Forget About The Console
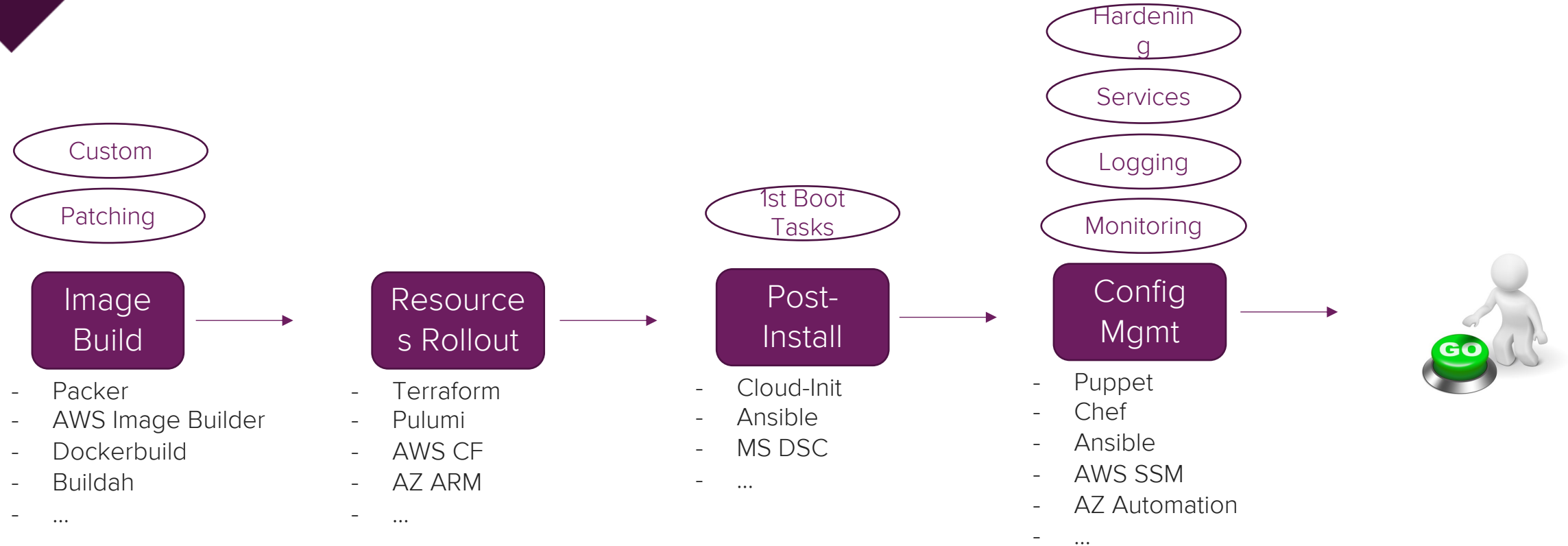
Avoiding Configuration Skews on our IaC Envs

Lucas Albuquerque | 09-03-2021

Agenda

- Typical IaC Wokflow

- IaC Goals

- Everything is fine, until is fine

- Battling Skews

- Discussion

Typical Workflow

Custom

Patching

1st Boot Tasks

Hardening

Services

Logging

Monitoring

Image Build

- Packer
- AWS Image Builder
- Dockerbuild
- Buildah
- ...

Resources Rollout

- Terraform
- Pulumi
- AWS CF
- AZ ARM
- ...

Post-Install

- Cloud-Init
- Ansible
- MS DSC
- ...

Config Mgmt

- Puppet
- Chef
- Ansible
- AWS SSM
- AZ Automation
- ...

GO

IaC Goals

- Reduced **Human Error** and Increased Institutional **Knowledge**

- **Repeatability** and **Consistency**

- Improved **Change Tracking** and **Auditability**

- Disaster Recovery

Everything is fine until is fine

- What if services are down

- What if instances not performing as expected

- Troubleshoot and debugging

- Quick fixes – Trial and Error approach

- Console = CLI

- Who/What track the changes?

Battling Skews...

- SCM tools can only track what's declared

- Isolate console and CLI - AWS SSM, IAP Proxy, Boundary, Bastions, etc

- OTP Credentials

- Login Notifications - Make some noise

- Falco Project – Kernel events

- OS Query – History, files, ps and ports monitoring

- *Post-mortem* Analysis

- "Flip the pancakes" once in a while

Thanks for Joining
Questions?

Lucas Albuquerque | 09-03-2021