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

开启实时通信 AWS

在上设计高度可用和可扩展的实时通信 (RTC) 工作负载的最佳实践 AWS

发布日期：2022年5月5日 (文档修订)

摘要

如今，许多组织都在寻求降低成本并实现实时语音、消息和多媒体工作负载的可扩展性。本白皮书概述了在 Amazon Web Services () 上管理实时通信 (RTC AWS) 工作负载的最佳实践，并包括满足这些要求的参考架构。本 paper 可为熟悉实时通信的人员提供指导，指导他们如何实现这些工作负载的高可用性和可扩展性。

本 paper 包括展示如何设置 RTC 工作负载的参考架构 AWS，以及优化解决方案以满足最终用户要求的最佳实践，同时针对云进行优化。Evolved Packet Core (EPC) 超出了本白皮书的范围，但此处详细介绍的最佳实践可以应用于虚拟网络功能 () VNFs。

您的架构是否良好？

当您在云端构建系统时，AWS Well-Architected Framework 可助您了解所作决策的利弊。利用此框架的六个支柱，您可以了解到设计和运行可靠、安全、高效、经济有效且可持续的系统的架构最佳实践。使用 AWS 管理控制台（需要登录）中免费提供的，您可以通过回答每个支柱的一组问题，根据这些最佳实践来查看您的工作负载。AWS Well-Architected Tool

有关云架构的更多专家指导和最佳实践（参考架构部署、图表和白皮书），请参阅 AWS 架构中心。

简介

使用语音、视频和消息传递作为渠道的电信应用程序是许多组织及其最终用户的关键要求。这些实时通信 (RTC) 工作负载具有特定的延迟和可用性要求，可以通过遵循相关的设计最佳实践来满足。过去，RTC 工作负载部署在具有专用资源的传统本地数据中心中。

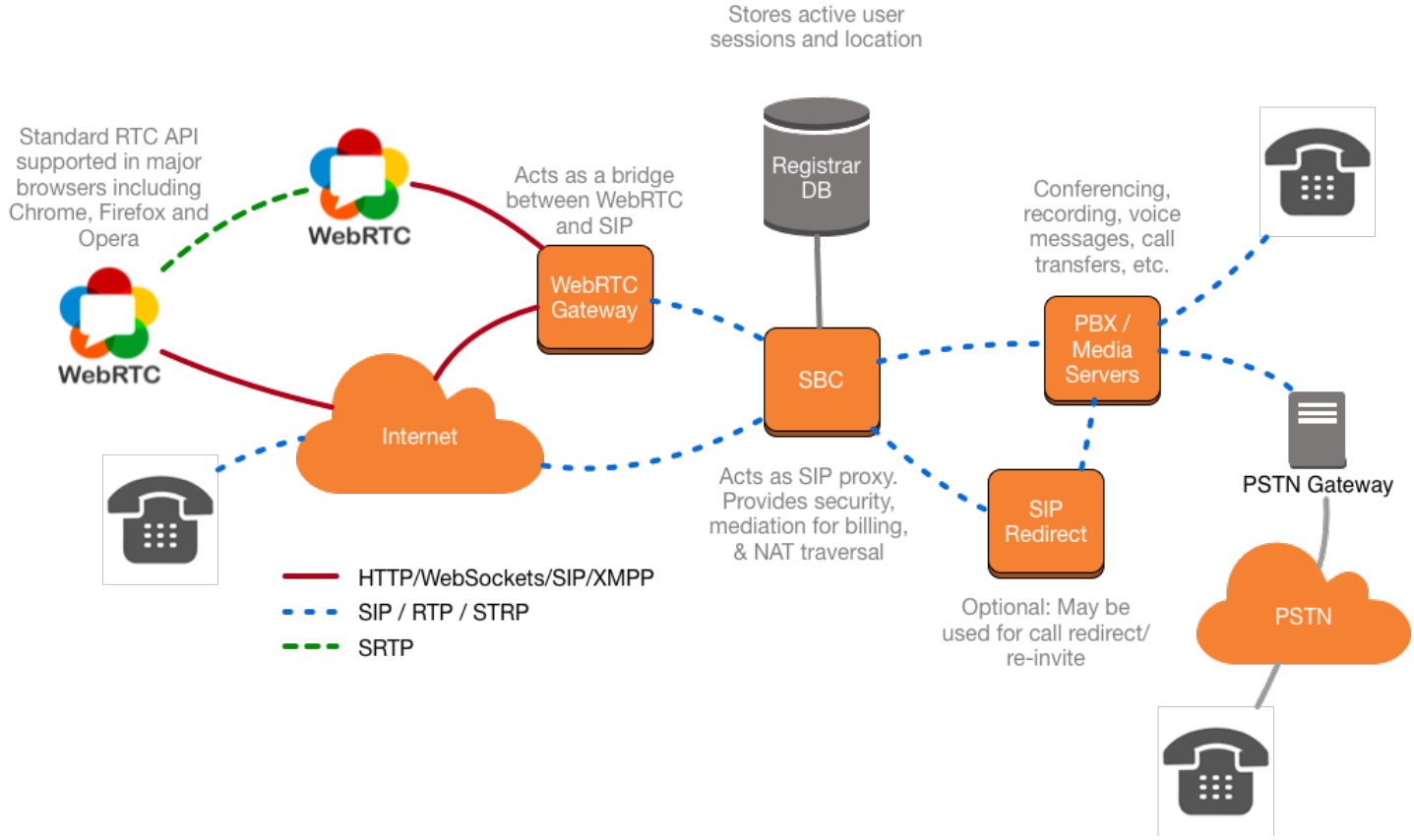
RTC 工作负载需要高度可扩展、弹性强且可用的环境。如今，客户在运行 RTC 工作负载时降低了成本，提高了敏捷性、弹性和上市时间。 AWS

RTC 架构的基本组件

在电信行业，RTC 通常指两个端点之间延迟最小的实时媒体会话。这些会议可能与以下内容有关：

- 双方之间的语音会话（例如电话系统、移动设备或 IP 语音 (VoIP)）
- 即时消息（例如聊天和即时中继聊天 (IRC)）
- 实时视频会话（例如视频会议和网真）

上述每种解决方案都有一些共同的组件（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）和一些特定于所传输媒体类型的组件（例如广播服务、消息服务器和队列等）。本节重点介绍如何定义基于语音和视频的 RTC 系统以及所有相关组件，如下图所示。



RTC 的基本架构组件

softSwitch/PBX

软交换机或 PBX 是语音电话系统的大脑，它为使用不同的组件在企业内部或外部建立、维护和路由语音呼叫提供智能。企业的所有用户都必须在 softswitch 上注册才能接听或拨打电话。softswitch 的一项重要功能是跟踪每个用户，以及如何使用语音网络中的其他组件与他们取得联系。

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，用于跟踪所有传入和传出的流量（包括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遭恶意使用。SBC 可用于与会话初始协议 (SIP) 中继互连以实现外部连接。有些 SBCs 还提供CODECs从一种格式转换为另一种格式的转码功能。大多数 SBCs 还提供网络地址转换 (NAT) 遍历功能，这有助于确保即使在有防火墙的网络中也能建立呼叫。

PSTN 连接

IP 语音 (VoIP) 解决方案使用公共交换电话网 (PSTN) 网关和 SIP 中继来连接传统 PSTN 网络。

PSTN 网关

PSTN 网关使用编解码器转码在实时传输协议 (RTP) SS7 和时分复用 (TDM) 之间转换 SIP 和媒体之间的信令。 PSTN 网关始终位于靠近 PSTN 网络的边缘。

SIP 中继

在 SIP 中继中，企业不会将呼叫终止到 TDM（SS7 基于）的网络，而是企业和电信公司之间的流量仍通过 IP 传输。大多数 SIP 中继都是通过使用 SBCs建立的。企业必须就电信公司的预定义安全规则达成一致，例如允许一定范围的 IP 地址、端口等。

媒体网关（转码器）

用户使用音频和/或视频以及可选数据和其他信息进行实时通信。要进行通信，两台设备需要能够为每个媒体轨道商定一个相互理解的编解码器，这样它们才能成功地通信和呈现共享媒体。所有兼容 WebRTC 的浏览器都必须支持在线定位用户支持 (OPUS) 和音频的 G711，以及视频的 H.264 受限基线VP8配置文件。

