Implementing Multi-Region Backup with Amazon S3 Cross-Region Replication

**SPL-DD-300-STS3BC-11-EN - Version 1.1.6**

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. All trademarks are the property of their owners.

Note: Do not include any personal, identifying, or confidential information into the lab environment. Information entered may be visible to others.

Corrections, feedback, or other questions? Contact us at [*AWS Training and Certification*](https://support.aws.amazon.com/#/contacts/aws-training).

**Lab overview**

Amazon Simple Storage Service (Amazon S3) is an object storage service built to store and retrieve any amount of data from anywhere on the Internet. It offers an extremely durable, highly available, and infinitely scalable data storage infrastructure at very low costs.

Amazon S3 supports Cross-Region Replication (CRR) for automatic, asynchronous copying of objects across buckets in different AWS Regions. Cross-Region Replication can help you:

* **Comply with compliance requirements** — Although Amazon S3 stores your data across multiple geographically distant Availability Zones by default, compliance requirements might dictate that you store data at even greater distances. Cross-region replication allows you to replicate data between distant AWS Regions to satisfy these requirements.
* **Minimize latency** — If your customers are in two geographic locations, you can minimize latency in accessing objects by maintaining object copies in AWS Regions that are geographically closer to your users.
* **Increase operational efficiency** — If you have compute clusters in two different AWS Regions that analyze the same set of objects, you might choose to maintain object copies in those Regions.
* **Maintain object copies under different ownership** — Regardless of who owns the source object you can tell Amazon S3 to change replica ownership to the AWS account that owns the destination bucket. This is referred to as the owner override option. You might use this option to restrict access to object replicas.

This lab demonstrates the process of configuring Cross-Region Replication (CRR) between two S3 buckets in separate regions.

TOPICS COVERED

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

* Create source and destination S3 buckets with versioning enabled.
* Create a Cross-Region Replication policy.
* Enable replication for an entire bucket, encrypted files, a specific folder, or a specific tag.
* Identify the conditions necessary for replicating objects.
* Delete replicated files and understand how deletions are replicated.

TECHNICAL KNOWLEDGE PREREQUISITES

To successfully complete this lab, you should be familiar with basic navigation of the AWS Management Console and Amazon S3 buckets.

ICON KEY

Various icons are used throughout this lab to call attention to certain aspects of the guide. The following list explains the purpose for each one:

* **Command:** The keyboard icon specifies that you must run a command.
* **Expected output:** The clipboard icon indicates that you can verify the output of a command or edited file by comparing it to the provided example.
* **Note:** The note icon specifies important hints, tips, guidance, or advice.
* **Additional information:** The “i” circle icon specifies where to find more information.
* **WARNING:** Draws special attention to actions that are irreversible and could potentially impact the failure of a command or process. Includes warnings about configurations that cannot be changed after they are made.
* **Copy/paste:** In some cases, you may run a script or apply a file that has been pre-created for you. This icon signifies a code block that is used to display the contents of the script or file you interacted with.

**Start lab**

1. To launch the lab, at the top of the page, choose **Start lab**.

 You must wait for the provisioned AWS services to be ready before you can continue.

1. To open the lab, choose **Open Console**.

You are automatically signed in to the AWS Management Console in a new web browser tab.

**Do not change the Region unless instructed.**

COMMON SIGN-IN ERRORS

**Error: You must first sign out**



If you see the message, **You must first log out before logging into a different AWS account:**

* Choose the **click here** link.
* Close your **Amazon Web Services Sign In** web browser tab and return to your initial lab page.
* Choose **Open Console** again.

**Error: Choosing Start Lab has no effect**

In some cases, certain pop-up or script blocker web browser extensions might prevent the **Start Lab** button from working as intended. If you experience an issue starting the lab:

* Add the lab domain name to your pop-up or script blocker’s allow list or turn it off.
* Refresh the page and try again.

**Task 1: Create and configure source and destination buckets**

Before Cross-Region Replication (CRR) can be enabled, you must first create the source and destination buckets. Versioning must be enabled for both buckets in order to configure CRR.

**WARNING:** Any objects that reside in the bucket before versioning is enabled will not be replicated. For more information about S3 Versioning, refer to *How S3 Versioning works* in the **Additional resources** section.

