Amazon Elasticsearch Service

Fully managed, reliable, and scalable Elasticsearch service.

Easy and Scalable Log Analytics

Inside a VPC

Windows Proxy Instructions

Configuring a proxy to talk to Amazon Elasticsearch Service deployed with the VPC deployment option (Windows).

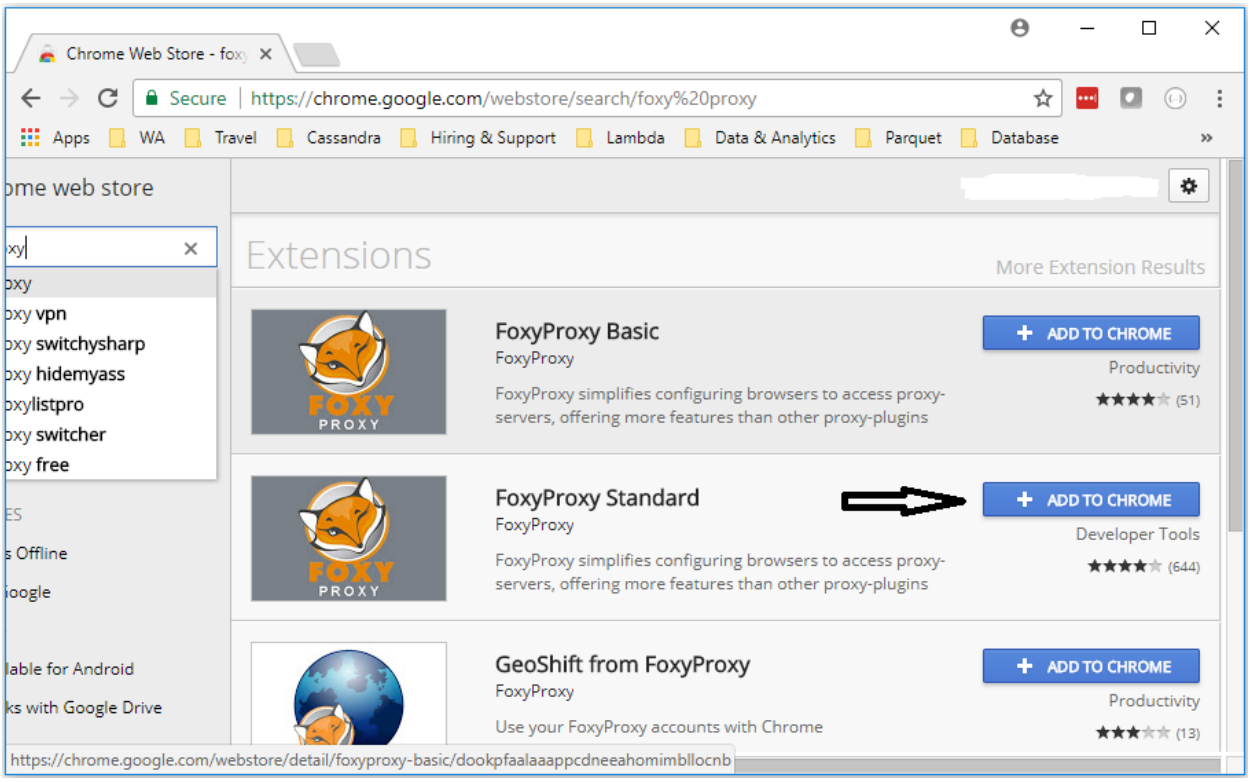
To interact with the Amazon Elasticsearch Service endpoints (the cluster and the Kibana interface) that are in the VPC deployment option, you will need to build a proxy over an SSH tunnel. This requires two things:

1) A browser proxy service like FoxyProxy
2) An SSH Client like PuTTY

Once these two items are installed, we can have some fun with the Amazon Elasticsearch Service cluster itself.

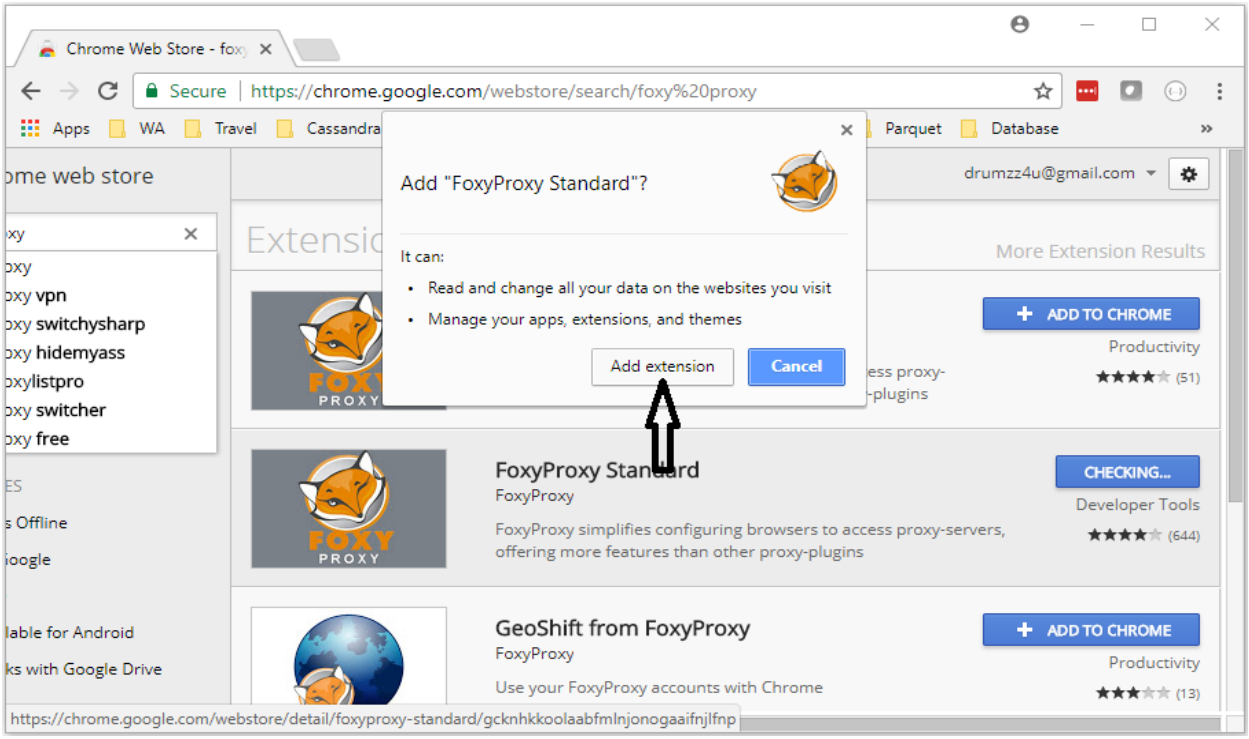
Installing FoxyProxy on Chrome

Navigate to the search bar and look for FoxyProxy (https://chrome.google.com/webstore/search/foxy%20proxy)

