



NABENIK

Do clickops para IaC warm standby, alta disponibilidade multiregião com OpenTofu e Kubernetes

Víctor Orozco - @tuxtor

19 de setembro de 2024

Nabenik

- **Objetivo da Palestra:**

- Conversar acerca da transformação de uma infraestrutura "clickops" para DR Warm Standby.
- Explicar como essa transformação ajudou a atingir um SLA de 99%.

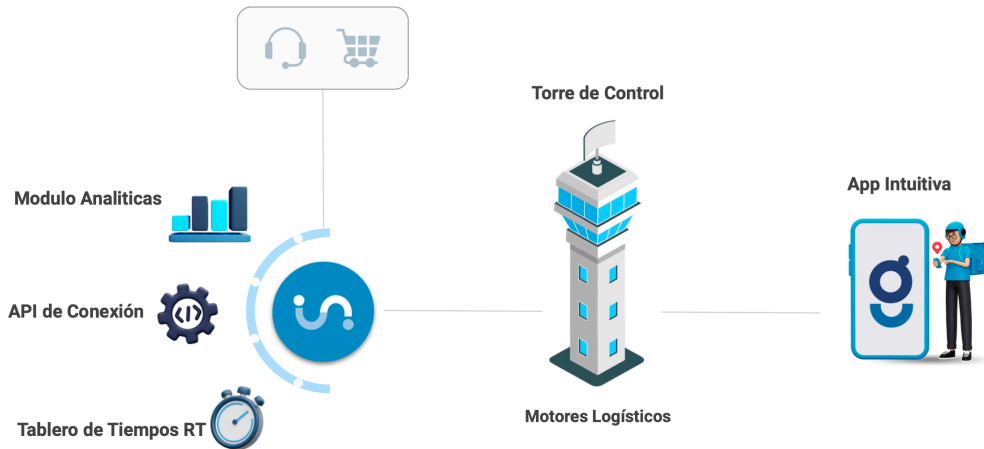
- **Visão geral dos tópicos:**

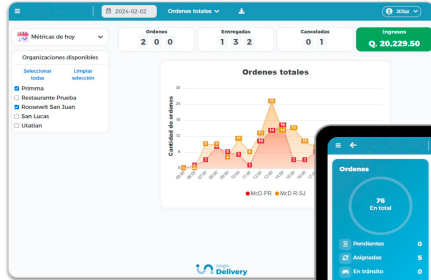
- O problema
- A solução
- Ideias importantes

O problema



Ecosistema de Delivery





Form for creating a new order. The interface includes fields for 'Nombre', 'Apellido', 'Teléfono', and 'Dirección'. The 'Dirección' field is populated with 'Palacio Nacional de Guatemala'. The 'Total' field shows 'Q. 150.00, 26.36'. A 'Crear orden' button is at the bottom.

Nueva orden

Los campos marcados con * son obligatorios

* Nombre: * Apellido:

Teléfono:

Dirección:

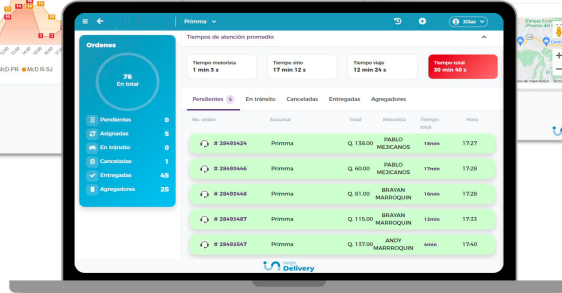
Cómo electroneo:

Notas:

¿Programar la orden? ☐

Total:

Crear orden



O problema

IDP v1

- A longo (dona do software) cria projetos de inovação digital em modalidade Lean
- Infraestrutura lean = Clickops

IDP v2

- **Mais clientes = SLA 99%**
- A infraestrutura lean estava ficando limitada
- 1% = 432 minutos = 7 horas por mês

¿O que é “Clickops”?

Definição

Gerenciamento manual da infraestrutura via console -e.g. AWS Console, OCI console-.

