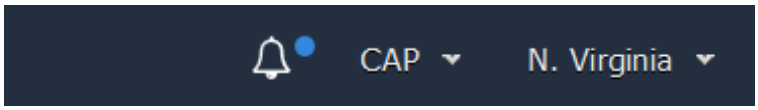
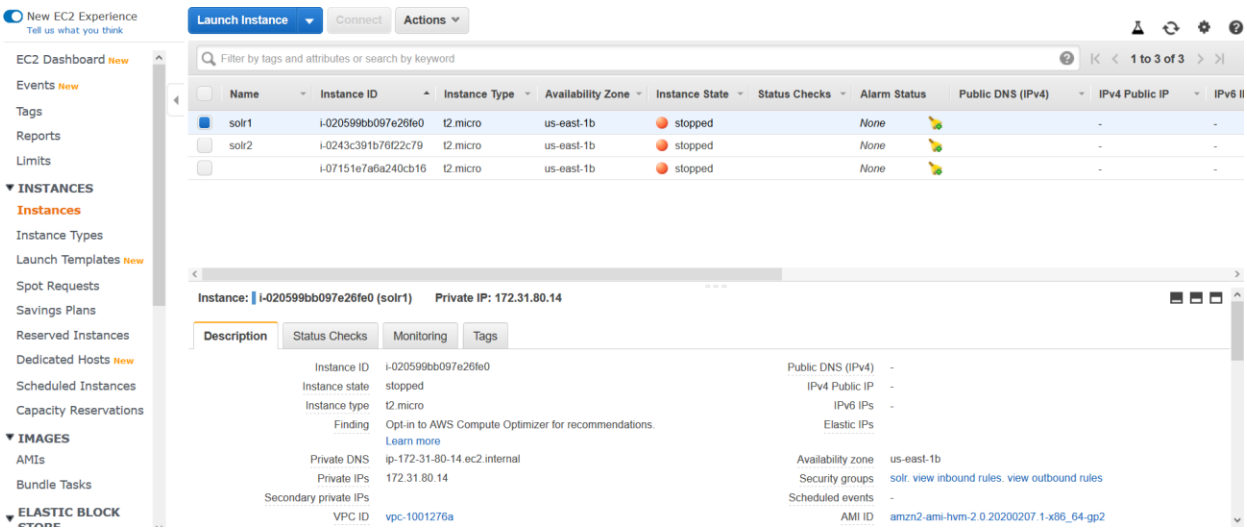
AWS Management Console Notes

1) AWS EC2 Servers

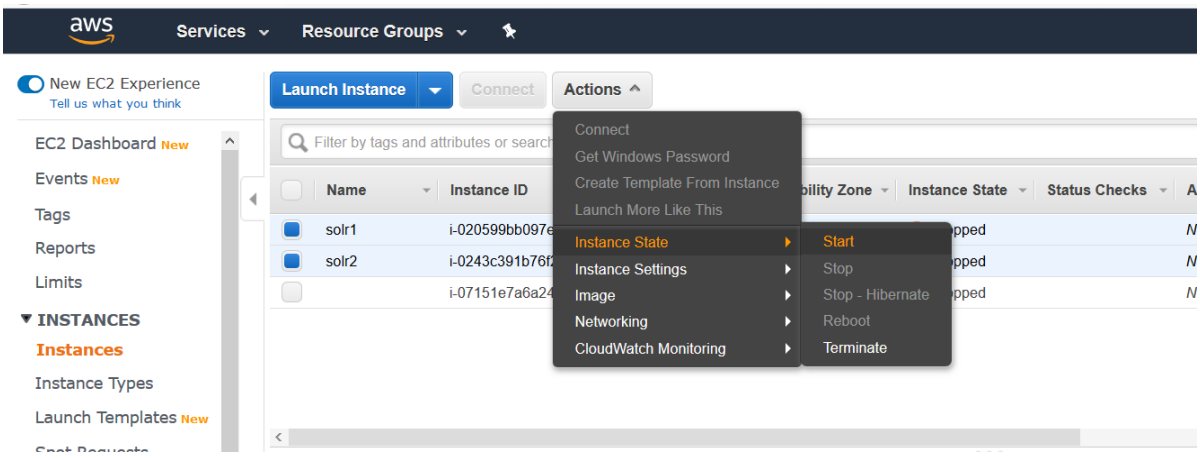
- In total, there are 3 servers that compose CAP, all of which are AWS EC2 servers (instances). One is for the web server and two are for Solr.
    - If you do not see any servers, check to make that you are in the correct region. Every server for this project is in the North Virginia region (N. Virginia). To change your region, click the dropdown at the top right corner of the screen that should either have N. Virginia there or another region and state.

