idexcel

Serverless CloudTrail Logs Dashboard with

Amazon QuickSight

CLOUDTRAIL LOGS DASHBOARDS - SOLUTION BRIEF

THE CHALLENGE: TRACKING CRITICAL CLOUDTRAIL EVENTS IN A SMALL BUSINESS IT ECOSYSTEM

Much like a living organism with complex structures in place and processes occurring, an IT ecosystem has an immense amount of activity going on. It can be tough to track so many service specific events, collect the data of that account activity occurring, then analyze it to troubleshoot or optimize for better performance. More organizations are taking advantage of the premier security benefits of AWS CloudTrail logs data to predict future events and avoid security breaches or compliance issues. Small businesses can especially benefit from this solution, since it is more difficult to adopt enterprise-level logging solutions for small scale needs. Security requirements and high operational costs of enterprise logging tools are major challenges faced by smaller enterprises, which increases immensely as the amount of data increases.

As a result of this challenge, small companies may miss critical health issues within their IT environment. The valuable log data critical to analyzing, visualizing, and tracking security concerns is a consistent system health report that enables immediate action to be taken if need be. CloudTrail events associated with every service in the system are also logged to better assess and address any related issues. Organizations need a secure alternative solution to monitor events to ensure optimized performance and IT infrastructure health. Developing CloudTrail log dashboards and reports enables smaller businesses to do so at an efficient price.

THE SOLUTION

Just as a medical professional would monitor a patient's health, CloudTrail logs dashboards track, measure, and analyze various 'vital' signs to identify potential risks to a system. Idexcel implements a secure and cost-effective analytics solution to creating CloudTrail log dashboards within the AWS cloud environment. This approach empowers small businesses with critical information to continue building a healthy and strong IT ecosystem.

WHY WE USE QUICKSIGHT AND ATHENA TO ANALYZE CLOUDTRAIL DATA

Cost-Conscious Solution: AWS Athena delivers the most robust and cost-effective solution to study logs data. Athena follows the 'pay per query' strategy, which makes pricing very straight forward and easy to scale as needed.

Effective Dashboards: Amazon Quicksight enables us to develop rich and interactive dashboards within the AWS cloud. Quicksight's SPICE (Super-fast, Parallel, In-memory, Calculation Engine) mechanism drives quick performance and allows multiple users to access Quicksight simultaneously.

HOW WE APPLY OUR SOLUTION ARCHITECTURE

1. **Storage of CloudTrail Data:** As seen below in Figure 1, AWS CloudTrail provides event history of the account activity in the form of logs. This log data is stored in the Amazon S3 bucket, an object storage service used to store and protect any amount of data of event history of your AWS account activity. This includes all actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services accessed within the IT infrastructure.

2. **Conversion of Data from JSON to Parquet format:** Every time a new trail is created in the S3 bucket, the Lambda function is invoked to complete data format modification. By default, CloudTrail stores data in JSON format, so we convert the data to Parquet format to reduce the size and complexity of the logs data.

3. **Store the Converted Data Back to S3:** The converted Parquet data is then stored again in S3 in a defined bucket to perform further exploratory analysis of the log data.

4. **Querying & Analysis of The Data:** A database is then created with required functionalities in Athena for the Parquet log files stored in the S3 bucket. This enables SQL query capabilities on the data, making the data straightforward and user-friendly to work with.

5. **Building Dashboards:** Dashboards and reports are created using the CloudTrail logs data refreshed from Athena. These reports provide valuable insights for leaders to perform stronger security analysis and risk management. See Figures 2, 3, and 4 below for sample dashboards.

