One Network to rule them all

Netnod 2018, 14-15 Mar

Christian Adell

Networking nowadays

Challenges

- Scalability
- Containerisation
- Distributed Systems
- Multi-platform, Cloud
- High Performance applications
- Efficiency

Traditional network architectures/operations are not good enough

Are we ready?

- Multi-vendor with legacy devices not well-suited for automation
- There is a lot of new things to learn
- Vendor trainings aren’t (weren’t) focused on this
- Automation amplifies everything (including mistakes)
- Usually, not close to developers, to the business

And most of the times, we don’t know where to start from…

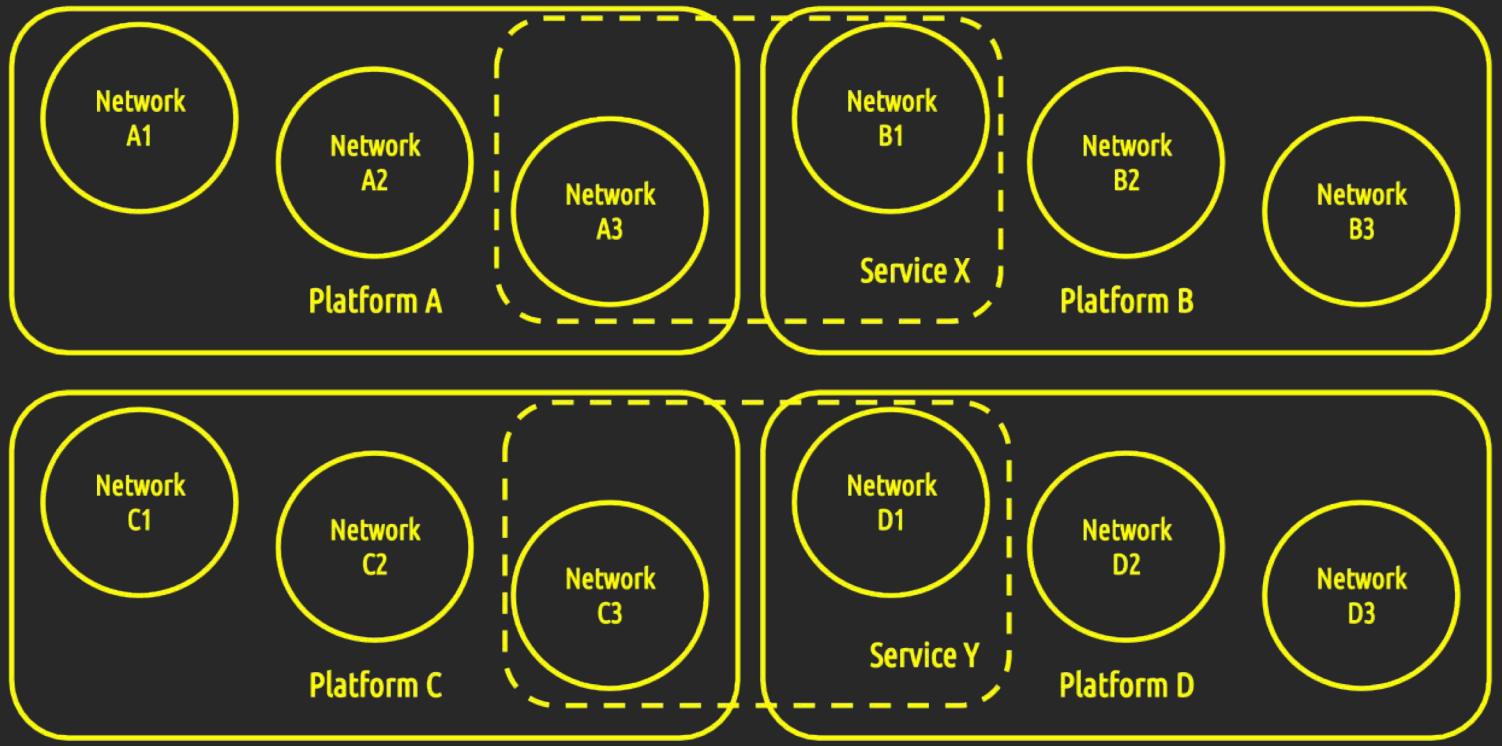
How can we approach it?