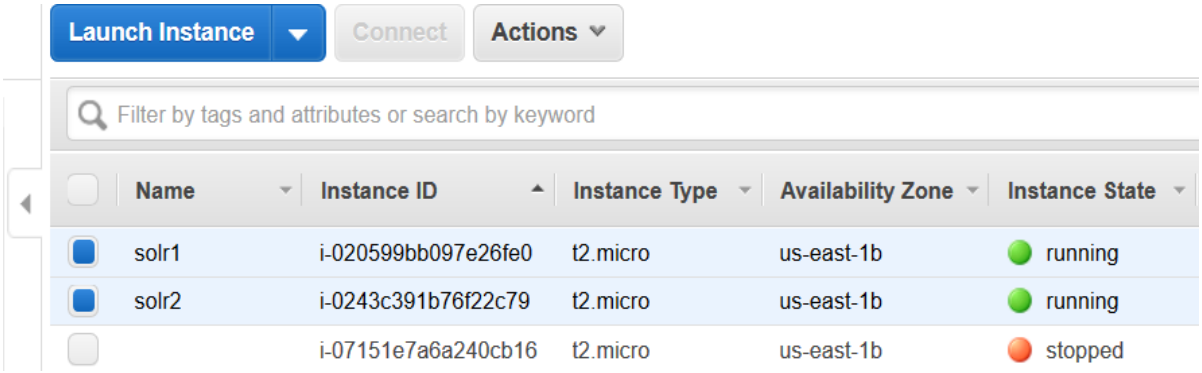


- Two of the servers are named “Solr1” and “Solr2” to differentiate between servers. These names can be changed at any time if need be. If the server names are changed, the servers can still be distinguished by what security group they belong to. Pictured below is the EC2 Management Console.
    - The “Solr1” server is selected and in the “Description” panel we can see that the server is in the “solr” security group. Both “Solr1” and “Solr2” belong to this security group.



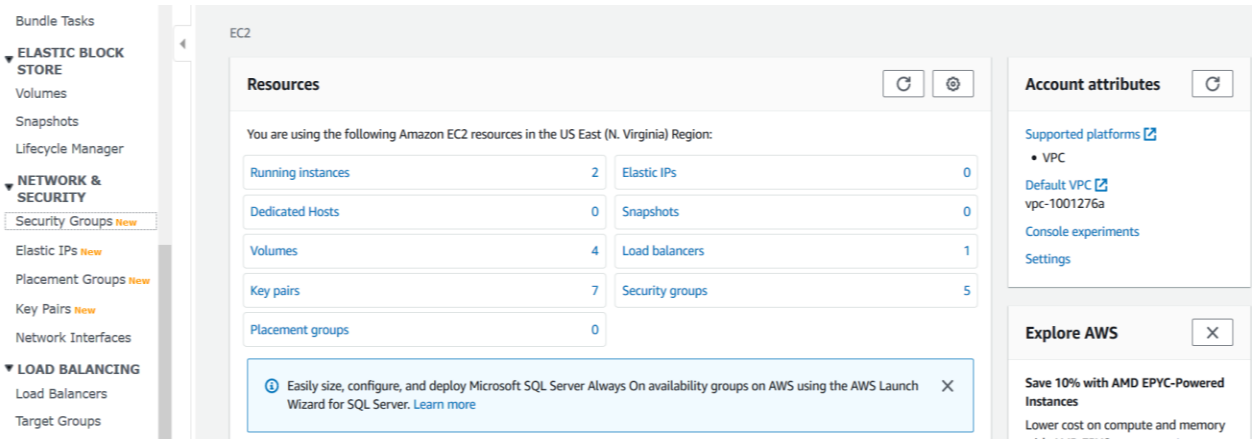
- The screenshot above shows that the instances are currently stopped. This is to not exceed the free tier limits that AWS has. To start the instances back again:
    - Select the instances you want to start up by clicking the grey squares to the left of the server name.
    - Click the “Actions” drop-down button, hover over the “Instance State” text then click “Start”. The instances will take some time to start up again (1-2 minutes).



