WeDo Telecom RAID Risk Management Solution in the AWS Cloud

June 2018

Archived

This paper has been archived. For the latest technical content, see the AWS Whitepapers & Guides page: https://aws.amazon.com/whitepapers

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Archived

Contents

Introduction 1

Revenue Assurance Overview 1

WeDo Revenue Assurance Platform Overview 3

Solution Capabilities 3

Functional Solution Architecture 9

WeDo Revenue Deployment on AWS Cloud 11

AWS Services for Deploying WeDo Revenue Assurance Solution 11

AWS Architecture Principles for Deploying WeDo Revenue Assurance Solution 15

WeDo Revenue Assurance Solution Deployment Architecture on AWS 16

Benefits of Deploying WeDo Revenue Assurance solution in the AWS Cloud19

Conclusion 21

Contributors 21

Archived

Abstract

This whitepaper provides an architectural overview of how the WeDo Revenue Assurance Solution operates on the AWS Cloud. It is written for executive, architect, and development teams that need to make a decision to deploy a revenue assurance solution for their consumer or enterprise business on the AWS Cloud.

Archived

Introduction

In an increasingly competitive market, Communications Service Providers (CSPs) are being forced to quickly adapt to meet customer expectations and market trends by differentiating themselves from competition with innovative and attractive services and best-in-class customer experience. At the same time, declining prices are creating pressure to reduce costs, forcing CSPs to become leaner while continuing to deliver high quality service and run their business profitably. By implementing an agile data processing environment that includes operationalizing, auditing and optimizing processes, these challenges can be met at a lower cost.

WeDo Technologies' RAID platform is an end-to-end Risk Management software that lets CSPs focus on growing their businesses by putting risks under control. The platform is available both on-premises and in the cloud, delivering advanced solutions that successfully support and assure traditional services, such as voice and data, and also the release of next generation services supported by core telecom networks as they evolve towards Virtualization, Cloud and 5G.

Risk Management Overview

Revenue Assurance: Between delivering a service and collecting its revenues, there is a huge amount of hidden risks that can arise and influence a communications service provider's bottom-line.

Service Providers, on average, lose 1 to 3 percent of their revenue because of operational shortcomings. These values can be influenced by factors such as networks and service type, geography, carrier type, and Revenue Assurance maturity level.

To ensure that the services provided to customers are actually being billed and collected accurately, Service Providers need to implement an effective control system capable of enhancing their end-to-end Revenue Assurance processes that responds to their current and future needs. RAID Revenue Assurance is a software tool specifically designed to tackle the critical challenges across the entire revenue chain while increasing a Service Provider's maturity level.

Archived

With the deployment of RAID, Service Provider's gain additional insights during the identification, monitoring and correlation of the root cause analysis of their revenue leakages to accelerate the process of capturing earnings previously lost.

Fraud Management: Communications Service Providers (CSPs), already feeling the impact of fraud across dedicated networks for voice and data traffic as well as converged networks, will now be facing additional fraud challenges associated with Next Generation Networks (NGN). Since NGNs are responsible for the provisioning of ground breaking services, operators have been placed in the difficult position of dealing with a whole raft of unanticipated fraud scenarios. Operators cannot tackle these challenges using conventional fraud management systems (FMS) because they were not built for today's increasingly complex networks.

More suitable tools are needed to improve NGN fraud detection without abandoning previous network environments. WeDo Technologies' solution, RAID Fraud Management, addresses a whole range of fraud types across a wide variety of environments. It can either be integrated into RAID's Risk Management framework or used as a standalone solution to support fraud detection teams. When combined, RAID is able to create direct linkages between fraud and revenue assurance cases, accelerating the prevention of future risks and threats. The technology is powered by cross-functional data feeds that are capable of producing interdepartmental alarms and flagged behaviors that ultimately can be consolidated into actionable reporting, and capable of showing a 360° view of a company's business performance.

RAID Fraud Management not only tackles current known fraud patterns, but also protects CSPs against upcoming threats. RAID Fraud Management can be tightly integrated into a CSP environment and is capable of interacting with numerous systems.

Business Assurance: More than just looking at the revenue value-chain there is a set of business support processes within the CSPs that are critical to audit in order to ensure that a company keeps its costs under control. Along these processes we can include order provisioning, sales incentives or collections among others.

RAID Business Assurance near real time data integration and auditing capabilities make it possible to closely keep track of the accuracy of the business

Archived

and internal process, leading to a cost effective management. Today's management require to keep track of leading indicators like outsourcing control, margin assurance, financial control and resource management. With RAID Business Assurance it is possible to collect data from all management support systems to ensure that a company's internal processes are aligned with the defined targets.

