

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 (<u>http://www.putty.org/</u>). I also like to pull in <u>pageant</u> 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.

| CloudFormation Stacks | | | | | | |
|--|--|---|------------------|-----------------------|-------------------------|----------------------|
| Create Stack - Actions - | Design template | | | | | C \$ |
| Filter: Active - By Stack Name | | | | | | Showing 7 stacks |
| Stack Name | Created Time | S | itatus | Des | scription | |
| aes-redis-1MWC7XFUF7K65 NEST | ED 2018-02-14 15:10:47 U | TC-0500 C | REATE_COMPL | ETE AES | S Logging Solution - Re | edis Cluster. **Atte |
| aes-network-115 | JF7K65 2018-02-14 15:07:10 U | TC-0500 C | REATE_COMPL | ETE AES | S Logging Solution - Ba | seline Networking |
| aes | 2018-02-14 15:07:05 U | TC-0500 C | REATE_COMPL | ETE AES | S Logging Solution - Mo | other of all AES Lo |
| Overview Outputs Resources | Events Template Param | eters Tags | Stack Policy | Change Sets | Rollback Triggers | 880 |
| Кеу | Value | Desci | ription | | Export Name | * |
| ApplicationLoadBalancerURL | http://aes-a-Appli-1MEELJ3RGk 921829.us-east-2.elb.amazonav | E8O-679 /s.com | s URL of the App | olication ALB | aes-ApplicationLoa | dBalancerURL |
| LinuxAndMacPortForwardingCommand | ssh -i /path/to/your/key.pem -N - pc-labdomain-eyuuha4ardsfggfr 5me.us-east-2.es.amazonaws.c 2-user@18.218.113.31 | L 9200:v nr3gynnh pm:80 ec | and MAC Port Fe | orwarding SSH | aes-LinuxAndMacF nd | PortForwardingComma |
| ElasticsearchEndpointForPortForwarding | vpc-labdomain-eyuuha4ardsfggt h5me.us-east-2.es.amazonaws. | xc-labdomain-eyuuha4ardsfggfmr3gynn 5me.us-east-2.es.amazonaws.com:80 Elastic Search Endpoint for Port Forwa aes-ElasticsearchEndpointForPortFor | | EndpointForPortForwar | | |
| SSHKeyName | kevin | evin SSH Key Name. aes-SSHKeyName | | | | |
| ManagementPortalUserAndHostIP | ec2-user@18.218.113.31 | Mana | gement portal pu | blic IP address. | aes-ManagementP | ortalUserAndHostIP |

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).

| 🕵 PuTTY Configuration | | ? | \times |
|---|---|--|-----------|
| Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial | Basic options for your PuTTY ses Specify the destination you want to connect Host traine (or in address) ec2-user@18.218.113.31 connection type: O Raw Telnet O Raw Telnet Connection type: O Raw Telnet O Ray Telnet | sion t to <u>Port</u> 22 Sa <u>v</u> <u>D</u> ele san exit | eņal d |
| <u>A</u> bout <u>H</u> elp | <u>O</u> pen | <u>C</u> ano | el |

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 | | | | |
|--|--|--|---|--|
| Create Stack - Actions - D | Design template | | C \$ | |
| Filter: Active - By Stack Name | | | Showing 7 stacks | |
| Stack Name | Created Time | Status Desc | ription | |
| aes-redis-1MWC7XFUF7K65 NESTED | 2018-02-14 15:10:47 UTC-0500 | CREATE_COMPLETE AES I | Logging Solution - Redis Cluster. **Atte | |
| aes-network-115MRTKOWX NESTED | 2018-02-14 15:07:10 UTC-0500 | CREATE_COMPLETE AES I | Logging Solution - Baseline Networking | |
| ✓ aes | 2018-02-14 15:07:05 UTC-0500 | CREATE_COMPLETE AES I | Logging Solution - Mother of all AES Lo | |
| Overview Outputs Resources Ev | vents Template Parameters Ta | ags Stack Policy Change Sets | Rollback Triggers | |
| ApplicationLoadBalancerURL 9 | http://aes-a-Appli-1MEELJ3RGKE8O-679 921829.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:v oc-labdomain-eyuuha4ardsfggfmr3gynnh 5me.us-east-2.es.amazonaws.com:80 ec 2-user@18.218.113.31 | Linux and MAC Port Forwarding SSH | aes-LinuxAndMacPortForwardingComma nd | |
| ElasticsearchEndpointForPortForwarding | vpc-labdomain-eyuuha4ardsfggfmr3gynn h5me.us-east-2.es.amazonaws.com:80 | Elastic Search Endpoint for Port Forwa | aes-ElasticsearchEndpointForPortForwar ding | |
| SSHKeyName k | kevin SSH Key Name. aes-SSHKeyName | | aes-SSHKeyName | |
| ManagementPortalUserAndHostIP e | 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 Configurati | on | | | | ? | × |
|---|-------------------|--|--|-----------------------|--|----|
| Category: Features Window Appearance Behaviour | ^ | Option Port forwarding Local ports Remote port | s controlling SSH po accept connections | from oth | rding her hosts | |
| Translation Selection Colours Onnection Data Proxy Telnet Rlogin SSH Kex Host keys Cipher Auth TTY X11 Tunnels Bugs | | Add new forwa Source port Destination () Local () Auto | s: 9200 k4i.us-east-1.es O Remote O IPv <u>4</u> | amazor O D O IF | Remo Add aws.cor ynamic V <u>6</u> | ve |
| About | Ƴ <u>H</u> elp | | <u>O</u> pen | | <u>C</u> anc | el |

