Monitoring & Testing Networks on AWS

Using native tools

Hitarth Asrani

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…

Agenda

10-15 mins talk, around 15 mins live demo

Introduction/Quick Recap of networking on AWS.

Monitoring networks using Cloudwatch and other tools on AWS

Testing your networks using 3 (or 4) different tools

Live Demo

Q&A / End

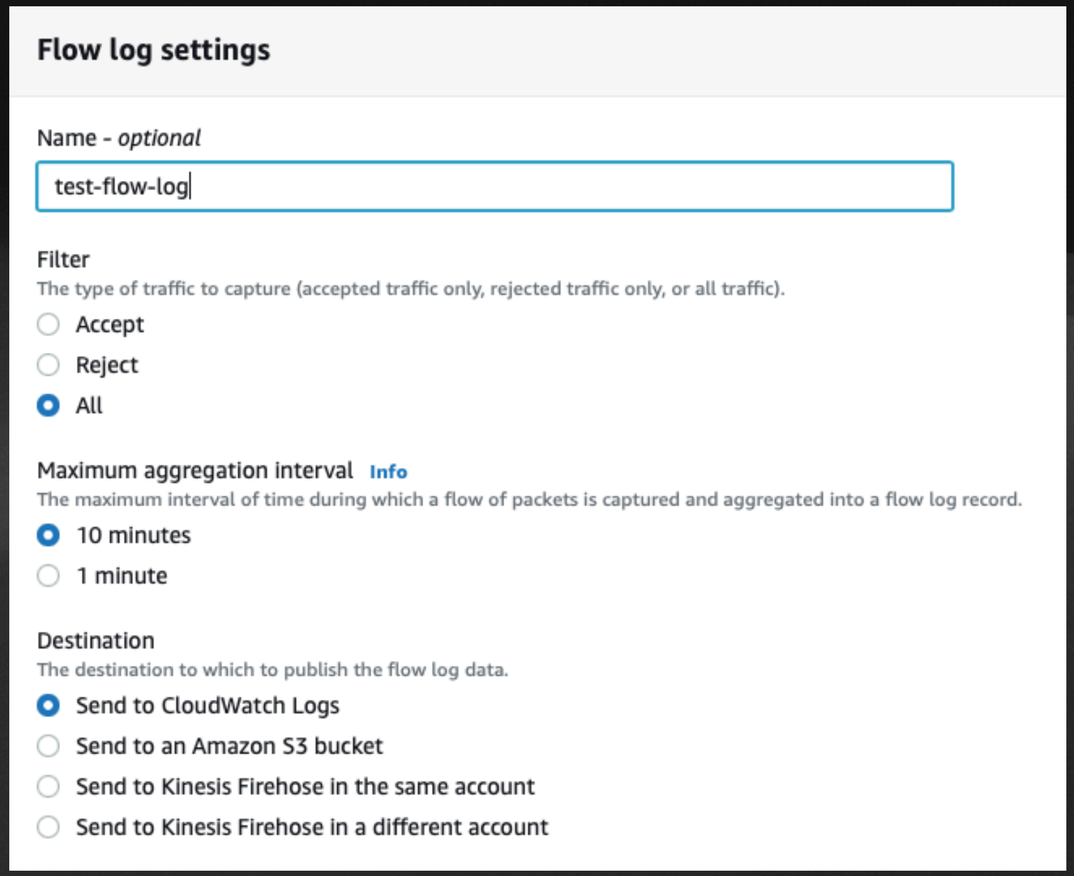
Networking on AWS Recap

VPC - Virtual Private Cloud
Subnets - segmented pieces of your VPC
Route Tables - Rules/Routes for your subnets or VPCs
Security Groups - set of rules for inbound and outbound traffic applied on resources