In order to help CSPs keep costs under control RAID Business Assurance is continually reading, aggregating and validating data over the audited processes, analyzing transactions and triggering call for action when deviations are detected.

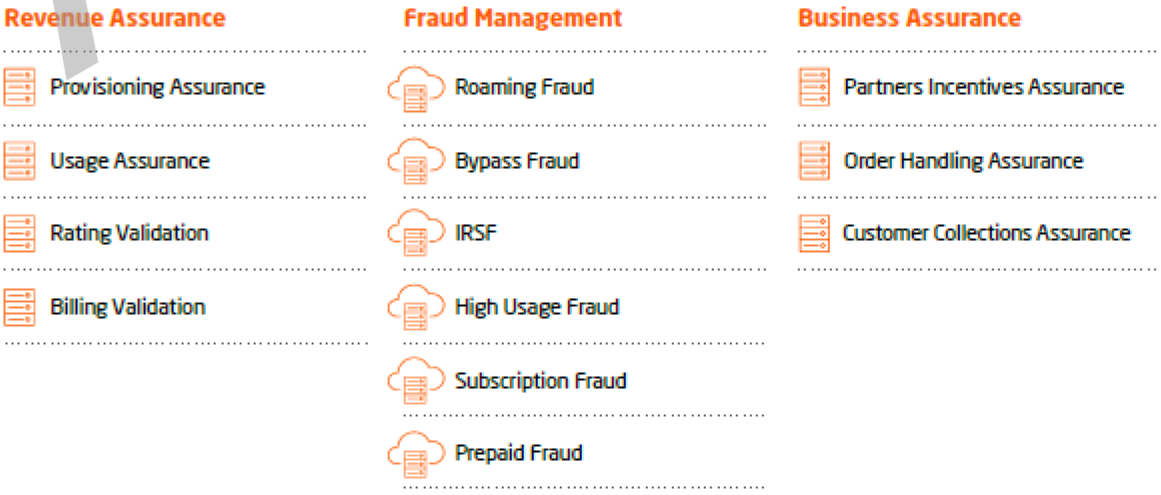
WeDo RAID Risk Management Platform Overview

Solution Capabilities

RAID is an all-in-one software that collects data across business applications and platforms to provide detailed monitoring of business activity to help improve corporate performance.

By providing the foundation for all your data integration, RAID removes the burden of maintaining silos of data sources, so you can run your operations safer, and make better business decisions to assure, manage and optimize your business.

RAID offers a modular approach to Risk Management with the following areas:



Revenue Assurance

- Provisioning Assurance
- Usage Assurance
- Rating Validation
- Billing Validation

Fraud Management

- Roaming Fraud
- Bypass Fraud
- IRSF
- High Usage Fraud
- Subscription Fraud
- Prepaid Fraud

Business Assurance

- Partners Incentives Assurance
- Order Handling Assurance
- Customer Collections Assurance

Archived

Additionally to the modular approach, the Risk Management solution can be configured to provide with customized validations tailored for specific needs of particulars CSP Operations.

Revenue Assurance

Provisioning Assurance: As CSPs scale their service portfolio, technology and subscriber base, their biggest challenge becomes the growing volume and complexity of orders which need to be provisioned during the activation and the deactivation of services and customers.

Main benefits may include:

- Detect errors arising from manual or automatic provisioning actions;
- Guarantee timely customer provisioning synchronization;
- Support the launch of new products and services;
- Reduce internal fraud;
- Maximize revenues with no delays in service delivery;
- Create a superior customer experience.

Usage Assurance: RAID's Usage Assurance modules collect session and signaling data from multiple measuring points along the revenue chain, and reconcile it using historical, cross-system and threshold validation rules, generating alarms that can be analyzed at detailed level by using RAID's Advanced Case Management features.

Main benefits may include:

- Guarantee that usage is accurately reflected in customer billing through control mechanisms that verify the flow of network events from the switch to their inclusion in the bill;
- Drill down into multiple view levels of the networks' xDR flows, giving access to high-level reports, KPIs, and aggregated views by service or revenue stream, as well as detailed CDR-level views for individual network elements;

Archived

- Frictionless data capturing from CSP’s multiple OSS/BSS systems and any additional endpoints.

Rating Validation: RAID Rating Validation module enables CSPs to control revenue leakage by efficiently tracking and correcting any underlying errors in the rating process. This module enables the deployment of a revenue assurance solution which validates rate plans configuration, rating charges, bundles, discounts and fees.