In this task, you create the source and destination buckets and enable versioning on each bucket.

TASK 1.1: CREATE THE SOURCE BUCKET

1. If you have not already done so, follow the steps in the [Start Lab](https://labs.skillbuilder.aws/sa/lab/arn%3Aaws%3Alearningcontent%3Aus-east-1%3A470679935125%3Ablueprintversion%2FSPL-DD-300-STS3BC-1%3A1.1.6-9105cc04/en-US#StartLab) section to log into the AWS Management Console.
2. At the top of the page, in the unified search bar, search for and choose

S3

1. On the Amazon S3 **Buckets** page, at the top-right corner, choose **Create bucket** .
2. On the **Create bucket** page:

* For **Bucket name**, enter the value of **SourceBucket** listed to the left of these instructions.
* For **AWS Region**, select the value of **PrimaryRegion** listed to the left of these instructions.
* Keep the remaining default values.

1. At the bottom of the page, choose **Create bucket** .

TASK 1.2: ENABLE VERSIONING ON THE SOURCE BUCKET

1. On the **Buckets** page, choose the link for the **source-bucket** bucket.
2. On the **source-bucket** details page, choose the **Properties** tab.
3. In the **Bucket Versioning** section, choose **Edit** .
4. On the **Edit Bucket Versioning** page:

* For **Bucket Versioning**, select **Enable**.

1. At the bottom right-hand corner of the page, choose **Save changes** .

You have now enabled versioning on the source bucket.

TASK 1.3: CREATE DESTINATION BUCKET AND ENABLE VERSIONING

Now that you have created the source bucket and enabled versioning on it, you create the destination bucket to replicate objects to. The destination bucket must have versioning enabled as well, but this time you enable it using the bucket creation wizard.

1. In the navigation breadcrumbs at the top of the page, choose the **Amazon S3** link to return to the **Buckets** page.
2. On the Amazon S3 **Buckets** page, at the top-right corner, choose **Create bucket** .
3. On the **Create bucket** page:

* For **Bucket name**, enter the value of **DestinationBucket** listed to the left of these instructions.
* For **AWS Region**, select the value of **SecondaryRegion** listed to the left of these instructions.
* For **Bucket Versioning**, select **Enable**.
* Keep the remaining default values.

1. At the bottom of the page, choose **Create bucket** .
2. On the **Buckets** page, choose the link for the **destination-bucket** bucket.
3. Choose the **Properties** tab.
4. In the **Bucket Versioning** section, verify **Bucket Versioning** is set to **Enabled**.
5. Return to the S3 **Buckets** page.

**Congratulations!** You have successfully created source and destination buckets and enabled versioning on each one.

**Task 2: Enable Cross-Region Replication on a bucket**

Now that you have created and configured the source and destination buckets, you can enable replication. Replication rules are used to determine which objects in a bucket are replicated. You can replicate an entire bucket, a specific folder within a bucket, or any objects with a specified tag. You can replicate objects to a bucket in the same or different regions. Since you are exploring Cross-Region Replication, you replicate to a different region.

**WARNING:** Objects that already exist in the bucket before replication is enabled will **NOT** be replicated. By default, only new objects uploaded to a bucket after replication is enabled are replicated. However, if you have a need to replicate existing objects, you can use S3 Batch Replication. For more information, refer to *Replicating existing objects with S3 Batch Replication* in the **Additional resources** section.

In this task, you create a replication policy to enable replication of an entire bucket. You then upload an object to the source bucket and verify that it is replicated to the destination bucket.

TASK 2.1: UPLOAD A FILE TO THE SOURCE BUCKET BEFORE ENABLING REPLICATION

First, upload a sample file to the source bucket to demonstrate how a replication policy does not apply to objects that exist in the bucket before creating the policy.

1. Download the following file to your device: [pre-crr.txt](https://us-west-2-tcprod.s3.us-west-2.amazonaws.com/courses/SPL-DD-300-STS3BC/v1.1.6.prod-81f3fb4e/sample_files/pre-crr.txt)
2. On the **Buckets** page, choose the link for the **source-bucket** bucket.
3. Choose **Upload** .
4. Choose **Add files** .
5. Browse to and select the **pre-crr.txt** file you downloaded previously.
6. At the bottom of the page, choose **Upload** .

