

How Ribbon Built a Scalable, Resilient Robocall Mitigation Platform

by Siva Rajamani and Shaun Bharrat | on 14 JAN 2022 | in [Amazon API Gateway](#), [Amazon DynamoDB](#), [Amazon Elastic Container Service](#), [Amazon QuickSight](#), [Amazon Route 53](#), [Amazon Simple Storage Service \(S3\)](#), [Architecture](#), [AWS Glue](#), [AWS Key Management Service](#), [AWS Lambda](#), [Elastic Load Balancing](#) | [Permalink](#) | [Share](#)

Ribbon provides communications software, and IP and optical networking end-to-end solutions that deliver innovation, unparalleled scale, performance, and agility to service providers and enterprise.

Ribbon is helping customers modernize their networks. In today's data-hungry, 24/7 world, this equates to improved competitive positioning and business outcomes. Companies are migrating from on-premises equipment for telephony services and looking for equivalent *as a service* (aaS) offerings. But these solutions must still meet the stringent resiliency, availability, performance, and regulatory requirements of a telephony service.

The telephony world is inundated with robocalls. In the United States alone, there were an estimated [50.5 billion robocalls in 2021](#)! In this blog post, we describe the Ribbon Identity Hub – a holistic solution for robocall mitigation. The Ribbon Identity Hub enables services that sign and verify caller identity, which is compliant to the [ATIS](#) standards under the [STIR/SHAKEN](#) framework. It also evaluates and scores calls for the probability of nuisance and fraud.

Ribbon Identity Hub is implemented in Amazon Web Services (AWS). It is a fully managed service for telephony service providers and enterprises. The solution is secure, multi-tenant, automatic scaling, and multi-Region, and enables Ribbon to offer managed services to a wide range of telephony customers. Ribbon ensures resiliency and performance with efficient use of resources in the telephony environment, where load ratios between busy and idle time can exceed 10:1.

Ribbon Identity Hub

The Ribbon Identity Hub services are separated into a data (call-transaction) plane, and a control plane.

Data plane (call-transaction)

The call-transaction processing is typically invoked on a per-call-setup basis where availability, resilience, and performance predictability are paramount. Additionally, due to high variability in load, automatic scaling is a prerequisite.

