How to launch an Amazon Web Service (AWS) server for the 2019 ISMRM educational session

Overview

This document shows how participants in the ISMRM educational session can launch an Amazon Web Service (AWS) server with the provided Amazon Machine Image (AMI) for each demo. Participants will be able to run the demos out-of-the-box without installing any software.

We will show how to launch an AWS server (called an EC2 instance), choose an ISMRM AMI, and login to the instance.

This document is based on the Deep Learning tutorial at the ISMRM Machine Learning Workshop 2018 by Peter Chang: https://github.com/peterchang77/dl_tutorial.

Table of Content

Overview 1
Table of Content 1

1) Register for an AWS account 2
2) Create an EC2 instance 3
2.1) Update the AWS EC2 region 4
2.2) Create a new EC2 instance 4
2.3) Choose the AMI for the ISMRM demo you want to try 5
2.4) Configure the instance 5
2.5) Create a key pair 6
3) Connect to the instance 7
3.1a) Connect to a Linux instance via SSH 7
3.1b) Connect to a Windows instance via Remote Desktop Connection 8
1) Register for an AWS account

To start, please sign up for an AWS account from: https://portal.aws.amazon.com/billing/signup#/start
2) Create an EC2 instance

After logging in you will arrive at a launch page of various AWS services. To navigate to the EC2 dashboard, click on the Services dropdown menu in the top left hand corner of the banner. You should now have a screen that looks like this:

Click on the EC2 link under the first Compute header within the first column. You have now arrived at the EC2 console (dashboard):
2.1) Update the AWS EC2 region

To ensure that you can access the ISMRM AMIs, make sure you are in region **US West (Oregon)**. You can choose the region of service by changing the context in the top right hand corner of the banner:

![AWS Region Selection](image1)

2.2) Create a new EC2 instance

To create an EC2 instance, log into the EC2 console (see instructions above) to begin creating a new EC2 instance. Click the **Instances** link on the left hand toolbar and subsequently click on the blue **Launch Instance** button.

![EC2 Instance Creation](image2)
2.3) Choose the AMI for the ISMRM demo you want to try

First, pick a software demo you want to try from https://www.ismrm.org/19/program_files/WE21.htm. Then click “Community AMIs” on the left panel, search for “ismrm” in the search bar, and select the appropriate AMI for that demo. Click the blue “Select” to proceed.

2.4) Configure the instance

For the second step, we need to choose the EC2 instance type. Unless you are asked to choose a more powerful machine, you should use the free tier instance **t2.micro**.
On the top set of links, click on **Review** to see a summary of the EC2 settings. Click on the bottom right hand **Launch** button.

### 2.5) Create a key pair

The final step is to create a key pair to remotely connect to your EC2 instance. To do so type in a key pair name (for example: default) and click **Download Key Pair**. It is important to remember the name and location of this downloaded key. If you lose this key you will be unable to access the EC2 instance. A recommended strategy to store AWS key pairs is to place it in a hidden folder easily accessible from your home folder (~/.aws). After downloading and saving the SSH key, click Launch Instance to complete the EC2 creation process.

Note that some OS’s may automatically append a *.txt to the end of your *.pem file when downloading. If so, please rename it. Also change the permissions on the SSH key to not be publicly viewable (otherwise SSH client will not accept the key):

```bash
chmod 400 ~/.aws/default.pem
```
3) Connect to the instance

There are separate instructions on connecting to Linux and Windows instances. If demos based on Linux, please go through 3.1a. For Windows, please go through 3.2b.

3.1a) Connect to a Linux instance via SSH

Instructions to ssh to the Linux instance can be found by selecting a particular EC2 instance (blue check box to the left of the instance name) and clicking the Connect button.

SSH to the instance the ssh key:

```
ssh -i "/path/to/your/pem/file" ubuntu@[ec2-public-dns]
```

Note the you should replace [ec2-public-dns] with your EC2 instances public DNS. In the above screenshot this would be ec2-35-160-231-250.us-west-2.compute.amazonaws.com. Assuming that your SSH key is located at ~/.aws/default.pem (if you followed the instructions per EC2 creation above) then the full command would be:

```
ssh -i "~/.aws/default.pem" ubuntu@c2-35-160-231-250.us-west-2.compute.amazonaws.com
```

You should now be successfully logged into your remote SSH session.

For demos with graphic interfaces, please add the -Y flag to enable X11:

```
ssh -i "/path/to/your/pem/file" -Y ubuntu@[ec2-public-dns]
```
For demos with Jupiter notebook, please add the `-L 127.0.0.1:8888:127.0.0.1:8888` flag to enable port tunneling (so that you can open the notebook in your local browser):

```
ssh -i "/path/to/your/pem/file" -L 127.0.0.1:8888:127.0.0.1:8888 ubuntu@[ec2-public-dns]
```

### 3.1b) Connect to a Windows instance via Remote Desktop Connection

To connect to a Windows EC2 instance, Windows and Mac users can use **Remote Desktop Connection**. This should be installed by default on Windows machines. For macOS, it can be downloaded from the App Store: [https://itunes.apple.com/us/app/microsoft-remote-desktop-10/id1295203466](https://itunes.apple.com/us/app/microsoft-remote-desktop-10/id1295203466) And for Ubuntu, you can use Remmina, which is included in the distribution.

Instructions to connect to the Windows instance can be found by selecting a particular EC2 instance (blue check box to the left of the instance name) and clicking the **Connect** button.
Click the **Download Remote Desktop file** to download a *.rdp file. Then click **Get Password** to get to the next page:

Click **Choose File** and select the *.pem Key pair you created in Step 2. Then click **Decrypt Password** and the password will be shown.

Open the *.rdp file you downloaded with the remote connection software, and then enter the password:

You should now be successfully logged into your remote Windows machine.