Main benefits may include:

- Automated and easy-to-use validation process that checks if rated records are correctly calculated according to the CSP rate plans;
- Matching tolerances and filters definition allow for control over which events should be validated and for the drilling down into calculations per independent CDR.

Billing Validation: RAID Billing Validation module is engineered to validate the accuracy of the customer invoicing process. This module ensures customer bills are fully validated for total expenditure, as well as for the total components of the invoice, by running independent external audits and verification procedures of the operators’ billing mechanisms. It compares the itemized invoices against the customer’s services and contracts, verifying billing data and customer invoice evolution according to the defined rules. Through the definition of thresholds and matching them against historical data, it can increase the accuracy of the billing cycle by looking at trend analysis.

Fraud Management

RAID provides with pre-built capabilities to monitor and detect the traditional technical fraud scenarios, such as: **Roaming Fraud, By pass, IRSF, High Usage, Subscription Fraud and Prepaid Fraud.**

Some examples of controls implemented in Fraud Management are:

Roaming Fraud controls:

Archived

- Evaluate traffic volume to identify high usage consumption or no to low traffic patterns;
- Identify traffic to known fraudsters through black list analysis;
- Apply specific rules and scores to visited and/or risky destination countries;
- Detect and be alerted to call collisions and roaming bypass.

Bypass Fraud controls:

- Evaluate traffic volume to identify high-usage consumption to a large number of different destinations;
- Identify call collision and call velocity above limit thresholds;
- Audit traffic to identify equipment serving multiple subscribers within short periods of time;
- Identify behaviors with deviations from expected usage or similar to known fraudsters.

IRSF controls:

- Evaluate traffic volume to specific international numbers to identify abnormal usage consumption;
- Identify behaviors with deviations from expected usage;
- Audit traffic to identify subscribers with multiple equipment and SIM replacements within short periods of time;
- Identify numbers with high similarity to known premium rate numbers.

High Usage Fraud controls:

- Audit all the traffic (on-net, national off-net, international or visitors) to identify abnormal usage related to large duration calls, high costs calls or high usage of SMS, data or voice services.

Subscription Fraud controls:

- Audit subscriptions list to identify multiple similar activations which may indicate fraudulent behavior;

Archived

- Audit new subscriptions with a high degree of similarity to known fraudsters.

Prepaid Fraud controls:

- Audit all recharges to identify a high number of occurrences, repeated recharges, unexpected recharge amounts and usage of scratch cards already used or not yet sold in the market.
- Identity account abuses related to unauthorized airtime transfers, unexpected changes in account balance and abnormal account type migrations.

Additionally to that, RAID Risk Management Solution can be configured with advanced analytics such as machine learning, predictive analysis, non-supervised models, etc. to broad and expend the reach of detection of suspicious activities.

Archived

Business Assurance

Partner Incentives Assurance: help to keep your sales force engaged and effective to ensure fraud and customer acquisition costs are kept to a minimum.

Main benefits may include:

- Assures that all relevant business data is received by Incentives System;
- Monitors to find human and system errors that generate increased costs;
- Assures that partner payments are correctly generated;
- Monitors partner disputes to detect abuse, including recurrent or rising conflict scenarios that generate large numbers of disputes, high dispute dollar amounts and resolution times;
- Detects fraud behavior that can damage a CSP’s image and high costs to fix if not detected earlier;
- Manages partners relations with a CSP and provides the tools to improve sales force engagement;
- Provides the tools to monitor the performance of incentives programs;

- Promotes pro-active and effective problem analysis;
- Centralizes within a single tool the management and resolution of issues detected by this process, and shares information between different operational and business teams;
- Tracks and measures Incentive issues;
- Measures the performance of CSP incentive processes and provides a set of out-of-the-box performance reports.

Customer Collections Assurance: enables CSPs to monitor your customer credit scoring process, along with your distinct collections and dunning strategies. It also measures the performance of internal and external debt recovery agencies.

Main benefits may include:

- Evaluates the credit risk for each subscriber including tracking credit scores, purchases and buying behavior over time;
- Monitors subscribers for credit fraud;
- Allows the collections team to evaluate the success of their collections strategy;
- Validates the eligibility rules used to create and assign debt packages to Data Collection Systems or to legal agencies;
- Provides a set of standard, out-of-the-box scoring, collections and debt recovery measures and KPIs, allowing the CSP to quickly evaluate the performance of their collections team;
- Measures the efficiency and accuracy of debt recovery and the associated commission plans.

