Success Story
Data Center Security

Enforcing S3 encryption with AWS Config and Lambda

ANM helped a financial services firm maintain strict compliance standards using AWS Config for simplified, automated monitoring and reporting, including custom exemptions.

Client Challenge

Financial services companies have the most stringent security and compliance requirements and are subject to the scrutiny of ongoing security audits. As a result, the security team must prove compliance frequently, across many areas.
One such requirement is the encryption of all data at rest. In this particular case, our client's public cloud storage solution, AWS S3 buckets, required encryption with a customer-owned key management service (KMS). However, certain 'public access' information did not require the same encryption and therefore needed to be excluded from the non-compliance report.

ANM Solution

Following a thorough on-site assessment with the client, ANM developed and deployed a centralized AWS Config solution to monitor compliance of all AWS S3 buckets. To accommodate public access information that did not require encryption, ANM configured a fully managed NoSQL database service, DynamoDB, with S3 exemptions. The solution also employed an AWS Rule Development Kit (RDK) to build and deploy the Config rules across multiple accounts and regions.

For the compute stage, ANM developed custom logic for AWS Lambda, supporting the Config rule to check encryption on each bucket, excluding exemptions, then report the compliance status back to corresponding bucket. If a bucket is marked as non-compliant, the Lambda function will automatically enable encryption (unless it is marked as exempt). The centralized account then aggregates the results to show the overall level of compliance for simplified, automated reporting.

Customized Approach

AWS Config

Because the client needed a detailed view of S3 encryption across buckets, as well as the ability to perform audits, ANM concluded that AWS Config was an ideal fit. The solution leveraged AWS Config to assess, audit and evaluate compliance of specified AWS resources. The trigger type of the AWS Config rule was set as 'configuration changes' to ensure reporting was as accurate as possible. Due to the complex requirements of the environment, ANM took advantage of the multi-account, multi-region data aggregation capabilities. Using the AWS Config Rule Development Kit (RDK) allowed ANM to manage the rules at scale. Management was done from a designated 'compliance account,' which contained an aggregated compliance view across all accounts. This enabled the client to easily report and track historical levels of encryption compliance.

Monitoring

With governance, compliance and auditing functionality already enabled with AWS CloudTrail, the client had existing account activity logged across each account. Those logs were sent to Amazon CloudWatch, then passed to the centralized account using an EventBus. With accurate monitoring in place, ANM focused on the necessary logic to properly configure the AWS Config rules.

Scripting

Using a 'compliance account,' the client is now able to manage the Config rule logic in one central place. Seeing that the built-in S3 encryption rule didn't quite match their needs, ANM customized a Config rule using a Lambda function. ANM used Python language and a developed a script to gather a list of unencrypted data across all accounts and regions. Keeping in mind that certain buckets of public access data were exempt from encryption requirements, the solution compares this list to a DynamoDB table of excluded buckets. The remaining buckets are then reported to AWS Config as non-compliant.

Infrastructure as Code

ANM knew that Infrastructure as Code (IAC) is always the prescribed approach when designing solutions in AWS. Its agility, repeatability and efficiency make it a paradigm-changing approach. Many AWS services use AWS CloudFormation behind-the-scenes to deploy various services. In this case the AWS RDK used CloudFormation to deploy the custom Config rules and corresponding Lambda function.

Security

For the strictest security standards, ANM used AWS Identity and Access Management (IAM). IAM allows users to access AWS resources through the management console programmatically and grants role-based access to entities and services, among many other things. It also possesses a very controllable level of granularity using customer-managed and AWS-managed policies. In this particular case, IAM was used to provide cross-account access to analyze S3 buckets outside of the centralized account. An existing role in the target accounts was used to perform any actions the Lambda required.

Benefits

Increased financial compliance and simplified reporting

Automated encryption functionality

Centralized IT configuration and administration

Customized policy exemptions for public access information

Robust security protocols, including role-based access and customer-managed granularity

The Results

Using our four-step solution methodology, ANM completed the project on time and on budget, in tandem with other high-priority projects. The automated nature of this solution also ensures that newly created accounts do not require additional deployment efforts.

About ANM

ANM's dedicated team of professionals provides innovative solutions and expert local service to large and mid-sized clients in markets throughout the U.S. The company designs, implements and supports IT solutions from industry-leading technology providers including Cisco, AWS, Pure Storage, VMware, Splunk and F5.

ANM is headquartered in Albuquerque with additional offices in Denver, Colorado Springs, Boise, Scottsdale and El Paso. A recognized leader in the IT industry, the firm enjoys a 98.6% customer satisfaction rating as well as excellent employee and customer retention rates.

anm

We'd love to hear from you.

☎ (866) 527-8822 ✉ info@anm.com anm.com