AWS 白皮书

AWS 上的实时通信

AWS 上的实时通信: AWS 白皮书

Table of Contents

AWS 上的实时通信

在 AWS 上设计高度可用且可扩展的实时通信 (RTC) 工作负载的最佳实践

发布日期：2020 年 2 月 13 日（文档修订）

摘要

如今，许多企业都希望降低成本，并实现实时语音、消息收发和多媒体工作负载的可扩展性。本白皮书概述了在 AWS 上管理实时通信工作负载的最佳实践，并提供了满足这些要求的参考架构。本白皮书为熟悉实时通信的人员提供了有关如何实现这些工作负载的高可用性和可扩展性的指南。

引言

使用语音、视频和消息收发作为渠道的电信应用程序是许多企业及其终端用户的关键需求。这些实时通信 (RTC) 工作负载具有特定的延迟和可用性要求，而企业可以通过遵循相关的设计最佳实践来满足这些要求。过去，RTC 工作负载部署在传统本地数据中心中，并且需要专用资源。

然而，尽管服务级别要求严格，但由于一系列成熟且不断发展的功能陆续推出，RTC 工作负载现在可以部署在 Amazon Web Services (AWS) 上，同时获得可扩展性、弹性和高可用性优势。如今，一些客户正在使用 AWS、其合作伙伴和开源解决方案来运行 RTC 工作负载，他们降低了成本、提高了敏捷性，能够在几分钟内触及全球，并能享受 AWS 服务的丰富功能。

利用 AWS 功能（例如通过 Elastic Network Adapter (ENA) 和最新一代 Amazon Elastic Compute Cloud (EC2) 实例实现增强联网）客户可以使用数据平面开发工具包 (DPDK)、单根 I/O 虚拟化 (SR-IOV)、大页面、NVM Express (NVMe)、非一致性内存访问 (NUMA) 支持以及裸机实例，以满足 RTC 工作负载要求。这些实例提供高达 100 Gbps 的网络带宽和相应的每秒数据包数，为网络密集型应用程序提供更高性能。在扩展方面，Elastic Load Balancing 提供了 Application Load Balancer，它提供 WebSocket 支持和网络负载均衡器，每秒可以处理数百万个请求。在网络加速方面，AWS Global Accelerator 提供了静态 IP 地址，充当 AWS 中应用程序终端节点的固定入口点。它支持负载均衡器的静态 IP 地址。在减少延迟、降低成本和增加带宽吞吐量方面，AWS Direct Connect 可建立从本地部署到 AWS 的专用网络连接。高度可用的托管 SIP 中继由 Amazon Chime Voice Connector 提供。使用 WebRTC 的 Amazon Kinesis Video Streams 可轻松流式传输实时双向媒体，并提供高可用性。

本白皮书包括介绍如何在 AWS 上设置 RTC 工作负载的参考架构，以及在针对云进行优化时，优化解决方案以满足终端用户要求的最佳实践。演进式数据包核心 (EPC) 不在本白皮书的讨论范围内，但可以将本白皮书中详细介绍的最佳实践应用于虚拟网络功能 (VNF)。

RTC 架构的基本组件

在电信行业，实时通信 (RTC) 通常是指两个终端节点之间延迟非常小的实时媒体会话。这些会话可能涉及：

- 双向语音会话（例如，电话系统、移动电话、VoIP）
- 即时消息收发（例如聊天、IRC）
- 实时视频会话（例如视频会议、远程呈现）

上述每种解决方案均有一些共同的组件（例如，提供身份验证、授权和访问控制、转码、缓冲和中继等的组件）和某些特定于所传输媒体类型的组件（例如广播服务、消息收发服务器和队列等）。本节重点介绍如何定义基于语音和基于视频的 RTC 系统以及图 1 中所示的所有相关组件。

图 1：RTC 的基本架构组件

主题

软交换机/PBX

软交换机或 PBX 是语音电话系统的大脑，它通过使用不同的组件为在企业内外建立、维护和路由语音呼叫提供智能支持。企业的所有订户都必须向软交换机注册才能接听或拨打电话。软交换机的一项重要功能是跟踪每个订户以及确定如何使用语音网络中的其他组件联系到他们。

会话边界控制器 (SBC)

会话边界控制器 (SBC) 位于语音网络的边缘，可跟踪所有传入和传出的流量（控制平面和数据平面）。SBC 的主要职责之一是保护语音系统免受恶意使用。SBC 可用于与会话初始协议 (SIP) 中继互连以实现外部连接。某些 SBC 还提供转码功能，用于将 CODEC 从一种格式转换为另一种格式。

最后，大多数 SBC 还提供 NAT 遍历功能，这将有助于确保呼叫得以建立，即使跨防火墙网络也是如此。

PSTN 连接

IP 语音 (VoIP) 解决方案使用 PSTN 网关和 SIP 中继来连接传统 PSTN 网络。

PSTN 网关

公共交换电话网 (PSTN) 网关可转换信令（在 SIP 和 SS7 之间）和媒体（在 RTP 和时分多路复用 [TDM] 之间使用编解码器转码）。 PSTN 网关始终位于靠近 PSTN 网络的边缘。

SIP 中继

在 SIP 中继中，企业不会终止其对 TDM（基于 SS7）网络的呼叫，而是企业和电信公司之间的流量仍然通过 IP 进行。大多数 SIP 中继都是使用 SBC 建立的。企业必须同意来自电信公司的预定义安全规则，例如允许使用一定范围的 IP 地址、端口等。

媒体网关（转码器）

典型的语音解决方案允许使用各种类型的编解码器。一些常见的编解码器为适用于北美地区的 G.711 μ-law、适用于北美地区以外的 G.711 A-law 以及 G.729 和 G.722。当使用两个不同编解码器的两台设备相互通信时，媒体服务器将转换不同设备之间的编解码器流。换句话说，媒体网关会处理媒体并确保终端设备能够相互通信。

WebRTC 和 WebRTC 网关

Web 实时通信 (WebRTC) 允许您从 Web 浏览器建立呼叫或使用 API 从后端服务器请求资源。该技术在设计时考虑了云技术，因此提供了可用于建立呼叫的各种 API。由于并非所有语音解决方案（包括 SIP）均支持这些 API，因此 WebRTC 网关需要将 API 呼叫转换为 SIP 消息，反之亦然。

图 2 显示了高度可用的 WebRTC 架构的设计模式。来自 WebRTC 客户端的传入流量由 Amazon Application Load Balancer 进行均衡，WebRTC 在属于 Auto Scaling 组的 EC2 实例上运行。