Order Handling Assurance: focuses on achieving efficient order management, improving customer satisfaction and loyalty by reducing delays and back-orders, enhancing order accuracy and making communication easier. It validates all steps to guarantee order accuracy.

Main benefits may include:

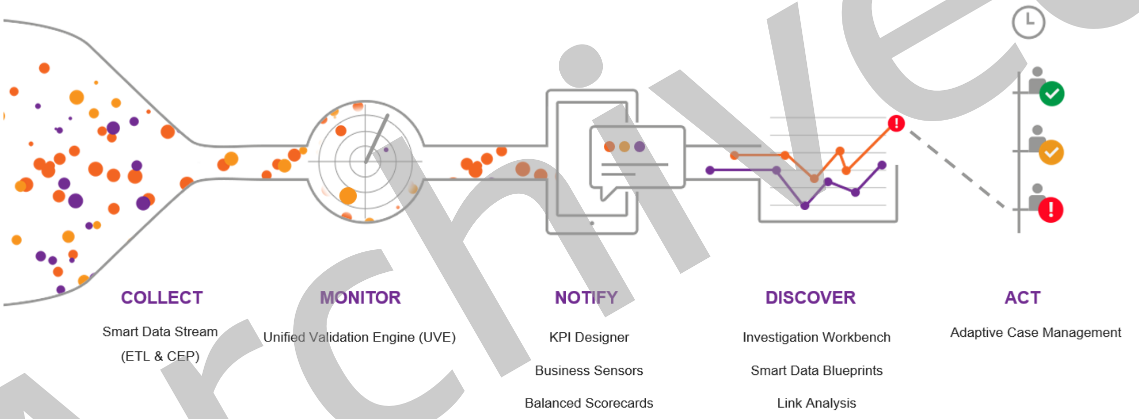
- Efficient order management with a minimum of delays and back-orders;

Archived

- Improved customer experience through on-time delivery, leading to greater customer satisfaction and loyalty;
- Improved order accuracy and communication among support teams;
- Identify provisioning flaws;
- Reduce order unfeasibility and identify potential backlog issues;
- Reducing costs by ensuring efficient allocation of resources.

Functional Solution Architecture

The solution capabilities described previously fit into a Functional Solution Architecture that can be divided into 5 major continuous steps:



Archived

The first step is **Collect**:

> To gain valuable insight into all the business applications data the solution uses WeDo's Smart Data Stream which is able to collect data stored in a great variety of file-based formats, relational databases and in Hadoop. This proven data integration solution has particularly developed for blending and enriching vast volumes of telecom data.

The second step is to **Monitor**:

> While collecting data from multiple sources the solution monitors it supporting full alarm traceability from the instant an alarm is triggered, to the validation and application of business rules. The WeDo's Unified Validation Engine keeps these business rules which are provided "out-of-

the-box" but can also be easily configured and managed through a visually intuitive rule designer that supports specific user profiles. Since the ETL is fully integrated with this rules engine the solution is able to deliver accurate and auditable results.

The third step is to **Notify**:

The solution provides dashboards and reports that can quickly provide understanding of what needs attention, which alerts need to be tracked and which tasks require follow-up. This visual experience is able to combine data sources, add filters and drill down into specific information with just a few clicks either users accessing it through a desktop PC, tablet or smartphone.

The fourth step is to **Discover**:

WeDo's Data Model and analytics tools enable business analysts, using self-service tools, to explore and visualize data and investigate deeper drilling-down for root cause analysis and for gaining real business insight. Users are able to access the business logic used and have instant access to data from internal and external sources stored in relational databases, Hadoop and NoSQL systems.

The fourth step is to **Act**:

With WeDo's Adaptive Case Management it's easy to allocate tasks across the business and quickly investigate and analyze cases for faster, more accurate decisions. It also enables teams to gather supporting evidence and compile ad-hoc or standard reports. The Adaptive Case Management also allows for easy tracking of all case activity and history through a case timeline. It also simplifies defining SLAs and escalation paths.

Archived

WeDo RAID Deployment on AWS Cloud

AWS Services for Deploying WeDo RAID Risk Management Solution

This section describes the AWS infrastructure and services that you need to run the WeDo RAID Risk Management platform on AWS.

Regions and Availability Zones

Each AWS Region is a separate geographic area that is isolated from the other Regions. Regions provide you the ability to place resources, such as Amazon Elastic Compute Cloud (Amazon EC2) instances and data in multiple locations. Resources aren't replicated across Regions unless you do so specifically.

