VPC Monitoring with Flow Logs

mmoorejr24@gmail.com

Logs ((10)								Ì	Export results	▼ Add to a	fashboard	0
Logs ((10)								[Export results	▼ Add to a	lashboard	0
Logs ((10)				Sh 762 records (10)	owing 10 of 753 res	cords matched ()	(67.8 kB/s)	[Export results	Add to a	lashboard Hide histo	© 97277
Logs ((10)				Sh 762 records (10)	iowing 10 of 753 red 5.6 kB) scanned in 1	cords matched () .6s @ 488 records/s (t	(67.8 kB/s)	[Export results	▼ Add to c	lashboard	© gram
20 15 10 5	(10)	Th	1	. ادار	Sh 762 records (10	iowing 10 of 753 res	cords matched @ .6s @ 488 records/s (((67.8 kB/s)) anth I	Export results	Add to c	fashboard //	© 97271
20 15 10 5 0	(10)	01:55	D DOLLA D2AM		5h 762 records (107 02 10	rowing 10 of 753 res 5.6 kB) scanned in 1 00 02 15	cords matched @ .fs @ 488 records/s (r l l	(67.8 kB/s) 02.25	(Export results	Add to c Add to c 0240	fashboard Hide histo	© 90am
Logs ((10)	01:55	02 AM bytestransferred	02.05	Sh 762 records (107 02 10	owing 10 of 753 re 5.6 kB) scanned in 1 02.15	cords matched O .6s @ 488 records/s (r 0 02 20	(67.8 kB/s) 02.25	(Export results	 Add to c Add to c Add to c 	Tashboard Hide histo 02:45	© 9000
Logs ((10) 01:50 src&ddr	01:55 dstAdr 18.1.6.138	U2 AM U2 AM LyttesTransferred	02:05	5 762 records (107 02:10	owing 10 of 753 re 5.6 kB) scanned in 1 	tords matched .6s @ 488 records/s (r .02.20	(67.8 kB/s) 00:25	02:30	Export results	Add to a	fashboard Hide histo 02:45	© 90271
Logs (20 15 15 0 ■ ■ 1 2	(10) 01:50 src&ddr 13.52.6.116 10.16.138	01:55 dstAddr 10:1:6:138 13:52:6:116	UZAM bytesTransferred 14696 12956	02:05	50 762 records (107 02:10	wing 10 of 753 res 5.6 kB) scanned in 1 02.15	cords matched @ .ss @ 488 records/s (r 02.20	(67.8 kB/s) 02.25) 	Export results	Add to c	tashboard Hide histo 02.45	© 902m
Logs (20 15 10 5 0 	(10) 01:50 src&dor 13.52.6.116 10.1.6.138 52.119.176.1.	01.55 dstAddr 10.1.6.138 13.52.6.116 - 10.1.6.138	02AM bytesTransferred 14696 12956 7262	02:05	Sh 762 records (107 02:10	rowing 10 of 753 re- 5.6 kB) scanned in 1 02.15	cords matched @ .5e @ 488 records/s (r 	(67.8 kB/s) 02.25	(Export results	 Add to c Add to c 02.40 	Jashboard Hide histo	© yaan
Logs (20 15 0,-	10) 1100 1100 1100 1100 1100 1100 1100 1100 1100 1100 1100 1	01.55 dstAddr 18.1.6.138 13.52.6.116 19.1.6.138	02AM bytestransferred 14696 12956 7161 7161	1	5h 762 records (10) 02:10	iowing 10 of 753 re 5.6 kB) scanned in 1 	cords matched .6s @ 488 records/s (i 02.20	678 kB/s) 678 kB/s) 0225	(Export results	 Add to c Add to c 02.40 	Iashboard Hide histo 02.45	© gan
Logs (20 15 10 5 0 - 1 1 2 3 4 5 5	10) 0150 0150 0150 0150 016.138 01.6.138 02.119.176.1 02.119.109.1 02.16.138	01:55 dstAddr 10.1.6.138 10.1.6.138 10.1.6.138 10.1.6.138 52.119.180	02 AM bytestransferred 14696 13966 7362 7316 3766	I	51 762 records (10 10 02:10	oving 10 of 755 re 5.6 kBj scanned in 1 ad 1 a a Q2 15	cordi matched 	167.8 kB/s) 02.25	(Export results	Add to a	lashboard Hide hate 02.45	© Statu
Logs (20 15 10 0 	110) 0150 0150 0150 0150 0150 0150 0150	01:55 dstAddr 10:1:6:138 33.52:6:116 10:1:6:138 10:1:6:138 20:119:176 52:119:176	02 AM bytestraesferred 14666 12066 7162 7162 7162 7162 7162 7162 7162 71	1 	Sh 762 records (107 0 210	coving 10 of 753 ref 56 kB) scanned in 1 add 0 a a a a a a a a a a a a a a a a a	cords matched .6a @ 488 records/s (r .0a .2a .0a .2a	67.8 kB/4) 02.25	(Export results	Add to o	lashboard Hide hite 02.45	© gram
Logs (20 15 10 5 0 7	10) 0150 srcker 1.5.2.4.136 0.1.6.138 12.119.126.1 22.119.126.1 23.14.14.138 10.1.6.138	01:55 dstAddr 10.1.6.138 10.1.6.138 10.1.6.138 20.116.138 52.119.180 52.119.180 10.2.8.174	02/48 bytestransferred 346/6 12956 7142 716 2396 2396 2396	02.05	51 762 records (10 02 10	ioxing 10 of 755 re 56 kB) scenned in 1 all 0 a a a a 02.15	cords matched () for () 458 records () () 1 1 2 2 2 458 records () () 0 2 30	67.8 kB/s) 02.25	02.30	Export results	Add to a	Ashboard Hide hist	© 902m
Logs (20 15 10 6 0 7 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8	10) 0150 src6867 13.52.6.136 19.1.6.138 19.1.6.138 19.1.6.138 19.1.6.138 19.1.6.138	01:55 dstAddr 10:1.6.138 3.52.6.136 10:1.6.138 20:1.9.16.138 52:119.176 10:2.8.174 10:1.6.38	22AA 22AA botestressferred 14666 7142 7158 7158 7158 7158 7158 7158 7158 7158	02.05	50 762 records (10 02 10	oving 10 of 753 res 5 6 kB scanned in 1 02 15	cords matched () 	67.8 kB/a) 02.25	02.30	Export results	 Add to a Add to a 02.49 	lashboard Hise hists 02.45	© 9247
Logs (20 15 5 0 - - - - - - - - - - - - - - - - -	10) 0150 0150 0150 0150 0150 0150 0150 0	01.55 dstAddr 10.1.6.138 13.525.4.116 10.1.6.138 52.119.180 52.119.178 10.1.6.138 9 10.1.6.138	02.04 02.04 09.04 1966 1966 1966 1966 1966	1 .11 .1	5h 762 records (10 a 1 b 1 b 62:10	owing 10 of 753 re 56 KB) scanned in 1 add 1 au	cords matched 0 . 6. g = 468 months () 1 1 2	67.8 kB/s) 02.25	(Export results	Add to e	Iashboard Mile hint 02.45	© gram



Introducing Today's Project!

What is Amazon VPC?

AWS VPC is a virtual network dedicated to your AWS account, allowing you to provision and manage a logically isolated section of the AWS cloud where you can launch AWS resources.

How I used Amazon VPC in this project

I used two Amazon VPCs for peer connecting to monitor logs using the CloudWatch service.

One thing I didn't expect in this project was...

I didn't expect this project to be so awesome.

This project took me...

This project took me about two hours and forty minutes to complete.



In the first part of my project...

Step 1 - Set up VPCs

In this step we will set up two VPCs from scratch in minutes. Network monitoring can still be done with just a single VPC, but it's great to have the extra challenge and tackle VPC peering in this project too!

Step 2 - Launch EC2 instances

In this step, we launch two EC2 instances - one in each VPC. Doing this is important to set up the remainder of our project. Our EC2 instances will generate traffic that the VPC Flow Logs with monitor.

Step 3 - Set up Logs

In this step, we are setting up VPC flow logs to start monitoring network traffic. We are also setting up a storage space for our flow logs.

Step 4 - Set IAM permissions for Logs

In this step, we provide VPC Flow Logs with the permission to create logs and upload them into our log group in CloudWatch.



Multi-VPC Architecture

I started my project by launching two VPCs! We created two public subnets (i.e. one public subnet in each VPC) with no private subnets.

