CIS 455/555: Internet and Web Systems

Spring 2014

Getting Started with Amazon Web Services

This document briefly summarizes how to get started in using Amazon's Elastic Compute Cloud. It is based on the Amazon "Getting Started" documentation but specialized to the needs of our class. This document assumes that you are using the VM image for the assignments; if you are not, you may need to install extra software on your computer, e.g., an `ssh` client and the Java 7 SDK.

1. Setup

1.1 Signing up for AWS

1. Go to http://aws.amazon.com/, click **Sign Up Now.** You'll be asked to enter some information, including payment info.
2. Log out, go to http://aws.amazon.com/awscredits/ and redeem your credit code.
3. Make a new subdirectory `.ec2` under your home directory.
4. Log in again (under http://aws.amazon.com/, 'Sign in to the AWS Management Console'), find the account menu in the upper right corner (with your name), and select **Security Credentials**.
5. Create a new **Key Pair**, and then save your **Access Key ID** and the **Secret Access Key** (click on **Show** to reveal it) to a text file somewhere, so you can cut and paste them to other files later.
6. Click on **Key Pair,** scroll down to the **Amazon EC2 Key Pairs** area, and click on **Access Your Amazon EC2 Key Pairs using the AWS Management Console**. Then click on **Key Pairs** in the sidebar on the left and **Create Key Pair**. Save the file as `~/.ec2/login.pem`.

1.2 Setting up the EC2 API tools

1. Edit the file `.bashrc` in the home directory, and add the following lines at the end:
```
export AWS_ACCESS_KEY=your-aws-access-key-id-goes-here
export AWS_SECRET_KEY=your-aws-secret-key-goes-here
```
2. Save the file and close any open terminal windows (your changes are only applied to newly opened terminals).
3. Open a new terminal window and run `ec2-describe-regions`. If everything went well, you should see a list of regions, including, e.g., `us-east-1`.
4. Run the command `chmod 400 ~/.ec2/login.pem` (if the permissions on your `ssh` key are too open, `ssh` will not accept the file)

1.3 Configuring the Default Security Group

Go to the **AWS Management Console (**https://console.aws.amazon.com/) and sign in.

1. Choose **EC2** from the big list (left column, second from the top, orange icon)
2. Choose **Security Groups** under **Networking & Security**.
3. Select the **default** security group.
4. The default permissions allow for unfirewalled access among Amazon EC2 nodes, but no access from outside.
5. We need to enable the HTTP protocol, which operates over TCP. Click on the **Inbound** tab, open the **Create a new rule** drop-down, and select **HTTP**. The **Source** should already be filled in as '0.0.0.0/0'. Click **Add rule**.
6. Repeat, but select SSH this time. Click **Add rule**.
7. If you use additional ports (for master/worker communication, etc.), you need to create additional rules for them.
8. Finally, click **Apply Rule Changes**.

2. Elastic Compute Cloud (EC2)

2.1 Launching an EC2 Instance

Go to the **AWS Management Console (**https://console.aws.amazon.com/) and sign in.

- Choose **EC2** from the big list (left column, second from the top, orange icon)
- Verify that the drop-down box on the upper right shows "**N. Virginia**", so you'll get an instance on the East coast.
- Click on the **Launch Instance** button. Now you need to choose a type of virtual machine. You'll probably want a one of the basic Linux machines, e.g., **Amazon Linux AMI 2014.03** or (if you prefer an environment like the one in the VM) **Ubuntu Server 13.10**. Go with the 64-bit version.
- Choose the number of machine instances you need, and the type of machine. You'll probably want one of the "General purpose" machines, e.g., **Small (m1.small)**. The 'micro' instances may be free, but their network performance is advertised as "very low". Click on "**Next: Configure Instance Details**".
- Enter the number of instances you want. You can leave the other options as they are, although you may want to enable termination protection (but first read up on it here!). The availability zone matters somewhat; if you use EBS volumes or are planning to start additonal instances later on, you should pick the same (specific) zone for all of them. Click "**Next: Add Storage**".
- Now you can choose how large a 'disk' your instance should have. The default 8GB should be a good starting point. Now click "**Next: Tag Instance**".
- Skip the tag page and click "**Next: Configure Security Group**".
- **Select an existing Security Group** and pick your **default** group. Click "**Review and Launch**".
- In the review screen, choose **Launch**.
- You will be asked to select an existing key pair. Choose the key pair you created initially, and check the box to acknowledge that you do have the private key file available. Click "**Launch Instances**". Recall that, from now on, you will be billed on an hourly basis, so don't forget to turn the instance(s) off later! Click **View Instances**.
- Wait for the instance list to indicate the instance(s) are ready (Status 'running', with a green dot next to it). If the status is 'pending', with a yellow dot next to it, you need to wait a bit.
- Click on the instance, look at the bottom of the pane (EC2 Instance: i-xxxxx), and scroll down until the **Public DNS** entry appears. This is your instance's public DNS name. Write it down.

2.2. Connecting to an EC2 Instance

You can connect to a Linux EC2 instance using `ssh` as follows:

1. Connect to your instance using the its public DNS name. For example, if instance's DNS name is `ec2-75-101-230-211.compute-1.amazonaws.com`, use the following command.

   ```
   ssh -i ~/.ec2/login.pem ec2-user@ec2-75-101-230-211.compute-1.amazonaws.com
   ```

   Note that you need to log in as `ec2-user`, and **not** as `cis555`, `root`, or your SEAS login!

   You should see a response like the following:

   ```
   The authenticity of host 'ec2-75-101-230-211.compute-1.amazonaws.com
   (75.101.230.211)' can't be established.
   RSA key fingerprint is fc:8d:0c:eb:0e:a6:4a:6a:61:50:00:c4:d2:51:78:66.
   Are you sure you want to continue connecting (yes/no)?
   ```

2. Enter `yes`. You'll see a response like the following:

   ```
   Warning: Permanently added ' ec2-75-101-230-211.compute-1.amazonaws.com' (RSA)
   to the list of known hosts.
   ```

You're now logged in and can work with the instance like you would any normal server. (For instance, you can now install Jetty and run servlets.) If you need root access, e.g., for mounting or unmounting volumes, you can use `sudo`. Just remember that you are being billed while the server is alive! Log out using `exit` or `logout`.

2.3 Terminating an EC2 Instance

Please note that you will be billed for AWS instances as they are alive, so you will want to terminate them when they aren't in direct use. Here are the Amazon instructions.

1. In the AWS Management Console (http://aws.amazon.com/console/), locate the instance in your list of instances on the **Instances** page.
2. Right-click the instance, and then click **Terminate**.
3. Click **Yes, Terminate** when prompted for confirmation.

Amazon EC2 begins terminating the instance. As soon as the instance status changes to shutting down or terminated, you stop incurring charges for that instance.

Similarly, you should delete EBS volumes (or any other resources) that you aren't using anymore. As shown in class, the EC2 Dashboard has an overview of the resources you're currently using.