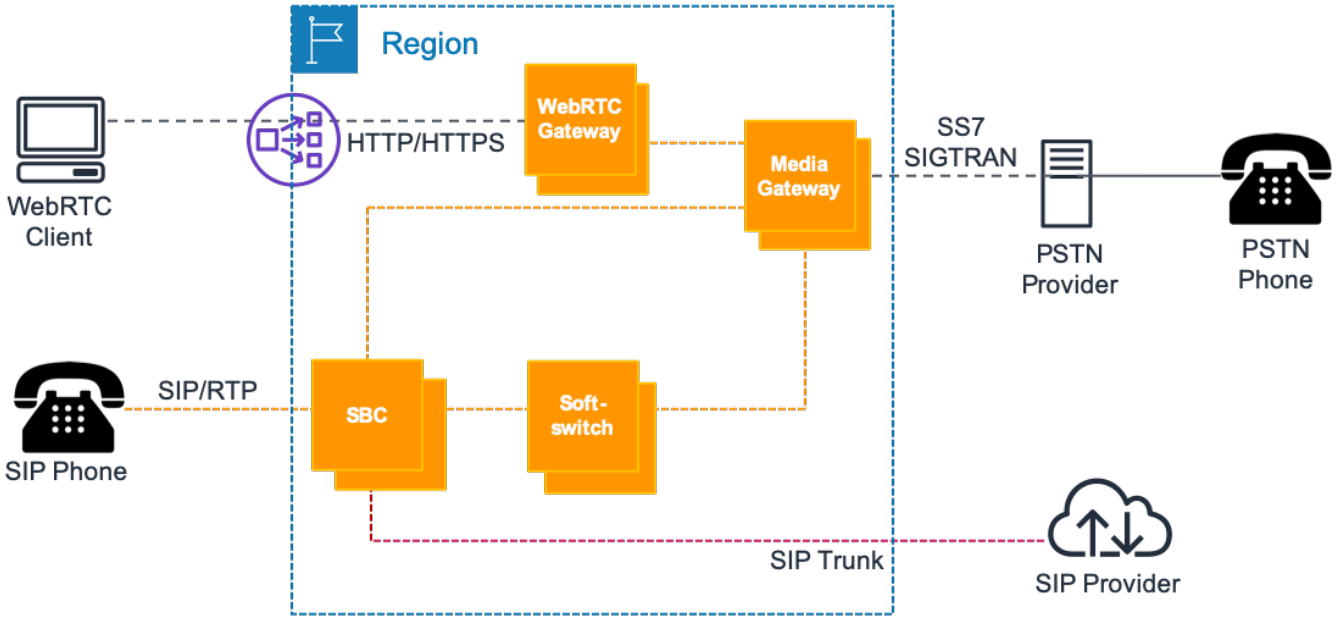

图 2：语音 RTC 系统的基本拓扑结构

SIP 和 RTP 流量的另一种设计模式是在 Amazon EC2 上以主动-被动模式跨可用区使用成对的 SBC（图 3）。在这里，弹性 IP 地址可以在发生无法使用 DNS 的故障时在不同实例之间动态移动。

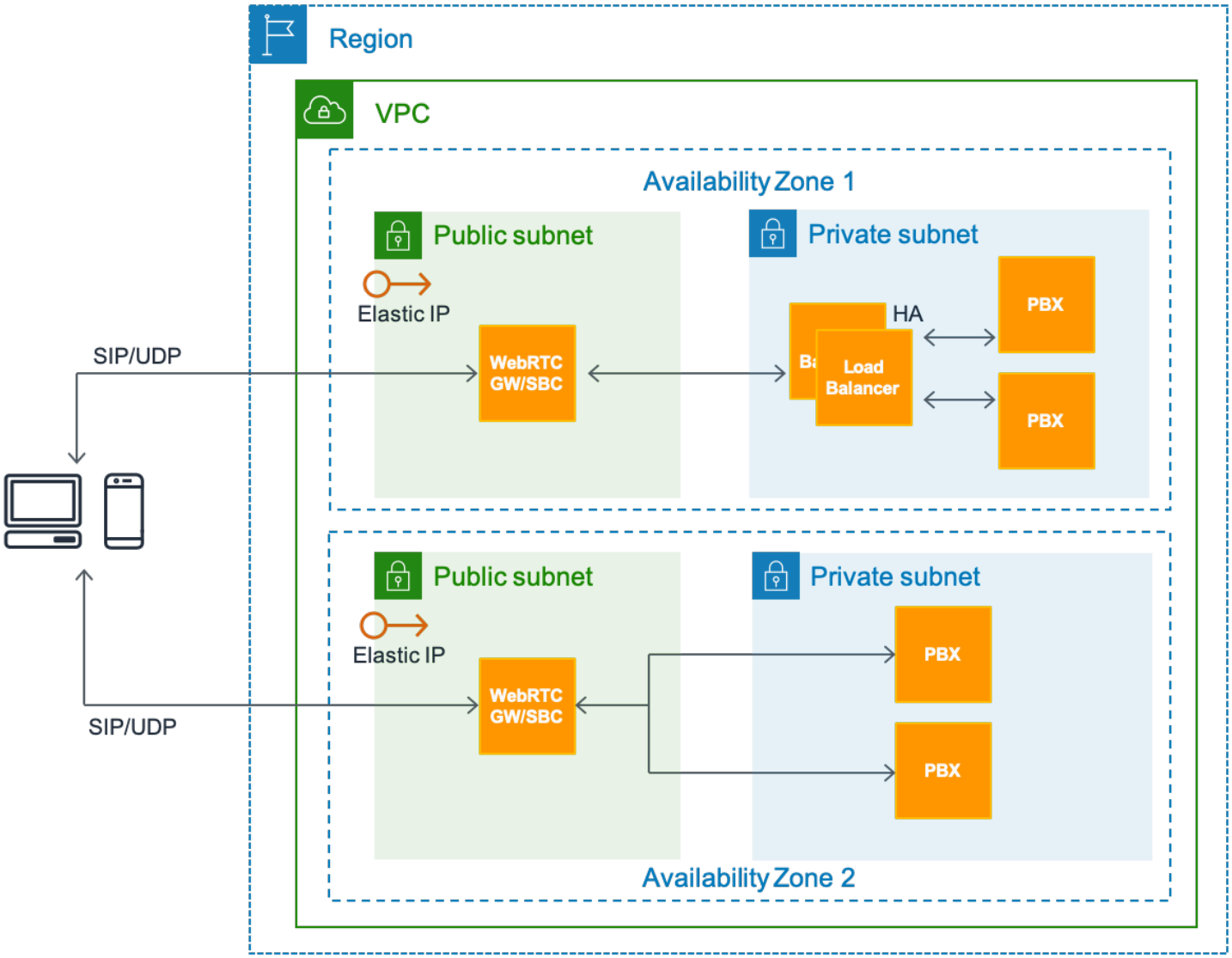

图 3：在 VPC 中使用 Amazon EC2 的 RTC 架构

在 AWS 上实现高可用性和可扩展性

大多数实时通信提供商都可提供可用性为 99.99% 至 99.999% 的服务级别。根据您想要的高可用性 (HA) 级别，您必须在应用程序的整个生命周期中采取日益复杂的措施。我们建议遵循以下准则，以实现稳健的高可用性级别：

