## **IMPLEMENTING BI-DIRECTIONAL CROSS-REGION REPLICATION (CRR) FOR AMAZON SIMPLE STORAGE SERVICE (AMAZON S3)**

## **Introduction**

## This hands-on lab will guide you through the steps to improve reliability of your service and its data using automatic asynchronous backup of encrypted data you store in Amazon S3. Your Amazon S3 data will be securely backed up to a different AWS region.

## TwoReplicationRules

By the end of this lab, you will be able to:

* Perform data backup automatically for objects in Amazon S3 buckets
* Secure and encrypt backups of objects in Amazon S3
* Automate disaster recovery (DR) of your objects in Amazon S3
* Query CloudTrail logs to improve your understanding of how cross-region replication works for Amazon S3

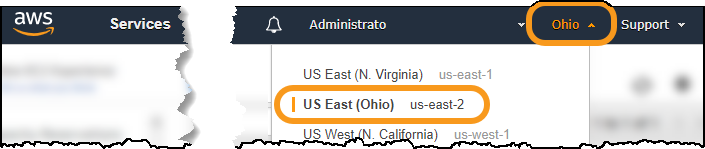
## **Deploy the Infrastructure**

### **1.1 Log into the AWS console**

### **1.2 Deploy the infrastructure in two AWS Regions using an AWS CloudFormation template**

You will deploy the infrastructure for two Amazon S3 buckets. Since these will be in two different regions, you will need to create an AWS CloudFormation stack in each region. You will use the same CloudFormation template for both regions.

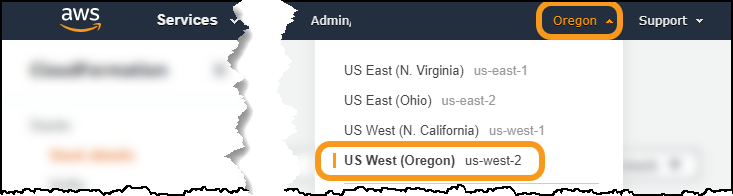
#### **1.2.1 Deploy east S3 bucket**

1. It is recommended that you deploy the east s3 bucket in the **Ohio** region. This region is also known as **us-east-2**.
   * Use the drop-down to select this region[](https://wellarchitectedlabs.com/Reliability/200_Bidirectional_Replication_for_S3/Images/SelectOhio.png)
   * If you choose to use a different region, you will need to ensure future steps are consistent with your region choice.
2. On the AWS Console go to the [CloudFormation console](https://console.aws.amazon.com/cloudformation" \t "_blank)
3. Select **Stacks**
4. Create a CloudFormation stack (with new resources) using the CloudFormation Template file and the **Upload a template file** option.
5. For **Stack name** use **S3-CRR-lab-east**
6. Under **Parameters** enter a **NamingPrefix**
   * This will be used to name your S3 buckets
   * Must be string consisting of lowercase letters, numbers, periods (.), and dashes (-) between five and 40 characters
   * This will be part of your Amazon S3 bucket name, which must be unique across all of S3.
   * Record this value in an accessible place – you will need it again later in the lab.
7. Click **Next** until the last page
8. At the bottom of the page, select **I acknowledge that AWS CloudFormation might create IAM resources with custom names**
9. Click **Create stack**
10. You can go ahead and create the west bucket before this CloudFormation stack completes

**Troubleshooting**: If your CloudFormation stack deployment fails with the error <bucket name> already exists

* You did not pick a unique enough **NamingPrefix**
* Delete the failed stack
* Start over and choose a more unique **NamingPrefix**
* Amazon S3 bucket names share a global name space across all of AWS (including all AWS regions)