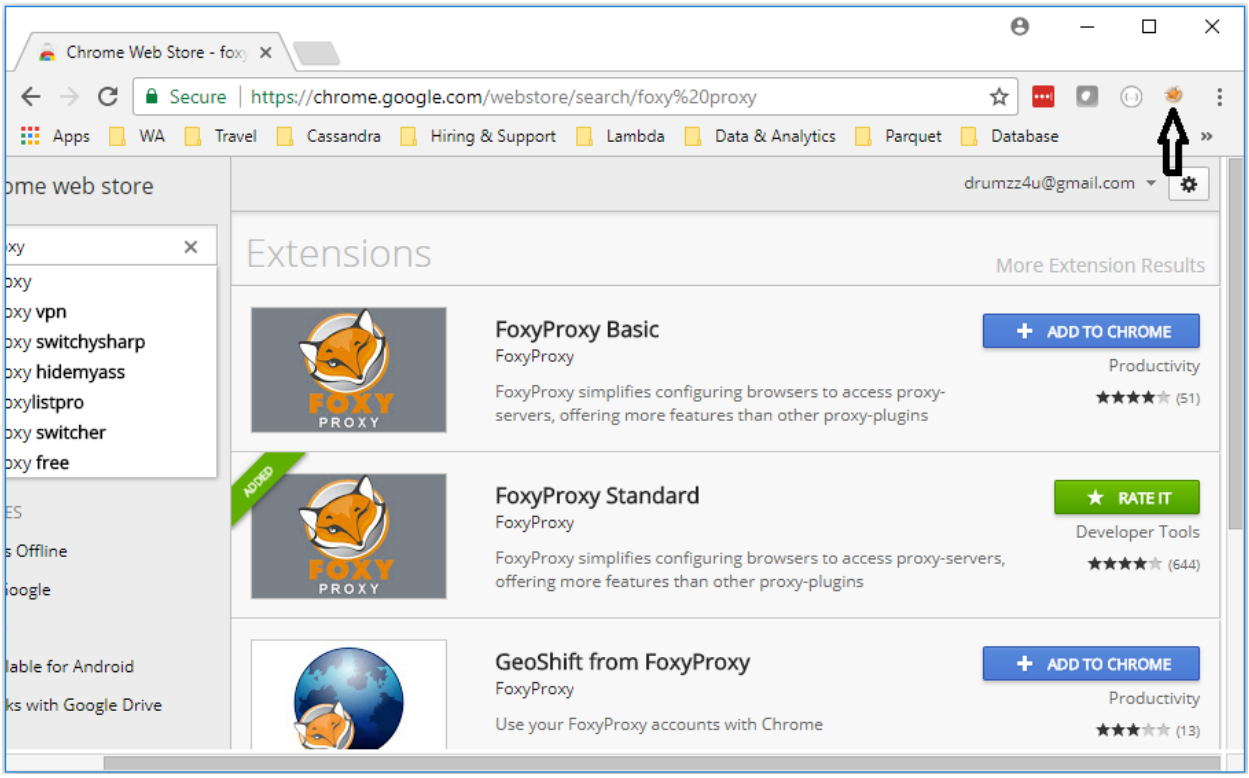


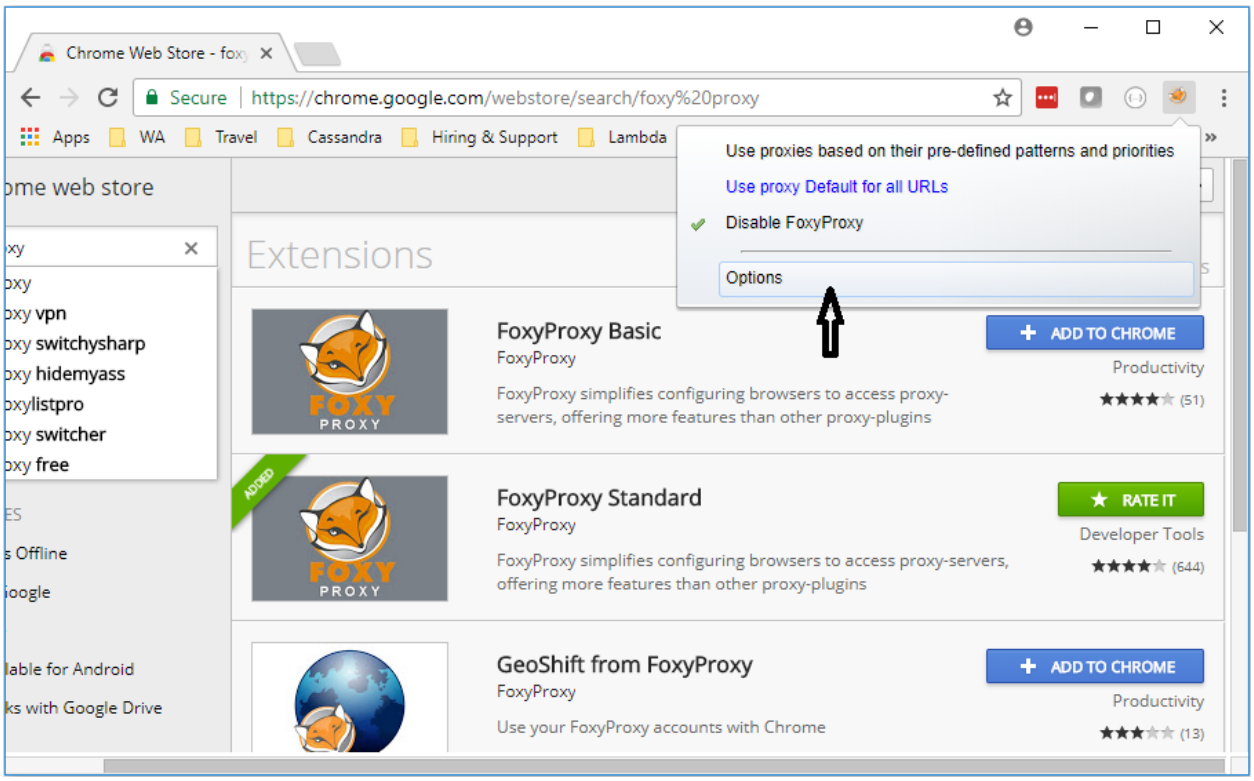
Click on the button to add to Chrome.

Next, you will be presented with a dialog box that asks you to add the extension. Go ahead an click the button.