The CIDR blocks for VPCs 1 and 2 are 10.1.0.0/16 and 10.2.0.0/16. They have to be unique because having overlapping CIDR blocks will cause network/routing traffic issues down the line when traffic is needing to go from one VPC to another.

I also launched EC2 instances in each subnet

My EC2 instances' security groups allow SSH and ICMP type traffic. This is because EC2 Instance Connect will need to access our EC2 instance using SSH-type traffic, and because we need to allow ICMP type traffic for connectivity tests later.



Logs

Logs are like diary entries for my computer systems - they are detailed records of any kind of activity related to the traffic/resource/AWS service that the log is tracking.

Log groups are groupings of logs i.e. logs that belong to the project/application/source are often in a log group together!

I also set up a flow log for VPC 1

Flow logs (1) Info Create flow log Q. Search < 1 > ③ Name V Flow log ID V Filter V Destination name V IAM role ARN V NextWorkVPCFlowLog fi-0286dc57ra37abecd9 ALL cloud-watch-logs NextWorkVPCFlowLogsGroup [2] annawsiam:088535984191:role/Next
Name V Flow log ID V Filter V Destination type V Destination name V IAM role ARN V NextWorkVPCFlowLog ft-0286dc57a37abccd9 ALL cloud-watch-logs NextWorkVPCFlowLogsGroup I2 amaxisiam:088535984191zrole/Next



IAM Policy and Roles

I created an IAM policy so that I can define a rule that allows policy holders e.g. our VPC Flow Logs service the ability to create log streams and upload them into CloudWatch.

I also created an IAM role because services like VPC Flow Logs have to be associated with a role instead of JSON! Creating an IAM role will be necessary to give our VPC Logs the access it needs to record and upload logs.

A custom trust policy is specific type of policy! They're different from IAM policies. While IAM policies help you define the actions a user/service can or cannot do, custom trust policies are used to very narrowly define who can use a role.





In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step, I am generating network traffic! This becomes important when we are communicating to cloudworks/cloud networking/or cloud engineering.

Step 6 - Set up a peering connection

In this step, we are setting up a peering connection so that VPCs 1 and 2 can talk directly with each other.

Step 7 - Update VPC route tables

In this step, we are updating the route tables for our two VPCs so that traffic bound for the other VPC can be directed to the peering connection instead of the public internet.

Step 8 - Analyze flow logs

In this step, we are tracking the network data that's been collected on our VPCs, and then analyze that data to extract insights.



Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means ICMP traffic could be blocked by security group/network ACLs; or maybe our traffic is being routed to a wrong path.

