

Screenshots

→ Configuring VPN tunnel and testing on GCP and AWS

Filter by tags and attributes or search by keyword							1 to 1 of 1	
Name	VPN ID	State	Virtual Private Gateway	Customer Gateway	Customer Gateway Ad			
aws-gcp-vpn	vpn-43f11556	available	vpgw-ec2387f2 aws-vpg	cgw-0d973013 to-gcp-gateway	35.197.18.50			

VPN Connection: vpn-43f11556

Details Tunnel Details Static Routes Tags

1 to 2 of 2				
Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details
34.208.155.47	169.254.12.196/30	UP	March 11, 2018 at 2:37:28 PM UTC-7	-
35.166.227.20	169.254.12.208/30	UP	March 11, 2018 at 2:38:49 PM UTC-7	-

Tunnels

Add VPN tunnel Delete

Filter by VPN tunnel properties Columns

Tunnel name	Status	Routing type	Peer IP address	
aws-gcp-vpn-tunnel-1	Established	Policy-based	34.208.155.47	
aws-gcp-vpn-tunnel-2	Established	Policy-based	35.166.227.20	

2018-03-15 15:16:04.925 PDT	sending packet: from 35.197.18.50[4500] to 35.166.227.20[4500] (92 bytes)
2018-03-15 15:16:11.149 PDT	received packet: from 34.208.155.47[4500] to 35.197.18.50[4500] (92 bytes)
2018-03-15 15:16:11.149 PDT	parsed INFORMATIONAL_V1 request 4184034875 [HASH N(DPD)]
2018-03-15 15:16:11.149 PDT	generating INFORMATIONAL_V1 request 115413418 [HASH N(DPD_ACK)]
2018-03-15 15:16:11.150 PDT	sending packet: from 35.197.18.50[4500] to 34.208.155.47[4500] (92 bytes)
2018-03-15 15:16:14.950 PDT	received packet: from 35.166.227.20[4500] to 35.197.18.50[4500] (92 bytes)
2018-03-15 15:16:14.950 PDT	parsed INFORMATIONAL_V1 request 4232024560 [HASH N(DPD)]
2018-03-15 15:16:14.951 PDT	generating INFORMATIONAL_V1 request 4022198291 [HASH N(DPD_ACK)]
2018-03-15 15:16:14.951 PDT	sending packet: from 35.197.18.50[4500] to 35.166.227.20[4500] (92 bytes)
2018-03-15 15:16:21.182 PDT	received packet: from 34.208.155.47[4500] to 35.197.18.50[4500] (92 bytes)
2018-03-15 15:16:21.183 PDT	parsed INFORMATIONAL_V1 request 762333660 [HASH N(DPD)]
2018-03-15 15:16:21.183 PDT	generating INFORMATIONAL_V1 request 3827310083 [HASH N(DPD_ACK)]
2018-03-15 15:16:21.183 PDT	sending packet: from 35.197.18.50[4500] to 34.208.155.47[4500] (92 bytes)
2018-03-15 15:16:24.897 PDT	sending DPD request
2018-03-15 15:16:24.897 PDT	generating INFORMATIONAL_V1 request 1682613584 [HASH N(DPD)]
2018-03-15 15:16:24.898 PDT	sending packet: from 35.197.18.50[4500] to 35.166.227.20[4500] (92 bytes)
2018-03-15 15:16:24.912 PDT	received packet: from 35.166.227.20[4500] to 35.197.18.50[4500] (92 bytes)
2018-03-15 15:16:24.913 PDT	parsed INFORMATIONAL_V1 request 3188976794 [HASH N(DPD_ACK)]