**Expected service output:**

**Upload succeeded**

1. At the top right-hand corner of the page, choose **Close** .

TASK 2.2: CREATE A REPLICATION RULE FOR THE ENTIRE BUCKET

1. On the **source-bucket** details page, choose the **Management** tab.
2. In the **Replication rules** section, choose **Create replication rule** .
3. On the **Create replication rule** page:

* In the **Replication rule configuration** section, for **Replication rule name**, enter

crr-full-bucket

* In the **Source bucket** section, for **Choose a rule scope**, select  **Apply to all objects in the bucket**.
* In the **Destination** section, for **Destination**, select  **Choose a bucket in this account**.
* For **Bucket name**, enter the value of **DestinationBucket** listed to the left of these instructions.
* In the **IAM role** section, select  **Choose from existing IAM roles** and for the **IAM role** drop-down menu, choose **S3-CRR-Role**.

 The **S3-CRR\_Role** IAM role grants permissions to the S3 service that allow it to perform Get, List, and Replicate operations on the source and destination buckets. The role looks similar to this, though the bucket names will differ:

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"s3:GetReplicationConfiguration",

"s3:ListBucket"

],

"Resource": [

"arn:aws:s3:::source-bucket-57538018"

]

},

{

"Effect": "Allow",

"Action": [

"s3:GetObjectVersionForReplication",

"s3:GetObjectVersionAcl",

"s3:GetObjectVersionTagging"

],

"Resource": [

"arn:aws:s3:::source-bucket-57538018/\*"

]

},

{

"Effect": "Allow",

"Action": [

"s3:ReplicateObject",

"s3:ReplicateDelete",

"s3:ReplicateTags"

],

"Resource": "arn:aws:s3:::destination-bucket-57538018/\*"

}

]

}

 For more information about the permissions required to enable replication, refer to *Setting up permissions* in the **Additional resources** section.

1. At the bottom of the page, choose **Save** .

**Note:** The browser opens the **Replicate existing objects** pop-up menu.

1. For the **Existing objects** option, choose  **No, do not replicate existing objects**.
2. Choose **Submit** .

**Expected service output:**

**Replication configuration successfully updated**

1. In the navigation breadcrumbs at the top of the page, choose the **Amazon S3** link to return to the **Buckets** page.
2. Choose the link for the **destination-bucket** bucket.

Notice that the destination bucket is empty, even though replication is enabled and the source bucket contains a file. Only **new** files uploaded to the source bucket **after** replication is enabled will be replicated to the destination bucket.

TASK 2.3: UPLOAD A NEW FILE AND VERIFY IT REPLICATES SUCCESSFULLY

1. Download the following file to your device: [crr-bucket.txt](https://us-west-2-tcprod.s3.us-west-2.amazonaws.com/courses/SPL-DD-300-STS3BC/v1.1.6.prod-81f3fb4e/sample_files/crr-bucket.txt)
2. In the navigation breadcrumbs at the top of the page, choose the **Amazon S3** link to return to the **Buckets** page.
3. On the **Buckets** page, choose the link for the **source-bucket** bucket.
4. Choose **Upload** .
5. Choose **Add files** .
6. Browse to and select the **crr-bucket.txt** file you downloaded previously.
7. At the bottom of the page, choose **Upload**

**Expected service output:**

**Upload succeeded**

1. At the top right-hand corner of the page, choose **Close** .
2. In the navigation breadcrumbs at the top of the page, choose the **Amazon S3** link to return to the **Buckets** page.
3. Choose the link for the **destination-bucket** bucket.

Notice that the destination bucket now contains the **crr-bucket.txt** file you uploaded to the source bucket.

 If no files are listed, wait a few seconds, and then choose the  refresh button above the list of objects. It may take a minute or two for the object to replicate.

**Congratulations!** You have successfully configured Cross-Region Replication for an entire S3 bucket.

**Task 3: Replicate encrypted files**

In this task, you upload an encrypted object to an S3 bucket and validate whether or not it replicates using the destination bucket.

