



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.

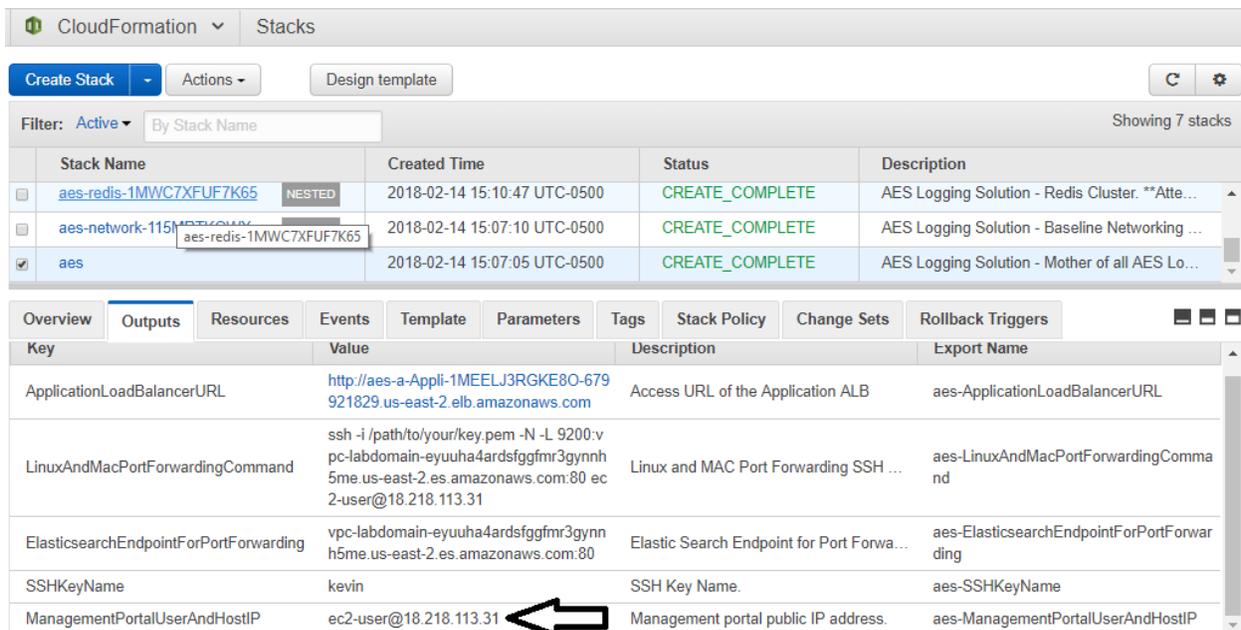
Install PuTTY and setup a tunnel.

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.



The screenshot shows the AWS CloudFormation console. At the top, there are tabs for 'CloudFormation' and 'Stacks'. Below that, there are buttons for 'Create Stack', 'Actions', and 'Design template'. A filter is set to 'Active' and 'By Stack Name'. A table lists three stacks:

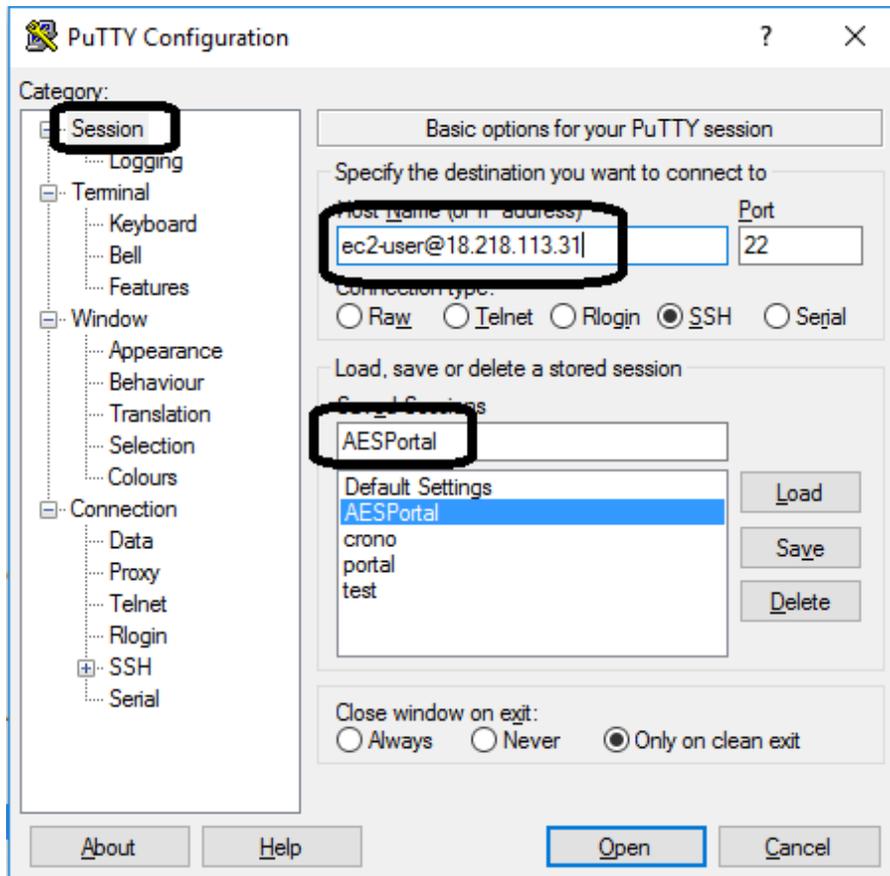
Stack Name	Created Time	Status	Description
aes-redis-1MWC7XFUF7K65	2018-02-14 15:10:47 UTC-0500	CREATE_COMPLETE	AES Logging Solution - Redis Cluster. **Atte...
aes-network-115M...	2018-02-14 15:07:10 UTC-0500	CREATE_COMPLETE	AES Logging Solution - Baseline Networking ...
✓ aes	2018-02-14 15:07:05 UTC-0500	CREATE_COMPLETE	AES Logging Solution - Mother of all AES Lo...