· #_	
~_ #### <u>_</u> ~~ _#####\	Amazon Linux 2023
~~ \### ~~ \#/ ~~ \\#/	https://aws.amazon.com/linux/amazon-linux-2023
~~~~ / / //	
ec2-user@ip-10-1-6-	-138 ~]\$ ping 10.2.8.174
C 10.2.8.174 (10.	.2.8.1/4) 56(64) bytes of data.
10.2.8.174 ping	statistics
./ packets transmitt	-
ec2-user@ip-10-1-6-	-138 ~]\$

I could receive ping replies if I ran the ping test using the other instance's public IP address, which means our second instance is actually allowing ICMP traffic.



## **Connectivity troubleshooting**

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because we do not have a route in our VPCs' route tables that directs traffic from one VPC to another.

## To solve this, I set up a peering connection between my VPCs

I also updated both VPCs' route tables so that traffic from one of the VPCs and heading to the other VPC's private IPV4 address can be directed to go through the peer connection instead of the public internet.

VPC > Route tables > rtb-0b45d7d3d1a3ba7	15				
rtb-0b45d7d3d1a3ba715	5 / NextWork-2-rtb-public				Actions 🔻
Details Info					
Route table ID rtb-0b45d7d3d1a3ba715 VPC vpc-0089b29b638773fd0   NextWork-2-vpc	Main		Explicit subnet associations subnet-009eeabb3f56ee9f7 / NextWork-2-subnet- public1-us-west-1a	Edge associations -	
Routes Subnet associations Edge a	associations Route propagation Tags				
Routes (3)					Both V Edit routes
Q. Filter routes		1			< 1 > @
Destination	▼ Target	~	Status		~
0.0.0.0/0	igw-0b8d9ccaa3134a39f		⊘ Active	No	
10.1.0.0/16	pcx-0a8b8b25ffc1785a0		⊘ Active	No	
10.2.0.0/16	local		⊘ Active	No	



## **Connectivity troubleshooting**

I received ping replies from Instance 2's private IP address! This means setting up the peering connection and then the route table solve the connectivity error of our VPCs' traffic not being able to navigate from one VPC to another.

<pre>44 bytes from 3.101.190.41: icmp_seq=4 ttl=126 time=0.911 ms 54 bytes from 3.101.190.41: icmp_seq=5 ttl=126 time=1.23 ms 55 67</pre>		
<pre>44 bytes from 3.101.190.41: icmp_seq=4 ttl=126 time=0.911 ms 44 bytes from 3.101.190.41: icmp_seq=5 ttl=126 time=0.741 ms 44 bytes from 3.101.190.41: icmp_seq=6 ttl=126 time=0.741 ms 45 bytes from 3.101.190.41: icmp_seq=6 ttl=126 time=1.23 ms 45 bytes from 10.2.0.174: icmp_seq=1 ttl=127 time=1.41 ms 46 bytes from 10.2.0.174: icmp_seq=2 ttl=127 time=1.41 ms 46 bytes from 10.2.0.174: icmp_seq=2 ttl=127 time=1.41 ms 46 bytes from 10.2.0.174: icmp_seq=6 ttl=127 time=0.915 ms 46 bytes from 10.2.0.174: icmp_seq=6 ttl=127 time=0.915 ms 46 bytes from 10.2.0.174: icmp_seq=1 ttl=127 time=0.915 ms 46 bytes from 10.2.0.174: icmp_seq=2 ttl=127 time=0.915 ms 46 bytes from 10.2.0.174: icmp_seq=6 ttl=127 time=0.916 ms 46 bytes from 10.2.0.174: icmp_seq=6 ttl=127 time=0.917 ms 46 bytes from 10.2.0.174: icmp_seq=6 ttl=127 time=0.937 ms 46 bytes from 10.2.0.174: icmp_seq=1 ttl=127 time=0.730 ms 46 bytes from 10.2.0.174: icmp_seq=1 ttl=127 time=0.740 ms 46 bytes from 10.2.0.174: icmp_seq=1 ttl=127 time=0.740 ms 46 bytes from 10.2.0.174: icmp_seq=1 ttl=127 time=0.637 ms 46 bytes from 10.2.0.174: icmp_seq=1 ttl=127 time=0.640 ms 46 bytes from 10.2.0.174: icmp_seq=1 ttl=127 time=0.640 ms 46 bytes from 10.2.0.174: icmp_seq=1 ttl=127 time=0.640 ms 46 bytes from 10.2.0.174: icmp_seq=1 ttl=127 time=0.641 ms 46 bytes from 10.2.0.174: icmp_seq=2 ttl=127 time=0.641 ms 46 bytes from 10.2.0.174: icmp_seq=2 ttl=127 time=0.641 ms 46 bytes from 10.2.0.174: icmp_seq=1 ttl=127 time=0.641 ms 46 bytes from 10.2.0.174: icmp_seq=2 ttl=127 time=0.671 ms 46 bytes from 10.2.0.174: icmp_</pre>		
<pre>44 bytes from 3.101.190.41: icmp_seq=4 ttl=126 time=0.911 ms 64 bytes from 3.101.190.41: icmp_seq=5 ttl=126 time=0.741 ms 64 bytes from 3.101.190.41: icmp_seq=6 ttl=126 time=1.23 ms 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7</pre>		
<pre>54 bytes from 3.101.190.41: icmp_seq=4 ttl=126 time=0.911 ms 54 bytes from 3.101.190.41: icmp_seq=5 ttl=126 time=0.741 ms 54 bytes from 3.101.190.41: icmp_seq=6 ttl=126 time=1.23 ms 7c</pre>		
<pre>54 bytes from 3.101.190.41: icmp_seq=4 ttl=126 time=0.911 ms 54 bytes from 3.101.190.41: icmp_seq=5 ttl=126 time=0.741 ms 54 bytes from 3.101.190.41: icmp_seq=5 ttl=126 time=1.23 ms 55 55 55 55 55 55 55 55 55 55 55 55 55</pre>		
<pre>S4 bytes from 3.101.190.41: icmp_seq=4 ttl=126 time=0.911 ms 64 bytes from 3.101.190.41: icmp_seq=5 ttl=126 time=0.741 ms 64 bytes from 3.101.190.41: icmp_seq=6 ttl=126 time=1.23 ms 75 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7</pre>		
<pre>54 bytes from 3.101.190.41: icmp_seq=4 ttl=126 time=0.911 ms 54 bytes from 3.101.190.41: icmp_seq=5 ttl=126 time=0.741 ms 54 bytes from 3.101.190.41: icmp_seq=6 ttl=126 time=1.23 ms 'C ' 3.101.190.41 ping statistics 6 packets transmitted, 6 received, 0% packet loss, time 5192ms ttt min/avg/max/mdev = 0.461/0.821/1.226/0.244 ms [ec2-used]p=10-1-6-138 -3p ping 10.2.8.174 FING 10.2.8.174 (10.2.8.174) 56(84) bytes of data. 64 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=1.41 ms 54 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=0.915 ms 54 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=0.915 ms 54 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=0.567 ms 54 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=0.685 ms 54 bytes from 10.2.8.174: icmp_seq=8 ttl=127 time=0.685 ms 54 bytes from 10.2.8.174: icmp_seq=3 ttl=127 time=0.740 ms 54 bytes from 10.2.8.174: icmp_seq=3 ttl=127 time=0.730 ms 54 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.730 ms 54 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.695 ms 54 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.698 ms 54 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.698 ms 54 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.617 ms 54 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.637 ms 54 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.618 ms 55 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.618 ms 56 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.618 ms 56 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.618 ms 56 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.618 ms 57 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.618 ms 56 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.618 ms 57 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.618 ms 56 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.618 ms</pre>		
<pre>54 bytes from 3.101.190.41: icmp_seq=4 ttl=126 time=0.911 ms 54 bytes from 3.101.190.41: icmp_seq=5 ttl=126 time=0.741 ms 56 bytes from 3.101.190.41: icmp_seq=6 ttl=126 time=1.23 ms 57 57 57 57 57 57 57 57 57 57 57 57 57</pre>		
<pre>64 bytes from 3.101.190.41: icmp_seq=4 ttl=126 time=0.911 ms 64 bytes from 3.101.190.41: icmp_seq=5 ttl=126 time=0.741 ms 54 bytes from 3.101.190.41: icmp_seq=6 ttl=126 time=1.23 ms 72 73.101.190.41 ping statistics 6 packets transmitted, 6 received, 0% packet loss, time 5192ms 74 transmitted, 6 received, 0% packet loss, time 5192ms 75 ttl=127 time=1.41 ms 75 tytes from 10.2.8.174; icmp_seq=1 ttl=127 time=1.41 ms 76 bytes from 10.2.8.174; icmp_seq=2 ttl=127 time=0.915 ms 76 tytes from 10.2.8.174; icmp_seq=2 ttl=127 time=0.915 ms 76 bytes from 10.2.8.174; icmp_seq=2 ttl=127 time=0.567 ms 76 bytes from 10.2.8.174; icmp_seq=2 ttl=127 time=0.637 ms 76 bytes from 10.2.8.174; icmp_seq=2 ttl=127 time=0.482 ms 76 bytes from 10.2.8.174; icmp_seq=3 ttl=127 time=0.482 ms 76 bytes from 10.2.8.174; icmp_seq=3 ttl=127 time=0.730 ms 76 bytes from 10.2.8.174; icmp_seq=3 ttl=127 time=0.740 ms 76 bytes from 10.2.8.174; icmp_seq=3 ttl=127 time=0.740 ms 76 bytes from 10.2.8.174; icmp_seq=3 ttl=127 time=0.740 ms 76 bytes from 10.2.8.174; icmp_seq=3 ttl=127 time=0.482 ms 76 bytes from 10.2.8.174; icmp_seq=3 ttl=127 time=0.740 ms 76 bytes from 10.2.8.174; icmp_seq=3 ttl=127 time=0.740 ms 76 bytes from 10.2.8.174; icmp_seq=3 ttl=127 time=0.681 ms 76 bytes from 10.2.8.174; icmp_seq=3 ttl=127 time=0.740 ms 76 bytes from 10.2.8.174; icmp_seq=3 ttl=127 time=0.680 ms 76 bytes from 10.2.8.174; icmp_seq=4 ttl=127 time=0.680 ms 76 bytes from 10.2.8.174; icmp_seq=4 ttl=127 time=0.680 ms 76 bytes from 10.2.8.174; ic</pre>		