#### **1.2.2 Deploy west S3 bucket**

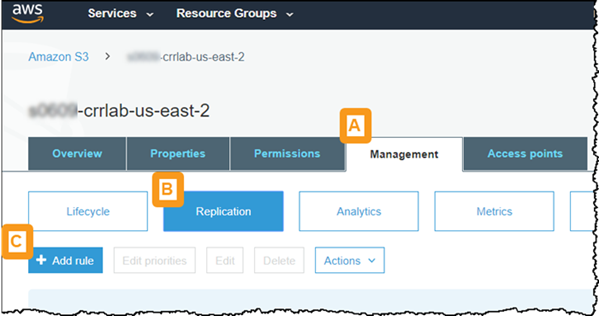
1. It is recommended that you deploy the west s3 bucket in the **Oregon** region for this lab. This region is also known as **us-west-2**.
   * Use the drop-down to select this region[](https://wellarchitectedlabs.com/Reliability/200_Bidirectional_Replication_for_S3/Images/SelectOregon.png)
   * If you choose to use a different region, you will need to ensure future steps are consistent with your region choice.
2. On the AWS Console go to the [CloudFormation console](https://console.aws.amazon.com/cloudformation" \t "_blank)
3. Select **Stacks**
4. Create a CloudFormation stack (with new resources) using the same CloudFormation Template file as before, and the **Upload a template file** option.
5. For **Stack name** use **S3-CRR-lab-west**
6. Under **Parameters** enter a **NamingPrefix**
   * You must use the same value as you did previously
7. Click **Next** until the last page
8. At the bottom of the page, select **I acknowledge that AWS CloudFormation might create IAM resources with custom names**
9. Click **Create stack**

#### **1.2.3 Get bucket information**

1. Go back to the **Ohio** AWS Region and wait for the CloudFormation stack you created there to complete
2. Click on the **Outputs** tab and record the **Value** of the S3 bucket name in an accessible location as east bucket
3. Go to the the **Oregon** AWS Region and do the same thing, copying that S3 bucket name down as west bucket
4. Go to the [Amazon S3 console](https://s3.console.aws.amazon.com/s3/home) and verify that both buckets were created.
   * Although S3 buckets are specific to an AWS region, the Amazon S3 console shows all buckets from all AWS Regions
   * The two S3 buckets you will work with begin with <your\_naming\_prefix>-crrlab
   * Note the regions for the two S3 buckets your created
   * There are also two new logging buckets – you will not need to do any actions with these.
5. Click on either the east region or west region bucket, and note the following
   * **This bucket is empty** - We will be adding objects to the bucket soon
   * Click on **Properties** and note what properties are Enabled
6. Versioning is Enabled: For S3 Replication, both source and destination buckets MUST have versioning enabled
7. Default encryption is Enabled: In our exercise we are demonstrating replication of encrypted objects. It is a best practice to encrypt your data at rest.
8. Object-level logging is Enabled: This logging will be used later in the lab. It is used to better understand replication operations AWS takes on your behalf.

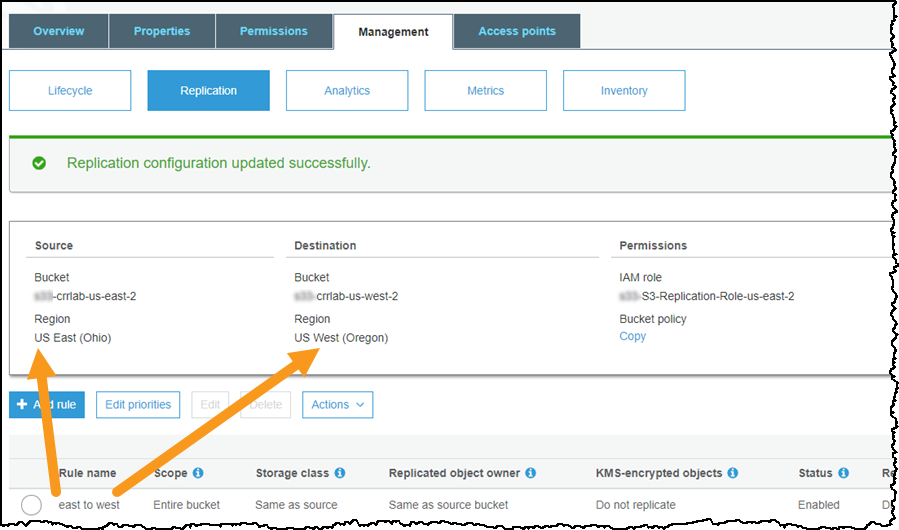
### **2.1 Setup rule #1 to replicate objects from east bucket to west bucket**

1. Go to the [Amazon S3 console](https://s3.console.aws.amazon.com/s3/home)
2. Click on the name of the east bucket
   * if you used **Ohio** the name will be <your\_naming\_prefix>-crrlab-us-east-2
3. Click on the **Management** tab (Step A in screenshot)
4. Click **Replication** (Step B in screenshot)
5. Click **+ Add Rule** (Step C in screenshot)

[](https://wellarchitectedlabs.com/Reliability/200_Bidirectional_Replication_for_S3/Images/AddRule.png)