- APIs everywhere, your network devices should support them
- Use Data Models, they will help you translate your will
- Take advantage of the information your network is providing
- Don't fear dynamic infrastructure
- Some coding skills will be needed
- Validate, validate and validate again

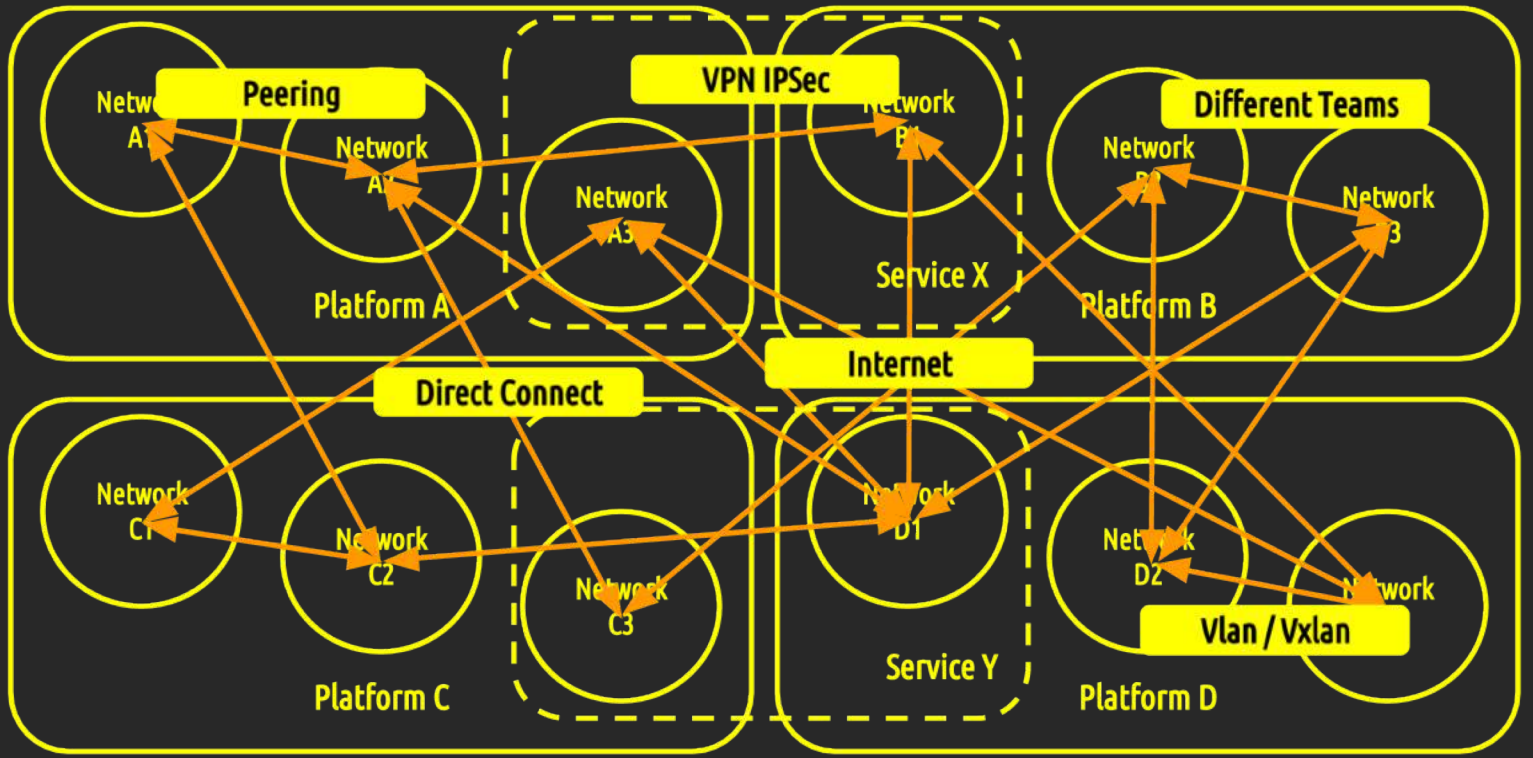
Start by solving simple problems... keeping applications on your focus