- 将系统设计为没有单点故障。对无状态组件和有状态组件使用自动监控、故障检测和故障转移机制

- 通常使用 N+1 或 2N 冗余配置消除单点故障 (SPOF)，其中 N+1 是通过活动-活动节点之间的负载均衡来实现的，而 2N 是通过采用活动-备用配置的一对节点来实现的。
- AWS 有多种方法可以通过这两种方式来实现高可用性，例如通过可扩展、负载均衡的集群或采用活动-备用对。

- 正确检测和测试系统可用性。
- 针对手动机制准备操作流程，以应对、缓解故障并从中恢复。

本节重点介绍如何使用 AWS 上提供的功能实现无单点故障。具体而言，本节介绍了一部分核心 AWS 功能和设计模式，这些功能和模式使您能够在平台上构建高度可用的实时通信应用程序。

主题

浮动 IP 模式可在活动-备用有状态服务器之间实现高可用性

浮动 IP 设计模式是一种众所周知的机制，用于在活动和备用硬件节点对（媒体服务器）之间实现自动故障转移。静态辅助虚拟 IP 地址将分配给活动节点。活动节点和备用节点之间的持续监控可检测故

障。如果活动节点出现故障，监控脚本会将虚拟 IP 分配给就绪备用节点，备用节点将接管主活动节点的功能。这样，虚拟 IP 就会在活动节点和备用节点之间浮动。

主题

RTC 解决方案的适用性

为同一组件配置多个活动实例并不总是可行的，例如有 N 个节点的活动-活动集群。活动-备用配置提供了实现高可用性的最佳机制。例如，RTC 解决方案中的有状态组件（包括媒体服务器或会议服务器，甚至是 SBC 或数据库服务器等）都非常适合活动-备用设置。SBC 或媒体服务器在给定时间具有多个长时间运行的会话或通道处于活动状态，并且在 SBC 活动实例发生故障的情况下，终端节点可以通过浮动 IP 重新连接到备用节点，而无需任何客户端侧配置。

在 AWS 中实施

您可以使用 Amazon Elastic Compute Cloud (Amazon EC2)、Amazon EC2 API、弹性 IP 地址中的核心功能以及 Amazon EC2 上对辅助私有 IP 地址的支持，在 AWS 上实施此模式。

1. 启动两个 EC2 实例以承担主节点和次节点的角色，其中，默认情况下，假定主节点处于活动状态。
2. 为主 EC2 实例分配额外的辅助私有 IP 地址。
3. 弹性 IP 地址（类似于虚拟 IP (VIP)）与辅助私有地址相关联。此辅助私有地址是外部终端节点用来访问应用程序的地址。
4. 要将辅助 IP 地址作为别名添加到主网络接口，需要进行一些操作系统配置。
5. 应用程序必须绑定到此弹性 IP 地址。对于 Asterisk 软件，您可以通过高级 Asterisk SIP 设置来配置绑定。
6. 在每个节点上运行监控脚本（自定义、Linux 上的 KeepAlive、Corosync 等）以监控对等节点的状态。如果当前活动节点发生故障，则对等节点会检测到此故障，并调用 Amazon EC2 API 将辅助私有 IP 地址重新分配给自己。
7. 因此，侦听与辅助私有 IP 地址关联的 VIP 的应用程序可通过备用节点供终端节点使用。

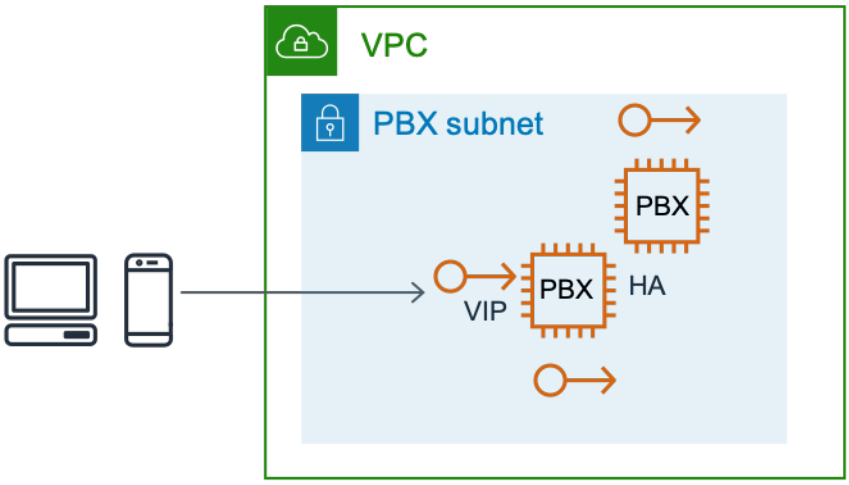

图 4：使用弹性 IP 地址在有状态 EC2 实例之间进行故障转移

优点

这种方法是一种可靠的低预算解决方案，可应对发生在 EC2 实例、基础设施或应用程序级别的故障。

局限性和可扩展性

这种设计模式通常仅限于单个可用区内。它可以跨两个可用区实施，但需要进行一些改动。在这种情况下，浮动弹性 IP 地址将通过重新关联可用的弹性 IP 地址 API，在不同可用区的活动和备用节点之间重新关联。在图 4 中所示的故障转移实施中，正在进行的呼叫中断，终端节点必须重新连接。可以通过复制基础会话数据来扩展此实施，从而提供会话的无缝故障转移或媒体连续性。

通过 WebRTC 和 SIP 进行负载均衡以实现可扩展性和高可用性

基于预定义的规则（例如轮询、亲和性或延迟等）对活动实例集群进行负载均衡，是一种因 HTTP 请求的无状态性而广泛普及的设计模式。实际上，对于许多 RTC 应用程序组件，负载均衡是一个可行的选项。

负载均衡器充当反向代理或入口点来处理所需应用程序的请求，该应用程序本身配置为同时在多个活动节点中运行。在任何给定时间点，负载均衡器都会将用户请求定向到已定义集群中的一个活动节点。负载均衡器对其目标集群中的节点执行运行状况检查，并且不会向未通过运行状况检查的节点发送传入请求。因此，通过负载均衡可以实现基本程度的高可用性。此外，由于负载均衡器在亚秒级时间间隔内对所有集群节点执行主动和被动运行状况检查，因此故障转移的时间是接近实时的。

有关定向到哪个节点的决定基于负载均衡器中定义的系统规则，包括：

- 轮询
- 会话或 IP 关联，可确保同一会话内或来自同一 IP 的多个请求被发送到集群中的同一个节点
- 基于延迟
- 基于负载

主题

RTC 架构的适用性

WebRTC 协议使得 WebRTC 网关可以通过基于 HTTP 的负载均衡器（例如 Elastic Load Balancing、Application Load Balancer 或 Network Load Balancer）轻松实现负载均衡。由于大多数 SIP 实施均依赖于通过 TCP 和 UDP 进行传输，因此需要支持基于 TCP 和 UDP 的流量的网络或连接级别的负载均衡。

