DevOps Art #1 : Migration

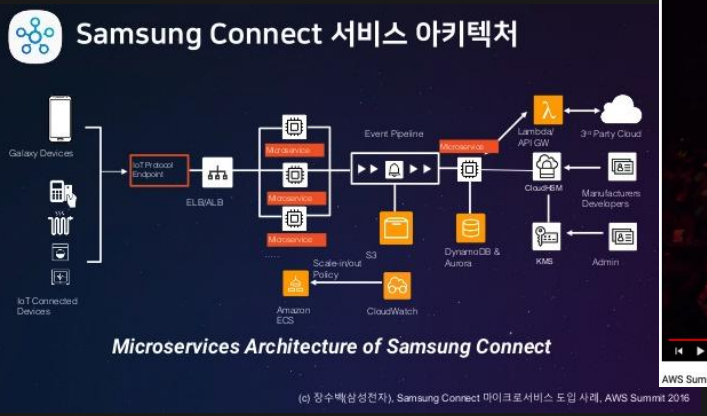
beNX

Devops Enginner

Introduction

- Samsung Knox
- Samsung Smartthings
- Samsung Account
- Bighit Group beNX

AWS Cloud 와 함께



(c) 장수백(삼성전자), Samsung Connect 마이크로서비스 도입 사례, AWS Summit 2016

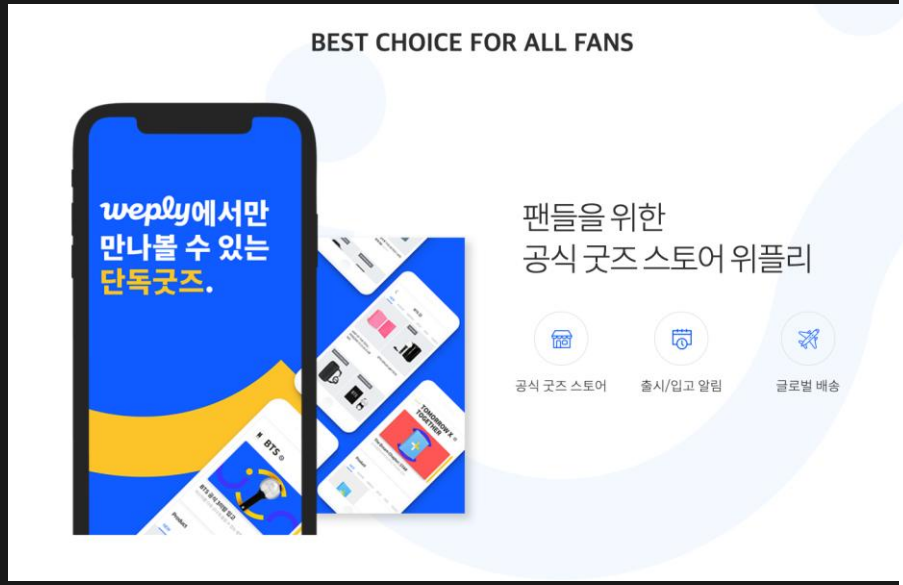
AWS Summit Seoul 2019 | 기조연설 - 정재연 상무(삼성전자)

AWS Container Day

[2:00 ~ 3:00] **도커의 기초**, AWS 김상필 SA
[3:00 ~ 3:30] **Case study - 삼성전자**, 송주영 선임
[3:30 ~ 3:50] **휴식시간**
[3:50 ~ 4:20] **Case study - Goorm IDE**, 남유석 개발팀장
[4:20 ~ 4:50] **Case study - VINGLE**, 조휘철 Software Engineer
[4:50 ~ 5:00] **휴식시간**
[5:00 ~ 6:00] **EC2 Container Service DeepDive** AWS 김기완 SA

AWS Container Day

beNX Service - weply.io



Overview

- Background
- What is Devops ?
- Migration
- Q&A

Background

- 9억명 사용자 멤버쉽 서비스
- 글로벌 서비스
- 무중단
- Cloud, On-Premise
- 2018. 7 ~ 2019. 4
- 4~7 명
- 10년 부채

- 수십만, 동접자 수만명 커머스 서비스
- Peak Traffic
- 글로벌 서비스
- 확장 가능성
- 2019. 3 ~ 2019. 6
- 2명
- 1년 부채

What is Devops?

- Culture
- Automation
- Measurement
- Sharing
- File up / Pile up

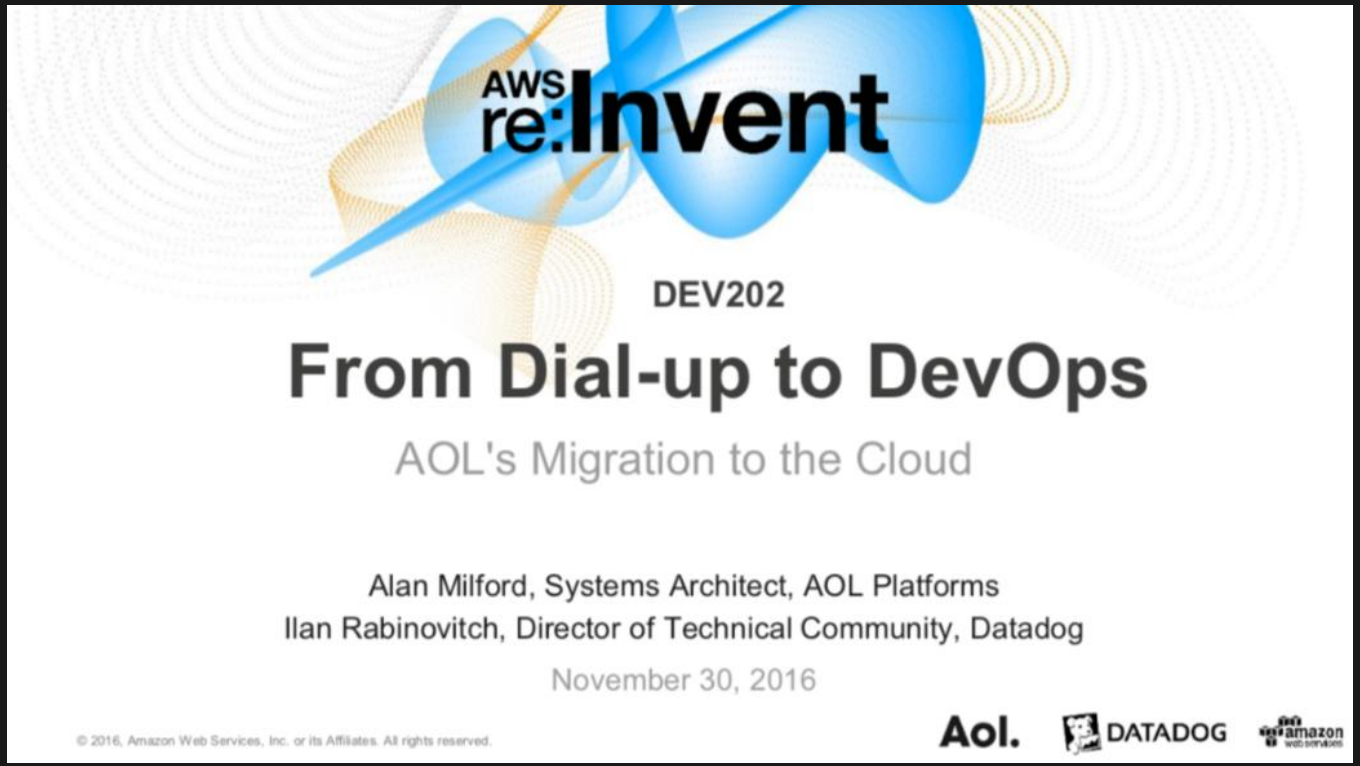
John Willis(@botchagalupe), Damon Edwards(@damonedwards)
Juyoung Song(@jupitersong)

What is Devops?

- Culture
- Automation
- Measurement
- Sharing
- File up / Pile up

John Willis(@botchagalupe), Damon Edwards(@damonedwards)
Juyoung Song(@jupitersong)

다른곳은?

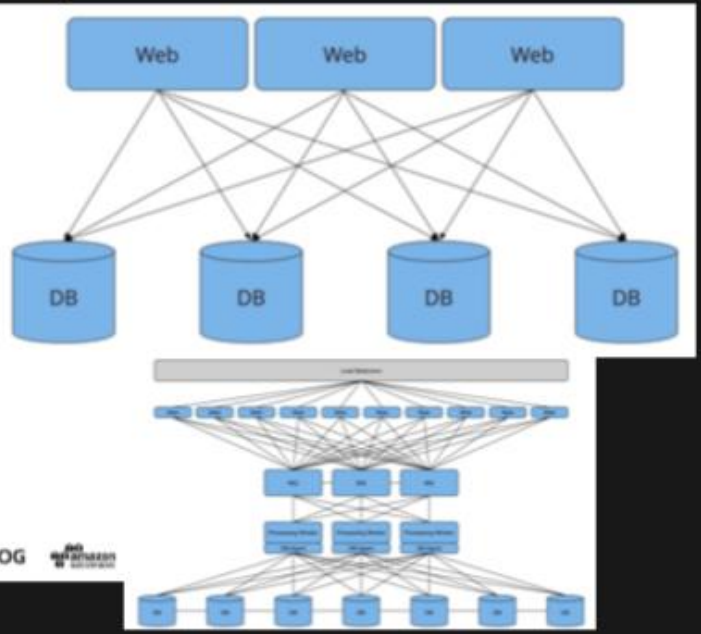

AWS re:Invent
DEV202
From Dial-up to DevOps
AOL's Migration to the Cloud
Alan Milford, Systems Architect, AOL Platforms
Ilan Rabinovitch, Director of Technical Community, Datadog
November 30, 2016
© 2016, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
Aol.
DATADOG
amazon web services

AOL? DevOps?