A brief story of a network service

Typical IT ecosystem



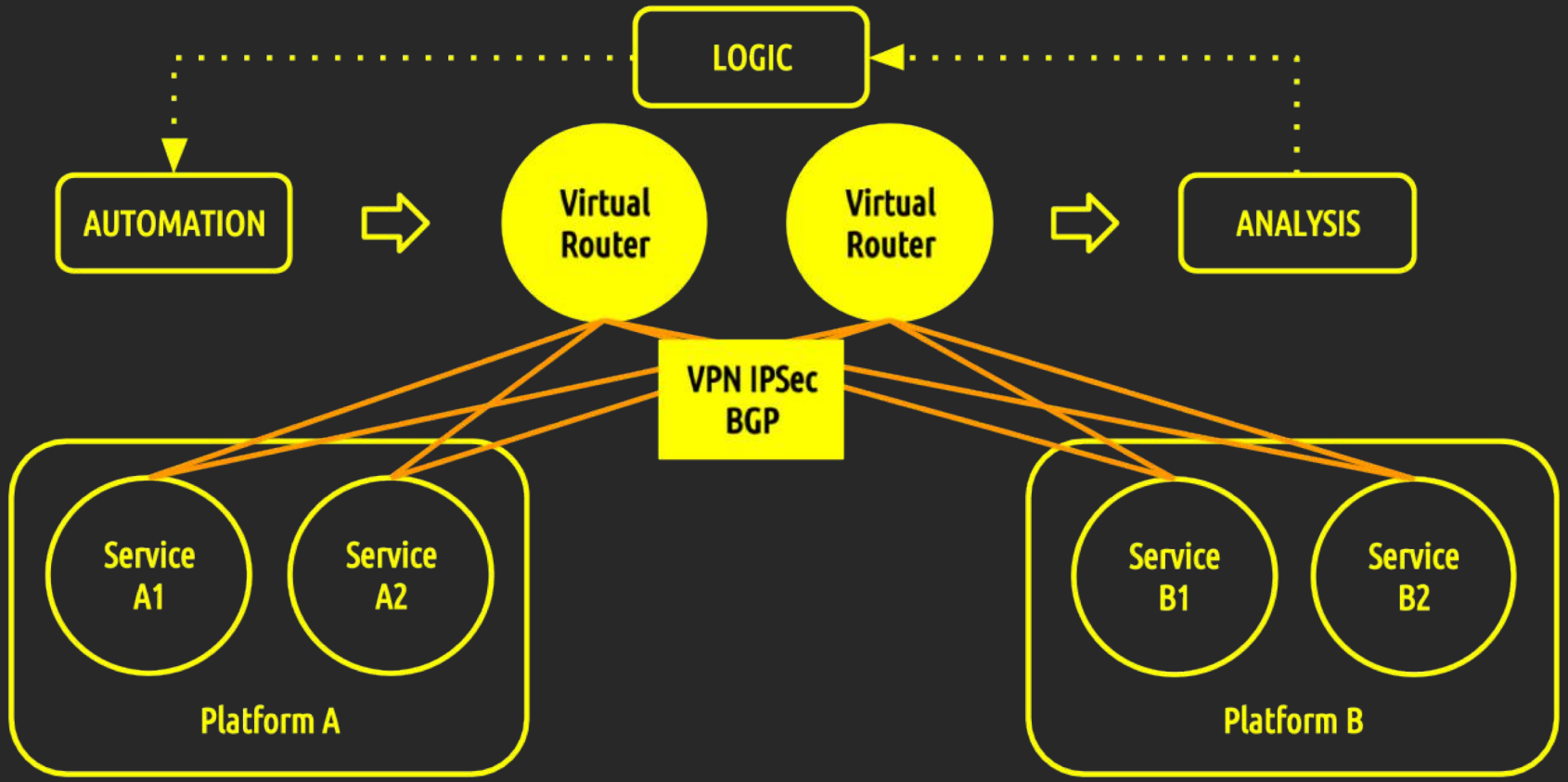
How the network looks like



Downsides

- By default, inter/intra platform communications use Internet which is not (always) the most performant, secure and cheapest communication channel
- Manual network provisioning doesn’t work in terms of speed and reliability
- Prone to errors and lack of consistency
- Some communications still need network layer security (no TLS)

