 DNS 政策時進行設定。

為了快速接觸全球使用者或滿足使用單個公有 IP 的要求，AWS Global Accelerator 也可以用於跨區域容錯移轉。AWS Global Accelerator 是一種聯網服務，可提高本地和全球覆蓋範圍的應用程式所達到的可用性和效能。AWS Global Accelerator 提供靜態 IP 地址，用作應用程式端點的固定入口點，例如一個或多個 AWS 區域中的 Application Load Balancer、Network Load Balancer 或 Amazon EC2 執行個體。它使用 AWS 全球網路優化從使用者到應用程式的路徑，從而提高效能，例如 TCP 和 UDP 流量的延遲。AWS Global Accelerator 持續監控應用程式端點的運作狀態，並在目前端點運作狀態不佳時自動將流量重新引導到最近的正常端點。對於額外的安全要求，加速 Site-to-Site VPN 使用 AWS Global Accelerator 以智慧的方式透過 AWS Global Network 和 AWS 節點路由流量，利用 AWS Global Accelerator 來改善 VPN 連接效能。

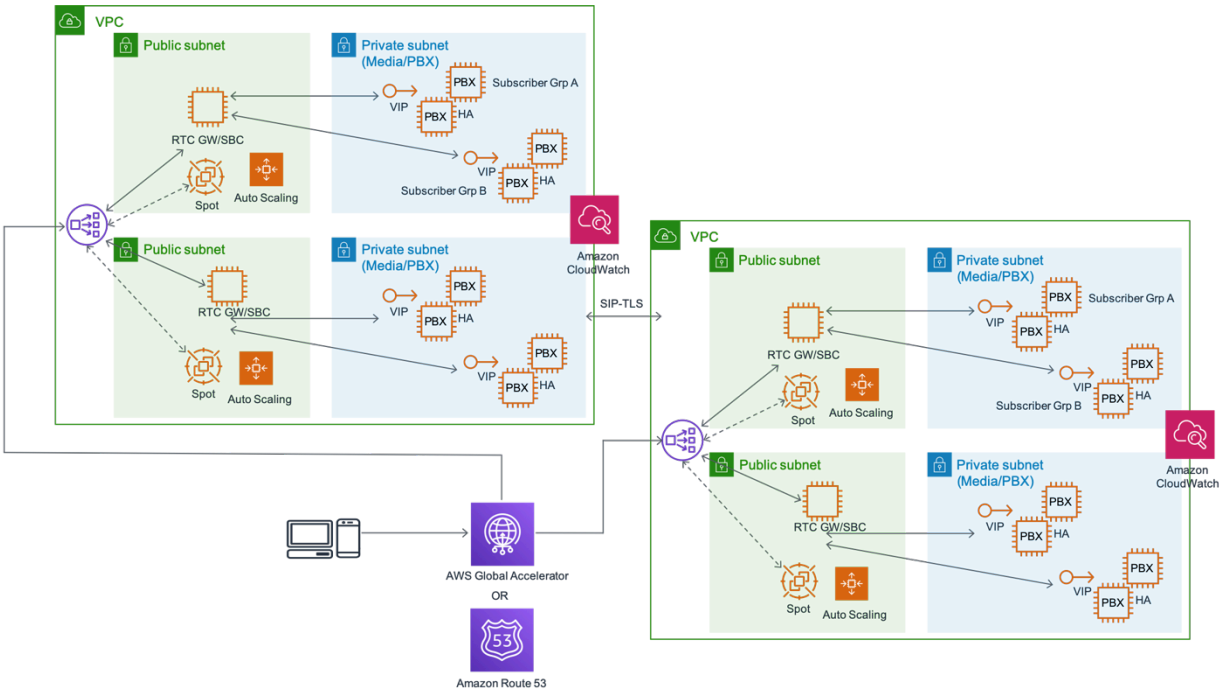

圖 7：使用 AWS Global Accelerator 或 Amazon Route 53 的區域間高可用性設計

持久性儲存的資料持久性和高可用性

大多數 RTC 應用程式依靠持久性儲存來存放和存取資料，以便進行身分驗證、授權、會計 (工作階段資料、通話詳細記錄等)、操作監控和日誌記錄。在傳統資料中心中，通常需要透過設定 SAN、RAID 設計和備份、恢復和容錯移轉處理過程來確保持久性儲存元件 (資料庫、檔案系統等) 的高可用性和持久性。AWS 雲端大幅簡化並增強了關於資料持久性和可用性的傳統資料中心實務。

