CIS 455/555: Internet and Web Systems

Spring 2010

Setting up Amazon Web Services (AWS)

This document briefly summarizes how to get started in launching an Amazon Elastic Compute Cloud (EC2) virtual machine and connecting to it. It is based on the Amazon "Getting Started" documentation but specialized to the needs of our class.

Getting Started: Required Software for Your Local Machine

You will need the following:

- ssh client
  - Linux: ssh should be installed by default; if not you will have to run `yum install openssh` or the equivalent
  - Mac OS X: ssh is installed by default
  - Windows:
    - Install cygwin (www.cygwin.com) and select **OpenSSH** in the **Networking** tab in the setup.
    - You may also want to install the PuTTY ssh terminal software, http://www.chiark.greenend.org.uk/~sgtatham/putty/, along with PuTTYGen
- Sun (*not* OpenJDK!) Java 6, http://java.sun.com/javase/6/
- Eclipse: Please install Eclipse 3.5

Getting Started: Creating AWS Account

1. Go to `aws.amazon.com`, click **Sign Up Now**
2. Find the link for **Amazon Elastic Compute Cloud** and click on it, then click on the button **Sign Up For Amazon EC2**
3. Find the menu **Your Account** and select **Security Credentials**
4. Click on the **X.509 Certificates** tab and create a new certificate; download it. Create an **Access Key**. Download the resulting private key file.
5. Create a new **Key Pair** and download this private key file. (Be sure you can distinguish between the name of this file and the private Access Key above.)
6. Make an `.ec2` subdirectory under your home directory, and copy all downloaded certificates there.
7. Look up your **AWS Account ID** under the same **Your Account** | **Security Credentials** area. This number, with dashes removed, is your account ID.

Getting Started: Client-Side Setup for AWS

Set up your ssh client to use the private key:

- **If you are using PuTTY**, you will need to run the accompanying PuTTYGen, then choose **Conversions** | **Import Key**, and select your private key's `.pem` file. Optionally choose a password to add, then save as a PuTTY `.ppk` file.
- **If you are using the regular ssh client**, you can copy the `.pem` file to `~/.ssh/id_rsa`, then later use `ssh {xyz}` where *{xyz}* is the Amazon virtual machine hostname you want to log into. Or you can use "`ssh -i` *{pem file pathname}*" to directly use the `.pem` file as a private key.

Next, download the Amazon AWS command-line tools from http://s3.amazonaws.com/ec2-downloads/ec2-api-tools.zip.

1. Unzip it to a particular path in your filesystem.
2. Set the EC2_HOME environment variable to point to the tools:
    a. Linux – bash: Add the following to `~/.profile`:
    `export EC2_HOME=`*{path}*
    b. Linux – csh: Add the following to `~/.cshrc`:
    `setenv EC2_HOME` *{path}*
    c. Windows XP: go into **Control Panel** | **System**, click on the **Advanced** tab and choose **Environment Variables**, then create a **User variable** `EC2_HOME` with the appropriate path.
    d. Windows Vista/7: go into **Control Panel** | **System and Maintenance** | **System** | **Advanced System Settings** and choose **Environment Variables**, then create a **User variable** `EC2_HOME` with the appropriate path.
3. Repeat the above procedure to set the variable `PATH` to point to the `bin` subdirectory of the tools you just installed.
4. If necessary, repeat the above to set JAVA_HOME to point to the base directory of your JDK, and the `PATH` to include the `bin` directory within the Java install.
5. Set the variable `EC2_CERT` to point to the path of the EC2 X.509 Certificate file.
6. Set the variable `EC2_PRIVATE_KEY` to point to the path of the EC2 Access Key private key certificate (not the keypair one used for ssh).

Getting Started: Configuring a Default Security Group

Go to **Resources** | **AWS Management Console** (under **Development Tools**) and sign in.

- Choose **Security Groups** under **Networking and Security**
- Select the **default** security group
- The default permissions allow for unfirewalled access among Amazon EC2 nodes, but no access from outside.
- Add a line with **Connection Method** `HTTP`, **Port** `80`, **Source** of `0.0.0.0/0` (note that this leaves the virtual machines unfirewalled, which is OK for test purposes but is not great for real production environments). Click **Save**.
- Add a line with **Connection Method** `SSH`, **Port** `22`, **Source** of `0.0.0.0/0`. Click **Save**.

Connecting to an AWS Instance

You can connect to a Linux AWS instance using ssh. Here are the Amazon instructions for doing so.

1. In a command line shell, change directories to the location of the private key file that you created when you launched the instance.

2. Use the `chmod` command to make sure your private key file isn't publicly viewable. For example, if your file were`GSG_Keypair.pem`, you would enter:

```
chmod 400 GSG_Keypair.pem
```

3. Connect to your instance using the instance's public DNS name (which you should have recorded earlier). For example, if the key file is `GSG_Keypair.pem` and the instance's DNS name is ec2-174-129-126-199.compute-1.amazonaws.com, use the following command.

```
ssh -i GSG_Keypair.pem root@ec2-174-129-126-199.compute-1.amazonaws.com
```

   You'll see a response like the following.

```
The authenticity of host 'ec2-174-129-126-199.compute-1.amazonaws.com
(10.254.142.33)'
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)? yes
```

4. Enter `yes`.

   You'll see a response like the following.

```
Warning: Permanently added 'ec2-174-129-126-199.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
```

You're now logged in as root and can work with the instance like you would any normal server. Just remember that you are being billed while the server is alive!

Terminating an AWS 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, 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.