We tried to solve all in one

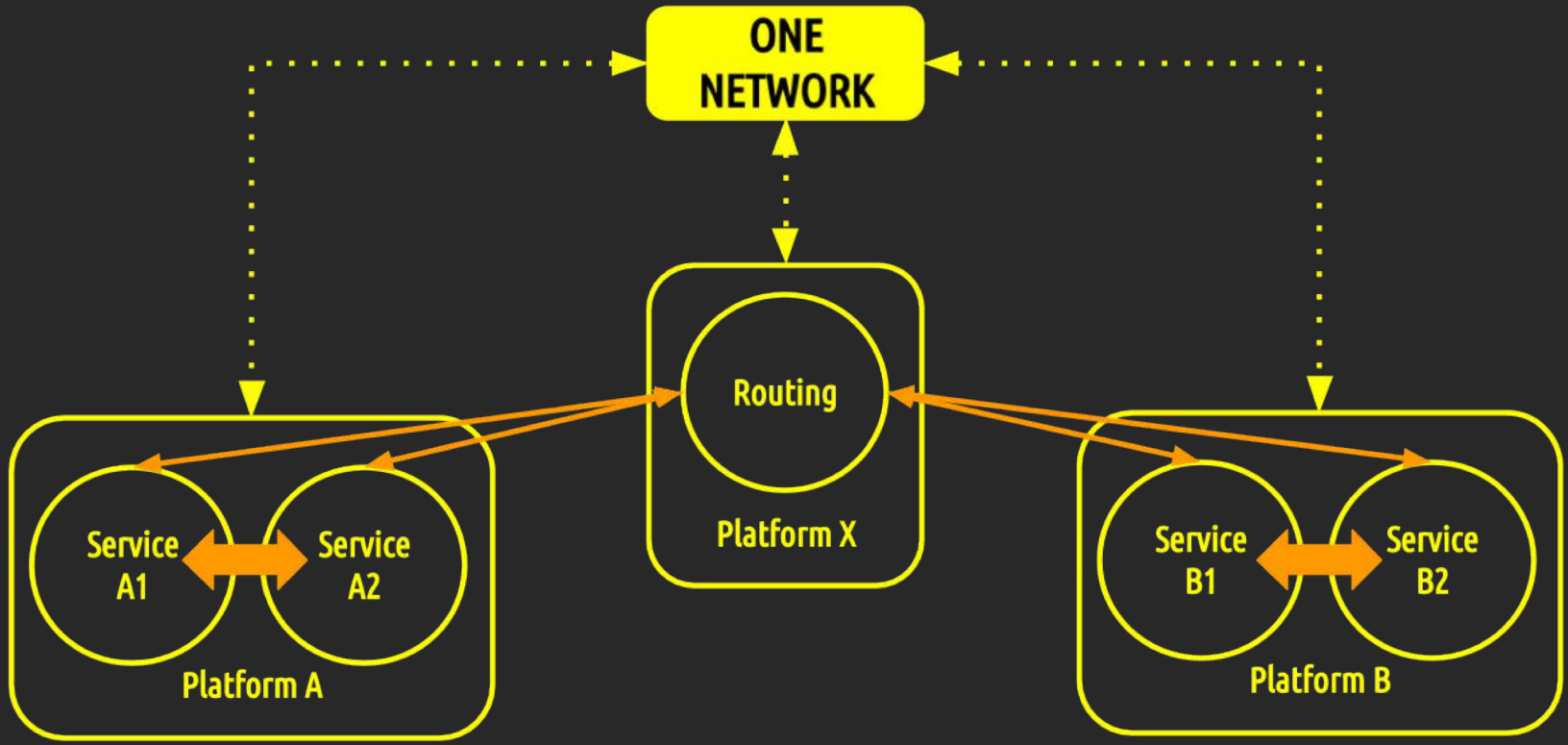

LOGIC
AUTOMATION
Virtual Router
Virtual Router
ANALYSIS
VPN IPSec BGP
Service A1
Service A2
Platform A
Service B1
Service B2
Platform B

… and we failed

(non-technical) Lessons learned

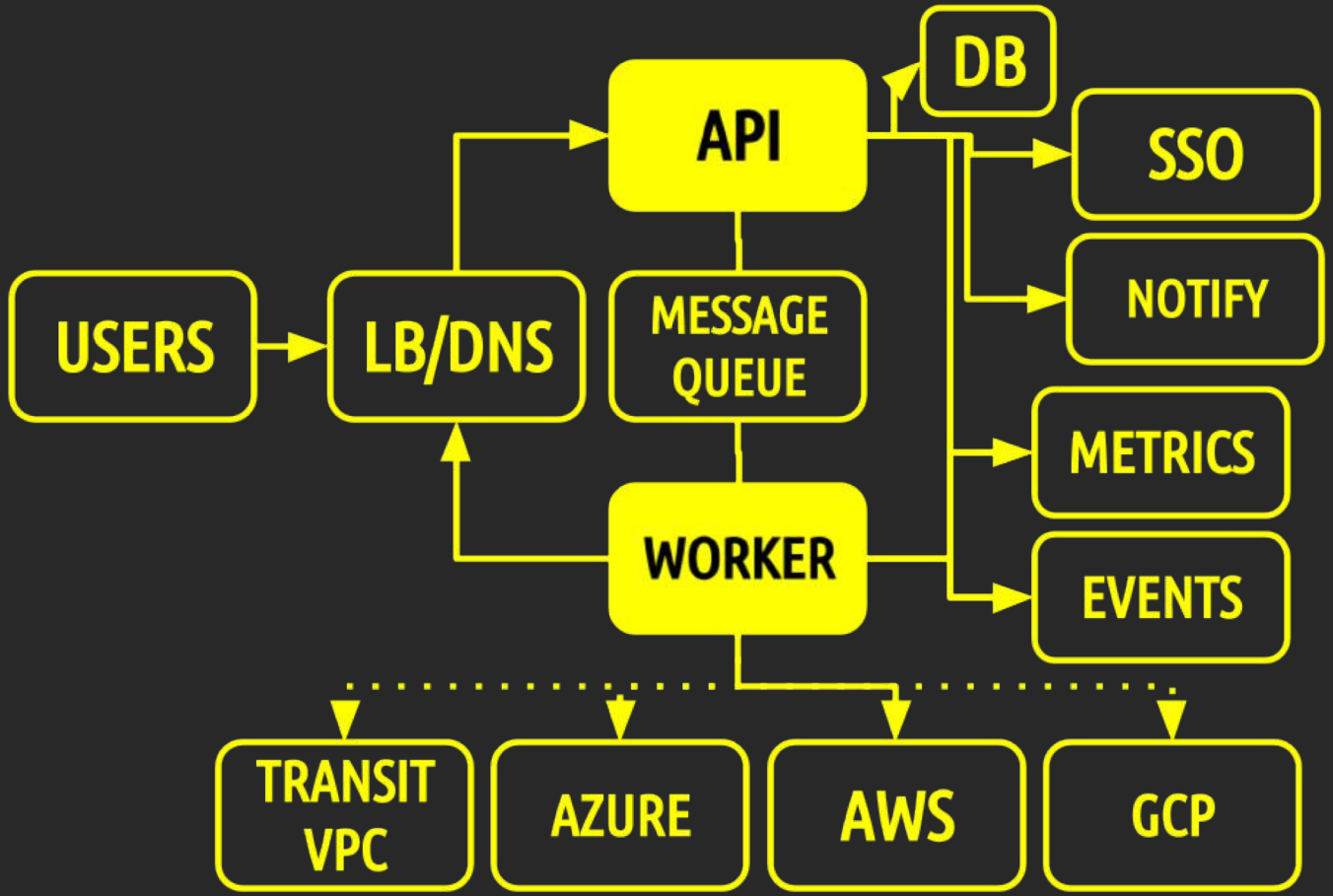
- Think as your users will do
- Get feedback as soon as possible, iterate!
- The solution should flexible enough to accommodate several underlying solutions
- Evaluate current needs case-per-case (capability, performance, cost, etc.)
- Apply Pareto Rule, focus on solving most urgent needs first