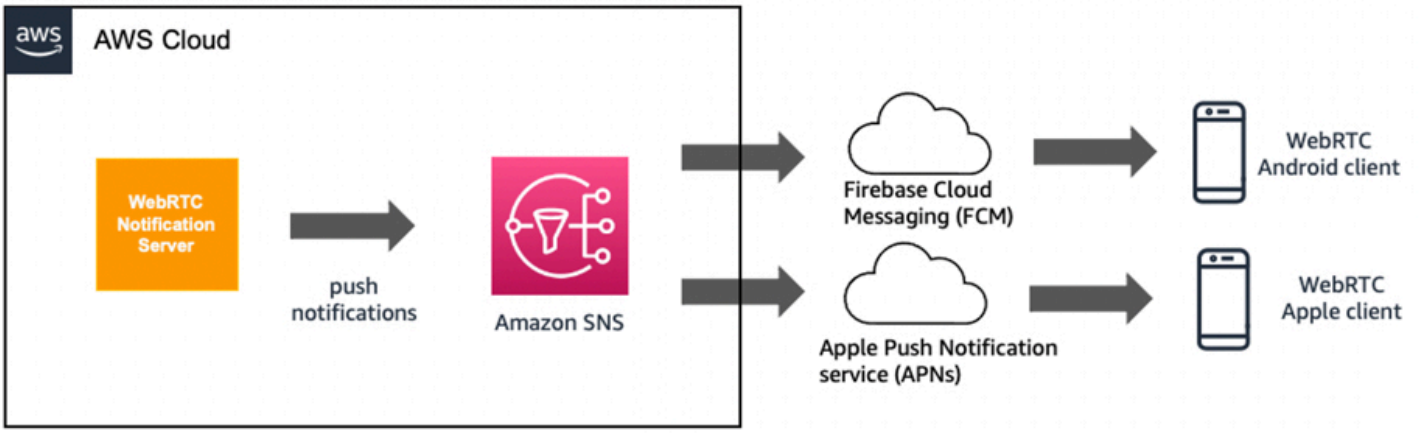
WebRTC生态系统之外的典型语音解决方案允许各种类型. CODECs 其中一些常见 CODECs 的是北美的 G.711 μ-law、G.711 a-law、G.729 和 G.722。当使用两种不同设备的两台设备相互 CODECs 通信

时，媒体网关会转换设备之间的编解码器流。换句话说，媒体网关处理媒体，并确保终端设备能够相互通信。

在 WebRTC 中推送通知

WebRTC的实现方式在移动设备上非常常见。与 Web 浏览器不同，移动设备无法长时间保持 websocket 连接处于打开状态。因此，它需要依靠来自WebRTC服务器的推送通知来处理所有结束请求，例如呼叫和消息。

亚马逊简单通知服务 (Amazon SNS) 允许您向移动设备上的应用程序发送推送通知。这些应用程序可以在各种操作系统上运行，例如苹果 iOS 或 Android。下图显示了从WebRTC通知服务器到WebRTC移动端点的推送通知流程的高级概述。