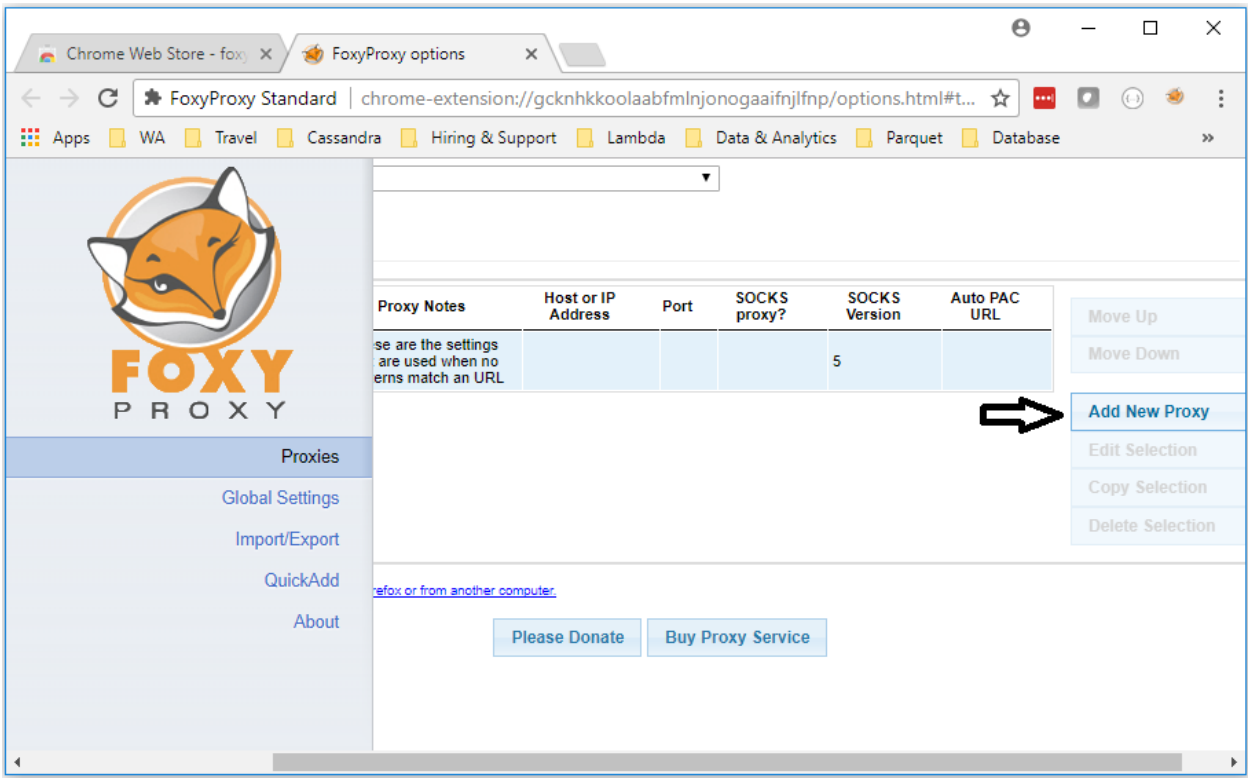


Once intalled, there should be an icon on the top right portion of your screen. Click on that icon.

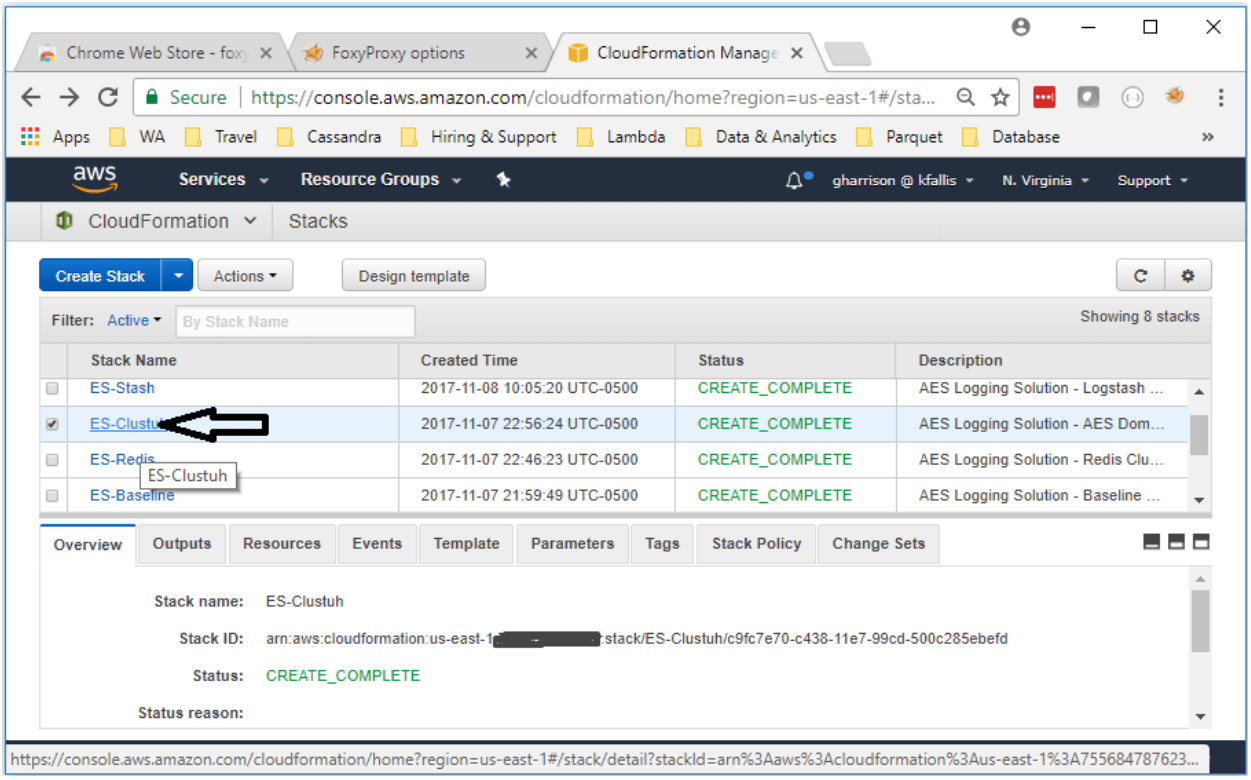




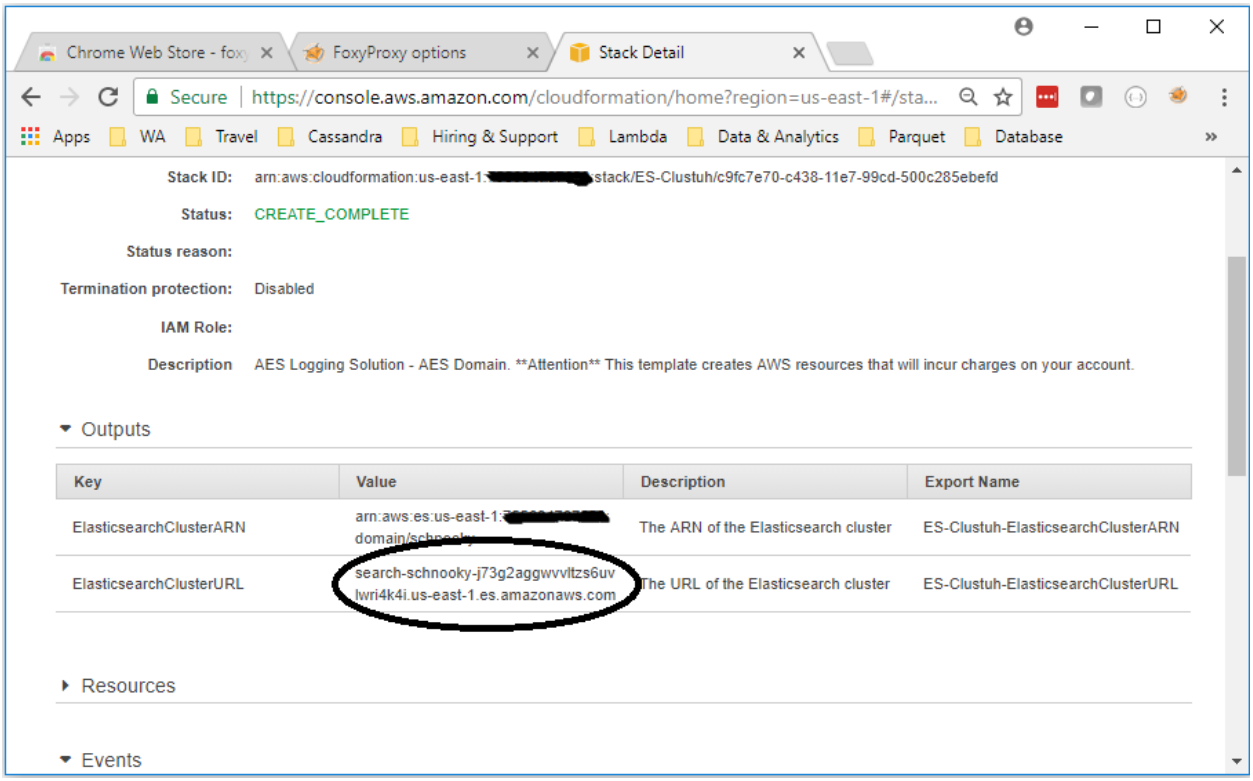
Click on the options. You should see a screen with some proxy configurations.