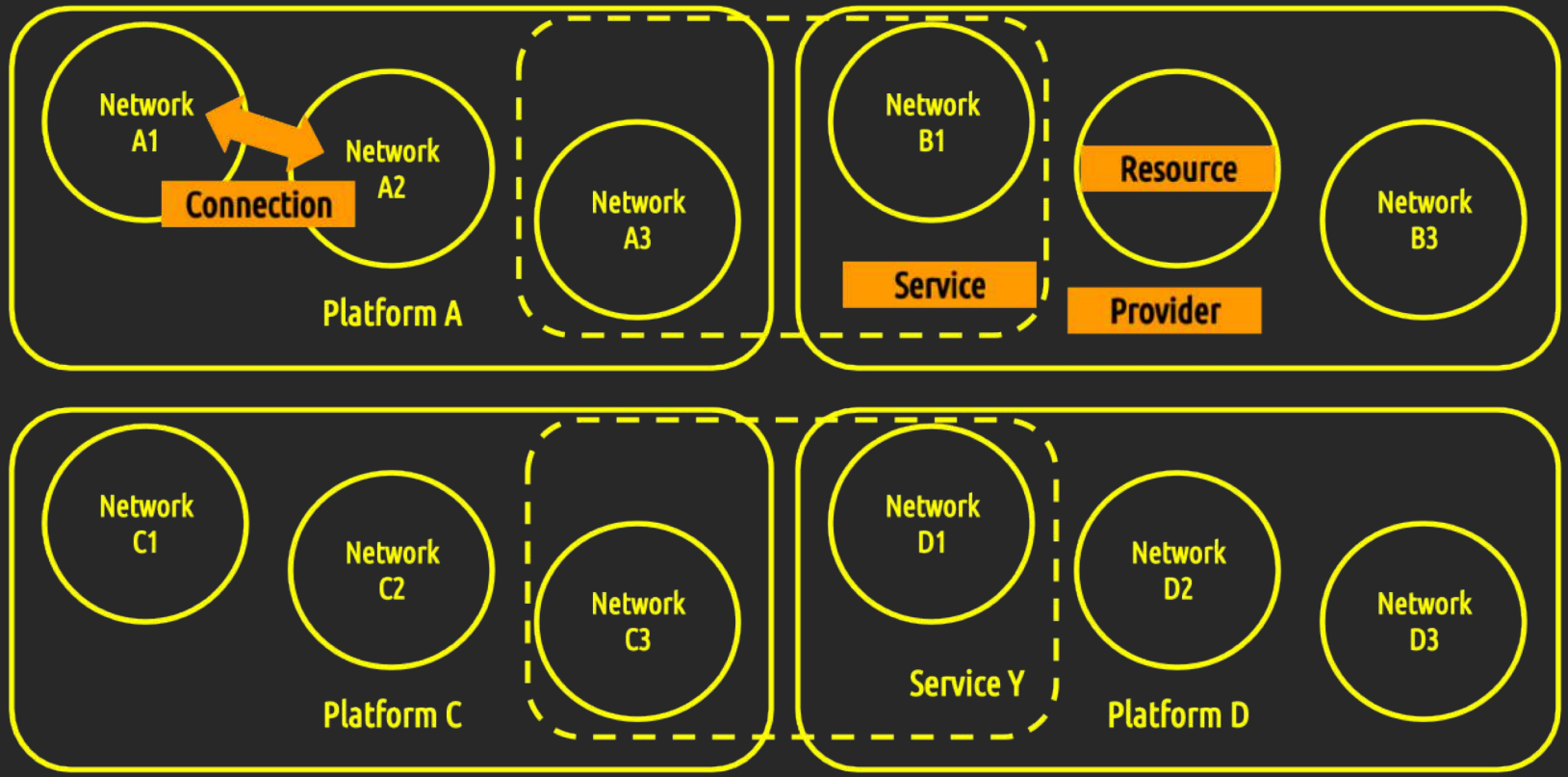
Then, we created a network service


ONE
NETWORK
Routing
Platform X
Service
A1
Service
A2
Platform A
Service
B1
Service
B2
Platform B