- 1983~, 2010~
- 68 acquisitions , 15 advertising companies
- Online advertising across Desktop, Mobile, TV
- So ...

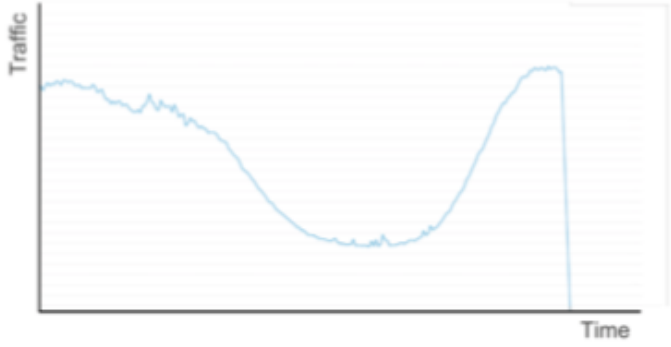
What that looks like internally

- Many complex systems
- High traffic, low latency response
- Downtime isn't an option
- Every transaction has a cost and value



Aol. DATADOG

Wait, what?



Aol. DA

What happened?

- Complete data centre outage (not our facility)
- Servers powered up in random order
- Data corruption
- Recovery time was out of our hands

Aol. DATADOG amazon

"Success consists of going from failure to failure without loss of enthusiasm."

Winston Churchill

Culture - Migration 준비, 첫번째

- 사람
- 프로세스
- 팀 구성, 서비스 성격
- 도구
- 일정

Culture - Migration 준비, 첫번째

- 사람 : 리더, 인원
- 프로세스 : 비용
- 팀 구성, 서비스 : 조직과 서비스의 성격
- 도구 : Trade off 기술 vs 속도 vs 편의성
- 일정 : 변경가능성, 보고

DevOps Tools

- AWS
- Infrastructure as a code : Terraform, Packer 
- C.I Tools : Gitlab CI, Circle CI, Jenkins 
- Deployment : Ansible, Custom script(python), Spinnaker 
- Communication : JIRA, Confluence, Slack 

What is Devops?

- Culture
- Automation
- Measurement
- Sharing
- File up / Pile up

John Willis(@botchagalupe), Damon Edwards(@damonedwards)
Juyoung Song(@jupitersong)

Automation - Migration 준비, 두번째

- Accounts / Security / Accessbility
- App / Language / Architecture
- CI / CD
- Monitoring
- Security

SEC303

Architecting Security & Governance across your AWS Landing Zone

Sam Elmalak
Solutions Architect
Amazon Web Services

David Ninnis
Senior Enterprise Architect, Cloud
BP

ENT350

AWS Landing Zone Deep Dive

Hitendra Nishar
Solutions Builder
AWS

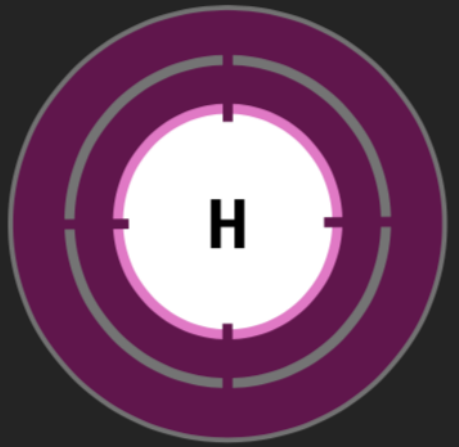
Lalit Grover
Solutions Builder
AWS

Brandon Bouier
Solutions Architect
AWS

Sherry Fairbank
Business Development
AWS

You need a “Landing Zone”

- A configured, secure, scalable, multi-account AWS environment based on AWS best practices
- A starting point for net new development and experimentation
- A starting point for customers’ application migration journey
- An environment that allows for iteration and extension over time



What you get with the AWS Landing Zone

Account Management

- Framework for creating and baselining a multi-account environment
- Initial multi-account structure including security, audit, & shared service requirements
- An account vending machine that enables automated deployment of additional accounts with a set of security baselines

---

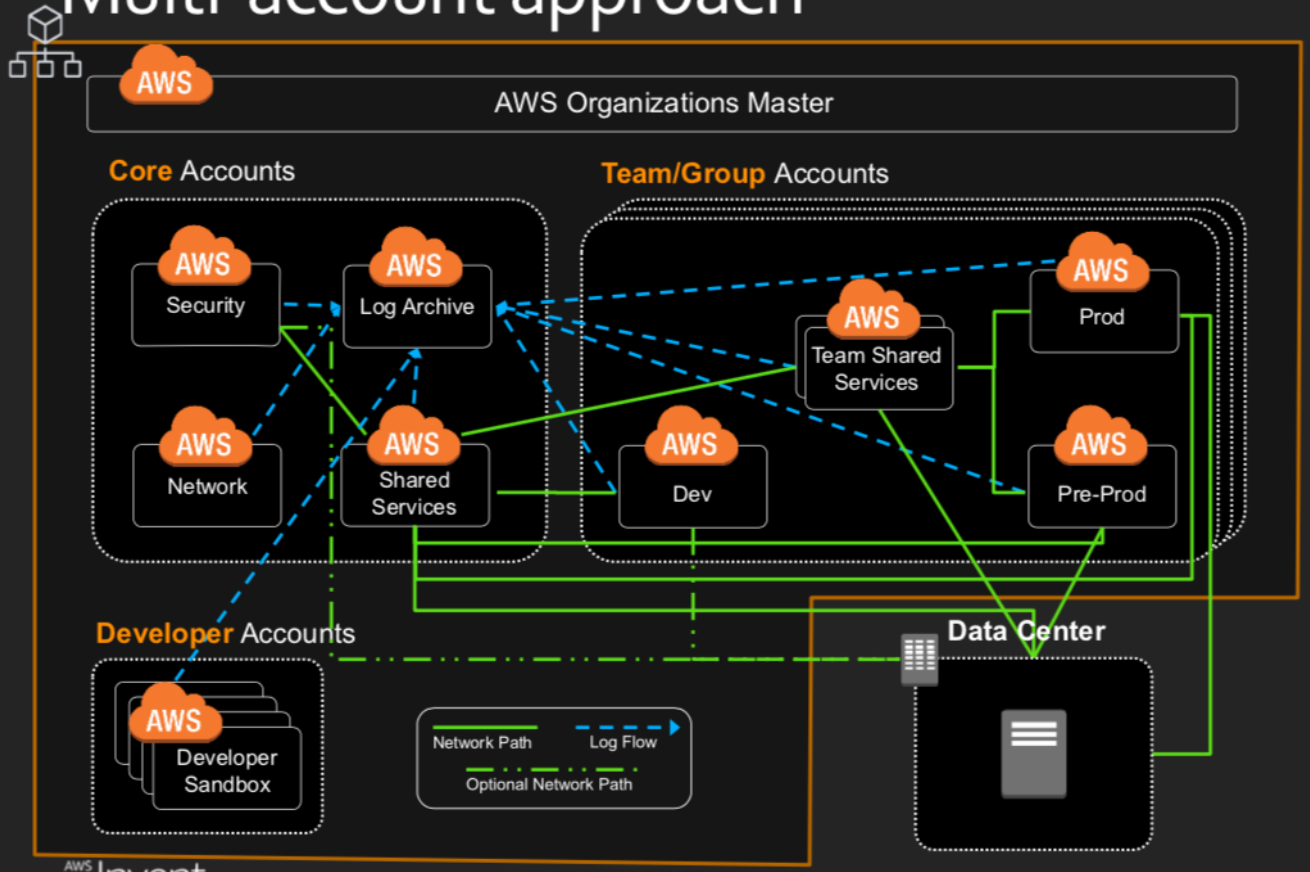
Identity & Access Management

- User account access managed through AWS SSO federation
- Cross-account roles enable centralized management

Security & Governance

- Multiple accounts enable separation of duties
- Initial account security and AWS Config rules baseline
- Network baseline

Multi-account approach



Orgs: Account management

Log Archive: Security logs

Security: Security tools, AWS Config rules

Shared services: Directory, limit monitoring

Network: Direct Connect

Dev Sandbox: Experiments, Learning

Dev: Development

Pre-Prod: Staging

Prod: Production

Team SS: Team Shared Services, Data Lake

aws

AWS IAM Role management.

