aws

# COMMUNITY DAY

AOTEAROA

aws COMMUNITY DAY

AOTEAROA

# Testing and Monitoring Networks on AWS Using Native Tools

HITARTH ASRANI | 6 Sept 2023.

aws COMMUNITY DAY AOTEAROA

# About Me

- Hitarth Asrani, AWS Cloud DevOps Engineer @ Leaven/CCL (Part of Spark Business Group) ~ 2 years in October
- 6 X AWS Certified. Talk to me after if you want to learn more about AWS Certification
- Spent the last year building and debugging a complex network for one of my clients.
- Held back trying to go Swimming during the Cyclone. It just seems wrong…

Spark Business Group | Spark nz | CCL | Qrious | leaven. | Digital Island*

aws COMMUNITY DAY AOTEAROA

# Agenda: 10-15 mins talk, ~15 mins Live Demo

Introduction / Quick Recap of networking on AWS.

Scenario: An Organization

Monitoring your network with CloudWatch

Testing your network with AWS Network Manager

Live Demo

Q&A / End

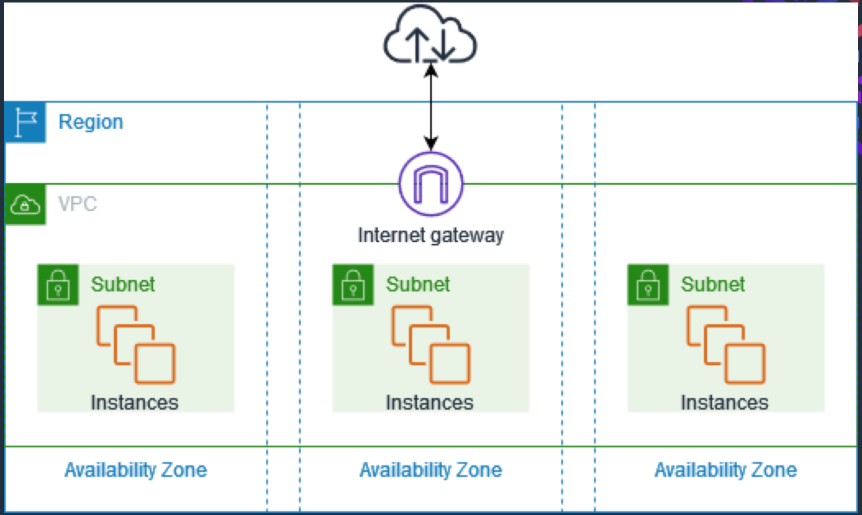
aws

COMMUNITY DAY

AOTEAROA

# Networking on AWS Recap

VPC – Virtual Private Cloud
Subnets – segmented pieces of your VPC
Route Tables – Rules/Routes for your subnets or VPC's
Security Groups – Set of rules for inbound and outbound traffic applied on resources
NACLS – Network ACL's allow and deny access based on rules on the VPC level.



# Scenario: An Organization

C-Level Execs: Charts and vital information

Security Team: Audit and Compliance with policies

Testing Team: Automated Testing in infrastructure

Ops Team: Fix infra/connectivity issues faster.

