aws training and certification

Lab 6: Configuring an Amazon CloudFront Distribution with an Amazon S3 Origin

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* .

Lab overview

Amazon Web Services (AWS) solutions architects must frequently design and build secure, high-performing, resilient, efficient architectures for applications and workloads to deliver content. Amazon CloudFront is a web service that provides a cost-effective way to distribute content with low latency and high data transfer speeds. You can use CloudFront to accelerate static website content delivery, serve video on demand or live streaming video, and even run serverless code at the edge location. In this lab, you configure a CloudFront distribution in front of an Amazon Simple Storage Service (Amazon S3) bucket and secure it using origin access identity (OAI) provided by CloudFront.

OBJECTIVES

After completing this lab, you should be able to do the following:

- Create an S3 bucket with default security settings.
- Configure an S3 bucket for public access.
- Add an S3 bucket as a new origin to an existing CloudFront distribution.
- Secure an S3 bucket to permit access only through the CloudFront distribution.
- Configure OAI to lock down security to an S3 bucket.
- Configure Amazon S3 resource policies for public or OAI access.

PREREQUISITES

This lab requires the following:

- Access to a notebook computer with Wi-Fi and Microsoft Windows, macOS, or Linux (Ubuntu, SuSE, or Red Hat)
- An internet browser, such as Chrome, Firefox, or Microsoft Edge

TECHNICAL KNOWLEDGE PREREQUISITES

To successfully complete this lab, you should be familiar with the AWS Management Console and have a basic understanding of edge services in the AWS Cloud.

DURATION

This lab requires approximately *60* minutes to complete.

ICON KEY

Various icons are used throughout this lab to call attention to different types of instructions and notes. The following list explains the purpose for each icon:

- **Note:** A hint, tip, or important guidance.
- **Learn more:** Where to find more information.
- **Caution:** Information of special interest or importance (not important enough to cause problems with the equipment or data if you miss it, but it can result in the need to repeat certain steps).
- **WARNING:** An action that is irreversible and can potentially impact the failure of a command or process (including warnings about configurations that cannot be changed after they are made).
- **Hint:** A hint to a question or challenge.
- **File contents:** A code block that displays the contents of a script or file you need to run that has been pre-created for you.
- **Copy edit:** A time when copying a command, script, or other text to a text editor (to edit specific variables within it) might be easier than editing directly in the command line or terminal.

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.

2. 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

You must first log out before logging into a different AWS account.

To logout, click here

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

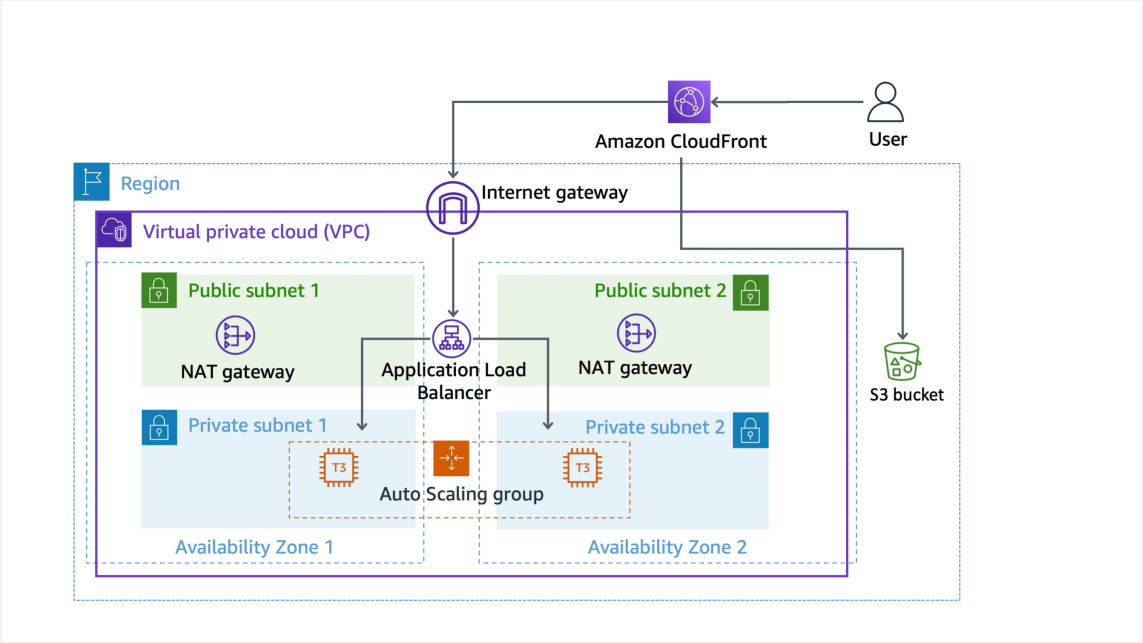
In some cases, certain pop-up or script blocker web browser extensions might prevent the **Start Lab** button from working as intended. If you experience an issue starting the lab:

- 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.