An AWS account provides multiple Regions so that you can launch your applications in locations that meet your requirements. For example, you might want to launch your applications in Europe to be closer to your European customers or to meet regulatory requirements.

Each Region has multiple, isolated locations known as Availability Zones. Each Availability Zone runs on its own physically distinct, independent infrastructure and is engineered to be highly reliable. Common points of failure, such as generators and cooling equipment, aren’t shared across Availability Zones. Each Availability Zone is isolated, but Availability Zones within a Region are connected through low-latency links.

For more information about Regions and Availability Zones, see Regions and Availability Zones in the *Amazon EC2 User Guide for Linux Instances*.[1]

Amazon Route 53

Amazon Route 53 provides highly available and scalable Domain Name System (DNS), domain name registration, and health-checking web services. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to internet applications by translating names like *example.com* into the numeric IP addresses, such as *192.0.2.1*, that computers use to connect to each other. You can combine your DNS with health-checking services to route traffic to healthy endpoints or to independently monitor and/or alarm on endpoints. You can also purchase and

Archived

manage domain names such as *example.com* and automatically configure DNS settings for your domains. Route 53 effectively connects user requests to infrastructure running in AWS – such as Amazon EC2 instances, Elastic Load Balancing load balancers, or Amazon S3 buckets – and can also be used to route users to infrastructure outside of AWS.

Amazon Elastic Compute Cloud

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud that is billed by the hour. You can run virtual machines (EC2 instances) ranging in size from 1 vCPU and 1 GB memory to 128 vCPU and 2 TB memory. You have a choice of operating systems including Windows Server 2008/2012, Oracle Linux, Red Hat Enterprise Linux, and SUSE Linux.

Elastic Load Balancing

Elastic Load Balancing (ELB) automatically distributes incoming application traffic across multiple EC2 instances in the cloud. It enables you to achieve greater levels of fault tolerance in your applications, seamlessly providing the required amount of load balancing capacity needed to distribute application traffic. You can use Elastic Load Balancing for load balancing web server traffic.

Amazon Elastic Block Store

Amazon Elastic Block Store (Amazon EBS) provides persistent block-level storage volumes for use with EC2 instances in the AWS Cloud. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, thereby offering high availability and durability. EBS volumes offer the consistent and low-latency performance needed to run your workloads.

Amazon Machine Image

An Amazon Machine Image (AMI) is a packaged-up environment that provides the information required to launch your EC2 instance. You specify an AMI when you launch an instance, and you can launch as many instances from the AMI as you need. For more information on AMIs, see the Documentation.[2] Amazon EC2 uses Amazon EBS and Amazon S3 to provide reliable, scalable storage of AMIs so that we can boot them when you ask us to do so.

Archived

Amazon Simple Storage Service

Amazon Simple Storage Service (Amazon S3) provides developers and IT teams with secure, durable, highly-scalable object storage. It provides a simple web services interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web. With Amazon S3, you pay only for the storage you actually use. There is no minimum fee and no setup cost.

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud in which you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own private IP address range, creation of subnets, and configuration of route tables and network gateways. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to EC2 instances in each subnet. Additionally, you can create a hardware virtual private network (VPN) connection between your corporate data center and your VPC, and then you can leverage the AWS Cloud as an extension of your corporate data center.

Amazon Relational Database Services

Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks.

AWS CloudTrail

With AWS CloudTrail, you can monitor your AWS deployments in the cloud[3] by getting a history of AWS API calls for your account, including API calls made via the AWS Management Console, the AWS SDKs, the command line tools, and higher-level AWS services. You can also identify which users and accounts called AWS APIs for services that support CloudTrail, the source IP address the calls were made from, and when the calls occurred. You can integrate CloudTrail into applications using the API, automate trail creation for your organization, check the status of your trails, and control how administrators turn CloudTrail logging on and off.

Archived

AWS CloudFormation

AWS CloudFormation provides a common language for you to describe and provision all the infrastructure resources in your cloud environment. CloudFormation allows you to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. This file serves as the single source of truth for your cloud environment.

AWS CloudFormation is available at no additional charge, and you pay only for the AWS resources needed to run your applications.

AWS Direct Connect

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your data center, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections.

