AWS ホワイトペーパー

AWS でのリアルタイム通信

AWS でのリアルタイム通信: AWS ホワイトペーパー

Table of Contents

AWS でのリアルタイム通信

AWS で可用性が高く、スケーラブルなリアルタイム通信 (RTC) ワークロードを設計するためのベストプラクティス

公開日：2020 年 2 月 13 日 (日改訂履歴)

要約

今日、多くの組織が、リアルタイムの音声、メッセージング、マルチメディアワークロードのコスト削減とスケーラビリティの実現を模索しています。このホワイトペーパーでは、AWS でリアルタイム通信ワークロードを管理するためのベストプラクティスを概説し、これらの要件を満たすリファレンスアーキテクチャについても説明します。このホワイトペーパーは、リアルタイム通信に精通している個人を対象に、これらのワークロードに対して高可用性とスケーラビリティを実現する方法に関するガイドとして役立ちます。

はじめに

音声、ビデオ、メッセージングをチャネルとして使用する通信アプリケーションは、多くの組織とそのエンドユーザーにとって重要な要件です。これらのリアルタイム通信 (RTC、real-time communication) ワークロードには、関連する設計のベストプラクティスに従うことで満たすことができる、特定のレイテンシーと可用性の要件があります。これまで、RTC ワークロードは、専用のリソースとともに、従来のオンプレミスデータセンターにデプロイされていました。

ただし、一連の機能が成熟し発展しているため、非常に厳しいサービスレベル要件でも RTC ワークロードをアマゾン ウェブ サービス (AWS) にデプロイできると同時に、スケーラビリティ、伸縮性、高可用性のメリットも得られます。現在、複数のお客様が、AWS、そのパートナー、およびオープンソースソリューションを使用して、コストの削減、より迅速な俊敏性、わずか数分でのグローバル展開を実現し、AWS のサービスの豊富な機能を利用して RTC ワークロードを実行しています。

お客様は、Elastic Network Adapter (ENA) による拡張ネットワーキングや、最新世代の Amazon Elastic Compute Cloud (EC2) インスタンスなどの AWS の機能を活用して、データプレーン開発キット (DPDK、data plane development kit)、シングルルート I/O 仮想化 (SR-IOV、single root I/O virtualization)、huge ページ、NVM Express (NVMe)、不均一メモリアクセス (NUMA、non-uniform memory access) のサポート、また RTC ワークロード要件を満たすベアメタルインスタンスのメリットを享受できます。これらのインスタンスは、最大 100 Gbps のネットワーク帯域幅とそれに見合った 1 秒あたりのパケット数を提供し、ネットワーク負荷の大きいアプリケーションのパフォーマンスを向上させます。スケーリングには、Elastic Load Balancing は WebSocket をサポートする Application Load Balancer と、1 秒あたり数百万のリクエストを処理できる Network Load Balancer を提供します。ネットワークアクセラレーションには、AWS Global Accelerator が AWS のアプリケーションエンドポイントへの固定エントリポイントとして機能する静的 IP アドレスを提供します。これは、ロードバランサーの静的 IP アドレスをサポートします。レイテンシーとコストの削減および帯域幅のスループット向上には、AWS Direct Connect がオンプレミスから AWS への専用ネットワーク接続を確立します。Amazon Chime Voice Connector により、可用性の高いマネージド SIP トランキングが提供されます。Amazon Kinesis Video Streams と WebRTC は、可用性が高いリアルタイムの双方向メディアを簡単にストリーミングできます。

この文書には、AWS で RTC ワークロードを設定する方法を示すリファレンスアーキテクチャと、ソリューションをクラウド向けに最適化しつつエンドユーザーの要件を満たすように最適化するためのベストプラクティスが含まれています。Evolved Packet Core (EPC) はこのホワイトペーパーの対象外ですが、説明されたベストプラクティスは仮想ネットワーク機能 (VNF) にも適用できます。

RTC アーキテクチャの基礎コンポーネント

通信業界では、リアルタイム通信 (RTC、real-time communication) とは通常、2 つのエンドポイント間でレイテンシーを最小限に抑えたライブメディアセッションを指します。このようなセッションは、以下のようなものに関連しています。

- 2 者間の音声セッション (電話システム、モバイル、VoIP など)
- インスタントメッセージ (チャット、IRC など)
- ライブビデオセッション (ビデオ会議、テレプレゼンスなど)

前述の各ソリューションには、共通のコンポーネント (認証、認可、アクセス制御、トランスコーディング、バッファリング、リレーなどを提供するコンポーネント) と、送信されるメディアのタイプに固有のコンポーネント (ブロードキャストサービス、メッセージングサーバー、キューなど) があります。このセクションでは、音声ベースおよびビデオベースの RTC システムと、図 1 に示すすべての関連コンポーネントの定義を取り上げます。

図 1: RTC に不可欠なアーキテクチャコンポーネント

トピック

ソフトスイッチ/PBX

ソフトスイッチまたは PBX は、音声電話システムの頭脳であり、さまざまなコンポーネントを使用して、社内外の音声コールを確立、保守、ルーティングするためのインテリジェンスを提供します。コールを送受信するには、企業のすべてのサブスクライバーが、ソフトスイッチに登録する必要があります。ソフトスイッチの重要な機能は、各サブスクライバーと、音声ネットワーク内の他のコンポーネントを使用してサブスクライバーに到達する方法を追跡し続けることです。

セッションボーダーコントローラー (SBC、session border controller)

セッションボーダーコントローラー (SBC、session border controller) は、音声ネットワークのエッジに配置され、すべての受発信トラフィック (コントロールプレーンとデータプレーンの両方) を追跡します。SBC の主な役割の 1 つは、音声システムを悪意のある使用から保護することです。SBC は、外部接続用のセッション初期化プロトコル (SIP、Session Initiation Protocol) トランクとの相互接続に使用できます。一部の SBC には、CODEC をある形式から別の形式に変換するためのトランスコーディング機能も用意されています。最後に、ほとんどの SBC は NAT トラバーサル機能も備えており、ファイアウォールで保護されたネットワーク間でも確実にコールが確立されます。

PSTN 接続

ボイスオーバー IP (VoIP、Voice over IP) ソリューションでは、PSTN ゲートウェイと SIP トランクを使用して、レガシー PSTN ネットワークに接続します。

PSTN ゲートウェイ

公衆交換電話網 (PSTN、public switched telephone network) ゲートウェイは、シグナリング (SIP と SS7 間) とメディア (RTP と、CODEC トランスコーディングを使用した時分割多重化 [TDM] 間) を変換します。 PSTN ゲートウェイは、常に PSTN ネットワークに近いエッジに配置されます。

SIP トランク

SIP トランクでは、企業が TDM (SS7 ベース) ネットワークでコールを終端するのではなく、企業と電話会社間のフローが IP 経由で維持されます。ほとんどの SIP トランクは SBC を使用して確立されます。企業は、特定範囲の IP アドレスやポートなど許可など、電話会社の定義済みセキュリティルールに同意する必要があります。

メディアゲートウェイ (トランスコーダー)

一般的な音声ソリューションでは、さまざまなタイプのコーデックを使用できます。一般的なコーデックには、北米向けの G.711 μ-law、北米以外の G.711 A-law、G.729、G.722 などがあります。2 つの異なるコーデックを使用する 2 つのデバイスが互いに通信する場合、メディアサーバーはデバイス間のコーデックフローを変換します。つまり、メディアゲートウェイはメディアを処理し、末端デバイスが相互に通信できるようにします。

WebRTC と WebRTC ゲートウェイ

Web リアルタイム通信 (WebRTC、web real-time communication) を使用すると、API を使用して、Web ブラウザからコールを確立したり、バックエンドサーバーからリソースをリクエストしたりできます。このテクノロジーはクラウドテクノロジーを念頭に置いて設計されているため、コールの確立に使用できるさまざまな API が提供されます。すべての音声ソリューション (SIP を含む) がこれらの API をサポートしているわけではないため、API コールを SIP メッセージに、またはその逆に変換するには、WebRTC ゲートウェイが必要です。