Dev Team: Develop and fix bugs faster w/o infra issues

aws COMMUNITY DAY

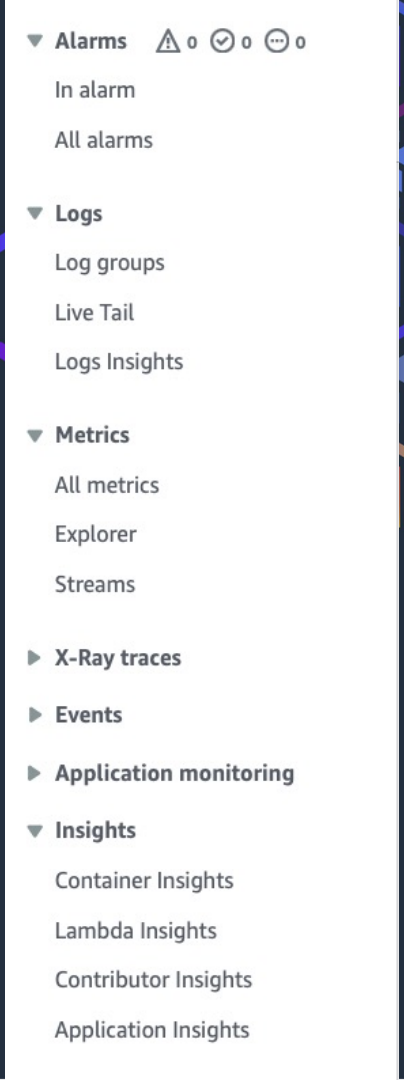
AOTEAROA

# Monitoring Your Networks

aws COMMUNITY DAY AOTEAROA

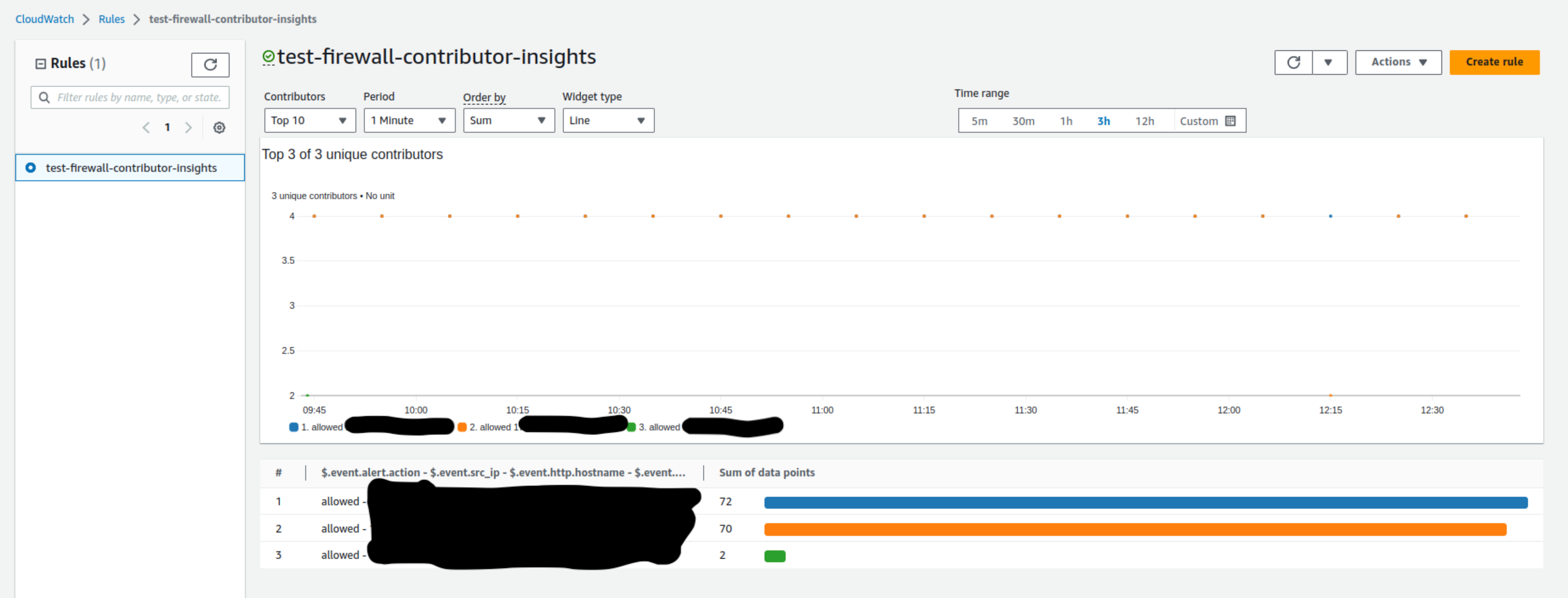
# C-Level Execs’ Fancy Charts = Logs + CW/S3