AWS-ID

- Account management.
- Start point.
- Every user

AWS-releng

- Release egineering
- Tools

AWS-preprod

- PREPROD
- Dev
- Stage
- Loadtest

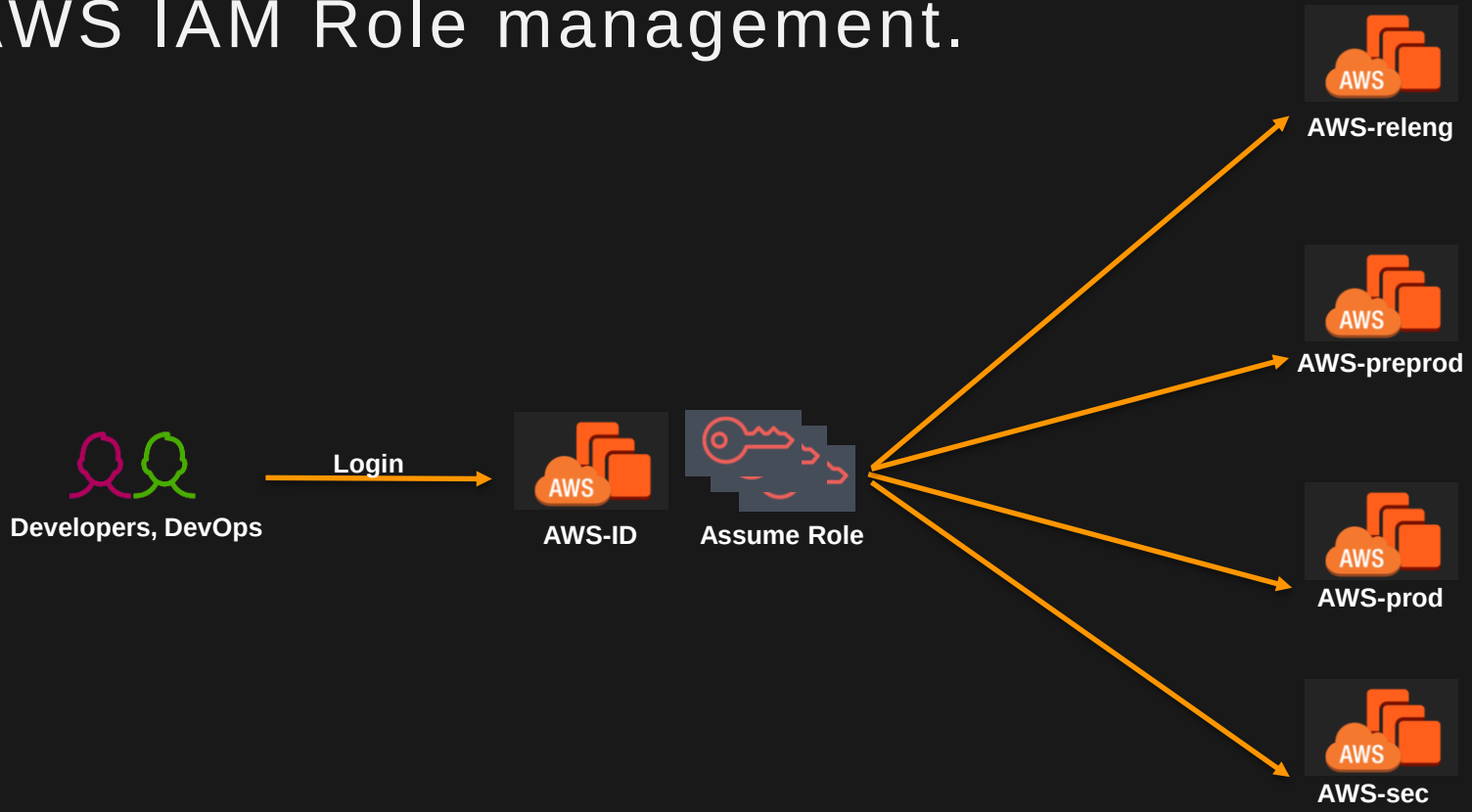
AWS-prod

- Production

AWS-sec

- Security

AWS IAM Role management.



Terraform code AWS IAM

```
# benx @ jupitersong-N in ~/github/benx_git/provisioning/terraform/iam/benx-id on git:master o [22:22:03]
$ ls
_module_userassume_policy          group_benx_developer_white.tf     userassume_policy_benx_legacy.tf
backend.tf                         group_benx_devops_black.tf        userassume_policy_benx_preprod.tf
bespin-readonly.tf                 group_benx_devops_white.tf        userassume_policy_benx_prod.tf
everyone.tf                        provider.tf                       userassume_policy_benx_releng.tf
group_benx_developer_black.tf      terraform.tfvars                  variables.tf
```

```
############## beNX Developer Group ##################
resource "aws_iam_group" "benx_developer_white" {
  name = "benx_developer_white"
}

resource "aws_iam_group_membership" "benx_developer_white" {
  name = "${aws_iam_group.benx_developer_white.name}"

  users = "${var.benx_developer_white_users}"

  group = "${aws_iam_group.benx_developer_white.name}"
}

#####################################################

########### beNX Developer users ####################
resource "aws_iam_user" "benx_developer_white_users" {
  count = "${length(var.benx_developer_white_users)}"
  name = "${var.benx_developer_white_users[count.index]}"
}

variable "benx_developer_white_users" {
  type        = "list"
  description = "benx developer black"
  default     = [
    "steve@bighitcorp.com",
    "claireseo@bighitcorp.com",
    "hello@bighitcorp.com",
    "leeyj@bighitcorp.com",
    "pinkred@bighitcorp.com",
    "johnn@bighitcorp.com",
    "jhpark@bighitcorp.com",
    "den@bighitcorp.com",
  ]
}
```

Access Control

	Gravitational Teleport	AWS Session manager
Audit log	Dynamo DB / S3	CloudWatch / S3
Session recording	Yes	Log
Easy to use	Easy	Very Easy
Price	Opensource / Enterprise	AWS
SSH Compatibility	Yes	No
Web ssh	Yes	Yes
…		

Terraform code

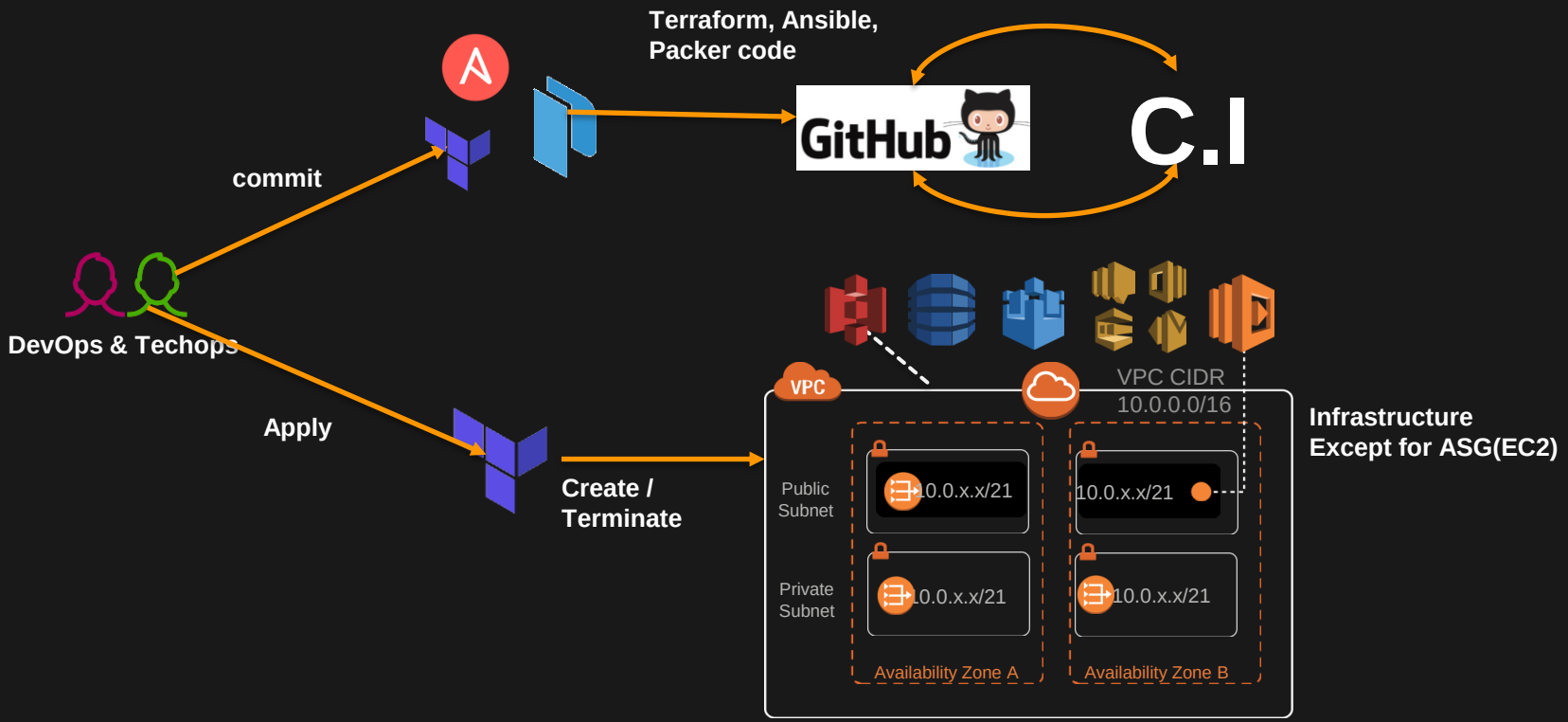
```
# benx @ jupitersong-N in ~/github/benx_git2/teleport on git:create_teleport_prd x [0:22:41]
$ tree
.
├── README.md
└── terraform
    ├── _modules
    │   ├── aws-efs
    │   │   ├── efs.tf
    │   │   ├── output.tf
    │   │   ├── security_group.tf
    │   │   ├── templates
    │   │   │   └── efs_config.sh
    │   │   ├── userdata.tf
    │   │   └── variables.tf
    │   ├── benx-aws-tags
    │   │   ├── main.tf
    │   │   ├── output.tf
    │   │   └── variables.tf
    │   └── teleport
    │       ├── auth
    │       │   ├── audits.tf
    │       │   ├── auth_asg.tf
    │       │   ├── data.tf
    │       │   ├── dynamodb.tf
    │       │   ├── dynamodb_autoscaling.tf
    │       │   ├── efs.tf
    │       │   ├── iam_auth.tf
    │       │   ├── lb_auth.tf
    │       │   ├── locals.tf
    │       │   ├── outputs.tf
    │       │   ├── sg_auth.tf
    │       │   ├── sg_nodes.tf
    │       │   ├── variables_env.tf
    │       │   └── variables_teleport.tf
    │       ├── bootstrap-ssm-parameter-store
    │       │   ├── README.md
    │       │   ├── data.tf
    │       │   ├── iam_policy.tf
    │       │   ├── kms.tf
    │       │   ├── outputs.tf
    │       │   ├── ssm.tf
    │       │   └── variables_env.tf
    │       ├── proxy
    │       │   ├── data.tf
    │       │   ├── efs.tf
    │       │   ├── iam_proxy.tf
    │       │   ├── output.tf
    │       │   ├── proxy_asg.tf
    │       │   ├── proxy_lb_external.tf
    │       │   ├── sg_proxy.tf
    │       │   ├── variables_env.tf
    │       │   └── variables_teleport.tf
```

```
    │       │   ├── variables_teleport.tf
    │       ├── userdata-config-auth-ssm-parameter-store
    │       │   ├── main.tf
    │       │   ├── output.tf
    │       │   ├── templates
    │       │   │   └── userdata
    │       │   │       └── teleport_config_auth.sh
    │       │   └── variables.tf
    │       ├── userdata-config-proxy-ssm-parameter-store
    │       │   ├── main.tf
    │       │   ├── output.tf
    │       │   ├── templates
    │       │   │   └── userdata
    │       │   │       └── teleport_config_proxy.sh
    │       │   └── variables.tf
    │       ├── userdata-install-enterprise-ssm-parameter-store
    │       │   ├── README.md
    │       │   ├── data.tf
    │       │   ├── output.tf
    │       │   ├── templates
    │       │   │   └── userdata
    │       │   │       ├── teleport_install_enterprise.sh
    │       │   │       └── teleport_install_license.sh
    │       │   ├── userdata.tf
    │       │   └── variables.tf
    │       └── userdata-install-startup-script
    │           ├── main.tf
    │           ├── output.tf
    │           ├── templates
    │           │   └── userdata
    │           │       ├── install_startup_systemd.sh
    │           │       └── install_startup_upstart.sh
    │           └── variables.tf
    └── bere_apnortheast2
        ├── acm.tf
        ├── backend.tf
        ├── common-user-data.tf
        ├── endpoints.tf
        ├── local.tf
        ├── outputs.tf
        ├── provider.tf
        ├── remote_state.tf
        ├── tags.tf
        ├── teleport-auth-userdata.tf
        ├── teleport-auth.tf
        ├── teleport-bootstrap.tf
        ├── teleport-proxy-userdata.tf
        ├── teleport-proxy.tf
        ├── templates
```