Requirements

- Easy onboarding / self serve
- Users should be autonomous to handle connections
- Abstract all network details from users and pick the best option in every case
- Support several providers/platforms
- Offer a secure service
- Continuous monitoring of connection status


DB
API
SSO
NOTIFY
USERS
LB/DNS
MESSAGE QUEUE
METRICS
WORKER
EVENTS
TRANSIT VPC
AZURE
AWS
GCP


Network A1
Network A2
Connection
Network A3
Platform A
Network B1
Resource
Network B3
Service
Provider
Network C1
Network C2
Network C3
Platform C
Network D1
Network D2
Network D3
Service Y
Platform D

SERVICE


```
{
   u'owners':[
      u'1ed3aef1-3e4d-4372-95e1-0890a1148a48'
   ],
   u'name':u'Dummy Service Name',
   u'providers':[
      u'6445dbee-3eaa-4911-b387-1ee79805f75e'
   ],
   u'id':u'd44ff67c-9ebf-4a96-b9f0-55336860f6b6',
   u'resources':[
      u'14b586c7-7b2a-4469-ba11-743a0d7ce219'
   ],
   u'description':u'Dummy service for testing purposes'
}
```


PROVIDER


```
{
   u'account':u'1111111111',
   u'name':u'Dummy Provider Name',
   u'service':u'd44ff67c-9ebf-4a96-b9f0-55336860f6b6',
   u'region':u'ap-southeast-1',
   u'id':u'6445dbee-3eaa-4911-b387-1ee79805f75e',
   u'provider_type':u'AWS'
}
```