<pre>94 bytes from 3.101.190.41: immp_seq=4 ttl=126 time=0.741 ms 64 bytes from 3.101.190.41: immp_seq=5 ttl=126 time=0.741 ms 64 bytes from 3.101.190.41: immp_seq=6 ttl=126 time=1.23 ms 70 70 70 70 70 70 70 70 70 70 70 70 70</pre>		
<pre>64 bytes from 3.101.190.41: icmp_seq=5 tl=126 time=0.741 ms 64 bytes from 3.101.190.41: icmp_seq=6 tl=126 time=1.23 ms C C 3.101.190.41 ping statistics 6 packets transmitted, 6 received, 0% packet loss, time 5192ms rtt min/syg/max/mdev = 0.461/0.821/1.226/0.244 ms lec2-usergip=10-1-6-16.138 -15 ping 10.2.8.174 FINO 10.2.8.174 (10.2.8.174) 56(84) bytes of data. 64 bytes from 10.2.8.174; icmp_seq=2 tl=127 time=1.41 ms 64 bytes from 10.2.8.174; icmp_seq=2 tl=127 time=0.915 ms 64 bytes from 10.2.8.174; icmp_seq=6 tt=127 time=0.567 ms 64 bytes from 10.2.8.174; icmp_seq=6 tl=127 time=0.57 ms 64 bytes from 10.2.8.174; icmp_seq=2 tl=127 time=0.57 ms 64 bytes from 10.2.8.174; icmp_seq=5 tl=127 time=0.637 ms 64 bytes from 10.2.8.174; icmp_seq=11 tl=127 time=0.637 ms 64 bytes from 10.2.8.174; icmp_seq=3 tl=127 time=0.637 ms 64 bytes from 10.2.8.174; icmp_seq=11 tl=127 time=0.637 ms 64 bytes from 10.2.8.174; icmp_seq=21 tl=127 time=0.637 ms 64 bytes from 10.2.8.174; icmp_seq=11 tl=127 time=0.637 ms 64 bytes from 10.2.8.174; icmp_seq=21 tl=127 time=0.637 ms 64 bytes from 10.2.8.174; icmp</pre>	64 bytes from 3.101.190.41: icmp_seq=4 ttl=126 time=0.911 ms	
<pre>64 bytes from 3.101.190.41: icmp_seq=6 ttl=126 time=1.23 ms C 3.101.190.41 ping statistics 6 packets transmitted, 6 received, 0% packet loss, time 5192ms rtt min/svg/max/mdev = 0.461/0.821/1.226/0.244 ms [ec2-user@ip-10-1-6-138 .15 ping 10.2.8.174 F1NS 10.2.8.174 i.cmp_seq=1 ttl=127 time=1.41 ms 64 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=0.11 ms 64 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=0.567 ms 64 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=0.567 ms 64 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=0.567 ms 64 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=0.985 ms 64 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=0.985 ms 64 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=0.985 ms 64 bytes from 10.2.8.174: icmp_seq=10 ttl=127 time=0.437 ms 64 bytes from 10.2.8.174: icmp_seq=1127 time=0.730 ms 64 bytes from 10.2.8.174: icmp_seq=1127 time=0.740 ms 64 bytes from 10.2.8.174: icmp_seq=1127 time=0.740 ms 64 bytes from 10.2.8.174: icmp_seq=1127 time=0.740 ms 64 bytes from 10.2.8.174: icmp_seq=1127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=1127 time=0.648 ms 64 bytes from 10.2.8.174: icmp_seq=1127 time=0.648 ms 64 bytes from 10.2.8.174: icmp_seq=1127 time=0.649 ms 64 bytes from 10.2.8.174: icmp_seq=1127 time=0.641 ms 70 10.2.8.174 icmp_seq=11127 time=0.649 ms 64 bytes from 10.2.8.174: icmp_seq=11127 time=0.649 ms 64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.641 ms 72 74 packets transmitted, 21 received, 0% packet loss, time 20567ms 74 75 packets transmitted, 21 received, 0% packet loss, time 20567ms 74 75 packets transmitted, 21 received, 0% packet loss, time 20567ms 75 packets from 3.101.190.411: icmp_seq=2 ttl=126 time=0.712 ms 76 bytes from 3.101.</pre>	64 bytes from 3.101.190.41: icmp_seq=5 ttl=126 time=0.741 ms	
<pre>^c </pre>	64 bytes from 3.101.190.41: icmp_seq=6 ttl=126 time=1.23 ms	
3.101.190.41 ping statistics 6 packets transmitted, 6 received, 0% packet loss, time 5192ms tt min/avg/max/mdev = 0.461/0.821/1.226/0.244 ms [ec2-user@jp-10-1-6-138 ~15 ping 10.2.8.174 FING 10.2.8.174 (10.2.8.174) 56(84) bytes of data. 64 bytes from 10.2.8.174; icmp_seq=1 ttl=127 time=1.14 ms 64 bytes from 10.2.8.174; icmp_seq=3 ttl=127 time=0.915 ms 64 bytes from 10.2.8.174; icmp_seq=3 ttl=127 time=0.915 ms 64 bytes from 10.2.8.174; icmp_seq=7 ttl=127 time=0.567 ms 64 bytes from 10.2.8.174; icmp_seq=7 ttl=127 time=0.985 ms 64 bytes from 10.2.8.174; icmp_seq=7 ttl=127 time=0.985 ms 64 bytes from 10.2.8.174; icmp_seq=7 ttl=127 time=0.985 ms 64 bytes from 10.2.8.174; icmp_seq=6 ttl=127 time=0.985 ms 64 bytes from 10.2.8.174; icmp_seq=7 ttl=127 time=0.11 ms 64 bytes from 10.2.8.174; icmp_seq=10 ttl=127 time=0.11 ms 64 bytes from 10.2.8.174; icmp_seq=11 ttl=127 time=0.740 ms 64 bytes from 10.2.8.174; icmp_seq=11 ttl=127 time=0.730 ms 64 bytes from 10.2.8.174; icmp_seq=11 ttl=127 time=0.730 ms 64 bytes from 10.2.8.174; icmp_seq=13 ttl=127 time=0.795 ms 64 bytes from 10.2.8.174; icmp_seq=11 ttl=127 time=0.792 ms 64 bytes from 10.2.8.174; icmp_seq=11 ttl=127 time=0.792 ms 64 bytes from 10.2.8.174; icmp_seq=11 ttl=127 time=0.634 ms 64 bytes from 10.2.8.174; icmp_seq=11 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174; icmp_seq=12 ttl=127 time=0.644 ms 64 bytes from 10.2.8.174; icmp_seq=2 ttl=127 time=0.649 ms 64 bytes from 10.2.8.174; icmp_seq=2 ttl=127 time=0.641 ms 70 71 packets transmitted, 21 received, 0% packet loss, time 20567ms 72 rec 72 rec 74 packets transmitted, 21 received, 0% packet loss, time 20567ms 74 mindymax/max/max/max/max/max/max/max/max/max/	^⊂	
<pre>6 packets transmitted, 6 received, 0% packet loss, time 5192ms trt min/way/max/makev = 0.461/0.821/1.226/0.244 ms lec2-user8ip=10-1-6-138 -15 ping 10.2.8.174 FING 10.2.8.174 (10.2.8.174) icmp_seq=2 ttl=127 time=1.41 ms 64 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=0.915 ms 64 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=0.915 ms 64 bytes from 10.2.8.174: icmp_seq=4 ttl=127 time=0.915 ms 64 bytes from 10.2.8.174: icmp_seq=4 ttl=127 time=0.978 ms 64 bytes from 10.2.8.174: icmp_seq=4 ttl=127 time=0.978 ms 64 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=0.978 ms 64 bytes from 10.2.8.174: icmp_seq=7 ttl=127 time=0.978 ms 64 bytes from 10.2.8.174: icmp_seq=7 ttl=127 time=0.978 ms 64 bytes from 10.2.8.174: icmp_seq=7 ttl=127 time=0.985 ms 64 bytes from 10.2.8.174: icmp_seq=9 ttl=127 time=0.985 ms 64 bytes from 10.2.8.174: icmp_seq=10 ttl=127 time=0.978 ms 64 bytes from 10.2.8.174: icmp_seq=10 ttl=127 time=0.730 ms 64 bytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.730 ms 64 bytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.730 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.728 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.463 ms 64 bytes from 10.2.8.174: icmp_seq=18 ttl=127 time=0.463 ms 64 bytes from 10.2.8.174: icmp_seq=18 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=18 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_s</pre>	3.101.190.41 ping statistics	
