Real-Time Insights on

AWS Account Activity

AWS Implementation Guide

Ryan Nienhuis, Chris Marshall, Arjun Gurumurthy

Secondary author’s name

January 2018



Contents

[Overview 3](#_Toc503260366)

[Cost 3](#_Toc503260367)

[Architecture Overview 4](#_Toc503260368)

[Solution Components 4](#_Toc503260369)

[Real-Time Event Monitoring 5](#_Toc503260370)

[Dashboard 5](#_Toc503260371)

[Customization 5](#_Toc503260372)

[Customization 5](#_Toc503260373)

[Design Considerations 5](#_Toc503260374)

[Regional Deployment 5](#_Toc503260375)

[AWS CloudFormation Template 5](#_Toc503260376)

[Automated Deployment 7](#_Toc503260377)

[Prerequisites 7](#_Toc503260378)

[What We’ll Cover 7](#_Toc503260379)

[Step 1. <Pre-Launch Tasks> 7](#_Toc503260380)

[Step 2. Launch the Stack 7](#_Toc503260381)

[Step 3. <Post-Configuration Tasks> 9](#_Toc503260382)

[Security 9](#_Toc503260383)

[Additional Resources 9](#_Toc503260384)

[Appendix A: Customizing the Dashboard 11](#_Toc503260385)

[Appendix B: Collection of Anonymous Data 11](#_Toc503260386)

[Send Us Feedback 12](#_Toc503260387)

[Document Revisions 12](#_Toc503260388)

About This Guide

This implementation guide discusses architectural considerations and configuration steps for deploying Real-Time Insights on AWS Account Activity on the Amazon Web Services (AWS) Cloud. It includes links to a [AWS CloudFormation](http://aws.amazon.com/cloudformation/) template that launches, configures, and runs the AWS services required to deploy this solution using AWS best practices for security and availability.

The guide is intended for IT infrastructure architects, administrators, and DevOps professionals who have practical experience architecting on the AWS Cloud.

# Overview

Amazon Web Services (AWS) enables customers to achieve significant gains in productivity, innovation, and cost reduction when they move to the AWS Cloud. AWS offers a variety of services and features that allow for flexible control of cloud computing resources and also of the AWS account(s) managing those resources. These options help to ensure proper cost allocation, agility, and security, however customers are sometimes unsure of how to best leverage the elasticity of the AWS Cloud to optimize their costs yet still meet their performance and capacity requirements.

Monitoring AWS account activity can provide valuable insight into how your resources are being used, enabling you to make well-informed decisions that increase efficiency and optimize costs. Many customers choose to build custom account monitoring solutions using AWS services because these services provide an efficient way to handle a large number of activity events in real time and flexibility to get specific metrics.

To help customers more easily monitor account activity, AWS offers the Real-Time Insights on AWS Account Activity solution. This solution automatically provisions and configures the services necessary to monitor the resource usage of your AWS account(s) in real time. The solution uses AWS CloudTrail to log account activity, Amazon Kinesis Data Analytics to compute metrics in real-time, and Amazon DynamoDB to durably store the computed data. The solution also features a dashboard that visualizes your account activity in real-time.

## Cost

You are responsible for the cost of the AWS services used while running this reference deployment. As of the date of publication, the cost for running this solution with default settings in the US East (N. Virginia) Region is approximately **$100 per month**. Prices are subject to change. For full details, see the pricing webpage for each AWS service you will be using in this solution.

## Architecture Overview

Deploying this solution with the **default parameters** builds the following environment in the AWS Cloud.