- CloudWatch (CW) is your central place for anything “monitoring” on AWS.
- Metrics, Logs, Alarms and others
- CloudWatch Contributor insights allow you to analyze log data and display it in time series
- CloudWatch Alarms allow you to respond to events from your metrics
- Logs Insights- Select a log group and run queries on it.



aws COMMUNITY DAY AOTEAROA

# CloudWatch Contributor insights example



CloudWatch > Rules > test-firewall-contributor-insights

⊟ Rules (1)
Filter rules by name, type, or state.
< 1 >
○ test-firewall-contributor-insights

## test-firewall-contributor-insights

Contributors: Top 10 ▼

Period: 1 Minute ▼

Order by: Sum ▼

Widget type: Line ▼

Time range: 5m 30m 1h **3h** 12h Custom

Top 3 of 3 unique contributors

3 unique contributors • No unit

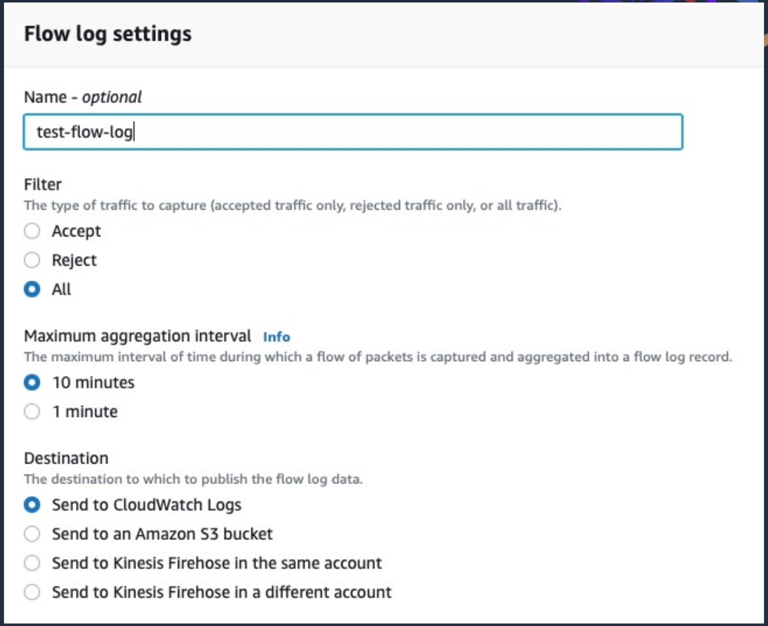
🟦 1. allowed [redacted] 🟧 2. allowed 1[redacted] 🟩 3. allowed [redacted]

| # | $.event.alert.action - $.event.src_ip - $.event.http.hostname - $.event.... | Sum of data points |
|---|---|---|
| 1 | allowed - [redacted] | 72 |
| 2 | allowed - [redacted] | 70 |
| 3 | allowed - [redacted] | 2 |

aws COMMUNITY DAY AOTEAROA

# Security Team: VPC Flow Logs and NFW Logs

- VPC Flow Logs capture information about traffic flowing through the network
- AWS Network Firewall can log to CloudWatch or S3.
- S3 + Athena can give you insights into logs.



**Flow log settings**

Name - *optional*

test-flow-log

Filter

The type of traffic to capture (accepted traffic only, rejected traffic only, or all traffic).

○ Accept

○ Reject

● All

Maximum aggregation interval Info

The maximum interval of time during which a flow of packets is captured and aggregated into a flow log record.

● 10 minutes

○ 1 minute

Destination

The destination to which to publish the flow log data.