TASK 3.1: UPLOAD A KMS-ENCRYPTED FILE

1. Download the following file to your device: [crr-encrypted.txt](https://us-west-2-tcprod.s3.us-west-2.amazonaws.com/courses/SPL-DD-300-STS3BC/v1.1.6.prod-81f3fb4e/sample_files/crr-encrypted.txt)
2. In the navigation breadcrumbs at the top of the page, choose the **Amazon S3** link to return to the **Buckets** page.
3. On the **Buckets** page, choose the link for the **source-bucket** bucket.
4. Choose **Upload** .
5. Choose **Add files** .
6. Browse to and select the **crr-encrypted.txt** file you downloaded previously.
7. At the bottom of the page, choose **Properties** to expand it.
8. In the **Server-side encryption settings** section:

* For **Server-side encryption**, select **Specify an encryption key**.
* For Encryption settings, select **Override bucket settings for default encryption**.
* For **Encryption key type**, select **AWS Key Management Service key (SSE-KMS)**.
* For **AWS KMS key**, Choose from your **AWS KMS keys**.
* For Available **AWS KMS keys**: Choose the key from the drop down

1. At the bottom of the page, choose **Upload** .

**Expected service output:**

**Upload succeeded**

1. At the top right-hand corner of the page, choose **Close** .
2. In the navigation breadcrumbs at the top of the page, choose the **Amazon S3** link to return to the **Buckets** page.
3. Choose the link for the **destination-bucket** bucket.

Notice that the destination bucket does not contain a copy of the KMS encrypted file, even though replication is enabled for the entire source bucket. When you created the replication rule, you kept the default option for encryption, which is to not replicate KMS-encrypted files. Since the file you just uploaded is KMS-encrypted, it was not replicated to the destination bucket.

TASK 3.2: EDIT THE REPLICATION RULE

Next, edit the replication rule to allow replication of KMS-encrypted files.

1. In the navigation breadcrumbs at the top of the page, choose the **Amazon S3** link to return to the **Buckets** page.
2. Choose the link for the **source-bucket** bucket.
3. On the **source-bucket** details page, choose the **Management** tab.
4. In the **Replication rules** section, select the **crr-full-bucket** rule you created previously, and then choose **Edit rule** .
5. On the **Edit replication rule** page:

* In the **Encryption** section, select **Replicate objects encrypted with AWS KMS**. Additional options appear.
* For **AWS KMS key for encrypting destination objects**, Choose from your **AWS KMS keys**.
* For Available **AWS KMS keys**: Choose the key from the drop down

1. At the bottom of the page, choose **Save** .

**Expected service output:**

**Replication configuration successfully updated**

**Note:** Changes to replication rules only affect objects that are uploaded **after** you change the rule. Next, upload the encrypted file again to invoke the replication rule.

TASK 3.3: TEST THE ENCRYPTED FILE REPLICATION RULE

1. In the navigation breadcrumbs at the top of the page, choose the **source-bucket** link to return to the source-bucket details page.
2. Choose **Upload** .
3. Choose **Add files** .
4. Browse to and select the **crr-encrypted.txt** file you downloaded previously.
5. At the bottom of the page, choose **Properties** to expand it.
6. In the **Server-side encryption settings** section:

* For **Server-side encryption**, select **Specify an encryption key**.
* For **Encryption key type**, select **AWS Key Management Service key (SSE-KMS)**.
* For **AWS KMS key**, select **AWS managed key (aws/s3)**.

1. At the bottom of the page, choose **Upload** .

**Expected service output:**

**Upload succeeded**

1. At the top right-hand corner of the page, choose **Close** .
2. In the navigation breadcrumbs at the top of the page, choose the **Amazon S3** link to return to the **Buckets** page.
3. Choose the link for the **destination-bucket** bucket.

Notice that the destination bucket now contains the **crr-encrypted.txt** file you uploaded to the source bucket.

**Note:** If the expected files are not listed, wait a few seconds, and then choose the  refresh button above the list of objects.

 For more information about replicating encrypted objects, refer to *Replicating objects created with server-side encryption (SSE-C, SSE-S3, SSE-KMS* in the **Additional resources** section.

