

## Lesson 08 Demo 08

### Creating a Kinesis Data Firehose

**Objective:** To create a Kinesis Data Firehose, set up an Amazon S3 bucket as the destination, and test the data delivery stream

**Tools required:** AWS Workspaces

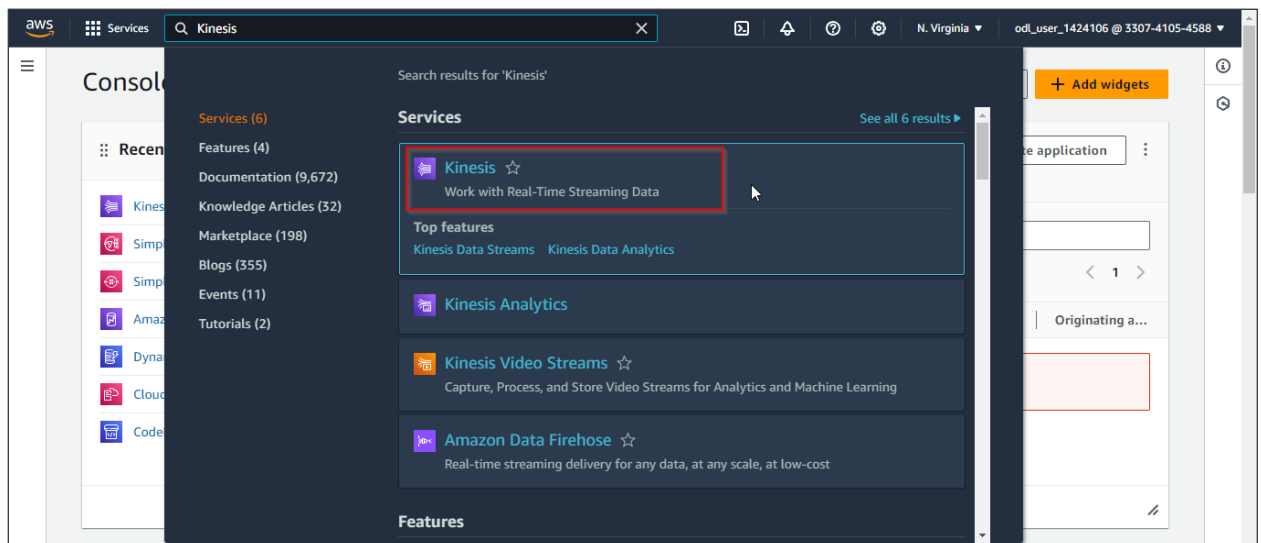
**Prerequisites:** Amazon account

Steps to be followed:

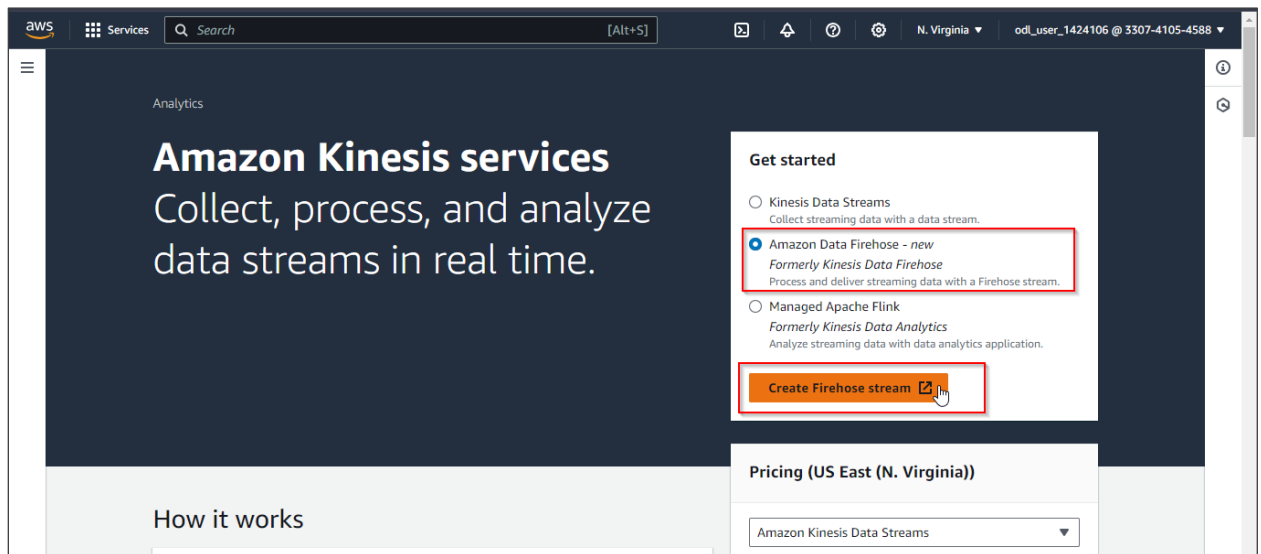
1. Create a Kinesis Data Firehose
2. Create an S3 bucket