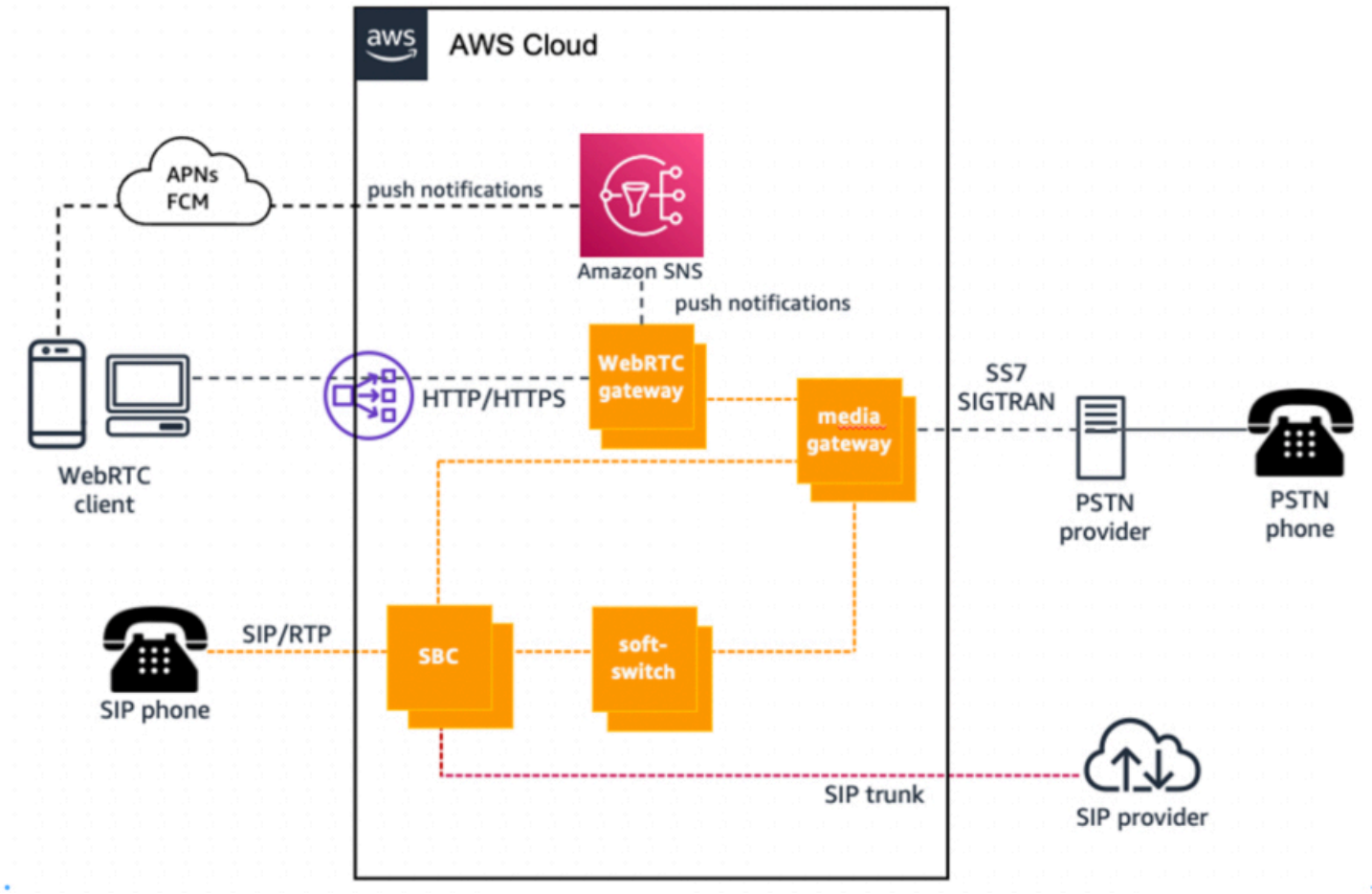


用于推送通知的 Amazon SNS

WebRTC 和 WebRTC 网关

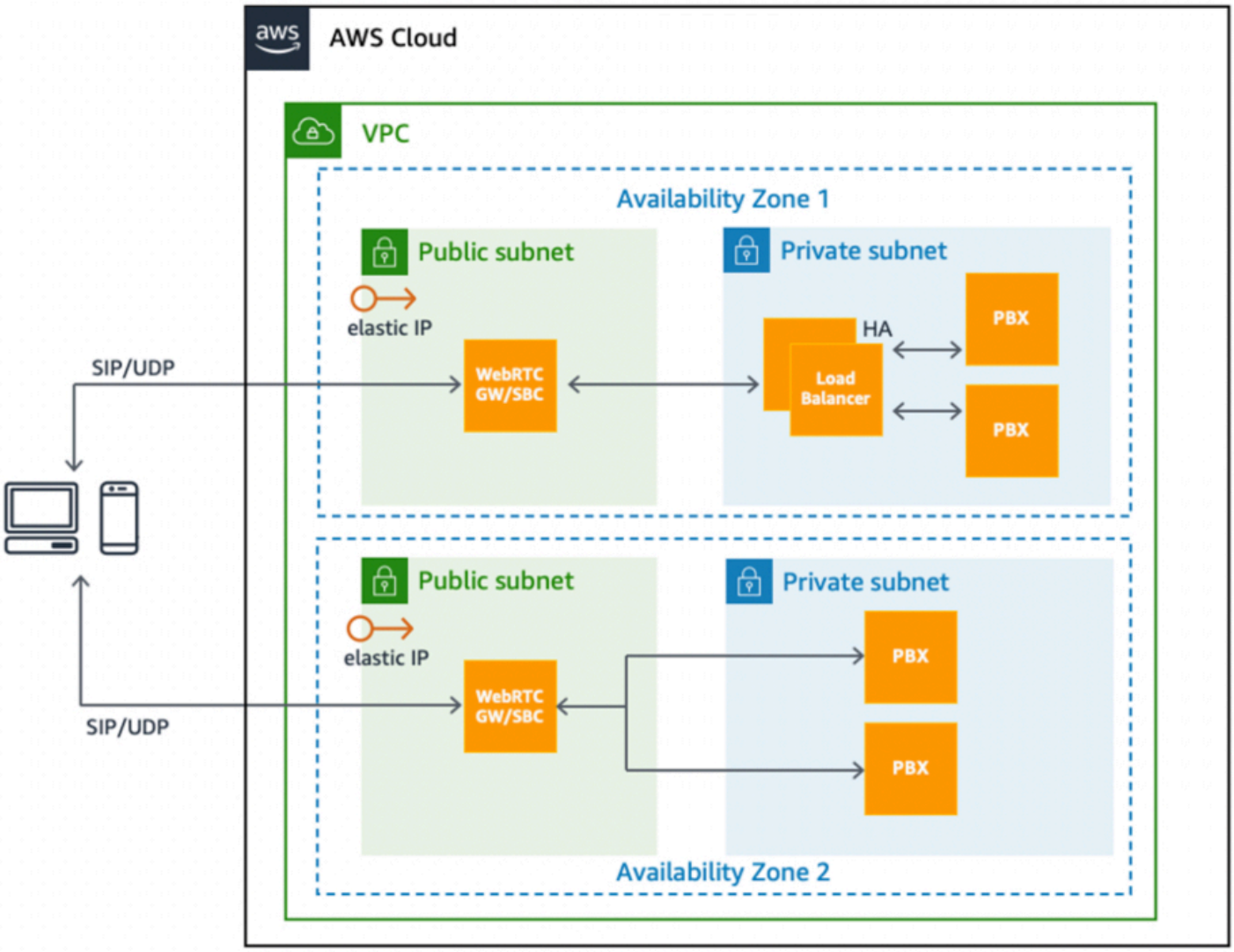
网络实时通信 (WebRTC) 允许您通过 Web 浏览器发起呼叫或使用 API 向后端服务器请求资源。该技术在设计时考虑了云技术，因此 APIs 提供了可用于建立呼叫的各种功能。由于并非所有语音解决方案（包括SIP）都支持这些 APIs，因此WebRTC网关需要将API调用转换为SIP消息，反之亦然。

下图显示了高可用性 WebRTC 架构的设计模式。来自WebRTC客户端的传入流量由应用程序负载均衡器（ALB）进行平衡，WebRTC 在属于Amazon Auto Scaling组的亚马逊弹性计算云 EC2（亚马逊）实例上运行。 EC2



用于语音的 RTC 系统的基本拓扑

SIP 和 RTP 流量的另一种设计模式是 EC2 在 Amazon SBCs 上以主动-被动模式在可用区之间使用成对的，如下图所示。在这里，弹性 IP 地址可以在无法使用域名服务 (DNS) 的实例发生故障时在实例之间动态移动。



在虚拟私有云 (VPC) EC2 中使用 Amazon 的 RTC 架构

开启了高可用性和可扩展性 AWS

大多数实时通信提供商都符合可用性从 99.9% 到 99.999% 的服务级别。根据所需的高可用性 (HA) 程度，您必须在应用程序的整个生命周期中采取越来越复杂的措施。AWS 建议遵循以下指南，以实现稳健的高可用性：

- 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 冗余配置可以消除单点故障 (SPOF)，其中 N+1 是通过主用-主动节点之间的负载平衡来实现的，而 2N 则由一对处于主用-备用配置的节点来实现。
  - AWS 有几种方法可以通过这两种方法实现 HA，例如通过可扩展、负载平衡的集群或假设主备对。
- 正确测试仪器和测试系统的可用性。
- 为手动机制准备操作程序，以响应、缓解故障并从故障中恢复。

本节重点介绍如何使用上提供的功能实现无单点故障 AWS。具体而言，本节介绍了一部分核心 AWS 功能和设计模式，这些功能和设计模式允许您构建高度可用的实时通信应用程序。

活动-备用状态服务器之间的 HA 浮动 IP 模式

浮动 IP 设计模式是一种众所周知的机制，用于在主用和备用硬件节点（媒体服务器）之间实现自动故障转移。为主动节点分配了静态辅助虚拟 IP 地址。在活动和备用节点之间进行持续监控可检测故障。如果主动节点出现故障，则监控脚本会将虚拟 IP 分配给就绪备用节点，备用节点接管主活动功能。这样，虚拟 IP 就会漂浮在主节点和备用节点之间。

RTC 解决方案中的适用性

并非总是可以让同一组件的多个活动实例投入使用，例如由 N 个节点组成的活动集群。主备配置为 HA 提供了最佳机制。例如，RTC 解决方案中的有状态组件，例如媒体服务器或会议服务器，甚至 SBC 或数据库服务器，都非常适合主备设置。SBC 或媒体服务器在给定时间有多个长时间运行的会话或通道处于活动状态，在 SBC 活动实例出现故障的情况下，由于浮动 IP，端点无需任何客户端配置即可重新连接到备用节点。

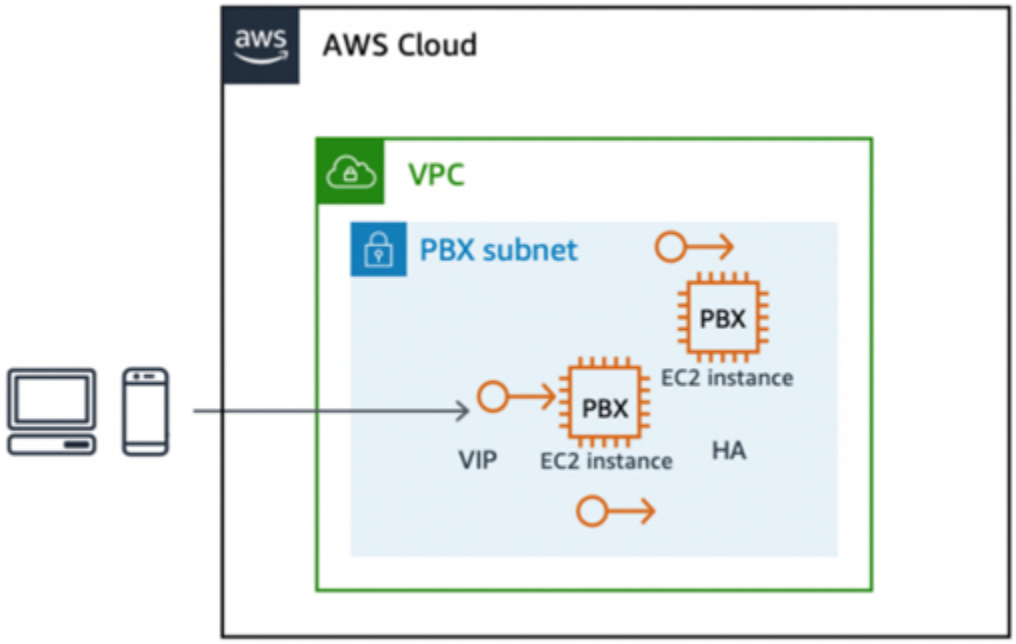
实施于 AWS

您可以使用亚马逊弹性计算云 (Amazon EC2) 中的核心功能、亚马逊 EC2 API、弹性 IP 地址以及亚马逊 EC2 对辅助私有 IP 地址的支持，在 AWS 上实现这种模式。

要在上实现浮动 IP 模式，请执行 AWS以下操作：

1. 启动两个 EC2 实例以扮演主节点和辅助节点的角色，其中假设主节点默认处于活动状态。
2. 为主 EC2 实例分配额外的辅助私有 IP 地址。
3. 弹性 IP 地址与虚拟 IP (VIP) 类似，与辅助私有地址相关联。此辅助私有地址是外部端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 (OS) 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 KeepAlive 上运行监控脚本（在 Linux、Corosync 等）上自定义，以监控对等节点的状态。如果当前的主动节点出现故障，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。