對於物件儲存和文件儲存，諸如 AWS services like Amazon Simple Storage Service (Amazon S3) 和 Amazon Elastic File System (Amazon EFS) 等 AWS 服務可提供受管的高可用性和可擴展性。Amazon S3 的資料持久性為 99.999999999%。

對於事務性資料儲存，客戶可以選擇利用完全受管的 Amazon Relational Database Service (Amazon RDS)，該服務以高可用性部署支援 Amazon Aurora、PostgreSQL、MySQL、MariaDB、Oracle 和 Microsoft SQL Server。對於註冊商功能、訂閱者設定檔或會計記錄儲存 (例如 CDR)，Amazon RDS 提供容錯、高可用性和可擴展性的選項。

使用 AWS Lambda、Amazon Route 53 和 AWS Auto Scaling 的動態擴展

AWS 允許將功能鏈接起來，並能夠根據基礎設施事件將自訂無伺服器功能整合為服務。在 RTC 應用程式中具有許多多功能用途的設計模式之一是將自動擴展生命週期掛鉤與 Amazon CloudWatch Events、Amazon Route 53 和 AWS Lambda 功能相結合。AWS Lambda 函數可以嵌入任何動作或邏輯。圖 8 展示了這些功能鏈接在一起如何透過自動化提高系統的可靠性和可擴展性。

