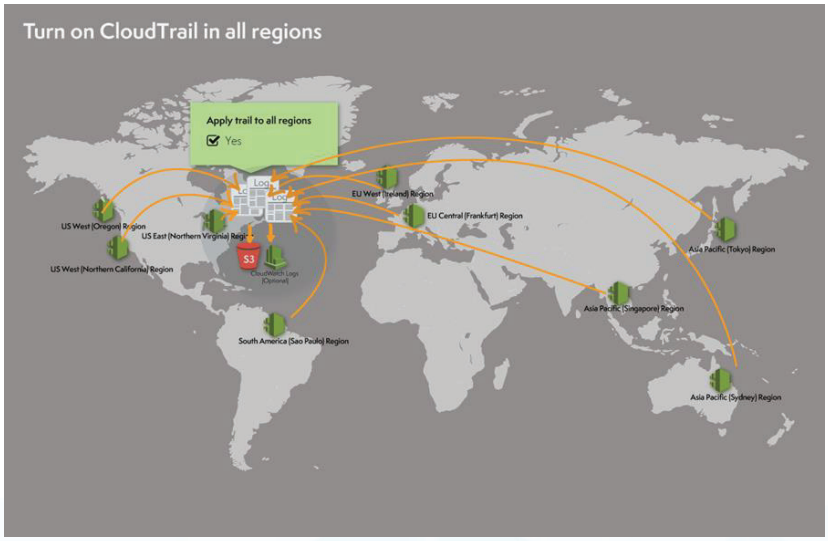
Cloud Checkr

whitepaper

THE PRACTICAL GUIDE TO **AWS CLOUDTRAIL**

AWS CloudTrail is an Amazon cloud service that records all AWS API events of your account, then delivers the log files to you. It tracks all calls made via the AWS UI Console, AWS SDKs, CLI, and other AWS services (such as AWS CloudFormation). The event log data is created and can be analyzed for security analysis and compliance auditing. The most basic example is enabling AWS CloudTrail logging so that you are alerted whenever instances are spun up.



AWS CloudTrail offers an innovative solution to a big problem: logging events in a dynamic cloud environment, and storing and managing those logs in a simple way. Many organizations have extensive logging infrastructures running internally, and getting logs from a cloud service back to the primary logging platforms has always been a challenging task. With AWS CloudTrail, logs can be generated, stored, and archived more easily, allowing event management in the cloud to finally integrate with existing log management systems.

Collecting the logs, however, is not enough. Users need log analytics to run robust cloud operations. And AWS CloudTrail is crucial for auditing access to your AWS- based IT environment. There are lots of hidden treasures within these events; however without the right tools and methods, you won't be able to form this data into information and take quick actions in time.

How AWS CloudTrail Works

AWS CloudTrail delivers the log file to a specified AWS S3 bucket, and can be configured to deliver the events to AWS CloudWatch. You can receive SNS notifications whenever the new log file was added to the AWS S3 bucket. You can also create a trail (a configuration that enables logging of the AWS API activity and related events in your account) with the AWS CloudTrail console, AWS CLI, or AWS CloudTrail API.

Two Types of Trails

1. Trail for All Regions

In this type of trail, whenever you create a trail, the same configuration applies to all regions. It records all events for all regions and stores the logs in the same AWS S3 bucket. SNS can also be configured for all region-related notifications.

2. Trail for Single Region

In this type of trail, you create a bucket through AWS CloudTrail in a region. It trails all the AWS API events specific to that region only, and stores them in an AWS S3 bucket.

It is highly recommended that you enable trails in every region, whether they are actively used or not. The purpose of auditing is to capture activities, including any activity that is unusual or suspicious. By failing to enable AWS CloudTrail in unused

regions, you leave the door open for unmonitored activity to occur. It is also important to note that by default, log files are encrypted using Amazon S3 server-side encryption.

Setting Up AWS CloudTrail

As mentioned, AWS CloudTrail requires an S3 bucket path for storing all log files. It can also be associated with Amazon SNS topics. Always create the S3 bucket for the logs through AWS CloudTrail only, as it creates the necessary IAM policies for you on the bucket.

Step-by-Step Guide to Setting up AWS CloudTrail

1. Log in to AWS Console and open the AWS CloudTrail dashboard.
2. Click on "Get Started".
3. Enter the trail name as well as the new S3 bucket name that needs to be created through AWS CloudTrail.
4. Select "Apply trail to all regions".