<pre>tt min/avg/max/mdev = 0.461/0.821/1.226/0.244 ms [ec2-userSip-10-1-6-138 -15 ping 10.2.8.174 FING 10.2.8.174 [10.2.8.174] 56(84) bytes of data. 64 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=1.14 ms 64 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=0.915 ms 64 bytes from 10.2.8.174: icmp_seq=3 ttl=127 time=0.918 ms 64 bytes from 10.2.8.174: icmp_seq=3 ttl=127 time=0.918 ms 64 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=0.567 ms 64 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=0.985 ms 64 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=0.985 ms 64 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=0.492 ms 64 bytes from 10.2.8.174: icmp_seq=10 ttl=127 time=0.730 ms 64 bytes from 10.2.8.174: icmp_seq=10 ttl=127 time=0.740 ms 64 bytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.730 ms 64 bytes from 10.2.8.174: icmp_seq=15 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=15 ttl=127 time=0.649 ms 64 bytes from 10.2.8.174: icmp_seq=15 ttl=127 time=0.649 ms 64 bytes from 10.2.8.174: icmp_seq=15 ttl=127 time=0.640 ms 64 bytes from 10.2.8.174: icmp_seq=15 ttl=127 time=0.649 ms 64 bytes from 10.2.8.174: icmp_seq=15 ttl=127 time=0.641 ms 64 bytes from 10.2.8.174: icmp_seq=15 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.641 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.621 ms 70 10.2.8.174 ping statistics 21 packets transmitted, 21 received, 0% packet loss, time 20567ms 71 min/avg/max/makev = 0.463/0.796/1.410/0.234 ms [ec2-user8ip-</pre>	6 packets transmitted, 6 received, 0% packet loss, time 5192ms	
<pre>tind 10.2.8.174 (10.2.8.174) 56(34) bytes of data. 64 bytes from 10.2.8.174: icmp_seq=1 ttl=127 time=1.41 ms 64 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=0.915 ms 64 bytes from 10.2.8.174: icmp_seq=4 ttl=127 time=0.708 ms 64 bytes from 10.2.8.174: icmp_seq=5 ttl=127 time=0.708 ms 64 bytes from 10.2.8.174: icmp_seq=7 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=7 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=9 ttl=127 time=0.492 ms 64 bytes from 10.2.8.174: icmp_seq=0 ttl=127 time=0.740 ms 64 bytes from 10.2.8.174: icmp_seq=10 ttl=127 time=0.740 ms 64 bytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.740 ms 64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.740 ms 64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.740 ms 64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.640 ms 64 bytes from 10.2.8.174: icmp_seq=14 ttl=127 time=0.640 ms 64 bytes from 10.2.8.174: icmp_seq=18 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=18 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=12 ttl=127 time=0.641 ms 65 bytes from 10.2.8.174: icmp_seq=12 ttl=127 time=0.641 ms 66 bytes from 10.2.8.174: icmp_seq=12 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=12 ttl=127 time=0.641 ms 65 bytes from 10.2.8.174: icmp_seq=12 ttl=127 time=0.641 ms 66 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.641 ms 67 67 67 67 67 67 67 67 67 67 67 67 67</pre>	rtt min/avg/max/mdev = 0.461/0.821/1.226/0.244 ms	
All 10.10.10.10.10.10.10.10.10.10.10.10.10.1	[ec2-usereip-10-1-6-136 ~] ping 10.2.6.174	
<pre>chapter from 10.2.8.174: icmp_seq=2 ttl=127 time=0.915 ms 64 bytes from 10.2.8.174: icmp_seq=3 ttl=127 time=0.915 ms 64 bytes from 10.2.8.174: icmp_seq=5 ttl=127 time=0.567 ms 64 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=0.567 ms 64 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=0.985 ms 64 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=0.985 ms 64 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=0.492 ms 64 bytes from 10.2.8.174: icmp_seq=10 ttl=127 time=0.492 ms 64 bytes from 10.2.8.174: icmp_seq=10 ttl=127 time=0.492 ms 64 bytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.730 ms 64 bytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.797 ms 64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.797 ms 64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.643 ms 64 bytes from 10.2.8.174: icmp_seq=17 ttl=127 time=0.644 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.614 ms 64 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=0.614 ms 64 bytes from 10.2.8.174: icmp_seq=2 ttl=226 time=0.716 ms 64 bytes fro</pre>	64 bytes from 10.2.8.174; jcmp seg=1 tt]=127 time=1 41 ms	
<pre>64 bytes from 10.2.8.174: icmp_seq=3 ttl=127 time=0.915 ms 64 bytes from 10.2.8.174: icmp_seq=4 ttl=127 time=0.708 ms 64 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=0.567 ms 64 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=0.985 ms 64 bytes from 10.2.8.174: icmp_seq=7 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=9 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=9 ttl=127 time=0.492 ms 64 bytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.730 ms 64 bytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.740 ms 64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.643 ms 64 bytes from 10.2.8.174: icmp_seq=16 ttl=127 time=0.643 ms 64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.644 ms 64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.644 ms 64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.649 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.641 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=26 time=0.718 ms 64 bytes</pre>	64 bytes from 10.2.8.174: jcmp seg=2 tt]=127 time=1.14 ms	
64 bytes from 10.2.8.174: icmp_seq=4 ttl=127 time=0.708 ms 64 bytes from 10.2.8.174: icmp_seq=5 ttl=127 time=0.567 ms 64 bytes from 10.2.8.174: icmp_seq=7 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=8 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=10 ttl=127 time=0.492 ms 64 bytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.730 ms 64 bytes from 10.2.8.174: icmp_seq=12 ttl=127 time=0.740 ms 64 bytes from 10.2.8.174: icmp_seq=12 ttl=127 time=0.740 ms 64 bytes from 10.2.8.174: icmp_seq=12 ttl=127 time=0.740 ms 64 bytes from 10.2.8.174: icmp_seq=12 ttl=127 time=0.780 ms 64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.870 ms 64 bytes from 10.2.8.174: icmp_seq=16 ttl=127 time=0.687 ms 64 bytes from 10.2.8.174: icmp_seq=16 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=16 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=16 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=18 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=18 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.641 ms 70 70 70 70 71 72 72 72 73 74 74 74 75 74 75 75 75 75 75 75 75 75 75 75	64 bytes from 10.2.8.174: icmp seg=3 ttl=127 time=0.915 ms	
64 bytes from 10.2.8.174: icmp_seq=5 ttl=127 time=0.567 ms 64 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=1.11 ms 64 bytes from 10.2.8.174: icmp_seq=8 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=9 ttl=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=10 ttl=127 time=0.492 ms 64 bytes from 10.2.8.174: icmp_seq=10 ttl=127 time=0.492 ms 64 bytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.492 ms 64 bytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.730 ms 64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.797 ms 64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.722 ms 64 bytes from 10.2.8.174: icmp_seq=14 ttl=127 time=0.463 ms 64 bytes from 10.2.8.174: icmp_seq=17 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=17 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=19 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.643 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.641 ms 65 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.641 ms 66 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.641 ms 67 10.2.8.174 ping statistics 21 packets transmited, 21 received, 0% packet loss, time 20567ms ctt min/avg/max/mdev = 0.463/0.798/1.410/0.234 ms [ec2-user8ip=10-1-6-188 -]\$ ping 3.101.190.41 FING 3.101.190.41 i.100.41 i.100.41 64 bytes from 3.101.190.41 i.icmp_seq=2 ttl=126 time=0.672 ms 64 bytes from 3.101.190.41 i.icmp_seq=2 ttl=126 time=0.672 ms 64 bytes from 3.101.190.41 i.icmp_seq=3 ttl=126 time=0.738 ms	64 bytes from 10.2.8.174: icmp seq=4 ttl=127 time=0.708 ms	