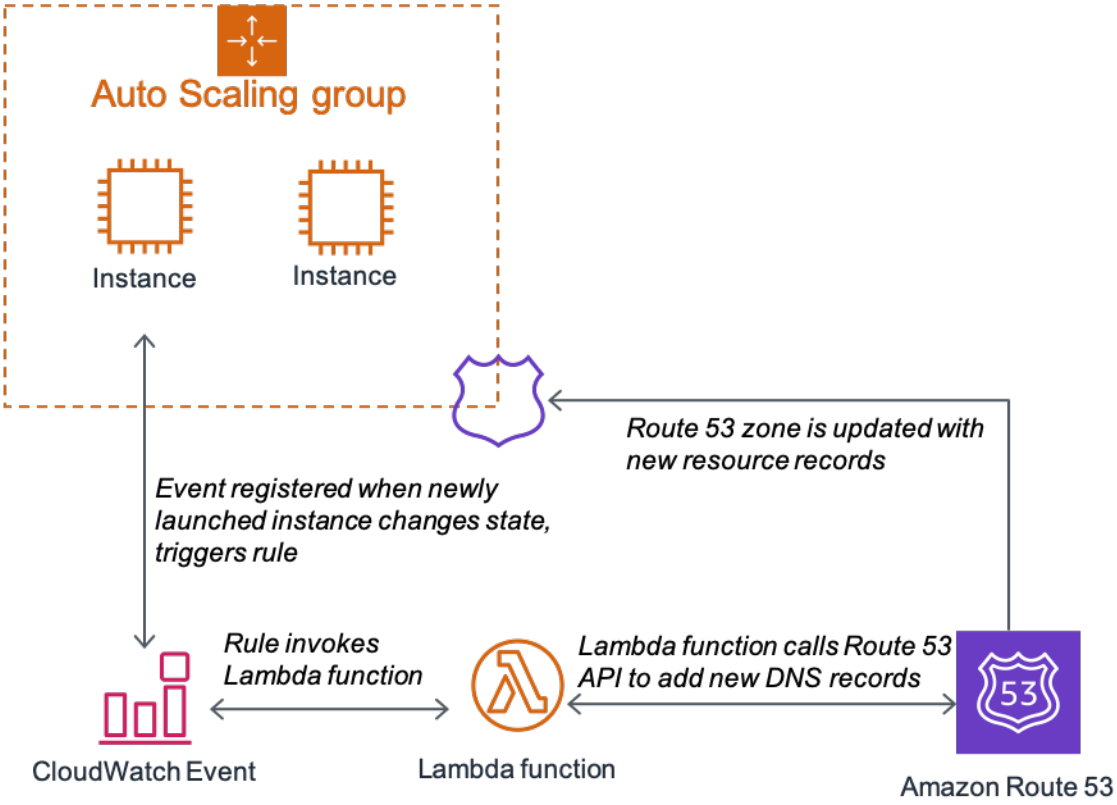

圖 8：使用 Amazon Route 53 的動態更新自動擴展

具有 Kinesis Video Streams 的高可用性 WebRTC

Amazon Kinesis Video Streams 透過 WebRTC 提供直播媒體串流，允許使用者擷取、處理和存放媒體串流，用於播放、分析和機器學習。這些串流達到高度可用性和可擴展性，並符合 WebRTC 標

準。Amazon Kinesis Video Streams 包含 WebRTC 傳送訊號端點，用於快速對等探索和安全連線建立。其包含受管 Session Traversal Utilities for NAT (STUN) 和 Traversal Using Relays around NAT (TURN) 端點，以便即時交換對等端之間的媒體。它還包含免費的開放原始碼 SDK，可直接與攝影機韌體整合，以針對對等探索和媒體串流，啟用與 Kinesis Video Streams 端點的安全通訊。最後，它提供適用於 Android、iOS 和 JavaScript 的用戶端程式庫，允許符合 WebRTC 的行動和 Web 播放器安全地探索，並與攝影機裝置連接，以進行媒體串流和雙向通訊。

具有 Amazon Chime Voice Connector 的高可用性 SIP 幹線

Amazon Chime Voice Connector 提供依用量付費的 SIP 主幹連線服務，讓公司能夠使用其電話系統安全且實惠撥打及/或接聽電話。Amazon Chime Voice Connector 是服務供應商 SIP 主幹連線或 Integrated Services Digital Network (ISDN) Primary Rate Interfaces (PRI) 的低成本替代產品。客戶可以選擇啟用撥入通話、外撥通話或同時啟用這兩者。該服務利用 AWS 網路，在多個 AWS 區域間提供高可用性通話體驗。您可以從 SIP 幹線電話通話串流傳輸音訊，或將基於 SIP 的媒體錄製 (SIPREC) 來源轉發到 Amazon Kinesis Video Streams，以即時從業務通話中獲取洞察。透過與 Amazon Transcribe 和其他常用機器學習庫整合，您可以快速建置音訊分析應用程式。

來自現場的最佳實務

本部分旨在總結執行大型即時工作階段啟動通訊協定 (SIP) 工作負載的一些最大和最成功 AWS 客戶所實施的最佳實務。希望在公有雲中執行自己的 SIP 基礎設施的 AWS 客戶會發現這些最佳實務很有價值，因為這些最佳實務有助於在發生不同類型的故障時提高系統的可靠性和彈性。雖然其中一些最佳實務是 SIP 特定的最佳實務，但其中大多數都適用於 AWS 上執行的任何即時通訊應用程式。