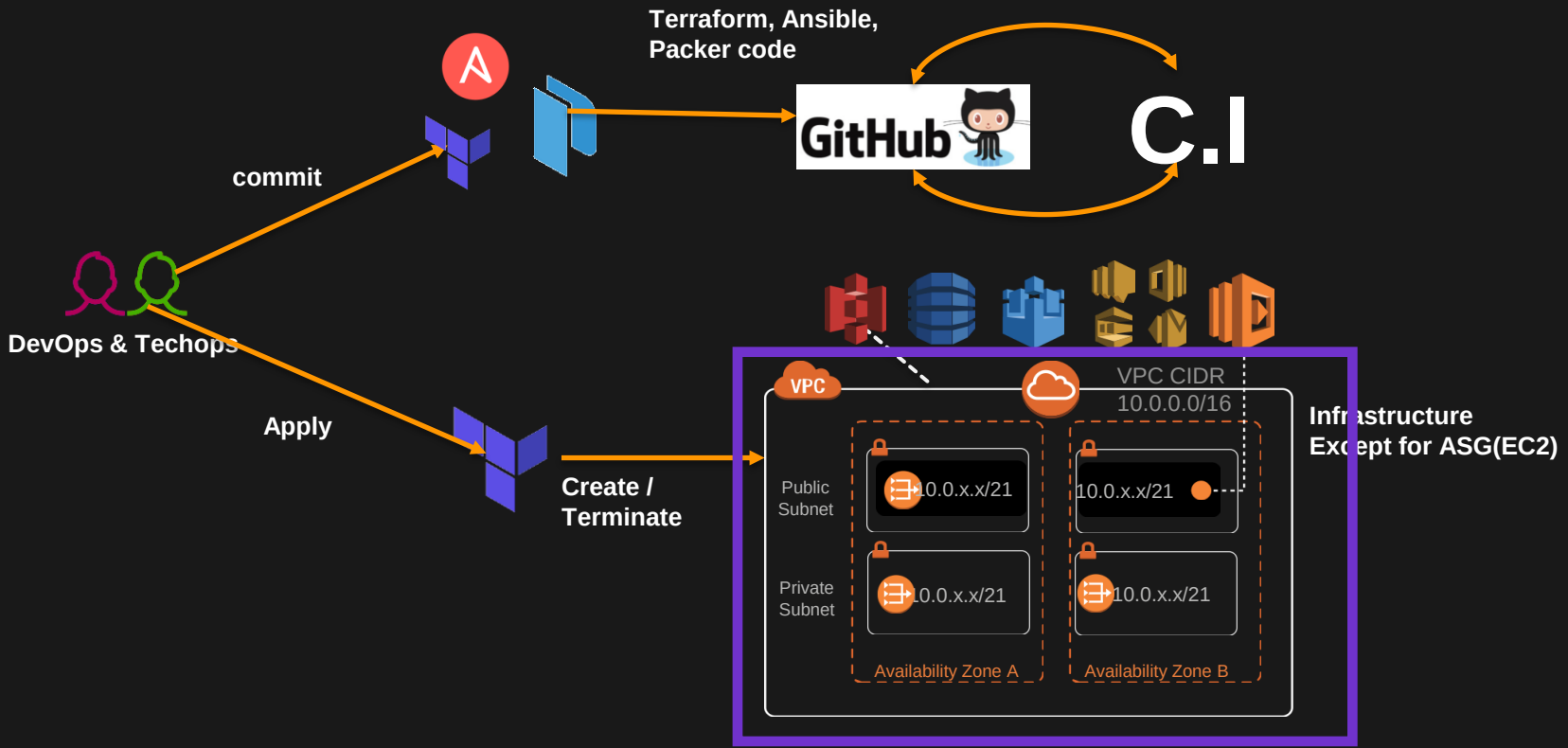
Automation - Migration 준비, 두번째

- Accounts / Accessbility
- App / Language / Architecture
- CI / CD
- Monitoring / Tools
- Security

