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 an SSH Client like PuTTY.

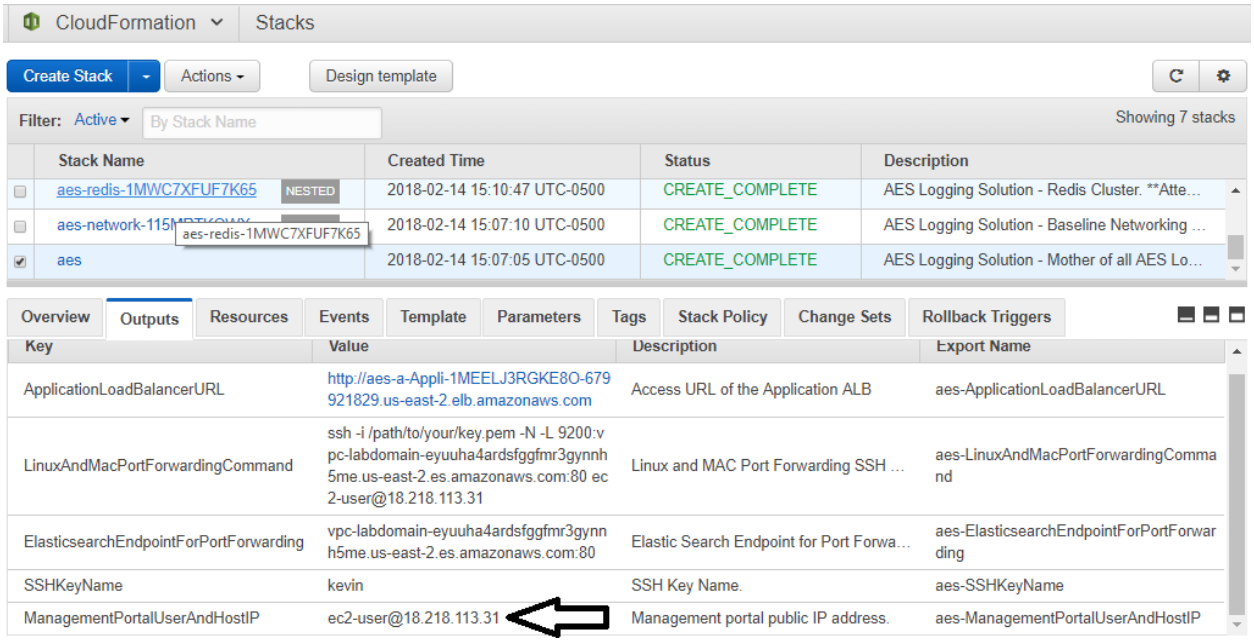
Once installed and configured, we can have some fun with the Amazon Elasticsearch Service endpoint for Kibana.

Install PuTTY and setup a tunnel.