5. Click on "Advanced" for additional configuration options.

6. Take note of the exact name of the S3 bucket you have designated as the destination bucket for your CloudTrail log files. A relevant S3 bucket name like “CloudTrail-Logs” will be best, considering a large number of S3 buckets are created for big applications.

7. Select “Enable log file validation” on S3, to validate any modification on the log file and determine whether a log file was modified after CloudTrail delivered it.

8. Create an Amazon SNS topic.

9. Click “Turn On” to enable CloudTrail.

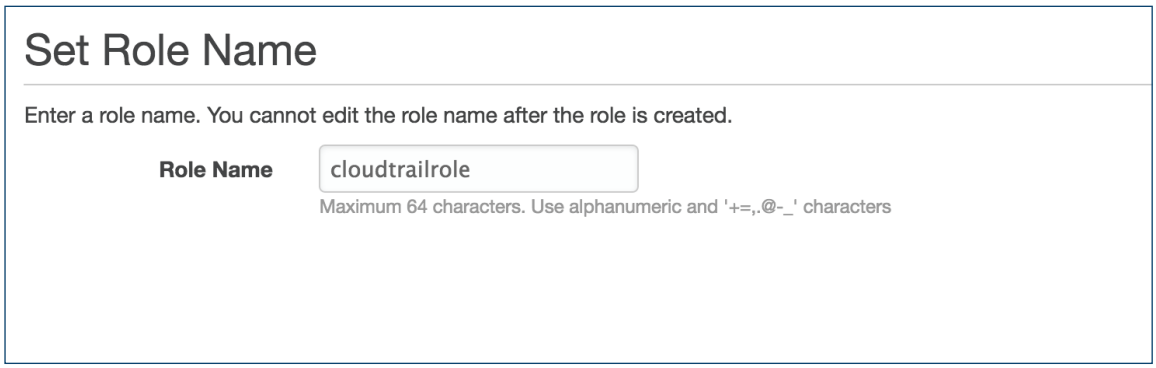
Sending AWS CloudTrail Events to AWS CloudWatch Logs

AWS CloudTrail can be configured to send all logs to AWS CloudWatch and monitor the AWS CloudTrail log events. Sending AWS CloudTrail events to AWS CloudWatch requires the steps below.