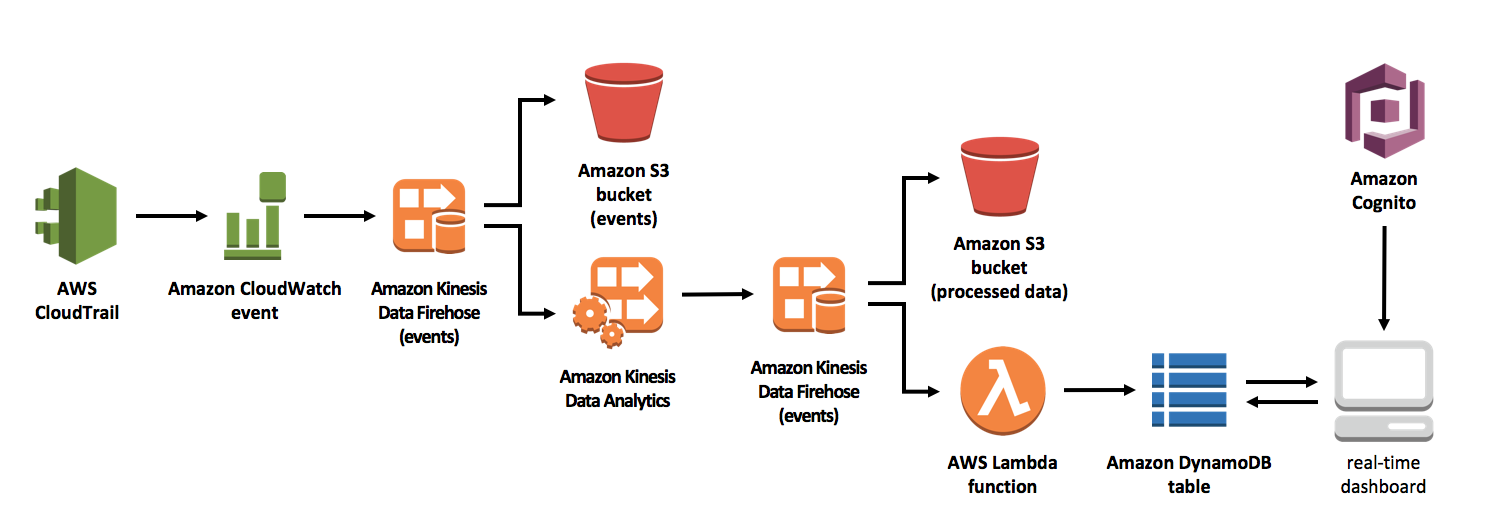
**

Figure 1: Real-Time Insights on AWS Account Activity architecture on AWS

The AWS CloudFormation template deploys an AWS CloudTrail trail, an Amazon CloudWatch event, an Amazon Kinesis Data Firehose delivery stream, Amazon Simple Storage Service (Amazon S3) buckets, an Amazon Kinesis Data Analytics application, an Amazon Kinesis Data stream, an AWS Lambda function, Amazon DynamoDB tables, an Amazon Cognito user pool, and a real-time dashboard.

The AWS CloudTrail trail logs events that occur in your AWS accounts such as action taken by a user, role, or service. When an event occurs, an Amazon CloudWatch event trigger sends data to an Amazon Kinesis Data Firehose delivery stream. The Firehose delivery stream archives the events in an Amazon S3 bucket and sends the data to an Amazon Kinesis Data Analytics application for processing.

Once the data is processed, it is sent to a Kinesis Data stream. An AWS Lambda function reads data from the stream and sends the data in real-time to a DynamoDB table to be stored.

The solution’s real-time dashboard, which is stored in an Amazon S3 bucket, pulls the processed data from the DynamoDB table and displays it. An Amazon Cognito user pool is used to add user registration and sign-in to the real-time dashboard.

# Solution Components

## Real-Time Event Monitoring

The Real-Time Insights on AWS Account Activity solution monitors most events that occur in your account in real-time. Some events, however, might take up to 15 minutes to arrive in Amazon Kinesis Data Firehose from AWS CloudTrail.

## Dashboard

The solution features a simple dashboard that loads data from Amazon DynamoDB into line charts every 10 seconds and bar charts every minute. The past 15 minutes of data are updated every minute to capture events that can take up to 15 minutes to arrive from AWS CloudTrail.