   因此，正在监听与辅助私有 IP 地址关联的 VIP 的应用程序可通过备用节点提供给端点。



使用弹性 IP 地址在有状态 EC2 实例之间进行故障转移

优势

这种方法是一种可靠的低预算解决方案，可以防止 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，但有所不同。在这种情况下，将通过可用的重新关联弹性 IP 地址 API 在不同可用区域的主用和备用节点之间重新关联浮动弹性 IP 地址。在上图所示的故障转移实现中，正在进行的呼叫将被丢弃，端点必须重新连接。可以通过复制底层会话数据来扩展这种实现，从而提供会话的无缝故障转移或媒体连续性。

使用 WebRTC 和 SIP 进行负载平衡以实现可扩展性和高可用性

基于预定义规则（例如轮询规则、亲和性或延迟等）对活动实例集群进行负载平衡是一种由 HTTP 请求的无状态性质而广泛推广的设计模式。实际上，对于许多 RTC 应用程序组件，负载平衡是一个可行的选择。

负载均衡器充当向所需应用程序发出的请求的反向代理或入口点，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。负载均衡器会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，通过负载平衡可以实现基本程度的高可用性。此外，由于负载均衡器以亚秒为间隔对所有群集节点执行主动和被动运行状况检查，因此故障转移的时间几乎是即时的。

定向哪个节点的决定取决于负载均衡器中定义的系统规则，包括：

- 轮询
- 会话或 IP 关联，可确保将一个会话中的多个请求或来自同一 IP 的多个请求发送到集群中的同一个节点
- 基于延迟
- 基于负载

在 RTC 架构中的适用性

WebRTC协议使WebRTC网关可以通过基于HTTP的负载均衡器轻松进行负载平衡，例如弹性负载平衡 (ELB)、应用程序负载均衡器 (ALB) 或网络负载均衡器 (NLB)。由于大多数 SIP 实现都依赖传输控制协议 (TCP) 和用户数据报协议 (UDP) 的传输，因此需要网络或连接级负载平衡，同时支持基于 TCP 和 UDP 的流量。

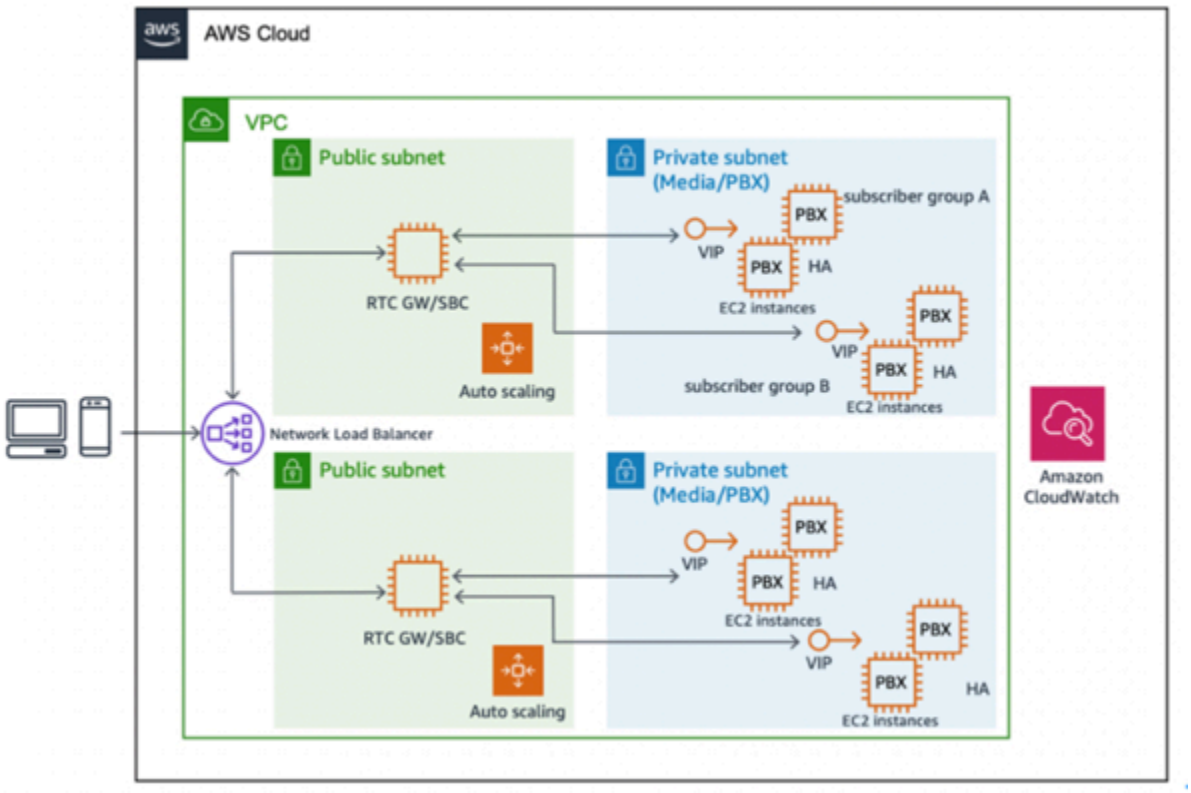
AWS 使用 Application Load Balancer 和 Auto Scaling 为 WebRTC 开启负载平衡

对于基于 WebRTC 的通信，Elastic Load Balancing 提供了一个完全托管、高度可用且可扩展的负载均衡器作为请求的入口点，然后将请求定向到与 Elastic Load Balancing 关联 EC2 的目标实例集群。

由于 WebRTC 请求是无状态的，因此您可以使用 Amazon A EC2 uto Scaling 来提供全自动且可控的可扩展性、弹性和高可用性。

Application Load Balancer 提供完全托管的负载平衡服务，该服务在使用多个可用区时具有高可用性，并且可扩展。这支持处理WebRTC应用程序信令的 WebSocket 请求的负载平衡，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，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个目标。如果您启用粘性会话，则同一目标会收到请求并可以使用 Cookie 恢复会话上下文。

下图显示了目标拓扑。



WebRTC 可扩展性和高可用性架构

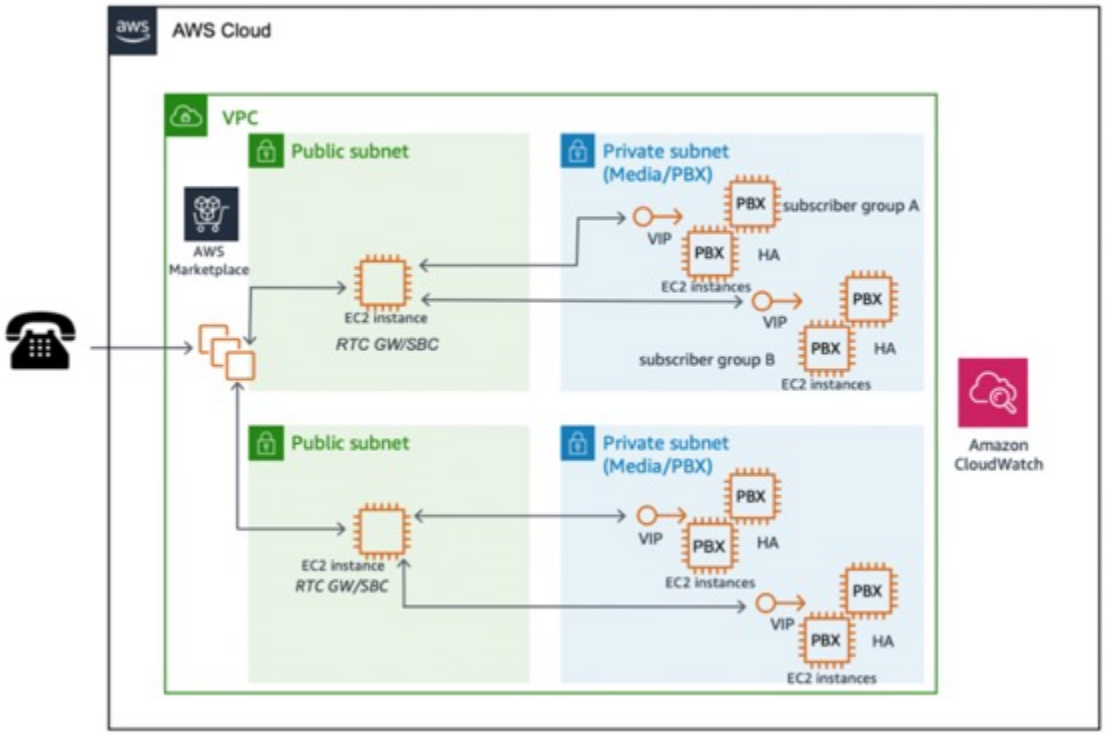
使用 Network Load Balancer 或 AWS Marketplace 产品实现 SIP