1. For **Set source** select **Entire bucket**
2. For **Replication criteria** leave **Replicate objects encrypted with AWS KMS** not selected
   * Our objects are encrypted using server-side encryption
   * However since you used SSE-S3 encryption, you do not need to select this option and do not need to provide a KMS key
   * SSE-S3 uses KMS keys, but these managed by Amazon S3 for the user
   * For more detail see [What Does Amazon S3 Replicate?](https://docs.aws.amazon.com/AmazonS3/latest/dev/replication-what-is-isnot-replicated.html)
3. Click **Next**
4. For **Destination bucket** leave **Buckets in this account** selected, and select the name of the west bucket from the drop-down
   * If you used **Oregon** the name will be <your\_naming\_prefix>-crrlab-us-west-2
   * **Troubleshooting**: If you get an error saying The bucket doesn’t have versioning enabled then you have chosen the wrong bucket. Double check the bucket name.
5. Click **Next**
6. For **IAM Role** select **<your-naming-prefix>-S3-Replication-Role-us-east-2** from the search results box
   * (If you chose a different region as your east region, then look for that region at the end of the IAM role name)
7. For **Rule name** enter east to west
8. Leave **Status** set to **enabled**
9. Click **Next**
10. Review the configuration
11. Click **Save**

The screen should say **Replication configuration updated successfully.** and display the Source, Destination, and Permissions of your replication rule

[](https://wellarchitectedlabs.com/Reliability/200_Bidirectional_Replication_for_S3/Images/RuleOneCreated.png)

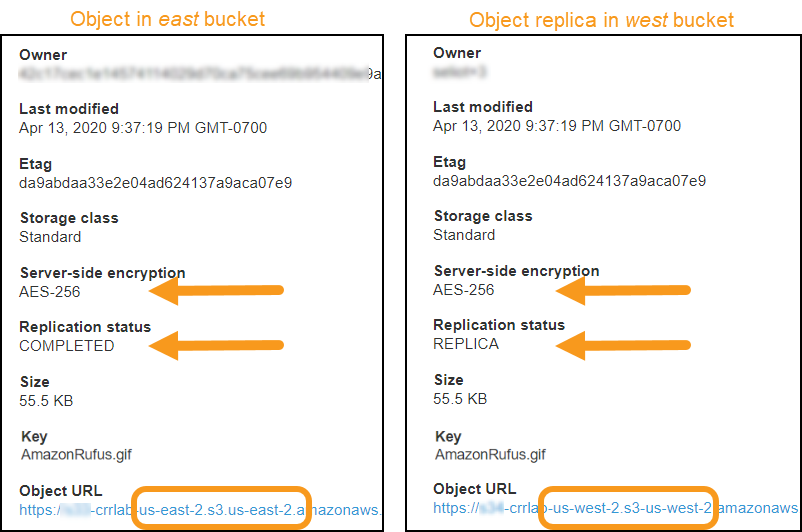
### **2.2 Test replication rule #1 - replicate object from east bucket to west bucket**

To test this rule you will upload an object into the east bucket and observe that it is replicated into the west bucket. For this step you will need a test object:

* This is a file that you will upload into the east S3 bucket.
* It should not be too big, as this will increase the time to upload it from your computer.
* If you do not have a file to use, you can save this image

Right-click and **Save image as…**[](https://wellarchitectedlabs.com/Reliability/200_Bidirectional_Replication_for_S3/Images/TestObject_AmazonRufus.gif)

1. Go to the [Amazon S3 console](https://s3.console.aws.amazon.com/s3/home) , or if you are already there click on **Amazon S3** in the upper left corner
2. Click on the name of the east bucket
   * if you used **Ohio** the name will be <your\_naming\_prefix>-crrlab-us-east-2
3. Click on **⬆ Upload**
4. Upload the file you will use as an object
   * Drag and drop the file or click **Add files**
   * Click **Upload** (note there is a **Next** button, but you do not need to click it)
5. When the file is finished uploading, click on the filename
   * It will look like the left side of the screenshot below
   * If **Replication status** is **PENDING**, wait and refresh until it says **COMPLETED** which should be just a few seconds.
6. At the top of the console click on **Amazon S3** and then click on the name of the west bucket
   * If you used **Oregon** the name will be <your\_naming\_prefix>-crrlab-us-west-2
7. Click on the filename of the file that you just uploaded to the other bucket (yes, it is here now too!)
   * It will look like the right side of the screenshot below

[](https://wellarchitectedlabs.com/Reliability/200_Bidirectional_Replication_for_S3/Images/ReplicatedObject.png)