LAB ENVIRONMENT

The lab environment provides you with some resources to get started. There is an Auto Scaling group of EC2 instances being used as publicly accessible web servers. The web server infrastructure is deployed in an Amazon Virtual Private Cloud (Amazon VPC) and configured for multiple Availability Zones. It also uses load balancers. The lab also provides a CloudFront distribution with this load balancer as an origin.

The following diagram shows the general expected architecture you should have at the end of this lab. During this lab, you create a new S3 bucket for the existing lab environment. You then configure this bucket as a new, secure origin to the existing CloudFront distribution.



SERVICES USED IN THIS LAB

Amazon CloudFront

CloudFront is a content delivery web service. It integrates with other AWS products so that developers and businesses can distribute content to end users with low latency, high data transfer speeds, and no minimum usage commitments.

You can use CloudFront to deliver your entire website, including dynamic, static, streaming, and interactive content, using a global network of edge locations. CloudFront automatically routes requests for your content to the nearest edge location to deliver content with the best possible performance. CloudFront is optimized to work with other AWS services, like Amazon S3, Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB), and Amazon Route 53. CloudFront also works seamlessly with any origin server that doesn't use AWS, which stores the original, definitive versions of your files.

Amazon Simple Storage Service (Amazon S3)

Amazon S3 provides developers and information technology teams with secure, durable, highly scalable object storage. Amazon S3 has a simple web services interface to store and retrieve any amount of data from anywhere on the web.

You can use Amazon S3 alone or together with other AWS services such as Amazon EC2, Amazon Elastic Block Store (Amazon EBS), and Amazon Simple Storage Service Glacier (Amazon S3 Glacier), along with third-party storage repositories and gateways. Amazon S3 provides cost-effective object storage for a wide variety of use cases, including cloud applications, content distribution, backup and archiving, disaster recovery, and big data analytics.

AWS SERVICES NOT USED IN THIS LAB

AWS services not used in this lab are turned off in the lab environment. In addition, the capabilities of the services used in this lab are limited to only what the lab requires. Expect errors when accessing other services or performing actions beyond those provided in this lab guide.

Task 1: Exploring the existing CloudFront distribution

In this task, you examine the existing CloudFront distribution that was built for web server content. Before making changes to an environment, it is a good practice to understand the existing configuration. If you want to use CloudFront distributions for your personal AWS environments, you need to build and configure the distribution itself first. In later tasks, you add an S3 bucket as a new origin to this CloudFront distribution.

TASK 1.1: OPENING THE CLOUDFRONT CONSOLE

3. If you have not already opened the console, follow the instructions in the Start Lab section to log in to the console.
4. At the top of the console, in the search bar, search for and choose `CloudFront`.

TASK 1.2: OPENING THE EXISTING CLOUDFRONT DISTRIBUTION

5. Choose the ID link for the only available distribution.

Note: If you do not find the list of distributions, ensure that you are at the correct page. Choose **Distributions** from the CloudFront navigation menu located on the left side of the console.

A page showing the details of the distribution is displayed.

TASK 1.3: EXPLORING THE PROPERTIES OF THE EXISTING DISTRIBUTION

In this task, you explore each tab of the distribution to review the existing configuration. In this lab, you are not configuring this CloudFront distribution in great detail. However, it is useful to know where all of the configurations you might need for managing a CloudFront distribution are located.

6. Examine the contents of the **General** tab.

This tab contains the details about the current configuration of this particular CloudFront distribution. It contains the most generally needed information about a distribution. It is also where you configure the common high-level items for the distribution, such as activating the distribution, logging, and certificate settings.

7. **Copy edit:** In the **General** tab, copy the Distribution domain value for the distribution from the **Distribution domain name** field.

The Distribution domain value for this distribution is also found to the left of these lab instructions under the listing *LabCloudFrontDistributionDNS*.

8. Paste the Distribution domain value you copied into a new browser tab.

A simple web page is loaded displaying the information of the web server from which CloudFront retrieved the content. By requesting content from the Distribution domain value for CloudFront distribution, you are verifying that the existing cache is working.