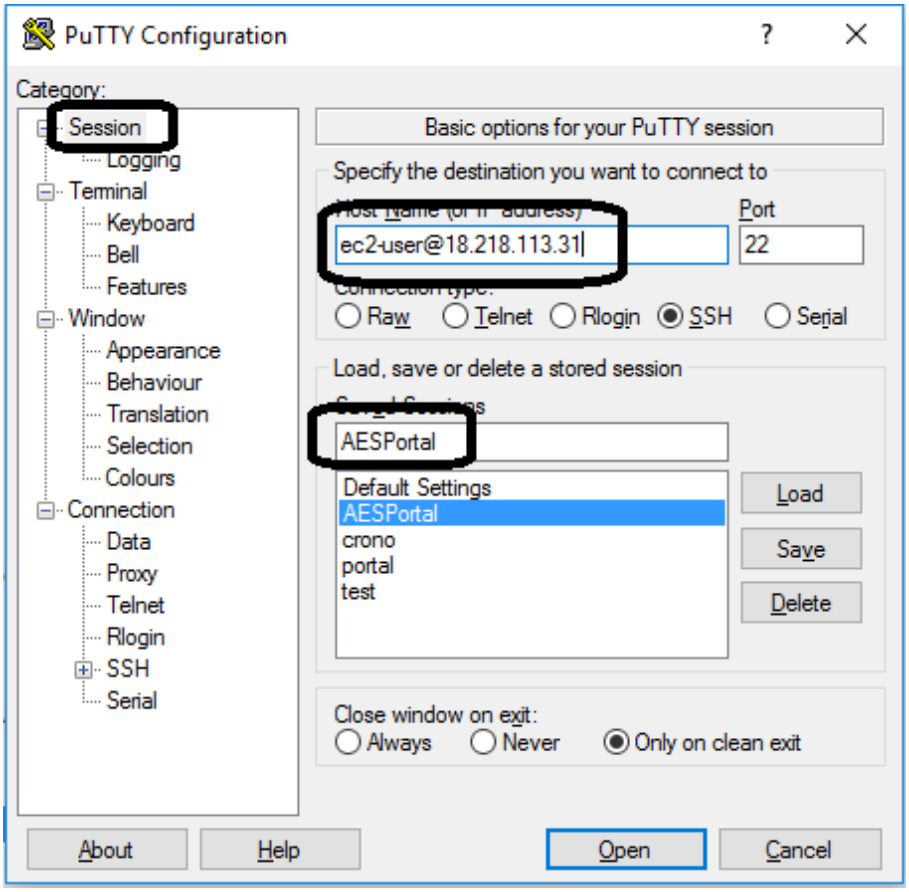
If you do not have putty installed, please download the package from (http://www.putty.org/). I also like to pull in ***pageant*** so I don't have to work about providing a path to the .ppk file. There are verbose instructions on the setup found here: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html.

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 LinuxManagementPortalUserHostAndIP found in the CloudFormation stack that has the description "AES Logging Solution – Mother of all AES Logging stacks." Use this username@address combo for setting up a new session.