### Customization

TK

## Customization

TK

# Design Considerations

## Supported Services

AWS CloudTrail records account activity and service events from most AWS services. Additionally, some AWS services do not enable logging of all APIs and events. Note that even if you configure logging all management and data events in a trail, you will not create a log with all possible AWS events. For the list of supported services, see [CloudTrail Supported Services](http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-supported-services.html) in the CloudTrail User Guide*.*

## Regional Deployment

This solution uses the Amazon Kinesis Data Firehose service, which is currently available in specific AWS Regions only. Therefore, you must launch this solution in an AWS Region where Amazon Kinesis Data Firehose is available.[[1]](#footnote-1) However, once deployed, this solution monitors all regions for events.

# AWS CloudFormation Template

This solution uses AWS CloudFormation to automate the deployment of the Real-Time Insights on AWS Account Activity solution. It includes the following CloudFormation template, which you can download before deployment:

**View template**

**real-time-insights-account-activity.template:** Use this template to launch the solution and all associated components. The default configuration deploys an AWS CloudTrail trail, an Amazon CloudWatch event, Amazon Kinesis Data Firehose delivery streams, Amazon Simple Storage Service (Amazon S3) buckets, an Amazon Kinesis Data Analytics application, an AWS Lambda function, Amazon DynamoDB tables, an Amazon Cognito user pool, and a real-time dashboard.

# Automated Deployment

Before you launch the automated deployment, please review the architecture and other considerations discussed in this guide. Follow the step-by-step instructions in this section to configure and deploy the Real-Time Insights on AWS Account Activity into your account.

**Time to deploy:** Approximately 5 minutes. <x minutes/hours>

## Prerequisites

TK

## What We’ll Cover

The procedure for deploying this architecture on AWS consists of the following steps. For detailed instructions, follow the links for each step.

Step 1. *Pre-launch tasks, if required*

* *Tasks in this step.*

Step 2. Launch the stack

* Launch the AWS CloudFormation template into your AWS account.
* Enter values for required parameters: *x*, *y*, *z*.
* Review the other template parameters, and adjust if necessary.

Step 3. *Post-launch tasks, as needed*

* *List of tasks, as necessary.*

## Step 1. <Pre-Launch Tasks>

TK

## Step 2. Launch the Stack

This automated AWS CloudFormation template deploys <solution> on the AWS Cloud. Please make sure that you’ve <prerequisites> before launching the stack. <Any other important introductory info>

**Note**: You are responsible for the cost of the AWS services used while running this solution. See the [Cost](#_Cost)  section for more details. For full details, see the pricing webpage for each AWS service you will be using in this solution.

**Launch   
Solution**

1. Log in to the AWS Management Console and click the button to the right to launch the real-time-insights-account-activity AWS CloudFormation template.   
   You can also [download the template](file:///C:\Users\sindona\AppData\Local\Temp\need) as a starting point for your own implementation.
2. The template is launched in the US East (N. Virginia) Region by default. To launch the solution in a different AWS Region, use the region selector in the console navigation bar.

**Note**: This solution uses the Amazon Kinesis Data Firehose service, which is currently available in specific AWS Regions only. Therefore, you must launch this solution an AWS Region where Amazon Kinesis Data Firehose is available. [[2]](#footnote-2)

1. On the **Specify Details** page, assign a name to your solution stack.
2. Under **Parameters**, review the parameters for the template and modify them as necessary. This solution uses the following default values.

|  |  |  |
| --- | --- | --- |
| Parameter | Default | Description |
| KeyPairName | *<Requires input>* | Public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region. |
| ADInstanceType | m3.xlarge | Amazon EC2 instance type for the first Active Directory instance |
| AD2InstanceType | m3.xlarge | Amazon EC2 instance type for the second Active Directory instance |
| *etc.* |  |  |
|  |  |  |
| Send Anonymous Usage Data | Yes | Send anonymous data to AWS to help us understand <solution> usage and <related cost savings, or other purpose> across our customer base as a whole. To opt out of this feature, select No.  For more information, see the appendix. |

1. Choose **Next.**
2. On the **Options** page, choose **Next**.
3. On the **Review** page, review and confirm the settings. Be sure to check the box acknowledging that the template will create AWS Identity and Access Management (IAM) resources.
4. Choose **Create** to deploy the stack.