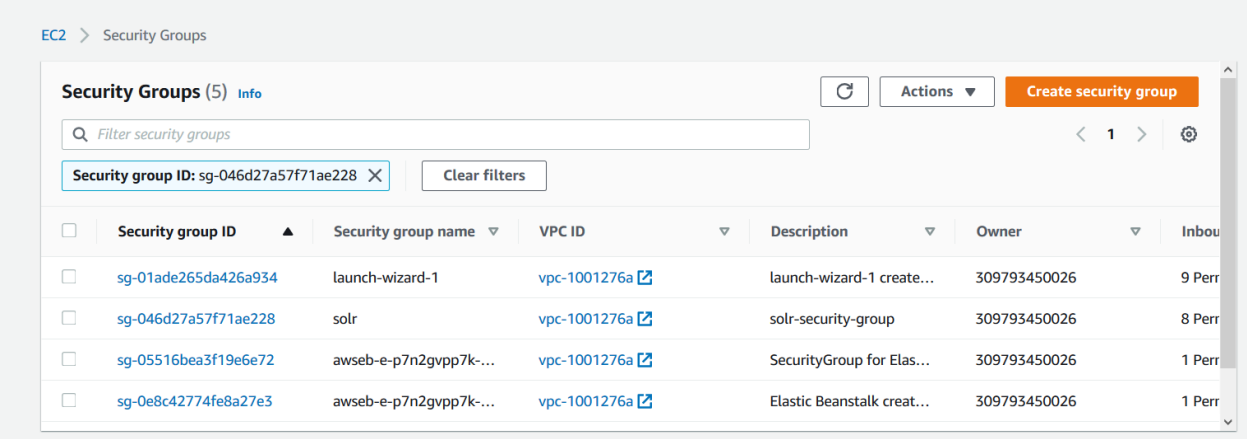


- If you need to stop or want to terminate the instances, follow the same steps above and then select the appropriate action.

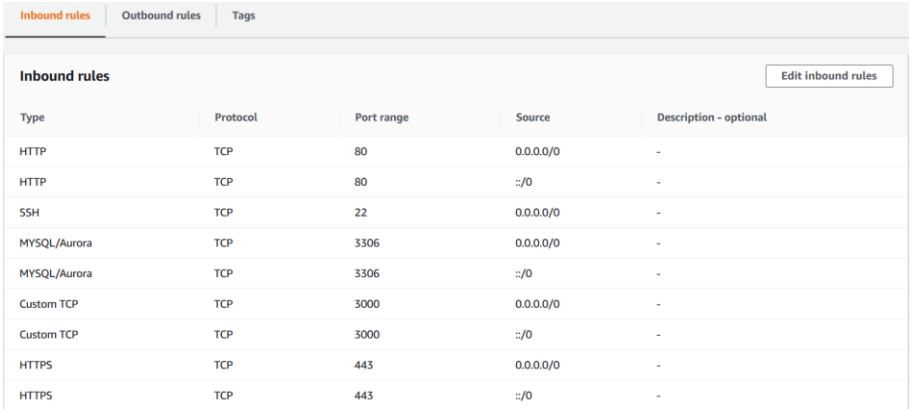
2) EC2 Security Groups
   - Each EC2 instance needs to belong to a security group so that each server knows what traffic, inbound and outbound, the server will accept.
   - To access the security groups of the EC2 instances, go to the EC2 Management Console page. From there you can either click the "Security Group" link in the "Resources" box in the middle of the screen or, on the left hand of the screen, scroll down to the "Network & Security" dropdown and then click "Security Groups".