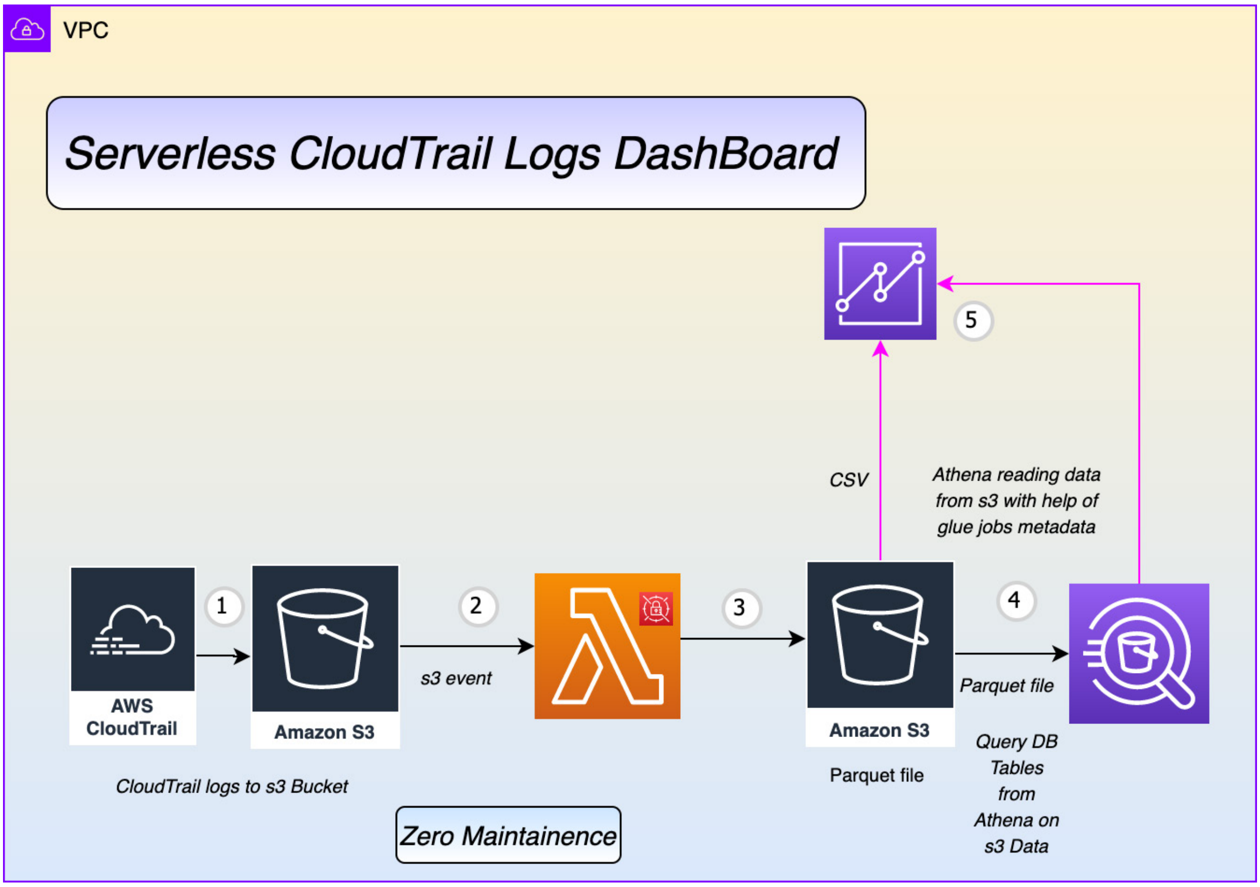
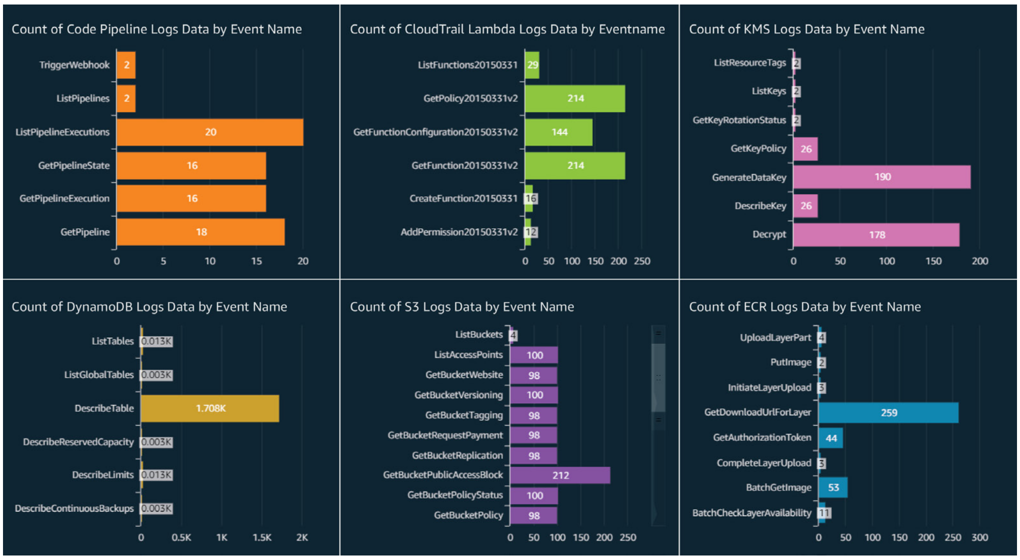