#### Step 1: Create a Kinesis Data Firehose

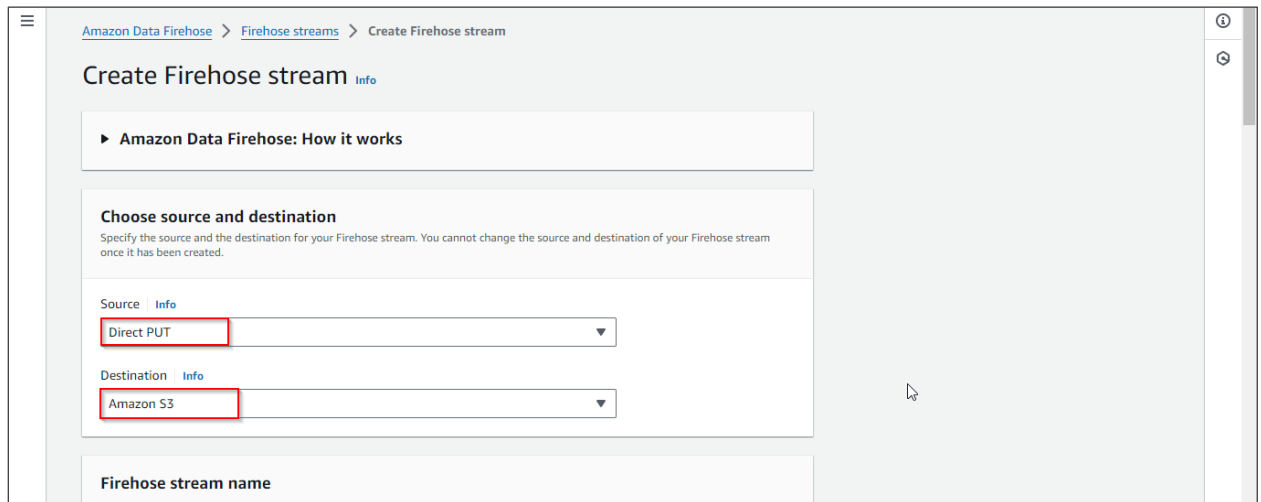
1.1 Navigate to the Amazon portal and search for and select **Kinesis**



## 1.2 Select the **Amazon Data Firehose** option and click **Create Firehose Stream**



## 1.3 Choose **Direct PUT** as the source and **Amazon S3** as the destination



## 1.4 Click on the **Create** button to set up an S3 bucket

**Destination settings** [Info](#)  
Specify the destination settings for your Firehose stream.

**S3 bucket**  
Choose a bucket or enter a bucket URI  
Format: s3://bucket  
Browse Create

**New line delimiter**  
You can configure your Firehose stream to add a new line delimiter between records in objects that are delivered to Amazon S3.  
☒ Not enabled  
☐ Enabled

**Dynamic partitioning** [Info](#)  
Dynamic partitioning enables you to create targeted data sets by partitioning streaming S3 data based on partitioning keys. You can partition your source data with inline parsing and/or the specified AWS Lambda function. You can enable dynamic partitioning only when you create a new Firehose stream. You cannot enable dynamic partitioning for an existing Firehose stream. Enabling dynamic partitioning incurs additional costs per GiB of partitioned data. For more information, see [Amazon Data Firehose pricing](#).  
☒ Not enabled  
☐ Enabled