Infrastructure as Code - Terraform



Infrastructure as Code - Terraform



ARC302

From One to Many

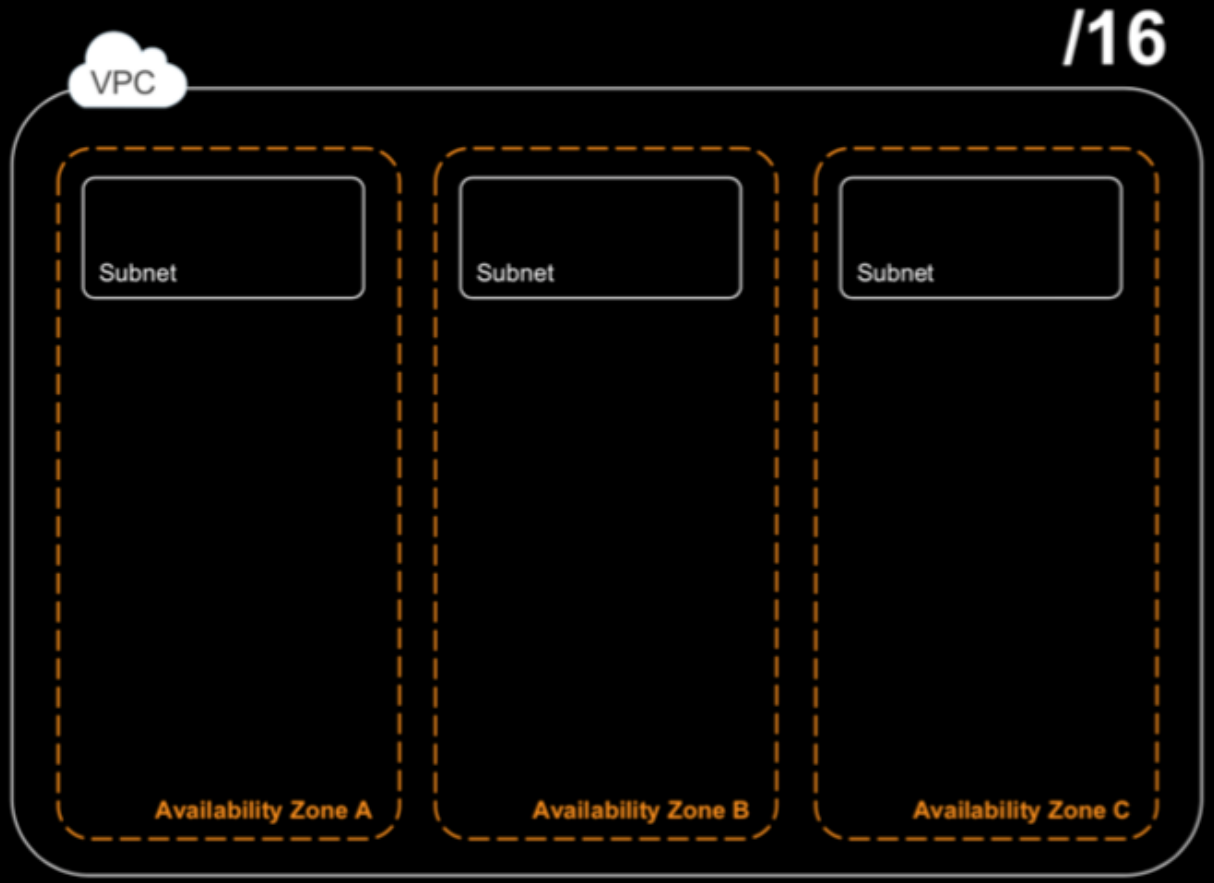
Evolving VPC Design

Rob Alexander, Principal Solutions Architect

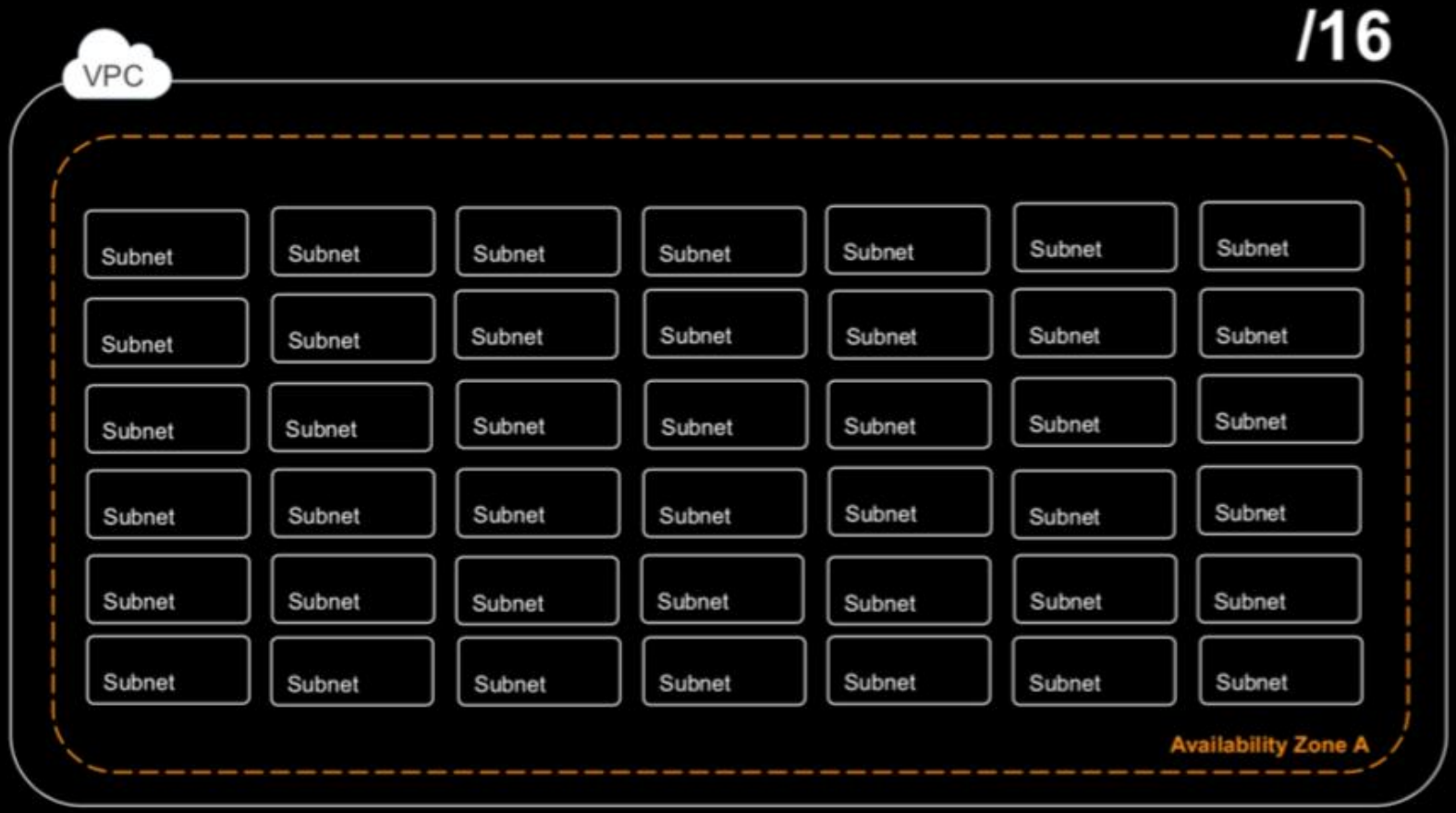
December 2, 2016

amazon web services

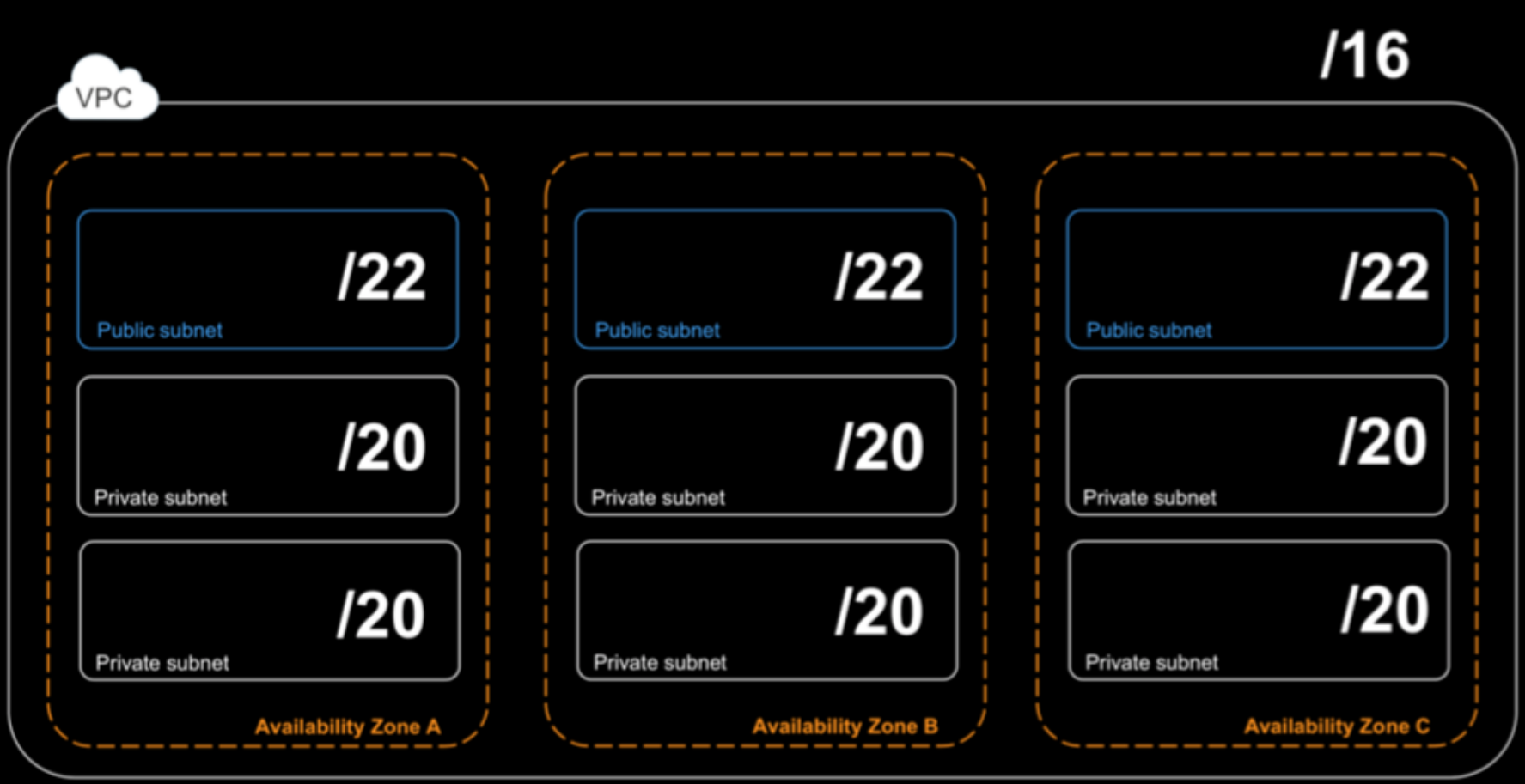
Create subnets



- Even distribution of IP space across AZs
- Use at least 2 AZs
- Subnets are AZ specific
- How big? How many?