VPC
Serverless CloudTrail Logs DashBoard
5
CSV
Athena reading data from s3 with help of glue jobs metadata
1
2
3
4
AWS CloudTrail
Amazon S3
s3 event
Amazon S3
Parquet file
CloudTrail logs to s3 Bucket
Parquet file
Query DB Tables from Athena on s3 Data
Zero Maintainence

Figure 1

AWS SERVICES CLOUDTRAIL DATA - EVENT NAMES

This sample dashboard monitors multiple AWS services and tracks their various operations on a single display screen.


Count of Code Pipeline Logs Data by Event Name

Count of CloudTrail Lambda Logs Data by Eventname

Count of KMS Logs Data by Event Name

Count of DynamoDB Logs Data by Event Name

Count of S3 Logs Data by Event Name

Count of ECR Logs Data by Event Name

Figure 2

CLOUDTRAIL DASHBOARDS – AWS LAMBDA LOGS DATA

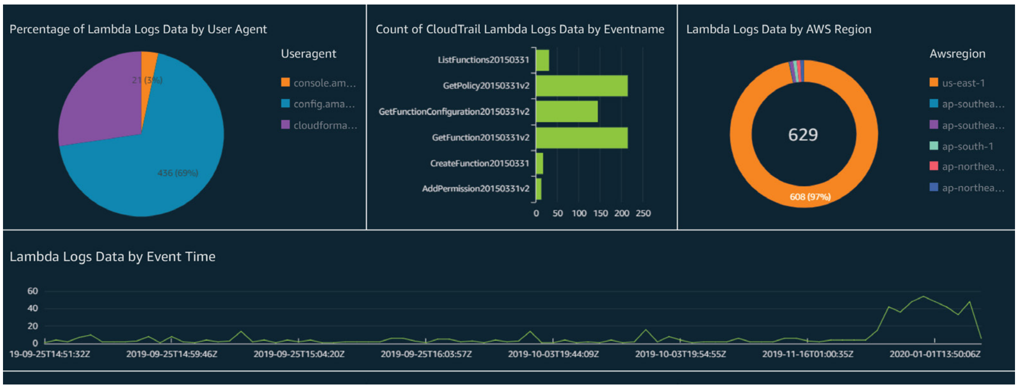


Figure 3

This dashboard view gives us a simple visual representation of Lambda activities. The important information tracked here helps us monitor which lambda resources are provisioned and if there are there any variations in the count of resources or lambda activities occurring that might affect the system threshold.

AWS CLOUDTRAIL DASHBOARD- S3 LOGS

From this dashboard, we can capture the history of changes in s3 activities with respect to multiple events or within a specific period of time. This helps us monitor security anomalies and troubleshoot any issues.