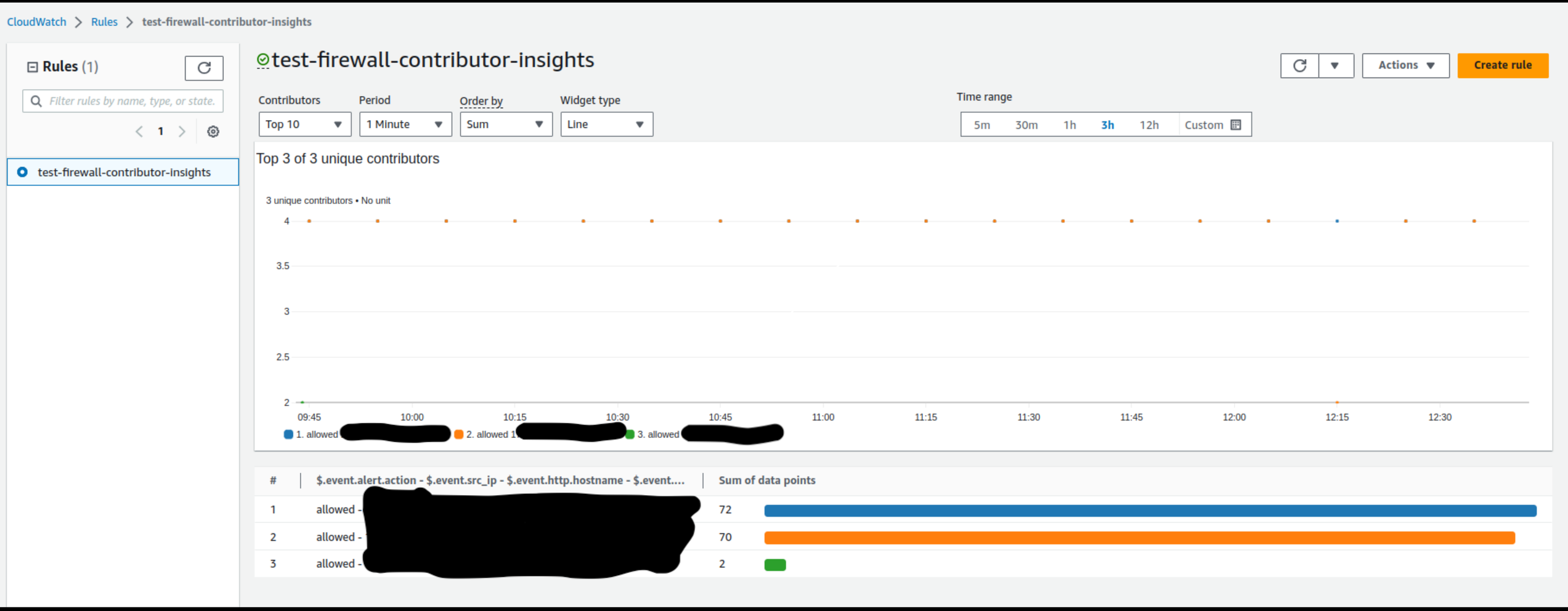
Monitoring Networks

Logs + (Cloudwatch or S3) = Fancy Charts

- Cloudwatch is your central place for anything monitoring on AWS
- VPC Flow logs capture …
- AWS Network Firewall can log to S3 or CW.
- Cloudwatch Contributor insights
- S3 + Athena can give you insights into logs on S3