→ Testing the Vpn tunnel

```
kaizercharania_ck@instance-1:/$ ping 172.31.19.173
PING 172.31.19.173 (172.31.19.173) 56(84) bytes of data.
64 bytes from 172.31.19.173: icmp_seq=1 ttl=64 time=14.4 ms
64 bytes from 172.31.19.173: icmp_seq=2 ttl=64 time=14.3 ms
64 bytes from 172.31.19.173: icmp_seq=3 ttl=64 time=14.3 ms
64 bytes from 172.31.19.173: icmp_seq=4 ttl=64 time=14.4 ms
64 bytes from 172.31.19.173: icmp_seq=5 ttl=64 time=14.4 ms
64 bytes from 172.31.19.173: icmp_seq=6 ttl=64 time=14.4 ms
^C
--- 172.31.19.173 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 14.340/14.428/14.487/0.088 ms
kaizercharania_ck@instance-1:/$
```

```
kaizercharania_ck@instance-1:/$ ping 172.31.16.143
PING 172.31.16.143 (172.31.16.143) 56(84) bytes of data.
64 bytes from 172.31.16.143: icmp_seq=1 ttl=254 time=16.4 ms
64 bytes from 172.31.16.143: icmp_seq=2 ttl=254 time=15.3 ms
64 bytes from 172.31.16.143: icmp_seq=3 ttl=254 time=15.2 ms
64 bytes from 172.31.16.143: icmp_seq=4 ttl=254 time=15.2 ms
^C
--- 172.31.16.143 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 15.206/15.580/16.459/0.526 ms
kaizercharania_ck@instance-1:/$
```

```
[ubuntu@ip-172-31-19-173:~$ ping 10.138.0.2
PING 10.138.0.2 (10.138.0.2) 56(84) bytes of data.
64 bytes from 10.138.0.2: icmp_seq=1 ttl=64 time=15.4 ms
64 bytes from 10.138.0.2: icmp_seq=2 ttl=64 time=14.4 ms
64 bytes from 10.138.0.2: icmp_seq=3 ttl=64 time=14.2 ms
64 bytes from 10.138.0.2: icmp_seq=4 ttl=64 time=14.2 ms
^C
--- 10.138.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 14.244/14.616/15.450/0.496 ms
ubuntu@ip-172-31-19-173:~$
```

```
[ec2-user@ip-172-31-16-143 /]$ ping 10.138.0.2
PING 10.138.0.2 (10.138.0.2) 56(84) bytes of data.
64 bytes from 10.138.0.2: icmp_seq=1 ttl=64 time=15.3 ms
64 bytes from 10.138.0.2: icmp_seq=2 ttl=64 time=14.6 ms
64 bytes from 10.138.0.2: icmp_seq=3 ttl=64 time=14.5 ms
64 bytes from 10.138.0.2: icmp_seq=4 ttl=64 time=14.5 ms
64 bytes from 10.138.0.2: icmp_seq=5 ttl=64 time=14.5 ms
^C
--- 10.138.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 14.503/14.732/15.394/0.358 ms
[ec2-user@ip-172-31-16-143 /]$
```

→ Load Balancer Registered Instances

Registered targets

IP address	Port	Availability Zone	Status
10.138.0.2	80	all	healthy ⓘ
172.31.16.143	80	us-west-2b	healthy ⓘ
172.31.19.173	80	us-west-2b	healthy ⓘ

Availability Zones

Availability Zone	Target count	Healthy?
us-west-2b	2	Yes
all	1	Yes

→ Creating Policies for web app and Load Balancer Log files

Policies
Identity providers
Account settings
Credential report
Encryption keys

Access keys (access key ID and secret access key)

You use access keys to sign programmatic requests to AWS services. To learn how to sign requests using your access keys, see the [signing documentation](#). For your protection, store your access keys securely and do not share them. In addition, AWS recommends that you rotate your access keys every 90 days.

Note: You can have a maximum of two access keys (active or inactive) at a time.