AWS Security and Compliance

The AWS Cloud security infrastructure has been architected to be one of the most flexible and secure cloud computing environments available today.[4] Security on AWS is similar to security in your on-premises data center, but without the costs and complexities involved in protecting facilities and hardware. AWS provides a secure global infrastructure, plus a range of features that you can use to help secure your systems and data in the cloud. To learn more about AWS Security, see the AWS Security Center.[5]

AWS Compliance enables you to understand the robust controls in place at AWS to maintain security and data protection in the cloud. AWS engages with external certifying bodies and independent auditors to provide you with extensive information regarding the policies, processes, and controls established and operated by AWS. To learn more about AWS Compliance, see the AWS Compliance Center.[6]

Archived

AWS Architecture Principles for Deploying WeDo Revenue Assurance Solution

The WeDo Revenue Assurance Solution (also designated as RAID) at the technical level is mainly composed of:

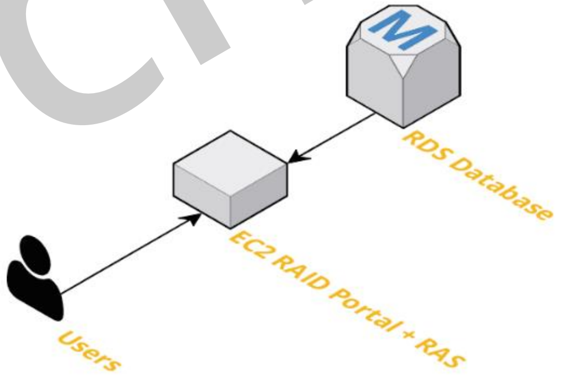
- a RAID Portal module
- one of more RAID Revenue Assurance Solution (RAS) modules
- a common database

The RAID Portal module, running on an Amazon EC2 compute instance, provides all the web-based interaction needed to configure, visualize and manage all the RAID Revenue Assurance Solution functionality.

The RAID Revenue Assurance Solution modules, running on Amazon EC2 compute instances, specifically handle each of the Revenue Assurance functionalities.

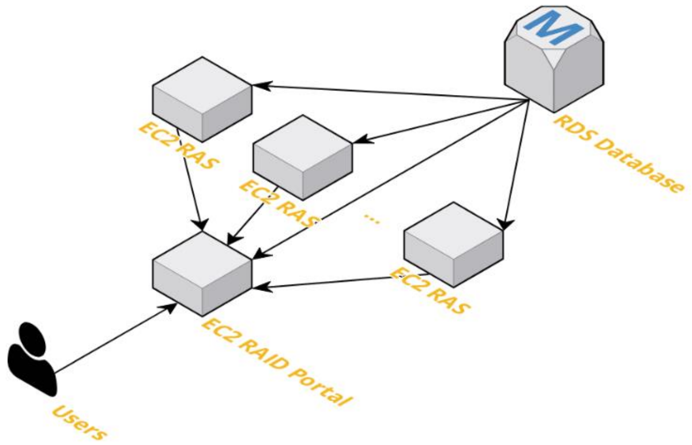
Both the RAID Portal as the RAID Revenue Assurance Solution modules use AWS based databases (like the AWS RDS).

Using these components the bare minimum simplified architecture, for a basic environment, could be composed of a single EC2 instance running the RAID Portal and a RAS module (Revenue Assurance Solution module):



Since more than one RAS module and other WeDo RAID based solutions can be combined on the same environment, the architecture can grow to have multiple RAS modules running on multiple EC2 instances for which access is centralized through the RAID Portal EC2 instance:

Archived



The RAID Portal offers a single user transparent point of entry for all RAID modules that become seamless to all team users.

WeDo RAID Risk Management Solution Deployment Architecture on AWS

To deploy RAID in AWS, WeDo recommends having, at least, three environments:

- **Development**
  Where all the solution configuration will be developed through the web-based GUI including incremental additions (e.g. Agile team)
- **Testing**
  Where the solution configuration and any change goes through quality checks.
- **Production**
  Where the solution configuration actually monitors and controls real data and end-users interact with the solution through the web-based GUI.