**Congratulations!** You have successfully configured a replication rule to allow for replication of KMS-encrypted files and verify the encrypted file was replicated.

**Task 4: Configure replication of a single folder**

In Amazon S3, folders are considered prefixes. For example, a folder in your S3 bucket named **Source** would be a prefix notated as **Source/**. A file inside that folder would be notated as **Source/File**.

In this task, you create a replication policy based on a prefix to replicate only objects in the specified folder. Choosing a folder to replicate allows you to replicate a specific set of objects easily, rather than an entire bucket.

TASK 4.1: CREATE A FOLDER IN THE SOURCE BUCKET

1. In the navigation breadcrumbs at the top of the page, choose the **Amazon S3** link to return to the **Buckets** page.
2. On the **Buckets** page, choose the link for the **source-bucket** bucket.
3. Choose **Create folder** .
4. On the **Create folder page**:

* For **Folder name**, enter

crr-test

1. At the bottom of the page, choose **Create folder** .

TASK 4.2: DELETE THE CURRENT REPLICATION POLICY

Next, delete the replication policy you created previously so it does not override the policy you create in an upcoming task.

1. On the **source-bucket** details page, choose the **Management** tab.
2. In the **Replication rules** section, select the  **crr-full-bucket** rule you created previously, and then choose **Delete** .
3. In the **Delete replication rule?** pop-up window, choose **Delete replication rule** .

TASK 4.3: CREATE A REPLICATION RULE FOR A SINGLE FOLDER

1. On the **source-bucket** details page, in the **Replication rules** section, choose **Create replication rule** .
2. On the **Create replication rule** page:

* In the **Replication rule configuration** section, for **Replication rule name**, enter

crr-folder-only

.

* For **Status**, choose  **Enabled**.
* In the **Source bucket** section, for **Choose a rule scope**, select  **Limit the scope of this rule using one or more filters**.
* For **Prefix**, enter

crr-test/

* In the **Destination** section, for **Destination**, select  **Choose a bucket in this account**.
* For **Bucket name**, enter the value of **DestinationBucket** listed to the left of these instructions.
* In the **IAM role** section, select  **Choose from existing IAM roles** and for the **IAM role** drop-down menu, choose **S3-CRR-Role**.

1. At the bottom of the page, choose **Save** .

**Note:** The browser opens the **Replicate existing objects** pop-up menu.

1. For the **Existing objects** option, choose  **No, do not replicate existing objects**.
2. Choose **Submit** .

**Expected service output:**

**Replication configuration successfully updated**

TASK 4.4: TEST THE FOLDER REPLICATION RULE

1. Download the following files to your device:

* [crr-folder.txt](https://us-west-2-tcprod.s3.us-west-2.amazonaws.com/courses/SPL-DD-300-STS3BC/v1.1.6.prod-81f3fb4e/sample_files/crr-folder.txt)
* [crr-folder-root.txt](https://us-west-2-tcprod.s3.us-west-2.amazonaws.com/courses/SPL-DD-300-STS3BC/v1.1.6.prod-81f3fb4e/sample_files/crr-folder-root.txt)

1. In the navigation breadcrumbs at the top of the page, choose the **source-bucket** link to return to the source-bucket details page.

First, upload a sample file to the root of the bucket.

1. Choose **Upload** .
2. Choose **Add files** .
3. Browse to and select the **crr-folder-root.txt** file you downloaded previously.
4. At the bottom of the page, choose **Upload** .

**Expected output:**

**Upload succeeded**

1. At the top right-hand corner of the page, choose **Close** .

Next, upload a file to the **crr-test** folder.

1. Choose the link for the **crr-test** folder.
2. Choose **Upload** .
3. Choose **Add files** .
4. Browse to and select the **crr-folder.txt** file you downloaded previously.
5. At the bottom of the page, choose **Upload** .

**Expected output:**

**Upload succeeded**

1. At the top right-hand corner of the page, choose **Close** .

Now that you have uploaded the two sample files, verify that the replication has taken place according to the replication rule you created.

1. In the navigation breadcrumbs at the top of the page, choose the **Amazon S3** link to return to the **Buckets** page.
2. On the **Buckets** page, choose the link for the **destination-bucket** bucket.

