

Mortgage bank transforms their cloud with AWS

Well-Architected Review

Every IT project accrues technical debt. Even the best engineering teams sometimes take shortcuts, resulting in waste and complexity. Cloud cost management can be challenging—are you spending too much? Are migrations taking longer than expected? Are you confident that you can meet your audit requirements?

A mortgage bank recently reviewed its AWS account and used this evaluation to fuel a rebuild of its entire AWS environment. As a result, they improved their PCI-DSS compliance and reduced application outages.

Background

A prominent mortgage bank initially started running on AWS Cloud with one or two small projects. Now several years later, the bank spends tens of thousands of dollars on AWS -- but since the account grew haphazardly in fits and starts by different cloud engineers with different requirements, they have little confidence that their account meets basic AWS best practices.

Their environment consisted of hundreds of instances, both Spot and On-Demand, which supported two core applications that needed to maintain Gramm-Leach-Bliley Act (GLBA) and Payment Card Industry (PCI-DSS 3.0) compliance. However, only some projects had sufficient access controls and backups, and their testing and code deployment processes were completely disorganized. All of this complexity meant that they had a 4-hour SLA and frequent application outages. When something went wrong, there were so many interdependent services that their IT team had to rebuild entire portions of their environment from backups.

The company knew that large portions of their environment had also "fallen out" of compliance. This isn't unusual; a recent study found that nearly 45% of companies fall out of PCI-DSS compliance within 9 months of certification.

As a result of this waste and mismanagement, they had not expanded their AWS usage by moving other applications to AWS. They understood that these architectural deficiencies were due an AWS skills gap, rather than gaps in the AWS services themselves.



"45% of companies fall out of PCI-DSS compliance within nine months of certification."

Source: Verizon



AWS Well-Architected

The company decided to seek out an AWS cloud expert to remediate their AWS account in accordance with AWS Well- Architected and Well-Operated Frameworks and take over long-term management. The Well-Architected Framework is a system of cloud best practices designed by AWS, based on their experience across millions of customers.

It includes five "pillars":

- > Operational Excellence
- > Cloud Security
- > Reliability
- > Performance Efficiency
- > Cost Optimization



The AWS Well-Architected Framework provides a single source of cloud architecture best practices for your team.

The Well-Architected Framework provides a single source of cloud architecture best practices for your team, so that each environment is maintained in a secure, efficient manner. It's the principle that AWS uses to evaluate architectures -- and the system that AWS uses to train and audit RapidScale to conduct reviews.

The mortgage bank approached RapidScale and quickly identified us as their desired managed services provider due to our staff of AWS certified and tenured engineers, pedigree in Financial Services, and flexible service tiers. The company wanted to rebuild their existing AWS environments in accordance with AWS best practices and PCI-DSS compliance standards, and supplement their internal AWS resources with a focus on operational support, DevOps automation, and cloud cost management.

Review and Rebuild

Within weeks, RapidScale' Certified AWS Engineers conducted a comprehensive review of the organization's existing AWS environment. This involved a series of interviews with the company's engineers, a hands-on evaluation of their account, and a review of available documentation and team processes.

As a result of this review, RapidScale produced a report that outlined the company's current state in terms of meeting the five pillars of the AWS Well-Architected Framework, and specific technical recommendations for improving their environment.

The gaps in their current environment were so extensive that the company decided to completely rebuild their AWS environment (while keeping their current AWS environment active), and conduct the cloud migration to the new AWS environment once complete. This resulted in a new architecture design produced in just 2 weeks according to AWS best practices, including specific technical features such as:

- › Hub-spoke AWS VPC architecture
- › CIS hardened AWS EC2 AMIs
- › Mature, easily replicated/destroyed code testing and deployment environments
- › Multi-factor authentication (MFA) on Bastion, AWS Console
- › AWS Key Management Service (KMS) for encryption of RDS, EBS, S3, etc.
- › Regular patching timetable and process
- › AWS log collection via CloudTrail logs
- › TrendMicro Anti-Virus for Linux, Windows Defender for Windows Server 2016
- › AWS CloudWatch Detailed Monitoring with best practice thresholds
- › Active Directory (AD) configuration and maintenance
- › AWS ElasticBeanstalk for application delivery
- › MS SQL on EC2 with License Mobility through Software Assurance

All architectures are deployed using AWS CloudFormation templates for easy repeatability, and the Management VPC includes RapidScale proprietary Central Automation Platform, which contains "bots" and scanners that enforce security configurations and best practices (built in AWS EC2 Systems Manager, Lambda, Inspector, Config, Puppet, and Jenkins). After build out in CloudFormation, all instances receive their configuration (including 3rd party security tools, packages, log configurations, etc.) from Puppet, which ensures that configurations are consistently implemented and maintained. This has a significant impact on the bank's compliance goals; they are now able to demonstrate to auditors that every instance continually "checks in" to a central manifest and thus is always in a "known good" state.

Result

After build-out, RapidScale and the mortgage bank collaborated on extensive cloud reliability and cloud security testing. The platform launched in production in July 2017, just 60 days after the initial design phase, and RapidScale now offers 24x7 cloud monitoring, ticket support, patching, updates, and select benefits of AWS Enterprise Support. As a result of working with RapidScale, the mortgage company is confident in their AWS Cloud architecture — and ready to move more workloads to AWS.

About RapidScale

Whether refreshing legacy IT systems or launching an app that will reach millions, RapidScale empowers your business with a complete set of private and public cloud solutions to simplify IT and unleash innovation.

From Infrastructure as a Service to AI, RapidScale brings you the best portfolio of managed services in the industry, backed by a deep bench of certified experts holding over 400 accreditations. RapidScale has helped hundreds of customers migrate to AWS and Azure while helping over 2000 customers drive the complexity and administration out of IT. **RapidScale makes technology your biggest competitive advantage.**

Speak to a RapidScale cloud expert today: meet@rapidscale.net