对于基于 SIP 的通信，连接通过 TCP 或 UDP 建立，大多数 RTC 应用程序都使用 UDP。如果 SIP/TCP 是首选的信号协议，那么使用 Network Load Balancer 进行完全托管、高度可用、可扩展和性能的负载平衡是可行的。

Network Load Balancer 在连接级别（第四层）运行，根据 IP 协议数据将连接路由到 Amazon EC2 实例、容器和 IP 地址等目标。网络负载平衡非常适合 TCP 或 UDP 流量负载平衡，能够每秒处理数百

万个请求，同时保持超低的延迟。它与其他流行的 AWS 服务集成，例如亚马逊 A EC2 uto Scaling、亚马逊弹性容器服务（亚马逊 ECS）、亚马逊 Elastic Kubernetes 服务（亚马逊 EK S）和。AWS CloudFormation

如果启动了 SIP 连接，则另一种选择是使用AWS Marketplace商业 off-the-shelf软件 (COTS)。 AWS Marketplace 提供了许多可以处理 UDP 和其他类型的第四层连接负载平衡的产品。COTS 通常包括对高可用性的支持，并且通常与 Amazon A EC2 uto Scaling 等功能集成，以进一步增强可用性和可扩展性。下图显示了目标拓扑：



利用 AWS Marketplace 产品实现基于 SIP 的 RTC

基于跨区域 DNS 的负载平衡和故障转移

Amazon Route 53 提供全球 DNS 服务，可用作 RTC 客户端注册和连接媒体应用程序的公共或私有终端节点。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状况良好的终端节点或独立监控应用程序的运行状况。

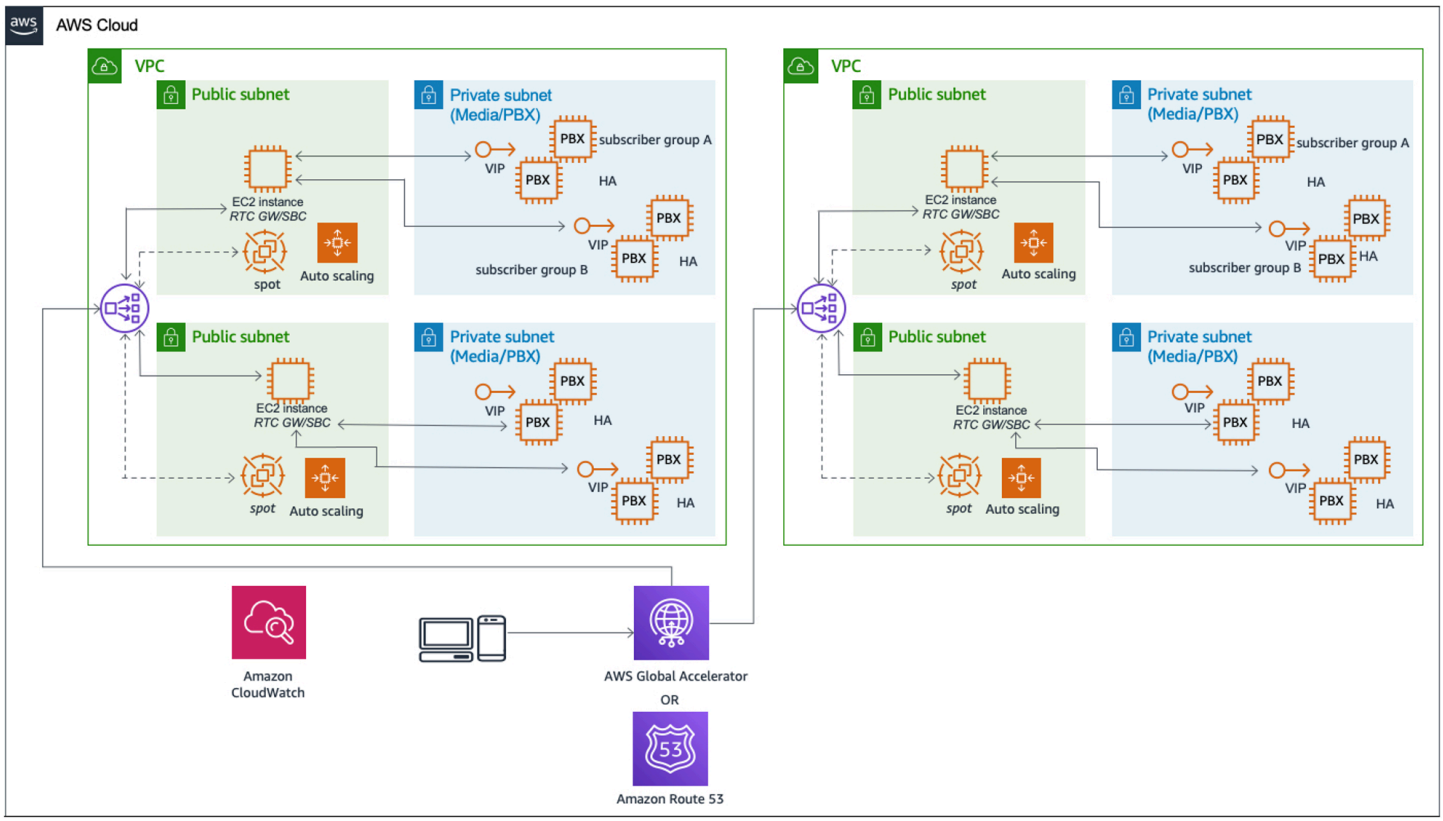
Amazon Route 53 Traffic Flow 功能使您可以轻松地通过各种路由类型管理全球流量，包括基于延迟的路由、地域 DNS、地理位置和加权回合，所有这些都可以与 DNS 故障转移结合使用，以实现各种低延迟、容错架构。Amazon Route 53 Traffic Flow 简易可视化编辑器允许您管理将最终用户路由到应用程序终端节点的方式，无论是在单个 AWS 区域还是分布在全球各地。

就全球部署而言，Route 53 中基于延迟的路由策略特别有用，可以将客户引导到最近的媒体服务器接入点，从而提高与实时媒体交换相关的服务质量。

请注意，要强制故障转移到新的 DNS 地址，必须刷新客户端缓存。此外，DNS 更改在全球 DNS 服务器上传播时可能会有延迟。您可以使用 “存活时间” 属性管理 DNS 查询的刷新间隔。此属性可在设置 DNS 策略时进行配置。

为了快速覆盖全球用户或满足使用单个公有 IP 的要求， AWS Global Accelerator 也可以用于跨区域故障转移。 AWS Global Accelerator是一项网络服务，可提高本地和全球覆盖的应用程序的可用性和性能。 AWS Global Accelerator 提供静态 IP 地址，这些地址充当应用程序终端节点的固定入口点，例如您的应用程序负载均衡器、网络负载均衡器或单个或多个 AWS 区域中的 Amazon EC2 实例。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 持续监控应用程序终端节点的运行状况，并在当前终端节点变为不健康时自动将流量重定向到最近的健康终端节点。为了满足其他安全要求，Accelerated VP Site-to-Site N 使用 AWS Global Accelerator 智能路由流量通过 AWS 全球网络和 AWS 边缘站点来提高 VPN 连接的性能。



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

数据持久性和高可用性（带有永久存储）

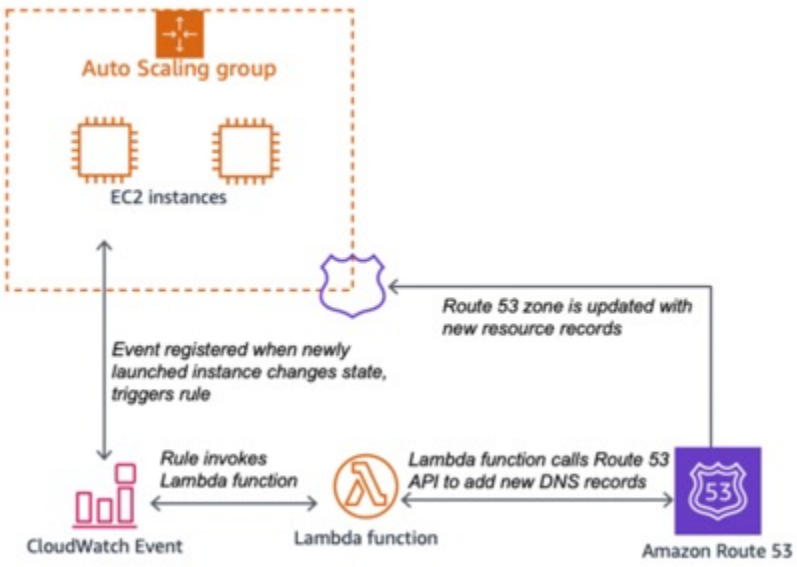
大多数 RTC 应用程序依靠永久存储来存储和访问用于身份验证、授权、记账（会话数据、呼叫详细记录等）、操作监控和日志记录的数据。在传统的数据中心中，确保永久存储组件（数据库、文件系统等）的高可用性和耐久性通常需要通过设置存储区域网络 (SAN)、独立磁盘冗余阵列 (RAID) 设计以及备份、恢复和故障转移处理流程来完成繁重的工作。这 AWS 云 极大地简化并增强了围绕数据持久性和可用性的传统数据中心实践。