図 2 は、高可用性 WebRTC アーキテクチャの設計パターンを示しています。WebRTC クライアントからの着信トラフィックは、Auto Scaling グループの一部である EC2 インスタンスで実行されている WebRTC を使用して、Amazon Application Load Balancer によって分散されます。

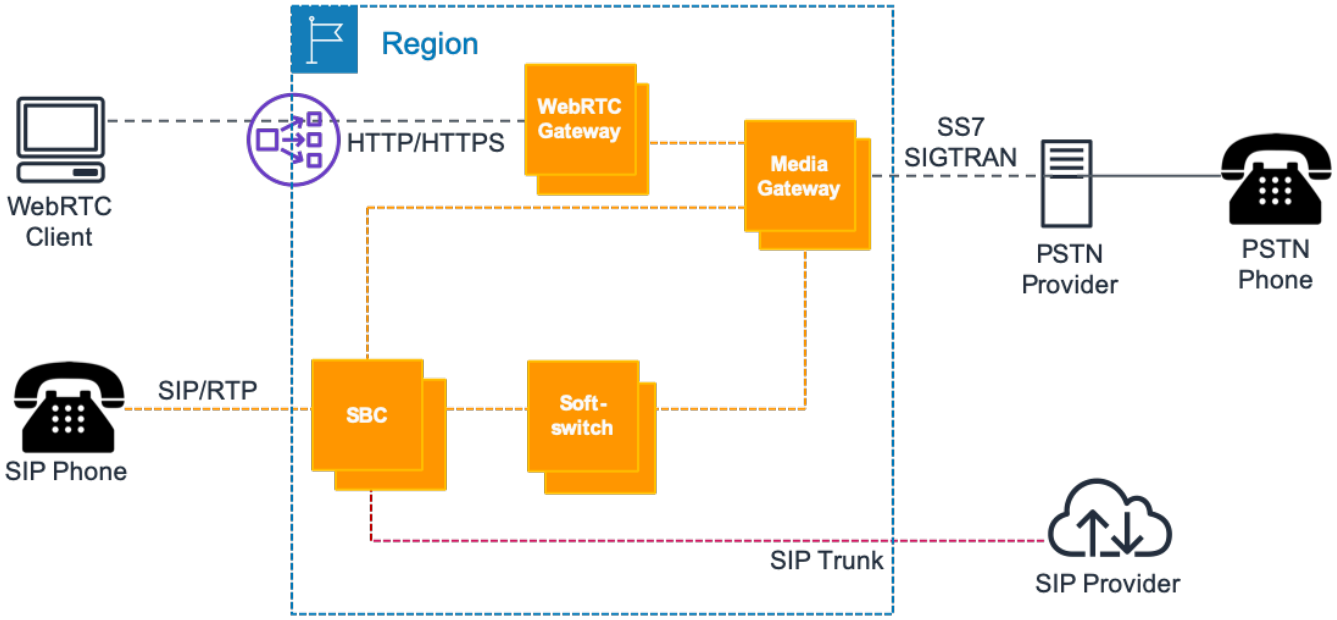

図 2: 音声用の RTC システムの基本トポロジ

SIP および RTP トラフィックのもう 1 つの設計パターンは、アベイラビリティーゾーン全体で、Amazon EC2 で SBC のペアをアクティブパッシブモードで使用することです (図 3)。ここでは、DNS を使用できない障害が発生した場合に、Elastic IP アドレスをインスタンス間で動的に移動できます。

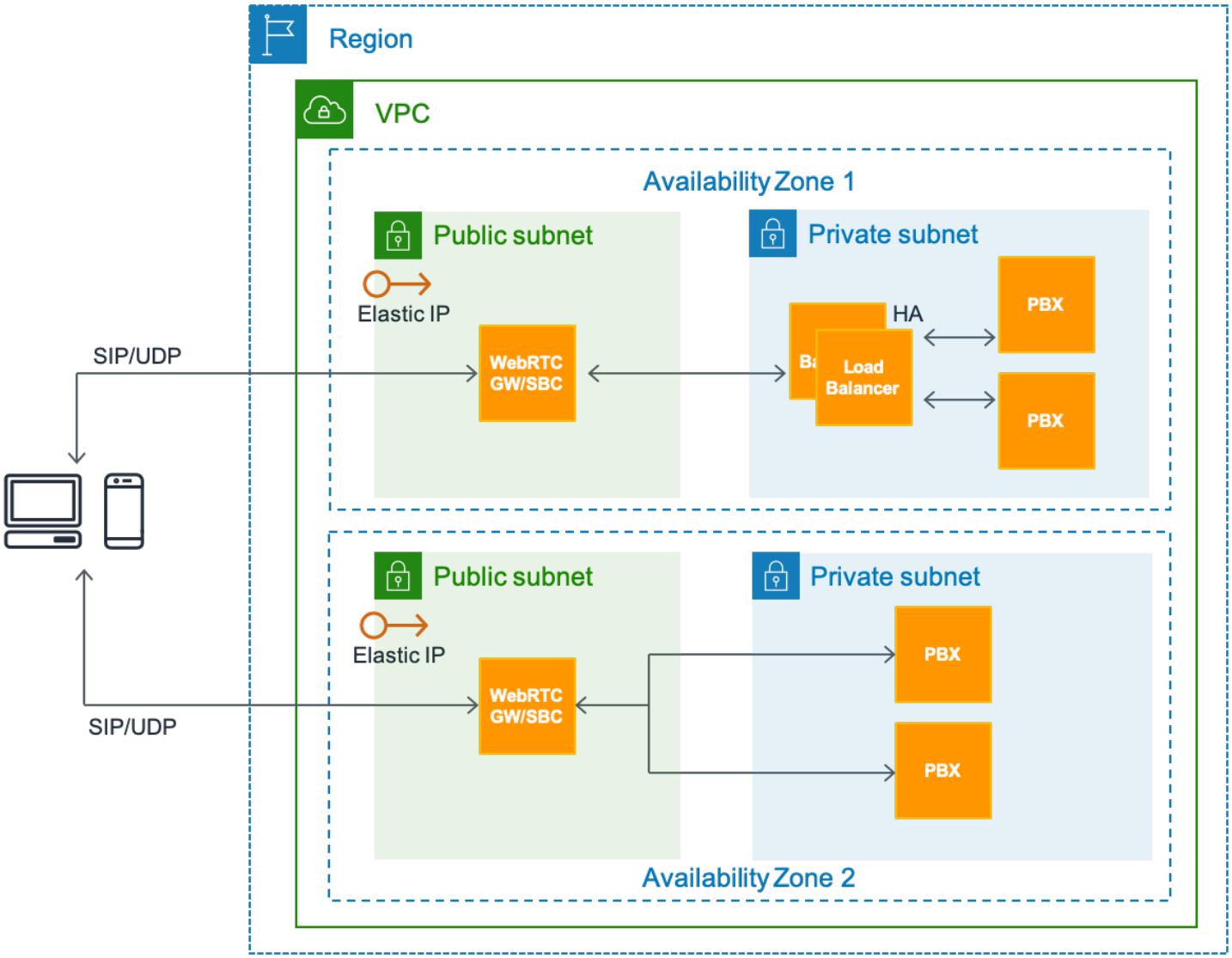

図 3: VPC で Amazon EC2 を使用した RTC アーキテクチャ

AWS での高可用性とスケーラビリティ

リアルタイム通信のほとんどのプロバイダーは、99.9% ~ 99.999% の可用性を提供するサービスレベルに対応しています。必要な高可用性 (HA) の程度によっては、アプリケーションのライフサイクル全体にわたって、ますます高度な対策を講じる必要があります。堅牢な高可用性を実現するには、次のガイドラインに従うことをお勧めします。

- 単一障害点がないようにシステムを設計します。ステートレスコンポーネントとステートフルコンポーネントの両方に対して、自動化されたモニタリング、障害検出、フェイルオーバーのメカニズムを使用します。

