Cloudpond S3 Connector Solution Architecture and Usage

Version 4.1

May 2023

By Starpond Inc.

Introduction

Welcome to the Cloudpond S3 Connector! Cloudpond S3 Connector is the fastest, easiest to install, most geographically focused and most user-friendly S3 Connector for Salesforce. Starpond Software proudly presents the Cloudpond S3 Connector 4.1 for Salesforce. Cloudpond will allow your organization's Force.com platform to connect quickly and easily to Amazon S3 as a Native Salesforce Application! What does this mean to you? As a Business Owner or Business Manager, it allows you to keep your costs down and your productivity up. No middle servers are involved and store your important files in your own country, region, or jurisdiction. Again, we are glad you are here, and please let us know if there is any way we can assist you. You may call support at any point during this setup process for immediate assistance or questions with Phone Support, US EST (703) 486-6258.

Architecture

Cloudpond S3 Connector allows your Salesforce Org to connect to your own designated AWS S3 Bucket in your region of choice. Simply install the connector, then proceed to the Cloudpond App settings page and provide your AWS key which will be stored in your Salesforce Encrypted Custom Settings. Choose your AWS region, your S3 Bucket, and the 'root' folder in which you would like your S3 uploads contained. Once this is completed you can proceed to your page layouts and add the Cloudpond S3 Connector to any page layout.

Cloudpond S3 Connector utilizes the AWS REST Signature Version 4 (the latest version) API to list, and upload S3 attachments directly from your Salesforce org to your own AWS S3 Org, there are no middle servers involved. Cloudpond S3 Connector is a native software solution for storing files in S3 which are affiliated with your Salesforce Records.

AWS Authenticating Requests using AWS Signature Version 4 on Cloudpond S3 Connector

The Amazon S3 REST API uses a custom HTTP scheme based on a keyed-HMAC (Hash Message Authentication Code) for authentication. To authenticate a request, Cloudpond S3 Connector first concatenates selected elements of the request to form a string. It then uses your AWS secret access key (kept in encrypted custom settings) to calculate the HMAC of that string. Informally, we call this process "signing the request," and we call the output of the HMAC algorithm the signature. Finally, we add this signature as a parameter of the request by using the syntax described in this section.

When the AWS S3 system receives an authenticated request, it fetches the AWS secret access key that you claim to have and uses it, in the same way, to compute a signature for the message it received. It then compares the signature it calculated against the signature presented by the requester. If the two signatures match, the AWS S3 system concludes that the requester must have access to the AWS secret access key and therefore acts with the authority of the principal to whom the key was issued. If the two signatures do not match, the request is dropped and the system responds with an error message.

The Signature element is the RFC 2104 HMAC-SHA1 of selected elements from the request, and so the Signature part of the Authorization header will vary from request to request. If the request signature calculated by the system matches the Signature included with the request, the requester will have demonstrated possession of the AWS secret access key. The request will then be processed under the identity, and with the authority, of the developer to whom the key was issued.

Time Stamp Requirement

A valid time stamp (using either the HTTP Date header or an x-amz-date alternative) is mandatory for authenticated requests. Furthermore, the client timestamp included with an authenticated request must be within 15 minutes of the Amazon S3 system time when the request is received. If not, the request will fail with the RequestTimeTooSkewed error code. The intention of these restrictions is to limit the possibility that intercepted requests could be replayed by an adversary.

Examples of REST Command that are used by Cloudpond S3 Connector to access your AWS S3 Buckets

1) **Object GET (from your AWS S3 Bucket)**

This example gets an object from the awsexamplebucket1 bucket.

GET /photos/puppy.jpg HTTP/1.1

Host: awsexamplebucket1.us-west-1.s3.amazonaws.com

Date: Tue, 27 Mar 2022 19:36:42 +0000

Authorization: AWS AKIAIOSFODNN7EXAMPLE:

qgk2+6Sv9/oM7G3qLEjTH1a1l1g=

2) **Object PUT (into your AWS S3 Bucket)**

This example puts an object into the awsexamplebucket1 bucket.

PUT /photos/puppy.jpg HTTP/1.1

Content-Type: image/jpeg

Content-Length: 94328

Host: awsexamplebucket1.s3.us-west-1.amazonaws.com

Date: Tue, 27 Mar 2022 21:15:45 +0000

Authorization: AWS AKIAIOSFODNN7EXAMPLE:

iqRzw+ileNPu1fhspnRs8nOjjIA=

3) List (items in your AWS S3 Bucket)

This example lists the content of the awsexamplebucket1 bucket.