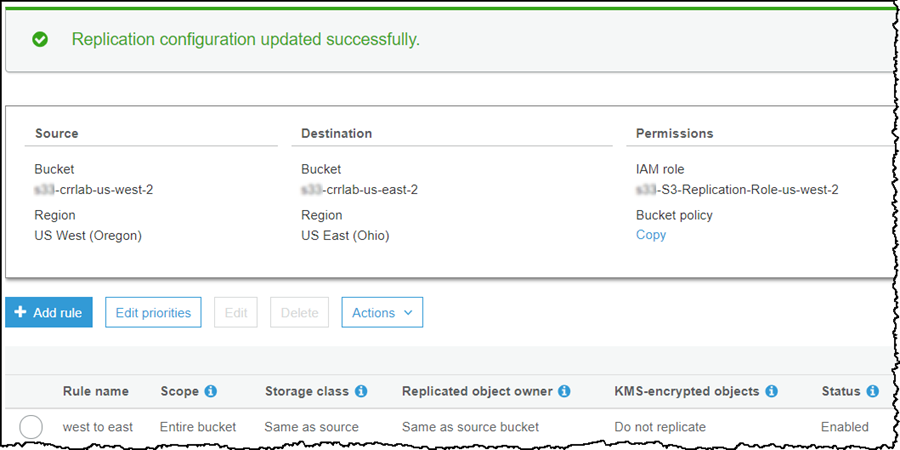
1. Note the following in from the object details:
   * **Replication status**: Note the different values for the source (east) and destination (west) S3 buckets. The value **REPLICA** in the west bucket is part of the solution how the system recognizes it should not replicate this object back again to the east bucket, which would cause an infinite loop.
   * **Server-side encryption**: The object was encrypted in the source (east) bucket, and remains encrypted in the destination (west) bucket.

### **2.3 Setup rule #2 to replicate objects from west bucket to east bucket**

After setting up the second rule, you will have completed configuration of bi-directional replication between our two Amazon S3 buckets.

1. Go to the [Amazon S3 console](https://s3.console.aws.amazon.com/s3/home) , or if you are already there click on **Amazon S3** in the upper left corner
2. Click on the name of the west bucket
   * if you used **Oregon** the name will be <your\_naming\_prefix>-crrlab-us-west-2
3. Click on the **Management** tab
4. Click **Replication**
5. Click **+ Add Rule**
6. For **Set source** select **Entire bucket**
7. For **Replication criteria** leave **Replicate objects encrypted with AWS KMS** not selected
   * Our objects are encrypted using server-side encryption
   * However since you used SSE-S3 encryption, you do not need to select this option and do not need to provide a KMS key
   * SSE-S3 uses KMS keys, but these managed by Amazon S3 for the user
   * For more detail see [What Does Amazon S3 Replicate?](https://docs.aws.amazon.com/AmazonS3/latest/dev/replication-what-is-isnot-replicated.html)
8. Click **Next**
9. For **Destination bucket** leave **Buckets in this account** selected, and select the name of the east bucket from the drop-down
   * If you used **Ohio** the name will be <your\_naming\_prefix>-crrlab-us-east-2
   * **Troubleshooting**: If you get an error saying The bucket doesn’t have versioning enabled then you have chosen the wrong bucket. Double check the bucket name.
10. Click **Next**
11. For **IAM Role** select **<your-naming-prefix>-S3-Replication-Role-us-west-2** from the search results box
    * (If you chose a different region as your west region, then look for that region at the end of the IAM role name)
12. For **Rule name** enter west to east
13. Leave **Status** set to **enabled**
14. Click **Next**
15. Review the configuration
16. Click **Save**

The screen should say **Replication configuration updated successfully.** and display the Source, Destination, and Permissions of your replication rule

[](https://wellarchitectedlabs.com/Reliability/200_Bidirectional_Replication_for_S3/Images/RuleTwoCreated.png)

### **3.1 Upload objects to their respective Amazon S3 buckets**

#### **3.1.1 Upload object #1 to the east S3 bucket**

1. Go to the [Amazon S3 console](https://s3.console.aws.amazon.com/s3/home) , or if you are already there click on **Amazon S3** in the upper left corner
2. Click on the name of the east bucket
   * if you used **Ohio** the name will be <your\_naming\_prefix>-crrlab-us-east-2
3. Click on **⬆ Upload**
4. Upload the file you will use as object #1
   * Drag and drop the file or click **Add files**
   * Click **Upload** (note there is a **Next** button, but you do not need to click it)