64 bytes from 10.2.8.174: icmp_seq=6 tt]=127 time=1.11 ms 64 bytes from 10.2.8.174: icmp_seq=7 tt]=127 time=0.985 ms 64 bytes from 10.2.8.174: icmp_seq=8 tt]=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=9 tt]=127 time=0.187 64 bytes from 10.2.8.174: icmp_seq=1 tt]=127 time=0.730 ms 64 bytes from 10.2.8.174: icmp_seq=11 tt]=127 time=0.730 ms 64 bytes from 10.2.8.174: icmp_seq=11 tt]=127 time=0.740 ms 64 bytes from 10.2.8.174: icmp_seq=13 tt]=127 time=0.722 ms 64 bytes from 10.2.8.174: icmp_seq=14 tt]=127 time=0.722 ms 64 bytes from 10.2.8.174: icmp_seq=16 tt]=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=16 tt]=127 time=0.643 ms 64 bytes from 10.2.8.174: icmp_seq=19 tt]=127 time=0.644 ms 64 bytes from 10.2.8.174: icmp_seq=20 tt]=127 time=0.644 ms 64 bytes from 10.2.8.174: icmp_seq=20 tt]=127 time=0.649 ms 64 bytes from 10.2.8.174: icmp_seq=20 tt]=127 time=0.641 ms 70 10.2.8.174 ping statistics 21 packets transmitted, 21 received, 0% packet loss, time 20567ms rtt min/avg/max/mdev = 0.463/0.798/1.410/0.234 ms [ec2-user8ip=10-1-6-138 .]5 ping 3.101.190.41 PING 3.101.190.41: icmp_seq=2 tt]=126 time=0.472 ms 64 bytes from 3.101.190.41: icmp_seq=2 tt]=126 time=0.672 ms 64 bytes from 3.101.190.41: icmp_seq=2 tt]=126 time=0.672 ms 64 bytes from 3.101.190.41: icmp_seq=3 tt]=126 time=0.738 ms	64 bytes from 10.2.8.174: icmp seq=5 ttl=127 time=0.567 ms	
64 bytes from 10.2.8.174: icmp_seq=7 tt]=127 time=0.985 ms 64 bytes from 10.2.8.174: icmp_seq=8 tt]=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=9 tt]=127 time=0.492 ms 64 bytes from 10.2.8.174: icmp_seq=11 tt]=127 time=0.730 ms 64 bytes from 10.2.8.174: icmp_seq=12 tt]=127 time=0.740 ms 64 bytes from 10.2.8.174: icmp_seq=12 tt]=127 time=0.670 ms 64 bytes from 10.2.8.174: icmp_seq=15 tt]=127 time=0.670 ms 64 bytes from 10.2.8.174: icmp_seq=16 tt]=127 time=0.670 ms 64 bytes from 10.2.8.174: icmp_seq=16 tt]=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=16 tt]=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=19 tt]=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=19 tt]=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=20 tt]=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=21 tt]=127 time=0.691 ms $^{\circ_{C}}$ $^{}$ 10.2.8.174 ping statistics 21 packets transmitted, 21 received, 0% packet loss, time 20567ms tt min/arg/max/mdev = 0.463/0.798/1.410/0.234 ms [ec2-user8ip-10-1-6-138 ~]\$ ping 3.101.190.41 FING 3.101.190.41: icmp_seq=2 tt]=126 time=0.472 ms 64 bytes from 3.101.190.41: icmp_seq=2 tt]=126 time=0.672 ms 64 bytes from 3.101.190.41: icmp_seq=3 tt]=126 time=0.738 ms	64 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=1.11 ms	
64 bytes from 10.2.8.174: icmp_seq=8 tt]=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=9 tt]=127 time=0.492 ms 64 bytes from 10.2.8.174: icmp_seq=11 tt]=127 time=0.492 ms 64 bytes from 10.2.8.174: icmp_seq=11 tt]=127 time=0.730 ms 64 bytes from 10.2.8.174: icmp_seq=11 tt]=127 time=0.740 ms 64 bytes from 10.2.8.174: icmp_seq=13 tt]=127 time=0.727 ms 64 bytes from 10.2.8.174: icmp_seq=14 tt]=127 time=0.870 ms 64 bytes from 10.2.8.174: icmp_seq=15 tt]=127 time=0.870 ms 64 bytes from 10.2.8.174: icmp_seq=16 tt]=127 time=0.870 ms 64 bytes from 10.2.8.174: icmp_seq=16 tt]=127 time=0.687 ms 64 bytes from 10.2.8.174: icmp_seq=16 tt]=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=18 tt]=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=21 tt]=127 time=0.641 ms 7c 7 10.2.8.174 ping statistics 21 packets transmitted, 21 received, 0% packet loss, time 20567ms 7tt min/avg/max/mdev = 0.463/0.798/1.410/0.234 ms [ec2-user8ip=10-1-6-138 -]\$ ping 3.101.190.41 FING 3.101.190.41; icmp_seq=1 tt]=126 time=0.472 ms 64 bytes from 3.101.190.41; icmp_seq=3 tt]=126 time=0.672 ms 64 bytes from 3.101.190.41; icmp_seq=3 tt]=126 time=0.738 ms	64 bytes from 10.2.8.174: icmp_seq=7 ttl=127 time=0.985 ms	
64 bytes from 10.2.8.174: icmp_seq=9 tt]=127 time=1.11 ms 64 bytes from 10.2.8.174: icmp_seq=10 tt]=127 time=0.492 ms 64 bytes from 10.2.8.174: icmp_seq=11 tt]=127 time=0.730 ms 64 bytes from 10.2.8.174: icmp_seq=11 tt]=127 time=0.740 ms 64 bytes from 10.2.8.174: icmp_seq=13 tt]=127 time=0.79 ms 64 bytes from 10.2.8.174: icmp_seq=16 tt]=127 time=0.722 ms 64 bytes from 10.2.8.174: icmp_seq=16 tt]=127 time=0.637 ms 64 bytes from 10.2.8.174: icmp_seq=16 tt]=127 time=0.643 ms 64 bytes from 10.2.8.174: icmp_seq=17 tt]=127 time=0.643 ms 64 bytes from 10.2.8.174: icmp_seq=19 tt]=127 time=0.644 ms 64 bytes from 10.2.8.174: icmp_seq=19 tt]=127 time=0.644 ms 64 bytes from 10.2.8.174: icmp_seq=20 tt]=127 time=0.649 ms 64 bytes from 10.2.8.174: icmp_seq=20 tt]=127 time=0.614 ms 64 bytes from 10.2.8.174: icmp_seq=20 tt]=127 time=0.614 ms 64 bytes from 10.2.8.174: icmp_seq=20 tt]=127 time=0.614 ms 64 bytes from 10.2.8.174: icmp_seq=21 tt]=127 time=0.614 ms 65 bytes from 10.2.8.174: icmp_seq=21 tt]=127 time=0.614 ms 66 bytes from 10.2.8.174: icmp_seq=21 tt]=127 time=0.614 ms 67 10.2.8.174 ping statistics 21 packets transmitted, 21 received, 0% packet loss, time 20567ms rtt min/avg/max/mdev = 0.463/0.798/1.410/0.234 ms [sc2-user8ip=10-1-6-188 -]\$ ping 3.101.190.41 FING 3.101.190.41: icmp_seq=2 tt]=126 time=0.472 ms 64 bytes from 3.101.190.41: icmp_seq=2 tt]=126 time=0.672 ms 64 bytes from 3.101.190.41: icmp_seq=3 tt]=126 time=0.738 ms	64 bytes from 10.2.8.174: icmp_seq=8 ttl=127 time=0.637 ms	
Abytes from 10.2.8.174: icmp_seq=10 ttl=12/ time=0.492 ms         Abytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.730 ms         Abytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.740 ms         Abytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.740 ms         Abytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.722 ms         Abytes from 10.2.8.174: icmp_seq=14 ttl=127 time=0.870 ms         Abytes from 10.2.8.174: icmp_seq=16 ttl=127 time=0.687 ms         Abytes from 10.2.8.174: icmp_seq=16 ttl=127 time=0.684 ms         Abytes from 10.2.8.174: icmp_seq=16 ttl=127 time=0.642 ms         Abytes from 10.2.8.174: icmp_seq=210 ttl=127 time=0.614 ms         Cover            10.2.8.174: icmp_seq=210 ttl=127 time=0.614 ms         Cover            11.120 ttl=127 time=0.614 ms         Cover            21 packets transmitted, 21 received, 0% packet loss, time 20567ms         rttmin/avg/max/mdev = 0.463/0.798/1.410/0.234 ms	64 bytes from 10.2.8.174: icmp_seq=9 ttl=127 time=1.11 ms	
0+ bytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.730 ms         64 bytes from 10.2.8.174: icmp_seq=12 ttl=127 time=0.579 ms         64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.579 ms         64 bytes from 10.2.8.174: icmp_seq=15 ttl=127 time=0.870 ms         64 bytes from 10.2.8.174: icmp_seq=15 ttl=127 time=0.870 ms         64 bytes from 10.2.8.174: icmp_seq=15 ttl=127 time=0.463 ms         64 bytes from 10.2.8.174: icmp_seq=16 ttl=127 time=0.687 ms         64 bytes from 10.2.8.174: icmp_seq=18 ttl=127 time=0.642 ms         64 bytes from 10.2.8.174: icmp_seq=18 ttl=127 time=0.642 ms         64 bytes from 10.2.8.174: icmp_seq=18 ttl=127 time=0.642 ms         64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.642 ms         64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.642 ms         64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.642 ms         64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.691 ms         70         71 packets transmitted, 21 received, 0% packet loss, time 20567ms         72 received ip=10-1-6-138 ~ J\$ ping 3.101.190.41         71 packets from 3.101.190.41; icmp_seq=2 ttl=126 time=0.472 ms         64 bytes from 3.101.190.41; icmp_seq=2 ttl=126 time=0.672 ms         64 bytes from 3.101.190.41; icmp_seq=3 ttl=126 time=0.738 ms	64 bytes from 10.2.8.174: icmp_seq=10 tt1=127 time=0.492 ms	