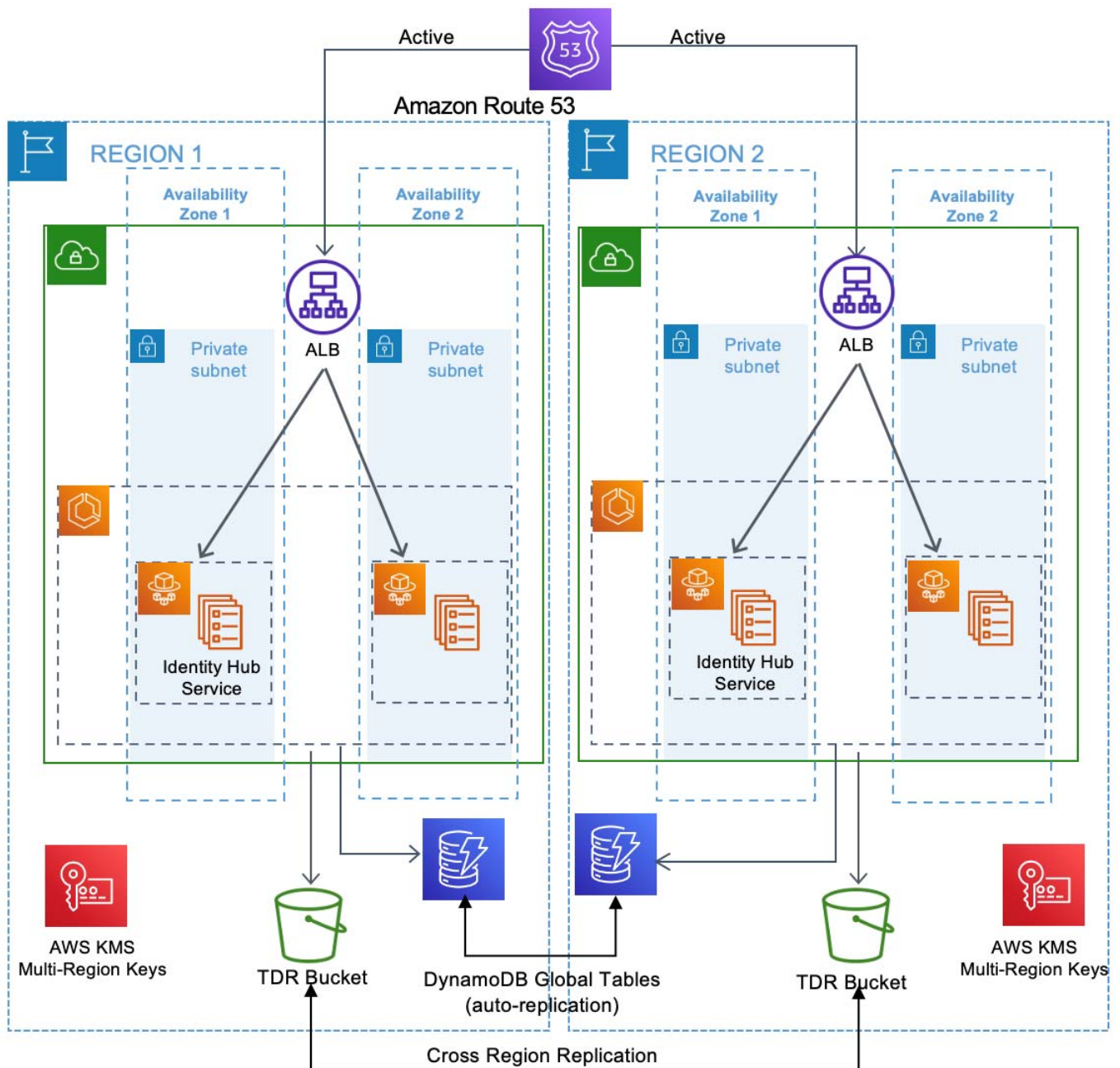


Figure 1. Data plane architecture

Several AWS services come together in a solution that meets all these important objectives:

1. [Amazon Elastic Container Service \(ECS\)](#): The ECS services are set up for automatic scaling and span two Availability Zones. This provides the horizontal scaling capability, the self-healing capacity, and the resiliency across Availability Zones.
2. [Elastic Load Balancing – Application Load Balancer \(ALB\)](#): This provides the ability to distribute incoming traffic to ECS services as the target. In addition, it also offers:
 - Seamless integration with the ECS Auto Scaling group. As the group grows, traffic is directed to the new instances only when they are ready. As traffic drops, traffic is drained from the target instances for graceful scale down.
 - Full support for canary and linear upgrades with zero downtime. Maintains full-service availability without any changes or even perception for the client devices.
3. [Amazon Simple Storage Service \(S3\)](#): Transaction detail records associated with call-related requests must be securely and reliably maintained for over a year due to billing and other contractual obligations. Amazon S3 simplifies this task with [high durability](#), [lifecycle rules](#), and [varied controls for retention](#).
4. [Amazon DynamoDB](#): Building resilient services is significantly easier when the compute processing can be stateless. Amazon DynamoDB facilitates such stateless architectures without compromise. Coupled with the availability of the [Amazon DynamoDB Accelerator \(DAX\)](#) caching layer, the solution can meet the extreme low latency operation requirements.

5. [AWS Key Management Service \(KMS\)](#): Certain tenant configuration is highly confidential and requires elevated protection. Furthermore, the data is part of the state that must be recovered across Regions in disaster recovery scenarios. To meet the security requirements, the KMS is used for envelope encryption using per-tenant keys. [Multi-Region KMS keys](#) facilitates the secure availability of this state across Regions without the need for application-level intervention when replicating encrypted data.
6. [Amazon Route 53](#): For telephony services, any non-transient service failure is unacceptable. In addition to providing high degree of resiliency through Multi-AZ architecture, Identity Hub also provides Regional level high availability through its multi-Region active-active architecture. Route 53 with [health checks](#) provides for dynamic rerouting of requests within minutes to alternate Regions.

Control plane

The Identity Hub control plane is used for customer configuration, status, and monitoring. The API is REST-based. Since this is not used on a call-by-call basis, the requirements around latency and performance are less stringent, though the requirements around high resiliency and dynamic scaling still apply. In this area, ease of implementation and maintainability are key.