You can close this tab.

9. Return to the **CloudFront** console.

10. Choose the **Origins** tab.

This tab contains the details about the current origins that exist for this particular CloudFront distribution. It is also the area of the console you can use to configure new or existing CloudFront origins. A *CloudFront Origin* defines the location of the definitive, original version of the content that is delivered through the CloudFront distribution.

Note: The only origin currently on the distribution is an ELB load balancer. This load balancer is accepting and directing web traffic for the auto scaling web servers in its target group.

11. **Copy edit:** Copy the load balancer's Domain Name System (DNS) value for this origin from the column labeled **Origin domain** .

Note : You can adjust the widths of most columns in the console by dragging the dividers in the header.

12. Paste the DNS value for the load balancer into a new browser tab.

The DNS value for this distribution is also found to the left of these lab instructions under the listing *LabLoadBalancerDNS*.

The simple web page hosted on the EC2 instances is displayed again. This web page displays the same content that was delivered by the CloudFront distribution earlier. However, by requesting from the load balancer directly you are not using the existing CloudFront caching system. In any single request, the IP address displayed on the page might differ because traffic is not always routed to the same EC2 instance behind the load balancer.

This step demonstrates that the origins defined for a distribution are the locations used to retrieve novel content when a request is made to the CloudFront distribution's frontend.

You can close this tab.

13. Return to the **CloudFront** console.

14. Choose the **Behaviors** tab.

Behaviors define the actions that the CloudFront distribution takes when there is a request for content, such as which origin to serve which content, Time To Live of content in the cache, cookies, and how to handle various headers.

This tab contains a list of current behaviors defined for the distribution. You configure new or existing behaviors here. Behaviors for the distribution are evaluated in the explicit order in which you define them on this tab.

Do the following to review or edit the configuration of any single behavior:

- Select the radio button in the row next to the behavior you want to modify.
- Choose Edit .
- Choose **Cancel** to close the page and return to the console.

There is only one behavior currently configured in this lab environment. The behavior accepts HTTP and HTTPS for both GET and HEAD requests to the load balancer origin.

15. Choose the **Error Pages** tab.

This tab details which error page is to be returned to the user when the content requested results in an HTTP 4xx or 5xx status code. You can configure custom error pages for specific error codes here.

16. Choose the **Geographic restrictions** tab.

This tab contains the distribution's configuration if you need to prevent users in specific countries from accessing your content. This feature is not configured for use in this lab.

17. Choose the **Invalidations** tab.

This tab contains the distribution's configuration for object invalidation. *Invalidated* objects are removed from CloudFront edge caches. A faster and less expensive method is to use versioned objects or directory names. There are no invalidations configured for CloudFront distributions by default.

18. Choose the **Tags** tab.

This tab contains the configuration for any tags applied to the distribution. You can view and edit existing tags and create new tags here. Tags help you identify and organize your distributions.

Congratulations! You have explored the existing CloudFront distribution.

Task 2: Creating an S3 bucket

In this task, you create and configure a new S3 bucket. This bucket is used as a new origin for the CloudFront distribution.

19. At the top of the console, in the search bar, search for and choose S3 .

20. In the **Buckets** section, choose **Create bucket** .

Note: If you do not find the Create bucket button, ensure you are at the correct page. Choose **Buckets** from the navigation menu located on the left side of the console.

The **Create bucket** page is displayed.

21. Copy the **LabBucketName** from left of the lab instructiions and paste into the **Bucket name** field.

Note: To simplify the written instructions in this lab, this newly created bucket is referred to as the *LabBucket* for the remainder of the instructions.

The AWS Region should match the *PrimaryRegion* value found to the left of these lab instructions.

22. Leave all other settings on this page as the default configurations.

23. Choose **Create bucket** .

The Amazon S3 console is displayed. The newly created bucket is displayed among the list of all the buckets for the account.

Congratulations! You have created a new S3 bucket with the default configuration.

Task 3: Configuring the S3 LabBucket for public access

In this task, you review the default access setting for S3 buckets. Next, you modify the permissions settings to allow public access to the bucket.

TASK 3.1: CONFIGURING THE LABBUCKET TO ALLOW PUBLIC POLICIES TO BE CREATED

24. Select the link for the newly created *LabBucket* found in the **Buckets** section.

A page with all of the bucket details is displayed.

25. Choose the **Permissions** tab.

26. Locate the **Block public access (bucket settings)** section.

27. Choose **Edit** .

The **Edit Block public access (bucket settings)** page is displayed.