- 単一障害点 (SPOF) は、通常 N+1 または 2N 冗長構成によって排除できます。N+1 はアクティブ - アクティブノード間のロードバランシングによって実現され、2N はアクティブ - スタンバイ構成のノードペアによって実現されます。
- AWS には、スケーラブルでロードバランスされたクラスターを使用する方法や、アクティブ - スタンバイペアを想定する方法など、両方のアプローチで HA を実現する方法がいくつかあります。

- システムの可用性を正しく計測し、テストします。
- 障害への対応、軽減、障害からの回復のための手動メカニズムの運用手順を準備します。

このセクションでは、AWS で利用できる機能を使用して単一障害点をなくす方法を取り上げます。具体的には、可用性の高いリアルタイム通信アプリケーションをプラットフォーム上に構築できる AWS のコア機能と設計パターンのサブセットについて説明します。

トピック

- アクティブ - スタンバイステートフルサーバー間の HA のフローティング IP パターン
- WebRTC と SIP によるスケーラビリティと HA のためのロードバランシング
- クロスリージョン DNS ベースのロードバランシングとフェイルオーバー
- 永続的ストレージによるデータの耐久性と高可用性
- AWS Lambda、Amazon Route 53、および AWS Auto Scaling を使用した動的スケーリング
- Kinesis Video Streams を使用した高可用性 WebRTC
- Amazon Chime Voice Connector による高可用性 SIP トランキング

アクティブ - スタンバイステートフルサーバー間の HA のフローティング IP パターン

フローティング IP 設計パターンは、ハードウェアノード (メディアサーバー) のアクティブとスタンバイのペア間で自動フェイルオーバーを実現するメカニズムとしてよく知られています。静的セカンダリ仮想 IP アドレスがアクティブノードに割り当てられます。アクティブノードとスタンバイノード間を継続的にモニタリングすると、障害が検出されます。アクティブノードに障害が発生すると、モニタリングスクリプトによって仮想 IP が ready 状態のスタンバイノードに割り当てられ、スタンバイノードがプライマリアクティブ機能を引き継ぎます。このようにして、仮想 IP はアクティブノードとスタンバイノードの間でフローティングします。

トピック

RTC ソリューションでの適用可能性

N 個のノードで構成されるアクティブ - アクティブクラスターなど、同じコンポーネントの複数のアクティブインスタンスを稼働させることがいつもできるわけではありません。アクティブ - スタンバイ構成は、HA に最適なメカニズムです。例えば、メディアサーバーや会議サーバー、または SBC サーバーやデータベースサーバーなどの RTC ソリューションのステートフルコンポーネントは、アクティブ - スタンバイのセットアップに適しています。SBC またはメディアサーバーでは、一定時間に複数の長時間実行セッションまたはチャネルがアクティブになっています。SBC アクティブインスタンスに障害が発生した場合、フローティング IP のおかげで、エンドポイントはクライアント側の設定なしでスタンバイノードに再接続できます。

AWS での実装

Amazon Elastic Compute Cloud (Amazon EC2)、Amazon EC2 API、Elastic IP アドレスのコア機能、および Amazon EC2 でのセカンダリプライベート IP アドレスのサポートを使用して、このパターンを AWS に実装できます。

1. 2 つの EC2 インスタンスを起動して、プライマリノードとセカンダリノードのロールを引き受けます。この場合、プライマリがデフォルトでアクティブ状態であると想定されます。

2. 追加のセカンダリプライベート IP アドレスをプライマリ EC2 インスタンスに割り当てます。
3. 仮想 IP (VIP) に似た Elastic IP アドレスが、セカンダリプライベートアドレスに関連付けられます。このセカンダリプライベートアドレスは、外部エンドポイントがアプリケーションにアクセスするために使用するアドレスです。
4. セカンダリ IP アドレスをエイリアスとしてプライマリネットワークインターフェイスに追加するには、多少の OS 構成が必要です。
5. アプリケーションはこの Elastic IP アドレスにバインドする必要があります。Asterisk ソフトウェアの場合は、Asterisk SIP の詳細設定でバインディングを設定できます。
6. 各ノードでモニタリングスクリプト (カスタム、Linux では KeepAlive、Corosync など) を実行して、ピアノードの状態をモニターします。現在のアクティブノードに障害が発生した場合、ピアがこの障害を検出し、Amazon EC2 API を呼び出して、セカンダリプライベート IP アドレスを自身に再割り当てします。
7. したがって、セカンダリプライベート IP アドレスに関連付けられた VIP をリッスンしていたアプリケーションは、スタンバイノードを経由してエンドポイントで使用できるようになります。

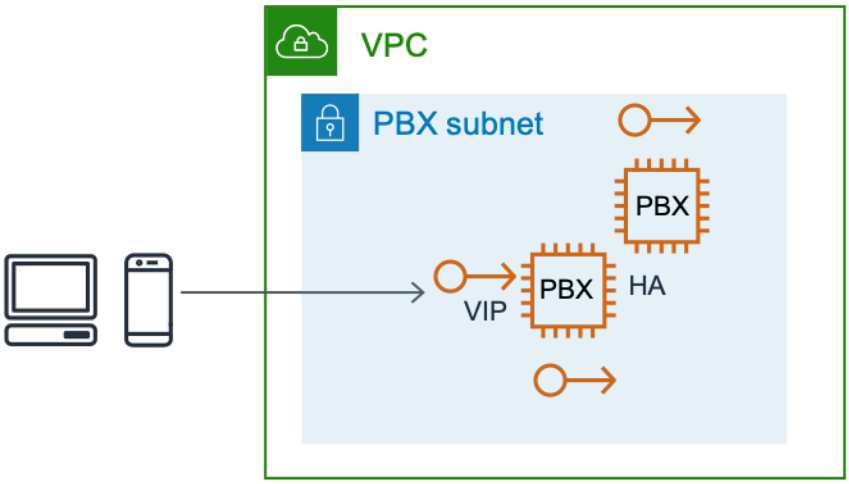

図 4: Elastic IP アドレスを使用したステートフル EC2 インスタンス間のフェイルオーバー

利点

このアプローチは、EC2 インスタンス、インフラストラクチャ、またはアプリケーションレベルでの障害から保護する、信頼性の高い低予算のソリューションです。

制限と拡張性

この設計パターンは通常、1 つのアベイラビリティーゾーン内に限定されます。2 つのアベイラビリティーゾーンにまたがって実装できますが、バリエーションがあります。この場合、利用可能な Elastic IP アドレスの再関連付け API を介して、異なるアベイラビリティーゾーンのアクティブノードとスタンバイノード間でフローティング Elastic IP アドレスが再関連付けされます。図 4 に示すフェイルオーバーの実装では、進行中のコールはドロップされ、エンドポイントは再接続する必要があります。基盤となるセッションデータのレプリケーションによってこの実装を拡張し、セッションのシームレスなフェイルオーバーやメディアの継続性も実現できます。

WebRTC と SIP によるスケーラビリティと HA のためのロードバランシング

ラウンドロビン、アフィニティ、レイテンシーなどの定義済みルールに基づいてアクティブインスタンスのクラスターをロードバランシングする設計パターンは、HTTP リクエストのステートレスな性質によって広く普及しています。実際、RTC アプリケーションコンポーネントが多い場合は、ロードバランシングは実用的な選択肢です。

ロードバランサーは、目的のアプリケーションに対するリクエストのリバースプロキシまたはエントリーポイントとして機能します。ロードバランサー自体は、複数のアクティブノードで同時に実行するように構成されています。ロードバランサーは、任意の時点で、定義されたクラスター内のアクティブノードの 1 つにユーザーリクエストを送信します。ロードバランサーはターゲットクラスター内のノードに対してヘルスチェックを実行し、ヘルスチェックに失敗したノードには受信リクエストを送信しません。したがって、ロードバランシングによって基本的な高可用性が実現されます。また、ロードバランサーは 1 秒未満の間隔ですべてのクラスターノードに対してアクティブおよびパッシブヘルスチェックを実行するため、フェイルオーバーにかかる時間はほぼ瞬時です。