● Send to CloudWatch Logs

○ Send to an Amazon S3 bucket

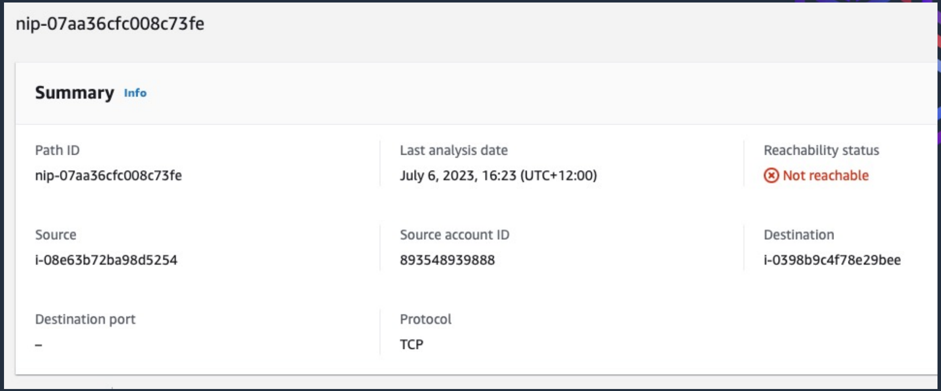
○ Send to Kinesis Firehose in the same account

○ Send to Kinesis Firehose in a different account

# Testing Your Networks

# Testing Team + Ops Team: VPC Reachability Analyzer

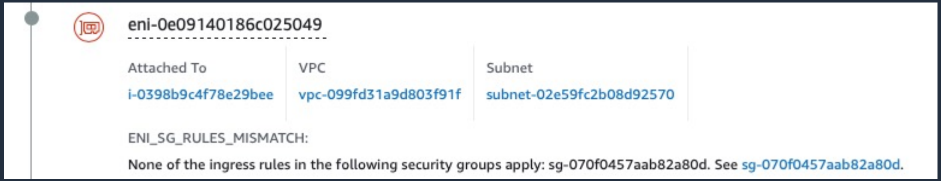
- Testing suite under “AWS Network Manager”
- Test connectivity between a source resource and a destination resource
- Price per analysis (ap-se-2) – $0.10
- Troubleshoot, verify and automate verification of connectivity



nip-07aa36cfc008c73fe

**Summary** Info

| | | |
|---|---|---|
| Path ID<br>nip-07aa36cfc008c73fe | Last analysis date<br>July 6, 2023, 16:23 (UTC+12:00) | Reachability status<br>⊗ Not reachable |
| Source<br>i-08e63b72ba98d5254 | Source account ID<br>893548939888 | Destination<br>i-0398b9c4f78e29bee |
| Destination port<br>– | Protocol<br>TCP | |



eni-0e09140186c025049

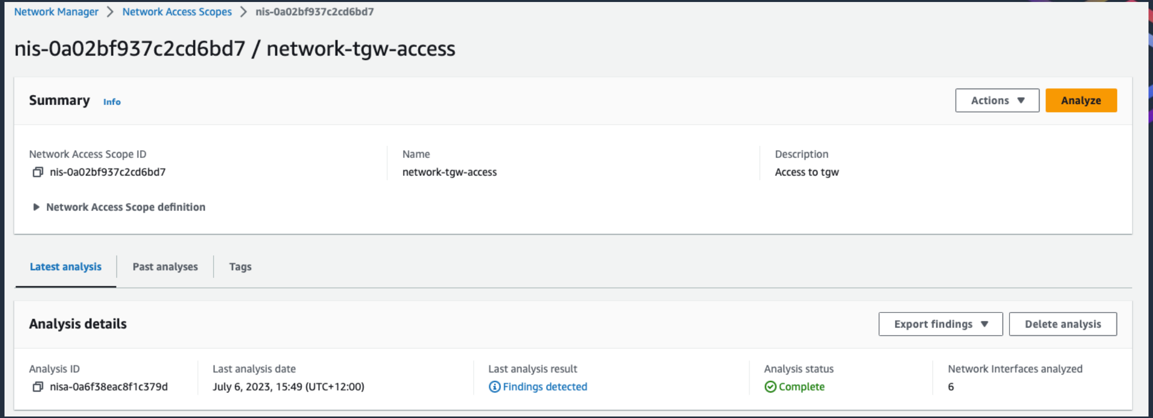
| Attached To | VPC | Subnet |
|---|---|---|
| i-0398b9c4f78e29bee | vpc-099fd31a9d803f91f | subnet-02e59fc2b08d92570 |

