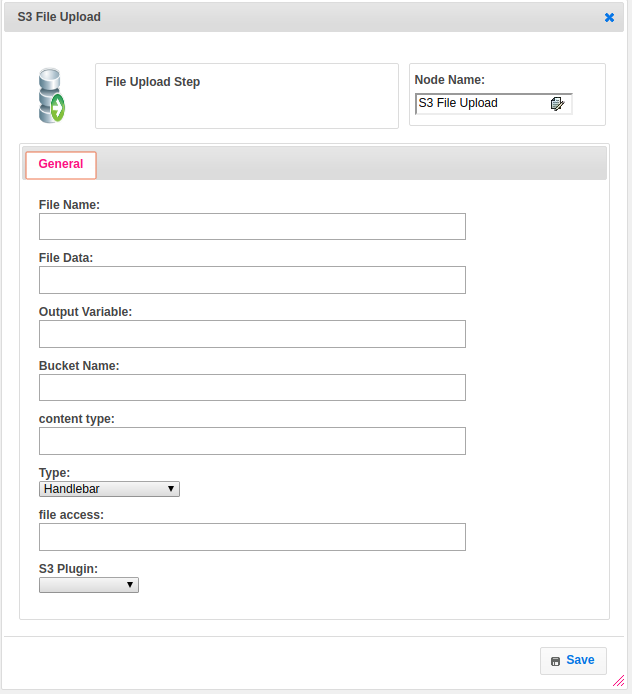
S3 File Upload Step

Objective:

It is used to Upload the files into given S3 location and return a URL for the uploaded file. the AWS Management Console to upload one or more files or entire folders to an Amazon S3 bucket. Before you can upload files and folders to an Amazon S3 bucket, you need write permissions for the bucket.

## UI

****

## Attributes:

|  |  |
| --- | --- |
| **Attributes** | **Description** |
| File Name | The name of the file which we need to create or use in given bucket name to upload the data. If name is present in given path it will use that file to insert the data otherwise it will create new file with same name which given by user. |
| File Data | The file data will get from previous step and upload this data into given bucket name and file name and data as array of bytes |
| Output Variable | Used to store the response of the step |
| Bucket Name | S3 bucket name has to be provided with the path which mentions the location of the required file to upload the data into that file as array of bytes. |
| content type | The type of the content is application/octet-stream by default, we can select other content types also based on the requirement |
| Type | To select type as free marker template or handlebar |
| file access | Amazon S3 access control lists (ACLs) enable you to manage access to buckets and objects. Each bucket and object has an ACL attached to it as a subresource. It defines which AWS accounts or groups are granted access and the type of access. |
| S3 Plugin | The name of the plugin which we configured earlier with access\_key, secret\_key and region |

## Executor Description:

In Executor class first it will connect to s3 in aws account based on the plugin credentials. Set the content type, length and take the data as array of bytes and upload into a file based on file name and backet name which given by user and return a url for the uploaded file.

## Dependent Plugins:

|  |  |
| --- | --- |
| **Attributes** | **Description** |
| access\_key | AWS Access Keys are used to sign the requests you send to Amazon S3. Like the Username/Password pair you use to access your AWS Management Console, Access Key Id and Secret Access Key are used for programmatic (API)access to AWS services. You can manage your Access Keys in AWS Management Console. |
| secret\_key | When we create access keys, we create the access key ID and secret access key as a set. During access key creation, AWS gives you one opportunity to view and download the secret access key part of the access key. |
| region | To reduce data latency in your applications, mostAmazon Web Services offer a regional endpoint to make your requests. An endpoint is a URL that is the entry point for a web service. For example, https://dynamodb.us-west-2.amazonaws.com is an entry point for the Amazon DynamoDB service. |

## Resource:

For more information please refer the below link

<https://docs.aws.amazon.com/AmazonS3/latest/user-guide/upload-objects.html>