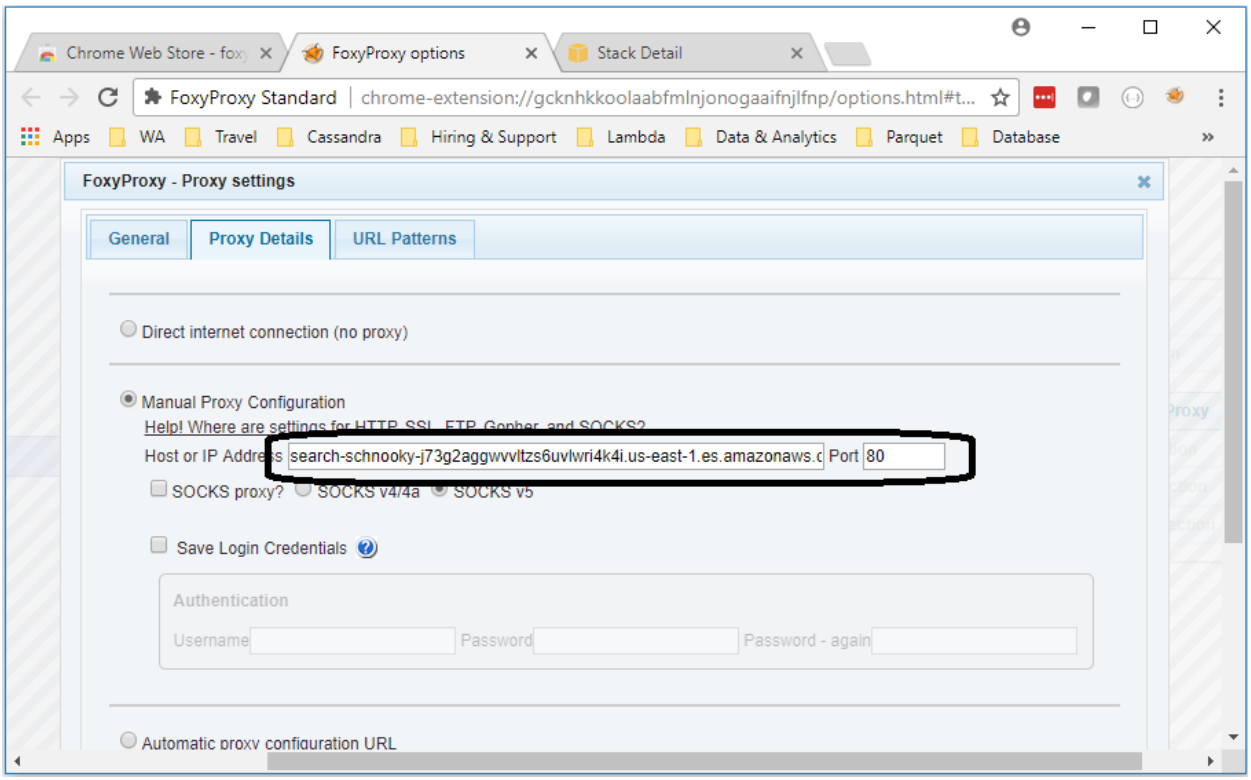


Navigate to your CloudFormation Service console and click on the template that built the cluster.

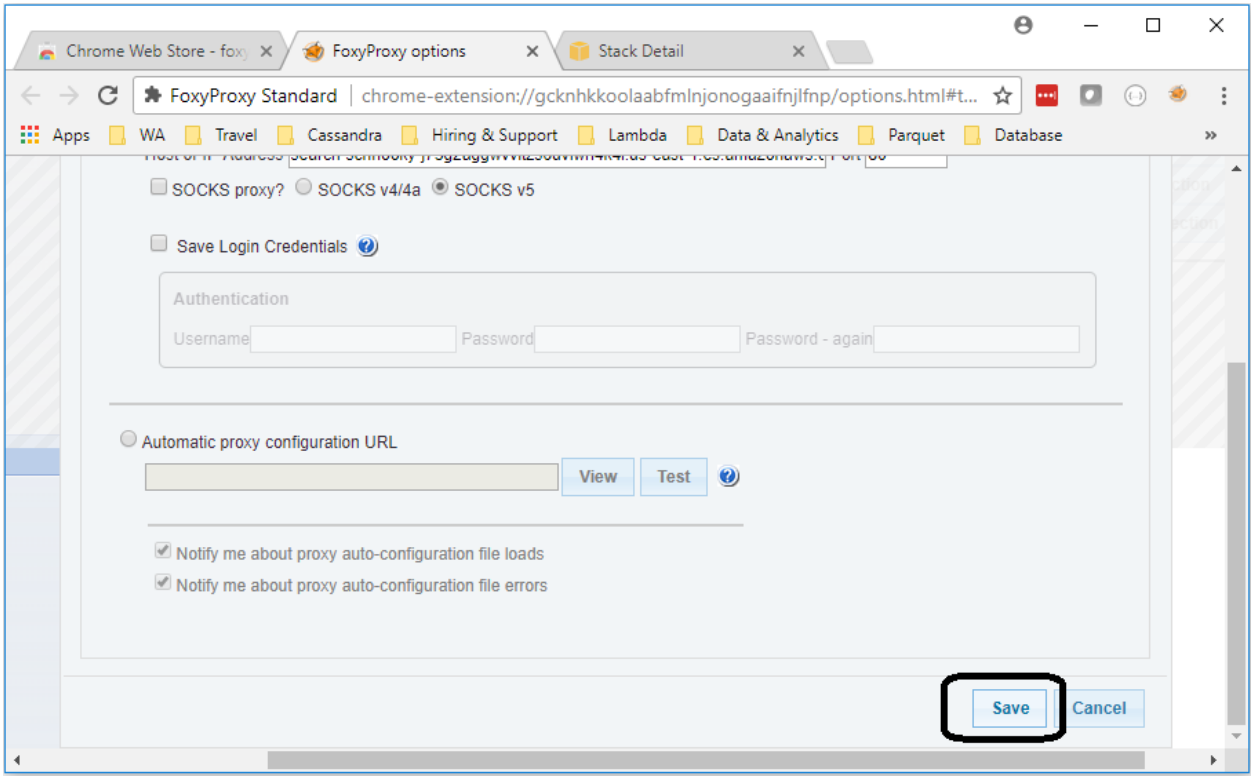


Click into the outputs section and pull back the DNS name (ElasticsearchClusterURL) and paste it in the FoxyProxy settings.