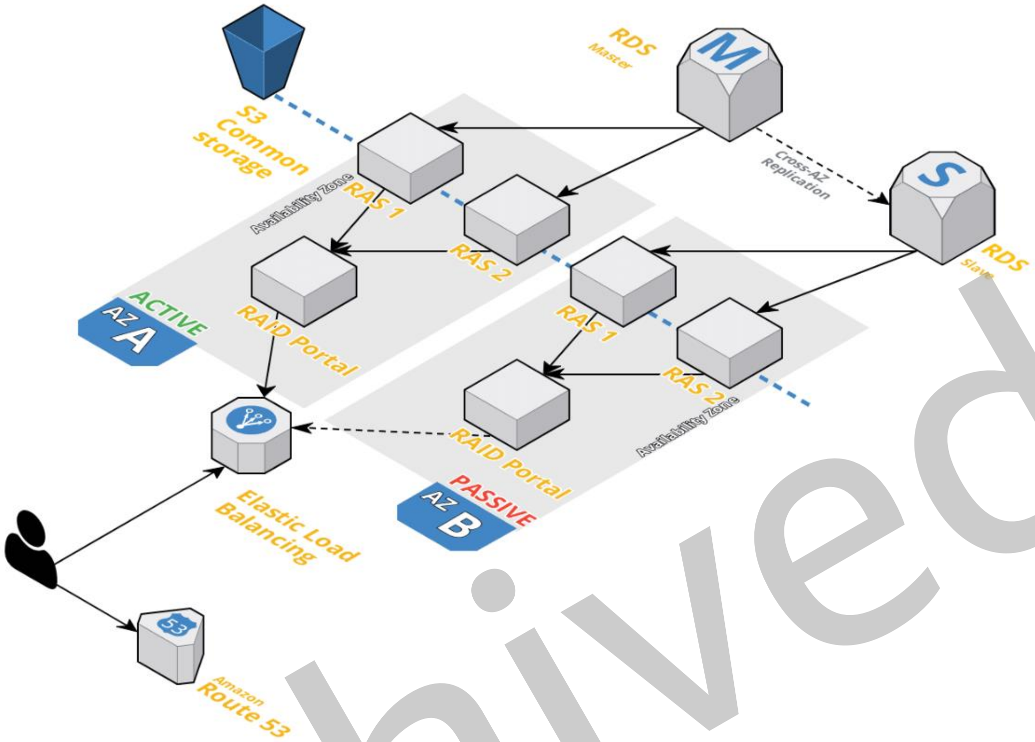
Depending on each case requirements, a simple or more complex AWS architecture can be required. WeDo recommends:

Archived

- Each environment should have its own separate AWS VPCs for isolation.
- Each environment should be only accessible through a VPN service ensuring private connectivity between the VPC and customer networks.
- AWS Security Groups should enforce restricted access to the several architecture components (RAID Portal, RAID RAS modules and Database). Keep in mind that end-users only need access to the RAID Portal and pretty much all of the solution functionality is accessible through web-based GUI.
- The EC2 compute instances should be EBC-backed.
- The production architecture should use multi availability zones for fault tolerance.
- Use AWS RDS instances for the database (using Multi-AZ for production architectures).
- Use AWS S3 service for storing shared data files between RAID RAS modules, log files and other operational related files (with VPC endpoints for private access)
- Use AWS CloudWatch for performance monitoring of each architecture component.
- Deploy a private domain using Amazon Route 53 and configure the inter-connection between architecture components by host names that should be equivalent between environments.

Archived

Given some of the recommendations, a production architecture might look like this:



Sample RAID RAS Platform Deployment Dimensioning

The sizing of a RAID RAS Platform Deployment depends on several variables driving both AWS EC2 compute instance types and volume storage requirements depending on your specific customer needs. For example, storage is largely dependent on data retention time period both for legal as well as business requirements. We recommend that you contact your WeDo team for a more accurate environment architecture dimensioning.

The following is a simple sample dimensioning assuming:

Generic sizing parameters	Value
Monitored Control Points	20
Number of concurrent users	10
Amount of xDRs per day	10 million

Archived

Number of subscribers	2 million
Retention period	Up to 90 days

Which would result on a sample dimensioning for AWS:

Component	AWS Instance Type	OS or DB	Volume Storage Type	Volume Type	Volume Storage (GB)
RAID Portal + RAID RAS	m4.large	RHEL	EBS	General Purpose (SSD)	55
Database	db.m4.large	RDS DB (Oracle 12c EE)	EBS	General Purpose (SSD)	529

The numbers and sizing listed above were meant to demonstrate a general approach to dimension the amount of resources required in AWS Cloud environment and may change according to the CSP needs and requirements.

Benefits of Deploying WeDo RAID Risk Management solution in the AWS Cloud

There are many benefits of deploying the WeDo RAID Risk Management solution on AWS:

Lower total cost of ownership – In an on-premises environment, it is typically necessary to pay for hardware, hardware support costs, virtualization licensing and support, and data center costs, including floor space, electricity, etc. These costs can be eliminated or dramatically reduced by moving to AWS. Benefits include economies of scale and efficiencies provided by AWS. You only pay for the compute, storage, and other resources that you use.