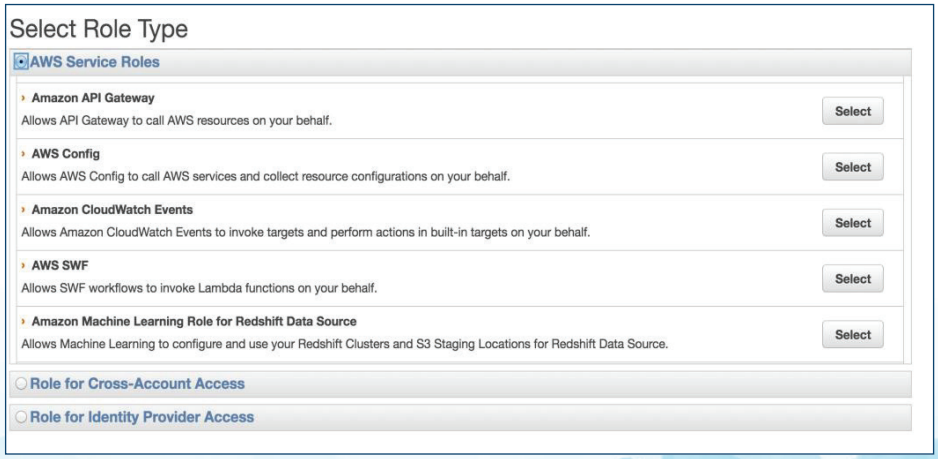
Create a Role

1. Go to the IAM dashboard. Select the Roles option and click “Create the new role”.

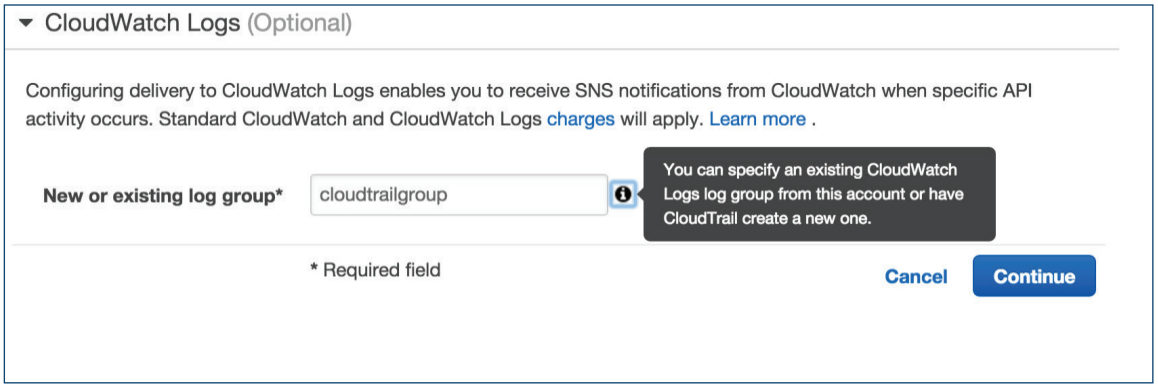
2. Enter the Role Name as per your requirement.



3. Next, select the role type for this role.



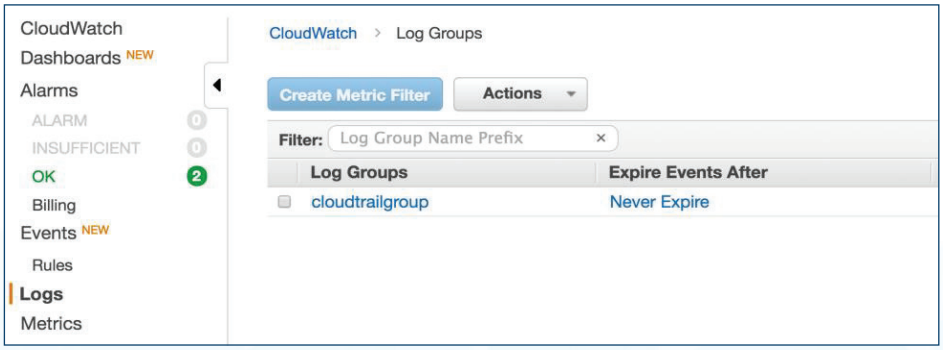
4. Select the policy that needs to be added in this Role. Click on “Continue”.



5. After clicking on Continue, AWS CloudTrail asks to create an IAM role. Here you need to mention the Role Name. This will also generate a policy attached to it. A policy is the access privileges available to that role. Normally it’s a JSON data file, as shown in the below image. Check “Policy Document”.

6. After verifying everything here, click “Allow”.

7. Now go to the AWS CloudWatch dashboard and select the Logs option. You should see your AWS CloudTrail group.



8. By creating a metric filter, you can create an alarm for CloudTrail events. This involves the following steps:

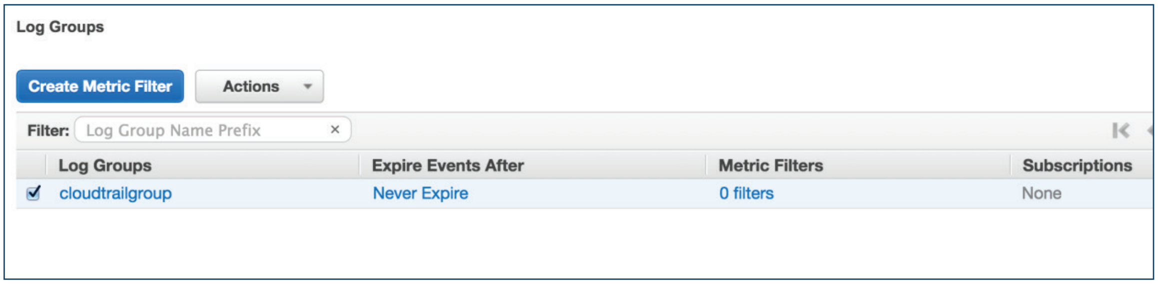
- Creating a metric filter
- Creating an alarm
- An action when an alarm is triggered (email list for notification)