使用 Application Load Balancer 和 Auto Scaling 在 AWS 上对 WebRTC 进行负载均衡

对于基于 WebRTC 的通信，Elastic Load Balancing 提供了一个完全托管式、高度可用且可扩展的负载均衡器作为请求的入口点，然后会将请求定向到与 Elastic Load Balancing 关联的 EC2 实例的目标集群。此外，由于 WebRTC 请求是无状态的，因此您可以使用 Amazon EC2 Auto Scaling 来提供完全自动化和可控的可扩展性、弹性和高可用性。

Application Load Balancer 提供完全托管式负载均衡服务，该服务使用多个可用区实现高度可用且可扩展。该工具支持对 WebSocket 请求进行负载均衡，WebSocket 请求可处理 WebRTC 应用程序的信令，以及使用长时间运行的 TCP 连接在客户端和服务器之间进行双向通信。Application Load Balancer 还支持基于内容的路由和粘性会话，从而可使用负载均衡器生成的 Cookie 将来自同一客户端的请求路由到同一目标。如果您启用了粘性会话，则同一目标将接收请求并使用 Cookie 恢复会话上下文。

图 5 显示的是目标拓扑。

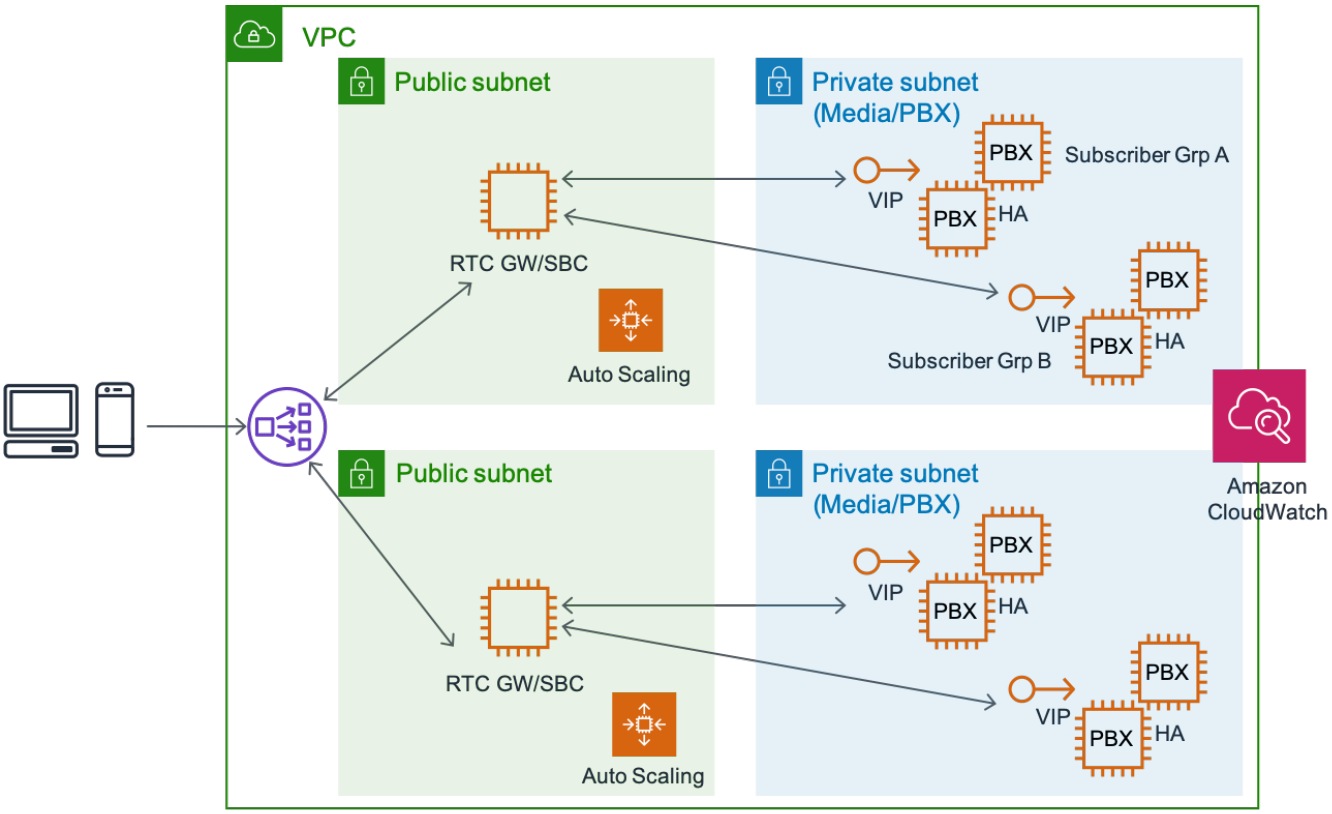

图 5：WebRTC 可扩展性和高可用性架构

使用 Network Load Balancer 或 AWS Marketplace 产品实施 SIP

对于基于 SIP 的通信，连接是通过 TCP 或 UDP 建立的，大多数 RTC 应用程序均使用 UDP。如果 SIP/TCP 为首选信号协议，则使用 Network Load Balancer 实现完全托管式、高度可用、可扩展和高性能负载均衡是可行的。

Network Load Balancer 在连接级别（第 4 层）运行，根据 IP 协议数据将连接路由至目标，例如 Amazon EC2 实例、容器和 IP 地址。网络负载均衡能够在保持超低延迟的同时每秒处理数百万个请求，是进行 TCP 或 UDP 流量负载均衡的理想选择。它与其他常见的 AWS 服务（例如 AWS Auto Scaling、Amazon Elastic Container Service (Amazon ECS)、Amazon Elastic Kubernetes Service (Amazon EKS) 和 AWS CloudFormation）集成。

如果启动了 SIP 连接，则另一种选项是使用 AWS Marketplace 商用现成软件 (COTS)。AWS Marketplace 提供了可以处理 UDP 和其他类型的第 4 层连接负载均衡的许多产品。这些 COTS 通常包括对高可用性的支持，并且通常与 AWS Auto Scaling 等功能集成，以进一步增强可用性和可扩展性。图 6 显示的是目标拓扑：