28. Unselect **Block *all* public access** .

29. Choose **Save Changes** .

A message window titled Edit Block public access (bucket settings) is displayed.

30. In the message field, enter `confirm` .

31. Choose **Confirm** .

You have removed the block on all public access policies for the LabBucket. You are now able to create access policies for the bucket that allow for public access. The bucket is currently not public, but anyone with the appropriate permissions can grant public access to objects stored within the bucket.

TASK 3.2: CONFIGURING A PUBLIC READ POLICY FOR THE LABBUCKET

You now create a public object read policy for this bucket.

32. On the **Permissions** tab, locate the **Bucket policy** section.

33. Choose **Edit** .

The **Edit bucket policy** page is displayed.

34. **Copy edit:** Copy and paste the **Bucket ARN** value into a text editor to save the information for later. It is a string value like *arn:aws:s3:::LabBucket* located above the *Policy* box.

The ARN value uniquely identifies this S3 bucket. You need this specific ARN value when creating bucket based policies.

35. **File contents:** Copy and paste the following JSON into a text editor.

```
{
    "Version": "2012-10-17",
    "Id": "Policy1621958846486",
    "Statement": [
        {
            "Sid": "OriginalPublicReadPolicy",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "RESOURCE_ARN"
        }
    ]
}
```

36. Replace the **RESOURCE_ARN** value in the JSON with the **Bucket ARN** value you copied in a previous step and append a `/*` to the end of the pasted **Bucket ARN** value.

By appending the `/*` wildcard to the end of the ARN, the policy definition applies to all objects located in the bucket.

Here is the example of the updated policy JSON:

```
{
    "Version": "2012-10-17",
    "Id": "Policy1621958846486",
    "Statement": [
        {
            "Sid": "OriginalPublicReadPolicy",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::LabBucket/*"
        }
    ]
}
```

37. Return to the **Amazon S3 console** .

38. Paste the completed JSON into the *Policy* box.

39. Choose **Save changes** .

Caution: If you receive an error message at the bottom of the screen, it's probably caused by a syntax error with JSON. The policy will not save until the JSON is valid. You can expand the error message in the Amazon S3 console for more information about correcting the policy.

By using the `*` wildcard as the Principal value, *all* identities requesting the actions defined in the policy document are allowed to do so. By appending the `/*` wildcard to the allowed Resources, this policy applies to all objects located in the bucket.

40. Notice there is a red warning for **Publicly accessible** under the bucket name. There is also a **Public** warning in the *Permissions overview* section.

These warnings notify you that the policies currently applied to the bucket make the objects in this bucket publicly readable.

In later lab steps, you configure the bucket to be accessible only from the CloudFront distribution.

Congratulations! You have configured an S3 bucket for public read access.

Task 4: Uploading an object into the bucket and testing public access

In this task, you upload a single object to the LabBucket. You use this object to test access in the remaining lab tasks.

TASK 4.1: CREATING A NEW FOLDER IN THE BUCKET

41. Choose the **Objects** tab.

42. Choose **Create folder** .

43. Enter `CachedObjects` into the **Folder name** field.

44. Leave all other settings on the page at the default values.

45. Choose **Create folder** .

TASK 4.2: UPLOADING AN OBJECT TO THE BUCKET

46. Download the object for these lab instructions by choosing logo.png and saving it to your local device.

47. Return to the **Amazon S3** Console.

48. Choose the link for the CachedObjects/ folder that you created previously.

49. Choose **Upload** .

The **Upload** page is displayed.

50. Choose **Add files** .

51. Choose the **logo.png** object from your local storage location.

52. Choose **Upload** .

The **Upload: status** page is displayed.

A **Upload succeeded** message is displayed on top of the screen.

TASK 4.3: TESTING PUBLIC ACCESS TO AN OBJECT

53. Choose the logo.png link from the **Files and folders** section.

A page with details about the Amazon S3 object is displayed.

54. Select the link located in the **Object URL** field.

The picture is displayed in a browser tab.

55. Inspect the URL for the object and notice it is an Amazon S3 URL.

56. Close this page with the object.

Congratulations! You have created a folder in an S3 bucket, uploaded an object, and tested that the object can be retrieved from the S3 URL.

Task 5: Adding the bucket as an additional origin to the distribution

In this task, you add the LabBucket as a new origin to the existing CloudFront distribution.