/16
VPC
Subnet
Availability Zone A


/16
VPC
1019 IPs
/22
Public subnet
4091 IPs
/20
Private subnet
Availability Zone A
/22
Public subnet
/20
Private subnet
Availability Zone B
/22
Public subnet
/20
Private subnet
Availability Zone C

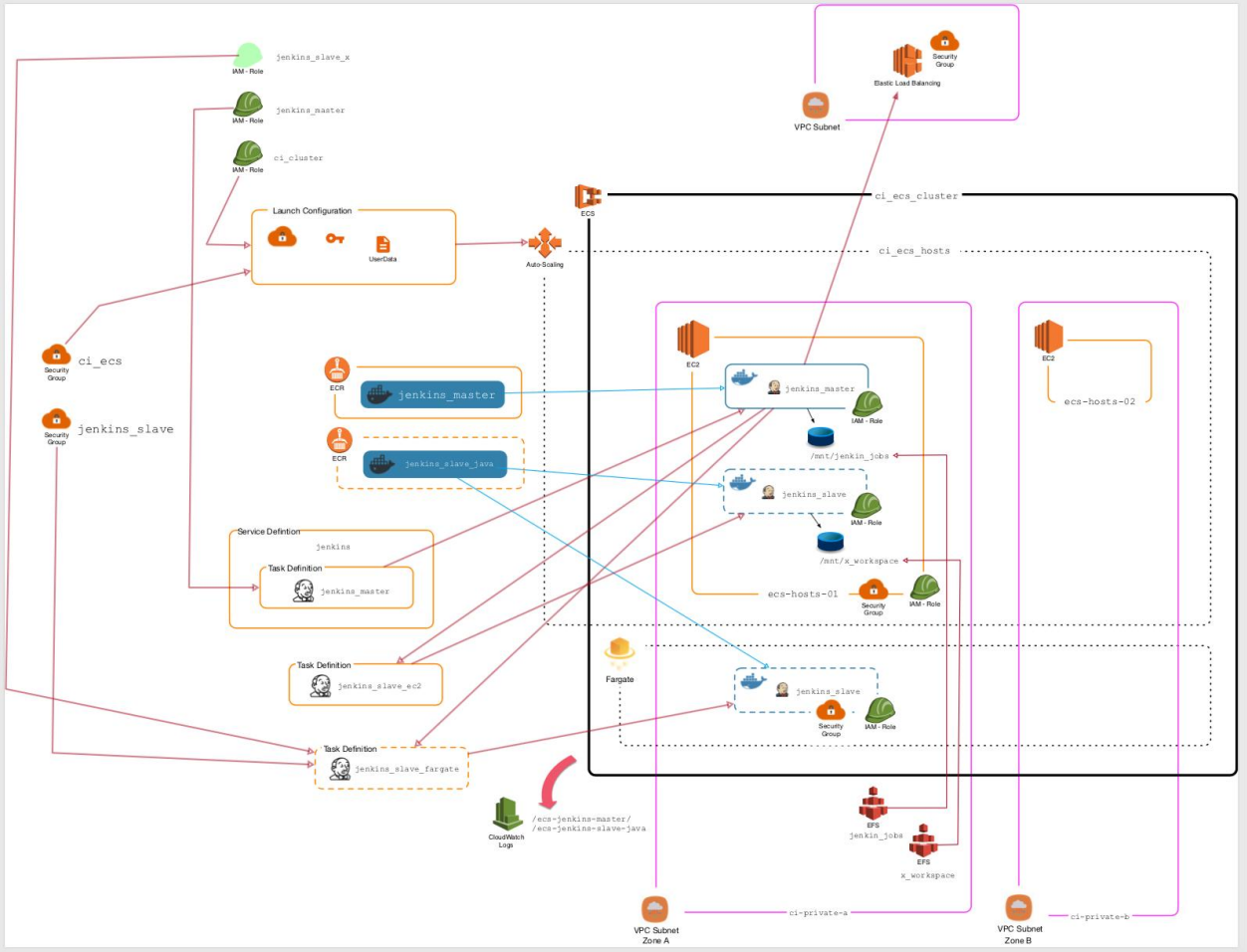

/16
VPC
/22
Public subnet
/20
Private subnet
/20
Private subnet
Availability Zone A
/22
Public subnet
/20
Private subnet
/20
Private subnet
Availability Zone B
/22
Public subnet
/20
Private subnet
/20
Private subnet
Availability Zone C

Automation - Migration 준비, 두번째

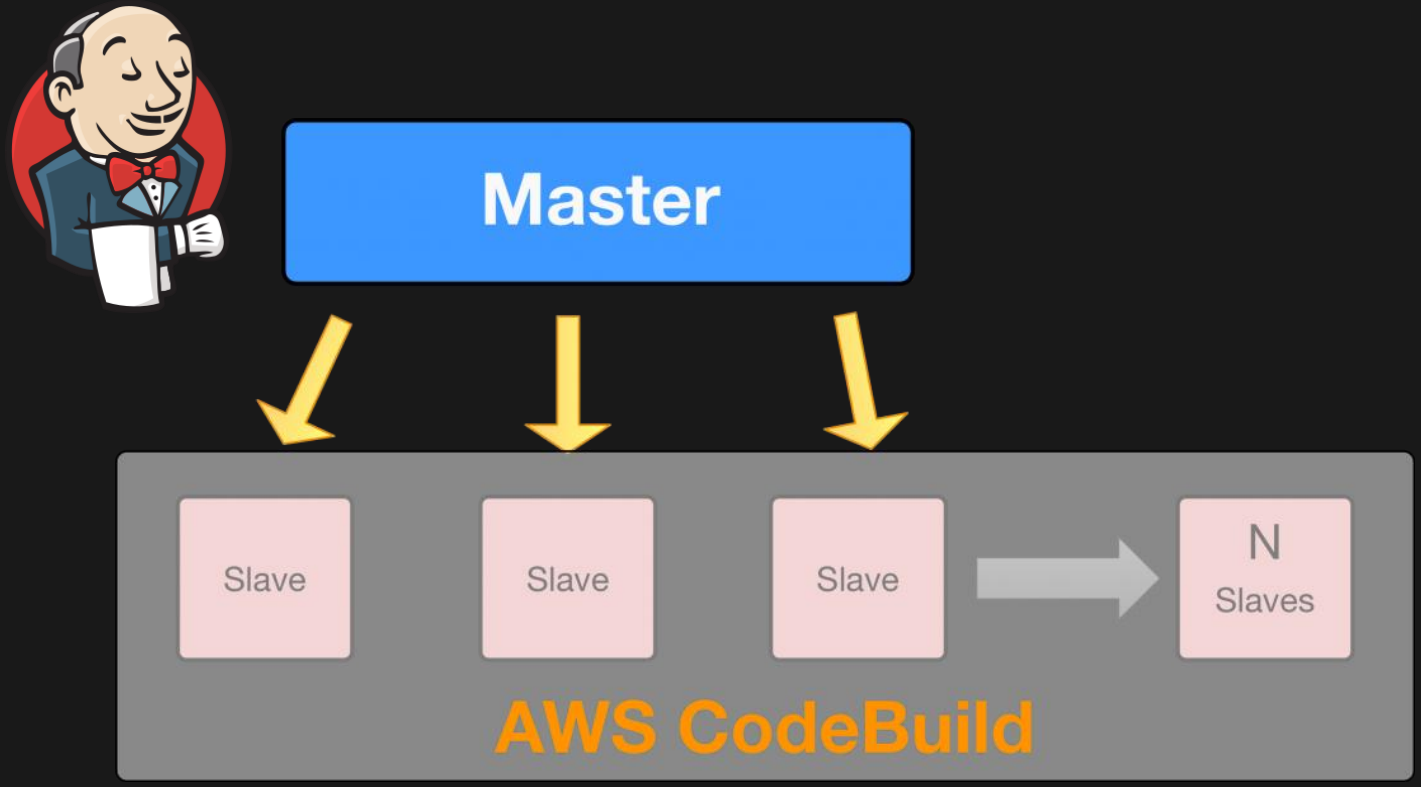
- App / Language / Architecture
- Accounts / Accessbility
- CI / CD
- Monitoring / Tools
- Security

Continuos Integration

Jenkins with ECS, Fargate



Jenkins with AWS Codebuild.