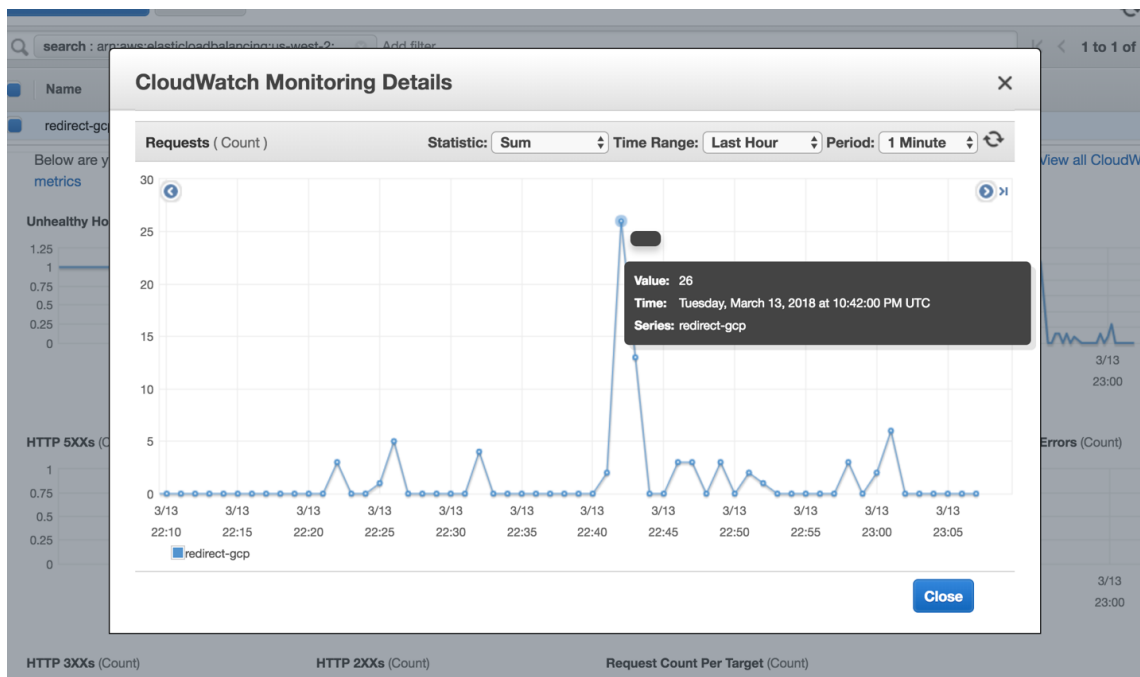
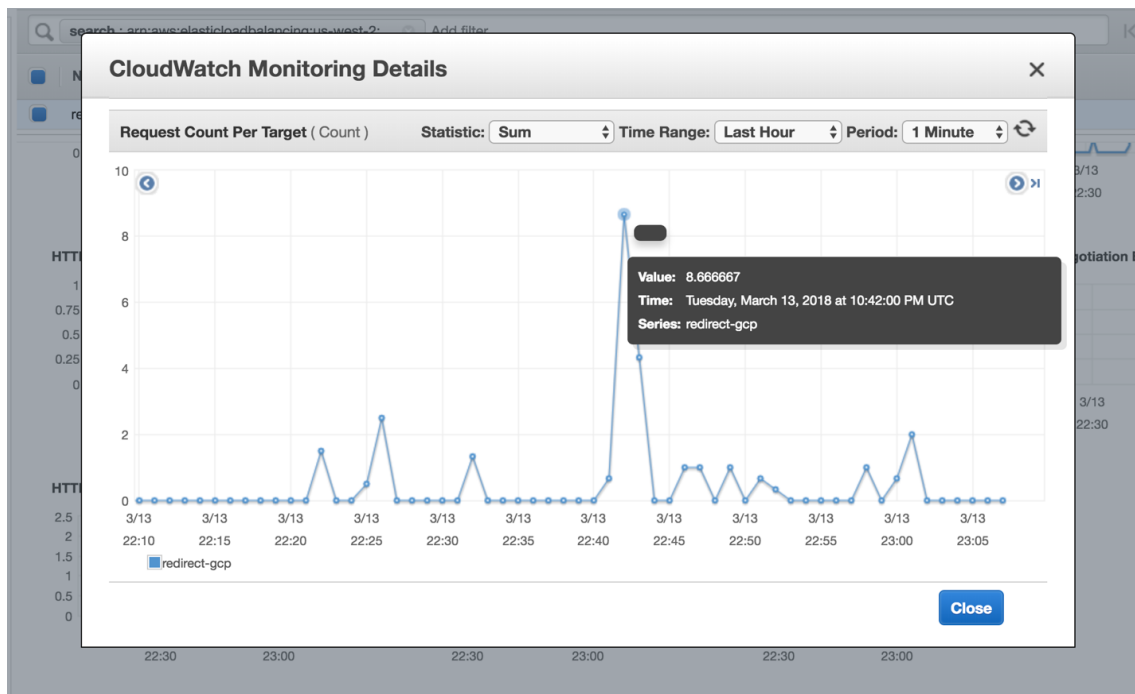
Created	Deleted	Access Key ID	Last Used	Last Used Region	Last Used Service	Status	Actions
Feb 15th 2018		AKIAJBAPAMRDGSRXKFKFA	2018-02-15 18:30 PDT	us-west-2	iotanalytics	Active	Make Inactive Delete
Mar 12th 2018		AKIAJCPKFITNYBWIAMDQ	2018-03-12 23:14 PDT	us-west-2	s3	Active	Make Inactive Delete
Mar 11th 2018	Mar 12th 2018	AKIAJCLYXOA7UKPJC33A	N/A	N/A	N/A	Deleted	
Mar 11th 2018	Mar 11th 2018	AKIAI4CR5ETLJWSSJ2KQ	N/A	N/A	N/A	Deleted	