どのノードを指定するかは、ロードバランサーに定義されているシステムルールに基づいて決定されます。これには以下が含まれます。

- ラウンドロビン
- セッションまたは IP アフィニティ。1 つのセッション内または同じ IP からの複数のリクエストが、クラスター内の同じノードに送信されるようにします。
- レイテンシーベース
- ロードベース

トピック

RTC アーキテクチャでの適用可能性

WebRTC プロトコルを使用すると、Elastic Load Balancing、Application Load Balancer、Network Load Balancer などの HTTP ベースのロードバランサーを介して、WebRTC ゲートウェイを簡単にロードバランシングできます。ほとんどの SIP 実装は TCP と UDP の両方での転送に依存しているため、TCP ベースと UDP ベースのトラフィックの両方をサポートするネットワークレベルまたは接続レベルのロードバランシングが必要です。

Application Load Balancer と Auto Scaling を使用した WebRTC の AWS でのロードバランシング

WebRTC ベースの通信の場合、Elastic Load Balancing はフルマネージド型で可用性が高くスケーラブルなロードバランサーを提供し、リクエストのエントリーポイントとして機能します。リクエストは、Elastic Load Balancing に関連付けられた EC2 インスタンスのターゲットクラスターに転送されます。また、WebRTC リクエストはステートレスのため、Amazon EC2 Auto Scaling を使用して、完全に自動化され制御可能なスケーラビリティ、伸縮性、高可用性を実現できます。

Application Load Balancer は、複数のアベイラビリティーゾーンを使用することで可用性が高く、スケーラブルな、フルマネージド型のロードバランシングサービスを提供します。これにより、WebRTC アプリケーションのシグナリングと、長時間実行される TCP 接続を使用するクライアントとサーバー間の双方向通信を処理する、WebSocket リクエストのロードバランシングがサポートされます。Application Load Balancer は、コンテンツベースのルーティングとスティッキーセッションもサポートし、ロードバランサーが生成した Cookie を使用して、同じクライアントからのリクエストを同じターゲットにルーティングします。スティッキーセッションを有効にすると、同一のターゲットでリクエストを受信し、cookie を使用してセッションのコンテキストを復元できます。

図 5 に、ターゲットトポロジを示します。

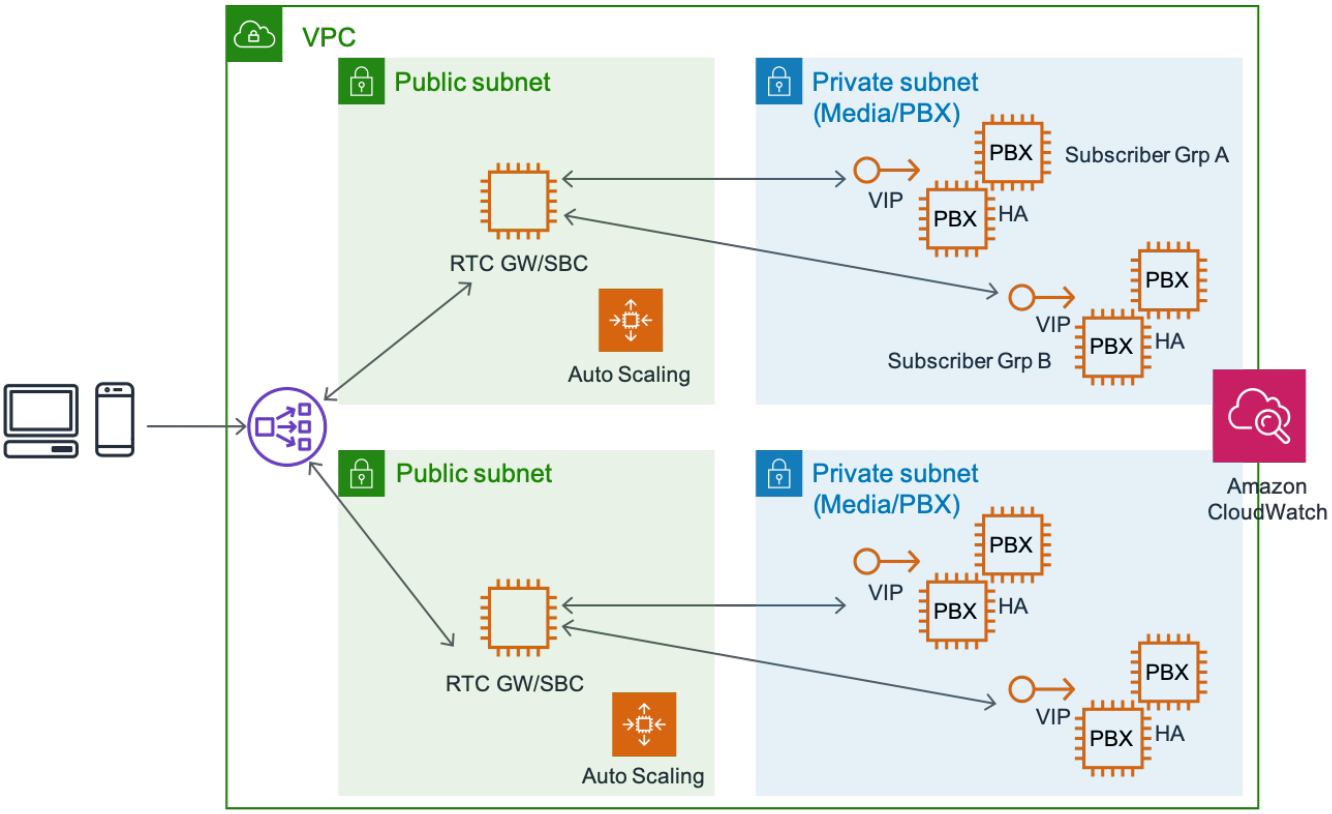

図 5: WebRTC のスケーラビリティと高可用性のアーキテクチャ

Network Load Balancer または AWS Marketplace 製品を使用した SIP の実装

SIP ベースの通信の場合、接続は TCP または UDP を介して行われ、RTC アプリケーションの大半は UDP を使用します。SIP/TCP が信号プロトコルとして選択される場合は、Network Load Balancer を使用し、フルマネージド型で可用性が高く、スケーラブルでパフォーマンスに優れたロードバランシングを実現できます。

Network Load Balancer は接続レベル (レイヤー 4) で動作し、IP プロトコルデータに基づいて Amazon EC2 インスタンス、コンテナ、IP アドレスなどのターゲットに接続をルーティングします。TCP または UDP トラフィックのロードバランシングに最適なネットワークロードバランシングでは、きわめて低いレイテンシーを維持しながら 1 秒間に数百万件ものリクエストを処理できます。このサービスは、AWS Auto Scaling、Amazon Elastic Container Service (Amazon ECS)、Amazon Elastic Kubernetes Service (Amazon EKS)、AWS CloudFormation など、他の人気のある AWS のサービスと統合されています。

SIP 接続が開始された場合は、AWS Marketplace の既製品の商用ソフトウェア (COTS、commercial off-the-shelf software) を使用する方法もあります。AWS Marketplace には、UDP やその他のタイプのレイヤー 4 接続のロードバランシングを処理できる製品が数多く用意されています。これらの COTS には通常、高可用性のサポートが含まれており、AWS Auto Scaling などの機能と統合して可用性とスケーラビリティをさらに強化するのが一般的です。図 6 に、ターゲットトポロジを示します。