You can view the status of the stack in the AWS CloudFormation Console in the **Status** column. You should see a status of CREATE\_COMPLETE in roughly **TK** minutes.

**Note:** In addition to the primary AWS Lambda function <function(s)..>, this solution includes the solution-helper Lambda function, which runs only during initial configuration or when resources are updated or deleted.

When running this solution, you will see <both> Lambda functions in the AWS console, but only the <function> function is regularly active. However, do not delete the solution-helper function as it is necessary to manage associated resources.

## Step 3. <Post-Configuration Tasks>

*Add steps as necessary.*

# Security

When you build systems on AWS infrastructure, security responsibilities are shared between you and AWS. This shared model can reduce your operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. For more information about security on AWS, visit the [AWS Security Center](http://aws.amazon.com/security/).

## AWS CloudTrail

By default, AWS CloudTrail log files are encrypted using Amazon Simple Storage Service (Amazon S3) Server Side Encryption (SSE) and placed into your Amazon S3 bucket. You can control access to log files by applying AWS Identity and Access Management (IAM) or S3 bucket policies. You can add an additional layer of security by enabling S3 [Multi Factor Authentication (MFA) Delete](http://docs.aws.amazon.com/AmazonS3/latest/dev/MultiFactorAuthenticationDelete.html) on your S3 bucket.

# Additional Resources

**AWS services**

* [AWS CloudFormation](http://aws.amazon.com/documentation/cloudformation/)
* [Amazon Kinesis Data Firehose](https://aws.amazon.com/kinesis/data-firehose/)
* [Amazon Kinesis Data Analytics](https://aws.amazon.com/kinesis/data-analytics/)
* [AWS CloudTrail](https://aws.amazon.com/cloudtrail/)
* [Amazon CloudWatch](https://aws.amazon.com/cloudwatch/)
* [AWS Lambda](https://aws.amazon.com/lambda)
* [Amazon DynamoDB](https://aws.amazon.com/dynamodb/)
* [Amazon Cognito](https://aws.amazon.com/cognito/)

# Appendix A: Customizing the Dashboard

TK

# Appendix B: Collection of Anonymous Data

This solution includes an option to send anonymous usage data to AWS. We use this data to better understand how customers use this solution and related services and products. When enabled, the following information is collected and sent to AWS each time TK:

*Give a description of each data type collected, for example:*

* **Solution ID:** The AWS solution identifier
* **Unique ID (UUID):** Randomly generated, unique identifier for each <solution> deployment
* **Timestamp:** Data-collection timestamp

Note that AWS will own the data gathered via this survey. Data collection will be subject to the [AWS Privacy Policy](https://aws.amazon.com/privacy/). To opt out of this feature, modify the AWS CloudFormation template mapping section as follows:

"Send" : {  
"AnonymousUsage" : { "Data" : "Yes" }  
},

to

"Send" : {  
"AnonymousUsage" : { "Data" : "No" }  
},

# Send Us Feedback

We welcome your questions and comments. Please post your feedback on the [AWS Solutions Discussion Forum](https://forums.aws.amazon.com/forum.jspa?forumID=226).

You can visit our [solution GitHub repository link] to download the templates and scripts for this solution, and to share your customizations with others.

# Document Revisions

|  |  |  |
| --- | --- | --- |
| Date | Change | In sections |
| January 2018 | Initial release | -- |

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

**Notices**

This document is provided for informational purposes only. It represents AWS’s current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS’s products or services, each of which is provided “as is” without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The Real-Time Insights on AWS Account Activity is licensed under the terms of the Amazon Software License available at <https://aws.amazon.com/asl/>.

1. For the most current Amazon Kinesis Data Firehose availability by region, see <https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/> [↑](#footnote-ref-1)
2. For the most current service availability by AWS Region, see <https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/> [↑](#footnote-ref-2)