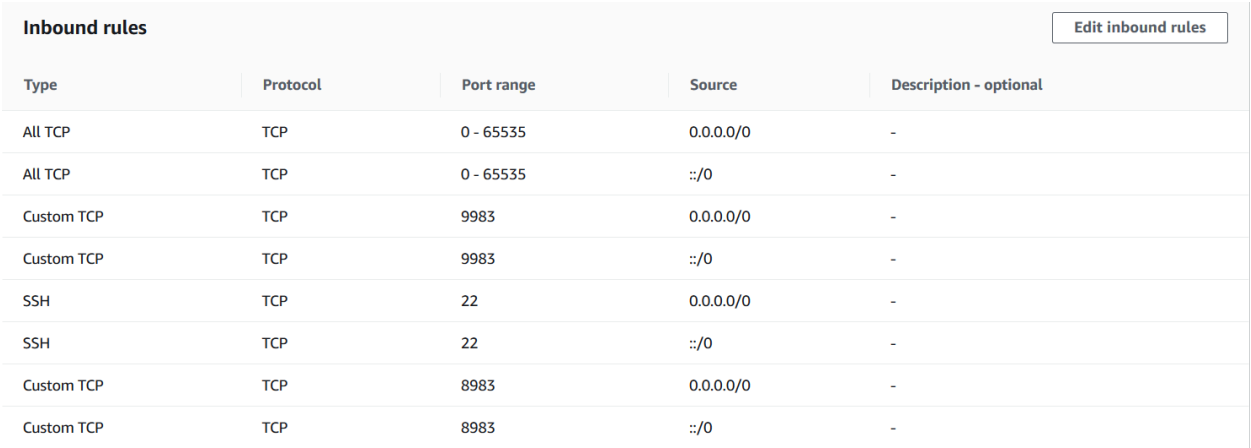
- You should now be able to see all security groups that have been created for the resources you have created.



  - "launch-wizard-1" is the web server security group
  - "solr" is the "Solr1" and "Solr2" security group
  - "awseb…" are the security groups belonging to Beanstalk (for more information view the documentation on AWS Beanstalk and AWS)
- If you click on any of the security groups you will be taken to a page that shows the inbound/outbound rules and tags. During development, the security rules allows for anyone to enter on any port so there are many rules all with the source 0.0.0.0/0 as shown below for the web server rule. The outbound rules allow for all traffic to flow out of the server which is generally acceptable.



- If you select the “solr” security group, you can see the inbound rules also accept any source from any port. The important rule for the Solr servers are the Custom TCP rules included. The associated port numbers (8983 and 9983) are the ports that must be specified when launching the Solr instances. (check the Solr document for launching Solr).



Inbound rules — Edit inbound rules

Type	Protocol	Port range	Source	Description - optional
All TCP	TCP	0 - 65535	0.0.0.0/0	-
All TCP	TCP	0 - 65535	::/0	-
Custom TCP	TCP	9983	0.0.0.0/0	-
Custom TCP	TCP	9983	::/0	-
SSH	TCP	22	0.0.0.0/0	-
SSH	TCP	22	::/0	-
Custom TCP	TCP	8983	0.0.0.0/0	-
Custom TCP	TCP	8983	::/0	-

- To edit, delete, or create rules, click the edit “Inbound” or “Outbound” rules button at the top right. Then, you can select the type of rule, the protocol, port range, and source. Deleting and editing rules may cause issues with launching or accessing resources so it is handy to keep a screenshot or log of the previous rules before modifying them.