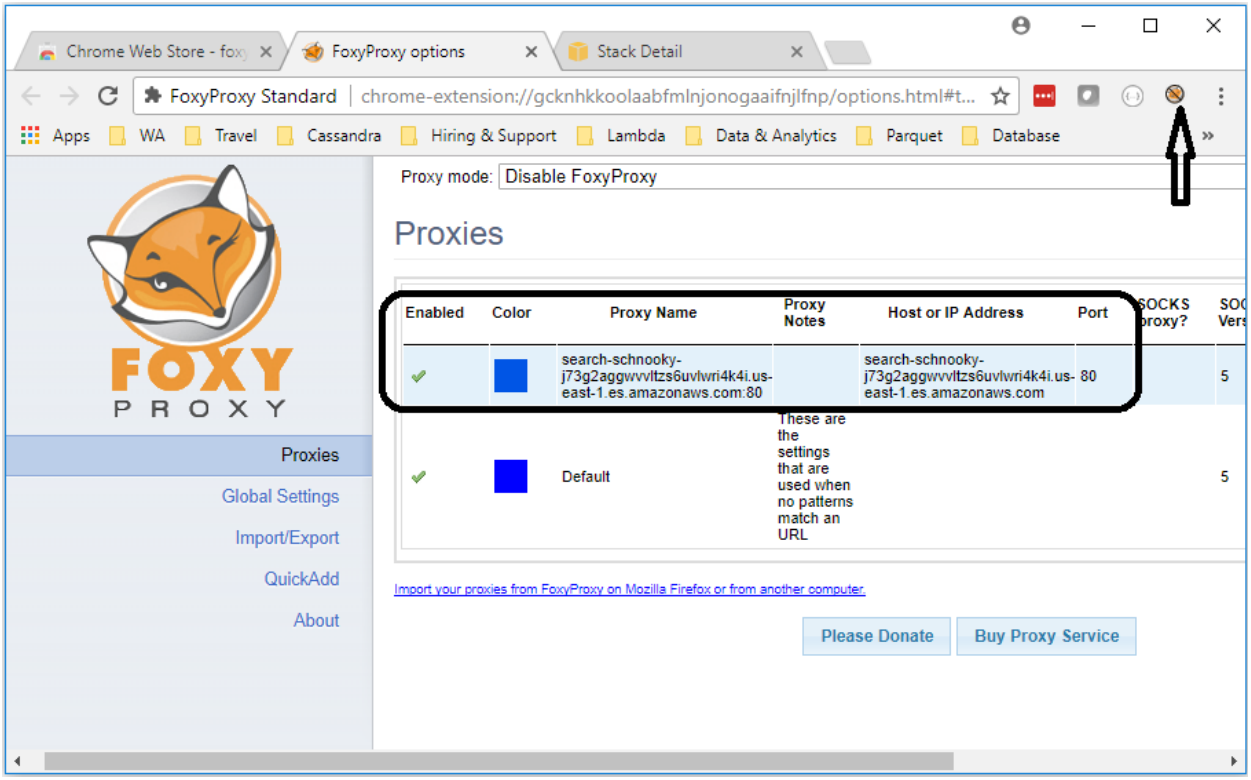




Add port 80 for the port and save the profile.



Now you should see the following:



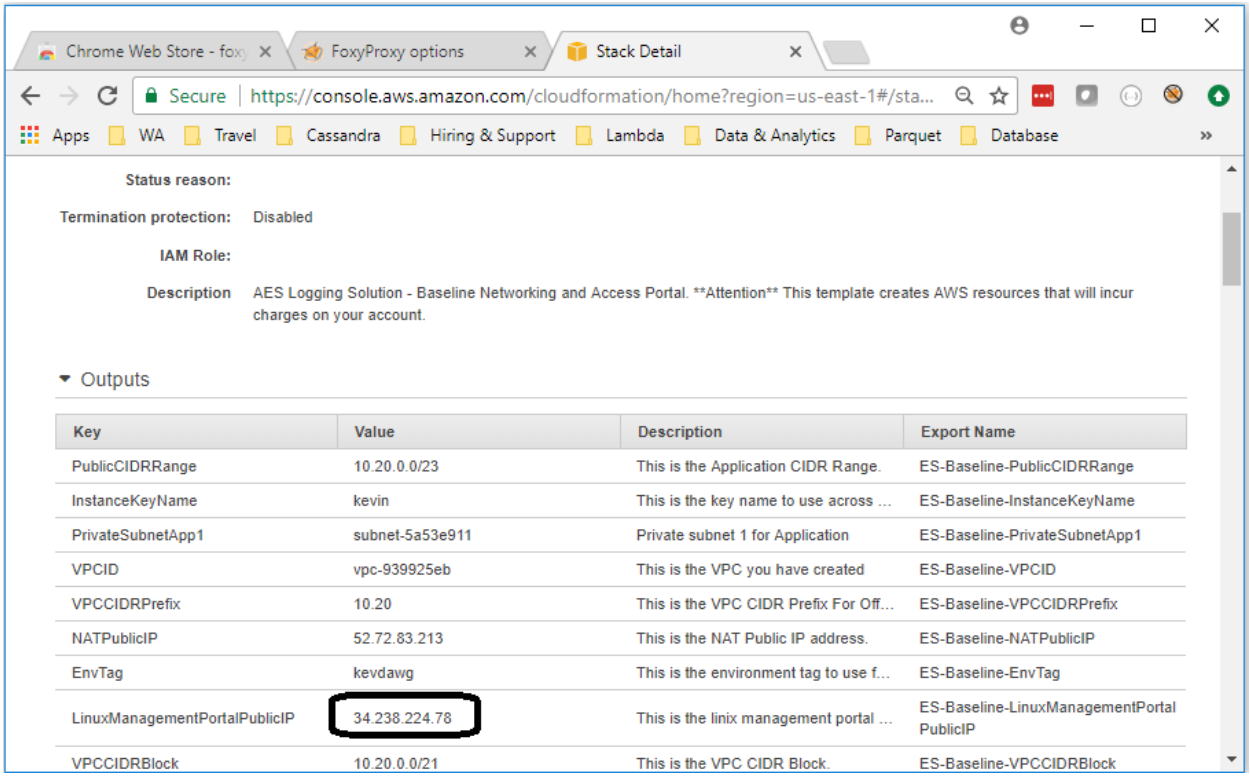
Now proceed to setting up the tunnel.

Install PuTTY and setup a tunnel.