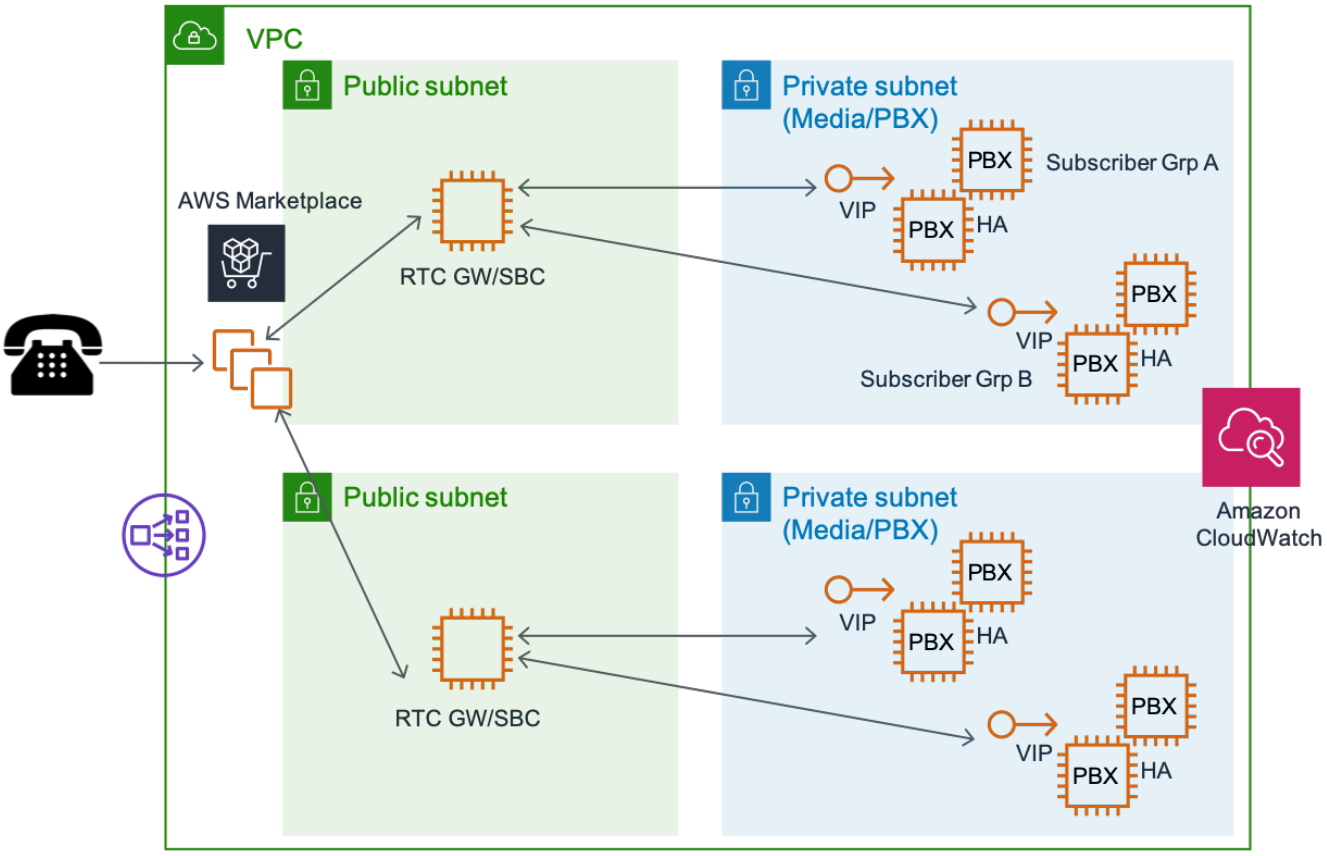

図 6: AWS Marketplace 製品による SIP ベースの RTC スケーラビリティ

クロスリージョン DNS ベースのロードバランシングとフェイルオーバー

Amazon Route 53 は、RTC クライアントがメディアアプリケーションを登録して接続するための、パブリックエンドポイントまたはプライベートエンドポイントとして使用できるグローバル DNS サービスを提供します。Amazon Route 53 では、DNS ヘルスチェックを設定して、トラフィックを正常なエンドポイントにルーティングしたり、アプリケーションの状態を個別にモニターしたりできます。Amazon Route 53 トラフィックフロー機能では、さまざまなルーティングタイプ (レイテンシーベースルーティング、Geo DNS、地理的近接性、加重ラウンドロビンなど) を使用してト

ラフィックをグローバルに簡単に管理できます。このすべてのルーティングタイプを DNS フェイルオーバーと組み合わせることができるため、低レイテンシーのさまざまなフォルトトレラントアーキテクチャを実現できます。Amazon Route 53 トラフィックフローのシンプルなビジュアルエディタを使用して、単一の AWS リージョンに存在するか、世界各地に分散されているかにかかわらず、エンドユーザーをアプリケーションのエンドポイントにルーティングする方法を管理できます。

グローバルデプロイの場合、Route 53 のレイテンシーベースのルーティングポリシーは、リアルタイムのメディア交換に関連するサービス品質を向上させるために、メディアサーバーの最寄りの POP (Point Of Presence) に顧客を誘導するのに特に役立ちます。

新しい DNS アドレスへのフェイルオーバーを強制するには、クライアントキャッシュをフラッシュする必要があることに注意してください。また、DNS の変更はグローバル DNS サーバー全体に伝播されるまで、遅延が発生することがあります。DNS ルックアップの更新間隔は、[Time to Live] 属性で管理できます。この属性は、DNS ポリシーのセットアップ時に構成できます。

グローバルユーザーにすばやく到達したり、単一のパブリック IP を使用する要件を満たすために、AWS Global Accelerator をクロスリージョンフェイルオーバーに使用することもできます。AWS Global Accelerator は、ローカルおよびグローバルに展開するアプリケーションの可用性とパフォーマンスを向上させるネットワーキングサービスです。AWS Global Accelerator は、単一または複数の AWS リージョンにある Application Load Balancer、Network Load Balancer、Amazon EC2 インスタンスなどのアプリケーションエンドポイントへの固定エントリポイントとして機能する静的 IP アドレスを提供します。AWS グローバルネットワークを使用して、ユーザーからアプリケーションへのパスを最適化し、TCP や UDP トラフィックのレイテンシーなどのパフォーマンスを向上させます。AWS Global Accelerator は、アプリケーションエンドポイントの正常性を継続的にモニターし、現在のエンドポイントが異常になった場合、トラフィックを最も近い正常なエンドポイントに自動的にリダイレクトします。追加のセキュリティ要件として、Accelerated Site-to-Site VPN は AWS Global Accelerator を使用し、AWS グローバルネットワークと AWS エッジロケーションを通じてトラフィックをインテリジェントにルーティングすることで、VPN 接続のパフォーマンスを向上させます。