ENI_SG_RULES_MISMATCH:
None of the ingress rules in the following security groups apply: sg-070f0457aab82a80d. See sg-070f0457aab82a80d.

aws COMMUNITY DAY AOTEAROA

# Security Team: VPC Network Access Analyzer

- Understand network access on your resources
- Verify whether security requirements are met
- Demonstrate Compliance
- Verify trusted network paths, network segmentation & trusted network access



Network Manager > Network Access Scopes > nis-0a02bf937c2cd6bd7

nis-0a02bf937c2cd6bd7 / network-tgw-access

**Summary** Info

Network Access Scope ID: nis-0a02bf937c2cd6bd7

Name: network-tgw-access

Description: Access to tgw

▶ Network Access Scope definition

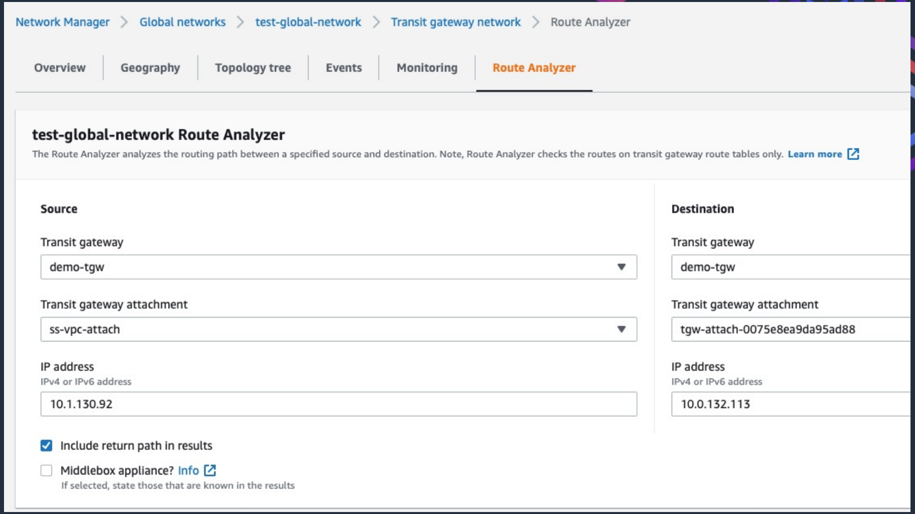
**Analysis details**

| Analysis ID | Last analysis date | Last analysis result | Analysis status | Network Interfaces analyzed |
|---|---|---|---|---|
| nisa-0a6f38eac8f1c379d | July 6, 2023, 15:49 (UTC+12:00) | Findings detected | Complete | 6 |

aws COMMUNITY DAY AOTEAROA

# Ops Team: Transit Gateway Route Analyzer

- AWS Transit Gateway – connect VPC’s from multiple internal and external accounts to your AWS environment.
- How do you test this?
- VPC -> Network Manager -> Create a Global Network -> Route Analyzer



Network Manager > Global networks > test-global-network > Transit gateway network > Route Analyzer

**test-global-network Route Analyzer**

The Route Analyzer analyzes the routing path between a specified source and destination. Note, Route Analyzer checks the routes on transit gateway route tables only. Learn more