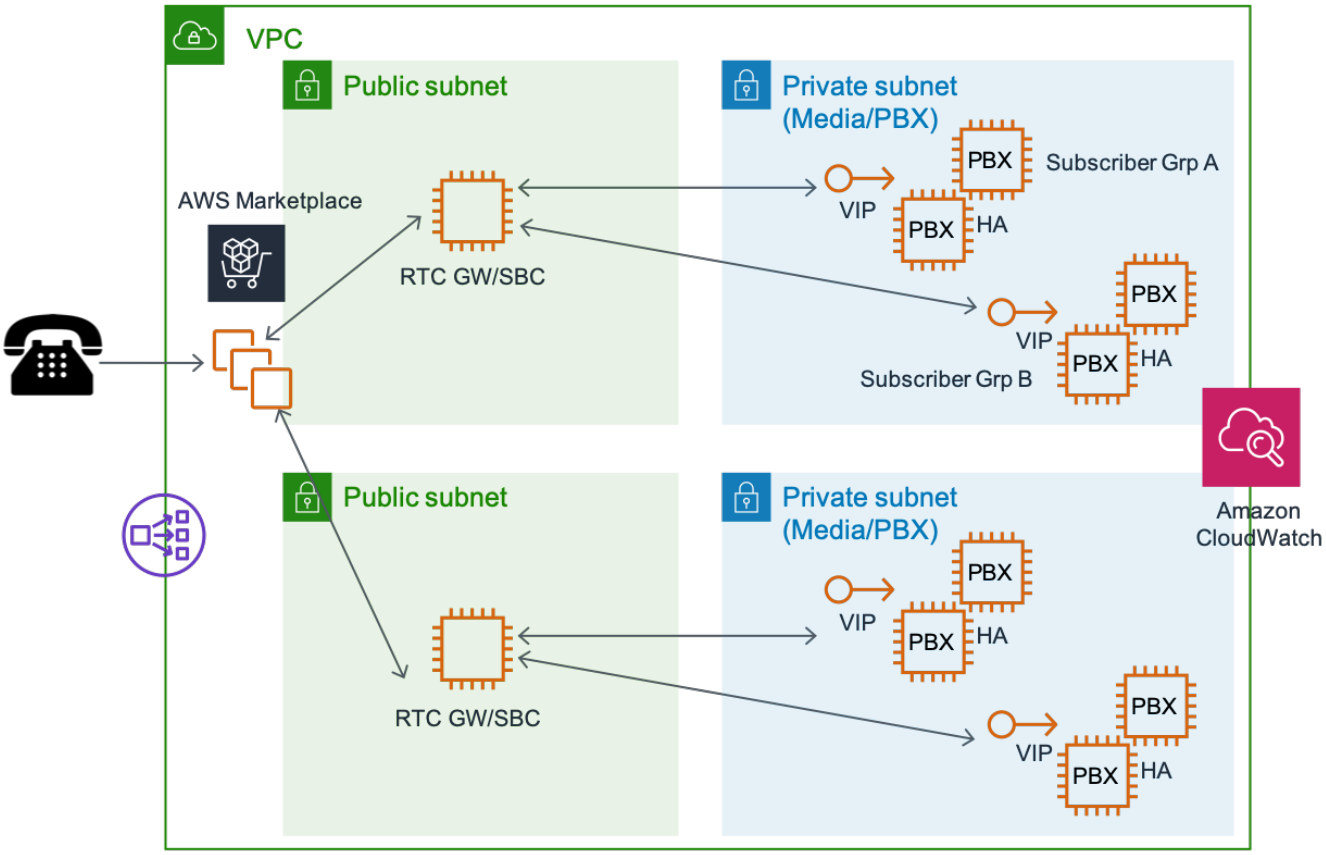

图 6：利用 AWS Marketplace 产品 实现基于 SIP 的 RTC 可扩展性

基于 DNS 的跨区域负载均衡和故障转移

Amazon Route 53 提供的全球性 DNS 服务可用作 RTC 客户端注册和连接媒体应用程序的公有或私有终端节点。借助 Amazon Route 53，可以将 DNS 运行状况检查配置为将流量路由到运行正常的终端节点或独立监控应用程序的运行状况。Amazon Route 53 Traffic Flow 功能让您可以通过多种路由类型（包括基于延迟的路由、Geo DNS、临近地理位置路由和加权轮询）轻松管理全球流量，所有路由类型都可与 DNS 故障转移进行组合，以实现各种低延迟容错架构。借助 Amazon Route 53 Traffic Flow 简洁的可视化编辑器，您可以管理如何将终端用户路由到应用程序的终端节点，不管这些终端节点是在单一 AWS 区域中，还是分布在全球范围内。

对于全球部署，Route 53 中基于延迟的路由策略特别适用于将客户定向到媒体服务器最近的接入点，可提高与实时媒体交流相关的服务质量。

请注意，要强制故障转移到新的 DNS 地址，必须清除客户端缓存。此外，DNS 更改在跨全球 DNS 服务器传播时可能会出现滞后。您可以使用生存时间属性来管理 DNS 查找的刷新间隔。此属性可在设置 DNS 策略时进行配置。

为了快速联系全球用户或满足使用单个公有 IP 的要求，AWS Global Accelerator 还可用于跨区域故障转移。AWS Global Accelerator 是一项网络服务，可提高覆盖本地和全球的应用程序的可用性和性能。AWS Global Accelerator 提供静态 IP 地址，作为应用程序终端节点（如 Application Load Balancer、Network Load Balancer 或单个/多个 AWS 区域中的 Amazon EC2 实例）的固定入口点。它使用 AWS 全球网络来优化从用户到应用程序的路径，从而提高性能，例如 TCP 和 UDP 流量的延迟。AWS Global Accelerator 会持续监控应用程序终端节点的运行状况，并在当前终端节点运行状况不佳时自动将流量重定向到运行状况正常的最近终端节点。为了满足额外的安全要求，Accelerated Site-to-Site VPN 采用 AWS Global Accelerator，通过借助 AWS 全球网络和 AWS 边缘站点智能路由流量来提高 VPN 连接的性能。