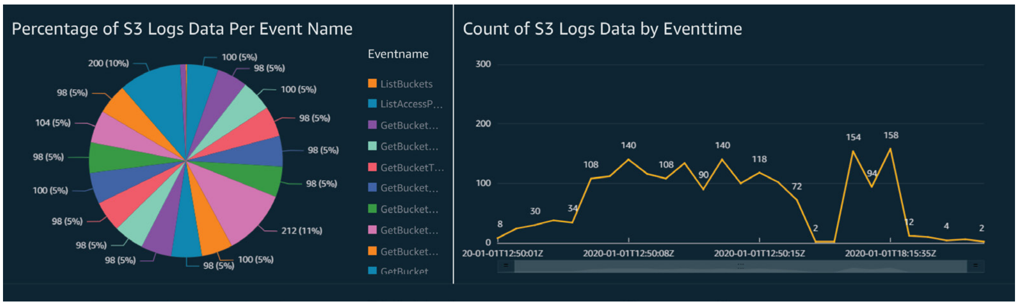


Figure 4

KEY ADVANTAGES OF THIS SOLUTION

Lower Operational Costs: The data is stored in Parquet format, but not other formats such as CSV/JSON. (which is the case in an enterprise-level solution) This method contributes to major reduction in overall costs on technology needs like data storage, analytics tools, reporting applications, and performance dashboard creation.

Better Information = Better Business Decisions: With valuable data analytics, insightful reporting, and robust dashboard views available, leaders are more informed to make critical decisions to help drive business success forward.

Straightforward Monitoring: By connecting AWS CloudTrail data to QuickSight, we can develop uncomplicated, dynamic dashboards that enable quick visibility to take action on non-compliance events or security alerts.

WHO SHOULD ADOPT THE SOLUTION?

- A company requiring a secure and closed environment without interaction from third party tools
- An organization that requires data to remain within its AWS network
- Businesses with small scale logs data
- Any organization that is currently utilizing AWS cloud ecosystem and its native service resources

FEATURES OF THIS APPROACH

Serverless Solution: All the services in the architecture belong to the AWS cloud environment, enabling applications and services to be built without the need for servers, increasing agility and innovative capabilities.

One-time Configuration: This architecture can be launched quickly in a one-time deployment (given no major changes in business rules occur), ensuring minimal disruption in operations.

Simple Approach: The solution can be developed within 2-3 weeks with simple user-friendly dashboards. ANSI SQL is used to query and perform transformations on the logs data to make it easier to retrieve critical insights.

Durable Data Storage: The CloudTrail data is stored in AWS S3, which provides long term and cost-effective storage of data when compared to the high cost of other enterprise tools.

Highly Secure and Reliable: Because this solution exclusively utilizes AWS Cloud Native services, security risks are significantly reduced in the absence of 3rd party integration processes.

CONSIDER:

- As Lambda functions are limited to a maximum execution time of fifteen minutes, this solution is not a great fit for bulk logs data.
- In the event of a larger scale of data queries, Athena pricing increases according to data scanned. This is impacted if the solution is used on a recurring basis.
- This solution is limited to query capabilities vs. search capabilities that are offered by enterprise logging solutions.
- Dashboard templates provided by Amazon Quicksight come standardized with limited options for customization.

Interested in learning more about tracking critical CloudTrail events to better manage your IT ecosystem? **Contact Idexcel** to schedule a workshop, request a demo, or to speak with someone from our team about how we can help implement this solution.

OUR AWS COMPETENCIES

aws
PARTNER
Advanced Tier
Services

- Public Sector
- Solution Provider
- DevOps Services Competency

- Financial Services Competency
- Migration Services Competency

Contact us

Idexcel, Inc.

459 Herndon Parkway Suite 10, Herndon, VA 20170
Tel: 703-230-2600
Email: inquiry@idexcel.com

idexcel

Find out how Idexcel solutions can help your business. Contact us today!

inquiry@idexcel.com | www.idexcel.com