Why you should take care of infrastructure drift

Cloud Native London Meetup, Feb 2021

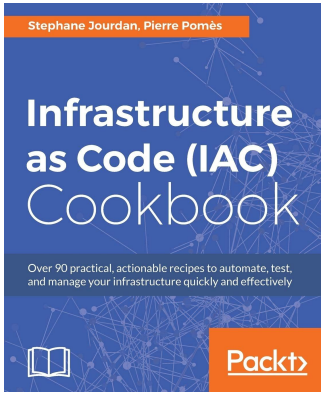
MIND THE GAP

between the code and the platform

whoami

Stephane Jourdan:

- @sjourdan (Twitter, GitHub, GitLab,...)
- 20 years (Dev)Ops
- Co-founded 3 tech companies (CAN/EU) and 1 sound studio.
- Driftctl tool co-founder! github.com/cloudskiff/driftctl
- “Infrastructure-as-Code Cookbook” author



Agenda

- IaC: How it started (3mn)
- IaC: How it’s going (6mn)
- Let’s drift! (5mn)
- Existing solutions (2mn)
- Driftctl CLI demo! (5mn)
- Rambly FTW!

Definition

Infrastructure Drift / ˈɪn frəˌstrʌk tʃər drɪft /

Noun

1. happens when the reality and the expectations don’t match.

Synonyms for Infrastructure Drift

1. omg

driftctl

How It Started

Multi-Cloud!

A single source of truth!

Credentials under control!

Versioning!

Skills!

Time!

Testing!

The code is the documentation!

GitOps!

CI/CD!

No more local stuff!

Collaboration FTW!

Immutable Infrastructure!

How It’s Going

“Do not expect Plato's ideal republic”

Marcus Aurelius, Roman Emperor

(and hundreds of us in interview)

How It’s Going

- Changes happen outside of IaC (lambdas, scripts, manual…)

How It’s Going

- Changes happen outside of IaC (lambdas, scripts, manual…)
- Commits don’t include the full scope of change
- The code documents a partial reality (half-blind), borken processes
- No one had time to learn & write IaC tests (and they are too costly to run anyway)
- E_TOO_MANY_TEAMS ; async(false);
- People still run terraform on their laptop, full CI/CD setup too complicated
- The move to immutable infrastructure still didn’t happen last year, too bad
- My [“boss”, “customer”, “coworker”] needs full console access for ${REASON}
- All team members aren’t still skilled on every IaaS provider
- Not everything that has an API is yet under IaC (GitHub etc.)

driftctl

How It's Going

- Drift!

driftctl

How It's Going

- Drift!

driftctl

But...Terraform plan/apply!

While we use and love Terraform (and other Hashicorp products), Terraform is an excellent provisioner.

But it's not a tool meant to manage what's outside its scope!

And security / compliance tools are another type of software.

```
Apply complete! Resources: 0 added, 0 changed, 0 destroyed.
```

Stories!

Quick AWS IAM Story

How an intern with read-only access ended up with rogue Administrative access and keys

- *without anyone noticing*

```
resource "aws_iam_user" "intern_user" {
  name = "INTERN-${random_string.prefix.result}"

  tags = {
    Name = "INTERN-${random_string.prefix.result} User"
  }
}

resource "aws_iam_access_key" "intern_user" {
  user = aws_iam_user.intern_user.name
}

resource "aws_iam_user_policy_attachment" "intern" {
  user       = aws_iam_user.intern_user.name
  policy_arn = "arn:aws:iam::aws:policy/ReadOnlyAccess"
}
```

Quick AWS Security Group Story

How an intern with rogue Administrative access opened everything to anyone on IPv4 & IPv6

- *without anyone noticing*

```
resource "aws_security_group" "supersecure" {
  name        = "supersecure"
  description = "Super Secure Security Group"

  tags = {
    Name = "Super Secure Security Group"
  }
}
```

```
resource "aws_security_group_rule" "supersecure_sg_rule_1" {
  type              = "ingress"
  from_port         = 22
  to_port           = 22
  protocol          = "tcp"
  cidr_blocks       = ["10.0.0.0/8"]
  security_group_id = aws_security_group.supersecure.id
}
```

Quick AWS S3 Story

How a scripting issue created a billing nightmare

- *With only billing noticing*

```
resource "aws_s3_bucket" "demo" {
  bucket = "${random_string.prefix.result}-demo"
  acl    = "private"
}
```

Existing Solutions

- **CI/CD Integration** (Jenkins, Terraform Cloud, Atlantis, env0...)
- **Static Analysis** (Checkov, TFLint, TFSec,...)
- **Testing & Verification** (Terratest, InSpec,...).
- **Policy & Compliance** (Sentinel,...)

driftctl

Our own open-source solution for drift management

driftctl

Our own open-source solution for drift management

```
sjourdan@quadskiff:~/src/github.com/cloudskiff/driftctl-demos/demo$ driftctl scan
Scanning AWS on region: us-east-1
Found unmanaged resources:
  aws_iam_policy_attachment:
    - INTERN-w7l7kb-arn:aws:iam::aws:policy/AdministratorAccess
  aws_s3_bucket:
    - fosdem2030
  aws_security_group_rule:
    - sgrule-916627219 (Type: ingress, SecurityGroup: sg-030d0e1b1d3f1a082, Protocol: All, Ports: All, Source: 0.0.0.0/0)
    - sgrule-2402827272 (Type: ingress, SecurityGroup: sg-030d0e1b1d3f1a082, Protocol: All, Ports: All, Source: ::/0)
  aws_iam_access_key:
    - AKIASBXWQ3AY3NLTNBMM
Found 15 resource(s)
 - 66% coverage
 - 10 covered by IaC
 - 5 not covered by IaC
 - 0 deleted on cloud provider
 - 0/10 drifted from IaC
```

driftctl

Our own open-source solution for drift management

- AWS Support (more to come)
- Terraform State support (local/S3)
- Filtering & Ignore support
- Written in Go
- Apache 2.0 License

About driftctl

Take control of infrastructure drift

FLOSS CLI that tracks, analyzes, prioritizes, and warns of infrastructure drift

cloudskiff/driftctl

MIND THE GAP

between the code and the platform