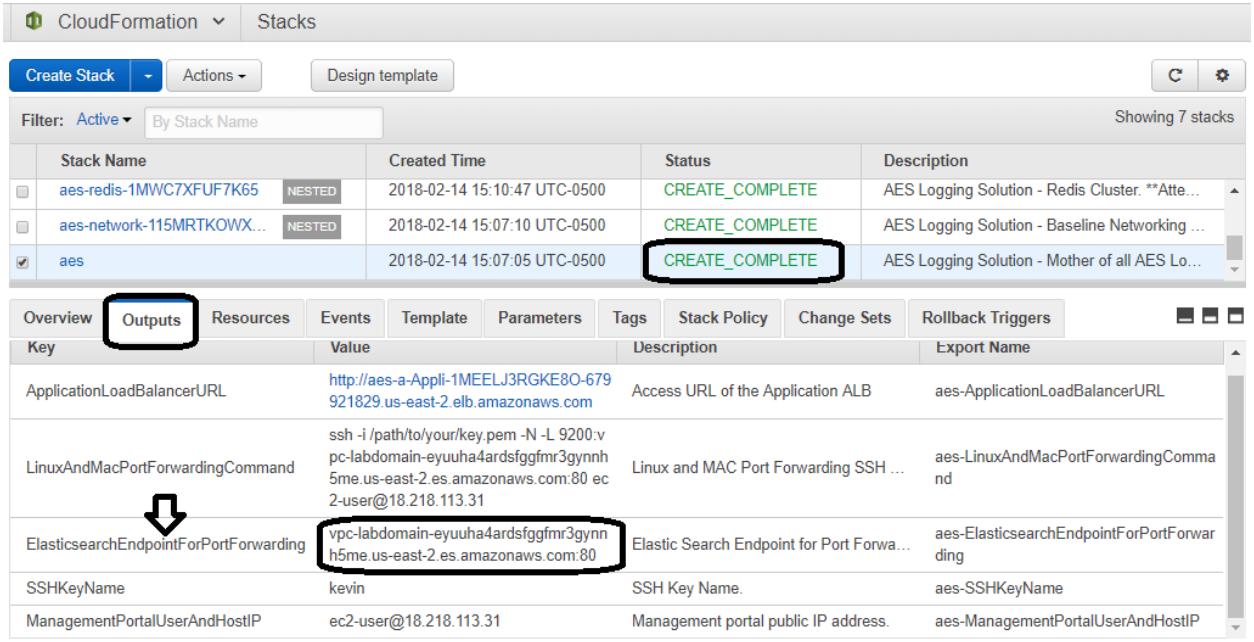


Launch PuTTY and create a new session. Use the IP address from the CloudFormation template for input. Give the session a name since we will want to save this in case we lose the session (low laptop battery, etc).

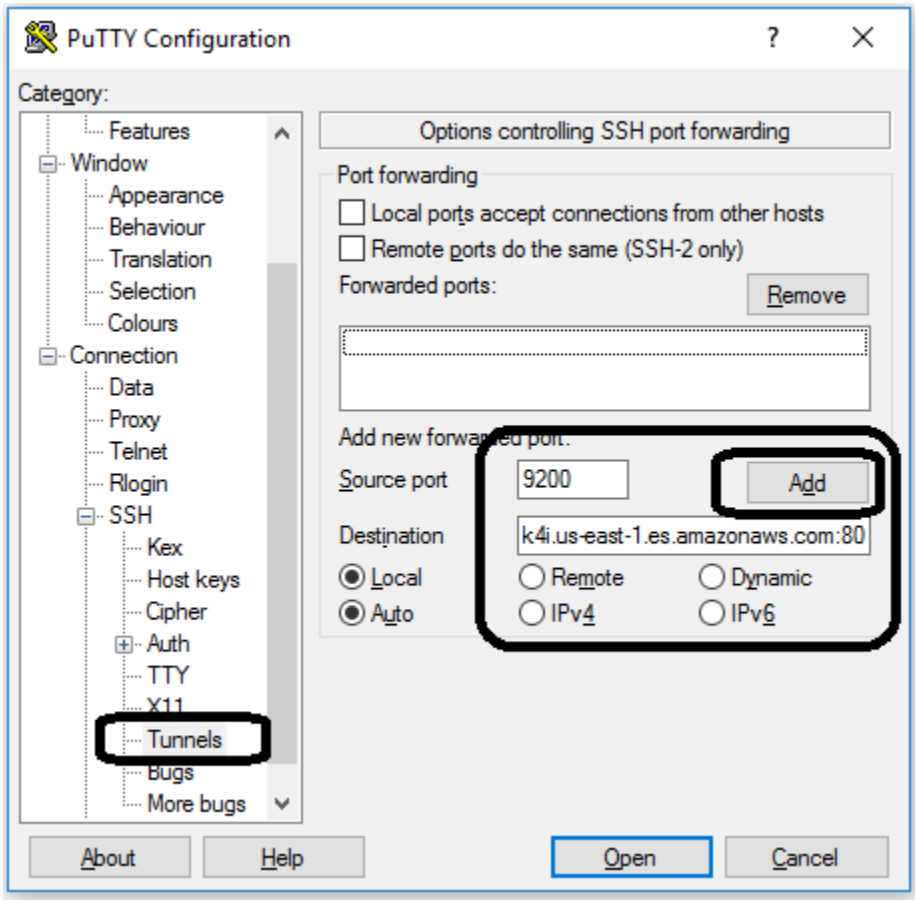


Expand the SSH section and navigate to the Tunnel.