9 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.740 ms         64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.722 ms         64 bytes from 10.2.8.174: icmp_seq=14 ttl=127 time=0.870 ms         64 bytes from 10.2.8.174: icmp_seq=16 ttl=127 time=0.463 ms         64 bytes from 10.2.8.174: icmp_seq=16 ttl=127 time=0.463 ms         64 bytes from 10.2.8.174: icmp_seq=16 ttl=127 time=0.664 ms         64 bytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.642 ms         64 bytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.642 ms         64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.642 ms         64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.671 ms         70         71 packets transmitted, 21 received, 0% packet loss, time 20567ms         72 packets transmitted, 21 received, 0% packet loss, time 20567ms         71 packets transmitted, 21 received, 0% packet loss, time 20567ms         71 packets transmitted, 21 stime_0.413 (0.101.190.41         72 use from 3.101.190.41: icmp_seq=1 ttl=126 time=0.472 ms	64 bytes from 10.2.8.1/4: 1cmp_seq=11 ttl=12/ time=0.730 ms	
b) 1 5005       from 10.2.8.174:       icmp_seq=14       t1=127       time=0.722       ms         64       bytes from 10.2.8.174:       icmp_seq=15       t1=127       time=0.870       ms         64       bytes from 10.2.8.174:       icmp_seq=16       t1=127       time=0.672       ms         64       bytes from 10.2.8.174:       icmp_seq=16       t1=127       time=0.643       ms         64       bytes from 10.2.8.174:       icmp_seq=19       t1=127       time=0.644       ms         64       bytes from 10.2.8.174:       icmp_seq=19       t1=127       time=0.644       ms         64       bytes from 10.2.8.174:       icmp_seq=20       t1=127       time=0.642       ms         64       bytes from 10.2.8.174:       icmp_seq=20       t1=127       time=0.643       ms         64       bytes from 10.2.8.174:       icmp_seq=20       t1=127       time=0.642       ms         64       bytes from 10.2.8.174:       icmp_seq=21       t1=127       time=0.614       ms         64       bytes from 10.2.8.174:       icmp_seq=21       t1=127       time=0.614       ms         62       c       1       recived, 0%       packet loss, time 20567ms       rtt <min avg="" max="" mdev="0.463/0.798/1.410/0.234&lt;/td"><td>64 bytes from 10.2.8.174: icmp_seq=12 tt1=127 time=0.740 ms</td><td></td></min>	64 bytes from 10.2.8.174: icmp_seq=12 tt1=127 time=0.740 ms	
64 bytes from 10.2.8.174: icmp_seq=15 ttl=127 time=0.870 ms 64 bytes from 10.2.8.174: icmp_seq=16 ttl=127 time=0.463 ms 64 bytes from 10.2.8.174: icmp_seq=16 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=19 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.649 ms 64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.641 ms 64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.691 ms 70 71 72 72 72 73 74 75 75 75 75 75 75 75 75 75 75	64 bytes from 10.2.8.174: icmp_seq=15 ttl=127 time=0.722 ms	
64 bytes from 10.2.8.174: icmp_seq=16 ttl=127 time=0.463 ms 64 bytes from 10.2.8.174: icmp_seq=17 ttl=127 time=0.694 ms 64 bytes from 10.2.8.174: icmp_seq=18 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=19 ttl=127 time=0.849 ms 64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.716 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.691 ms 7c 10.2.8.174 ping statistics 21 packets transmitted, 21 received, 0% packet loss, time 20567ms ttmin/arg/max/mdev = 0.463/0.798/1.410/0.234 ms [ec2-user@ip=10-1-6-138 -]\$ ping 3.101.190.41 FING 3.101.190.41; icmp_seq=1 ttl=126 time=0.472 ms 64 bytes from 3.101.190.41; icmp_seq=2 ttl=126 time=0.672 ms 64 bytes from 3.101.190.41; icmp_seq=3 ttl=126 time=0.738 ms	64 bytes from 10.2.8.174: icmp seg=15 ttl=127 time=0.870 ms	
64 bytes from 10.2.8.174: icmp_seq=17 ttl=127 time=0.694 ms 64 bytes from 10.2.8.174: icmp_seq=18 ttl=127 time=0.694 ms 64 bytes from 10.2.8.174: icmp_seq=19 ttl=127 time=0.684 ms 64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.716 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.691 ms ^c 10.2.8.174 ping statistics 21 packets transmitted, 21 received, 0% packet loss, time 20567ms rtt min/avg/max/mdev = 0.463/0.798/1.410/0.234 ms [ec2-user8ip=10-1-6-138 .]\$ ping 3.101.190.41 PING 3.101.190.41: scmp_seq=1 ttl=126 time=0.472 ms 64 bytes from 3.101.190.41: icmp_seq=2 ttl=126 time=0.672 ms 64 bytes from 3.101.190.41: icmp_seq=3 ttl=126 time=0.738 ms	64 bytes from 10.2.8.174: icmp seq=16 ttl=127 time=0.463 ms	
64 bytes from 10.2.8.174: icmp_seq=18 ttl=127 time=0.642 ms 64 bytes from 10.2.8.174: icmp_seq=19 ttl=127 time=0.849 ms 64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.716 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.691 ms ^c 10.2.8.174 ping statistics 21 packets transmitted, 21 received, 0% packet loss, time 20567ms rtt min/arg/max/mdev = 0.463/0.798/1.410/0.234 ms [ec2-user@ip=10-1-6-138 ~]\$ ping 3.101.190.41 Fing 3.101.190.41 (3.101.190.41) 56(84) bytes of data. 64 bytes from 3.101.190.41: icmp_seq=1 ttl=126 time=0.472 ms 64 bytes from 3.101.190.41: icmp_seq=2 ttl=126 time=0.672 ms 64 bytes from 3.101.190.41: icmp_seq=3 ttl=126 time=0.738 ms	64 bytes from 10.2.8.174: icmp_seq=17 ttl=127 time=0.694 ms	
64 bytes from 10.2.8.174: icmp_seq=19 ttl=127 time=0.849 ms 64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.716 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.691 ms ^c 10.2.8.174 ping statistics 21 packets transmitted, 21 received, 0% packet loss, time 20567ms tt min/arg/max/mdev = 0.463/0.798/1.410/0.234 ms [ec2-user@ip=10-1-6-138 ~]\$ ping 3.101.190.41 FING 3.101.190.41 (3.101.190.41) 56(84) bytes of data. 64 bytes from 3.101.190.41: icmp_seq=2 ttl=126 time=0.472 ms 64 bytes from 3.101.190.41: icmp_seq=2 ttl=126 time=0.672 ms 64 bytes from 3.101.190.41: icmp_seq=3 ttl=126 time=0.738 ms	64 bytes from 10.2.8.174: icmp_seq=18 ttl=127 time=0.642 ms	
64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.716 ms 64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.691 ms ^C 10.2.8.174 ping statistics 21 packets transmitted, 21 received, 0% packet loss, time 20567ms rtt min/avg/max/mdev = 0.463/0.798/1.410/0.234 ms [ec2-user@ip=10-1-6-138 ~]S ping 3.101.190.41 FNG 3.101.190.41 (3.101.190.41) 56(64) bytes of data. 64 bytes from 3.101.190.41: icmp_seq=1 ttl=126 time=0.472 ms 64 bytes from 3.101.190.41: icmp_seq=2 ttl=126 time=0.672 ms 64 bytes from 3.101.190.41: icmp_seq=3 ttl=126 time=0.738 ms	64 bytes from 10.2.8.174: icmp_seq=19 ttl=127 time=0.849 ms	
64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.691 ms ^c 10.2.8.174 ping statistics 21 packets transmitted, 21 received, 0% packet loss, time 20567ms rtt min/avg/max/mdev = 0.463/0.798/1.410/0.234 ms [ec2-user@ip-10-1-6-138 *]\$ ping 3.101.190.41 PING 3.101.190.41 (3.101.190.41) 56(84) bytes of data. 64 bytes from 3.101.190.41: icmp_seq=1 ttl=126 time=0.472 ms 64 bytes from 3.101.190.41: icmp_seq=3 ttl=126 time=0.738 ms	64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.716 ms	
<pre>^cc  10.2.8.174 ping statistics 21 packets transmitted, 21 received, 0% packet loss, time 20567ms rtt min/arg/max/mdev = 0.463/0.798/1.410/0.234 ms [ec2-user@ip-10-1-6-138 ~]\$ ping 3.101.190.41 [rNG 3.101.190.41 (3.101.190.41) 56(84) bytes of data. 64 bytes from 3.101.190.41: icmp_seq=1 ttl=126 time=0.472 ms 64 bytes from 3.101.190.41: icmp_seq=2 ttl=126 time=0.738 ms</pre>	64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.691 ms	
10.2.0.1/4 ping statistics 21 packets transmitted, 21 received, 0% packet loss, time 20567ms tt min/arg/max/mdev = 0.463/0.798/1.410/0.234 ms [ec2-user@ip-10-1-6-138 -]\$ ping 3.101.190.41 [rNG 3.101.190.41 (3.101.190.41) : 6(84) bytes of data. 64 bytes from 3.101.190.41: icmp_seq=1 ttl=126 time=0.472 ms 64 bytes from 3.101.190.41: icmp_seq=2 ttl=126 time=0.672 ms 64 bytes from 3.101.190.41: icmp_seq=3 ttl=126 time=0.738 ms		