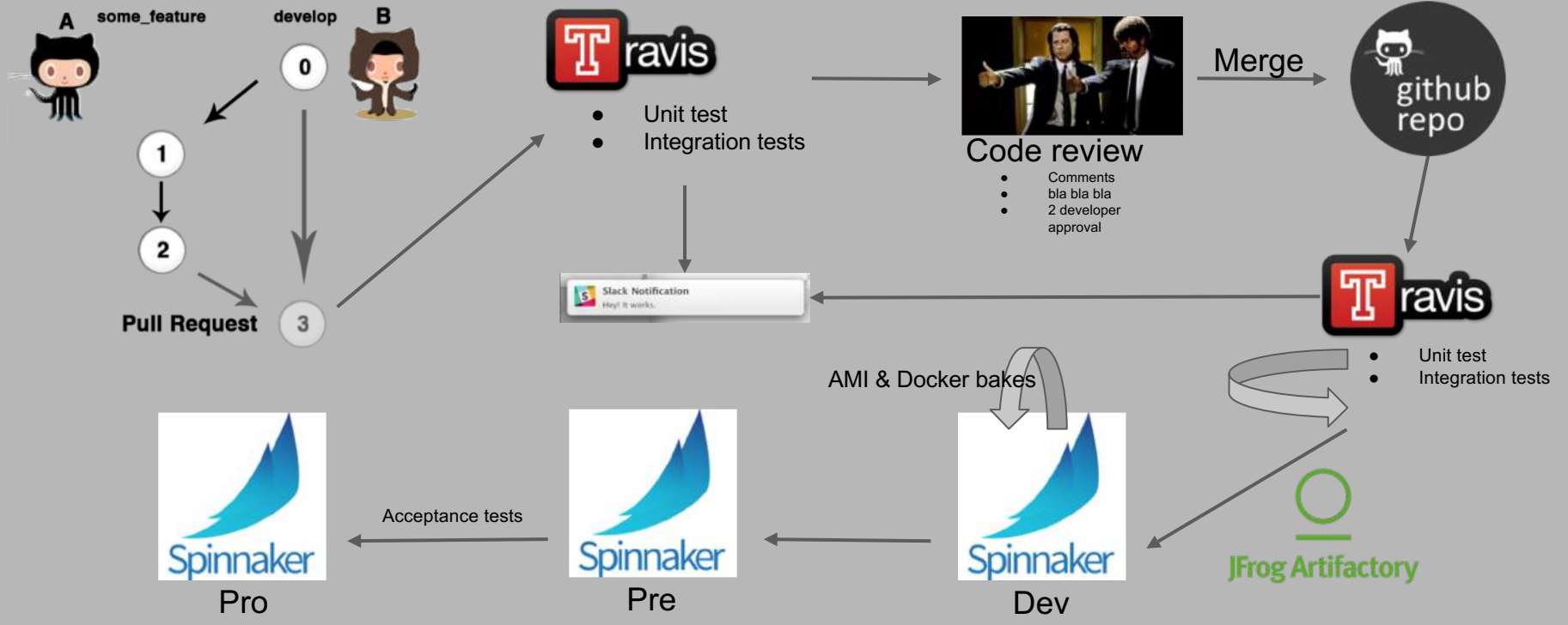

CONNECTION


```
{
   u'state':u'ESTABLISHED',
   u'name':u'Dummy Connection Name',
   u'desired_state':u'ESTABLISHED',
   u'id':u'e975ecfd-9bd6-4ea3-ab56-6193bb752cba',
   u'resource_left':u'14b586c7-7b2a-4469-ba11-743a0d7ce219',
   'details':{
      u'peering_id':u'pcx-1a1a1a1a'
   },
   u'resource_right':u'342ac6d7-74fd-4290-a52c-fbdd325b95ef',
   u'ctype':u'AWS_PEERING'
}
```


RESOURCE

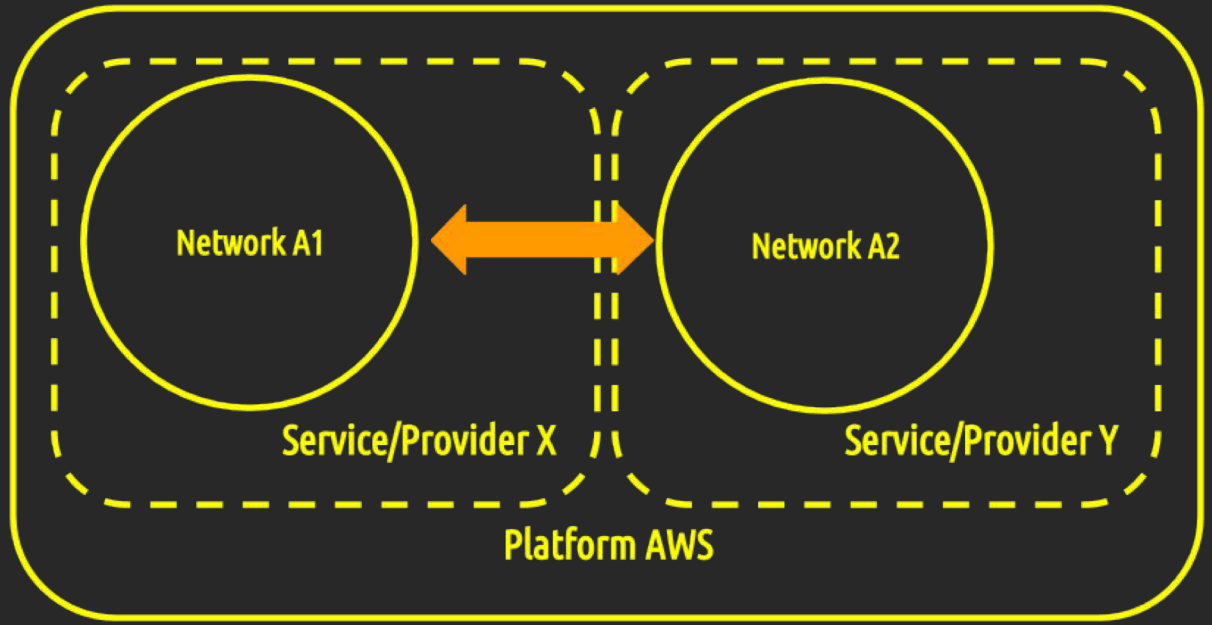

```
{
   u'subnet':u'10.69.249.192/28',
   u'name':u'AWS\\vpc-1a1a1a1a',
   u'service':u'd44ff67c-9ebf-4a96-b9f0-55336860f6b6',
   u'l4filters':[ ],
   u'provider':u'6445dbee-3eaa-4911-b387-1ee79805f75e',
   u'id':u'14b586c7-7b2a-4469-ba11-743a0d7ce219'
}
```