对于对象存储和文件存储，亚马逊简单存储 AWS 服务 (Amazon S3) 和亚马逊弹性文件系统 (Amazon EFS) 等服务提供托管的高可用性和可扩展性。Amazon S3 的数据持久性为 99.999999999%（11 个 9）。

对于交易数据存储，客户可以选择利用完全托管的亚马逊关系数据库服务（Amazon RDS），该服务支持具有高可用性部署的亚马逊 Aurora、PostgreSQL、MySQL、MariaDB、Oracle 和微软 SQL Server。对于注册商功能、订阅者资料或会计记录存储（例如 CDRs），Amazon RDS 提供了容错、高度可用和可扩展的选项。

使用 AWS Lambda Amazon Route 53 和 Amazon A EC2 uto Scaling 进行动态扩展

AWS 允许将功能链接起来，并能够根据基础架构事件将自定义的无服务器功能作为服务合并。其中一种在 RTC 应用程序中具有多种用途的设计模式是将自动扩展生命周期挂钩与 Amazon Ev CloudWatch ents、Amazon Route 53 和AWS Lambda函数相结合。 AWS Lambda 函数可以嵌入任何动作或逻辑。下图演示了将这些功能链接在一起如何通过自动化增强系统的可靠性和可扩展性。



通过 Amazon Route 53 的动态更新自动扩展

搭载亚马逊 Kinesis Video Streams 的高可用性 WebRTC Amazon Kinesis Video St

Amazon Kinesis Vid eo Streams 通过 WebRTC 提供实时媒体流，允许用户捕获、处理和存储媒体流，以便播放、分析和机器学习。这些直播具有高可用性、可扩展性，并且符合WebRTC标准。Amazon Kinesis Video Streams 包括 WebRTC 信号终端节点，用于快速发现对等设备和建立安全连接。它包括用于 NAT (STUN) 的托管会话遍历实用程序，以及在 NAT (TURN) 端点周围使用中继进行遍历，用于在对等体之间实时交换媒体。它还包括一个免费的开源 SDK，该软件开发工具包直接与相机固件集成，可实现与 Amazon Kinesis Video Streams 端点的安全通信，从而实现同行发现和媒体直播。最后，它提供了适用于Android、iOS的客户端库，允许 JavaScript 符合WebRTC标准的移动和网络玩家安全地发现摄像设备并与之连接，以进行媒体流和双向通信。

使用 Amazon Chime 语音连接器实现高度可用的 SIP 中继

Amazon Chime Voice Connec tor 提供 pay-as-you-go SIP 中继服务，使公司能够使用其电话系统拨打和/或接听安全、廉价的电话。Amazon Chime Voice Connector 是服务提供商 SIP 中继或综合服务数字网络 (ISDN) 主速率接口 () 的低成本替代方案 ()。PRIs客户可以选择启用入站呼叫、出站呼叫或两者兼而有之。

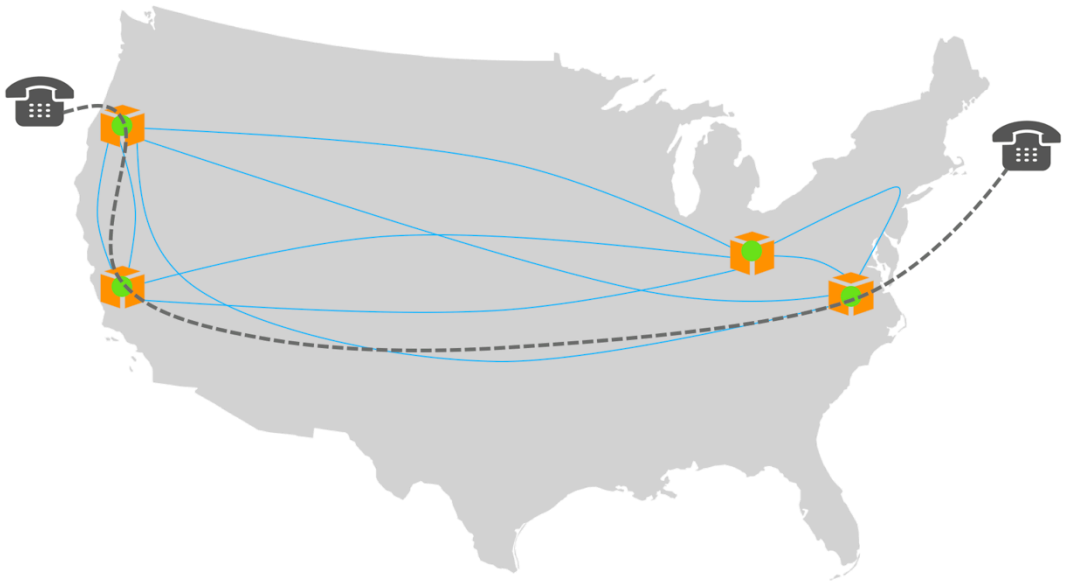
该服务使用 AWS 网络在多个网络上提供高度可用的通话体验 AWS 区域。您可以将来自 SIP 中继电话的音频流式传输，或者将基于 SIP 的媒体录制 (SIPREC) 源转发到 Amazon Kinesis Video Streams Amazon Kinesis Video Streams，以实时从商务电话中获取见解。通过与 Amazon Tran scribe 和其他常见的机器学习库集成，您可以快速构建用于音频分析的应用程序。

来自现场的最佳实践

本节总结了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 客户实施的最佳实践。 AWS 想要在公共云中运行自己的 SIP 基础设施的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弹性，以防出现不同类型的故障。尽管其中一些最佳实践是特定于 SIP 的，但其中大多数都适用于运行的任何实时通信应用程序 AWS。

创建 SIP 叠加层

AWS 具有强大、可扩展和冗余的网络主干，可在不同网络之间提供连接 AWS 区域。当网络事件（例如光纤中断）使 AWS 主干链路降级时，流量会使用网络级路由协议（例如边界网关协议 (BGP)）快速故障转移到冗余路径。这种网络级别的流量工程对客户来说是一个黑匣子，大多数 AWS 客户甚至没有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传递）的客户有时会注意到这些事件。那么， AWS 客户如何在网络层面提供的 AWS 流量基础上实施自己的流量工程呢？ 解决方案是在许多不同的地方部署 SIP 基础架构 AWS 区域。作为呼叫控制功能的一部分，SIP 还提供通过特定的 SIP 代理路由呼叫的功能。



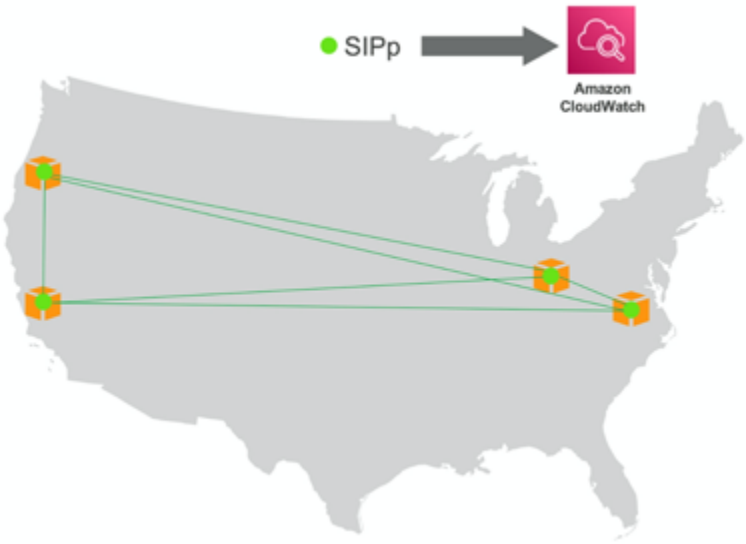
使用 SIP 路由覆盖网络路由

在上图中，SIP 基础架构（由立方体内的绿点表示）正在美国所有四个地区运行。蓝色的实线代表了对骨干的虚构描绘。 AWS 如果未实施 SIP 路由，则来自美国西海岸并发往美国东海岸的呼叫将通过直接连接俄勒冈州和弗吉尼亚州的骨干链路进行。该图显示了客户如何使用SIP路由覆盖网络级路由，在俄