Creating a Metric Filter for AWS CloudTrail Group

1. Select the Log groups for which you want to create a Metric filter.

2. In the navigation pane, select Logs.

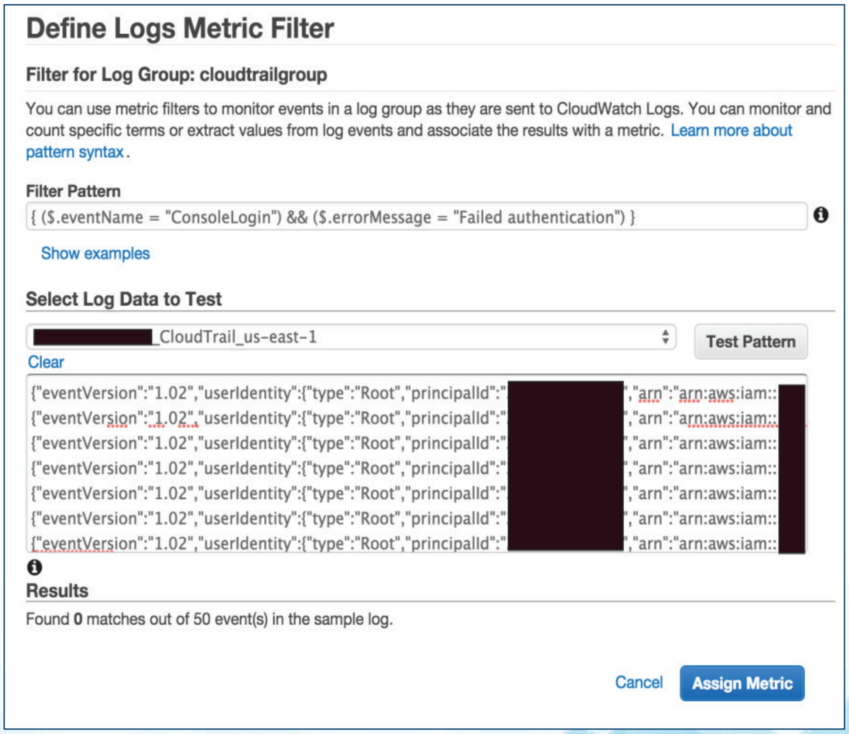
3. Select the log group you created for AWS CloudTrail log events.



4. Click on the Create Metric Filter button. On the filter pattern, you will need to write a pattern for AWS CloudTrail log events.

Below is the pattern for failed authentication:

```
{($.eventName = “ConsoleLogin”) && ($.errorMessage = “Failed authentication”)}
```



1. Click Assign Metric. On the Create Metric Filter, assign a Metric screen. In the Filter Name box, enter ConsoleSignInFailures.

2. Under metric details in the Metric Namespace box, enter LogMetrics.

3. In the Metric Name box, enter loginFailureCount.

4. In the Metric Value box, enter 1.

5. When finished, click Create Filter.

Configuring an Alarm

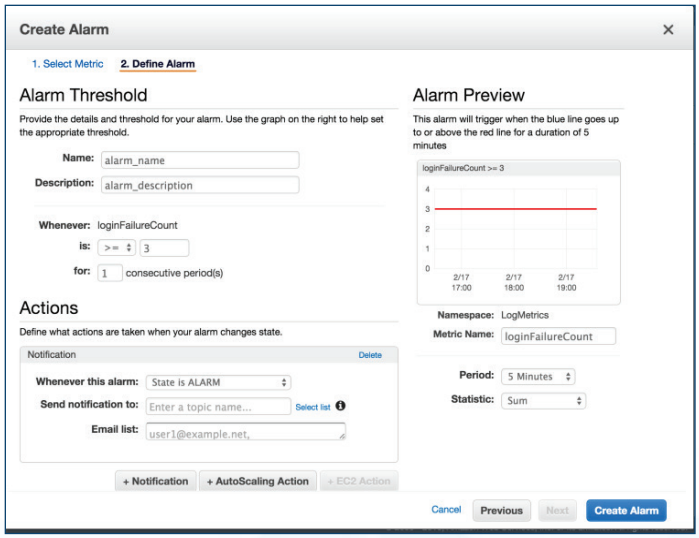
After creating a filter metric, on the "Filters for cloudtrailgroup" page next to the filter name, click on "Create Alarm".

On the Create Alarm dialog page, enter all the alarm related details, such as:

Name: Alarm_name

Description: Alarm_description value of alarm (>=3) whenever for 1 (5 min) consecutive period.

Email list: Your email list where notifications should be sent.



After finished with these details, click on Create Alarm, as shown in the dialog below.

AWS CloudTrail Pricing

There are three elements to AWS CloudTrail pricing:

1. AWS CloudTrail pricing is reasonable. AWS CloudTrail charges $2.00 per 100,000 events recorded for each trail. There is no charge for creating a trail.