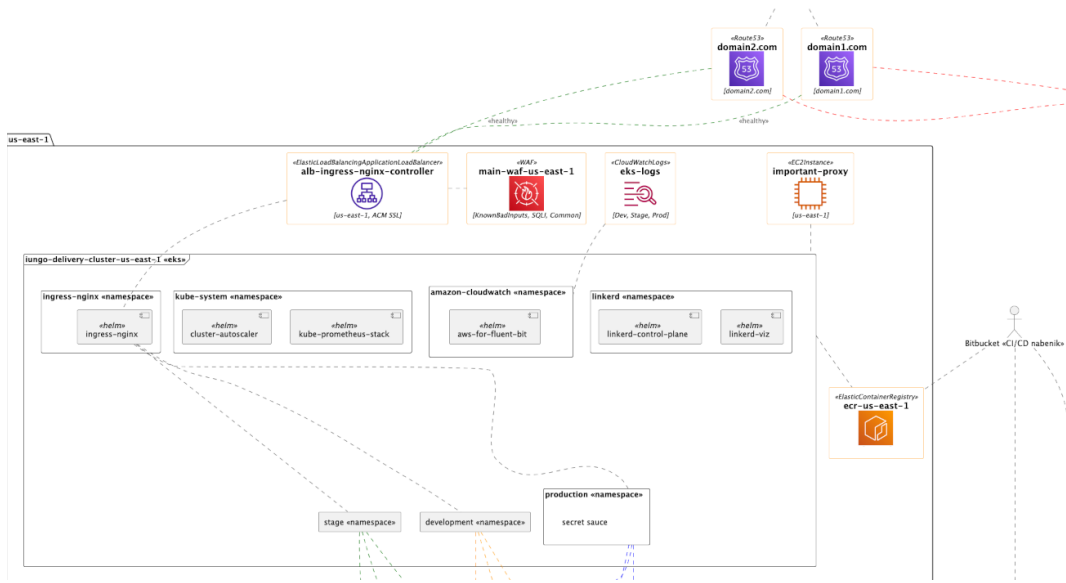
- **Desvantagens:**
 - Falta de consistência (multi A-Z)
 - **Falta de homologação (multirregião)**
 - Risco de erros humanos
 - SREs mudam, é a vida
 - Auditorias são complicadas com Runbooks

December 5, 2022: AWS Outage in US-East 2 Availability Zone

In December 2022, a 40-minute outage hit AWS's US-East 2 region, the second outage for the zone in 2022. AWS published no incident summary for this outage, and a spokesperson told *Data Center Knowledge* the company does "not publish Post-Event Summaries ... for every service event."

Figura 1: AWS Outage

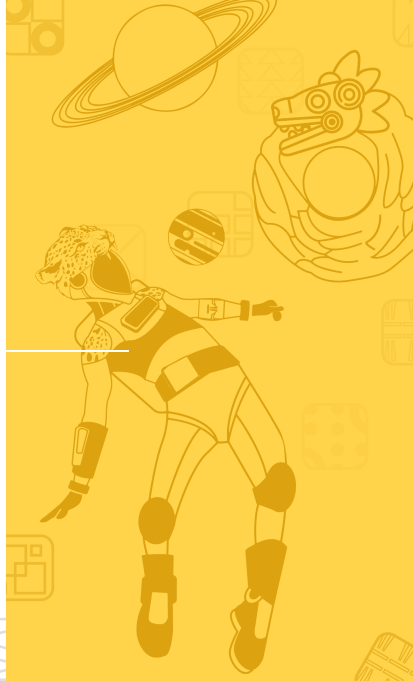
<https://www.datacenterknowledge.com/outages/a-history-of-aws-cloud-and-data-center-outages>