Below the stack list, the 'Outputs' tab is selected for the 'aes' stack. It shows a table of outputs:

Key	Value	Description	Export Name
ApplicationLoadBalancerURL	http://aes-a-Appli-1MEELJ3RGKE8O-679921829.us-east-2.elb.amazonaws.com	Access URL of the Application ALB	aes-ApplicationLoadBalancerURL
LinuxAndMacPortForwardingCommand	ssh -i /path/to/your/key.pem -N -L 9200:vpc-labdomain-eyuuha4ardsfggfmr3gynnh5me.us-east-2.es.amazonaws.com:80 ec2-user@18.218.113.31	Linux and MAC Port Forwarding SSH ...	aes-LinuxAndMacPortForwardingCommand
ElasticsearchEndpointForPortForwarding	vpc-labdomain-eyuuha4ardsfggfmr3gynnh5me.us-east-2.es.amazonaws.com:80	Elastic Search Endpoint for Port Forwa...	aes-ElasticsearchEndpointForPortForwarding
SSHKeyName	kevin	SSH Key Name.	aes-SSHKeyName
ManagementPortalUserAndHostIP	ec2-user@18.218.113.31	Management portal public IP address.	aes-ManagementPortalUserAndHostIP

A black arrow points to the 'ManagementPortalUserAndHostIP' output value 'ec2-user@18.218.113.31'.

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.

CloudFormation Stacks

Filter: Active By Stack Name Showing 7 stacks

Stack Name	Created Time	Status	Description
aes-redis-1MWOC7XFUF7K65	2018-02-14 15:10:47 UTC-0500	CREATE_COMPLETE	AES Logging Solution - Redis Cluster. **Atte...
aes-network-115MRTKOWX...	2018-02-14 15:07:10 UTC-0500	CREATE_COMPLETE	AES Logging Solution - Baseline Networking ...
aes	2018-02-14 15:07:05 UTC-0500	CREATE_COMPLETE	AES Logging Solution - Mother of all AES Lo...

Overview **Outputs** Resources Events Template Parameters Tags Stack Policy Change Sets Rollback Triggers

Key	Value	Description	Export Name
ApplicationLoadBalancerURL	http://aes-a-Appli-1MEELJ3RGKE80-679921829.us-east-2.elb.amazonaws.com	Access URL of the Application ALB	aes-ApplicationLoadBalancerURL
LinuxAndMacPortForwardingCommand	ssh -i /path/to/your/key.pem -N -L 9200:vpc-labdomain-eyuuha4ardsfggfmr3gynnh5me.us-east-2.es.amazonaws.com:80 ec2-user@18.218.113.31	Linux and MAC Port Forwarding SSH ...	aes-LinuxAndMacPortForwardingCommand
ElasticsearchEndpointForPortForwarding	vpc-labdomain-eyuuha4ardsfggfmr3gynnh5me.us-east-2.es.amazonaws.com:80	Elastic Search Endpoint for Port Forwa...	aes-ElasticsearchEndpointForPortForwarding
SSHKeyName	kevin	SSH Key Name.	aes-SSHKeyName
ManagementPortalUserAndHostIP	ec2-user@18.218.113.31	Management portal public IP address.	aes-ManagementPortalUserAndHostIP

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

PuTTY Configuration

Category:

- Features
- Window
 - Appearance
 - Behaviour
 - Translation
 - Selection
 - Colours
- Connection
 - Data
 - Proxy
 - Telnet
 - Rlogin
 - SSH
 - Kex
 - Host keys
 - Cipher
 - Auth
 - TTY
 - X11
 - Tunnels**
 - Bugs
 - More bugs

Options controlling SSH port forwarding

Port forwarding

Local ports accept connections from other hosts

Remote ports do the same (SSH-2 only)

Forwarded ports: [Remove]

Add new forwarded port.

