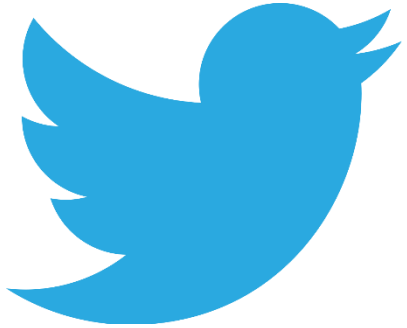
# Q&A: Common Questions About AWS VPCs



@nigelpoulton

# Question:

## What is the biggest/most common mistake people make with AWS VPCs?

## A: Getting the network range (CIDR block) wrong

- Make sure it's not already in use on your existing networks
- Talk to your network team and get them involved
- Treat your VPC network addresses the same way you treat your existing corporate networks

# Question:

## What is the most misunderstood AWS VPC concept?

## A: Private and Public IPs

- Instances don't know about Public IPs
- Public IPs are implemented on Internet Gateways (IGW)
- Use Elastic IPs (EIP) for public IP addresses that won't change

# Question:

Should multiple environments (dev, test, UAT, prod etc.) be in a single VPC?

A: No　Nein　Non　没有　κανένα　Het

# Question:

## Which of the two should I use: Network ACLs or Security Groups?

A: Both!

- Think *defence in depth*
- Protect at the subnet level with Network ACLs
- Protect at the Instance level with Security Groups
- Feel free to also use additional 3rd party security technologies

# Question:

## How do I mitigate against AWS outages?

A: Spread services over as much of AWS as possible

- Spread across Availability Zones (AZ)
- Spread across Regions
- Spread across cloud platforms

# Question:

## When should I use public subnets, and when should I use private subnets?

## A: Use public subnets sparingly (not very often/don't put too much in them)

- Try to use public subnets just for things like:
  - load balancers
  - firewalls
  - proxy servers
  - …

# Coming Up Next…

## Course Summary and "What Next"