NABENIK
Tecnología para tu éxito

A solução



Warm Standby

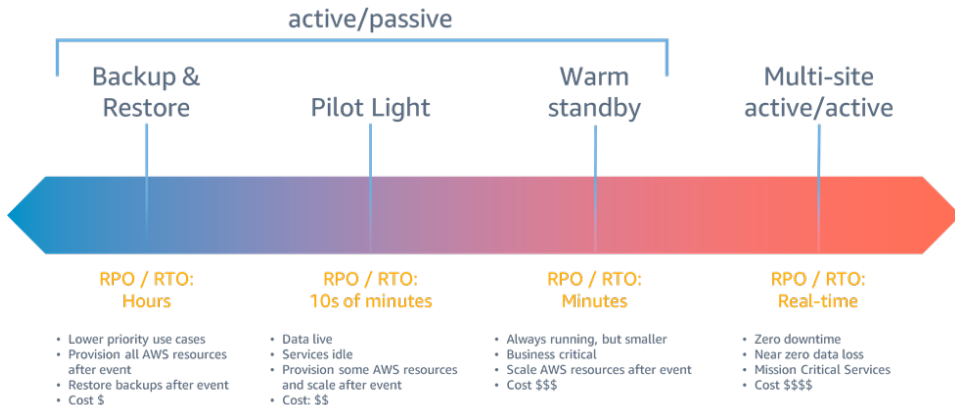


Figura 2: Disaster recovery strategies

- **Visão Geral do DR Warm Standby:**
 - Infraestrutura (reduzida) pronta para failover.
 - Capacidade de recuperação rápida.
 - Multi A-Z
- **Desafios com o “Clickops”:**
 - Sem recuperação rápida
 - Impossível criar a parte WARM sem errar
 - Os aplicativos estavam prontos para IaC, mas a infraestrutura não

Warm Standby

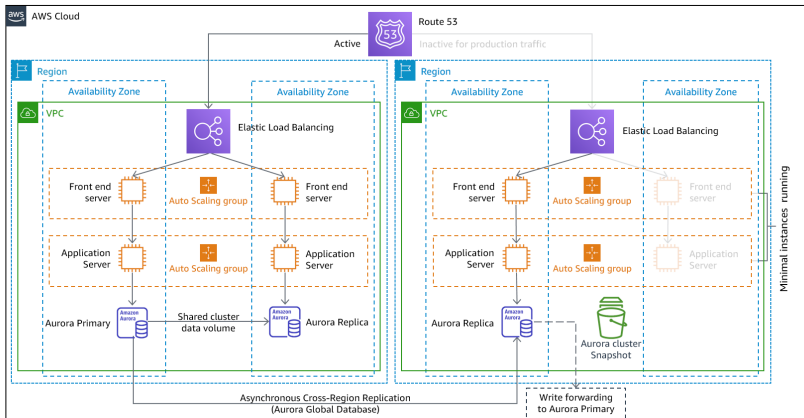


Figura 3: Warm Standby






Ideias importantes



Ideia 0: Seja cloud native sempre

TL;DR: Um bom chassis de microserviço facilita tudo

Na capa de aplicativos, precisamos reconfigurar os pipelines, **SÓ!**

| | | | | |
|---|----------------------------|-------------------------|---------------------------------|---|
|  | Victor Orozco | 138a99f | Fixing typo |  |
|  | Victor Orozco | cd1897c | Fixing cluster name |  |
|  | Victor Orozco | 789f6cc | Adding support for new clusters |  |
|  | Marta Celia Sarina Bola... | 9fee435 | New release start 1.0.35 |  |

Ideia 0: Seja cloud native sempre

Backend: Java (Quarkus) + Eclipse JKube

1. Codebase: Github Flow
2. Dependencies: Maven
3. Config: MicroProfile Config, Vault
4. Backing services: Kafka (SmallRye Reactive Messaging), JPA + Hibernate Panache, MicroProfile Config
5. Build, release, run: Maven, Eclipse JKube
6. Processes: JAX-RS, MicroProfile Rest Client

Ideia 0: Seja cloud native sempre

Backend: Java (Quarkus) + Eclipse JKube

1. Port Binding: Kubernetes + MicroProfile Config
2. Concurrency: HPA + MicroProfile Health + MicroProfile Metrics
3. Disposability: Supersonic and subatomic (Quarkus)
4. Dev/prod parity: Maven profile + Quarkus Profiles + MicroProfile Config
5. Logs: ElasticSearch Operator
6. Admin processes: Flyway

Ideia 0: Seja cloud native sempre

Frotend: TypeScript (Angular) + Kustomize

1. Codebase: Github Flow
2. Dependencies: NPM
3. Config: Angular Profiles
4. Backing services: Ingress, ALB
5. Build, release, run: NPM, Kustomize
6. Processes: Container NGINX

Ideia 0: Seja cloud native sempre

Backend: TypeScript (Angular) + Kustomize

1. Port Binding: Kubernetes + Angular Profiles + Pipelines
2. Concurrency: HPA + Kubernetes Operator + Linkerd
3. Disposability: Nginx
4. Dev/prod parity: Angular Profile
5. Logs: ElasticSearch Operator
6. Admin processes: N/A

Ideia 1: Separar os ciclos de vida

- **1. Infraestrutura - Não muda frequentemente - OpenTofu:**
 - Infraestrutura cloud
 - Kubernetes operators
 - Secret vaults
- **2. Aplicativos - Muda constantemente - CI/CD:**
 - Java - JKube
 - JavaScript - Kustomize
 - CI/CD Bitbucket, single source of truth
 - Um pipeline, duas AZ
 - AWS AutoScaler + HPA = Infraestrutura reduzida!