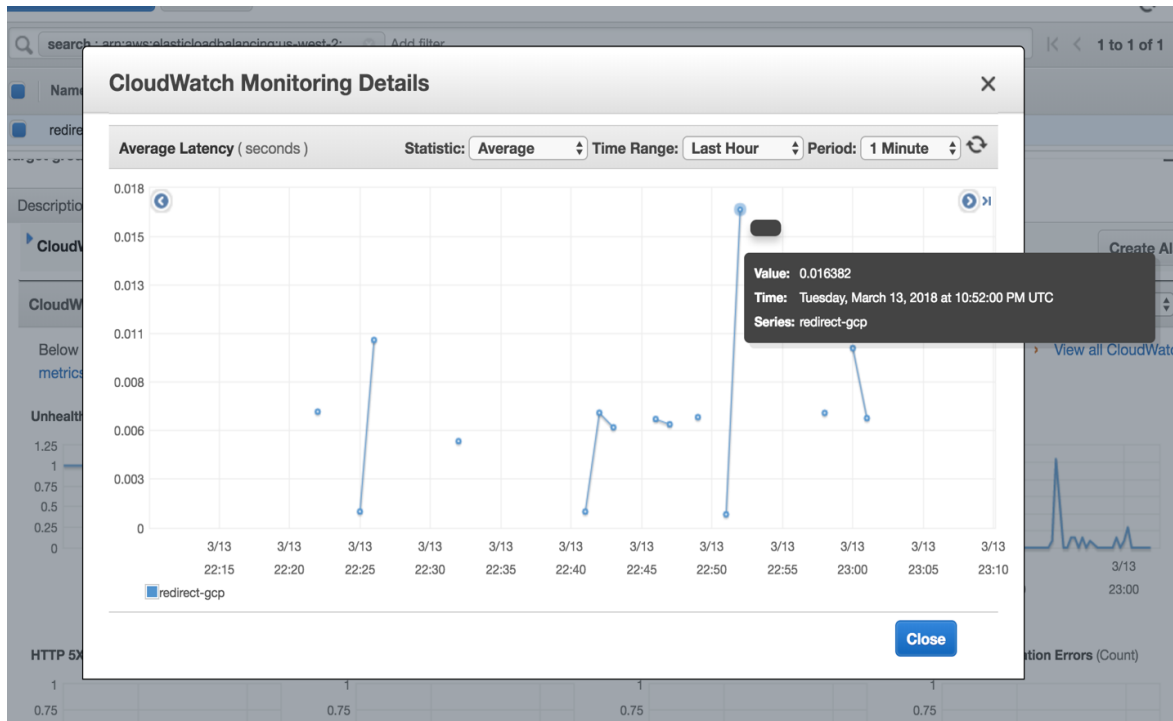
[Create New Access Key](#)

Important Change - Managing Your AWS Secret Access Keys
As described in a [previous announcement](#), you cannot retrieve the existing secret access keys for your AWS root account, though you can still create a new root access key at any time. As a [best practice](#), we recommend [creating an IAM user](#) that has access keys rather than relying on root access keys.

+ CloudFront key pairs
+ X.509 certificate

→ Testing the Load Balancer and Verifying it using Log Files





```
http 2018-03-13T22:32:23.286758Z app/aws-gcp-loadbalancer/b82d0c3b705f3022 129.210.115.112:1182 172.31.19.173:80 0.001 0.001 0.000 200 200 559 1593 "GET http://aws-gcp-loadbalancer-1503451061.us-west-2.elb.amazonaws.com:80/ HTTP/1.1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.186 Safari/537.36" - - arn:aws:elasticloadbalancing:us-west-2:629762831643:targetgroup/redirect-gcp/abbd3608f9d976a0 "Root=1-5aa85177-d0cd70bd8c5ee7c381429722" "-" "-" 0
http 2018-03-13T22:32:25.848290Z app/aws-gcp-loadbalancer/b82d0c3b705f3022 129.210.115.112:1182 172.31.16.143:80 0.001 0.001 0.000 200 200 559 3116 "GET http://aws-gcp-loadbalancer-1503451061.us-west-2.elb.amazonaws.com:80/ HTTP/1.1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.186 Safari/537.36" - - arn:aws:elasticloadbalancing:us-west-2:629762831643:targetgroup/redirect-gcp/abbd3608f9d976a0 "Root=1-5aa85179-0c37c7111762e8fc5aff9f41" "-" "-" 0
http 2018-03-13T22:32:26.482243Z app/aws-gcp-loadbalancer/b82d0c3b705f3022 129.210.115.112:1182 10.138.0.2:80 0.015 0.015 0.000 200 200 554 1682 "GET http://aws-gcp-loadbalancer-1503451061.us-west-2.elb.amazonaws.com:80/ HTTP/1.1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.186 Safari/537.36" - - arn:aws:elasticloadbalancing:us-west-2:629762831643:targetgroup/redirect-gcp/abbd3608f9d976a0 "Root=1-5aa8517c-d0c71b59cc872e32c9efaa61" "-" "-" 0
http 2018-03-13T22:32:48.491323Z app/aws-gcp-loadbalancer/b82d0c3b705f3022 129.210.115.112:1182 172.31.19.173:80 0.001 0.001 0.000 200 200 559 1593 "GET http://aws-gcp-loadbalancer-1503451061.us-west-2.elb.amazonaws.com:80/ HTTP/1.1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.186 Safari/537.36" - - arn:aws:elasticloadbalancing:us-west-2:629762831643:targetgroup/redirect-gcp/abbd3608f9d976a0 "Root=1-5aa85190-33b977a9d4ac9e14959b89f0" "-" "-" 0
```