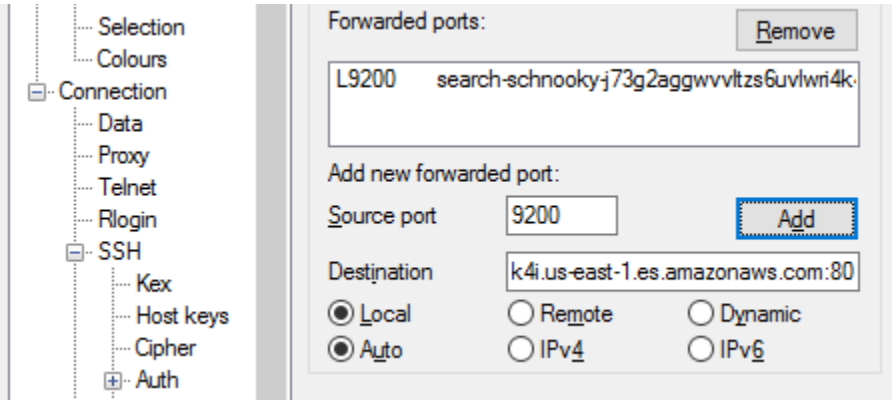
Using the ElasticsearchEndpointForPortForwarding Output parameter, create a tunnel with a local port of 9200 and a destination found in the value of this param as seen below.



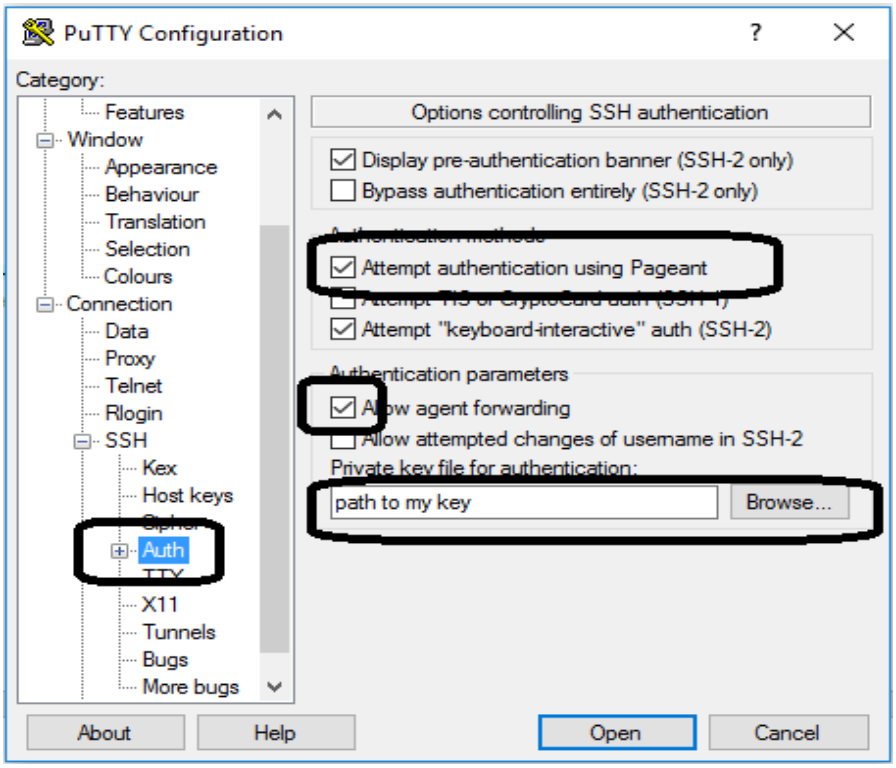
For example: **vpc-labdomain-eyuuha4ardsfggfmr3gynnh5me.us-east-2.es.amazonaws.com:80**



