Success Story
A Western State Governor's Office of Information Technology (OIT)

Monitoring automation using CloudWatch, CloudTrail, and Lambda

This western state Governor's Office of Information Technology (OIT) strives to improve the lives of all people to create a safer, happier and healthier state. Using technology to drive sustainable and intelligent business decisions, the group envisions a future where user experience will shape design and data analytics will transform how state government serves its residents.

Challenge

ANM has been a trusted partner for OIT since 2014, helping the group address networking, security and data center issues. ANM has also assisted OIT with standardization and architectural guidelines for consumption of AWS services. OIT engaged ANM to automate many of the standards defined in the architectural guidelines project and provide support for AWS adoption.

OIT needed to deploy CloudWatch alarms for all of its newly created Amazon Elastic Compute Cloud (EC2) instances in a consistent way. The group was already creating infrastructure as code (IaC) using CloudFormation, so ANM proposed a solution that would leverage Lambda automation (packaged inside of a template) that could be passed through necessary parameters specific to each account. This would give OIT the flexibility and portability to deploy a solution in multiple regions as well as across multiple accounts with a single template.

ANM Solution

ANM worked with OIT to develop a set of Python-based Lambda functions that were triggered by CloudWatch events to deploy a predefined set of CloudWatch alarms. The functions and triggers were all deployable with CloudFormation, allowing different teams to utilize the solution in multiple accounts. The solution was set up to handle deletion of alarms upon termination of EC2 instances. A separate standalone Python script was also included as a one-time solution to add the same CloudWatch alarms to existing EC2 instances.

Monitoring/Alerting

OIT needed to ensure its instances were being properly monitored without having to worry about manually configuring things individually with each deployment. Due to the nature of the EC2 instance workloads, it was important to monitor the CPU Utilization and generate the proper alerts to business owners. A combination of CloudWatch and Amazon Simple Notification Service (SNS) gave OIT a powerful and effective solution.

Using the built-in monitoring of CloudWatch, ANM was able to easily track compute without the need to for configuring the agent on the instances. Although not necessary in this case, the CloudWatch agent could have been included for tracking memory usage. Additionally, ANM utilized existing CloudTrail logging to monitor for API calls of creation and deletion of instance and filtered those results with CloudWatch. When a CloudWatch alarm would be triggered, it would notify the proper business owners using Amazon SNS. At instance creation, the CloudTrail API call would produce a CloudWatch event that would trigger the Lambda function. At this point, the CloudWatch alarms would be created for the new instance without any manual intervention. Deletion followed a similar pattern, essentially being triggered by the API deletion record in CloudTrail.

Scripting

Handling the creation of alarms in an automated fashion was done by using a Lambda function. This function would be triggered by CloudWatch events that were generated by CloudTrail API calls. The Lambda function's Python runtime environment employed the AWS SDK (boto3) to interact with the AWS API to query, create and delete resources.

Infrastructure as Code

IaC provides many benefits, such as being a single source of truth for infrastructure, allowing automated and consistent deployment of resources, automatic rollback capability, and the ability to use version control solutions such as CodeCommit or GitLab. Using a script to build your infrastructure is much faster than having to manually provision resources, and far less error prone.

Being AWS's go-to solution for IaC and, as mentioned earlier, a tool that OIT had previous experience with, CloudFormation was a natural choice. It is versatile language-wise (JSON and YML are both acceptable), it has a much more direct way of performing API calls to AWS services it provisions than third-party tools and it's more approachable overall than other solutions. In this case, CloudFormation initially deployed the Lambda functions (both the new instance and existing instance functions) as well as CloudWatch events that reported new instances being spun up, SNS for notifying relevant stakeholders and the prerequisite IAM role for Lambda to execute with.

Security

Identity Access Management is an extremely powerful tool for controlling access to AWS assets. In this case, ANM utilized IAM roles assigned to Lambda to perform the tasks it needed to execute. The policies attached to the roles followed the principal of least privilege, ensuring that Lambda had just as much access as it needed but nothing more.

Additional Tools

Taking advantage of GitLab, the OIT team was able to keep its source code in a single repository for collaboration and necessary modifications. GitLab version control allowed the group to track changes over time and easily revert their code to a previous state if needed. With multiple engineers managing multiple accounts, this repository made it easy for the OIT team to easily access the necessary files and update the accounts as needed without the time-consuming process of trying to locate the source files. This enabled them to have a secure and flexible method of managing code.

About ANM

ANM is one of the fastest growing IT consulting companies in the U.S. with a strong local focus. When you need assistance, we show up with a problem-solving attitude and a mind for innovation. We're great communicators when it comes to assessing your needs and laying out your options. We also carry the highest levels of engineering certifications and recognitions from industry-leading manufacturers like Cisco, VMware, AWS, Splunk and F5.

BENEFITS

The implementation was delivered and easily met the proposed timeline. Utilizing a Python script to manage the previously deployed instances let ANM focus on a solution for how new instances would be handled without adding code to the Lambda function. This kept the function streamlined for this particular use case. OIT now has consistent, comprehensive and automatic deployment of CloudWatch Alarms for all newly created EC2 instances. They can rest assured that all their instances are being watched carefully by CloudWatch and that the appropriate personnel will be notified with any issues. This automation allows administrators to deploy instances and benefit from CloudWatch's built-in monitoring and alarms, without having to understand or specify how it works.

anm

We'd love to hear from you.

☎ (866) 527-8822 info@anm.com anm.com