主題

建立 SIP 重疊

AWS 擁有強大、可擴展且備援的骨幹網路，可在不同區域之間提供連線。當網路事件 (例如光纖切斷) 降低 AWS 骨幹網路連結時，流量會使用網路層級路由通訊協定 (如 BGP) 快速容錯移轉到備援路徑。此網路級流量工程對 AWS 客戶來說是黑箱，大多數客戶甚至沒有注意到這些容錯移轉事件。但是，執行即時工作負載 (例如語音、高畫質視訊和低延遲訊息傳送) 的客戶有時會注意到這些事件。因此，AWS 客戶如何在 AWS 提供的網路層級實施自己的流量工程？ 該解決方案正在多個不同的 AWS 區域部署 SIP 基礎設施。做為通話控制功能的一部分，SIP 也提供透過特定 SIP 代理路由傳輸通話的功能。

圖 9：使用 SIP 路由取代網路路由

在圖 9 中，SIP 基礎設施 (以綠點表示) 在美國所有四個區域運作。藍線代表 AWS 骨幹網路的虛構描述。如果未實施 SIP 路由，則來自美國西海岸並發往美國東海岸的通話將直接連接俄勒岡州和弗吉尼亞州區域的骨幹網路連結。該圖顯示了客戶如何取代網路層級路由，並在俄勒岡和弗吉尼亞之間使用 SIP 路由透過加利福尼亞州進行相同的通話。這種類型的 SIP 流量工程可以使用 SIP 代理和基於網路指標 (例如 SIP 重新傳輸和客戶特定業務偏好) 的媒體閘道來實現。

執行詳細監控

即時語音和視訊應用程式的最終使用者希望獲得與傳統電話服務相同的效能。因此，當他們遇到應用程式問題時，最終供應商的聲譽會受到損害。為了主動而不是被動，對於為最終使用者服務的系統，必須在系統的每個部分部署詳細監控。

圖 10：使用 SIPp 監控 VoIP 基礎設施

許多開放原始碼工具 (例如 iPerf 或 SIPp) 和 VOIPMonitor，可用於監控 SIP/RTP 流量。在上面的範例中，在用戶端和伺服器模式下執行 SIPp 的節點正在測量 SIP 指標，例如在所有四個美國 AWS 區域之間成功通話和 SIP 重新傳輸。然後，可以使用自訂指令碼將這些指標匯出到 Amazon CloudWatch 中。使用 CloudWatch，客戶可以根據特定閾值對這些自訂指標建立警示。然後，可以根據這些 CloudWatch 警示的狀態執行自動或手動補救動作。

如果客戶不希望分配開發和維護自訂監控系統所需的工程資源，市場上有許多優質的 VoIP 監控解決方案，例如 ThousandEyes。補救動作的一個範例是根據增加的 SIP 重新傳輸變更 SIP 路由。

將 DNS 用於負載平衡和浮動 IP 進行容錯移轉

支援 DNS SRV 功能的 IP 電話服務用戶端可以透過將用戶端負載平衡到不同的 SBCS/PBX 來有效地使用基礎設施中內建的備援。

圖 11：使用 DNS SRV 記錄對 SIP 用戶端進行負載平衡

圖 11 顯示了客戶如何使用 SRV 記錄對 SIP 流量進行負載平衡。任何支援 SRV 標準的 IP 電話用戶端都會尋找 SRV 類型 DNS 記錄中的 sip._<transport protocol> 前綴。在此範例中，DNS 的接聽部分包含在不同 AWS 可用區域中執行的兩個 PBX。但是，除了端點 URI 之外，SRV 記錄也包含三個額外的資訊：

- 第一個數字是優先順序 (上面範例中為 1)。較低的優先順序優先於較高的優先順序。
- 第二個數字是權重 (在上面的範例中為 10)。
- 第三個數字是要使用的連接埠 (5060)。

由於兩台 PBX 伺服器的優先順序相同 (1)，因此用戶端使用權重在兩個 PBX 之間進行負載平衡。在這種情況下，由於權重相同，所以 SIP 流量應在兩個 PBX 之間進行負載平衡。