勒冈州和弗吉尼亚州之间拨打通过加利福尼亚路由的相同呼叫。这种类型的 SIP 流量工程可以使用基于 SIP 重传和客户特定业务偏好等网络指标，使用 SIP 代理和媒体网关来实现。

执行详细监控

实时语音和视频应用程序的最终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。为了主动而不是被动，必须在为最终用户服务的系统的每个部分部署详细的监控。



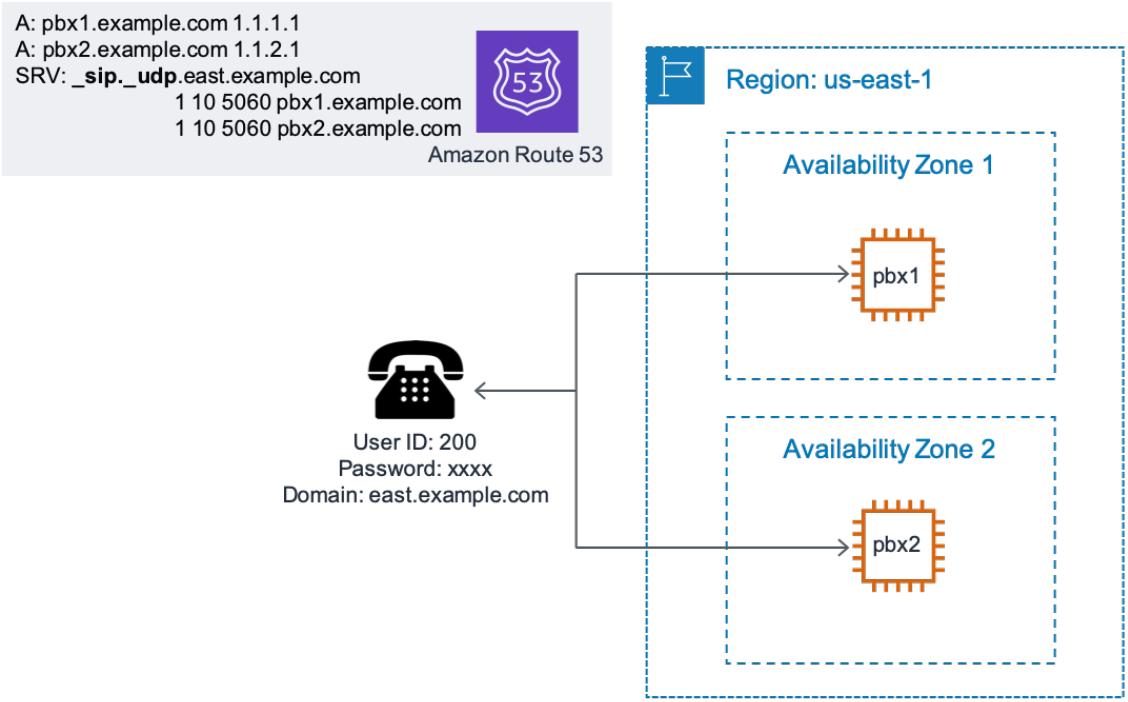
SIPp 用于监控 VoIP 基础架构

许多开源工具，例如 iPerf 或SIPpVOIPMonitor、和，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 SIP 的节点正在测量 SIP 指标，例如成功呼叫和所有四个美国之间的 SIP 重新传输。 AWS 区域然后，可以使用自定义脚本将这些指标导出到 Amazon CloudWatch 。使用 CloudWatch，客户可以根据特定的阈值针对这些自定义指标创建警报。然后，可以根据这些 CloudWatch 警报的状态采取自动或手动补救措施。

对于不想分配开发和维护定制监控系统所需的工程资源的客户，市场上有许多不错的VoIP监控解决方案可供选择，例如ThousandEyes。补救措施的一个示例是根据增加的 SIP 重传次数更改 SIP 路由。

使用 DNS 进行负载平衡，使用浮动 IPs 进行故障转移

支持 DNS SRV 功能的 IP 电话客户端可以通过将客户端的负载平衡到不同的 SBCs/，从而有效地利用基础架构中内置的冗余。PBXs



使用 DNS SRV 记录对 SIP 客户端进行负载平衡

上图显示了客户如何使用 SRV 记录对 SIP 流量进行负载平衡。任何支持 SRV 标准的 IP 电话客户端都将寻找 sip。 <transport protocol>SRV 类型的 DNS 记录中的前缀。在示例中，来自 DNS 的答案部分包含在不同 AWS 可用区中 PBXs 运行的两者。但是，除了端点之外 URIs，SRV 记录还包含另外三条信息：

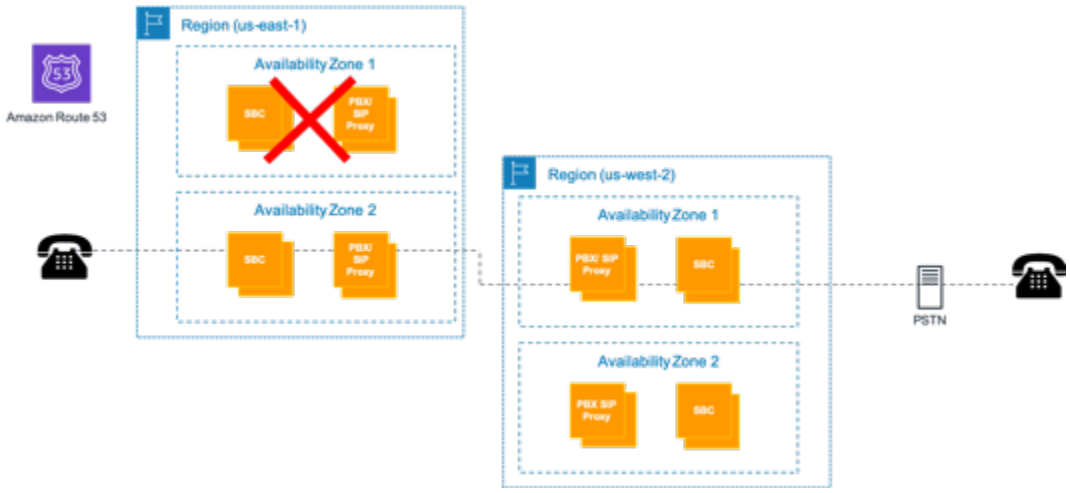
- 第一个数字是优先级（在上面的示例中为 1）。优先级越低，优先级越高。
- 第二个数字是重量（在上面的示例中为 10）。
- 第三个数字是要使用的端口 (5060)。

由于两 PBXs 台服务器的优先级相同 (1)，因此客户端使用权重在两者之间进行负载平衡 PBXs。在这种情况下，由于权重相同，因此 SIP 流量应在两者之间均衡负载 PBXs。

DNS 可能是客户端负载平衡的好解决方案，但是通过更改/更新 DNS “A” 记录来实现故障转移又如何呢？ 由于发现客户端和中间节点内的 DNS 缓存行为不一致，因此不建议使用此方法。在 SIP 节点集群之间进行可用区内故障转移的更好方法是使用 EC2 IP 重新分配，即使用 API 将受损主机的 IP 地址立即重新分配给运行正常的主机。 EC2 再加上详细的监控和运行状况检查解决方案，故障节点的 IP 重新分配可确保流量及时转移到运行状况良好的主机，从而最大限度地减少对最终用户的干扰。

使用多个可用区

每个可用区 AWS 区域 都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，因此形成了一个隔离的故障域。在的结构中 AWS，鼓励客户在多个可用区中运行其工作负载。这样可以确保客户应用程序甚至可以承受可用区完全出现故障，这本身就是一种非常罕见的事件。此建议也适用于实时 SIP 基础架构。