TASK 5.1: CREATING A NEW ORIGIN AND OAI

57. At the top of the console, in the search bar, search for and choose `CloudFront` .

58. From the **CloudFront Distributions** page, choose the ID link for the only available distribution.

A page showing the details of the distribution is displayed.

59. Choose the **Origins** tab.

60. Choose **Create origin** .

The **Create Origin** page is displayed.

61. From the **Origin domain** field, choose the name of your LabBucket from the **Amazon S3** section.

Note: Recall that the S3 bucket in this lab is never configured as a website. You have only changed the bucket policy regarding who is allowed to perform GetObject API requests against the S3 bucket into an *Allow Public* read policy.

62. Leave the entry for **Origin path** empty.

Note: The Origin Path field is optional and configures which directory in the origin CloudFront should forward requests to. In this lab, rather than configuring the origin path, you leave it blank and instead configure a behavior to return only objects matching a specific pattern in the requests.

63. For **Name** , enter `My Amazon S3 Origin`

64. For **Origin access** , select **Legacy access identities** .

65. Select **Create new OAI** .

A **Create new OAI** message box is displayed.

66. Enter a name you can remember for later steps. For these lab instructions, this value is `S3OAI`

67. Select **Create** .

Note : Choosing this option creates a new OAI and requires that users always access your Amazon S3 content using CloudFront URLs. You assign a special CloudFront user—an OAI—to your origin. Any existing OAI can also be used for origins rather than creating new ones.

OAI is a virtual identity that you use to require users to access your content through CloudFront URLs instead of Amazon S3 URLs. It is usually used with CloudFront private content.

68. For **Bucket policy** , ensure **No, I will update the bucket policy** is selected.

Note : You update the S3 bucket in later tasks so that the OAI is the only allowed principal to read objects from the bucket. By selecting *yes*, CloudFront would append an update to the S3 bucket policy that allows the OAI specified during this origin creation with read permissions. This is in addition to the public read permissions already present.

69. Choose **Create origin** .

The **Distribution details** page is displayed.

TASK 5.2: CREATING A NEW BEHAVIOR FOR THE AMAZON S3 ORIGIN

In this task, you create a new behavior for the Amazon S3 origin so that the distribution has instructions for how to handle incoming requests for the origin.

70. Choose the **Behaviors** tab.

71. Choose **Create behavior** .

The **Create behavior** page is displayed.

72. In the **Path pattern** field, enter `CachedObjects/*.png`

This field configures which matching patterns of object requests the origin can return. Specifically, in this behavior only .png objects stored in the *CachedObjects* folder of the Amazon S3 origin can be returned. Unless there is a behavior configured for them, all other requests to the Amazon S3 origin would result in an error being returned to the requester. Typically, users would not be requesting objects directly from the CloudFront distribution URL in this manner; instead, your frontend application would generate the correct object URL to return to the user.

73. From the **Origin and origin groups** dropdown menu, choose **My Amazon S3 Origin** .

74. From the **Cache key and origin requests** section, ensure **Cache policy and origin request policy (recommended)** is selected.

75. From the **Cache policy** dropdown menu, ensure **CachingOptimized** is selected.

76. Leave all other settings on the page at the default values.

77. Choose **Create behavior** .

A Successfully created new cache behavior CachedObjects/*.png. message is displayed on top of the screen.

TASK 5.3: OBTAINING THE OAI CANONICAL ID

78. Choose the **General** tab.

79. From the CloudFront navigation menu, under the **Security** section, choose **Origin access** . You might need to expand the navigation menu by first choosing the ☰ menu icon.

The **Origin access** page is displayed.

80. Select the **Identities (legacy)** tab.

81. Choose the value under the **Amazon S3 canonical user ID** column. (Double-click the value to highlight it.)

82. **Copy edit:** Copy the value to a notepad. The value is needed for AWS Identity and Access Management (IAM) policies in later tasks.

Congratulations! You have created a new origin, OAI, and distribution behavior on a CloudFront distribution.

Task 6: Securing the bucket with CloudFront OAI

You added LabBucket as an origin to the CloudFront distribution, created a new OAI, and set a distribution behavior to handle specific requests to the CachedObjects folder. It is now time to edit the LabBucket access policy so that the access to the bucket is allowed *only* from the CloudFront OAI.

TASK 6.1: EDITING THE ALLOWED PRINCIPAL IN THE BUCKET POLICY

Setting the bucket policy with the OAI as the only principal allows bucket access through CloudFront without allowing public access to the GetObject API call.