**S3 bucket prefix - optional**  
By default, Amazon Data Firehose appends the prefix "YYYY/MM/dd/HH" (in UTC) to the data it delivers to Amazon S3. You can override this default by specifying a custom prefix that includes expressions that are evaluated at runtime.  
Enter a prefix

## Step 2: Create an S3 bucket

### 2.1 Name the bucket **mybucket2325**

**General configuration**

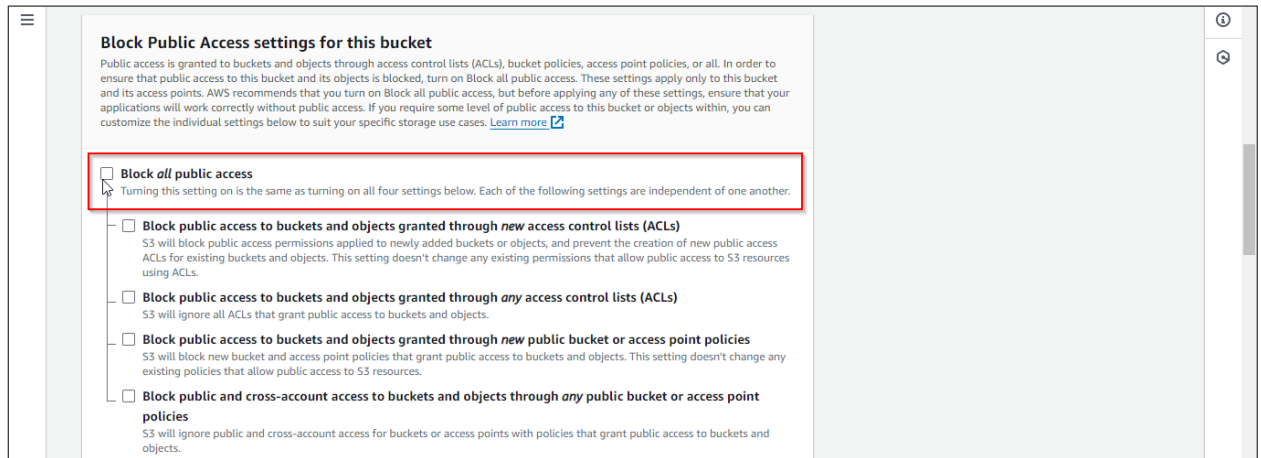
**AWS Region**  
US East (N. Virginia) us-east-1

**Bucket type** [Info](#)  
☒ General purpose  
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.  
☐ Directory - New  
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

**Bucket name** [Info](#)  
mybucket2325  
Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

**Copy settings from existing bucket - optional**  
Only the bucket settings in the following configuration are copied.  
Choose bucket  
Format: s3://bucket/prefix

