

If you need to run SMRT® Analysis but do **not** have access to a server with CentOS 5.6 or later or Ubuntu 10.0.4 or later, you can use the public SMRT® Analysis **Amazon Machine Image** (AMI).

The AMI we provide is **single-node** only, and does **not** support distributed computing. It is useful for running small to medium-sized secondary analysis jobs, and for using command-line tools.

Note: After you are **finished** working with the AMI, please remember to **stop** the instance, as you are charged an hourly rate.

To analyze data with SMRT® Analysis using the AMI, follow these steps:

Step	Running SMRT® Analysis on Amazon	Links
1	Setting up the Amazon Machine Image	page 1
2	Setting up SMRT® Portal on the Amazon Machine Image	page 5
3	Uploading Your Data to SMRT® Portal using one of these three methods: a) FileZilla b) <code>rsync</code> c) <code>scp</code>	page 5 page 5 page 6
4	Using SSH to access your instance	page 6
5	Stopping or terminating the Amazon Machine Image Instance	page 6

Step 1: Setting up the Amazon Machine Image

1. Go to <http://aws.amazon.com> and create an Amazon Web Services™ account.
2. Click **My Account/Console**, then choose **AWS Management Console**. (Sign in first if asked.)
3. Click **EC2**.
4. Click **Instances**, then click **Launch Instance**.

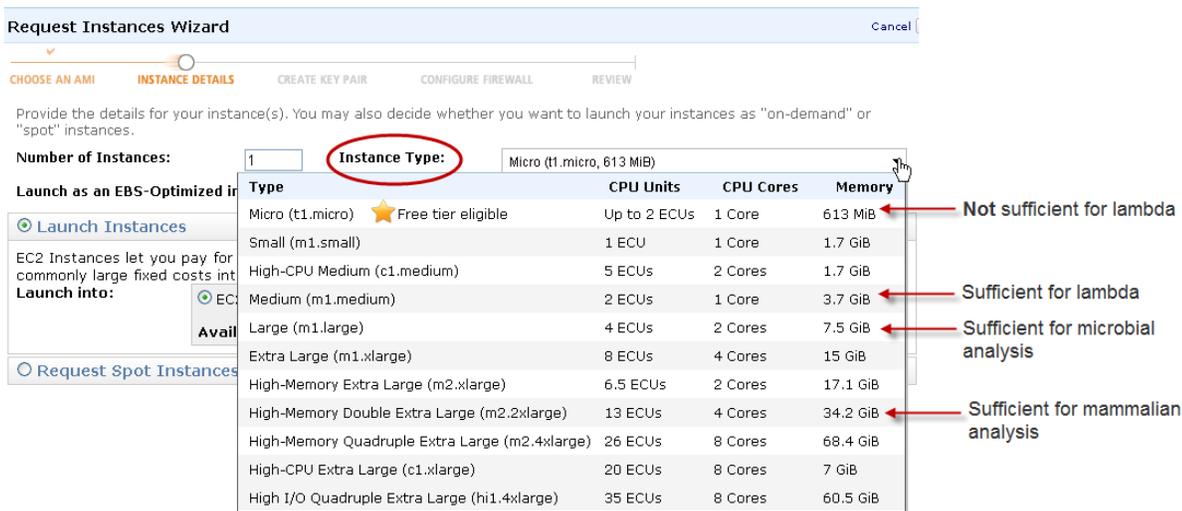


5. Click **Classic Wizard**, then **Continue**.
6. Click the **Community AMIs** tab.
7. Search for `ami-fbbbcf92`, then click **Select**. (This may take several minutes to load.)