83. At the top of the console, in the search bar, search for and choose `S3` .

84. Choose the link to the **LabBucket** from the list of available buckets.

85. Choose the **Permissions** tab.

86. Locate the **Bucket policy** section.

87. Choose **Edit** .

The **Edit bucket policy** page is displayed.

88. Locate the **Principal** value in the JSON document, at approximately line 8.

89. Replace the *Principal* value with the following JSON statement:

```
"Principal": {"CanonicalUser": "Amazon_S3_Canonical_User_ID_Placeholder"},
```

90. Replace *Amazon_S3_Canonical_User_ID_Placeholder* with the **Amazon S3 canonical user ID** value you copied from the CloudFront console in a previous step, keeping the quotation marks.

The only principal in the policy now allowed to call the *GetObject* and *GetObjectVersion* actions on your LabBucket should be the CloudFront OAI.

91. Choose **Save changes** .

Warning : If you receive an error message at the bottom of the screen, it is probably caused by a syntax error with JSON. Try again to copy and paste the policy from the policy generator. The policy will not save until the JSON is valid. For more information about correcting the policy, you can expand the error message in the Amazon S3 console.

By using the **Amazon S3 canonical user ID** value, the current ARN value of the OAI will be substituted in for the Principal.

The following is an example of a finished JSON policy:

```
{
    "Version": "2012-10-17",
    "Id": "Policy1621958846486",
    "Statement": [
        {
            "Sid": "UpdatedPublicReadPolicy",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity E1OOWD1GW"
```

```
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::LabBucket/*"
        }
    ]
}
```

A ✓ Successfully edited bucket policy. message is displayed on top of the screen.

Note: The previous warnings regarding public access are now gone.

TASK 6.2: ENABLING THE PUBLIC ACCESS BLOCKERS

92. On the **Permissions** tab, locate the **Block public access (bucket settings)** section.

93. Choose Edit .

The **Edit Block public access (bucket settings)** page is displayed.

94. Select ☑ **Block *all* public access** .

95. Choose **Save changes** .

A message window titled Edit Block public access (bucket settings) is displayed.

96. In the field of the message window, enter confirm .

97. Choose **Confirm** .

A ✓ Successfully edited Block Public Access settings for this bucket. message is displayed on top of the screen.

A page with all the bucket details is displayed.

Congratulations! You have edited the S3 bucket policy so that the only principal allowed to read objects is the OAI, which was created earlier.

Task 7: Testing direct access to a file in the bucket using the Amazon S3 URL

In this task, you test if the object can still be directly accessed using the Amazon S3 URL.

98. Choose the **Objects** tab.

99. Choose the link for the CachedObjects/ folder.

100. Choose the link for the logo.png object.

101. Select the link located in the **Object URL** field.

An error message is displayed with Access denied messages. This is expected because the new bucket policy does not allow access to the object directly from Amazon S3 URLs. By denying access to S3 objects directly through Amazon S3, users can no longer bypass the controls provided by CloudFront cache, which can include logging, behaviors, signed URLs, or signed cookies.

Congratulations! You have confirmed the object is no longer directly accessible from the Amazon S3 URL.

Task 8: Testing access to the object in the bucket using the CloudFront distribution

In this task, you confirm that you can access objects in the Amazon S3 origin for the CloudFront distribution.

102. **Copy edit:** Copy the CloudFront distribution's domain DNS value from the left side of these lab instructions under the listing *LabCloudFrontDistributionDNS*.

103. Paste the DNS value into a new browser tab.

A simple web page is loaded displaying the information of the web server where CloudFront retrieved the content from.

104. Append /CachedObjects/logo.png to the end of the CloudFront distribution's domain DNS and press **Enter** .

The browser makes a request to the CloudFront distribution and the object is returned from the Amazon S3 origin.

Hint: If the CloudFront URL redirects you to the Amazon S3 URL, or if the object isn't immediately available, the CloudFront distribution might still be updating from your recent changes. Return to the CloudFront console. Select **Distributions** from the navigation menu. Confirm that the Status column is ✓ Enabled and the Last modified column has a timestamp. You need to wait for this before testing the new origin and behavior. After you have confirmed the status of the distribution, wait a few minutes and try this task again.

Congratulations! You have confirmed that the object is returned from a CloudFront request.

Optional Task 9: Replicating an S3 bucket across AWS Regions

This optional task is provided to you if you have extra lab time or want to learn something a little more advanced. This task is not necessary to complete. You can end the lab now if you choose by following the steps to end the lab ; otherwise, keep reading.