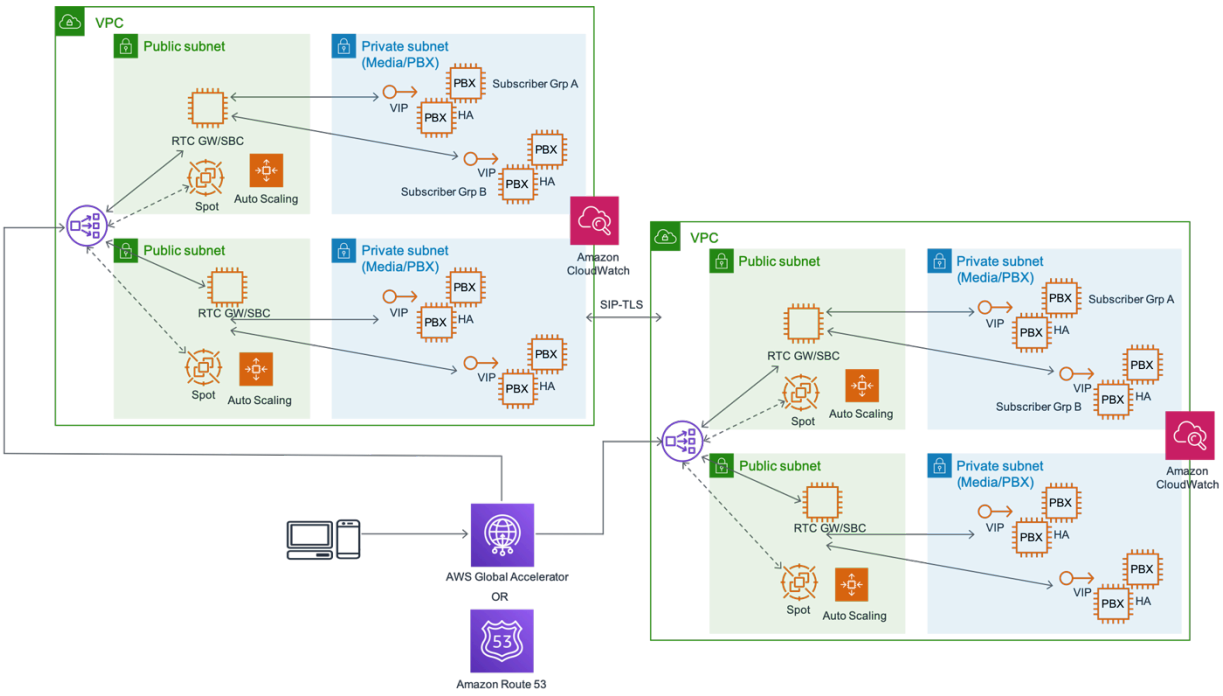

図 7:AWS Global Accelerator または Amazon Route 53 を使用したリージョン間高可用性設計

永続的ストレージによるデータの耐久性と高可用性

ほとんどの RTC アプリケーションは、認証、認可、アカウンティング (セッションデータ、コール詳細レコードなど)、運用モニタリング、ロギングのためのデータの保存とアクセスを、永続的ストレージに依存しています。従来のデータセンターでは、永続的ストレージコンポーネント (データベース、ファイルシステムなど) の高可用性と耐久性を確保するには、通常、SAN、RAID 設計、またバックアップ、リストア、フェイルオーバー処理のプロセスのセットアップによる、多大な労力を要します。AWS クラウドは、データの耐久性と可用性に関する従来のデータセンター実務を大幅に簡素化し、強化します。

オブジェクトストレージとファイルストレージについては、Amazon Simple Storage Service (Amazon S3) や Amazon Elastic File System (Amazon EFS) などの AWS のサービスが、マネージド型の高可用性とスケーラビリティを提供します。Simple Storage Service (Amazon S3) のデータ耐久性は 11 ナインです。

トランザクションデータストレージでは、Amazon Aurora、PostgreSQL、MySQL、MariaDB、Oracle、Microsoft SQL Server を高可用性デプロイでサポートする、フルマネージド型の Amazon Relational Database Service (Amazon RDS) を活用できます。レジストラ機能、サブスクライバープロファイル、またはアカウンティングレコードストレー

ジ (CDR など) ついては、Amazon RDS が耐障害性と高可用性に優れ、スケーラブルなオプションを提供します。

AWS Lambda、Amazon Route 53、および AWS Auto Scaling を使用した動的スケーリング

AWS では、機能の連鎖と、インフラストラクチャイベントに基づくサービスとしてカスタムのサーバーレス関数を組み込むことができます。RTC アプリケーションで多くの用途がある設計パターンの 1 つに、オートスケーリングライフサイクルフックと Amazon CloudWatch Events、Amazon Route 53、AWS Lambda 関数を組み合わせたものがあります。AWS Lambda 関数は、任意のアクションまたはロジックを埋め込むことができます。図 8 は、これらの機能を連鎖させて、オートメーションによってシステムの信頼性とスケーラビリティを向上させる方法を示しています。

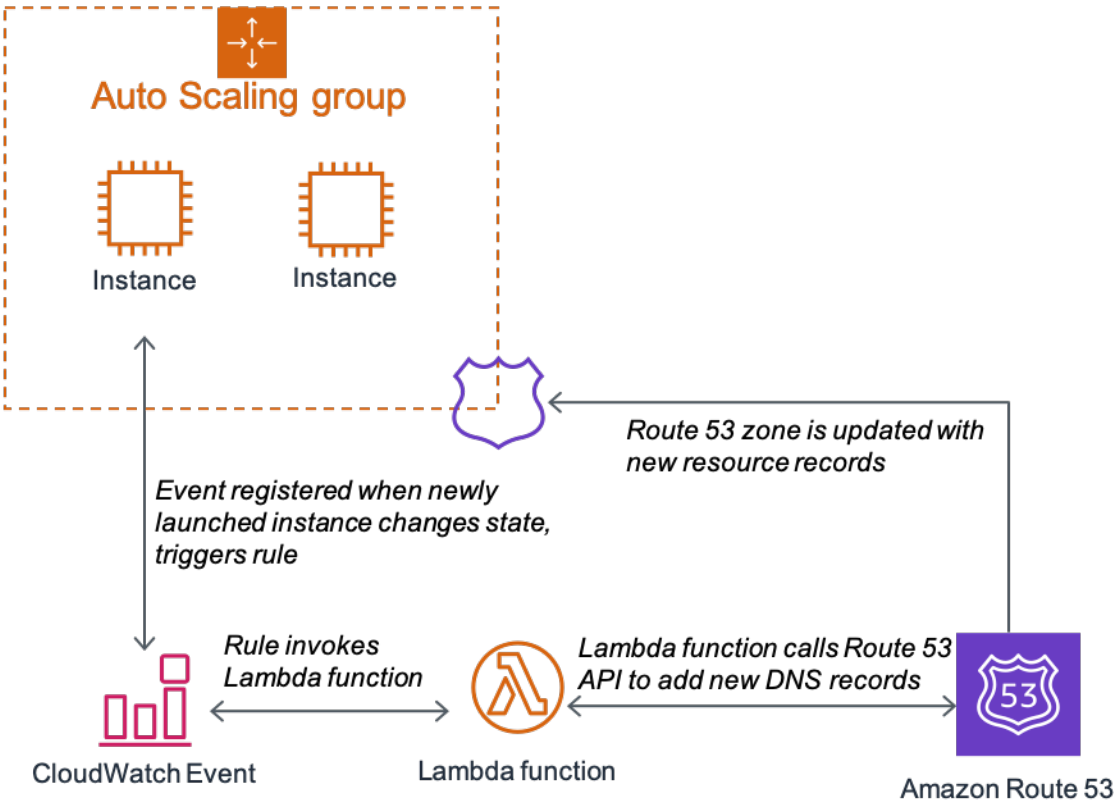

図 8: Amazon Route 53 への動的更新によるオートスケーリング

Kinesis Video Streams を使用した高可用性 WebRTC

Amazon Kinesis Video Streams では、WebRTC を介したリアルタイムのメディアストリーミングが提供され、ユーザーは再生、分析、機械学習のためにメディアストリームをキャプチャ、処理、保

存できます。これらのストリーミングは可用性が高く、スケーラブルで WebRTC 標準に準拠しています。Amazon Kinesis Video Streams には、高速ピア検出と安全な接続の確立のための WebRTC シグナリングエンドポイントが含まれています。マネージド型の Session Traversal Utilities for NAT (STUN) と Traversal Using Relays around NAT (TURN) エンドポイントが含まれ、ピア間でリアルタイムでメディアの交換を行えます。また、カメラファームウェアと直接統合する無料のオープンソース SDK が含まれ、Kinesis Video Streams エンドポイントとの安全な通信を可能にし、ピア検出やメディアストリーミングが行えます。最後に、Kinesis Video Streams は Android、iOS、JavaScript 用のクライアントライブラリを提供します。これにより、WebRTC に準拠したモバイルおよびウェブプレーヤーがメディアストリーミングと双方向通信のためにカメラデバイスを安全に検出して接続できます。

Amazon Chime Voice Connector による高可用性 SIP トランキング

Amazon Chime Voice Connector は従量制料金の SIP トランキングサービスであり、企業はこれを使用することで、従来の電話システムにおいて安全かつ手頃に電話の発信、着信サービスを利用できるようになります。Amazon Chime Voice Connector はサービスプロバイダーの SIP トランクまたは Integrated Services Digital Network (ISDN) Primary Rate Interfaces (PRIs) の低価格な代替手段です。お客様は通話の着信、発信、またはその両方を有効にすることを選択できます。本サービスは複数の AWS リージョン間で、可用性の高い通話体験を提供するために、AWS ネットワークを活用しています。SIP トランキング通話、または転送された SIP ベースのメディアレコーディング (SIPREC) フィードからの音声を Amazon Kinesis Video Streams にストリーミングして、ビジネスコールからリアルタイムでインサイトを得ることができます。Amazon Transcribe やその他の一般的な機械学習ライブラリとの統合により、オーディオ分析用のアプリケーションをすばやく構築できます。