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

| Selection Colours | Forwarded ports | 3: | <u>R</u> emove |
|-----------------------------|-----------------|---------------------|---------------------|
| ⊡ ·· Connection ··· Data | L9200 sea | rcn-schnooky-j7.3g. | 2aggwvvitzs6uviwn4k |
| Telnet | Add new forwar | rded port: | |
| Rlogin | Source port | 9200 | Add |
| E- SSH | Destination | k4i.us-east-1.e | s.amazonaws.com:80 |
| Host keys | Local | ◯ Remote | O Dynamic |
| ···· Cipher ⊡·· Auth | ● Auto | ○ IPv <u>4</u> | ○ IPv <u>6</u> |

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

| 🕵 PuTTY Configurati | on | | ? | \times |
|------------------------------------|------|--|--------------------|----------|
| Category: | | | | |
| Features | ^ | Options controlling SSH authentic | ation | |
| Appearance Behaviour | | Display pre-authentication banner (SSH Bypass authentication entirely (SSH-2 of | H-2 only) only) | |
| ···· Translation ···· Selection | | | | |
| Colours | | Attempt authentication using Pageant | لي_ | |
| Data Proxy | | Attempt "keyboard-interactive" auth (S | SH-2) | |
| Rlogin | | Abw agent forwarding | in 994.2 | |
| ⊡ ·· SSH | | Private key file for authentication: | III 33H-2 | |
| Host keys | | path to my key | Browse | |
| Auth TTY | | | | |
| ···· X11 ···· Tunnels | | | | |
| ···· Bugs ···· More bugs | ~ | | | |
| About | Help | Open | Cance | I |

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

| 🕵 PuTTY Configuration | n | ? | × |
|---|--|---|-----|
| Category: Features Window Behaviour Translation | Options controlling th Sending of null packets to keep Seconds between keepalives (0 Low-level TCP connection option Disable Nagle's algorithm (TC Enable TCP keepalives (SO Internet protocol version | fe connection session ctive to tum ff) 10 ns CP_NODELAY option _KEEPALIVE option | |
| Proxy Telnet Rlogin SSH Kex Host keys Cipher Auth TTY X11 Tunnels Bugs Bugs | Auto IPv4 Logical name of remote host Logical name of remote host (e.g | O IPv6 | (qı |
| About | elp Ope | en Cance | el |

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

| 🕵 PuTTY Configuration | | ? | × |
|--|--|---|-----|
| Category: | | | |
| Session Logging Logging Logging Logging Logging Logging Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial | Basic options for your PuTTY set Specify the destination you want to conner Host Name (or IP address) ec2-user@18.218.113.31 Connection type: O Raw O Telnet O Raw O Telnet Nave or delete a stored session Saved Sessions AESPortal Default Settings AESPortal crono portal test Close window on exit: O Always Never O Only on close | ssion ct to Port 22 C Ser Load Save Delete | jal |
| <u>A</u> bout <u>H</u> elp | <u>O</u> pen | <u>C</u> ance | 1 |



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

| | Chrome Web Store - † 🗙 | 😌 - 🗆 X 👘 Stack Detail X 🔀 Kibana X |
|------|------------------------|---|
| ← - | C 🛈 localhost: | 9200/_plugin/kibana/app/kibana#/discover?_g=()&_a=(columns:!(_source),index:'lo 🛧 🔤 🔽 💿 📎 📀 |
| 🔛 Ap | ops 📙 WA 📙 Trave | el 🦲 Cassandra 📙 Hiring & Support 📙 Lambda 🔜 Data & Analytics 📃 Parquet 📙 Database 🛛 🛸 |
| | kibana | 58 hits New Save Open Share Isometry Isometry |
| | KIDalla | Search (e.g. status:200 AND extension:PHP) Uses lucene query syntax Q |
| Ø | Discover | Add a filter 🕂 |
| Ш | | logstash-* |
| © | Dashboard | Selected Fields |
| 8 | Timelion | ? _source |
| يو | Dev Tools | Available Fields |
| \$ | Management | November 8th 2017, 20:41:50.798 - November 8th 2017, 20:56:50.798 - Auto |
| 0 | Collapse | 2- 1.5- tig 0.5- 0.5- |