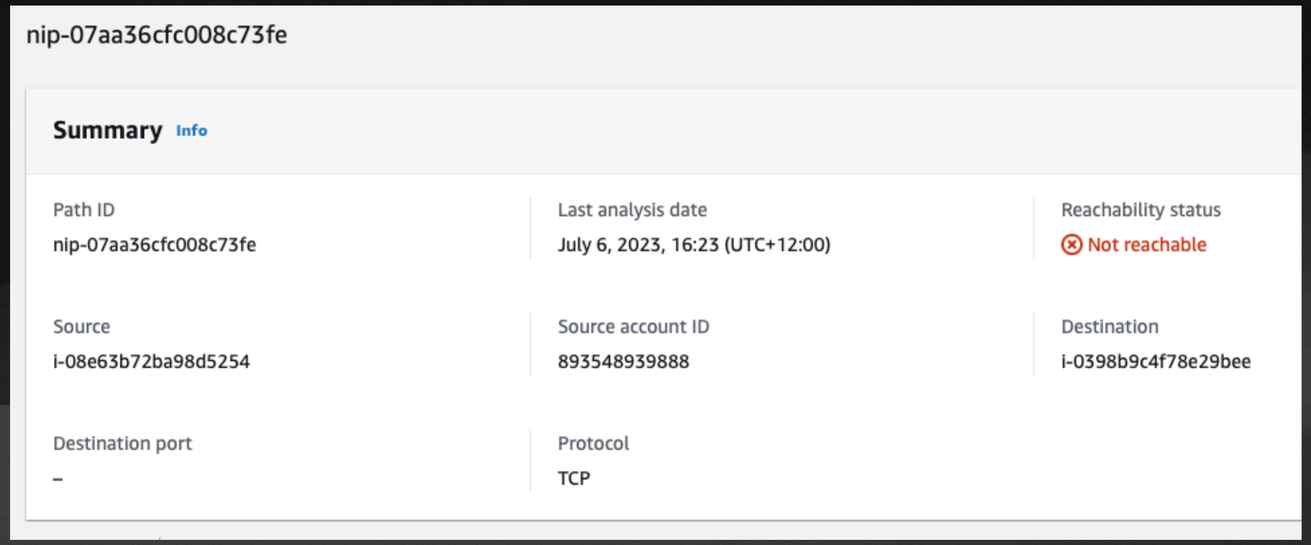


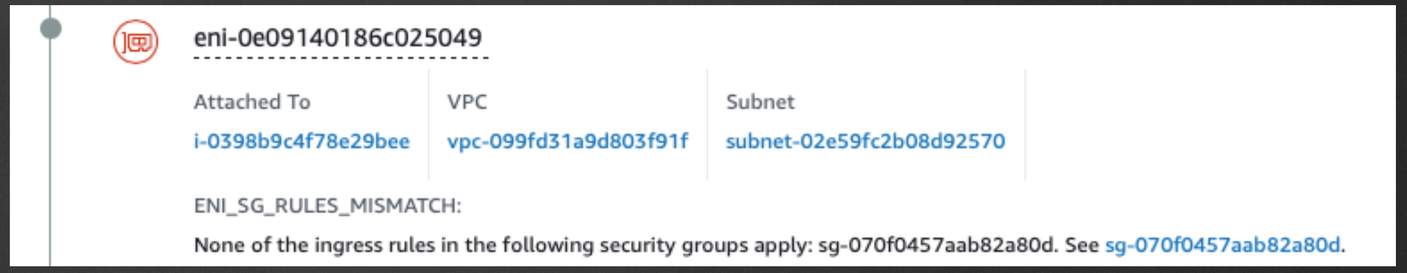
CloudWatch Contributor Insight Example



Testing Networks - I

VPC Reachability Analyser



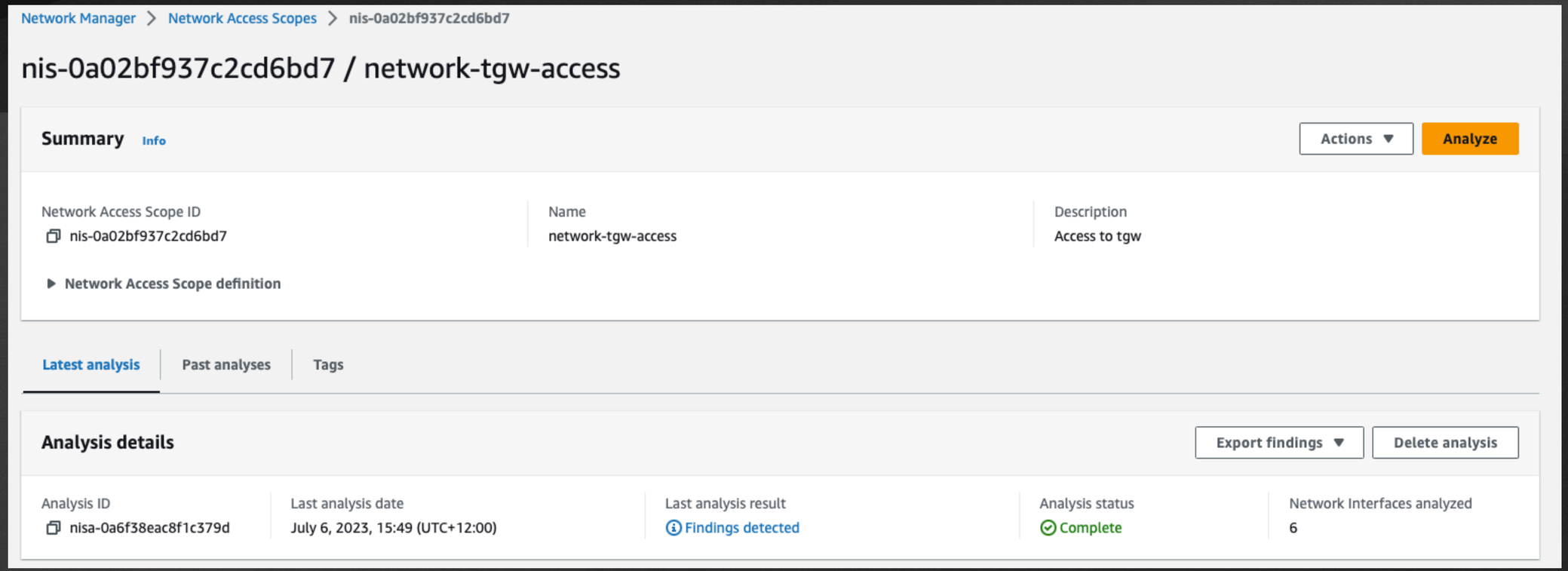


- Testing suite under AWS Network Manager
- Test connectivity between a source resource and destination resource