#### **3.1.2 Upload object #2 to the west S3 bucket**

1. Click on **Amazon S3** in the upper left corner of the Amazon S3 console
2. Click on the name of the west bucket
   * if you used **Oregon** the name will be <your\_naming\_prefix>-crrlab-us-west-2
3. Click on **⬆ Upload**
4. Upload the file you will use as object #2
   * Drag and drop the file or click **Add files**
   * Click **Upload** (note there is a **Next** button, but you do not need to click it)

### **3.2 Verify bi-directional replication**

1. You are already looking at the objects in the west bucket
   * Verify that object #1, that you uploaded to the east bucket is present here also
   * Note the **Replication status** is **REPLICA**
2. Click on **Amazon S3** in the upper left corner
3. Click on the name of the east bucket
   * Verify that object #2, that you uploaded to the west bucket is present here also
   * Note the **Replication status** is **REPLICA**

### **3.3 Explore which Amazon S3 events trigger replication and which do not**

#### **3.3.1 Use CloudWatch Logs Insights to query the CloudTrail logs**

AWS CloudTrail is a service that provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. You will use AWS CloudTrail to explore which Amazon S3 events trigger replication to occur.

1. Change back to the east AWS region
   * If you used the directions in this lab, then this is **Ohio (us-east-2)**
2. The CloudFormation template you deployed configured CloudTrail to deliver a trail to CloudWatch Logs. Therefore:
   * Go to the [CloudWatch console](https://console.aws.amazon.com/cloudwatch" \t "_blank)
   * Click on **Insights** (under **Logs**) on the left
3. Where it says **Select log group(s)** select the one named CloudTrail/logs/<your\_prefix\_name>
4. Right below that is where you can enter a query
   * Delete the query that is there
   * and enter the following query. It returns all PutObject requests on S3 buckets
   * fields @timestamp, requestParameters.key AS key,
   * | requestParameters.bucketName AS bucket,
   * | userIdentity.invokedBy AS invokedBy,
   * | userIdentity.arn AS arn,
   * | userIdentity.sessionContext.sessionIssuer.userName AS UserName
   * | filter eventName ='PutObject'
   * | sort @timestamp desc
   * | limit 20
5. Click **Run query**
6. Look at the results at the bottom of the screen

#### **3.3.2 Difference between uploaded and replicated objects in S3 bucket**

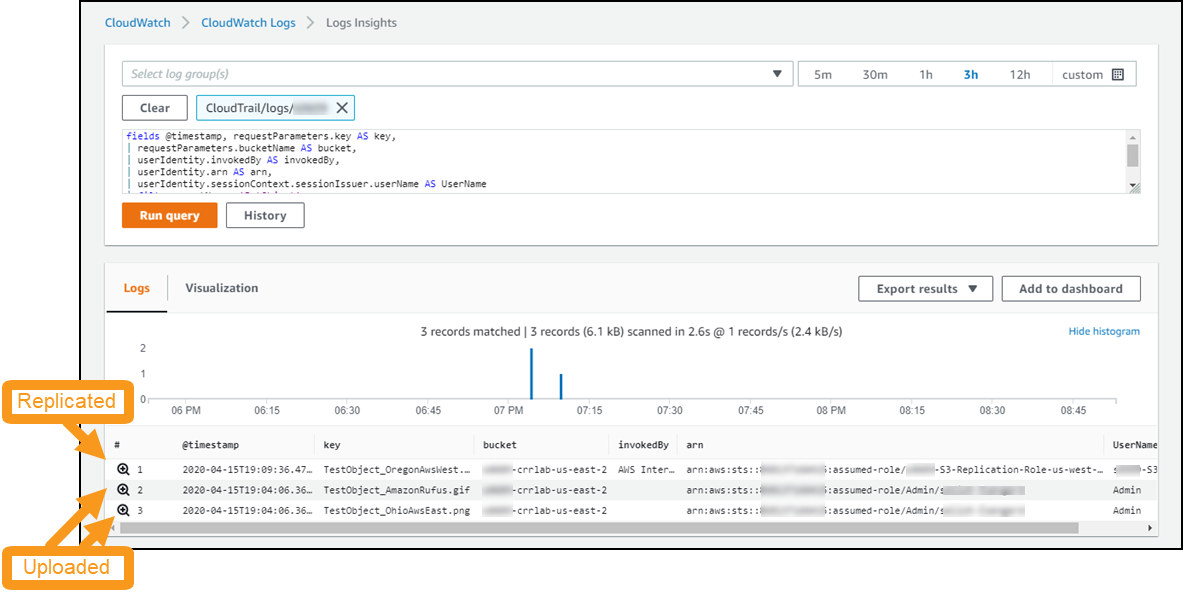
You are looking for three results, one for each of the test objects you uploaded. Use the key field to see the test object names.