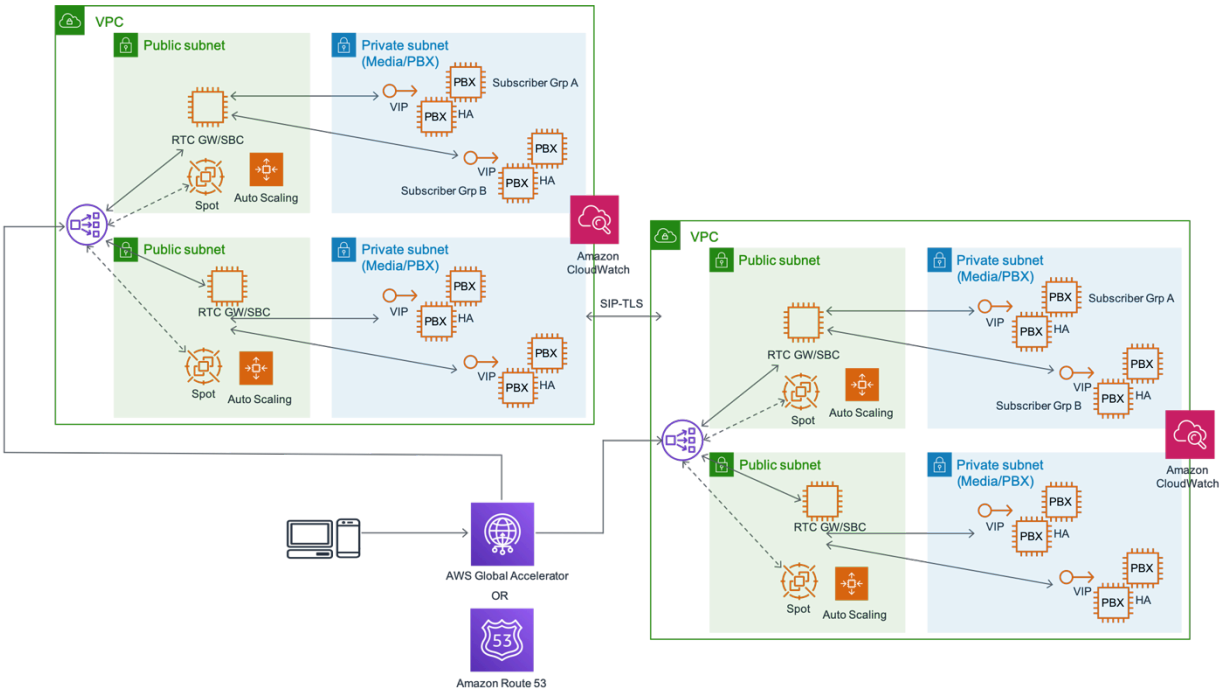

图 7：使用 AWS Global Accelerator 或 Amazon Route 53 进行区域间高可用性设计

通过持久性存储实现数据持久性和高可用性

大多数 RTC 应用程序均依赖于持久性存储来存储和访问用于身份验证、授权、会计（会话数据、呼叫详细记录等）、操作监控和日志记录的数据。在传统的数据中心中，要确保持久性存储组件（数据库、文件系统等）的高可用性和持久性，通常需要构建 SAN、RAID 设计以及备份、还原和故障转移处理流程，这些都是繁重的工作。AWS 云可显著简化并增强围绕数据持久性和可用性的传统数据中心实践。

在对象存储和文件存储方面，Amazon Simple Storage Service (Amazon S3) 和 Amazon Elastic File System (Amazon EFS) 等 AWS 服务可提供托管的高可用性和可扩展性。Amazon S3 的数据持久性为“11 个 9”。

在事务性数据存储方面，客户可以选择利用完全托管式 Amazon Relational Database Service (Amazon RDS)，该服务支持对 Amazon Aurora、PostgreSQL、MySQL、MariaDB、Oracle 以及 Microsoft SQL Server 实现高可用性部署。在注册商功能、订户配置文件或会计记录存储（如 CDR）方面，Amazon RDS 提供了容错、高度可用且可扩展的选项。

利用 AWS Lambda、Amazon Route 53 和 AWS Auto Scaling 实现动态扩展

AWS 允许链接功能，并能够根据基础设施事件将自定义无服务器功能作为服务进行整合。一种在 RTC 应用程序中具有多种用途的此类设计模式是自动扩展生命周期钩子与 Amazon CloudWatch Events、Amazon Route 53 和 AWS Lambda 功能的组合。AWS Lambda 功能可嵌入任何操作或逻辑。图 8 演示了将这些功能链接在一起如何能够通过自动化技术增强系统的可靠性和可扩展性。

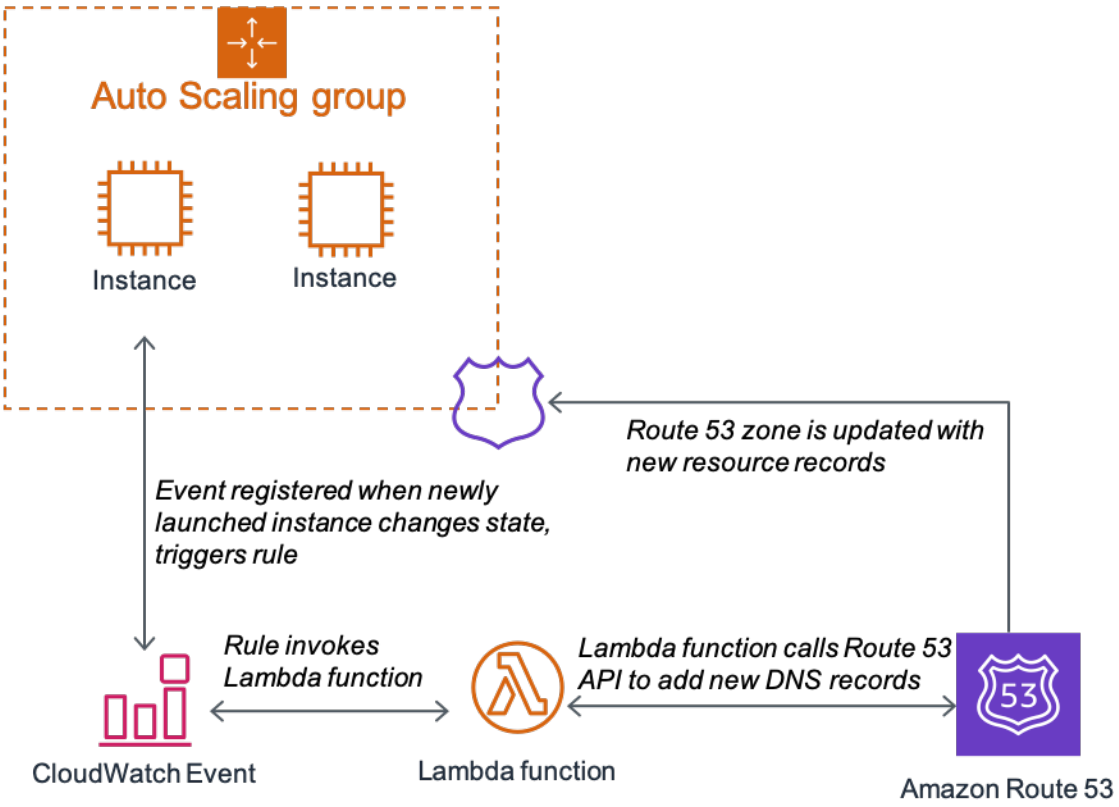

图 8：通过对 Amazon Route 53 的动态更新实现自动扩展

借助 Kinesis Video Streams 实现高度可用的 WebRTC

Amazon Kinesis Video Streams 通过 WebRTC 提供实时媒体流式传输，允许用户捕获、处理和存储媒体流，以用于播放、分析和机器学习。这些流具有高可用性、可扩展性并且符合 WebRTC 标