Cross-Region replication is a feature of Amazon S3 that allows for automatic copying of your data from one bucket to another bucket located in a different AWS Region. It is a useful feature for disaster recovery. After the cross-Region replication feature is enabled for a bucket, every *new* object that you currently have read permissions for, which is created in the source bucket, is replicated into the destination bucket you define. This means that objects replicated to the destination bucket have the same names. Objects encrypted using an Amazon S3 managed encryption key are encrypted in the same manner as their source bucket.

To perform *Cross-Region replication*, you must enable object versioning for both the source and destination buckets. To maintain good data orderliness with versioning enabled, you can deploy lifecycle policies to automatically archive objects to Amazon S3 Glacier or to delete the objects.

OPTIONAL TASK 9.1: ENABLING VERSIONING ON YOUR SOURCE BUCKET

105. Return to the browser tab open to the AWS Management Console.

106. At the top of the console, in the search bar, search for and choose S3 .

107. Select the link for the LabBucket found in the **Buckets** section.

A page with all the bucket details is displayed.

108. Select the **Properties** tab.

109. Locate the **Bucket Versioning** section.

110. Choose Edit .

The **Edit Bucket Versioning** page is displayed.

111. Select **Enable** for **Bucket Versioning** .

112. Choose **Save changes** .

OPTIONAL TASK 9.2: CREATING A DESTINATION BUCKET FOR CROSS-REGION REPLICATION

113. From the Amazon S3 navigation menu, choose **Buckets** .

114. Choose **Create bucket** .

The **Create bucket** page is displayed.

115. In the **Bucket name** field, enter a unique bucket name.

To the left of these instructions are values for the *primary* and *secondary* Regions supported by the lab environment. The lab is initially launched in the *primary* Region.

116. Select the **AWS Region** that matches the *SecondaryRegion* value found to the left of these lab instruction.

117. In the **Block Public Access settings for this bucket** section, unselect **Block all public access** .

118. In the warning message, select **I acknowledge that the current settings might result in this bucket and the objects within becoming public** .

You do not need to have public access enabled for your personal buckets to use the cross-Region replication feature. It is enabled in this lab so that you can quickly test if objects are retrievable from the Amazon S3 URL.

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

120. Choose **Create bucket** .

The **Amazon S3 console** is displayed.

The newly created bucket is displayed among the list of all the buckets for the account.

Note: To simplify the narrative in this lab, this newly created bucket is referred to as the *DestinationBucket* in the remainder of instructions.

OPTIONAL TASK 9.3: CONFIGURING A PUBLIC READ POLICY FOR THE NEW DESTINATION BUCKET

You now create a public object read policy for this bucket.

121. From the Amazon S3 navigation menu, choose **Buckets** .

122. Choose the link for the **DestinationBucket** from the list of buckets.

123. Choose the **Permissions** tab.

124. Locate the **Bucket policy** section.

125. Choose **Edit** .

The **Edit bucket policy** page is displayed.

126. **Copy edit:** Copy and paste the **Bucket ARN** value into a text editor to save the information for later. It is a string value like *arn:aws:s3:::LabBucket* located above the *Policy* box.

The ARN value uniquely identifies this S3 bucket. You need this specific ARN value when creating bucket-based policies.

127. **File contents:** Copy and paste the following JSON into a text editor:

```
{
    "Version": "2012-10-17",
    "Id": "Policy1621958846486",
    "Statement": [
        {
            "Sid": "OriginalPublicReadPolicy",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "RESOURCE_ARN"
        }
    ]
}
```

128. Replace the **RESOURCE_ARN** value in the JSON with the **Bucket ARN** value you copied in a previous step and append a /* to the end of the pasted **Bucket ARN** value.

Here is the example of the updated policy JSON:

```
{
    "Version": "2012-10-17",
    "Id": "Policy1621958846486",
    "Statement": [
        {
            "Sid": "OriginalPublicReadPolicy",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::DestinationBucket/*"
        }
    ]
}
```

129. Return to the **Amazon S3 console** .

130. Paste the completed JSON into the *Policy* box.

131. Choose **Save changes** .

The **bucket details** page is displayed.

132. Notice there is a red warning for **Publicly accessible** under the bucket name. There is also a **Public** warning in the Permissions overview section.

These warnings notify you that the policies currently applied to the bucket make the objects in this bucket publicly readable.