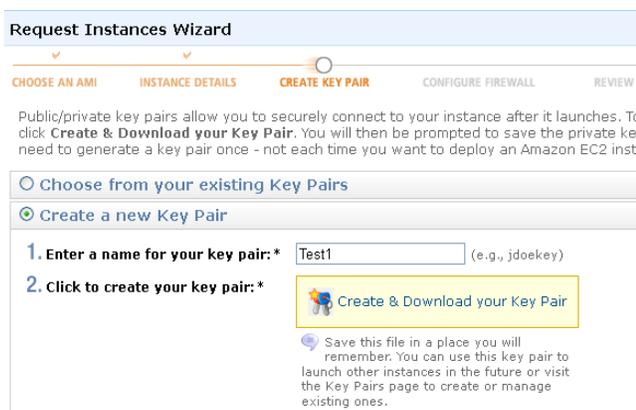
Note: If you get a “JSON Error” message, we recommend that you use the Firefox® or Internet Explorer® web browsers.



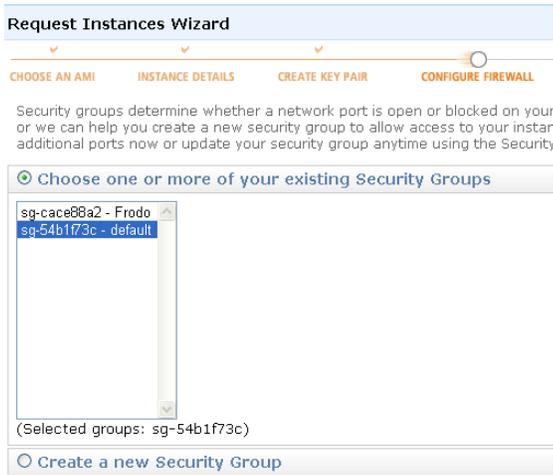
8. Choose an appropriate **Instance Type** for your analysis, then click **Continue**.
Note: A micro instance is **not** sufficient to analyze lambda.



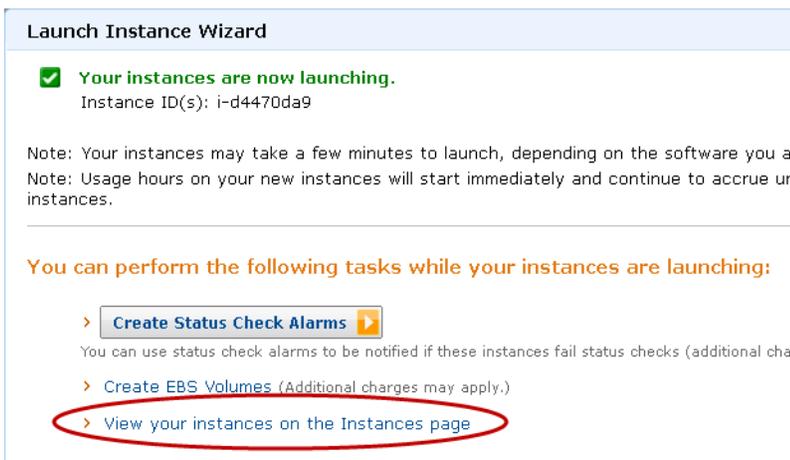
9. Leave the **Advanced Instance Options** as default, then click **Continue**.
10. Leave the **Storage Device Configuration** as default, then click **Continue**.
11. Enter an arbitrary string for the **Name** value, then click **Continue**. (smrtportal is a good default.)
12. Select **Create a new key pair**.
13. Enter a name for your key pair, then click **Create & Download your Key Pair**.



