

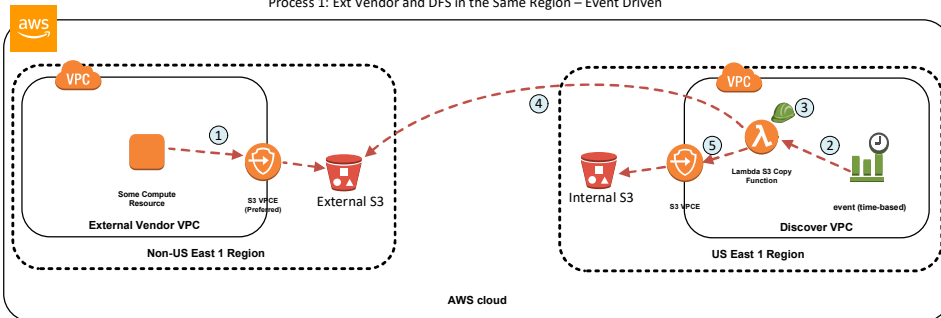
Process 1: Ext Vendor and DFS in the Same Region – Event Driven

Process

- 1 – External Vendor loads data into External S3 Bucket. DFS Prefers the S3 Data be loaded through a VPC Endpoint.
- 2 – S3 Bucket Event is triggered and send a notification to DFS SNS Topic.
- 3 – A Lambda Function assumes a role and Gets the objects from External Vendor S3 bucket.
- 4 – A Lambda Function copies the data into the Internal S3 bucket via VPC Endpoint. The data is encrypted at rest.

Set Up

- 1 – Create both Internal and External Buckets
- 2 – Create bucket policies on both buckets that restrict access to VPCE. The External Bucket would permit both VPCEs and the Internal only the DFS VPCE.
- 3 – Create an IAM Role with Two IAM policies. One policy to permit access to put objects into Internal S3 and another to get objects from external S3.
- 4 – Update the External Bucket policy to permit the IAM Role in step 3.
- 5 – Create a SNS Topic that permits publishing via the External S3 bucket within the DFS account.
- 6 – Create an event on the External S3 bucket to watch for any create object operation (can be more specific) and send notifications to the SNS ARN.



Process 2: Ext Vendor and DFS in Different Regions – Time Driven

Process

- 1 – External Vendor loads data into External S3 Bucket. DFS Prefers the S3 Data be loaded through a VPC Endpoint.
- 2 – A CloudWatch alarm, set for midnight CST (anytime time/interval works), will trigger a Lambda Function.
- 3 – A Lambda Function assumes a role to get the objects from External Vendor S3 bucket.
- 4 – A Lambda Function lists the bucket to determine if new files have been loaded.
- 5 – A Lambda Function copies the data into the Internal S3 bucket via VPC Endpoint. The data is encrypted at rest.

Set Up

- 1 – Create both Internal and External Buckets
- 2 – Create bucket policies on both buckets that restrict access to VPCE. The External Bucket would permit both VPCEs and the Internal only the DFS VPCE.
- 3 – Create an IAM Role with Two IAM policies. One policy to permit access to put objects into Internal S3 and another to get objects from external S3.
- 4 – Update the External Bucket policy to permit the IAM Role in step 3.
- 5 – Create a CloudWatch Alarm to alarm at a particular time or interval.