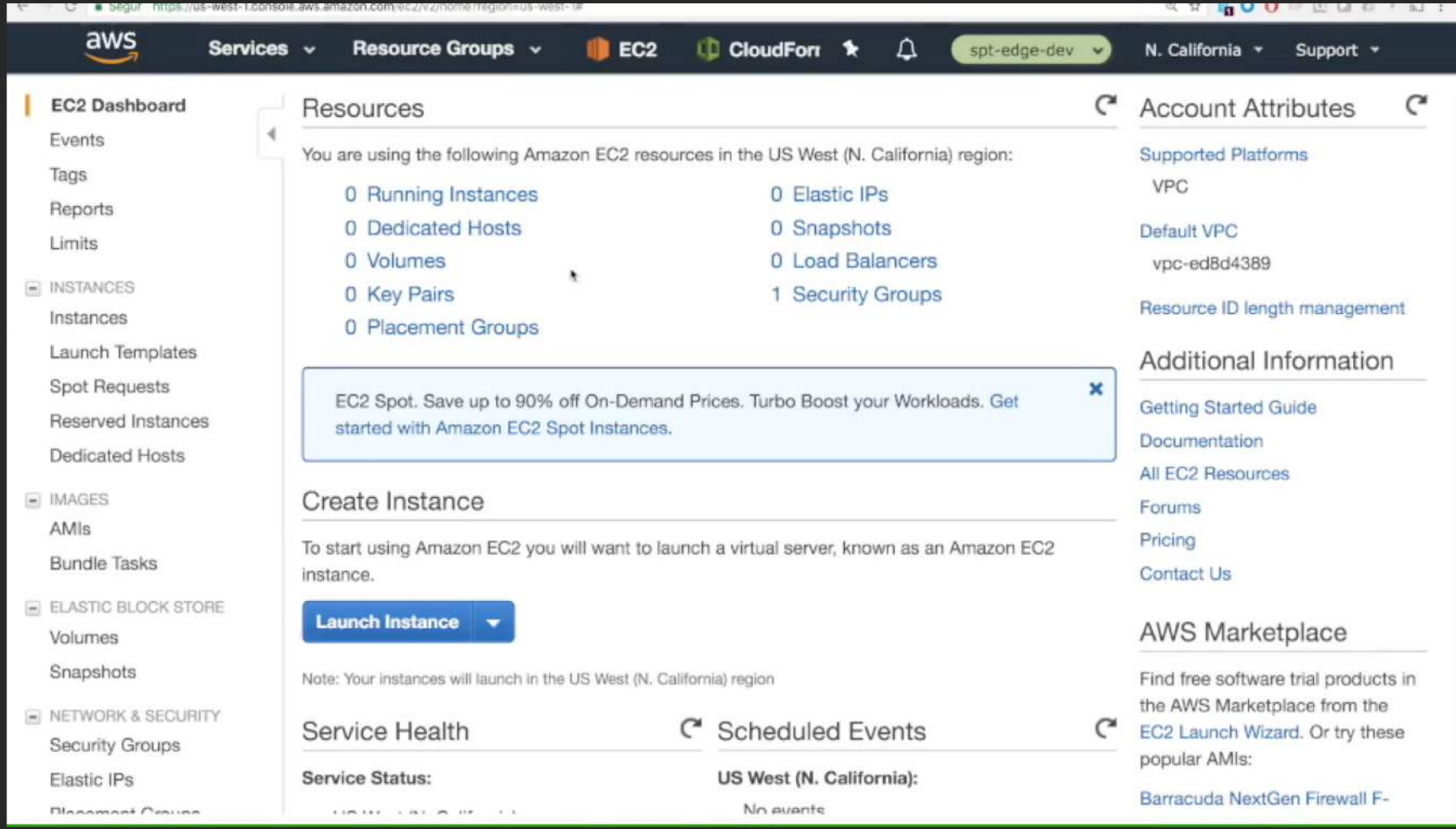
Continuous Integration & Deployment



Demo

Scenario


Network A1
Network A2
Service/Provider X
Service/Provider Y
Platform AWS


aws
Services
Resource Groups
EC2
CloudFor
spt-edge-dev
N. California
Support
EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Launch Templates
Spot Requests
Reserved Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Resources
You are using the following Amazon EC2 resources in the US West (N. California) region:
0 Running Instances
0 Dedicated Hosts
0 Volumes
0 Key Pairs
0 Placement Groups
0 Elastic IPs
0 Snapshots
0 Load Balancers
1 Security Groups
EC2 Spot. Save up to 90% off On-Demand Prices. Turbo Boost your Workloads. Get started with Amazon EC2 Spot Instances.
Create Instance
To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.
Launch Instance
Note: Your instances will launch in the US West (N. California) region
Service Health
Service Status:
Scheduled Events
US West (N. California):
No events
Account Attributes
Supported Platforms
VPC
Default VPC
vpc-ed8d4389
Resource ID length management
Additional Information
Getting Started Guide
Documentation
All EC2 Resources
Forums
Pricing
Contact Us
AWS Marketplace
Find free software trial products in the AWS Marketplace from the EC2 Launch Wizard. Or try these popular AMIs:
Barracuda NextGen Firewall F-

Why our developers use it?

- They don't care about underlying network details
- They always use the best possible network solution
- They have one API to handle everything
- They are notified about connections' health
- They need an out-of-the-box multiple platform connectivity
- They get visibility about network dependencies

Takeaways

- Don’t be afraid of going out of your comfort zone
- Learning coding will give you superpowers
- At some point, you will need to join pieces
- Adopting a DevOps approach will speed up your business (and career)
- Networking is a key skill in IT, bring it close to the business

Thanks for your attention

Related material

Some learning stuff: https://github.com/chadell/learning

Q/A