- Price per analysis (ap-se-2) - $0.10
- Troubleshoot, verify and automate verification of connectivity

Testing Networks - II

VPC Network Access Analyser

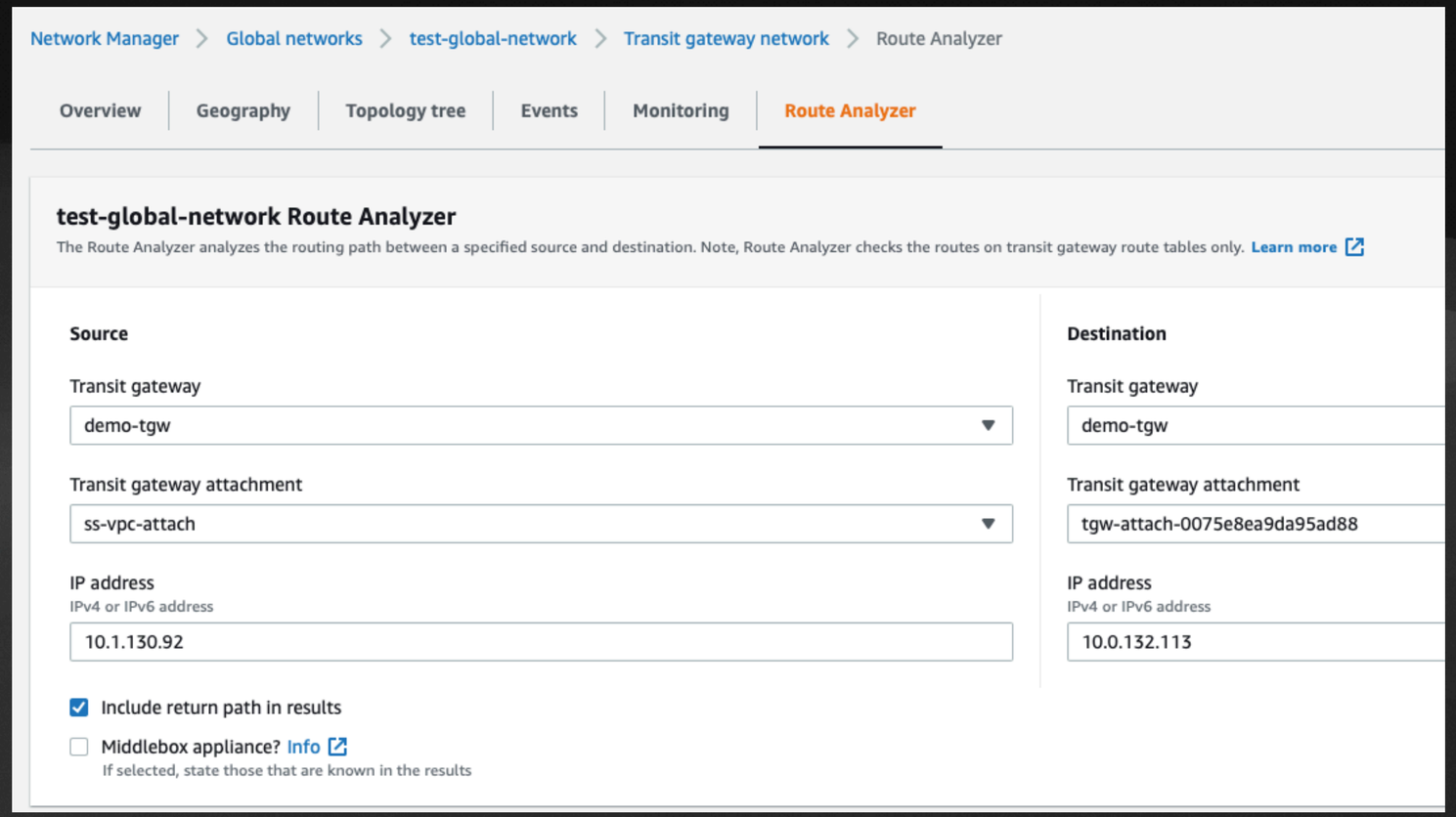
- Understand network access on your resources.
- Verify that this meets your security requirements
- Demonstrate Compliance