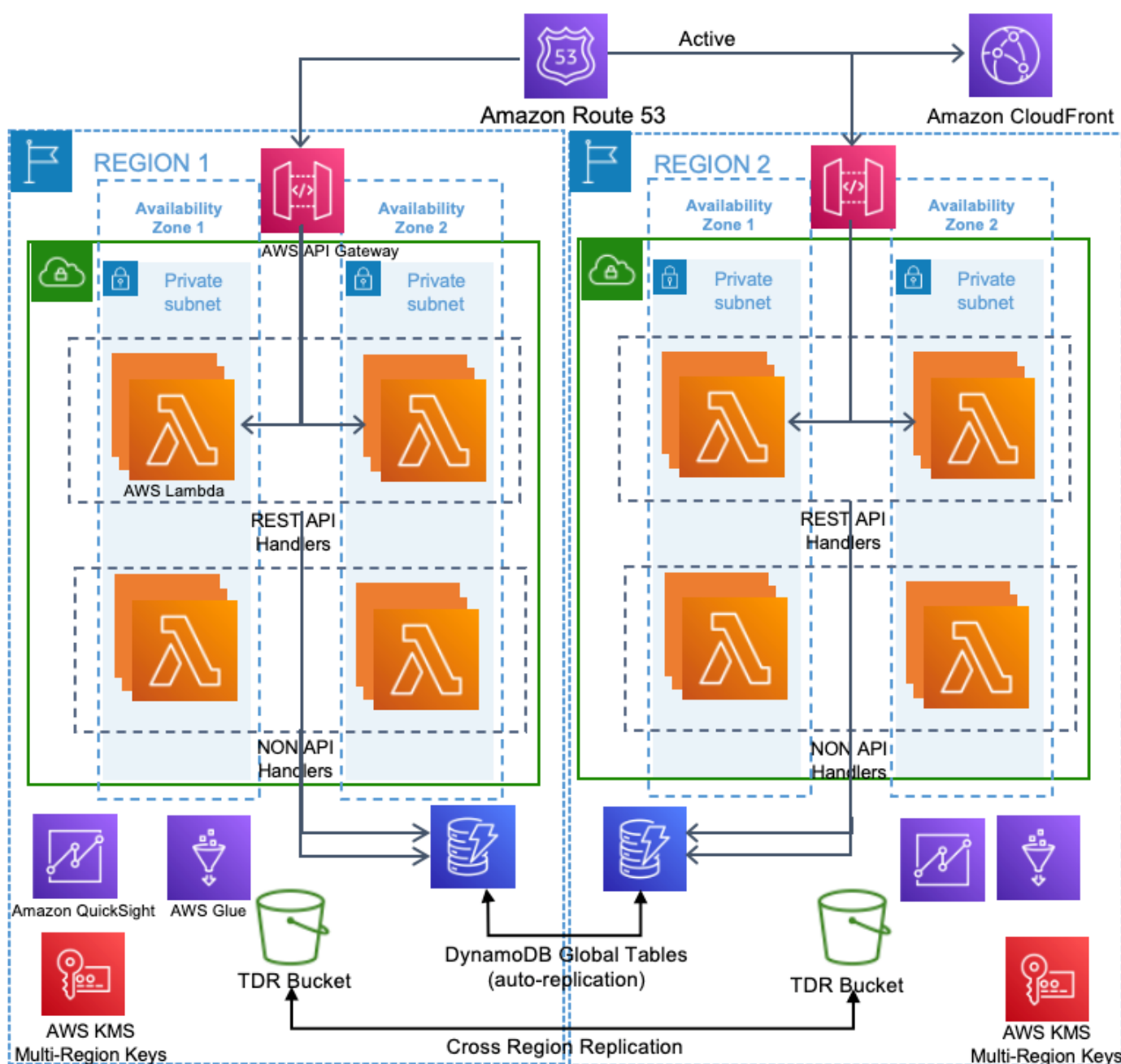


Figure 2. Control plane architecture

The following AWS services implement our control plane:

1. [Amazon API Gateway](#): Coupled with a custom authenticator, the API Gateway handles all the REST API credential verification and routing. Implementation of an API is transformed into implementing handlers for

each resource, which is the application core of the API.

2. [AWS Lambda](#): All the REST API handlers are written as Lambda functions. By using the Lambda's serverless and concurrency features, the application automatically gains self-healing and auto-scaling capabilities. There is also a significant cost advantage as billing is per millisecond of actual compute time used. This is significant for a control plane where usage is typically sparse and unpredictable.
3. [Amazon DynamoDB](#): A stateless architecture with Lambda and API Gateway, all persistent state must be stored in an external database. The database must match the resilience and auto-scaling characteristics of the rest of the control plane. DynamoDB easily fits the requirements here.

The customer portal, in addition to providing the user interface for control plane REST APIs, also delivers a rich set of user-customizable dashboards and reporting capability. Here again, the availability of various AWS services simplifies the implementation, and remains non-intrusive to the central call-transaction processing.

Services used here include:

1. [AWS Glue](#): Enables extraction and transformation of raw transaction data into a format useful for reporting and dashboarding. AWS Glue is particularly useful here as the data available is regularly expanding, and the use cases for the reporting and dashboarding increase.
2. [Amazon QuickSight](#): Provides all the business intelligence (BI) functionality, including the ability for Ribbon to offer separate author and reader access to their users, and implements tenant-based access separation.

Conclusion

Ribbon has successfully deployed Identity Hub to enable cloud hosted telephony services to mitigate robocalls. Telephony requirements around resiliency, performance, and capacity were not compromised. Identity Hub offers the benefits of a 24/7 fully managed service requiring no additional customer on-premises equipment.

Choosing AWS services for Identity Hub gives Ribbon the ability to scale and meet future growth. The ability to dynamically scale the service in and out also brings significant cost advantages in telephony applications where busy hour traffic is significantly higher than idle time traffic. In addition, the availability of global AWS services facilitates the deployment of services in customer-local geographic locations to meet performance requirements or local regulatory compliance.