准。Amazon Kinesis Video Streams 包含一个 WebRTC 信令终端节点，用于快速发现对等节点和建立安全连接。它包括托管的 Session Traversal Utilities for NAT (STUN) 和 Traversal Using Relays around NAT (TURN) 端点，用于在对等节点之间实时交换媒体。它还包括一个免费的开源开发工具包，该开发工具包直接与摄像头固件集成，以实现与 Kinesis Video Streams 端点的安全通信，允许进行对等节点发现和媒体流传输。最后，它还提供了适用于 Android、iOS 和 JavaScript 的客户端库，这些客户端库使符合 WebRTC 的移动和网络播放器可以安全地发现摄像头设备并与这些设备连接，以进行媒体流式传输和双向通信。

利用 Amazon Chime Voice Connector 实现高可用性 SIP 中继

Amazon Chime Voice Connector 可提供随用随付的 SIP 中继服务，使公司可以通过其电话系统拨打和/或接听电话，既安全又便宜。Amazon Chime Voice Connector 是服务提供商 SIP 中继或综合业务数字网 (ISDN) 基群速率接口 (PRI) 的低成本替代方案。客户可以选择启用入站呼叫、出站呼叫，或启用两者。该服务利用 AWS 网络在多个 AWS 区域之间打造高度可用的通话体验。您可以将来自 SIP 中继电话呼叫的音频或基于 SIP 的转发媒体录制内容 (SIPREC) 源流式传输到 Amazon Kinesis Video Streams，以便从业务呼叫中实时获得洞察力。通过与 Amazon Transcribe 和其他常用机器学习库集成，您可以快速构建用于音频分析的应用程序。

现场最佳实践

本节旨在汇总一些运行大型实时会话初始协议 (SIP) 工作负载的最大、最成功的 AWS 客户所实施的最佳实践。希望在公有云中运行自己的 SIP 基础设施的 AWS 客户会发现这些最佳实践很有价值，因为它们可以帮助提高系统的可靠性和恢复能力，以防出现各种不同的故障。尽管其中一些最佳实践是特定于 SIP 的，但大多数最佳实践适用于在 AWS 上运行的任何实时通信应用程序。

主题

创建 SIP 叠加

AWS 拥有强大、可扩展且冗余的骨干网络，可在不同区域之间提供连接。当网络事件（如光纤切断）降级 AWS 骨干网络链路时，流量将通过网络级路由协议（如 BGP）迅速故障转移至冗余路径。对 AWS 客户来说，这种网络级流量工程可谓是“暗箱操作”，大多数客户甚至都不会注意到这些故障转移事件。但是，运行实时工作负载（例如语音、高质量视频和低延迟消息收发）的客户有时确实会注意到这些事件。那么，AWS 客户如何在网络级别由 AWS 提供的服务之上实施自己的流量工程呢？ 解决方案是在许多不同的 AWS 区域部署 SIP 基础设施。作为呼叫控制功能的一部分，SIP 还提供通过特定 SIP 代理路由呼叫的功能。

图 9：使用 SIP 路由覆盖网络路由

在图 9 中，SIP 基础设施（用绿点表示）在所有四个美国区域运行。蓝线表示 AWS 骨干网络。如果未实施 SIP 路由，则从美国西海岸传输到美国东海岸的呼叫走的是直接连接俄勒冈和弗吉尼亚区域的骨干网络链路。该图显示了客户可如何覆盖网络级路由，转而使用 SIP 路由，经由加利福尼亚州传输俄勒冈州和弗吉尼亚州之间的相同呼叫。可以使用 SIP 代理和媒体网关基于网络指标（如 SIP 重新传输和客户特定的业务偏好）来实现这种类型的 SIP 流量工程。

执行详细监控

实时语音和视频应用程序的终端用户期望获得与传统电话服务相同的性能水平。因此，当他们遇到应用程序问题时，最终会损害提供商的声誉。要积极主动而不是被动应对，就必须在为终端用户提供服务的系统的每个部分部署详细监控。

图 10：使用 SIPp 监控 VoIP 基础设施

许多开源工具（例如 iPerf 或 SIPp 和 VOIPMonitor）都可用于监控 SIP/RTP 流量。在前面的示例中，在客户端和服务器模式下运行 SIPp 的节点测量所有四个美国 AWS 区域之间的 SIP 指标，例如成功呼叫和 SIP 重新传输数量。然后，可以使用自定义脚本将这些指标导出到 Amazon CloudWatch。使用 CloudWatch，客户可以基于特定阈值针对这些自定义指标创建警报。然后，可以基于这些 CloudWatch 警报的状态执行自动或手动修正操作。

对于不想分配开发和维护自定义监控系统所需的工程资源的客户，市场上有许多良好的 VoIP 监控解决方案，例如 ThousandEyes。修正操作的一个示例是基于增加的 SIP 重新传输来更改 SIP 路由。

使用 DNS 进行负载均衡，使用浮动 IP 进行故障转移

支持 DNS SRV 功能的 IP 电话客户端可以通过对客户端进行负载均衡，将其分布到不同的 SBC/PBX 来高效地使用基础设施中内置的冗余。

图 11：使用 DNS SRV 记录对 SIP 客户端进行负载均衡

图 11 显示了客户可如何使用 SRV 记录对 SIP 流量进行负载均衡。任何支持 SRV 标准的 IP 电话客户端都将在 SRV 类型的 DNS 记录中查找 sip._<transport protocol> 前缀。在该示例中，来自 DNS 的应答部分包含在不同 AWS 可用区中运行的两个 PBX。但是，除了终端节点 URI 之外，SRV 记录还包含三条附加信息：

- 第一个数字为优先级（上例中为 1）。数字小的优先级优先于数字大的优先级。
- 第二个数字为权重（上例中为 10）。
- 第三个数字为要使用的端口 (5060)。

由于两个 PBX 服务器的优先级相同（都是 1），因此客户端使用权重在两个 PBX 之间进行负载均衡。在这种情况下，由于权重相同，因此在两个 PBX 之间对 SIP 流量进行负载均衡时应该平均分布。

DNS 可能是实现客户端负载均衡的一个良好解决方案，但是能否通过更改/更新 DNS“A”记录来实现故障转移呢？ 不建议采用此方法，因为在客户端和中间节点内的 DNS 缓存行为中发现不一致性。在集群的 SIP 节点之间进行 AZ 内部故障转移的更好方法是使用 EC2 IP 重新分配，在此情况下，通过使用 EC2 API 将受损主机的 IP 地址立即重新分配给正常运行的主机。故障节点的 IP 重新分配与详细监控和运行状况检查解决方案配合使用，可确保流量及时转移到正常运行的主机，从而最大限度地减少对终端用户的干扰。