**Source**

Transit gateway: demo-tgw

Transit gateway attachment: ss-vpc-attach

IP address (IPv4 or IPv6 address): 10.1.130.92

**Destination**

Transit gateway: demo-tgw

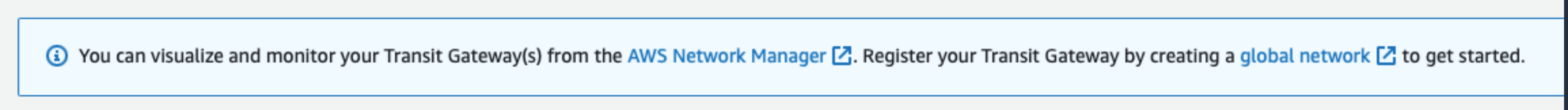
Transit gateway attachment: tgw-attach-0075e8ea9da95ad88

IP address (IPv4 or IPv6 address): 10.0.132.113

☑ Include return path in results

☐ Middlebox appliance? Info

If selected, state those that are known in the results



You can visualize and monitor your Transit Gateway(s) from the AWS Network Manager. Register your Transit Gateway by creating a global network to get started.

aws

COMMUNITY DAY

AOTEAROA

# Live Demo Time

# Additional Reading

Monitor your Network Load Balancers
Query NLBs with Athena

VPC Traffic Mirroring

Use 3rd party tools like Datadog: Datadog-VPC-Flow-Logs

Failover testing your Direct Connect connection

aws COMMUNITY DAY AOTEAROA

# Summary

Monitoring  - CloudWatch, S3, Athena, VPC Flow Logs
Testing – AWS Network Manager
Testing – VPC Reachability Analyser
Testing – VPC Network Access Analyser
Testing – Transit Gateway Route Analyser

aws COMMUNITY DAY AOTEAROA

# Thank You. Questions?

Find me @ ”Hitarth Asrani” on LinkedIn

aws

# COMMUNITY DAY

AOTEAROA

aws

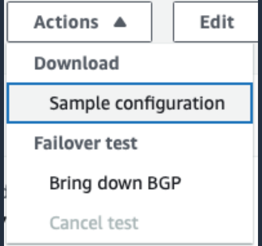
COMMUNITY DAY

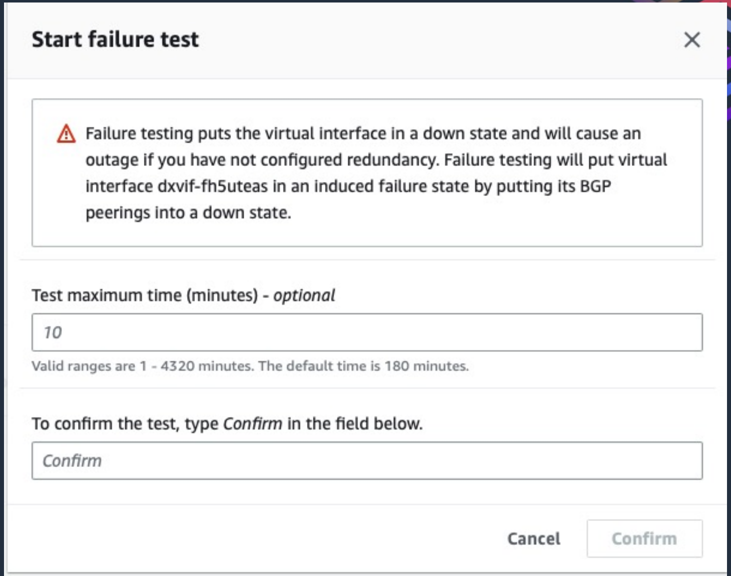
AOTEAROA

# Special Mention – Not in the live demo

Failover test your Direct Connect connections

- New news for me too.
- Test Virtual Interfaces (VIF's)
- Natively within AWS.
- This is probably an acceptance criteria for your highly available connections.




**Start failure test**

⚠ Failure testing puts the virtual interface in a down state and will cause an outage if you have not configured redundancy. Failure testing will put virtual interface dxvif-fh5uteas in an induced failure state by putting its BGP peerings into a down state.

Test maximum time (minutes) - *optional*

*10*

Valid ranges are 1 - 4320 minutes. The default time is 180 minutes.

To confirm the test, type *Confirm* in the field below.

*Confirm*