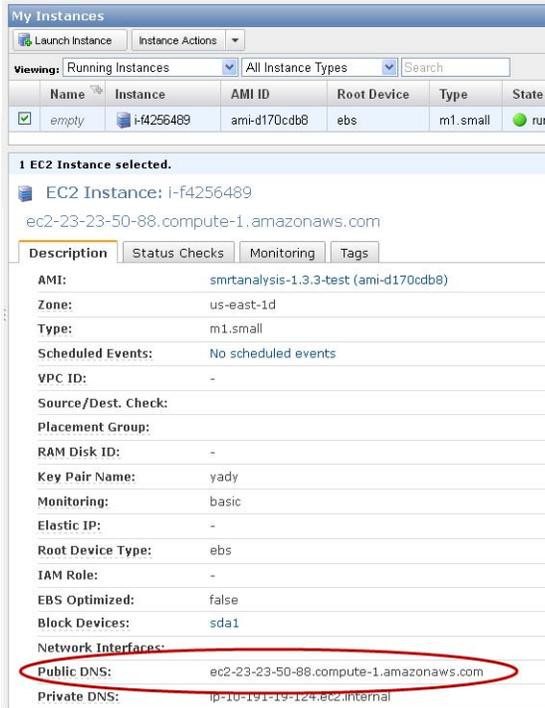
14. Save the key pair file to a safe location on your local machine. (The key pair file has a .pem extension.)
15. Select the security group to associate with the instance, then click **Continue**. (default is fine.)



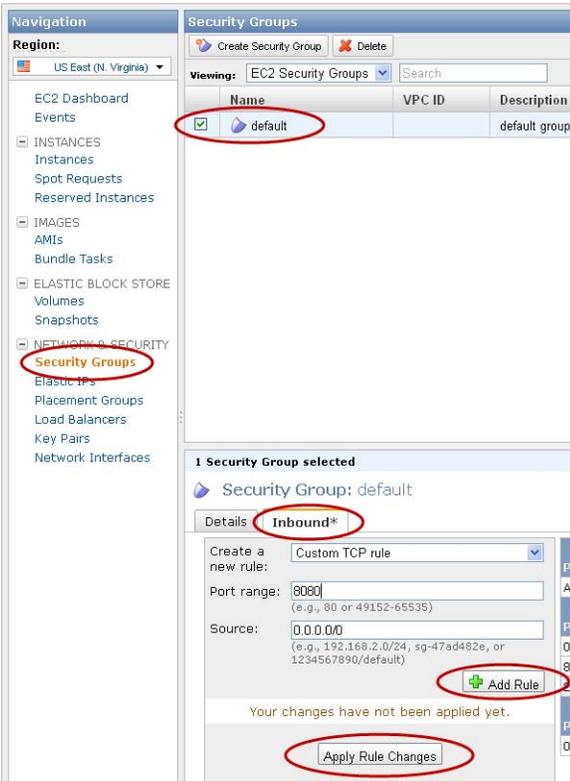
16. Review the settings for your instance, then click **Launch**. **Your instances are now launching** should display.
17. Click **View your instances on the Instances page**. Your instance will take a few minutes to boot up and run through a status check.



18. Select the instance you just created and note the Public DNS address in the **Description** tab. **Note:** You will need this address later on.



19. Click the **Security Group** tab and select the group you specified in Step 15. (If you selected `default`, the values in steps 20-24 are already filled in.)
20. Click the **Inbound** tab at the bottom of the screen.
21. Enter `8080` in the **Port Range** field. (This opens the port necessary for SMRT Portal web access.)
22. Click **+ Add Rule**.
23. Enter `22` in the **Port Range** field. (This opens the port necessary for SSH access.)
24. Click **+ Add Rule**.
25. Click **Apply Rule Changes**. (Note: Your changes are **not** saved until you click this button.)



Step 2: Setting up SMRT® Portal on the Amazon Machine Image

Create a SMRT® Portal administrative user. (You only need to do this **once**.)

26. Use your web browser to access the cloud SMRT® Portal instance by entering `http://<public_dns>:8080/smrtportal`
27. Click **Register** at the top right.
28. Create a user named `administrator` (all lowercase). This user is special, as it is the only user that does **not** require activation on creation.
29. Enter the user name `administrator`.
30. Enter an email address. All administrative emails, such as new user registrations, will be sent to this address. **Note:** You won't actually be able to receive email unless you specify an email server that your instance of AMI can see.
31. Enter the password and confirm the password.

Note: For Step 3, you can upload data to SMRT® Portal using one of three methods: **FileZilla**, **rsync**, or **scp**.