* For these events look at the tabular attributes returned by the query at the bottom of the page
  + However, if you want to see all the attributes, you can click to the left of each event
* The three events correspond to each of the objects you put into the S3 buckets
  + The object you put into the east bucket testing rule #1
  + The object you put into the east bucket testing bi-directional replication
  + The object you put into the west bucket testing bi-directional replication
    - Look at the bucket for this event. This event is for the east bucket
    - This is actually the replication event for the object you put into the west bucket
* What is different between events where you uploaded the object into the bucket and events where the object was put into the bucket by replication?

Replicated objects have a userIdentity.invokedBy value of “AWS Internal”

The userIdentity is different - see the arn and username

The CloudWatch Logs Insights page should look like this:

[](https://wellarchitectedlabs.com/Reliability/200_Bidirectional_Replication_for_S3/Images/CloudTrailForS3.png)

The result is:

* For an object uploaded by you
  + Amazon S3 triggers the rule you configured to replicate it to another bucket
  + And sets **Replication status** to **COMPLETED**
* For an object replicated from another bucket
  + Amazon S3 knows not to re-replicate the object
  + And sets **Replication status** to **REPLICA**

### **3.4 Additional exercises**

These are optional. They help you to explore and understand bi-direction cross-region replication on Amazon S3.

* Look at the **Permissions** on the **<your-naming-prefix>-S3-Replication-Role-…** IAM Roles
  + Why do they have the policies that they do?
* What happens when you rename an object in one of the buckets?
  + Hint: if you cannot figure it out consider that versioning is enabled (and must be enabled for replication to work)
* Switch to the west AWS region and run the same CloudWatch Insights Query there.
  + What do you expect?

### **3.5 Summary**

You created two S3 buckets in two different AWS regions. You then setup bi-directional cross-region replication (CRR) between the two Amazon S3 buckets. Putting an object in either bucket resulted in the object asynchronously being backed up to the other bucket. Objects encrypted in their original bucket are also encrypted in their replication bucket. Objects are replicated once – replication “looping” is prevented.

### **Empty the S3 buckets**

You cannot delete an Amazon S3 bucket unless it is empty, so you need to empty the buckets you created. There are a total of four buckets:

* Replication bucket in east region: <your\_naming\_prefix>-crrlab-us-east-2
* Replication bucket in west region: <your\_naming\_prefix>-crrlab-us-west-2
* Logging bucket in east region: logging-<your\_naming\_prefix>-us-east-2
* Logging bucket in west region: logging-<your\_naming\_prefix>-us-west-2

Go to the [Amazon S3 console](https://s3.console.aws.amazon.com/s3/home) , or if you are already there click on **Amazon S3** in the upper left corner

**For each of the four buckets do the following:**

1. Select the radio button next to the bucket
2. Click **Empty**
3. Type the bucket name in the confirmation box
4. Click **Empty**
5. After you see the message **Successfully emptied bucket** then click **Exit**
6. For the logging buckets it is also recommended your delete the bucket now to prevent the logs from writing more data there after you empty it
   * Follow the same steps as above, but click the **Delete** button (instead of Empty)

### **Remove AWS CloudFormation provisioned resources**

#### **How to delete an AWS CloudFormation stack**

If you are already familiar with how to delete an AWS CloudFormation stack, then skip to the next section: **Delete workshop CloudFormation stacks**

1. Go to the AWS CloudFormation console: <https://console.aws.amazon.com/cloudformation>
2. Select the CloudFormation stack to delete and click **Delete**
3. In the confirmation dialog, click **Delete stack**
4. The **Status** changes to DELETE\_IN\_PROGRESS
5. Click the refresh button to update and status will ultimately progress to DELETE\_COMPLETE
6. When complete, the stack will no longer be displayed. To see deleted stacks use the drop down next to the Filter text box.
7. To see progress during stack deletion
   * Click the stack name
   * Select the Events column
   * Refresh to see new events

#### **Delete CloudFormation stacks**

1. First delete the **S3-CRR-lab-east** CloudFormation stack in **Ohio** (**us-east-2**)
2. Then delete the **S3-CRR-lab-west** CloudFormation stack in **Oregon** (**us-west-2**)