現場のベストプラクティス

このセクションでは、大規模なリアルタイムセッション初期化プロトコル (SIP、Session Initiation Protocol) ワークロードを実行している、大規模かつ最も成功している AWS のお客様の一部が実施してきたベストプラクティスの概要をご紹介します。パブリッククラウドで独自の SIP インフラストラクチャを実行する AWS のお客様は、さまざまな種類の障害が発生した場合のシステムの信頼性と回復力の向上に役立つこれらのベストプラクティスが、有用だとご理解いただけるでしょう。SIP 固有のベストプラクティスの場合もありますが、そのほとんどは AWS で実行されるすべてのリアルタイム通信アプリケーションに適用できます。

トピック

SIP オーバーレイの作成

AWS には、異なるリージョン間の接続を提供する、堅牢でスケーラブル、かつ冗長なネットワークバックボーンがあります。ファイバーカットなどのネットワークイベントによって AWS のバックボーンリンクが低下すると、BGP などネットワークレベルのルーティングプロトコルを使用して、トラフィックが冗長パスにすばやくフェイルオーバーされます。このネットワークレベルのトラフィックエンジニアリングは AWS のお客様にとってはブラックボックスであり、ほとんどのお客様はこのフェイルオーバーイベントに気付いていません。ただし、音声、高画質ビデオ、低レイテンシーメッセージングなどのリアルタイムワークロードを実行しているお客様は、これらのイベントに気付くことがあります。では、AWS のお客様は、ネットワークレベルで AWS が提供するトラフィックエンジニアリングに加えて、どのようにして独自のトラフィックエンジニアリングを実装できるでしょうか。 解決策は、さまざまな AWS リージョンに SIP インフラストラクチャをデプロイすることです。コール制御機能の一部として、SIP は特定の SIP プロキシ経由でコールをルーティングする機能も備えています。

図 9: SIP ルーティングを使用したネットワークルーティングのオーバーライド

図 9 では、SIP インフラストラクチャ (緑の点で表される) が米国の 4 つのリージョンすべてで稼働しています。青い線は、架空の AWS バックボーンを表しています。SIP ルーティングが実装されていない場合、米国西海岸から発信され、米国東海岸を宛先とするコールは、オレゴンとバージニアのリージョンを直接接続しているバックボーンリンクを経由します。この図表は、顧客がネットワークレベルのルーティングをオーバーライドし、オレゴンとバージニア間の同じコールを SIP ルーティングを使用してカリフォルニア経由で発信する方法を示しています。このタイプの SIP トラフィックエンジニアリングは、SIP 再送信や顧客固有のビジネスプリファレンスなどのネットワークメトリクスに基づいて、SIP プロキシとメディアゲートウェイを使用して実装できます。

詳細モニタリングの実行

リアルタイムの音声およびビデオアプリケーションのエンドユーザーは、従来のテレフォニーサービスと同じレベルのパフォーマンスを期待しています。そのため、アプリケーションで問題が発生すると、プロバイダの評判が損なわれることになります。事後対応ではなくプロアクティブにするには、エンドユーザーにサービスを提供するシステムのあらゆる部分に詳細なモニタリングをデプロイすることが不可欠です。

図 10: SIPp を使用した VoIP インフラストラクチャのモニター

iPerf や SIPp、VOIPMonitor など、SIP/RTP トラフィックのモニターに使用できる多くのオープンソースツールが用意されています。前述の例では、クライアントモードとサーバーモードで SIPp を実行しているノードが、米国の 4 つの AWS リージョンすべての間で成功したコールや SIP 再送信などの SIP メトリクスを測定しています。これらのメトリクスは、カスタムスクリプトを使用して Amazon CloudWatch にエクスポートできます。CloudWatch を使用すると、お客様は特定のしきい値に基づいて、これらのカスタムメトリクスに関するアラームを作成できます。その後、これらの CloudWatch アラームの状態に基づいて、自動または手動による修正アクションを実行できます。

カスタムモニタリングシステムの開発と保守に必要なエンジニアリングリソースを割り当てたくないお客様には、ThousandEyes などの優れた VoIP モニタリングソリューションが多く市販されています。修復アクションの例として、SIP 再送信の増加に基づいて SIP ルーティングを変更することが挙げられます。

ロードバランシングに DNS を使用し、フェイルオーバーにフローティング IP を使用する

DNS SRV 機能をサポートする IP テレフォニークライアントは、クライアントをさまざまな SBC/PBX にロードバランシングすることで、インフラストラクチャに組み込まれている冗長性を効率的に使用できます。

図 11: DNS SRV レコードを使用した SIP クライアントのロードバランス

図 11 は、SRV レコードを使用して SIP トラフィックのロードバランスを行う方法を示しています。SRV 標準をサポートする IP テレフォニークライアントは、SRV タイプの DNS レコードで sip._<transport protocol> プレフィックスを検索します。この例では、DNS の回答セクションに、異なる AWS アベイラビリティーゾーンで実行されている PBX が両方とも含まれています。ただし、SRV レコードには、エンドポイント URI に加えて、次の 3 つの追加情報が含まれます。

- 最初の数字は優先度です (上の例では 1)。高い優先度よりも低い優先度が優先されます。
- 2 番目の数値はウェイトです (上の例では 10)。
- 3 番目の数字は使用するポートです (5060)。

両方の PBX サーバーで優先度が同じ (1) であるため、クライアントはウェイトを使用して 2 つの PBX 間のロードバランスを行います。この場合、ウェイトが同じであるため、SIP トラフィックは 2 つの PBX 間で均等にロードバランスされる必要があります。

DNS はクライアントのロードバランシングに適したソリューションですが、DNS の「A」レコードを変更/更新してフェイルオーバーを実装するのはどうでしょうか。 この方法は、クライアントノードと中間ノード内の DNS キャッシュの動作に整合性が取れないため、推奨されません。SIP ノードのクラスター間の AZ 内フェイルオーバーでより効果的なアプローチは、EC2 IP 再割り当てを使用することです。この再割り当てでは、障害のあるホストの IP アドレスが EC2 API を使用して正常なホストに即座に再割り当てされます。詳細なモニタリングとヘルスチェックソリューションを組み合わせることで、障害が発生したノードの IP 再割り当てにより、トラフィックが正常なホストにタイムリーに転送され、エンドユーザーの中断が最小限に抑えられます。

複数のアベイラビリティーゾーンを使用する

各 AWS リージョンは個別のアベイラビリティーゾーンに細分されます。各アベイラビリティーゾーンにはそれぞれ独自の電力、冷却機能、ネットワーク接続があり、隔離された障害ドメインを形成し

ます。AWS の構成では、複数のアベイラビリティーゾーンでワークロードを実行することが常に推奨されています。これにより、お客様のアプリケーションは、アベイラビリティーゾーン全体の障害 (それ自体が非常にまれなイベントですが) にも耐えることができます。この推奨事項は、リアルタイム SIP インフラストラクチャにも当てはまります。

図 12: アベイラビリティーゾーンの障害の処理

壊滅的なイベント (カテゴリ 5 のハリケーンなど) によって、us-east-1 リージョンでアベイラビリティーゾーンが完全に停止したと仮定します。図表に示すようにインフラストラクチャが稼働している状態で、元は障害が発生したアベイラビリティーゾーンのノードに登録されていたすべての SIP クライアントが、アベイラビリティーゾーン #2 で実行されている SIP ノードに再登録されます。(この動作をご使用の SIP クライアント/電話機でテストして、動作がサポートされていることを確認してください)。アベイラビリティーゾーンの停止時にアクティブだった SIP コールは失われますが、新しいコールはすべてアベイラビリティーゾーン #2 を経由してルーティングされます。