Step 3a: Uploading Your Data to SMRT® Portal using FileZilla

32. Download and install **FileZilla**, a free FTP client. (<http://filezilla-project.org/download.php>)
33. In **FileZilla**, choose **Edit > Settings**, then click **Connection > SFTP**.
34. Click **Add keyfile...** and select the `.pem` file you downloaded in Step 14.
35. You see a dialog box asking for permission to convert the file. Click **Yes** and save the file with a different name, such as `smrtportal_filezilla.ppk`.
36. Click **OK**
37. Enter the Public DNS address (from Step 18) in the **Host** field.
38. Enter `ubuntu` in the **username** field.
39. Enter `22` in the **Port** field.
40. Click **Quickconnect** to log on to the remote SMRT Portal instance.



41. In the **Remote Site** box, enter `/opt/smrtanalysis/common/inputs_dropbox`.
42. In the **Local Site** box, locate the files to transfer and drag them over to the **Remote Site** box.

You can now use SMRT® Portal to scan inputs and run analysis jobs.

Step 3b: Uploading Your Data to SMRT® Portal using rsync

Open a terminal session and use `rsync` to push, from your local machine, input data into the SMRT® Portal dropbox:

- **RSYNC:**
`rsync -r -e 'ssh -i customer.pem' <path to local data directory> ubuntu@{amazon-dns}:/opt/smrtanalysis/common/inputs_dropbox`

Step 3c: Uploading Your Data to SMRT® Portal using scp

Open a terminal session and use `scp` to push, from your local machine, input data into the SMRT® Portal dropbox:

- **SCP:**
`scp -r -i customer.pem <path to local data directory> ubuntu@{amazon-dns}:/opt/smrtdanalysis/common/inputs_dropbox`

Step 4: Using SSH to Access your Instance

1. Ensure that the permissions for the key pair file (with a `.pem` extension) you saved in Step 14 are correct:

From a terminal window, enter the following:

```
$ chmod 400 KEYPAIR.pem
```

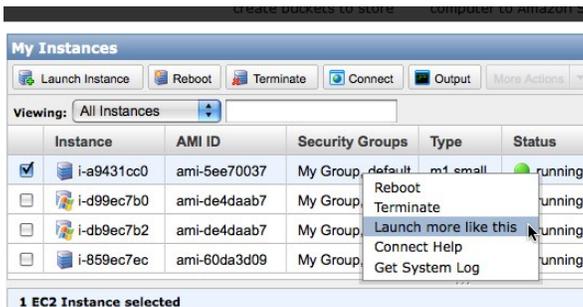
2. From a terminal window, enter the following:

```
$ ssh -i KEYPAIR.pem ubuntu@{amazon-dns}
```

You should now be logged in to your instance using SSH.

Step 5: Stopping or Terminating the Amazon Machine Instance

- When the instance is **stopped**, you are **not** charged hourly, but you **are** charged for storage.
 - When the instance is **terminated**, you are **not** charged hourly, nor are you charged for storage.
1. Click **Instances**, then right-click the running instance and choose **Stop**.
 2. Click **Instances**, then right-click a non-running instance and choose **Terminate**.



For Research Use Only. Not for use in diagnostic procedures. © Copyright 2010 - 2013, Pacific Biosciences of California, Inc. All rights reserved. Information in this document is subject to change without notice. Pacific Biosciences assumes no responsibility for any errors or omissions in this document. Certain notices, terms, conditions and/or use restrictions may pertain to your use of Pacific Biosciences products and/or third party products. Please refer to the applicable Pacific Biosciences Terms and Conditions of Sale and the applicable license terms at <http://www.pacificbiosciences.com/licenses.html>.

Pacific Biosciences, the Pacific Biosciences logo, PacBio, SMRT and SMRTbell are trademarks of Pacific Biosciences in the United States and/or certain other countries. All other trademarks are the sole property of their respective owners.

Amazon Web Services and AWS are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries.

P/N 100-184-200-05