Packet Analysis in the Cloud

I can’t see in the rain

Matthew York
Advance7
Clouds are big and getting bigger
Cloud causing low visibility...

• SharkFest’16:

  “Packet capture in the cloud is tcpdump”

• SharkFest’18 Europe:

  “Packet capture in the cloud is tcpdump but that’s OK”
To manage or not to manage
Give me some packets
Scale this some

Things to Consider:
- Burst v Provision
- Lifecycle Management
- Instance Bandwidth
Your captures are killing me

• You’ve got a bunch of options:
  • Get a bigger instance
  • Use autoscaling groups
Your captures are still killing me

• What happens in a VPC:
What can we do?

• Do some NAT’ing
We’re using containers
Scale this more
What to do with the data
It’s not you, it’s me

Packet Capture Unit
e.g. server running dumpcap or Viavi GigaStor
What’s next?

• Filling in the gaps
• Increase parallelism and reduce uptime on analysis
Questions