要約すると、DNS SRV レコードは、各アベイラビリティーゾーンに 1 つずつ、複数の「A」レコードをクライアントに指定する必要があります。また、これらの「A」レコードはそれぞれ、そのアベイラビリティーゾーン内の SBC/PBX の複数の IP アドレスを指す必要があり、AZ 内および AZ 間両方で復元力を提供します。IP がパブリックの場合、IP 再割り当てを使用することで、AZ 内フェイルオーバーと AZ 間フェイルオーバーの両方を実装できます。ただし、プライベート IP はアベイラビリティーゾーン間で再割り当てできません。お客様がプライベート IP アドレス指定を使用している場合、AZ 間フェイルオーバーでは、バックアップ SBC/PBX に再登録する SIP クライアントに依存せざるを得ない場合があります。す。

1 つのアベイラビリティーゾーン内でトラフィックを維持し、EC2 プレイスメントグループを使用する

このベストプラクティスは、アベイラビリティーゾーンアフィニティとも呼ばれ、これもアベイラビリティーゾーン全体に障害が発生するというまれなイベントにも当てはまります。1 つのアベイラビリティーゾーンに入った SIP または RTP トラフィックが、そのリージョンを出るまでそのアベイラビリティーゾーンに留まるように、クロス AZ トラフィックを排除することをお勧めします。

図 13: アベイラビリティーゾーンアフィニティ (最大で 50% のアクティブコールが失われる)

図 13 は、アベイラビリティーゾーンアフィニティを使用する簡略化されたアーキテクチャを示しています。このアプローチで比較的優位な点は、アベイラビリティーゾーンの完全な停止の影響を考慮

すれば明らかになります。図表に示すように、Availability Zone #2 が失われると、最大でアクティブコールの 50% が影響を受けます (アベイラビリティーゾーン間で均等なロードバランシングを前提とした場合)。アベイラビリティーゾーンアフィニティが実装されていない場合、一部のコールが 1 つのリージョンのアベイラビリティーゾーン間で流れるため、障害が発生するとアクティブなコールの 50% 以上に影響する可能性が高くなります。

さらに、トラフィックのレイテンシーを最小限に抑えるため、各アベイラビリティーゾーン内で EC2 プレイスメントグループの使用を検討することをお勧めします。同じ EC2 プレイスメントグループ内で起動されたインスタンスは、帯域幅が広く、レイテンシーが小さくなります。EC2 では、これらのインスタンスが相互にネットワーク的に近接していることが保証されるためです。

拡張ネットワーキング EC2 インスタンスタイプを使用する

Amazon EC2 で適切なインスタンスタイプを選択すると、システムの信頼性とインフラストラクチャの効率的な使用が保証されます。EC2 は、さまざまなユースケースのために最適化されたインスタンスタイプの幅広い選択肢を提供します。インスタンスタイプは、CPU、メモリ、ストレージ、ネットワーク容量のさまざまな組み合わせで構成されているため、アプリケーションに最適なリソースの組み合わせを柔軟に選択できます。これらの拡張ネットワーキングインスタンスタイプでは、そこで実行されている SIP ワークロードが安定した帯域幅にアクセスでき、総レイテンシーが比較的低くなります。Amazon EC2 に最近追加されたのは、最大 100 Gbps の帯域幅を提供する Elastic Network Adapter (ENA) の可用性です。EC2 インスタンスタイプと関連機能の最新カタログは、EC2 インスタンスタイプのページにあります。

ほとんどのお客様にとって、最新世代のコンピューティング最適化インスタンスは、コストに見合った最高の価値を提供できるはずです。例えば、C5N は、1 秒あたり数百万パケット (PPS) の最大 100 Gbps の帯域幅を持つ新しい Elastic Network Adapter をサポートしています。ほとんどのリアルタイムアプリケーションでも、ネットワークパケット処理を大幅に向上させる インテルデータプレーンデベロッパーキット (DPDK、Data Plane Developer Kit) を使用するとメリットが得られます。

ただし、要件に応じてさまざまな EC2 インスタンスタイプをベンチマークして、どのインスタンスタイプが最適かを確認することが常にベストプラクティスです。ベンチマークでは、特定のインスタンスタイプが一度に処理できるコールの最大数など、他の設定パラメータを見つけることもできます。

セキュリティに関する考慮事項

RTC アプリケーションコンポーネントは通常、インターネットに接続する Amazon EC2 インスタンスで直接実行されます。フローは、TCP に加えて、UDP や SIP などのプロトコルを使用します。このような場合、AWS Shield Standard は UDP リフレクション攻撃、DNS リフレクション、NTP リフレクション、SSDP リフレクションなどの一般的なインフラストラクチャレイヤー (レイヤー 3 および 4) DDoS 攻撃から Amazon EC2 インスタンスを保護します。AWS Shield Standard では、明確に定義された DDoS 攻撃シグニチャが検出されると自動的に使用される優先順位に基づくのトラフィックシェーピングなど、さまざまな手法が使用されます。

また、AWS は Elastic IP アドレスで AWS Shield Advanced を有効にすることで、これらのアプリケーションに対する大規模で高度な DDoS 攻撃に対する高度な保護を提供します。AWS Shield Advanced では、AWS リソースのタイプと EC2 インスタンスのサイズを自動的に検出し、SYN または UDP フラッドに対する保護とともに、事前定義された適切な緩和策を適用する拡張 DDoS 検出を提供します。AWS Shield Advanced を使用すると、お客様は年中無休の AWS DDoS レスポンスチーム (DRT) と協力して、また独自のカスタム緩和ポリシーを作成することもできます。AWS Shield Advanced はまた DDoS 攻撃中に、お客様のすべての Amazon VPC Network アクセスコントロールリスト (ACL) が AWS ネットワークの境界で自動的に強化されて、追加の帯域幅と洗浄キャパシティーにアクセスできるようになり、大容量の DDoS 攻撃を緩和できるようになります。

まとめ

リアルタイム通信 (RTC、real-time communication) ワークロードをアマゾン ウェブ サービス (AWS) にデプロイし、主要な要件を満たしながら、スケーラビリティ、伸縮性、高可用性を実現できます。現在、複数のお客様が、AWS、そのパートナー、およびオープンソースソリューションを使用して、コストの削減、より迅速な俊敏性、グローバルフットプリントの削減を実現しながら RTC ワークロードを稼働させています。

このホワイトペーパーで紹介されているリファレンスアーキテクチャとベストプラクティスは、お客様が AWS で RTC ワークロードを適切にセットアップし、エンドユーザーの要件を満たすようにソリューションを最適化すると同時に、クラウド向けにも最適化するのに役立ちます。

寄稿者

本ドキュメントは、次の人物および組織が寄稿しました。

- アマゾン ウェブ サービス、シニアソリューションアーキテクト、Ahmad Khan
- アマゾン ウェブ サービス、AWS Support、プリンシパルエンジニア、Tipu Qureshi
- アマゾン ウェブ サービス、シニアテクニカルアカウントマネージャー、Hasan Khan
- アマゾン ウェブ サービス、テレコム、WW テクニカルリーダー、Shoma Chakravarty

ドキュメントの改訂

このホワイトペーパーの更新に関する通知を受け取るには、RSS フィードをサブスクライブしてください。

update-history-change	update-history-description	update-history-date
ホワイトペーパーの更新	最新のサービスと機能を反映しました。	2020 年 2 月 13 日
初版公開	ホワイトペーパーの初回公開。	2018 年 10 月 1 日

注意

お客様は、この文書に記載されている情報を独自に評価する責任を負うものとします。本書は、(a) 情報提供のみを目的とし、(b) AWS の現行製品と慣行について説明しており、これらは予告なしに変更されることがあり、(c) AWS およびその関連会社、サプライヤーまたはライセンサーからの契約上の義務や保証をもたらすものではありません。AWS の製品やサービスは、明示または暗示を問わず、一切の保証、表明、条件なしに「現状のまま」提供されます。お客様に対する AWS の責任は、AWS 契約により規定されます。本書は、AWS とお客様の間で締結されるいかなる契約の一部でもなく、その内容を修正するものでもありません。