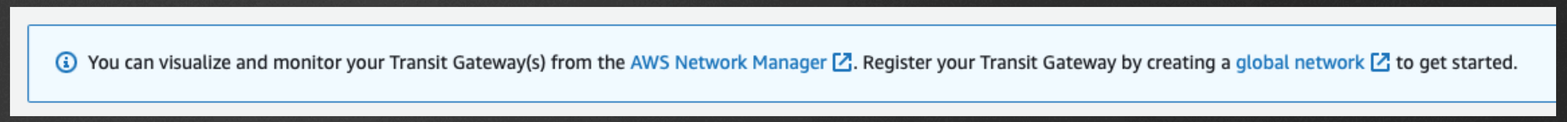


Testing Networks - III

TGW Route Analyser

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

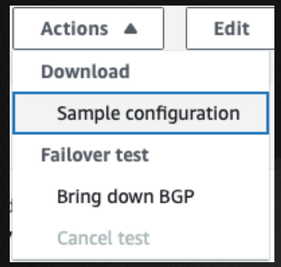


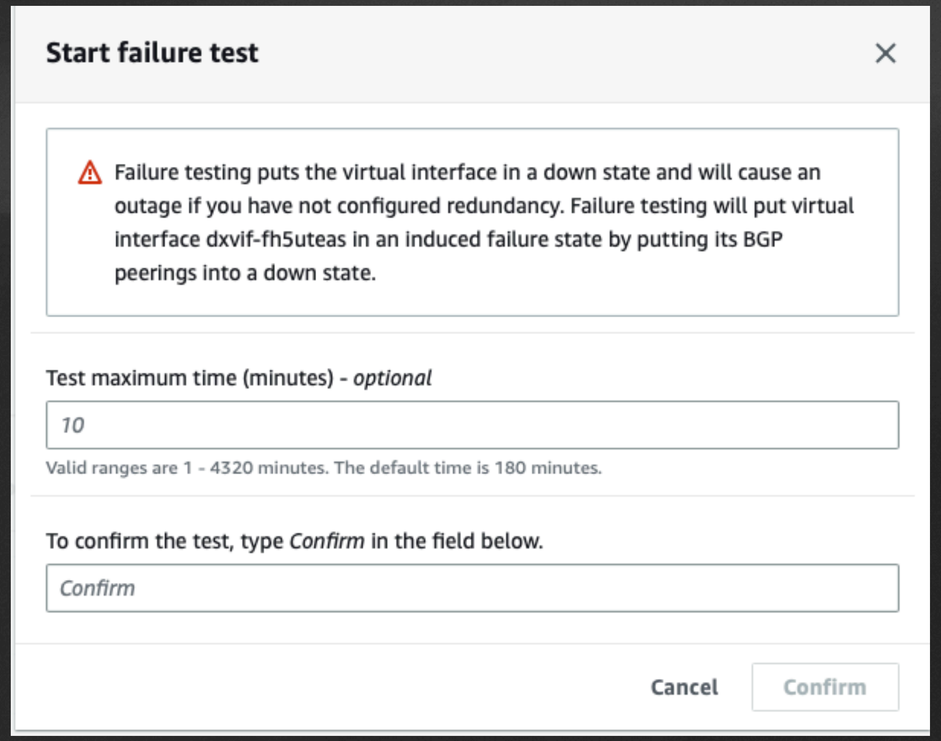


Bonus {not in the live demo :(}

Failover testing your Direct Connect connections

- I didn’t know this until recently.
- Test virtual interfaces
- You can failover-test your Direct Connect connections.
- This is probably one of your acceptance criteria for a HA connection between your on-prem and AWS.
- https://docs.aws.amazon.com/directconnect/latest/UserGuide/resiliency_failover.html





Live Demo Time

Thank You

Find me - “Hitarth Asrani” on LinkedIn