Infrastructure Automation at

Zach Steindler
Orchestructure 2019 Jan

dozen	AWS Accounts
half-dozen	regions
dozen	services
~thousand	app servers

Requirements

- Must work across accounts / regions
- Must be able to scale past a thousand nodes
- Must enforce security properties

kubernetes

ANSIBLE

2009

2010

2011

2012 

2013 

2014

2015 

2016

2017 

2018 

Ansible - in General

- Push, not pull
- Playbooks → roles → tasks
- Call AWS APIs (“infrastructure”), then SSH (“config”)
- “Idempotent”

Ansible - at Duo

ansible/

library/	- custom tasks
roles/	- collections of tasks
<playbooks>	- collection of roles
group_vars/	- config for a particular service
vars/	- config for an AWS account

Deploy Example

1. Pick one app server
2. Remove from LB
3. Download build
4. Downgrade check
5. Install build
6. Validate config
7. Apply DB schema updates
8. Start service
9. Health check passing
10. Return to LB

… repeat for more app servers

Meta: Enforcing Properties at Work

Person - “It’s _____’s job to answer the phone”

Place - “We go over PTO at our weekly meeting”

Process - “We don’t deploy until tests are green”

Security Properties w/ Ansible

roles/

<service>-infra/	- provision infra for service
infra-redis/	- firewall rules, password
infra-rds/	selection, encryption, ...
infra-ec2-and-elb/	- firewall rules, TLS, health checks
ec2-instance/	- firewall rules, OS security, ...

Non-Obvious Benefits

- Security compliance is much easier
- People w/o prod access can propose changes!
  - They can test them in dev!
- Changes across the fleet (usually) painless


Thanks!