Source port: 9200 [Add]

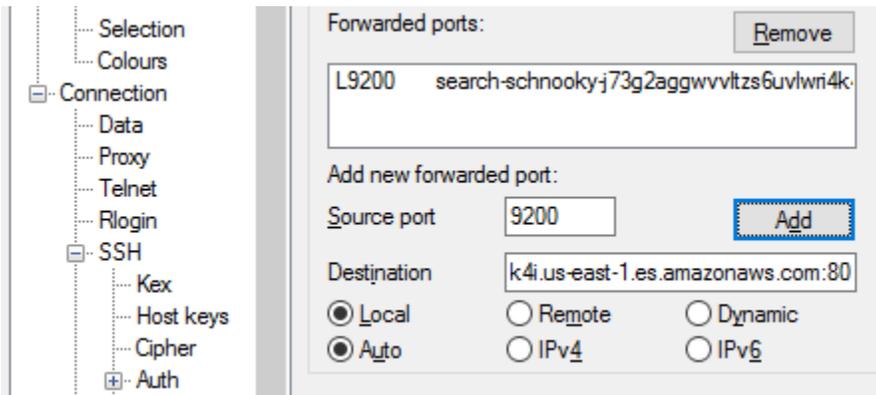
Destination: k4i.us-east-1.es.amazonaws.com:80

Local Remote Dynamic

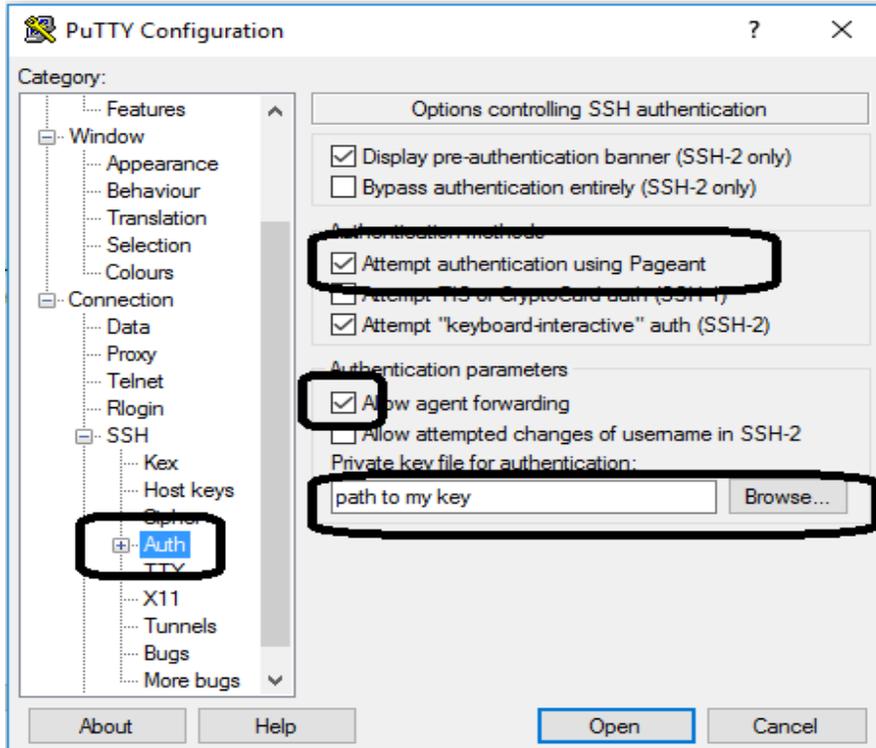
Auto IPv4 IPv6

[About] [Help] [Open] [Cancel]

