Configuring Access Credentials

In this lesson, you will learn how to set up access credentials for AWS CLI.

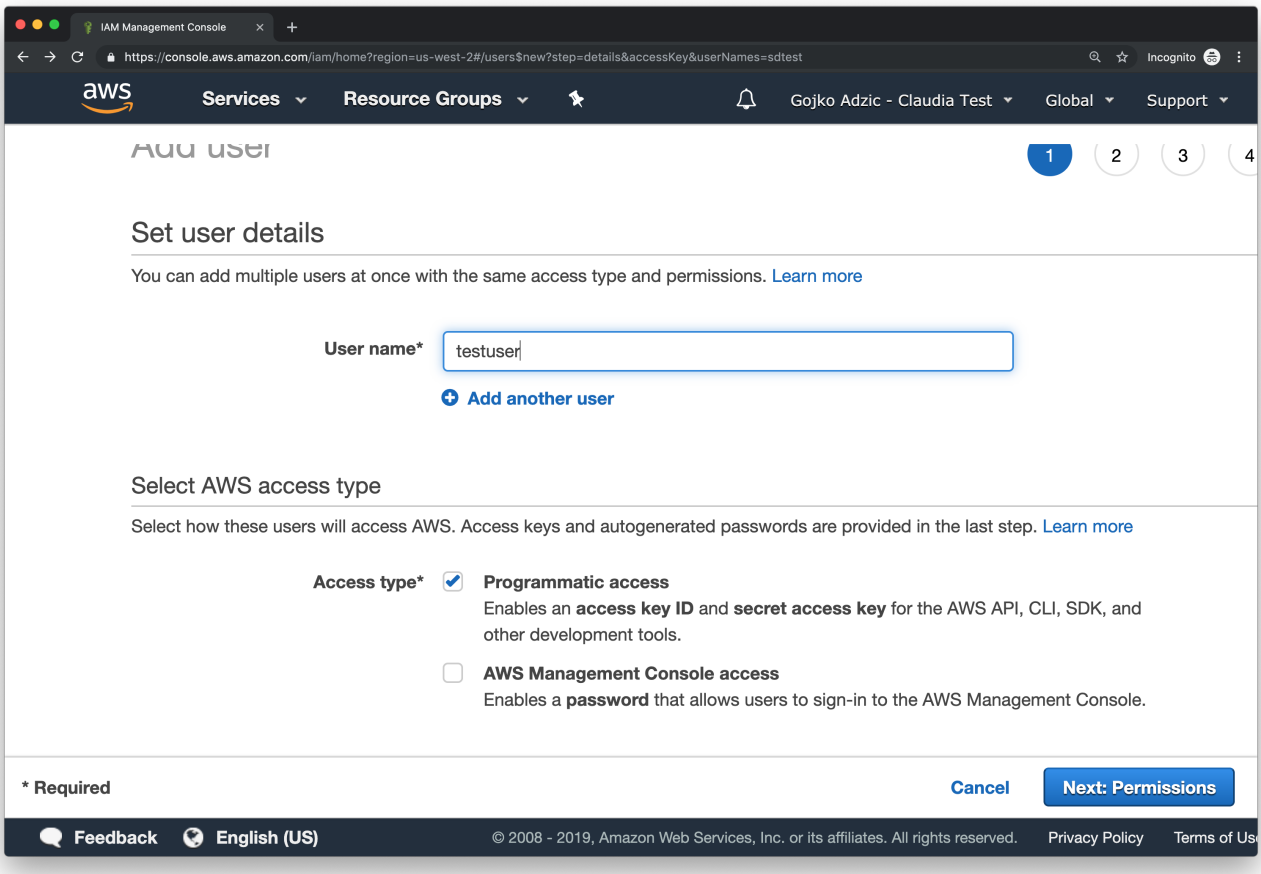
WE'LL COVER THE FOLLOWING

SAM configuration

AWS SAM CLI reuses the credential configurations from AWS command-line tools. If you already have credentials set up for AWS CLI, skip this section.

