AWS CLI

By

Reyaz

AWS CLI

- Using CLIs, you can automate the deployment and management of your AWS services using simple code and script, much like how you would use bash and shell scripting.
- Prerequisite:
  - The AWS CLI can be either installed on a Windows or a Linux machine.
- Windows, AWS provides an easy-to-use installer
  - The 64-bit AWS CLI installer for Windows can be downloaded from
  - https://s3.amazonaws.com/aws-cli/AWSCLI64.msi.

Setting up AWS CLI

- Python versions supported are Python 2 version 2.6.5 and above or Python 3 version 3.3 and above.
- Install the Python
  - **Yum install –y python**
- Verify the Python Installation
  - **python --version**

Installation of AWSCLI

- Download the Python setup tools:
- wget https://pypi.python.org/packages/source/s/setuptools/setuptools-7.0.tar.gz

- tar xvf setuptools-7.0.tar.gz
- cd setuptools-7.0
- python setup.py install

- wget https://bootstrap.pypa.io/get-pip.py
- python get-pip.py
- pip install awscli

- aws –version

Managing access and security using the AWS CLI

- Configuring the AWS CLI
  - **# aws configure**
- you will be prompted to enter the user's **Access Key ID and the Secret Access Key, along with the default region name and the default output format to use.**
- The default region name is a mandatory field and can be any of the regions from which your users will be operating, for example, us-east-1, us-west-2, and so on
- The output format accepts any of these three values as the preferred method to display the output of the commands: table, text, or json.
- Note: Any of these values can be changed at any time by rerunning the aws configure command.

Accessing CLI Commands

- AWS will store these credentials and configuration details in two separate files named ~/.aws/credentials and ~/.aws/config, respectively.
- let's try out the CLI by executing some commands. To start off, let's try listing the users present in our account.
  - **# aws iam list-users --profile admin**

Managing Users using AWSCLI

- Configuring the AWS CLI:
- >> aws configure
- >> aws configure --profile admin
- >> aws iam list-users --profile admin
- >> aws iam create-user --user-name YoYo --profile admin
- >> aws iam create-login-profile --user-name YoYo --password P@$$w0rD --profile admin (--password-reset-
- required)
- >> aws iam create-access-key --user-name YoYo --profile admin
- >> aws iam create-group --group-name SuperUsersGroup --profile admin
- >> aws iam add-user-to-group --user-name YoYo --group-name SuperUsersGroup --profile admin
-
-

Managing Users using AWSCLI

- # vi /tmp/MyPolicy.json
- Add the following contents to your policy file as shown:
- {
- "Version": "2012-10-17",
- "Statement": [
- {
- "Effect": "Allow",
- "Action": "*",
- "Resource": "*"
- }
-]
- }

- Next, run the following command to attach this policy document to your newly created group:
- # aws iam put-group-policy --group-name SuperUsersGroup --policy-name Admin-Access-All --policy-document file:///vagrant/myPolicy.json --profile admin

Now I Know AWS CLI !!!!!!