Cost savings for nonproduction environments – WeDo Revenue Assurance on AWS enables you to shut down nonproduction environments when they are not being used in order to save costs. For example, if a

Archived

development environment is used for only 40 hours a week (8 hours a day, 5 days a week), you would only pay for 40 hours of Amazon EC2 compute charges, as opposed to 168 hours based on 24/7 usage in an on-premises environment. This represents up to a 75% savings.

Replace CapEx with OpEx – You can implement an RAID BSS solution or project on AWS without any upfront cost or commitment for compute, storage, or network infrastructure.

Unlimited environments – An on-premises environment usually provides a limited set of environments to work with—provisioning additional environments can take a long time or might not be possible. With AWS, you can create virtually any number of new environments in minutes as required.

In addition, you can create separate environments for each major project, thereby enabling each of your teams to work independently with the resources they need. Teams can subsequently converge in a common integration environment when they are ready. At the conclusion of a project, you can terminate the environment and cease payment.

Right size anytime – Customers often over-size on-premises environments for the initial phases of a project, but are subsequently unable to cope with growth in later phases. With AWS, you can scale your compute usage up or down at any time. You pay only for the individual services you need, for as long as you use them. In addition, you can change instance sizes in minutes through the AWS Management Console, the AWS Application Programming Interface (API), or Command Line Interface (CLI).

Low-cost disaster recovery – You can build low-cost standby disaster recovery environments for existing deployments. Costs are incurred for the duration of any outage that occurs.

Ability to test application performance – Although performance testing is recommended prior to any major change to an RAID BSS solution environment, most customers only performance test their RAID BSS application during the initial launch in the yet-to-be-deployed production hardware. Later releases are usually never performance tested due to the expense and lack of environment required for performance testing. AWS minimizes the risk of discovering performance issues later in production. You can create an AWS Cloud

Archived

environment easily and quickly just for the duration of the performance test and only use it when needed. You are charged only for the hours the environment is used.

Simple integration from RAID to AWS Cloud for analytics and machine learning – RAID platform offers rich product and service management capabilities which can be integrated with AWS Cloud Analytics for use cases such as subscriber, customer, and usage analytics. These can then be used for various loyalty and retention programs leveraging machine learning models on AWS Cloud using services like Amazon SageMaker.

No end of life for hardware or platform – All hardware platforms have end-of-life dates, at which point the hardware is no longer supported and you are forced to purchase new hardware again. AWS requires only a simple upgrade of your platform instances to new AWS instance types (via a single click) without incurring any cost.

Conclusion

RAID is de platform developed by WeDo Technologies for Risk Management Solution and provides out-of-the-box capabilities to monitor the CSPs revenue and cost chains as well as detect fraud threats to support the organization strive in operational efficiency. RAID also includes advanced analytics capabilities implementing machine learning, predictive analysis and non-supervised models to capture suspicious activities that wouldn’t be possible to detect otherwise using traditional supervised monitoring.

RAID is AWS Cloud ready and have many success cases where the CSPs can leverage all the benefits AWS offers on having applications deployed in the cloud including security & compliance making it possible to handle sensitive customer information required to further operate the Risk Management practice.

Archived

Contributors

The following individuals and organizations contributed to this document:

- Nuno Miguel Aguiar, Team Lead – Professional Services, WeDo Technologies

- Andre Thomaz, Engagement Manager – Business Consulting, WeDo Technologies
- Robin Harwani, Strategic Partner Solutions Lead – Telecoms, Amazon Web Services

About WeDo Technologies

Founded in 2001, is the market leader in Revenue Assurance and Fraud Management software solutions to Telecom, Media and Technology organizations worldwide.

WeDo Technologies provides software and expert consultancy across +105 countries, through a +600 network of highly skilled professional experts, present in the US, Europe, Asia-Pacific, Middle East, Africa, Central and South America.

WeDo Technologies' software analyzes large quantities of data allowing to monitor, control, manage and optimize processes, ensuring revenue protection and risk mitigation.

With over 180 customers - including some of the world's leading blue chip companies – WeDo Technologies has long been recognized as the constant innovator in assuring the success of its customers along a journey of continuous transformation. For more information, please visit http://www.wedotechnologies.com/

Notes

[1] http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

[2] https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html

[3] https://aws.amazon.com/what-is-cloud-computing/

[4] https://d0.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf

[5] https://aws.amazon.com/security/

[6] https://aws.amazon.com/compliance/

Archived