Assume for example that your AWS account had 500,000 API calls in a region per month, and you turned on 5 Trails for an entire month in a region. Your charges will be calculated as follows:

Charges for 500,000 events recorded in the 5 Trails = (5 * 500,000 * 0.00002)

Total AWS CloudTrail Monthly charges = $50

2. AWS CloudTrail logs in S3 bucket will apply based on your usage. Typical Amazon S3 charges are based on 10 API calls/sec or 26 million API calls/month. Most AWS customers make fewer than 26 million API calls per account per month, hence monthly Amazon S3 charges for AWS CloudTrail usage are typically less than $3 per account.

3. Here let's assume an Amazon SQS endpoint for the SNS topic. AWS CloudTrail publishes one SNS notification per 5 minutes, or 8,640 SNS notifications per month. The Amazon SNS and Amazon SQS free tiers offer 1 million requests per month. Monthly Amazon SNS charges for AWS CloudTrail usage are typically less than $1 per account.

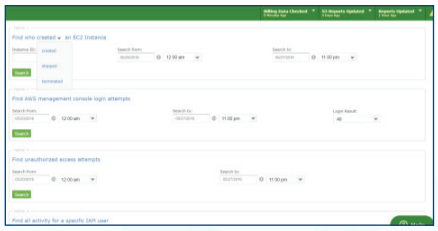
As this pricing example illustrates, users should not be deterred by cost considerations. AWS CloudTrail is very affordable even when used at scale.

Challenges

Once AWS CloudTrail is properly enabled, you will need to tightly monitor and implement the right tools, in order to make sense of the logs collected and cope with the data growth. AWS CloudTrail logs data is important when it comes to your AWS cloud security; however, without a proper implementation you won't be able to quickly track usage anomalies and mitigate security events.

Access Management

Logs contain sensitive information that you will need in case of an event, and you need to make sure these are isolated from the logged environment. To maintain the integrity of your log data, it is important to carefully manage access to your log files. The ability to view or modify your log data



should be restricted to only authorized users. As your AWS usage increases with your application growth, you need a security administrator to handle

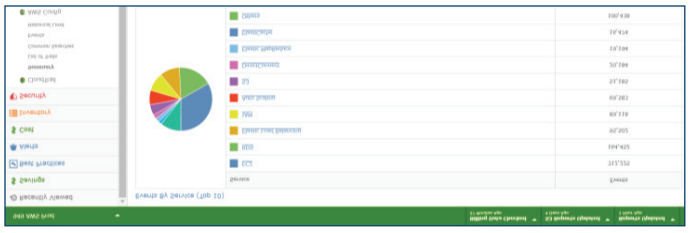
AWS CloudTrail. Log access should be provided to security teams only, who will be performing periodic reviews of the security configuration and vulnerabilities of each AWS account in the organization.

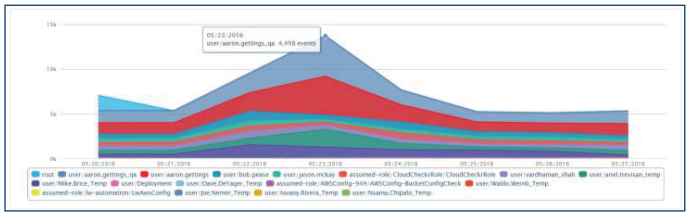
AWS CloudTrail can also be configured to aggregate log files across multiple accounts, so that log files are delivered to a single S3 bucket. This is especially useful for enterprises, where multiple AWS accounts are depended on by so many users.

Storage Costs

As your application grows, there will be a huge amount of log files stored in S3. To save on costs, old log files should be archived using services like Glacier. However, currently there is no support for logging to Amazon Glacier calls via Glacier APIs instead of S3 APIs. Until this is available, users should create their own archiving schedule to reduce long-term, aggregate S3 storage costs.