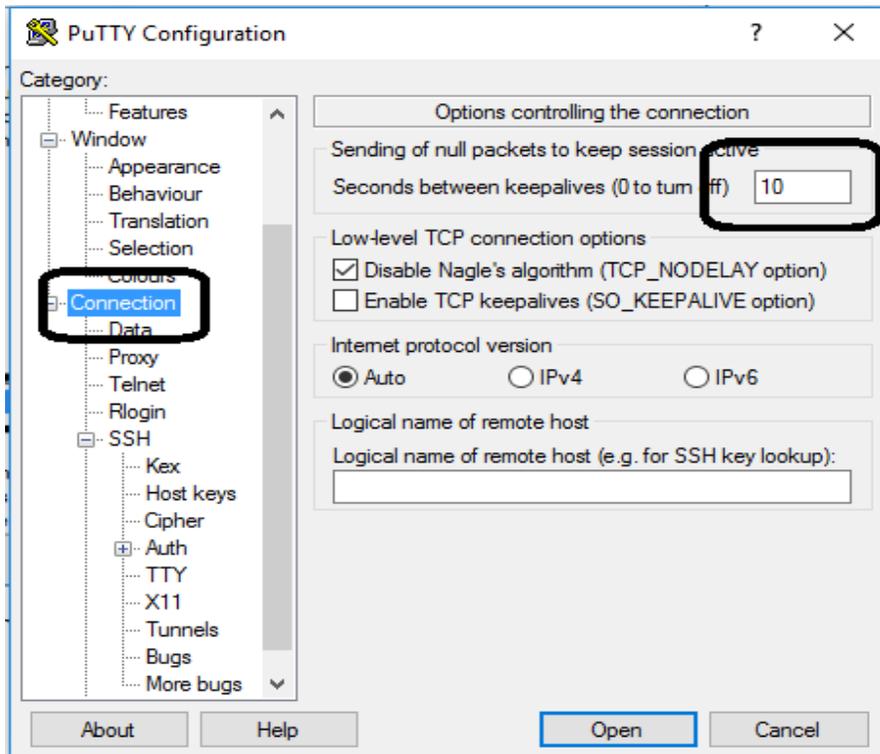
Click the Add button and you should now see something like pictured below:



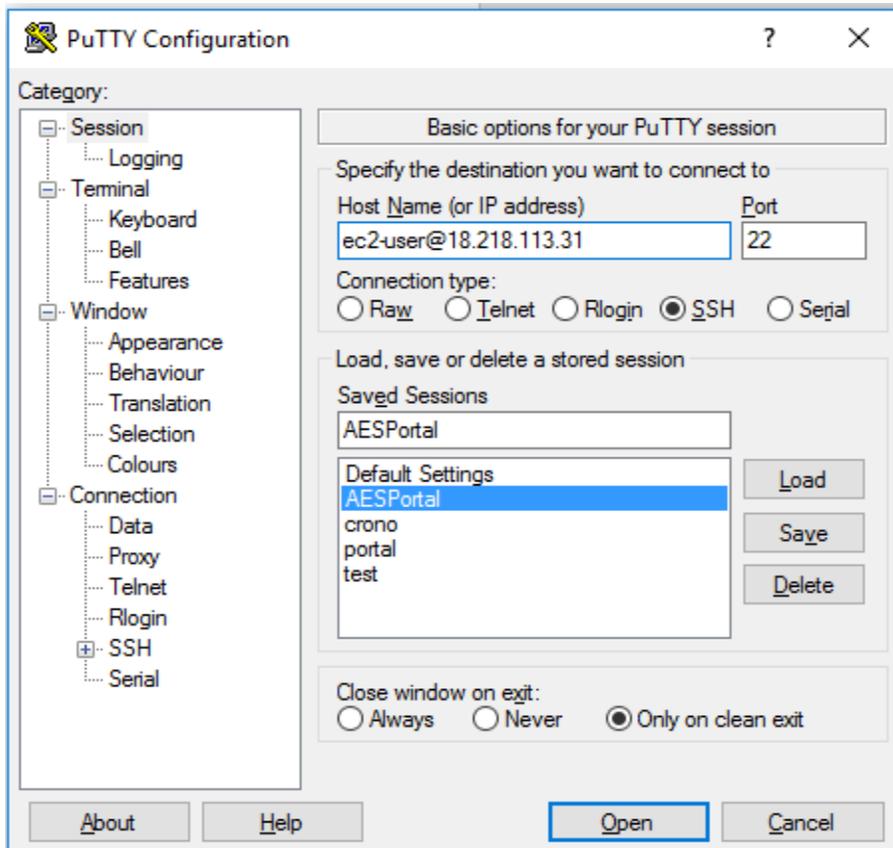
Navigate to the SSH section and add your key or if using pageant, allow agent forwarding:



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.



```
ec2-user@ip-10-20-1-101:~  
login as: ec2-user  
Authenticating with public key "imported-openssh-key" from agent  
Last login: Thu Nov  9 00:24:28 2017 from 72.21.196.64  
  
  _ | _ | _ )  
  _ | ( _ | /  Amazon Linux AMI  
  _ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/  
3 package(s) needed for security, out of 19 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-10-20-1-101 ~]$ █
```

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