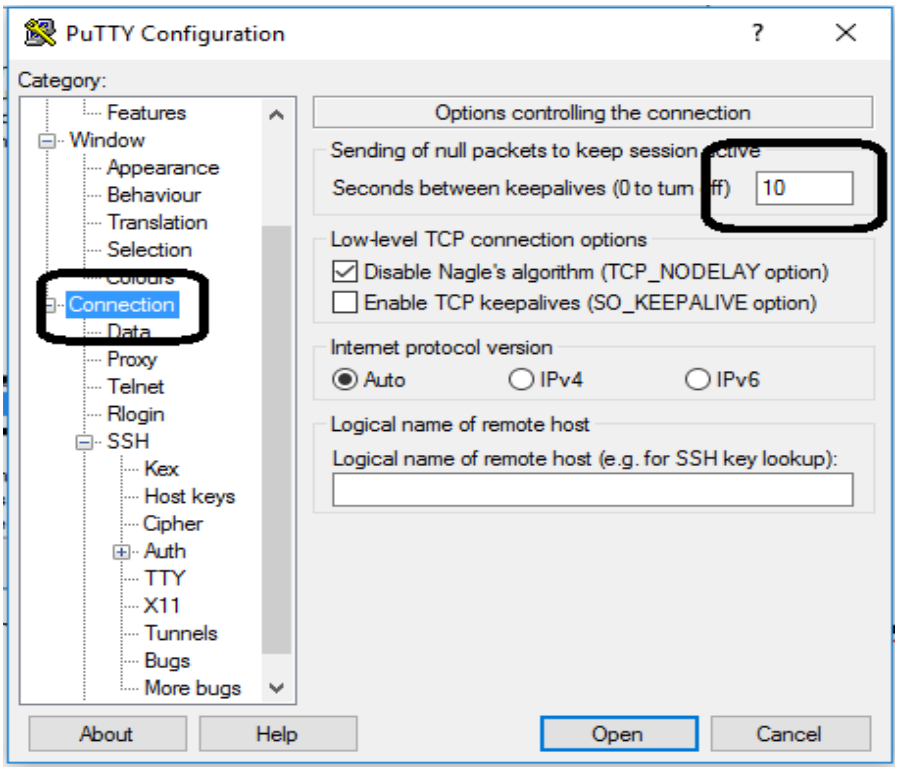
Click the Add button and you should now see something like pictured below:



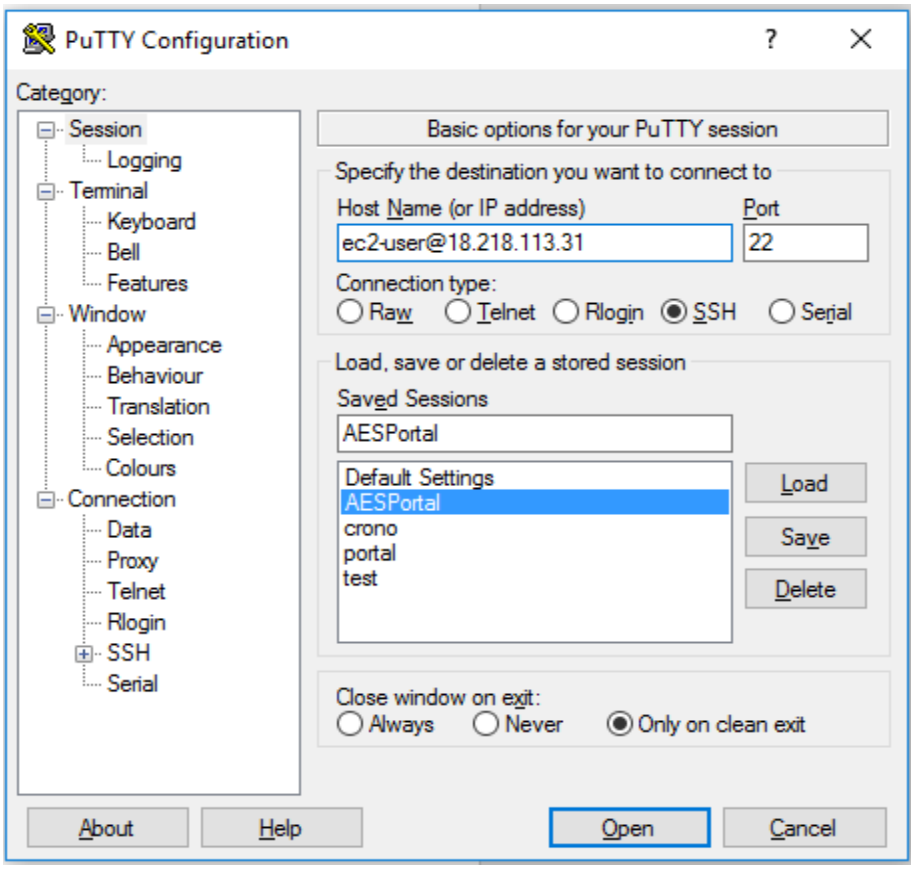
Navigate to the SSH section and add your key or if using pageant, allow agent forwarding:

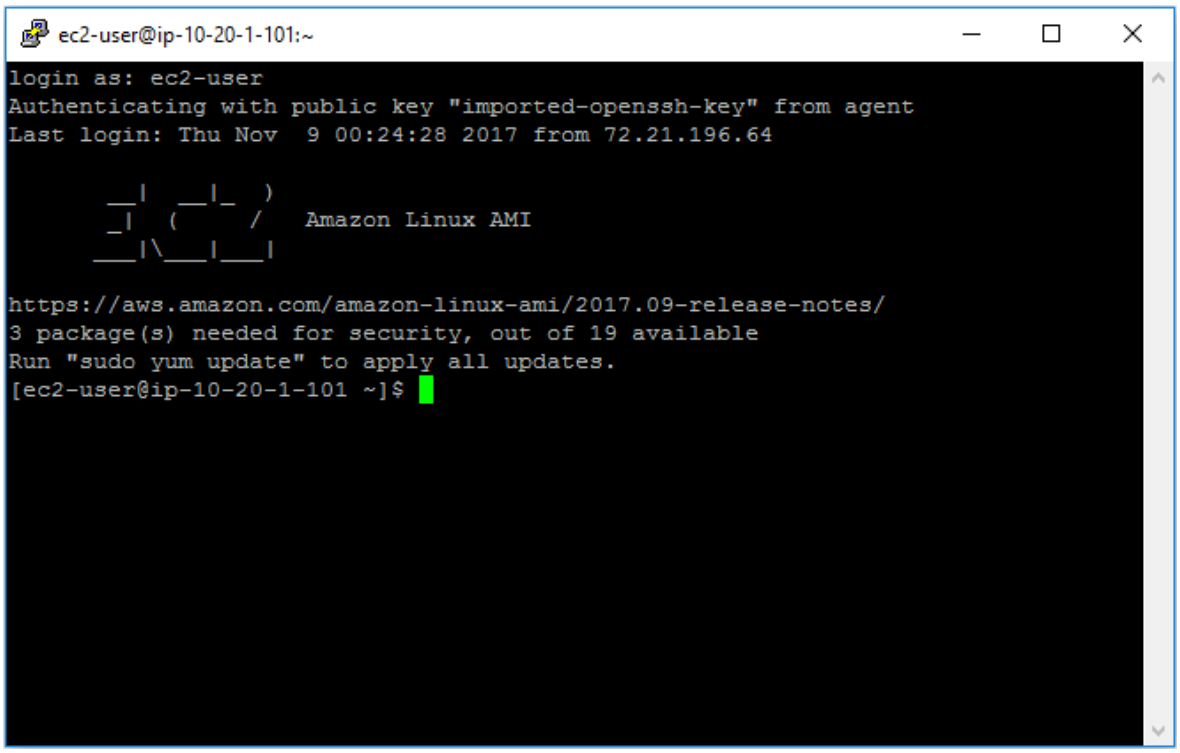


Now set the connection keep-alives so our session does not die. This is in the connection section.



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: