**Lincoln FG - AWS Services**

Revision History 1

**Architecture** [**1**](https://docs.google.com/document/d/1DRaXbKv5SK1pglXf6de1srX4U4-TUdbqefTTD1mY3gc/edit#heading=h.2g4f3oyrec32)

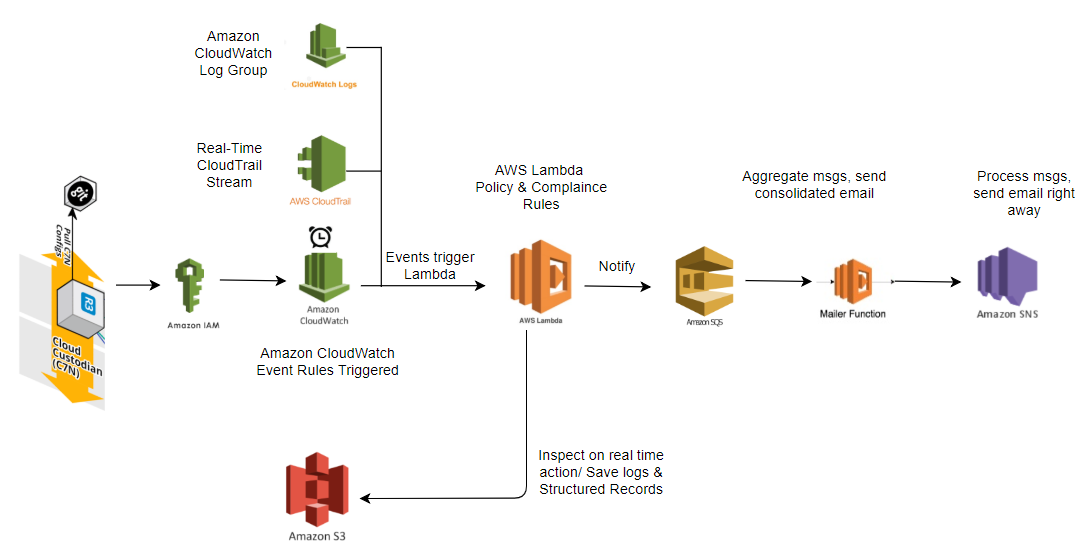
**Cloud Custodian infrastructure with AWS** [**2**](https://docs.google.com/document/d/1DRaXbKv5SK1pglXf6de1srX4U4-TUdbqefTTD1mY3gc/edit#heading=h.tq8i30ovt27e)

**Communication between AWS Managed Services**

**IAM Roles Required** 2

**Reference Links 2**

**Cloud Custodian Architecture and AWS Services**

****

Cloud Custodian (a.k.a C7N) notifies users in real-time AWS resources behavior changes, Compliance (Security/Access Control, Encryption, Backups, etc) and drives Cost savings (Off-hours, Monitoring and Garbage Collection of unused and underutilized resources).

**Cloud Custodian infrastructure with AWS**

IAM, CloudWatch, Lambda Function, SQS, SES

**Communication between managed services**

Cloud Custodian is checking for policy violation by script deployed as an lambda function which consist of policy correction logic ..resource with violated policy will be rectified and will proceed triggering the CloudWatch event on any detection, Which in turn will trigger the lambda mailer function for notifying the end user via SES. Lambda will queue up the event received from cloudwatch onto the SQS service will then proceed to pass on the event to the SES service for the email delivery.

Toggle functionality for correcting the resource with violated policy in cloud Custodian is implemented via an API call made within an Lambda function.

**IAM Roles Required**

IAM managed policy with appropriate Roles and Permissions to provide an access to certain AWS Resources and then attach a Policy to an IAM Role.

**IAM**

5 Actions - ListAccountAlias, ListUsers, GenerateCredentialReport, GetCredentialReport, PassRole

**S3**

7 Actions – ListBuckets, GetBucketAcl, GetBucketPolicy, PutBucketAcl, PutBucketPolicy, GetBucketVersioning, PutBucketVersioning

**Lambda**

6 Action - ListFunctions, ListTags, CreateFunction, UpdateFunctionCode, AddPermission, GetFunction

**CloudWatchLogs**

3 Actions - CreateLogGroup, CreateLogStream, PutLogEvents

**CloudWatchEvent**

2 Actions - PutRule, PutTargets, ListTargetByRule, DescribeRule

**SQS**

17 Actions - GetQueueAttribute, GetQueueURl, ListDeadLetterSourceQueues, SetQueueAttributes, ChangeMessageVisibilityBatch, CreateQueue, DeleteQueue, PurgeQueue, DeleteMessageBatch, TagQueue, ListQueueTags, SendMessage, ReceiveMessage, SendMessageBatch, ChangeMessageVisibility, DeleteMessage, UntagQueue

**SES**

2 Actions - SendRawEmail, SendEmail

**ResourceGroupTagging**

1 Action - GetResources

**Note:** We can customize this IAM Policy according to our Security aspects to allow/deny users to perform certain actions on AWS Resources.

Reference sample IAM Policy:



**Reference Links**

**Lambda Support using Cloud Custodian**

[**https://github.com/capitalone/cloud-custodian/blob/master/docs/source/policy/lambda.rst**](https://github.com/capitalone/cloud-custodian/blob/master/docs/source/policy/lambda.rst)

**S3 - Configure New Buckets Settings and Standards using Custodian**

<https://www.capitalone.io/docs/usecases/s3configurenewbucket.html>

**Cloud Custodian Supported Usecases/AWS Modules:**

These usecases provide examples of specific policies for individual AWS modules.

<http://capitalone.github.io/cloud-custodian/docs/usecases/index.html>

**Custodian Mailer**

<https://github.com/capitalone/cloud-custodian/tree/master/tools/c7n_mailer>