**Introduction**

Automate creating secure s3 Hana Database backup, and create cross region replication bucket as offsite backup or use as DR using AWS CloudFormation and Lamdba.

Many of our customer requested to create Hana backup DR or offsite backup in other region, and how to protect the backup data in s3 bucket. The security feature of the solution as below

* Use custom KMS key and grant fine-grained access to AWS admin account and grant access to EC2 role (Need to run the backup) to encrypt and decrypt. Creating in this solution two KMS key one in each region
* Deny any upload are not encrypted using aws:kms
* Enable bucket versioning
* Enable bucket logging
* Replicate objects which has been encrypted in source bucket and the objects are encrypted in the target backup.

Other feature is creating lifecycle policy to move the backup after 7 days to glacier and delete it from glacier after one year.

**Challenge**

When create the source bucket and enable the replication, the target bucket should be ready in other region.

Using CloudFormation you cannot create target backup in different region of the source bucket. To create destination bucket in same CloudFormation of source bucket, You can use AWS Lambda-backed custom resource in the same template.

**Solution overview**

The CloudFormation template uses an AWS Lambda-backed custom resource to create an S3 destination bucket in one region and a source S3 bucket in the same region

**Note:** In this solution CloudFormation is not aware of destination CMK key and bucket which are created by Lambda, so the CloudFormation will not delete destination CMK key or bucket when stack is delete. It will be logged on CloudWatch logs to delete when delete the stack.

**Solution Details**

When launch the CloudFormation, CloudFormation detects the current region and set it as source region for source CMK and bucket.

To custom the solution, CloudFormation will pass parameters values when launch the stack.

These parameters are user input values as below:

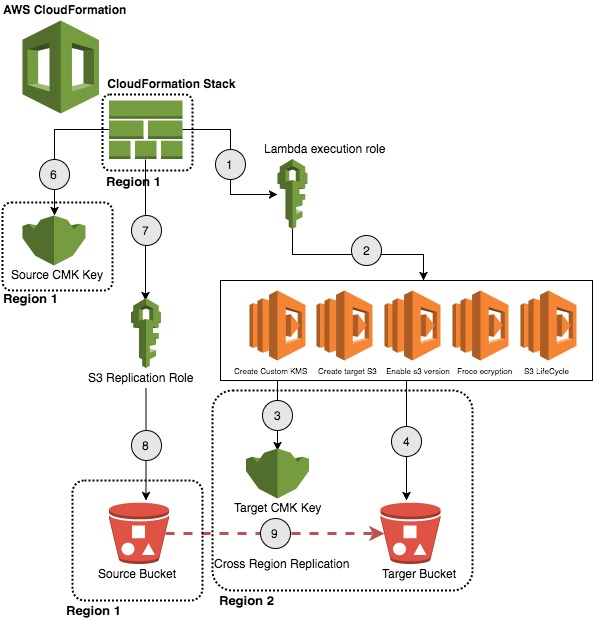
* ReplicationRegion
* ReplicationBucketName
* ReplicationCMKAlias
* OriginalBucketName
* OriginalCMKAlias
* EC2RoleToRunBackup
* KMSAdminRole
* BucketNameForLambdaCode

**Sequence of creating resources:**

When launch the CloudFormation the below is Sequence of creating resources and configuration:

1. Create Lambda execution role
2. Create and trigger Lambda functions to launch destination resources in other region
3. Create destination CMK key and create Alias. . Allow only EC2 role to encypt and decrypt and admin role to maintain the key.
4. Create and trigger Lambda functions to create and configure destination bucket
   1. Create destination bucket
   2. Update bucket properties to enable bucket versioning
   3. Update bucket properties to default encryption using aws:kms and created CMK
   4. Update bucket policy to deny upload objects which are not encrypted
   5. Update bucket lifecycle to move objects from standard s3 to glacier. Rotation period 7 days in stander s3 and one year in glacier before delete them from glacier.
5. Create source CMK key and create Alias in current region. Allow only EC2 role to encypt and decrypt and admin role to maintain the key.
6. Create s3 service role to allow s3 replication. Create custom policy to allow only replication objects which are encrypt using source CMK and encrypt them back using target CMK key.
7. Create and configure source bucket
   1. Update bucket properties to enable bucket versioning
   2. Update bucket properties to default encryption using aws:kms and created CMK
   3. Update bucket policy to deny upload objects which are not encrypted
   4. Update **bucket p**roperties to default encryption using aws:kms and created CMK
   5. Update bucket policy to deny upload objects which are not encrypted
   6. Update bucket lifecycle to move objects from standard s3 to glacier. Rotation period 7 days in stander s3 and one year in glacier before delete
8. Enable bucket replication.

**Note**: The creation of the IAM role and Lambda function is automated in the template. You do not need not create them manually.



**Step-by-step Instructions**

1. Download the CFT and Lamdba from code.amazon.com.
2. Create s3 bucket for Lambda code. The Bucket name will be as Parameters when launch the CFT
3. Copy the createDesbucket.zip to above bucket.
4. Launch the CloudFormation in the region to create source bucket.
5. Enter the parameters as defined in this document