DNS 可以是用戶端負載平衡的適當解決方案，但透過變更/更新 DNS「A」記錄來實現容錯移轉怎麼辦？ 由於用戶端和中間節點中的 DNS 快取行為出現不一致，因此不鼓勵使用此方法。在 SIP 節點叢集之間進行可用區域內容錯移轉的更好方法是使用 EC2 IP 重新分配，其中使用 EC2 API 將受損主機的 IP 地址立即重新分配給正常執行的主機。與詳細的監控和運作狀態檢查解決方案配合使用，故障節點的 IP 重新分配可確保流量適時移動到正常執行的主機，從而盡可能減少最終使用者中斷。

使用多個可用區域

每個 AWS 區域被細分為個別的可用區域。每個可用區域都有自己的電源、冷卻和網路連線，因此構成孤立的故障網域。在 AWS 的構造中，始終鼓勵客戶在多個可用區域中執行其工作負載。這可確保客戶應用程式甚至能夠承受完整的可用區域故障，這本身就是非常罕見的事件。此建議也代表即時 SIP 基礎設施。

圖 12：處理可用區域故障

假設災難性事件 (例如第 5 類颶風) 會導致 US-East-1 可用區域完全停機。基礎設施如圖所示執行後，所有最初向故障可用區域中的節點註冊的 SIP 用戶端都應向可用區域 #2 中執行的 SIP 節點重新註冊。(使用 SIP 用戶端/手機測試此行為，以確保它受支援。)儘管可用區域中斷時的進行中 SIP 通話將中斷，但所有新通話都會透過可用區域 #2 路由傳送。

總而言之，DNS SRV 記錄應該將用戶端指向多個「A」記錄，每個可用區域內有一個記錄。相反地，每個「A」記錄都應指向該可用區域中 SBCS/PBX 的多個 IP 地址，同時提供可用區域內和區域間的恢復能力。如果 IP 是公有，則可以透過使用 IP 重新分配來實現可用區域內和可用區間的容錯移轉。但是，私有 IP 不能跨可用區域重新分配。如果客戶使用私有 IP 地址，則必須依靠 SIP 用戶端重新註冊到備份 SBC/PBX 進行可用區域間容錯移轉。

將流量保持在一個可用區域內，並使用 EC2 置放群組

此最佳實務也稱為可用區域關聯性，也適用於發生完整可用區域故障的罕見事件。建議您消除任何跨可用區域流量，以便進入一個可用區域的所有 SIP 或 RTP 流量都應保留在該可用區域中，直到這些流量離開該區域為止。

圖 13：可用區域相關性 (最多 50% 的進行中通話中斷)

圖 13 顯示使用可用區域關聯性的簡化架構。如果考慮到完全可用區域中斷的影響，此方法的相對優勢就會變得清楚。如圖所示，如果可用區域 #2 中斷，則 50% 的進行中通話最多受到影響 (假設可用區域

之間的負載平衡相等)。如果未實現可用區域關聯性，則某些通話將在一個區域的可用區域之間流動，故障很可能會影響 50% 以上的進行中通話。

此外，為了盡可能減少流量的延遲，我們也建議您考慮在每個可用區域內使用 EC2 放置群組。在同一個 EC2 置放群組中啟動的執行個體具有更高的頻寬和更低的延遲，因為 EC2 可確保這些執行個體相對於彼此之間的網路接近。

使用增強型聯網 EC2 執行個體類型

在 Amazon EC2 上選擇正確的執行個體類型可確保系統的可靠性以及基礎設施的有效利用。EC2 提供各式各樣的最佳化執行個體類型，以滿足不同的使用案例。執行個體類型由不同的 CPU、記憶體、儲存體和聯網容量組合而成，讓您為應用程式靈活性選擇適當的資源組合。這些增強型聯網執行個體類型可確保其中執行的 SIP 工作負載能夠存取一致的頻寬和相對較低的聚合延遲。Amazon EC2 最近增加的一項功能是彈性網路轉接器 (ENA) 的可用性，該轉接器可提供高達 100 Gbps 的頻寬。EC2 執行個體類型和相關功能的最新目錄可在 EC2 執行個體類型頁面找到。