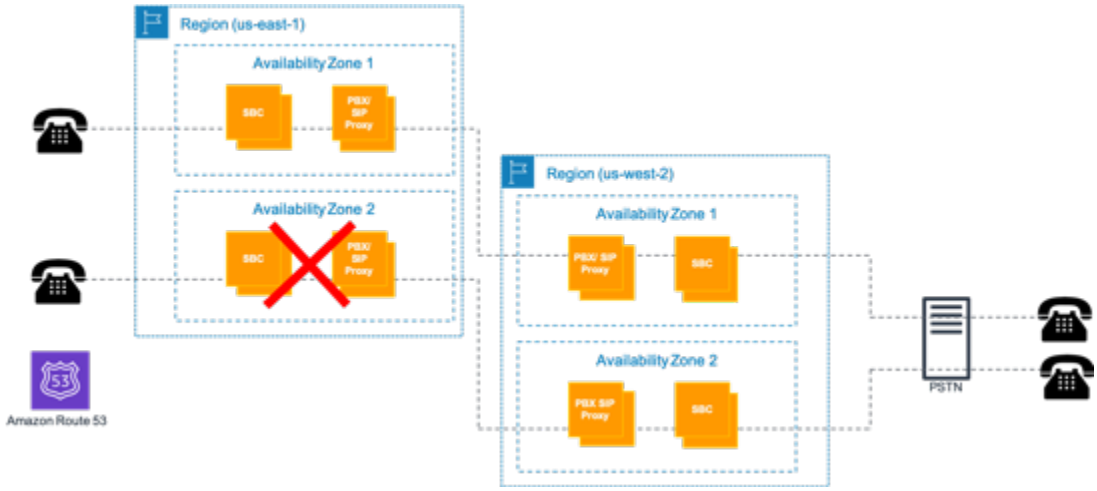
处理可用区故障

假设灾难性事件（例如五级飓风）导致 us-east-1 区域的可用区完全中断。基础设施如图所示运行，所有最初在故障可用区节点上注册的 SIP 客户端都应向可用区 #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，确保支持该行为。）尽管可用区中断时处于活动状态的 SIP 呼叫会丢失，但任何新的呼叫都将通过可用区 2 进行路由。

总而言之，DNS SRV 记录应将客户端指向多个 “A” 记录，每个可用区都有一个。反过来，每个 “A” 记录都应指向该可用区PBXs 中 SBCs /的多个 IP 地址，从而提供可用区内和可用区间弹性。可用区内和可用区间故障切换均可通过使用 IP 重新分配来实现（如果它们是公共的）。 IPs 但是 IPs，私有不能跨可用区重新分配。如果客户使用私有 IP 地址，则他们必须依靠在备份 SBC/PBX 中重新注册的 SIP 客户端进行可用区间故障转移。

将流量保持在一个可用区内并使用 EC2 置放群组

此最佳实践也称为可用区关联性，也适用于可用区完全出现故障的罕见事件。建议您消除任何跨可用区流量，以便进入一个可用区域的任何 SIP 或 RTP 流量都应保留在该可用区中，直到它退出该区域。



可用区关联性（最多 50% 的活动呼叫丢失）

上图显示了使用可用区关联性的简化架构。如果考虑到可用区完全中断的影响，这种方法的比较优势就会显而易见。如图所示，如果可用区 2 中断，则最多有 50% 的活动呼叫受到影响（假设可用区之间的负载平衡相等）。如果未实施可用区关联性，则某些呼叫将在一个区域的可用区之间流动，而故障很可能会影响超过 50% 的活跃呼叫。

为了最大限度地减少流量延迟，AWS 还建议您考虑在每个可用区内使用EC2 置放群组。在同一 EC2置放群组内启动的实例具有更高的带宽和更短的延迟， EC2 从而确保了这些实例彼此之间的网络距离。

使用增强型联网 EC2 实例类型

在 Amazon 上选择正确的实例类型 EC2 可确保系统的可靠性以及基础设施的有效利用。 EC2 提供了多种经过优化的实例类型，以适应不同的用例。实例类型包括 CPU、内存、存储和网络容量的不同组合，便于您灵活选择适合应用程序的资源组合。这些增强的联网实例类型可确保在其上运行的 SIP 工作负载能够获得稳定的带宽和相对较低的聚合延迟。Amazon 最近又推出了一 EC2 款弹性网络适配器 (ENA)，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的成本价值。例如，C5N 支持新的弹性网络适配器，其带宽高达 100 Gbps，每秒可处理数百万个数据包 (PPS)。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套件 (DPDK)，它可以极大地提高网络数据包处理能力。

但是，最佳做法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找到其他配置参数，例如特定实例类型一次可以处理的最大呼叫数。

安全性注意事项

RTC 应用程序组件通常直接在面向互联网的 Amazon EC2 实例上运行。除了 TCP 之外，流量还使用 UDP 和 SIP 等协议。在这些情况下， AWS Shield Standard 可以保护 Amazon EC2 实例免受常见的基础设施层（第 3 层和第 4 层） DDo攻击，例如 UDP 反射攻击、DNS 反射、NTP 反射、SSDP 反射等。 AWS Shield Standard 使用各种技术，例如基于优先级的流量整形，当检测到定义明确的 DDo S 攻击特征码时，这些技术会自动启用。

AWS 还通过在弹性 IP 地址 AWS Shield Advanced 上启用，为这些应用程序提供针对大型复杂的 DDo S 攻击的高级保护。 AWS Shield Advanced 提供增强的 DDo S 检测，可自动检测 AWS 资源类型和 EC2实例大小，并应用适当的预定义缓解措施，并防止 SYN 或 UDP 洪水。借助 AWS Shield Advanced，客户还可以联系全天候的 AWS DDo S 响应团队 (DRT)，创建自己的自定义缓解档案。 AWS Shield Advanced 还可确保在 DDo S 攻击期间，您的所有 Amazon VPC 网络访问控制列表 (ACLs) 都会自动在 AWS 网络边界强制执行，从而为您提供额外的带宽和清理容量，从而缓解大容量 DDo S 攻击。

结论

可以部署实时通信 (RTC) 工作负载， AWS 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，从而降低成本、提高灵活性并减少全球占地面积。

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

首字母缩略词

本文档中使用的首字母缩略语包括：

ACL-访问控制列表

ALB — Application Load Balancer

APNs — Apple 推送通知服务

BGP — 边界网关协议

CDR-通话详细记录

COTS — 商业 off-the-shelf软件

DDoS — 分布式 denial-of-service

DNS — 域名系统

DPDK — 英特尔数据平面开发人员套件

DRT — DDo S 响应小组

ENA — 弹性网络适配器

EPC — 进化分组核心

FCM — Firebase 云消息传递

HA — 高可用性

IRC — 互联网中继聊天

ISDN — 综合服务数字网络

NAT — 网络地址转换

OPUS — 在线定位用户支持

PBX — 专用交换机

PRI — 主速率接口

PSTN — 公共交换电话网络

RAID — 独立磁盘冗余阵列

RTC — 实时通信

RTP —实时传输协议

SAN — 存储区域网络

SBC — 会话边界控制器

SIP —会话初始化协议

SPOF — 单点故障

SRV — 服务

SS7 — 信号系统 n.7

STUN — 适用于 NAT 的会话遍历实用程序

SYN —同步

TCP — 传输控制协议

TDM — 时分多路复用

TURN — 使用 NAT 周围的中继进行遍历

UDP — 用户数据报协议

URI-统一资源标识符

VIP — 虚拟 IP

VNF — 虚拟网络功能

VoIP — IP 语音

VPC — 虚拟私有云

WebRTC — 网络实时通信

贡献者

以下个人和组织参与了本文档的编撰：

- Mounir Chennana，亚马逊 Web Services 高级解决方案架构师
- Mohammed Al-Mehdar，Amazon Web Services 高级解决方案架构师
- Ejaz Sial，Amazon Web Services 高级解决方案架构师
- Ahmad Khan，Amazon Web Services 高级解决方案架构师
- Tipu Qureshi，首席工程师，亚马逊 Web Serv AWS 支持 ices
- Hasan Khan，亚马逊 Web Services 高级技术客户经理
- Shoma Chakravarty，亚马逊 Web Services 电信业务全球技术负责人

文档修订

如需获取有关该白皮书更新的通知，请订阅 RSS 信息源。

变更	说明	日期
已更新白皮书	已更新以获取最新的服务和功能。	2022 年 5 月 5 日
已更新白皮书	已更新以获取最新的服务和功能。	2020 年 2 月 13 日
初次发布	白皮书首次发布。	2018 年 10 月 1 日

版权声明

AWS 词汇表

有关最新 AWS 术语，请参阅《AWS 词汇表 参考资料》中的AWS 词汇表。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。