## 2.2 Scroll down and enable the **Unblock all public access** dialog box



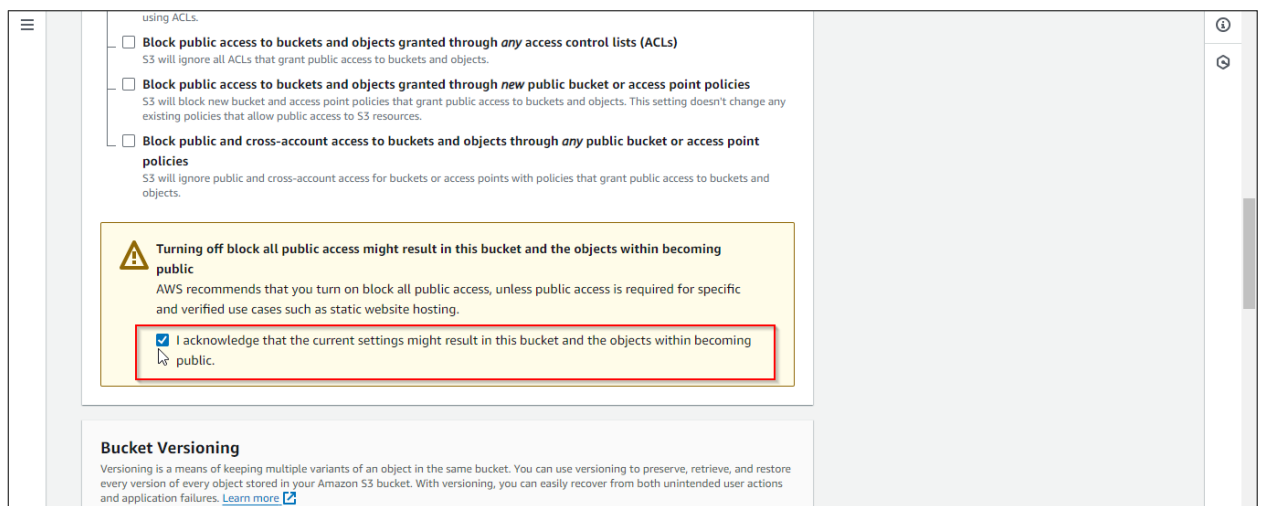
**Block Public Access settings for this bucket**

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☐ **Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
- ☐ **Block public access to buckets and objects granted through new public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

## 2.3 Check the **acknowledgment** box to confirm



☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.

☐ **Block public access to buckets and objects granted through new public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

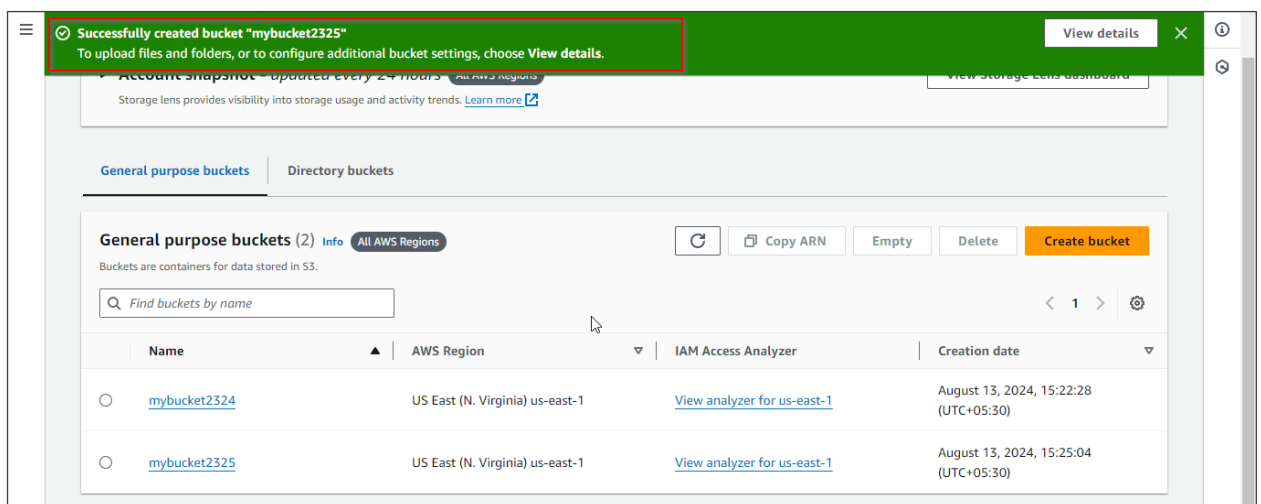
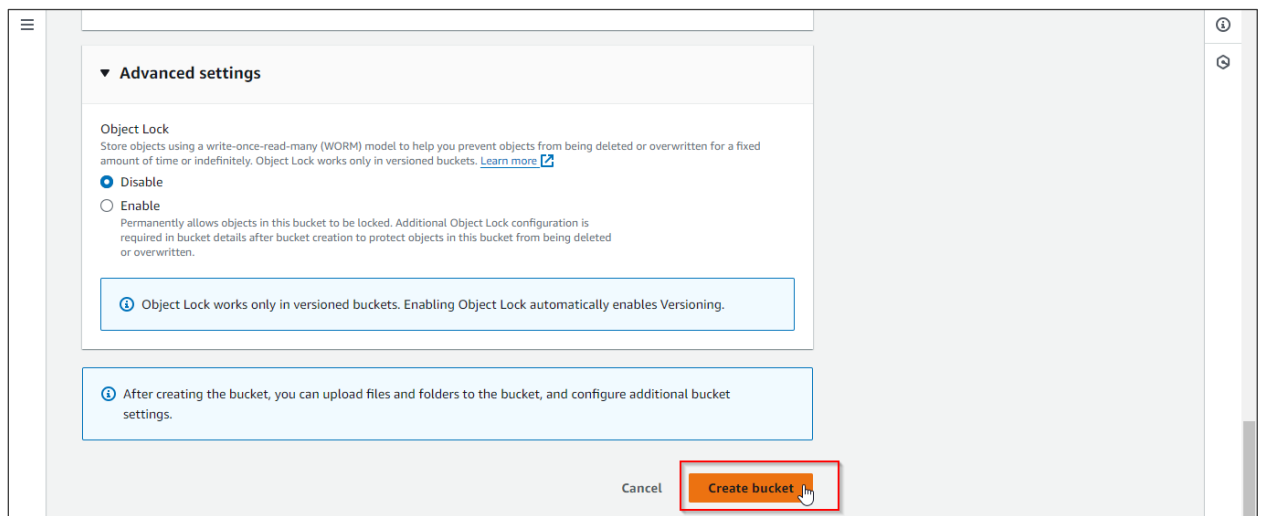
☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