對於大多數客戶來說，最新一代的運算優化執行個體應能為成本提供最佳價值。例如，C5N 支援頻寬高達 100 Gbps 的新彈性網路轉接器，每秒數百萬個封包 (PPS)。大多數即時應用程式也將受益於使用 Intel Data Plane Developer Kit (DPDK)，該套件可大幅提升網路封包處理能力。

不過，最佳實務是，根據您的要求對各種 EC2 執行個體類型進行基準測試，以查看哪種執行個體類型最適合您。基準測試也使您能夠尋找其他配置參數，例如某個執行個體類型一次可處理的最大通話次數。

安全考量

RTC 應用程式元件通常直接在面向網際網路的 Amazon EC2 執行個體上執行。除了 TCP 之外，流程也使用 UDP 和 SIP 等通訊協定。在這些情況下，AWS Shield Standard 可以保護 Amazon EC2 執行個體免受常見的基礎設施層 (第 3 層和第 4 層) DDoS 攻擊，例如 UDP 反射攻擊、DNS 反射、NTP 反射、SSDP 反射等。AWS Shield Standard 使用各種技術，如基於優先順序的流量調整，當偵測到明確定義的 DDoS 攻擊特徵碼時，會自動使用這些技術。

AWS 也在彈性 IP 地址啟用 AWS Shield Advanced，為這些應用程式提供針對大型複雜 DDoS 攻擊的進階保護。AWS Shield Advanced 提供增強型 DDoS 偵測功能，可自動偵測 AWS 資源的類型和 EC2 執行個體的大小，並套用適當的預先定義緩解措施，並針對 SYN 或 UDP 泛洪提供保護。藉由 AWS Shield Advanced，客戶也可以透過與全天候 AWS DDoS 回應團隊 (DRT) 聯繫建立自己的自訂緩解設定檔。另外，AWS Shield Advanced 可確保您的所有 Amazon VPC 網路存取控制清單 (ACL) 在 DDoS 攻擊期間會自動在 AWS 網路邊界執行，讓您存取額外的頻寬和清理中容量，以減緩大規模 DDoS 攻擊。

結論

即時通訊 (RTC) 工作負載可部署在 Amazon Web Services (AWS) 上，以實現可擴展性、彈性和高可用性，同時滿足關鍵要求。如今，一些客戶正在使用 AWS、合作夥伴和開放原始碼解決方案來執行 RTC 工作負載，以降低成本、提高敏捷性並減少全球使用量。

本白皮書中提供的參考架構和最佳實務可幫助客戶在 AWS 上成功設定 RTC 工作負載，並優化解決方案以滿足最終使用者的要求，同時針對雲端進行優化。

作者群

協力完成本文件的個人與組織如下：

- Ahmad Khan，Amazon Web Services 資深解決方案架構師
- Tipu Quresh，Amazon Web Services AWS Support 首席工程師
- Hasan Khan，Amazon Web Services 資深技術客戶經理
- Shoma Chakravarty，Amazon Web Services 電信全球技術負責人

文件修訂

若要收到此白皮書更新的通知，請訂閱 RSS 摘要。

update-history-change	update-history-description	update-history-date
白皮書已更新	已更新最新的服務和功能。	2020 年 2 月 13 日
初次出版	白皮書初始出版。	2018 年 10 月 1 日

聲明

客戶應負責對本文件中的資訊自行進行獨立評估。本文件：(a) 僅供參考之用，(b) 代表目前的 AWS 產品供應與實務，如有變更恕不另行通知，以及 (c) 不構成 AWS 及其附屬公司、供應商或授權人的任何承諾或保證。AWS 產品或服務以「現況」提供，不提供任何明示或暗示的擔保、主張或條件。AWS 對其客戶之責任與義務，應受 AWS 通訊協定之約束，且本文件並不屬於 AWS 與其客戶間之任何通訊協定的一部分，亦非上述通訊協定之修改。