OPTIONAL TASK 9.4: CREATING A REPLICATION RULE

133. From the Amazon S3 navigation menu, choose **Buckets** .

134. In the **Buckets** section, choose the link for the **LabBucket** .

135. Choose the **Management** tab.

136. Locate the **Replication rules** section.

137. Choose Create replication rule .

The **Create replication rule** page is displayed.

138. In the **Replication rule name** field, enter `MyCrossRegionReplication`

139. Verify that **LabBucket** is set for **Source bucket name** . If it is not, then you chose the incorrect bucket before choosing the replication rules.

140. In the **Choose a rule scope** section, select **Apply to all objects in the bucket** .

141. Locate the **Destination** section.

142. Choose Browse S3 .

143. Select the **DestinationBucket** .

144. Select **Choose path** .

145. Locate the **IAM Role** section.

146. Select **Choose from existing IAM roles** .

147. From the **IAM role** dropdown menu, select **Create new role** .

148. Leave all other options as their default selection.

149. Choose **Save** .

150. If the Replicate existing objects window is displayed, select **No, do not replicate existing objects** then choose **Submit** .

The **Replication rules** page for the LabBucket is displayed.

A **Replication configuration successfully updated** If changes to the configuration aren't displayed, choose the refresh button. Changes apply only to new objects. To replicate existing objects with this configuration, choose **Create replication job** . message is displayed on top of the screen.

All newly created objects in the LabBucket are replicated into the DestinationBucket.

Note: It is possible to replicate existing objects between buckets, but that is beyond the scope of this lab. You can find more information about this topic in the document linked in the Appendix section.

OPTIONAL TASK 9.5: VERIFYING OBJECT REPLICATION

151. From the Amazon S3 navigation menu, choose **Buckets** . You might need to expand the menu by choosing the ☰ menu icon.

152. In the **Buckets** section, choose the link for the **LabBucket** .

153. Download the object for these lab instructions by right-clicking logo2.png and saving it to your local device.

154. Return to the **Amazon S3** console.

155. Choose the link for the CachedObjects/ folder.

Note: If you do not find the CachedObjects folder, choose **Buckets** from the navigation menu located on the left side of the console. Then choose the link for the **LabBucket** from the list. Finally, choose the **Objects** tab to ensure that you are at the correct page.

156. Choose **Upload** .

The **Upload** page is displayed.

157. Choose Add files .

158. Choose the **logo2.png** object from your local storage location.

159. Choose **Upload** .

The **Upload: status** page is displayed.

A **Upload succeeded** message is displayed on top of the screen.

160. Choose the link for the logo2.png from the **Files and folders** section.

A page with details about the Amazon S3 object is displayed.

161. In the **Object management overview** section, examine *Replication status* and refresh the page periodically until it changes from *PENDING* to *COMPLETED*.

162. From the Amazon S3 navigation menu, select **Buckets** .

163. In the **Buckets** section, choose the link for the **DestinationBucket** .

A page with all the bucket details is displayed.

164. Choose the link for the CachedObjects/ folder.

165. In the **Files and folders** section, choose the link for the logo2.png .

A page with details about the Amazon S3 object is displayed.

166. In the **Object management overview** section, examine *Replication Status*. It displays **REPLICA** .

167. Choose the link located in the **Object URL** field.

The picture is displayed in a browser tab.

Congratulations! You have completed setting up cross-Region replication for all new objects uploaded into the LabBucket.

Consider these follow-up questions to this optional task:

- How can you restrict access to objects in the DestinationBucket?
- What steps are needed to add the DestinationBucket to the CloudFront distribution?

Conclusion

Congratulations! You now have successfully done the following:

- Created an S3 bucket with default security settings.
- Configured an S3 bucket for public access.
- Added an S3 bucket as a new origin to an existing CloudFront distribution.
- Secured an S3 bucket to allow access only through the CloudFront distribution.
- Configured OAI to lock down security to an S3 bucket.
- Configured Amazon S3 resource policies for public or OAI access.

End lab

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

168. Return to the **AWS Management Console** .

169. At the upper-right corner of the page, choose **AWSLabsUser** , and then choose **Sign out** .

170. Choose End lab and then confirm that you want to end your lab.

Additional resources

- For more information about S3 bucket naming rules, see Bucket naming rules.
- For more information about serving private content through CloudFront, see Serving private content with signed URLs and signed cookies.
- For more information about restricting S3 buckets to OAI, see Giving an origin access identity permission to read files in the Amazon S3 bucket.
- For more information about replicating existing objects between buckets, see Replicating existing objects between S3 buckets in the AWS Storage Blog.

For more information about AWS Training and Certification, see *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* .