使用多个可用区

每个 AWS 区域都被细分为单独的可用区。每个可用区都有自己的电源、冷却和网络连接，因此构成一个隔离的故障域。在 AWS 系统中，始终鼓励客户在多个可用区中运行其工作负载。这样可确保客户应用程序甚至可以承受整个可用区出现故障，这本身就是一种非常罕见的事件。此建议也适用于实时 SIP 基础设施。

图 12：处理可用区故障

假设灾难性事件（比如五级飓风）会导致美国东部 1 区域中的可用区完全中断。对于按图中所示运行的基础设施，最初注册到故障可用区中节点的所有 SIP 客户端都应向在可用区 2 中运行的 SIP 节点重新注册。（使用您的 SIP 客户端/电话测试此行为以确保它受支持。）尽管在可用区中断时，活动 SIP 呼叫会丢失，但任何新呼叫都会通过可用区 2 进行路由。

总而言之，DNS SRV 记录应将客户端指向多条“A”记录，其中每个可用区中均有一条记录。而这些“A”记录中的每一条都应指向该可用区中 SBC/PBX 的多个 IP 地址，从而提供 AZ 内和 AZ 间的恢复能力。如果 IP 为公有 IP，则 AZ 内和 AZ 间的故障转移均可通过使用 IP 重新分配来实现。但是，私有 IP 不能跨可用区重新分配。如果客户使用私有 IP 地址，则他们必须依靠向备份 SBC/PBX 重新注册的 SIP 客户端进行 AZ 间故障转移。

将流量保持在一个可用区内并使用 EC2 置放群组

这种最佳实践又称为可用区关联，也适用于整个可用区出现故障的罕见情况。建议您消除任何跨可用区流量，以便进入一个可用区的任何 SIP 或 RTP 流量在退出该区域之前都应保留在该可用区内。

图 13：可用区关联（最多有 50% 的活动呼叫丢失）

图 13 显示了使用可用区关联的简化架构。如果考虑到整个可用区完全中断的影响，则这种方法的相对优势就显而易见了。如图所示，如果可用区 2 出现中断，则最多有 50% 的活动呼叫会受到影响（假设

不同可用区之间的负载均衡相等）。如果未实施可用区关联，则某些呼叫将在一个区域中的可用区之间流动，而故障很可能会影响 50% 以上的活动呼叫。

此外，为了最大限度减少流量延迟，还建议您考虑在每个可用区内使用 EC2 置放群组。在同一 EC2 置放群组中启动的实例具有更高的带宽和更低的延迟，因为 EC2 可确保这些实例彼此之间的网络邻近。

使用增强联网 EC2 实例类型

在 Amazon EC2 上选择正确的实例类型可确保系统可靠性以及基础设施的高效使用。EC2 提供多种经过优化、适用于不同用例的实例类型以供选择。实例类型由 CPU、内存、存储和网络容量组成不同的组合，可让您灵活地为您的应用程序选择适当的资源组合。这些增强型联网实例类型可确保在其上运行的 SIP 工作负载能够访问一致的带宽，并实现相对较低的总延迟。Amazon EC2 最近新增的一项功能是弹性网络适配器 (ENA)，该适配器可提供高达 100 Gbps 的带宽。EC2 实例类型和相关功能的最新目录可在 EC2 实例类型页面上找到。

对于大多数客户而言，最新一代的计算优化型实例应能提供最佳成本效益。例如，C5N 支持带宽高达 100 Gbps 的全新弹性网络适配器，每秒数据包处理量 (PPS) 达数百万。大多数实时应用程序还将受益于使用英特尔数据平面开发工具包 (DPDK)，它可以显著提高网络数据包处理能力。

但是，最佳实践始终是根据您的要求对各种 EC2 实例类型进行基准测试，以了解哪种实例类型最适合您。基准测试还使您能够了解其他配置参数，例如特定实例类型一次可处理的最多呼叫次数。

安全考虑因素

RTC 应用程序组件通常直接在面向 Internet 的 Amazon EC2 实例上运行。除了 TCP 之外，流还使用 UDP 和 SIP 等协议。在这些情况下，AWS Shield Standard 可保护 Amazon EC2 实例免受常见基础设施层（第 3 层和第 4 层）的 DDoS 攻击，例如 UDP 反射、DNS 反射、NTP 反射、SSDP 反射等攻击。AWS Shield Standard 使用多种技术（例如基于优先级的流量整形）应对攻击，并且，当检测到定义明确的 DDoS 攻击特征时会自动使用这些技术。

AWS 还通过在弹性 IP 地址上启用 AWS Shield Advanced，为这些应用程序提供针对大型复杂 DDoS 攻击的高级保护。AWS Shield Advanced 提供了增强的 DDoS 检测功能，可自动检测 AWS 资源的类型和 EC2 实例的大小，并应用适当的预定义缓解措施，防止 SYN 或 UDP 泛洪。借助 AWS Shield Advanced，客户还可以通过与全天候的 AWS DDoS 响应团队 (DRT) 联系，来创建自己的自定义缓解配置文件。AWS Shield Advanced 还可确保在 DDoS 攻击期间，您的所有 Amazon VPC 网络访问控制列表 (ACL) 都会在 AWS 网络边界自动执行，从而使您能够访问额外的带宽并清理容量，以缓解大规模的 DDoS 攻击。

总结

可以将实时通信 (RTC) 工作负载部署在 Amazon Web Services (AWS) 上，以实现可扩展性、弹性和高可用性，同时满足关键要求。如今，一些客户正在使用 AWS、其合作伙伴和开源解决方案来运行 RTC 工作负载，他们降低了成本、提高了敏捷性，同时减少了全球足迹。

本白皮书中提供的参考架构和最佳实践可以帮助客户在 AWS 上成功设置 RTC 工作负载并优化解决方案以满足终端用户的需求，同时针对云进行优化。

贡献者

以下是对本文做出贡献的个人和组织：

- Ahmad Khan，Amazon Web Services 高级解决方案构架师
- Tipu Qureshi，Amazon Web Services AWS Support 首席工程师
- Hasan Khan，Amazon Web Services 高级技术客户经理
- Shoma Chakravarty，Amazon Web Services 电信部门全球技术负责人

文档修订

要获得有关此白皮书的更新通知，请订阅 RSS 源。

更新-历史记录-更改	更新-历史记录-描述	更新-历史记录-日期
已更新白皮书	已更新最新服务和功能。	2020 年 2 月 13 日
初次发布	首次发布白皮书。	2018 年 10 月 1 日

声明

客户负责对本文档中的信息进行独立评估判断。本文档：(a) 仅供参考；(b) 代表当前提供的 AWS 产品和实践，如有更改，恕不另行通知；并且 (c) AWS 及其附属机构、供应商或许可方不做任何承诺或保证。AWS 产品或服务“按原样”提供，不提供任何形式的保证、陈述或条件，无论是明示还是暗示。AWS 对其客户的责任和义务由 AWS 协议决定，本文档与 AWS 和客户之间签订的任何协议无关，亦不影响任何此类协议。