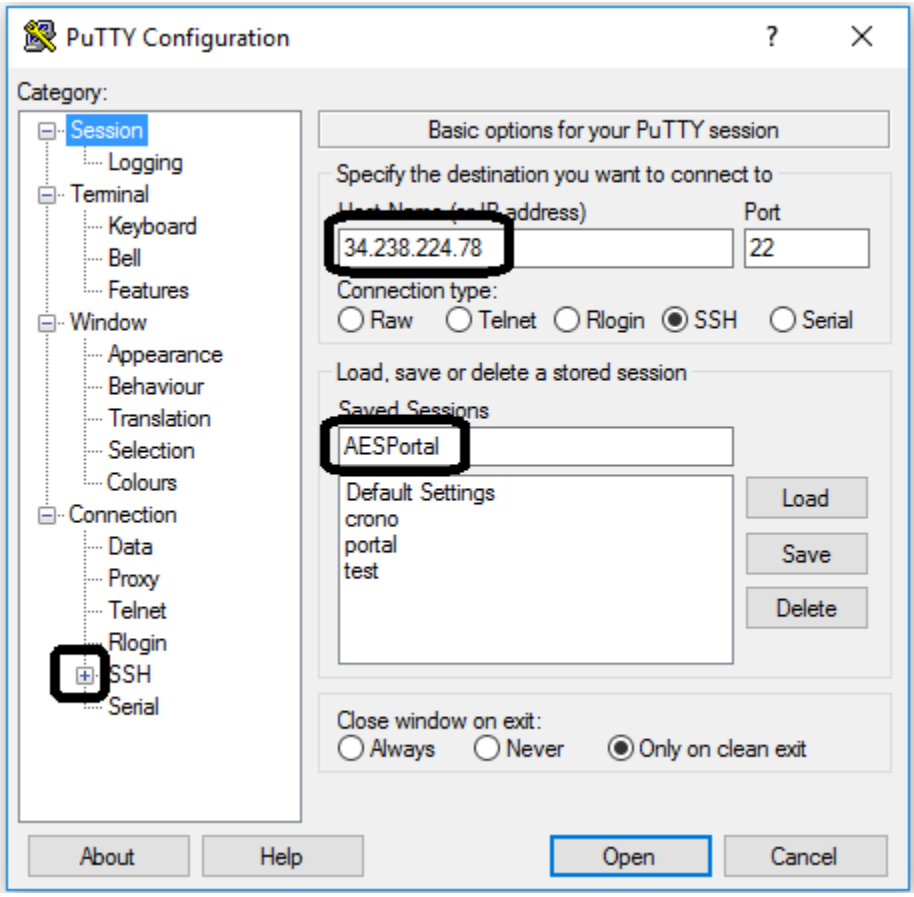
If you do not have putty installed, please download the package from (http://www.putty.org/). I also like to pull in pageant so I don't have to work about providing a path to the .ppk file. There are verbose instructions on the setup found here: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html.

The remainder of these instructions assume that you have an SSH key in .ppk format (not .pem). Instructions on how to convert are also in the instructions above. Additionally, an assumption is made that you have some familiarity with PuTTY.

You will want to take the address of the LinuxManagementPortalPublicIP found in the CloudFormation stack that has the description "AES Logging Solution - Baseline Networking and Access Portal." Use this address for setting up a new session.

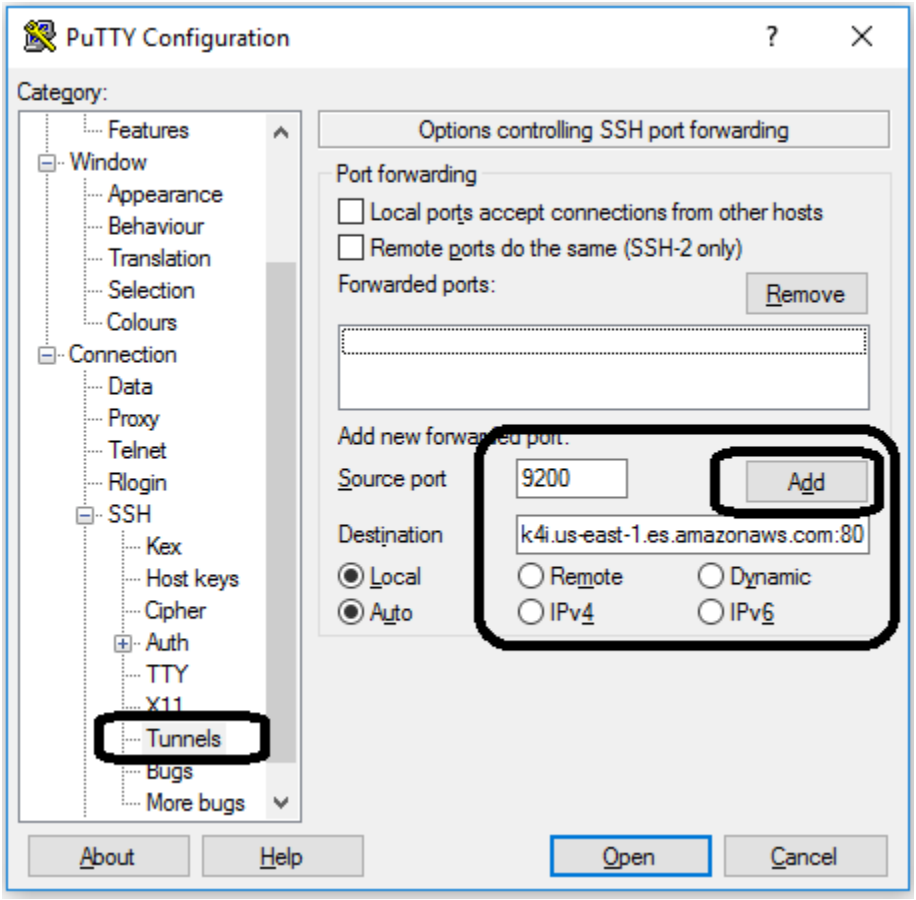


Launch PuTTY and create a new session. Use the IP address from the CloudFormation template for input. Give the session a name since we will want to save this in case we lose the session (low laptop battery, etc).

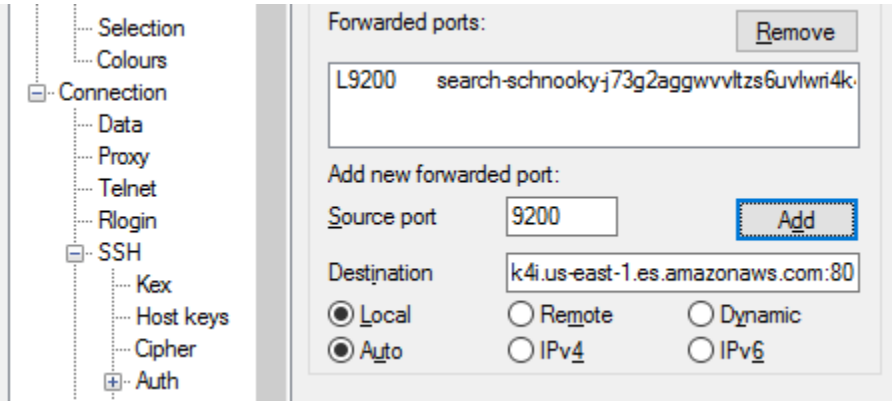


Expand the SSH section and navigate to the Tunnel.