**Turning off block all public access might result in this bucket and the objects within becoming public**  
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

**Bucket Versioning**  
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

## 2.4 Once the bucket creation is complete, click **Create bucket**



The bucket has been successfully created.

2.5 Now, navigate back to the **Kinesis** dashboard and click on the **Browse** button

**S3 bucket**

Choose a bucket or enter a bucket URI

Format: s3://bucket

**Browse** **Create**

**New line delimiter**

You can configure your Firehose stream to add a new line delimiter between records in objects that are delivered to Amazon S3.

☒ Not enabled

☐ Enabled

**Dynamic partitioning** [Info](#)

Dynamic partitioning enables you to create targeted data sets by partitioning streaming S3 data based on partitioning keys. You can partition your source data with inline parsing and/or the specified AWS Lambda function. You can enable dynamic partitioning only when you create a new Firehose stream. You cannot enable dynamic partitioning for an existing Firehose stream. Enabling dynamic partitioning incurs additional costs per GiB of partitioned data. For more information, see [Amazon Data Firehose pricing](#).

☒ Not enabled

☐ Enabled

**S3 bucket prefix - optional**

By default, Amazon Data Firehose appends the prefix "YYYY/MM/dd/HH" (in UTC) to the data it delivers to Amazon S3. You can override this default by specifying a custom prefix that includes expressions that are evaluated at runtime.

Enter a prefix

You can repeat the same keys in your S3 bucket prefix. Maximum S3 bucket prefix characters: 1024.

2.6 Select the bucket name and click on **Choose**

**Choose a bucket in Amazon S3**

**Buckets (1/2)**

Find buckets

Name	Region
<input type="radio"/> mybucket2324	US East (N. Virginia)
<input checked="" type="radio"/> mybucket2325	US East (N. Virginia)

Cancel **Choose**

**Destination settings** [Info](#)

Specify the destination settings for your Firehose stream.

**S3 bucket**

[Browse](#) [Create](#)

Format: s3://bucket

**New line delimiter**

You can configure your Firehose stream to add a new line delimiter between records in objects that are delivered to Amazon S3.

☒ Not enabled  
☐ Enabled

**Dynamic partitioning** [Info](#)

Dynamic partitioning enables you to create targeted data sets by partitioning streaming S3 data based on partitioning keys. You can partition your source data with inline parsing and/or the specified AWS Lambda function. You can enable dynamic partitioning only when you create a new Firehose stream. You cannot enable dynamic partitioning for an existing Firehose stream. Enabling dynamic partitioning incurs additional costs per GiB of partitioned data. For more information, see [Amazon Data Firehose pricing](#).