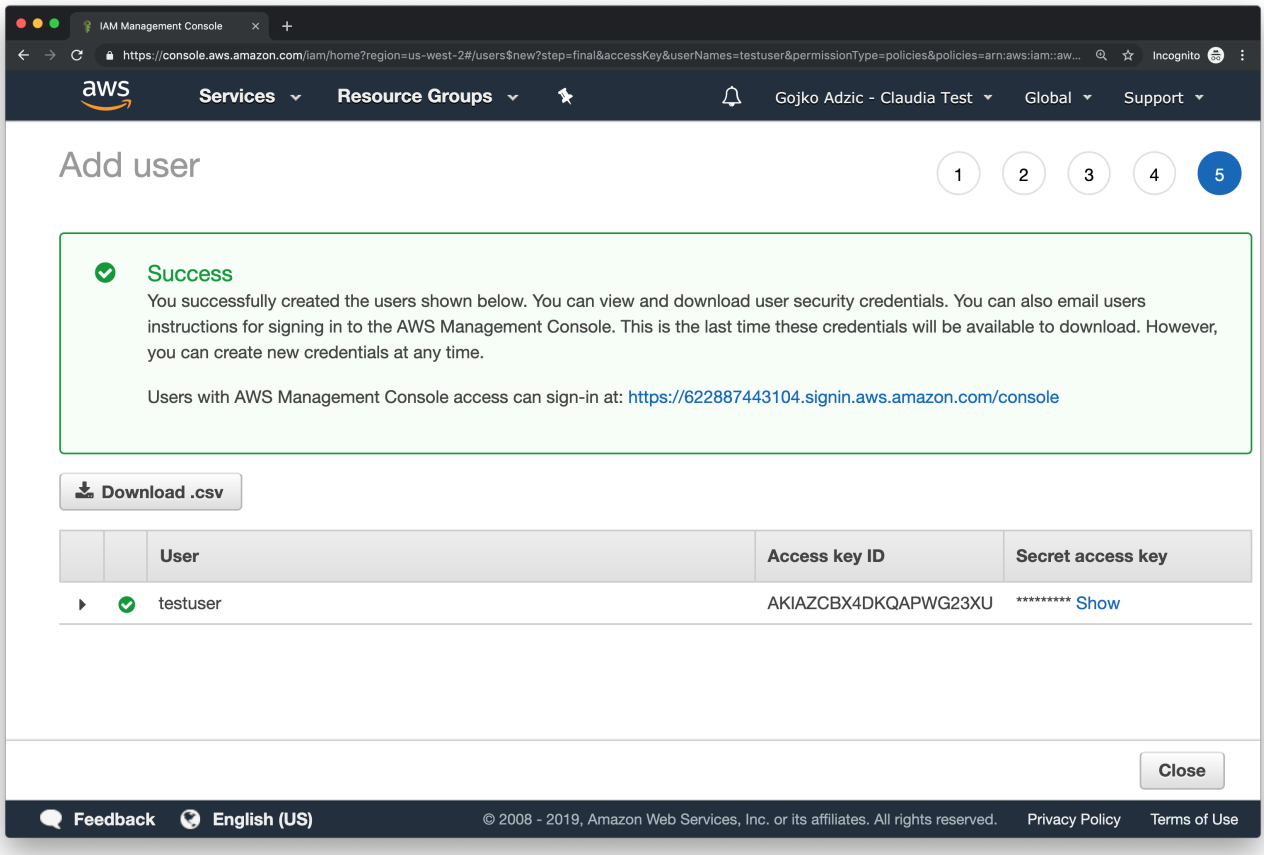
To deploy software to the AWS cloud, you will need an access key ID and a secret key ID associated with your user account. If you do not have these already, here is how you can generate a set of keys:

1. Sign in to the AWS Web Console at https://aws.amazon.com/.
2. Select the Identity and Access Management (IAM) service.
3. In the left-hand IAM menu, select *Users*.
4. Click on the *Add User* button.
5. On the next screen, enter a name for the user account then, in the 'Select AWS access type' section, select *Programmatic access*.



Create a user with programmatic access rights for SAM and AWS command line tools.

6. Click the *Next* button to assign permissions, then select *Attach existing policies directly*.
7. In the list of policies, find the `PowerUserAccess` and `IAMFullAccess` policies and tick the checkboxes next to them.
8. You can skip the remaining wizard steps. The final page will show the access key ID and show a link to reveal the secret key as shown in the figure below. Reveal the secret key and copy both keys somewhere.



In the final step, reveal and copy the access key and secret key.

Once you have the access keys, you may run the following command to save the keys to your local machine:

```
aws configure
```

When the AWS utility asks you about the keys, paste what you copied in the previous step. You will also likely be asked to enter a default region and a default output format.

For the default output format, enter `json`, or just press Enter to keep it unset.

For the region, use `us-east-1` or check whether your IT administrators have a preference. Because AWS adds new regions and services frequently, for a full list of available options, it is best to check out the *AWS regions and endpoints* documentation page.

> For the sake of this course, please enter your access key ID, secret access key and `us-east-1` in the fields `AWS_ACCESS_KEY_ID` and

`AWS_SECRET_ACCESS_KEY`, and `AWS_REGION` respectively.

> **AWS regions**
>
> AWS has data centers all over the world. The region setting tells the command line tools which data center to use. Region selection is useful to ensure that user data is hosted in a specific country for compliance reasons and to speed up data transfers by using the closest available access point. The original AWS data center in North Virginia is `us-east-1`. Generally, new services launch in that region first, so it is a safe setting for experiments.

Verification

Check that your credentials are correctly configured by running the following command line:

```
aws sts get-caller-identity
```

If this command prints a result similar to the following, everything works correctly in the terminal provided above:

```
$ aws sts get-caller-identity
{
    "UserId": "111111111111",
    "Account": "222222222222",
    "Arn": "arn:aws:iam:1111111111:root"
}
```

If you get an error, check out the section *Configuring the AWS CLI* from the AWS CLI user guide for troubleshooting information.

Now that you are done with the account configurations, you'll see how to run the AWS services with restricted user accounts.