You should see three objects listed in the bucket:

* crr-bucket.txt
* crr-encrypted.txt
* crr-test/

**Note:** The **crr-folder-root.txt** file that you uploaded to the root of the source bucket was not replicated to the destination bucket.

1. Choose the link for the **crr-test** folder.

You should see the **crr-folder.txt** file you uploaded to the crr-test folder in the source bucket.

**Note:** If the expected files are not listed, wait a few seconds, and then choose the  refresh button above the list of objects.

**Congratulations!** You have successfully configured Cross-Region Replication for a single folder within an S3 bucket.

**Task 5: Configure replication using tags**

Tags can be used to identify specific objects to replicate, rather than replicating the entire bucket or folder.

In this task, you create a replication rule to replicate any object with a specific tag.

**WARNING:** Much like versioning, objects with tags must be uploaded to the source bucket **after** the replication policy using tags has been created and enabled. Objects that are uploaded and tagged prior to the policy being created will **not** replicate.

TASK 5.1: DELETE THE CURRENT REPLICATION POLICY

First, delete the replication policy you created previously so it does not override the policy you create in an upcoming task.

1. In the navigation breadcrumbs at the top of the page, choose the **Amazon S3** link to return to the **Buckets** page.
2. On the **Buckets** page, choose the link for the **source-bucket** bucket.
3. On the **source-bucket** details page, choose the **Management** tab.
4. In the **Replication rules** section, select the **crr-folder-only** rule you created previously, and then choose **Delete** .
5. In the **Delete replication rule?** pop-up window, choose **Delete replication rule** .

TASK 5.2: CREATE A REPLICATION RULE FOR TAGGED OBJECTS

1. On the **source-bucket** details page, in the **Replication rules** section, choose **Create replication rule** .
2. On the **Create replication rule** page:

* In the **Replication rule configuration** section, for **Replication rule name**, enter

crr-tag-only

* In the **Source bucket** section, for **Choose a rule scope**, select **Limit the scope of this rule using one or more filters**.
* For **Tags**, choose **Add tag** A new set of fields appears.
* For **Key**, enter

replicate

* For **Value**, enter

yes

**Note:** Tag keys and values are case sensitive. For more information about tags, refer to *Tagging AWS Resources* in the **Additional resources** section.

* In the **Destination** section, for **Destination**, select **Choose a bucket in this account**.
* For **Bucket name**, enter the value of **DestinationBucket** listed to the left of these instructions.
* In the **IAM role** section, for **IAM role**, select **S3-CRR-Role**.

1. At the bottom of the page, choose **Save** .

**Expected output:**

**Replication configuration successfully updated**

TASK 5.3: TEST THE TAG REPLICATION RULE

1. Download the following files to your device:

* [crr-no-tag.txt](https://us-west-2-tcprod.s3.us-west-2.amazonaws.com/courses/SPL-DD-300-STS3BC/v1.1.6.prod-81f3fb4e/sample_files/crr-no-tag.txt)
* [crr-tag.txt](https://us-west-2-tcprod.s3.us-west-2.amazonaws.com/courses/SPL-DD-300-STS3BC/v1.1.6.prod-81f3fb4e/sample_files/crr-tag.txt)

1. In the navigation breadcrumbs at the top of the page, choose the **source-bucket** link to return to the source-bucket details page.

First, upload a sample file that is not tagged.

1. On the **source-bucket** details page, choose **Upload** .
2. Choose **Add files** .
3. Browse to and select the **crr-no-tag.txt** file you downloaded previously.
4. At the bottom of the page, choose **Upload** .

**Expected output:**

**Upload succeeded**

1. At the top right-hand corner of the page, choose **Close** .

Next, upload a sample file that is tagged.

1. Choose **Upload** .
2. Choose **Add files** .
3. Browse to and select the **crr-tag.txt** file you downloaded previously.
4. At the bottom of the page, choose **Properties** to expand it.
5. In the **Tags** section, choose **Add tag** and then:

* For **Key**, enter

replicate

* For **Value**, enter

yes

1. At the bottom of the page, choose **Upload** .

**Expected output:**

**Upload succeeded**

1. At the top right-hand corner of the page, choose **Close**

Now that you have uploaded the two sample files, verify that the replication has taken place according to the replication rule you created.