Logs are Not Actionable Insights



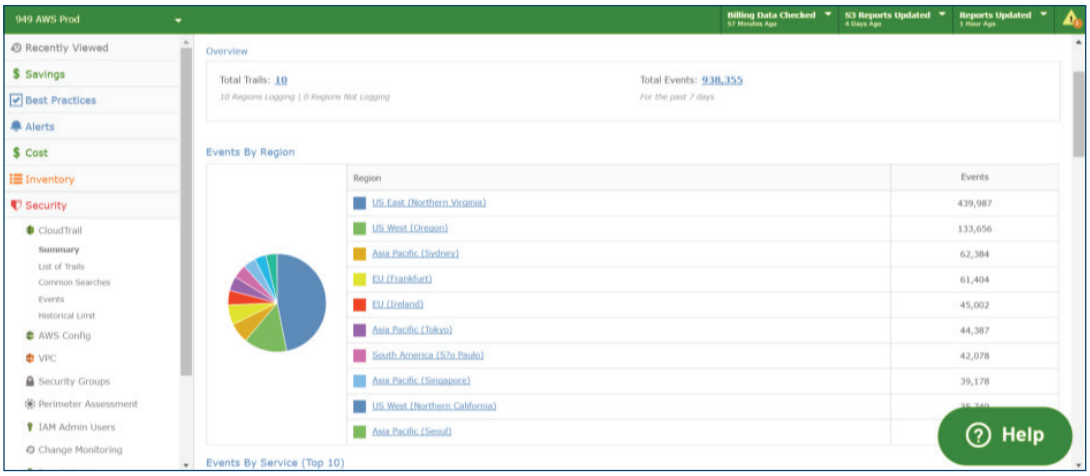


In order to monitor AWS CloudTrail, you will need to translate the API events into meaningful terms. One of the hardest parts of effective monitoring is understanding what to monitor and what it means. AWS often offers multiple events that, from a user's perspective, have very similar-appearing outcomes.

Logs should be configured and collected so that they can be searched and filtered efficiently. When collecting, one option is to integrate AWS CloudTrail with CloudSearch for efficient search. Another is to use third party tools such as CloudCheckr. The advantage of using a 3rd party tool is that it will add context to your logs. It will decipher the 100s of AWS CloudTrail events into actionable information. CloudSearch does not provide this translation.

Making Sense of Your AWS Logs

Because CloudCheckr is designed from the ground up specifically for AWS CloudTrail, it provides you with a deep understanding of AWS events, and is able to tie back to AWS resources and IAM users. CloudCheckr ingests both the configuration and logs from AWS CloudTrail to provide visibility about your resources in AWS. It will automatically identify important events based upon user specified monitoring criteria. Using CloudCheckr, you can analyze, search, understand, and alert on changes to resources and API activity recorded by AWS CloudTrail.



CloudCheckr also automatically finds and ingests your AWS CloudTrail logs into a format that can be searched and analyzed. CloudCheckr thoroughly checks your logs, finding security events and highlighting abnormal activity. Using the search engine, you can visualize the activities of a specific user or a specific resource, and hone in on failed activities, specific actions, or specific IP addresses. Once set up, the system continuously looks through the logs for new events, and automatically generates email notifications on anomalies to support fast remediation.

About CloudCheckr

CloudCheckr is a cost and security platform that unifies IT, Security & Finance teams who need to keep their cloud in check across Amazon Web Services (AWS). CloudCheckr turbo-charges your cloud with cost optimization, continuous security and resource utilization solutions to help be more efficient and secure while saving money.

Government organizations and Global 2000 enterprises trust CloudCheckr to unify their native AWS data to deliver the most robust cloud optimization and governance solution

in today's marketplace. The CloudCheckr platform continuously monitors and measures AWS data sources including AWS CloudTrail logs, AWS Config, AWS Virtual Private Cloud (VPC) flow logs, AWS CloudWatch and AWS API calls.

CloudCheckr generates a complete picture of a user's environment which shows billing details, multi-accounts, security events, resources, configurations, permissions, changes, and more. It then optimizes and analyzes that picture to provide actionable clarity on costs, security and resources data.

CloudCheckr's software as-a-service (SaaS) platform integrates within your existing tools and processes, providing unified governance across your cloud.

Amazon provides the Amazon Management Console to configure and set up your AWS account. CloudCheckr takes it from there. It does not replace the functionality of the Amazon Management Console – in fact you don't ever make any updates to AWS through CloudCheckr. CloudCheckr is designed to report on and analyze what resources you are and are not using, where your spending is not optimized, what your account looked like historically, and what is changing in your account.

CloudCheckr uses the Amazon Web Services API to look at your AWS setup. CloudCheckr connects to your AWS account and grabs a "snapshot" of all of the settings and details on your account. This snapshot is then used to analyze your usage, costs, and provide best practice advice.

CloudCheckr capabilities include:

- Discovering and visualizing what's running in AWS
- Understanding costs in AWS
- Analyzing your usage in AWS
- Monitoring for security events & changes in your AWS environment
- Hundreds of best practice checks covering security, availability, cost, and usage
- Maintaining a historical, audit-ready record of your cloud environment

CloudCheckr is the only advanced technology solution to achieve the AWS Security certification.

Contact Us

sales@cloudcheckr.com
585-413-0869
www.cloudcheckr.com