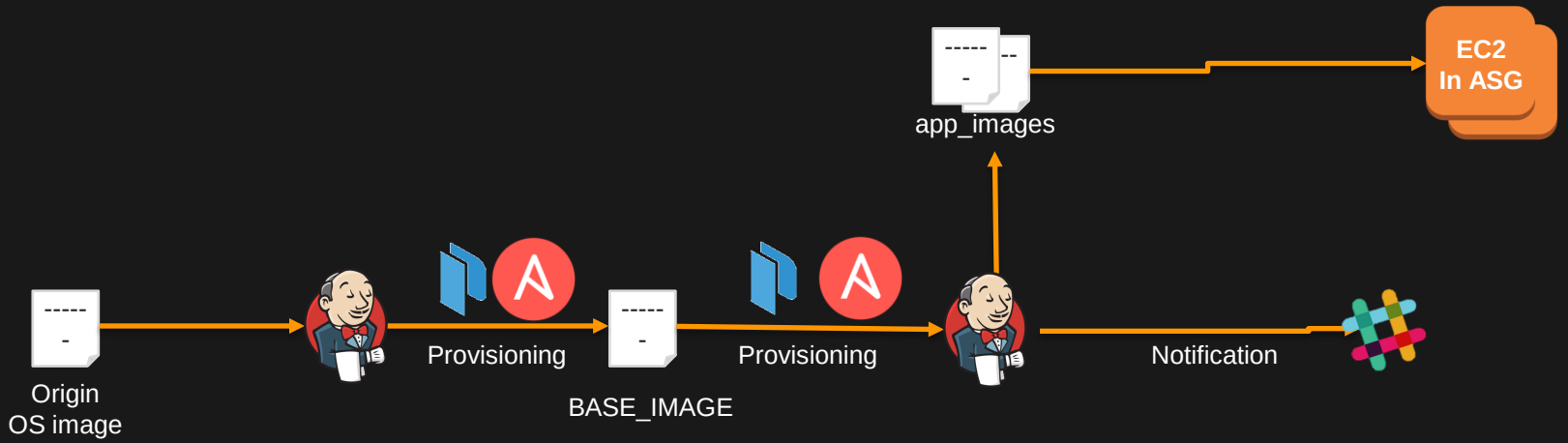


Infrastructure as Code - Jenkins

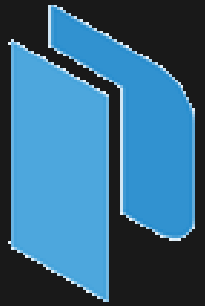
```
# benx @ jupitersong-N in ~/github/benx_git/jenkins/terraform on git:create_prd_jenkins x [22:43:28]
$ ls -l
total 24
drwxr-xr-x   3 benx  staff    96 May 13 18:21 _module
drwxr-xr-x  10 benx  staff   320 May 24 22:32 bere_apnortheast2
drwxr-xr-x  10 benx  staff   320 May 24 22:14 bered_apnortheast2
-rw-r--r--   1 benx  staff   157 May 13 18:21 provider.tf
-rw-r--r--   1 benx  staff   635 May 24 22:14 remote_state.tf
-rw-r--r--   1 benx  staff  1020 May 24 22:14 variables.tf
```

```
# benx @ jupitersong-N in ~/github/benx_git/jenkins/terraform/_module/jenkins on
$ ls -l
total 48
-rw-r--r--  1 benx  staff  3001 May 24 22:14 asg.tf
-rw-r--r--  1 benx  staff   789 May 24 22:14 efs.tf
-rw-r--r--  1 benx  staff  7853 May 24 22:44 iam.tf
-rw-r--r--  1 benx  staff  2170 May 24 22:14 jenkins.tf
-rw-r--r--  1 benx  staff     0 May 13 18:21 outputs.tf
drwxr-xr-x  6 benx  staff   192 May 24 22:14 userdata-install-startup-script
-rw-r--r--  1 benx  staff  2589 May 24 22:14 variables.tf
```

Immutable Infrastructure - Golden AMI



Infrastructure as Code - Packer



```
# benx @ jupitersong-N in ~/github/benx_git/guidserver-deploy on git:master o [0:28:21]
$ tree
.
├── Jenkinsfile
├── README.md
├── buildspec-packer.yml
├── group_vars
│   ├── platform_apnortheast2
│   │   └── service.yml
│   ├── platform_aws
│   │   └── service.yml
│   ├── platform_preprod
│   │   └── service.yml
│   ├── platform_prod
│   │   └── service.yml
│   ├── we_apnortheast2
│   │   └── service.yml
│   ├── wed_apnortheast2
│   │   └── service.yml
│   ├── wes_apnortheast2
│   │   └── service.yml
│   └── wet_apnortheast2
│       └── service.yml
├── inventories
│   ├── we_apnortheast2.ini
│   ├── wed_apnortheast2.ini
│   ├── wes_apnortheast2.ini
│   └── wet_apnortheast2.ini
├── packer.json
├── playbook.yml
├── requirements.yaml
```

```
# benx @ jupitersong-N in ~/github/benx_git/guidserver-deploy on git:master o [0:29:57]
$ ls
README.md             group_vars    packer.json          requirements.yaml  scripts
buildspec-packer.yml  inventories   playbook.yml         roles              services
```

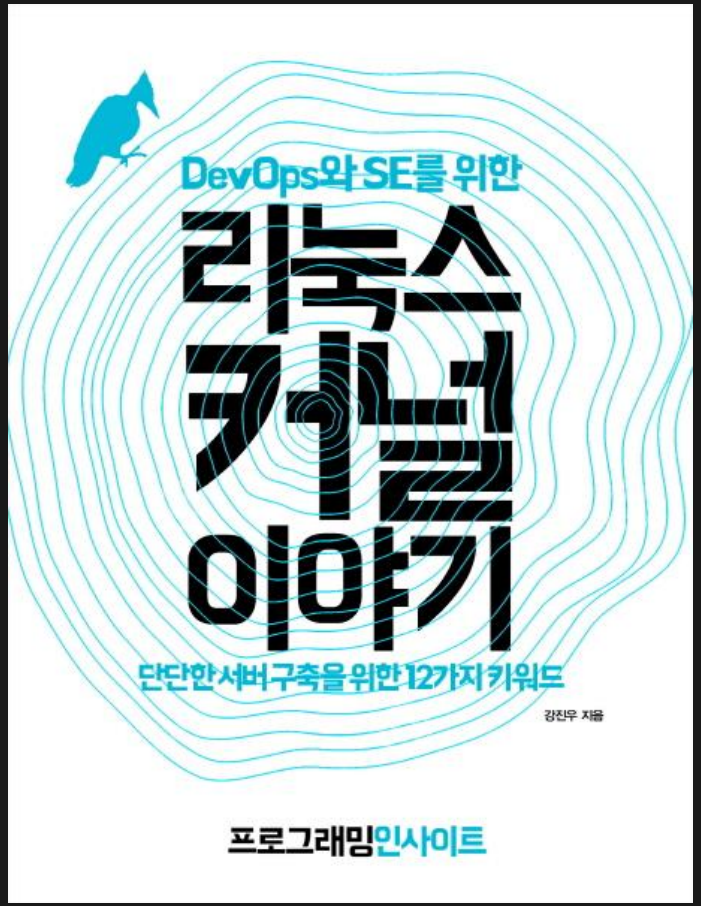
```
        ├── templates
        │   ├── bootstrap.yml.j2
        │   └── systemd.service.j2
        └── vars
            └── main.yml
```

Automation - Migration 준비, 두번째

- App / Language / Architecture
- Accounts / Accessbility
- CI / CD
- Monitoring / Tools
- Security

Monitoring - SaaS 전성시대

Infrastructure as Code - ELK, Kafka



- Senior System Engineer
- Pair DevOps
- Linux
- ELK
- Performance

https://brunch.co.kr/@alden

What is Devops?

- Culture
- Automation
- Measurement
- Sharing
- File up / Pile up

John Willis(@botchagalupe), Damon Edwards(@damonedwards)
Juyoung Song(@jupitersong)

Measurement

- If it moves, Measure it
- How is the application performing ?
- Are things getting Better or Worse ?
- Remove the guesswork from decisions

AWS re:INVENT

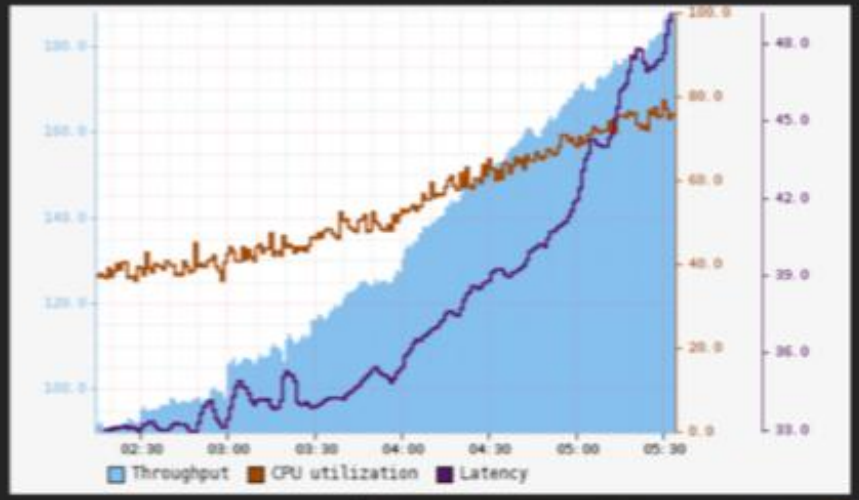
Tools Won't Fix Your Broken DevOps

Nicole Forsgren, PhD @nicolefv
Jez Humble @jezhumble

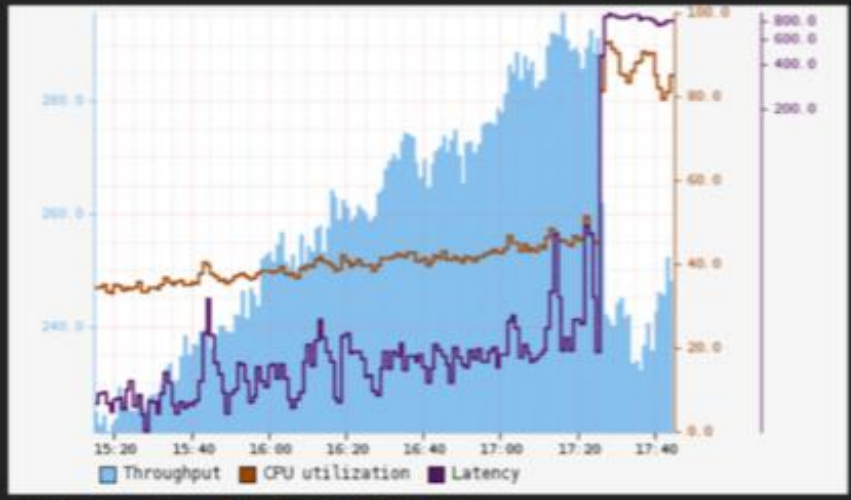
November 28, 2017

Understanding failures

NETFLIX



vs.