☒ Not enabled  
☐ Enabled

**S3 bucket prefix - optional**

By default, Amazon Data Firehose appends the prefix "YYYY/MM/dd/HH" (in UTC) to the data it delivers to Amazon S3. You can override this default by specifying a custom prefix that includes expressions that are evaluated at runtime.

The S3 bucket has now been successfully added.

## 2.7 Click on the **Create Firehose stream** button

**S3 bucket error output prefix - optional**

You can specify an S3 bucket error output prefix to be used in error conditions. This prefix can include expressions for Amazon Data Firehose to evaluate at runtime.

**S3 bucket and S3 error output prefix time zone** [Info](#)

Choose a time zone that you want to use for date and time in S3 prefixes

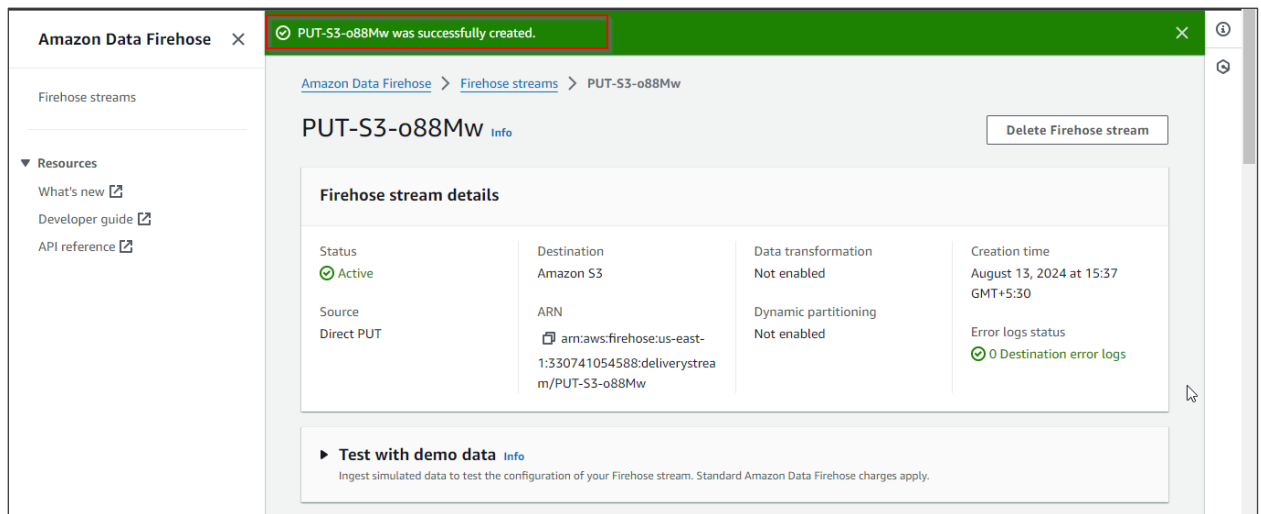
**► Buffer hints, compression, file extension and encryption**

The fields below are pre-populated with the recommended default values for S3. Pricing may vary depending on storage and request costs.

