Cambria Cluster: Amazon AWS Credentials and S3/EC2 Setup

Objective

This document provides the instructions for setting up Cambria FTC to work with Amazon Web Services. Included are steps to setup credentials and S3/EC2 permissions to allow CloudExtend to create EC2 instances and use S3 to read/write files.

User/Credentials

The simplest way to set up credentials as suggested by the SDK is to use a local file with the credential information, this is what we use. This file doesn't use any encryption. But, since the plan is to move to pre-signed URLs eventually, we have not focused on more secure methods.

Credential Setup:

Creating a txt file with the security credentials:

1. Go to the following page: https://aws.amazon.com/
2. Sign in and then search and navigate to the IAM page.
3. Once in the IAM Management Console, Select **Users** from the left sidebar.
4. Click **Add User** to add a new user.
5. Enter a user name of your choice (Ex: capellaS3ReadWrite). After entering a user name click on the Next button to set permissions.
6. Set the permissions for this new user by clicking on **Attach existing policies directly**. If you want to enable S3, then search for **AmazonS3FullAccess** and enable that permission. If you want to enable EC2, then click **Clear filters** and search for **AmazonEC2FullAccess**. After adding the permissions that you need, then click on **Next**.
7. Add a tag if you want, but this step can be skipped. When finished with this step click **Create user**.
8. Once the user is created you will receive a success message. Now, find the user that you just created on the Users page and click on the name.
9. Click on **Security credentials** and click on **Create access key**
10. Click **Third-party service** and check the box below. Click **Next** and add a tag if you want or just click **Create access key**.
11. You will now see a page where there is an access key and a secret access key. Make sure to save the secret access key somewhere safe because you will not be able to see it again.
12. Create a credentials.txt file that has the security credentials information in this format (our example is as below, you will need to generate your own):

Cambria Cluster: Amazon AWS Credentials and S3/EC2 Setup

[default]
aws_access_key_id = FKIAI4FADFFAWFSAFA
aws_secret_access_key = +LAEKgsCdddfadsft0m/gMNe+6ggTsdfPHuija/uewu

Modify the .txt file and place the credentials file to the two locations specified below for every Cluster and FTC machine:

1) Remove the ".txt" extension of credentials.txt file.
2) Take the credential file and add it to the following locations:
    a) C:\Users\USERNAME\.aws (in Windows you can create a new folder named .aws)
        i) If this does not work do this:
            (1) Open Command Prompt in Windows.
            (2) Navigate to the path in which you want to create a folder name starting with dot(.)
            (3) Now type mkdir<space>.FolderName
    b) C:\Windows\system32\config\systemprofile\.aws\

NOTE: Once the Credential File is set up you should be able to use FTC to import/export files to your mapped locations.