1. In the navigation breadcrumbs at the top of the page, choose the **Amazon S3** link to return to the **Buckets** page.
2. On the **Buckets** page, choose the link for the **destination-bucket** bucket.

You should see four objects listed in the bucket:

* crr-bucket.txt
* crr-encrypted.txt
* crr-tag.txt
* crr-test

Notice that the **crr-tag.txt** file that you tagged was replicated to the destination bucket. However, the **crr-no-tag.txt** file that you did not tag was not replicated.

**Note:** If the expected files are not listed, wait a few seconds, and then choose the  refresh button above the list of objects.

**Congratulations!** You have successfully configured Cross-Region Replication for tagged objects within an S3 bucket.

**Task 6: Deleting replicated files**

To protect against malicious intent and accidental deletion, object deletions that occur in a source bucket are not replicated to the destination bucket by default.

In this task, you delete a file that has been replicated and then observe the results.

1. In the navigation breadcrumbs at the top of the page, choose the **Amazon S3** link to return to the **Buckets** page.
2. On the **Buckets** page, choose the link for the **source-bucket** bucket.
3. On the **source-bucket** details page, select the **crr-tag.txt** object, and then choose **Delete** .
4. On the **Delete objects** page:

* For **Delete objects?**, enter

delete

1. At the bottom of the page, choose **Delete objects** .
2. At the top right-hand corner of the page, choose **Close** .

**Note:** When you delete an object in a versioning-enabled S3 bucket, the object is not actually deleted. Instead, a delete marker is created as the latest version of the object. For more information, refer to *Working with delete markers* in the **Additional resources** section.

1. Verify the **crr-tag.txt** file has been deleted from the source bucket.
2. In the navigation breadcrumbs at the top of the page, choose the **Amazon S3** link to return to the **Buckets** page.
3. On the **Buckets** page, choose the link for the **destination-bucket** bucket.
4. You should notice that the *crr-tag.txt* file still exists in the destination bucket.

**Note:** If you have a business requirement to replicate deleted objects, you can modify your replication rule to enable **Delete marker replication**. For more information, refer to *Replicating delete markers between buckets* in the **Additional resources** section.

**Congratulations!** You have discovered that deleting an object from a source bucket does not delete it from the destination bucket.

**Conclusion**

**Congratulations!** You now have successfully:

* Configured S3 buckets for versioning.
* Created S3 Cross-Region Replication rules.
* Replicated objects with rules for full buckets, encrypted files, folders, and tags.
* Observed how the replication of deletions is handled.

**Additional resources**

* [Amazon S3 Cross-Region Replication](https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html)
* [How S3 Versioning works](https://docs.aws.amazon.com/AmazonS3/latest/userguide/versioning-workflows.html)
* [Replicating existing objects with S3 Batch Replication](https://docs.aws.amazon.com/AmazonS3/latest/userguide/s3-batch-replication-batch.html)
* [Setting up permissions](https://docs.aws.amazon.com/AmazonS3/latest/userguide/setting-repl-config-perm-overview.html)
* [Replicating objects created with server-side encryption (SSE-C, SSE-S3, SSE-KMS)](https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-config-for-kms-objects.html)
* [Tagging AWS resources](https://docs.aws.amazon.com/general/latest/gr/aws_tagging.html)
* [Working with delete markers](https://docs.aws.amazon.com/AmazonS3/latest/userguide/DeleteMarker.html)
* [Replicating delete markers between buckets](https://docs.aws.amazon.com/AmazonS3/latest/userguide/delete-marker-replication.html)

**End lab**

Follow these steps to close the console and end your lab.

1. Return to the **AWS Management Console**.
2. At the upper-right corner of the page, choose **AWSLabsUser**, and then choose **Sign out**.
3. Choose **End lab** and then confirm that you want to end your lab.

For more information about AWS Training and Certification, see [*https://aws.amazon.com/training/*](https://aws.amazon.com/training/).

*Your feedback is welcome and appreciated.*  
If you would like to share any feedback, suggestions, or corrections, please provide the details in our [*AWS Training and Certification Contact Form*](https://support.aws.amazon.com/#/contacts/aws-training).