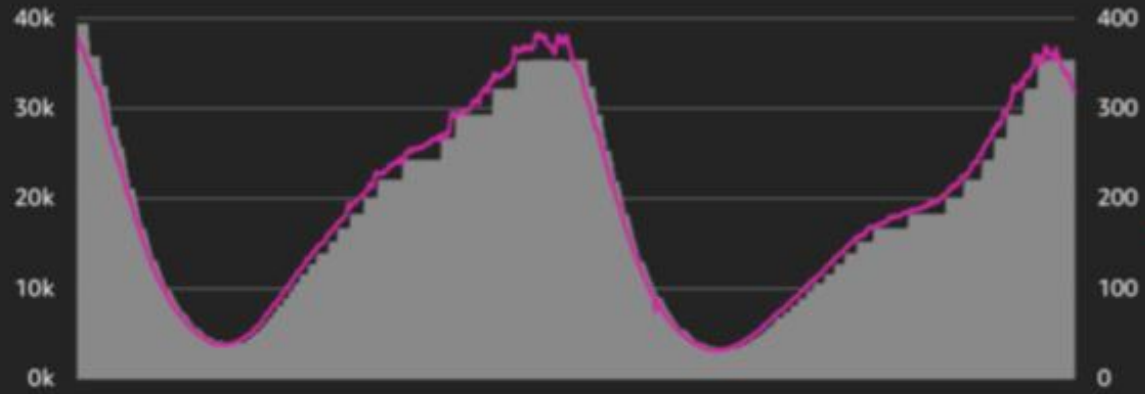


aws

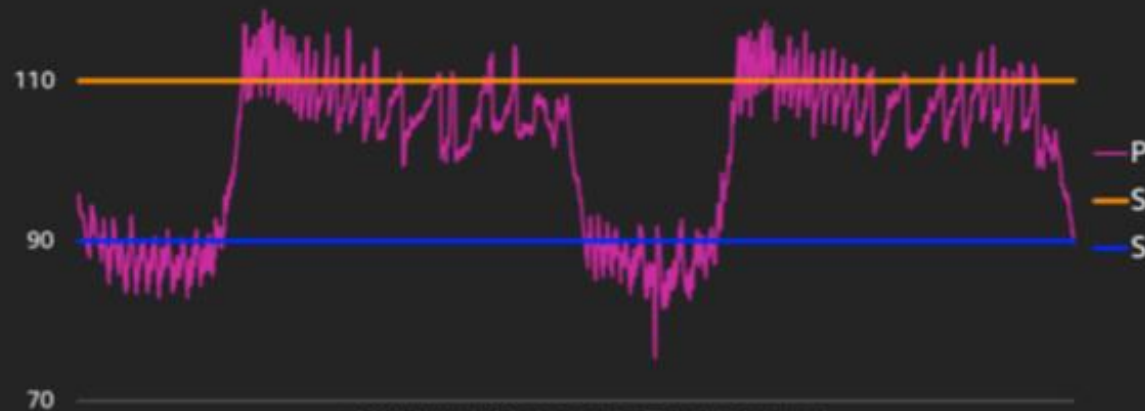
What could go wrong?

NETFLIX

Auto Scaling group throughput and size



Per-instance throughput



aws

CON310

Breaking Containers

Chaos Engineering for Modern Applications on AWS

Adrian Cockcroft
AWS VP Cloud Architecture Strategy

Ana Medina
Gremlin Inc. Chaos Engineer

aws re:Invent

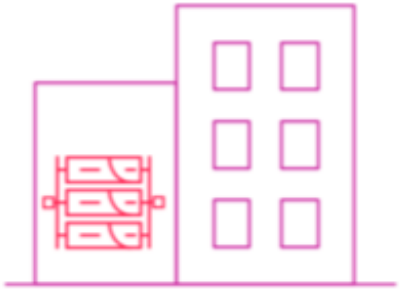
aws

Chaos engineering

is the discipline of experimenting
on a distributed system in order
to build confidence in the systems
capacity to withstand turbulent conditions
in production

Principles of Chaos Engineering

Past — Present — Future



Disaster recovery

Chaos engineering

Resilient critical systems

Gremlin

Failure as a service

Resource, network, state attacks on hosts or containers

Application-level fault injection for serverless

Easy to use API and UI

CHAOS EXPERIMENT FORM

APPLICATION NAME

EKS Guestbook

MONITORING TOOLS

DataDog

THE EXPERIMENT

Experiment #3
EXPERIMENT NAME

Shutdown Container
FAILURE TO INJECT

Redis Primary
IMPACT OF FAILURE

Primary container
SCOPE OF FAILURE

1 minute
DURATION OF FAILURE

Shutdown Gremlin
TOOL TO USE

THE HYPOTHESIS

If redis primary container is killed, the redis replica will get promoted to primary.

THE RESULTS

Unexpected, redis replica did not get promoted to primary. Data Loss has happened

ABORT CONDITIONS

Data Loss
HTTP 500s

ACTION ITEMS

Re-configure redis replication of primary to replicas

Gremlin

JOIN US ON SLACK: GREMLIN.COM/SLACK

What is Devops?

- Culture
- Automation
- Measurement
- Sharing
- File up / Pile up

John Willis(@botchagalupe), Damon Edwards(@damonedwards)
Juyoung Song(@jupitersong)

Sharing

- Encourage teams to share their data
- Help people to solve their own issues
- Everyone plays a part in getting to production
- Play nice with others

What did we learn?

- Push hard to refactor applications
- Changing mindsets is harder than changing tech
- Empower people to make their own decisions
- Give them the data to do it

Aol. DATADOG amazon web services

This is a learning process

- Don't search for a silver bullet
- Data is key to knowing what's going on
- Understand workloads
- You wouldn't heat your home all day in summer

Build a culture that can adapt quickly to change

Process should make life easier, not be a checklist

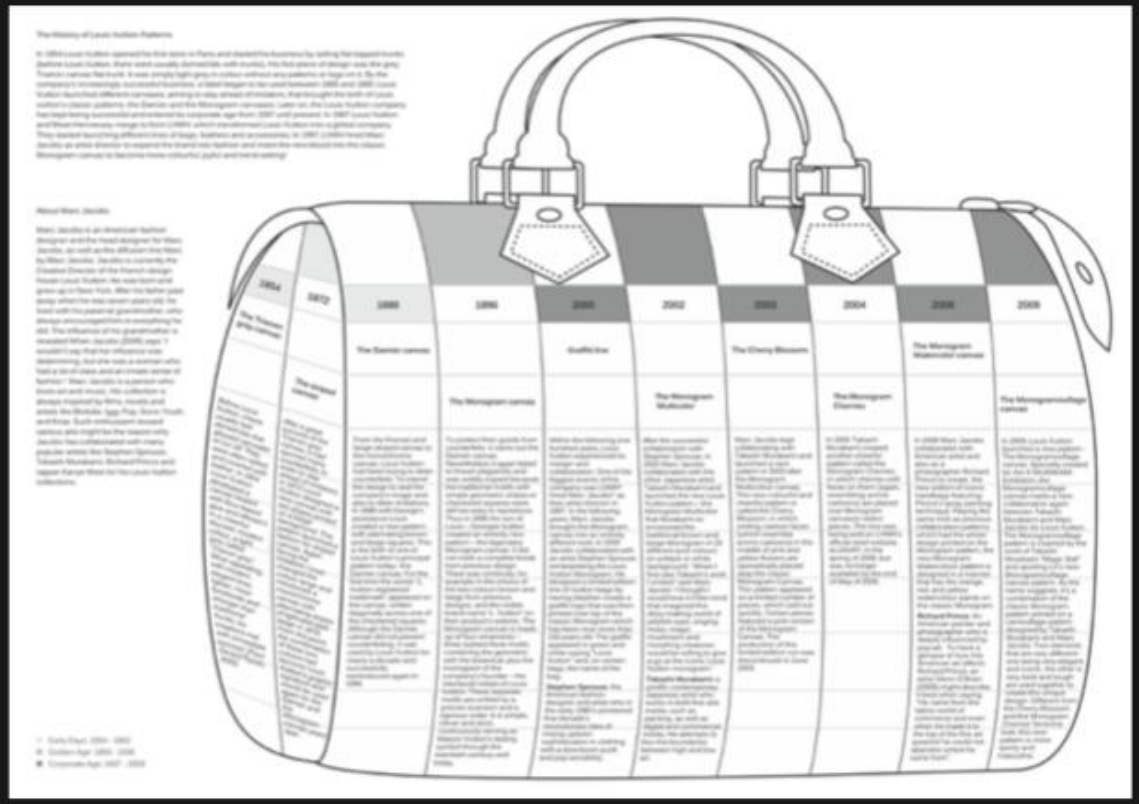
Don't get complacent; technology moves quicker than people

What is Devops?

- Culture
- Automation
- Measurement
- Sharing
- File up / Pile up

John Willis(@botchagalupe), Damon Edwards(@damonedwards)
Juyoung Song(@jupitersong)

Louis Vuitton



Louis Vuitton

From Tech to Art

Be Artist! from Techition!

Question n Answer

References

AWS re:invent 2016

- ARC302 From One to Many VPC Design

- From Dial-up to DevOps

AWS re:invent 2017

- dev345-tools-won-t-fix-your-broken-devops

AWS re:invent 2018

- Architecture Pattern for Multi-region Active-Active Applications

- breaking-containers-chaos-engineering-CON310

- capacity-management-made-easy-

- ENT306 AWS Landing Zone Deep Dive

- Architecting security and governance across your AWS Landing Zone