**► Advanced settings**

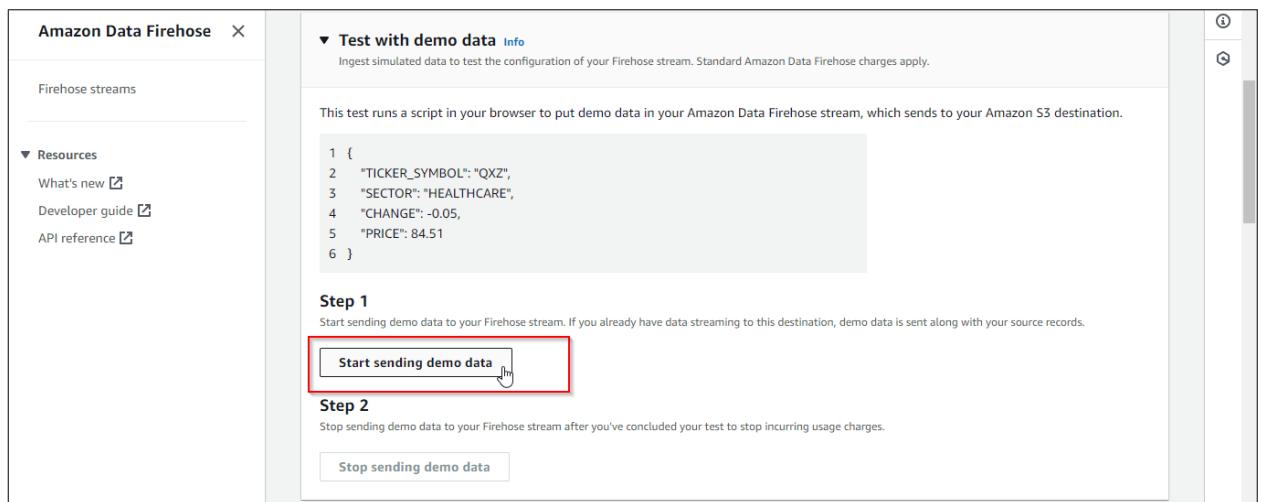
Server-side encryption not enabled; error logging enabled; IAM role KinesisFirehoseServiceRole-PUT-S3-o88Mw-us-east-1-1723543475925; no tags.

[Cancel](#) [Create Firehose stream](#)

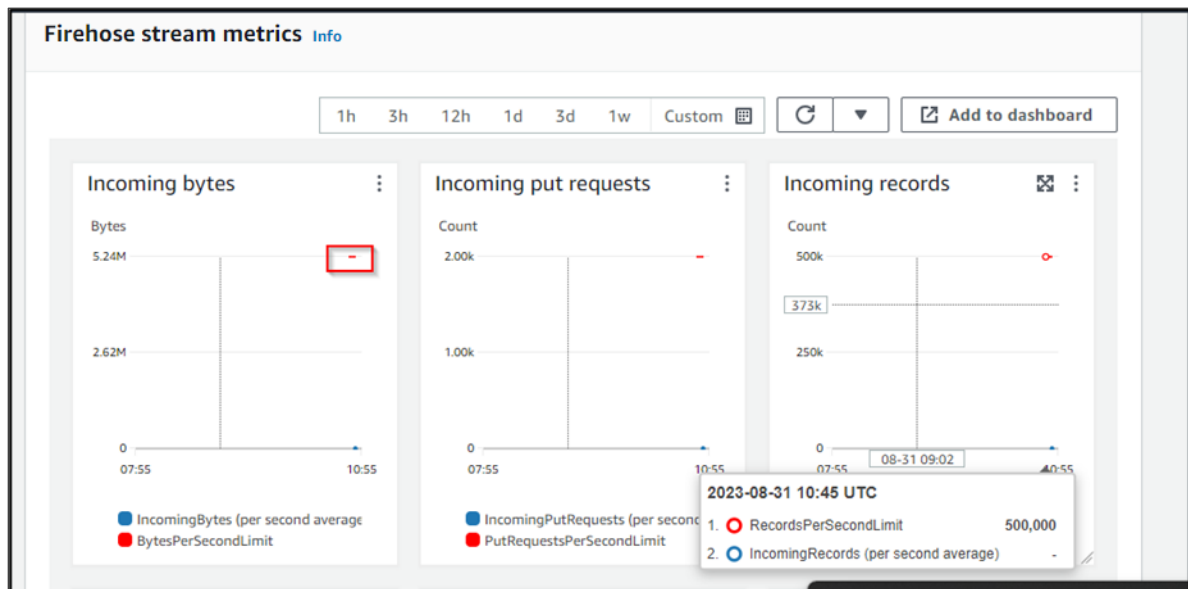


The Amazon Data Firehose has been successfully created.

## 2.8 Under **Test with demo data**, click **Start sending demo data**







The **Firehose stream metrics** information will appear here.

By following these steps, you have successfully created a Kinesis Data Firehose, set up an Amazon S3 bucket as the destination, and tested the data delivery stream.