21 packets transmitted, 21 received, 0* packet 1058, time 2006/ms         21 th min/arg/max/medv = 0.463/0.798/1.410/0.234 ms         [ec2-user@ip-10-1-6-138 ~]\$ ping 3.101.190.41         PING 3.101.190.41 (3.101.190.41) 56(84) bytes of data.         64 bytes from 3.101.190.41: icmp_seq=1 ttl=126 time=0.472 ms         64 bytes from 3.101.190.41: icmp_seq=2 ttl=126 time=0.672 ms         64 bytes from 3.101.190.41: icmp_seq=3 ttl=126 time=0.738 ms	10.2.8.1/4 ping statistics	
<pre>[ec2-user@ip-10-16-138 .]s ping 3.101.190.41 PING 3.101.190.41 (3.101.190.41) 56(84) bytes of data. 64 bytes from 3.101.190.41: icmp_seq=1 ttl=126 time=0.472 ms 64 bytes from 3.101.190.41: icmp_seq=2 ttl=126 time=0.738 ms</pre>	rtt min/aug/max/mdex = 0 463/0 798/1 410/0 234 ma	
Find 3.101.190.41 (3.101.190.41) 56(64) bytes of data. 64 bytes from 3.101.190.41: icmp_seq=1 ttl=126 time=0.472 ms 64 bytes from 3.101.190.41: icmp_seq=2 ttl=126 time=0.738 ms	$ec2 = user Rin = 10 - 1 - 6 - 138 \sim 15 ning 3, 101, 190, 41$	
64 bytes from 3.101.190.41: icmp_seq=1 ttl=126 time=0.472 ms 64 bytes from 3.101.190.41: icmp_seq=2 ttl=126 time=0.672 ms 64 bytes from 3.101.190.41: icmp_seq=3 ttl=126 time=0.738 ms	PING 3.101.190.41 (3.101.190.41) 56(84) bytes of data.	
64 bytes from 3.101.190.41: icmp_seq=2 ttl=126 time=0.672 ms 64 bytes from 3.101.190.41: icmp_seq=3 ttl=126 time=0.738 ms	64 bytes from 3.101.190.41: icmp seq=1 ttl=126 time=0.472 ms	
64 bytes from 3.101.190.41: icmp_seq=3 ttl=126 time=0.738 ms	64 bytes from 3.101.190.41: icmp seq=2 ttl=126 time=0.672 ms	
	64 bytes from 3.101.190.41: icmp_seq=3 ttl=126 time=0.738 ms	



## Analyzing flow logs

Flow logs tell us about the source and destination of the network traffic, the amount of data being transferred, whether the traffic is being rejected or accepted.

For example, the flow log I've captured tells us that traffic went from one address to another. We can also extract that the traffic was accepted by the security groups and network ACLs of my VPC.

*	2024-08-10T02:35:30.000Z	2 088535904191 eni-0dc00736cd776693a 13.52.6.116 10.1.6.138 24862 22 6 2 172 1723257330 1723257374 4CCEPT OK	
	2 088535984191 eni-0dcb0736cd77e693a 1	3.52.6.116 10.1.6.138 24662 22 6 2 172 1723257339 1723257374 KCCEPT OK	Ø
*	2024-08-10T02:35:30.000Z	2 088535904191 eni-0xcb0736cx77e6930 10.1.6.138 13.52.6.116 22 24862 6 1 88 1723257330 1723257374 ACCEPT OK	
	2 088535984191 eni-0dcb0736cd77e693a 1	8.1.6.138 13.52.6.116 22 24662 6 1 88 1723257338 1723257374 ACCEPT OK	ð
٣	2024-08-10T02:36:06.000Z	2 088535904191 eni-0xcb0736cc077e6930 89.248.163.200 10.1.6.138 54964 5432 6 1 40 1723257366 1723257399 REJECT OK	
	2 088535984191 eni-0dcb0736cd77e693# 8	9.246.163.200 16.1.6.138 54644 5432 6 1 40 1723257366 1723257399 REJECT OK	ø
*	2024-08-10T02:36:06.000Z	2 088535994191 eni-0scb0736cc77e693a 162.216.150.98 10.1.6.138 54769 52975 6 1 44 1723257366 1723257399 REJECT OK	
	2 088535984191 eni-0dcb0736cd77e693a 1	62.216.158.58 10.1.6.138 54769 51875 6 1 44 1723257360 1723257399 REDECT OK	ø
*	2024-08-10T02:36:06.000Z	2 088535984191 eni-06cb0736cc77e693a 170.187.163.90 10.1.6.138 52196 25462 6 1 44 1723257366 1723257399 REJECT OK	
	2 088535984191 eni-0dcb0736cd77e693a 1	78.187.161.50 10.1.6.138 52196 25442 6 1 44 1723257366 1723257399 REDECT OK	ø
*	2024-08-10T02:36:06.000Z	2 088535984191 eni-&dcb0736cc776693a 4.246.247.164 10.1.6.138 48521 1527 6 1 40 1723257366 1723257399 REJECT OK	
	2 088535984191 eni-0dcb0736cd77e693a 4	.246.247.164 10.1.6.130 48521 1527 6 1 40 1723257366 1723257399 REJECT OK	ø



## Logs Insights

Logs Insights is a CloudWatch feature that analyzes your logs. In Log Insights, you use queries to filter, process and combine data to help you troubleshoot problems or better understand your network traffic!

I ran the query "Top 10 byte transfers by source and destination IP addresses". This query analyzes the top 10 biggest data transfers between IP addresses in your network!

Logs ('	(10)		Export results 🔻 Add to da	ishboard 💿
			Showing 10 of 753 records matched	Hide histogram
20			762 records (105.6 kB) scanned in 1.6s @ 488 records/s (67.8 kB/s)	
15 10 5 0	01:50	01:55	L 1111-11-1 1	02:45
15 10 5 0	01:50	01:55 dstAddr	ImplIII_I         Impl_III_I         Impl_IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	02:45
15 10 5 0	01:50 srcAddr 13.52.6.116	01:55 dstAddr 10.1.6.138	Implall_l         Impl_all_l         Impl_a	02:45
15 10 5 0	01:50 srcAddr 13.52.6.116 10.1.6.138	01:55 dstAddr 10.1.6.138 13.52.6.116	Impl_and_a         Impl_and	02:45
# 15 10 5 0 1 1 2 3	01:50 srcAddr 13.52.6.116 10.1.6.138 52.119.176.1.	01:55 dstAddr 10.1.6.138 13.52.6.116 10.1.6.138	Image: and and and and and and and and an antiparticipant and antiparticipant antitext antitext antiparticipant antitext antiparticipant antipartic	02:45
# 15 10 5 0 1 1 2 3 4	01:50 srcAddr 13.52.6.116 10.1.6.138 52.119.176.1_ 52.119.180.1_	01:55 dstAddr 10.1.6.138 13.52.6.116 10.1.6.138 10.1.6.138	No. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10	02:45
15 10 5 0,	01:50 srcAddr 13:52:6:116 10:1:6:138 52:119:176:1. 52:119:180:1. 10:1:6:138	01:55 dstAddr 10.1.6.138 13.52.6.116 10.1.6.138 10.1.6.138 52.119.180	Implementation         Impleme	02:45
15 10 5 0 7 1 2 3 3 4 5 5 6	01:50 srcAddr 13.52.6.116 10.1.6.138 52.119.176.1. 52.119.180.1. 10.1.6.138 10.1.6.138	01:55 dstAddr 10.1.6.138 13.52.6.116 10.1.6.138 10.1.6.138 52.119.180 52.119.176	Image: serie         Image: serie<	02:45
15 10 5 0 1 2 3 3 4 5 5 6 6 7	01:50 srcAddr 13.52.6.116 10.1.6.138 52.119.176.1. 52.119.180.1. 10.1.6.138 10.1.6.138 10.1.6.138	01:55 dstAddr 10.1.6.138 13.52.6.116 10.1.6.138 52.119.180 52.119.176 10.2.8.174	02.40       02.05       02.10       02.15       02.20       02.25       02.30       02.35       02.40         bytestransferred                02.40       02.35       02.30       02.35       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40       02.40	92.45
15 10 5 0 1 1 2 3 3 4 4 5 5 6 6 5 7 8 8	01:50 srcAddr 13.52.6.116 19.1.6.138 52.119.176.1. 52.119.176.1. 19.1.6.138 19.1.6.138 19.1.6.138 19.1.6.138	01:55 dstAddr 10.1.6.138 13.52.6.116 10.1.6.138 10.1.6.138 52.119.180 52.119.176 10.2.8.174 10.1.6.138	Image: Application         Image:	02.45
15         10         5         0         1         2         3         4         5         6         7         8         9         1	01:50 srcAddr 13.52.6.116 10.1.6.138 52.119.176.1. 52.119.180.1. 10.1.6.138 10.1.6.138 10.1.6.138 10.2.8.174 134.226.18.89	01:55 dstAddr 10.1.6.138 13.52.6.116 10.1.6.138 10.1.6.138 52.119.180 52.119.176 10.2.8.174 10.1.6.138 10.1.6.138	Image: Application of the state of the	02.45
15         10         5         0         1         2         3         4         5         6         7         8         9         180	01:50 srcAddr 13.52.6.116 10.1.6.138 52.119.176.1. 52.119.180.1. 10.1.6.138 10.1.6.138 10.1.6.138 10.2.8.174 154.216.18.89 3.101.198.41	01:55 dstÄddr 10.1.6.138 10.1.6.138 10.1.6.138 10.1.6.138 10.1.6.138 10.1.6.138 10.1.6.138 10.1.6.138 10.1.6.138	Addition	02.45
#         #         1         2         3         4         5         6         7         8         9         10	01:50 srcAddr 13.52.6.116 13.52.6.116 52.119.176.1. 52.119.180.1. 10.1.6.138 10.1.6.138 10.2.8.174 13.2.8.174 13.2.8.18.09 3.101.199.41	01:55 dstAddr 10.1.6.138 13.52.6.116 10.1.6.138 10.1.6.138 52.119.180 52.119.176 10.2.8.174 10.1.6.138 10.1.6.138 10.1.6.138	Application	02.45



## Everyone should be in a job they love.

Check out <u>nextwork.org</u> for more projects