GET /?prefix=photos&max-keys=50&marker=puppy HTTP/1.1

User-Agent: Mozilla/5.0

Host: awsexamplebucket1.s3.us-west-1.amazonaws.com

Date: Tue, 27 Mar 2022 19:42:41 +0000

Authorization: AWS AKIAIOSFODNN7EXAMPLE:

m0WP8eCtspQl5Ahe6L1SozdX9YA=

4) Delete (items from your AWS S3 Bucket)

This example deletes an object from the 'awsexamplebucket1' bucket using the path-style and Date alternative.

DELETE /awsexamplebucket1/photos/puppy.jpg HTTP/1.1

User-Agent: dotnet

Host: s3.us-west-1.amazonaws.com

Date: Tue, 27 Mar 2022 21:20:27 +0000

x-amz-date: Tue, 27 Mar 2022 21:20:26 +0000

Authorization: AWS AKIAIOSFODNN7EXAMPLE:XbyTlbQdu9Xw5o8P4iMwPktxQd8=

5) Upload (items to your AWS S3 Bucket)

This example uploads an object to a CNAME style virtual hosted bucket with metadata.

PUT /db-backup.dat.gz HTTP/1.1

User-Agent: curl/7.15.5

Host: static.example.com:8080

Date: Tue, 27 Mar 2022 21:06:08 +0000

x-amz-acl: public-read

content-type: application/x-download

Content-MD5: 4gJE4saaMU4BqNR0kLY+lw==

X-Amz-Meta-ReviewedBy: joe@example.com

X-Amz-Meta-ReviewedBy: jane@example.com

X-Amz-Meta-FileChecksum: 0x02661779

X-Amz-Meta-ChecksumAlgorithm: crc32

Content-Disposition: attachment; filename=database.dat

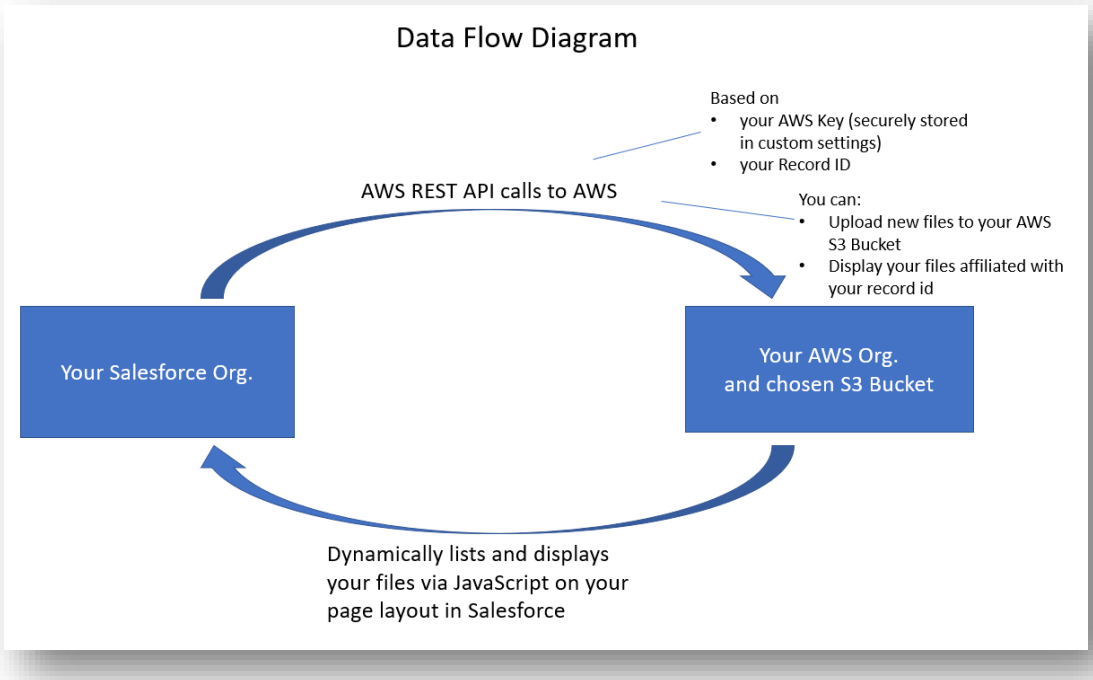
Content-Encoding: gzip

Content-Length: 5913339

Authorization: AWS AKIAIOSFODNN7EXAMPLE:

dKZcB+bz2EPXgSdXZp9ozGeOM4I=

Data Flow Diagram for Cloudpond S3 Connector



For any solution architectural questions, please contact sales@cloudpond.com or call 1-703-486-6258 during business hours (US EST).