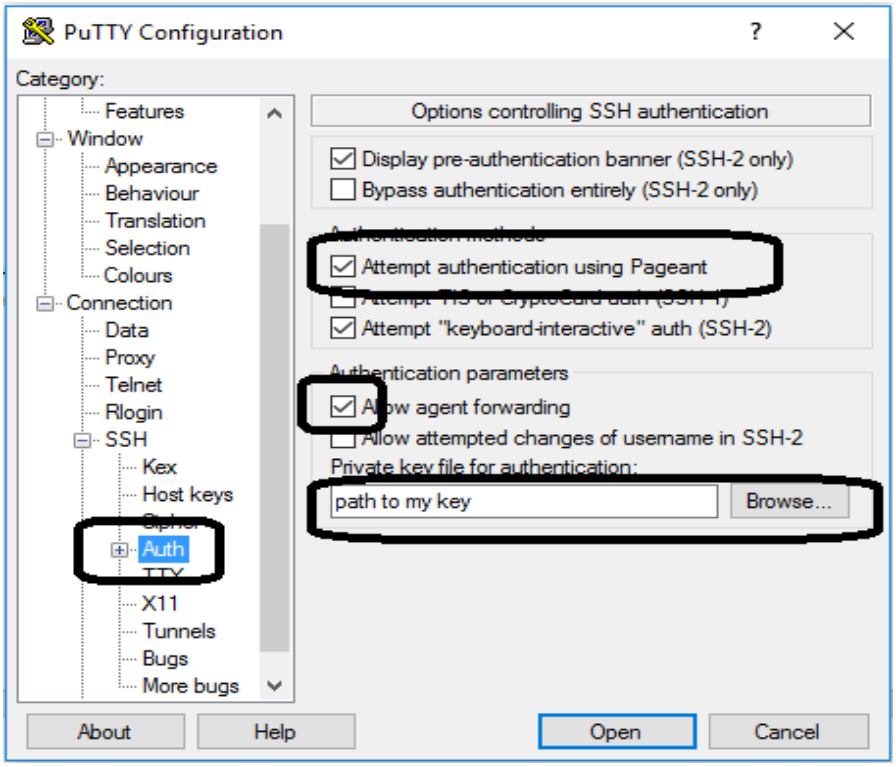
Using the DNS name of the Amazon Elasticsearch Service domain, create a tunnel with a local port of 9200 and a destination of <your cluster DNS>:80. For example search-schnooky-j73g2aggwvvltzs6uvlwri4k4i.us-east-1.es.amazonaws.com:80.



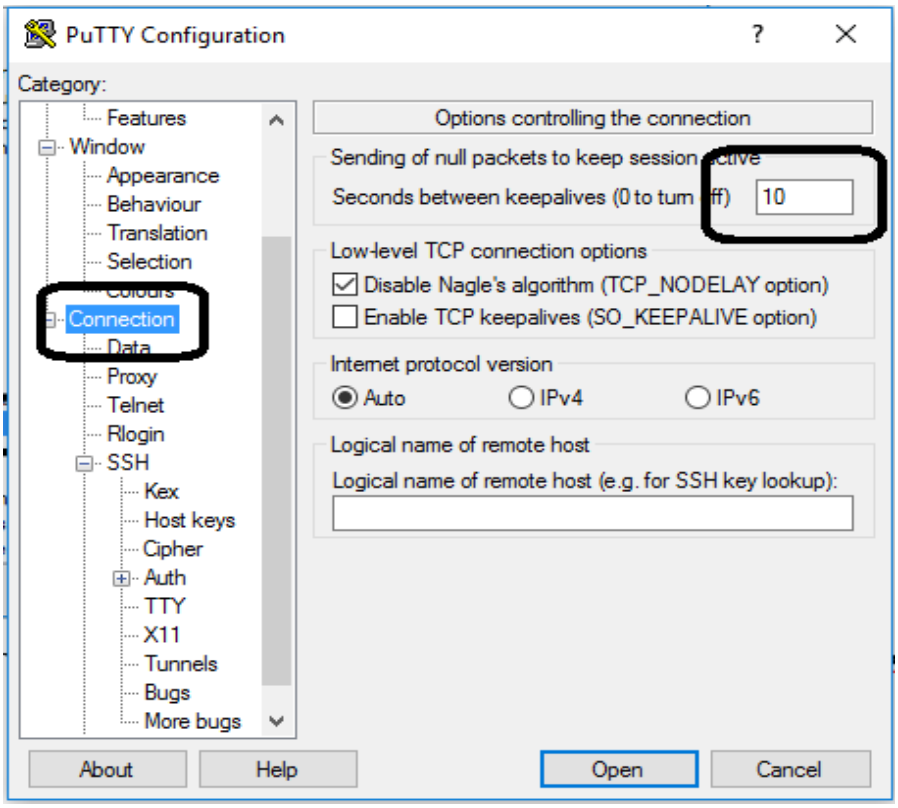
Click the Add button and you should now see something like so:



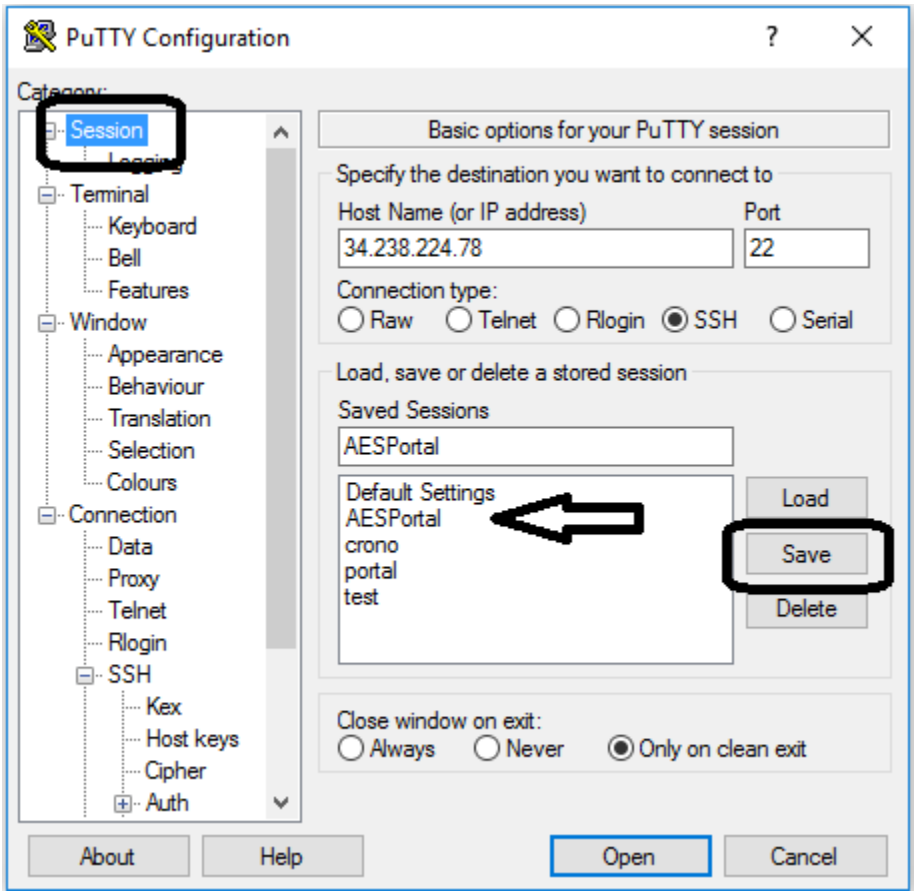
Navigate to the SSH section and add your key or if using pageant, allow agent forwarding:

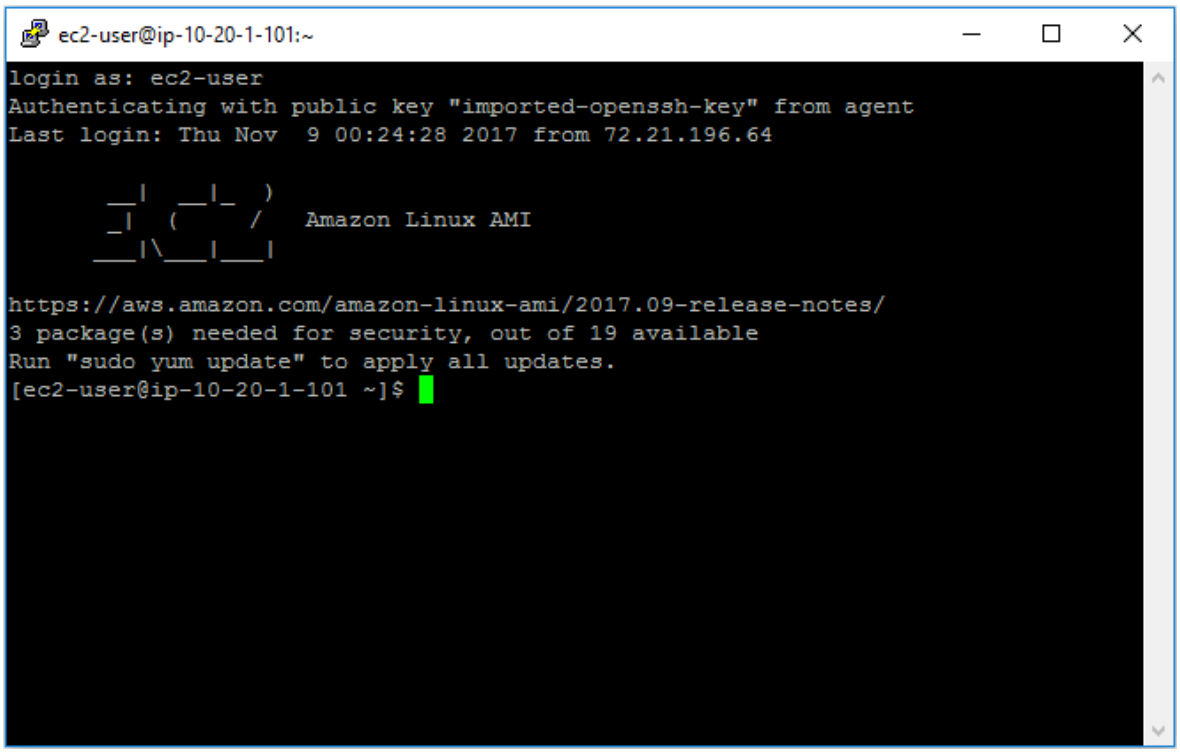


Now set the connection keep-alives so our session does not die. This is in the connection section.

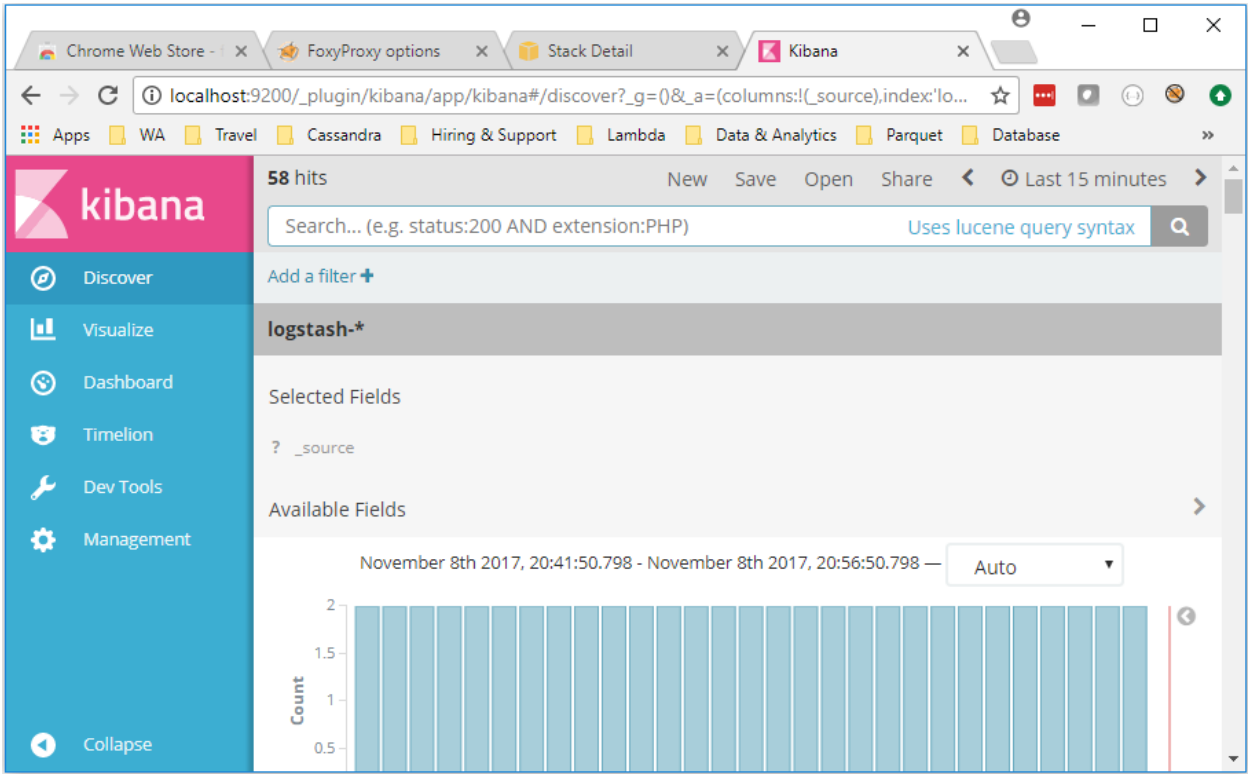


Finally, save the config by scrolling back up to session and clicking save. Go ahead and open the session.





Now, go to your browser and type in “localhost:9200/_plugin/kibana” and you should see something similar to this:



Kibana is now in place and with your browser and a proxy, you can treat the Amazon Elasticsearch Domain and another destination on localhost:9200. Feel free to use postman and other tools to interact with your domain.