Ideia 1: Separar os ciclos de vida

Opções:

- Terraform
- **Opentofu**
- Cloudformation (AWS)
- Pulumi
- Serverless Framework

OpenTofu:


- Gestão e provisionamento da infraestrutura
- Deploy automatizado
- **Feature parity com Terraform mas ainda falta documentação**

 #55 Rerun



🔗 18b55a6 Adding docks with mkdocs





👤 main

📖 [Learn more about reports](#)

🕒 4min 16 sec 📅 4 months ago 

Pipeline







Security Scan
1m 9s

Build tofu plan
2m 18s

Create documentation with mkdocs
1m 17s

Apply tofu plan
40s

 Redeploy

Ideia 2: Diferenciar compartilhado vs. global

Os módulos do HCL são nossos amigos, bem planejados eles podem ser reutilizados

- **Recursos globais:** IAM, Route53, Cloudfront
- **Recursos regionais:** EKS, ECR, EC2, MKS, CloudWatch
- **Especial:** RDS replication

```
— README.md
— bitbucket-pipelines.yml
— main.tf
— modules
  — cloudfront
  — ec2
  — ecr
  — eks
  — helm
  — iam
  — k8s
  — networking
  — public-ec2
  — rds-mysql
  — rds-postgres
  — route53
  — sg
  — waf
— output
— provider.tf
— regions
  — global
```

```
module "us_east_1" {
  source              = "./regions/us-east-1"
  iam-role-rds-monitoring-arn = module.global.iam-role-rds-monitoring-arn
  region              = "us-east-1"
  ...
}

module "us_west_1" {
  source              = "./regions/us-west-1"
  iam-role-rds-monitoring-arn = module.global.iam-role-rds-monitoring-arn
  region              = "us-west-1"
  ...
}

module "global" {
  source              = "./regions/global"
  ...
  us-east-1_lb        = module.us_east_1.aws_lb
  us-west-1_lb        = module.us_west_1.aws_lb
}
```

```
module ecr {
  source = "../../modules/ecr"
  region = local.region
}

module "eks" {
  source = "../../modules/eks"
  region = local.region
  vpc_id = module.vpc.vpc_id
  ...
}

module "helm" {
  source = "../../modules/helm"

  cluster_certificate = module.eks.kubeconfig-certificate-authority-data
  cluster_endpoint    = module.eks.endpoint
  cluster_name        = module.eks.name
  region              = local.region
  ...
}
```

Figura 4: regions/us-east-1.tf

- **Melhoria no SLA:**
 - 99.00% uptime atingido e resiliência testada
- **Redução de riscos e erros:**
 - Menos erros manuais.
 - Redução de riscos operacionais.
- **Maior eficiência operacional:**
 - Deploys mais rápidos.
 - Menos esforço manual.
- **Preparação para o Futuro:**
 - Suporte a crescimento e novas demandas.

```
k9s
Context: arn:aws:eks:us-east-1
Cluster: arn:aws:eks:us-east-1
User: arn:aws:eks:us-east-1
K9s Rev: v0.32.5
K8s Rev: v1.29.7-eks-2f46c53
CPU: 4%
MEM: 58%

Pod(namespace) [9]
NAME PF READY STATUS RESTARTS CPU MEM %CPU/R %CPU/L %MEM/R %MEM/L IP NO
● 1/1 Running 0 2 175 2 0 68 34 10.0.7.111 ip
● 1/1 Running 0 0 2 n/a n/a n/a n/a 10.0.7.106 ip
● 1/1 Running 0 0 2 n/a n/a n/a n/a 10.0.7.220 ip
● 1/1 Running 0 1 170 1 0 66 33 10.0.5.24 ip
● 1/1 Running 0 1 162 1 0 63 31 10.0.5.57 ip
● 1/1 Running 0 2 218 2 0 85 42 10.0.7.107 ip
● 1/1 Running 0 2 224 2 0 87 43 10.0.5.239 ip
● 1/1 Running 0 1 166 1 0 64 32 10.0.5.94 ip
● 1/1 Running 0 3 327 3 0 128 16 10.0.7.174 ip
```

Perguntas?



Oracle ACE
Pro



- vorozco@nabenik.com
- @tuxtor
- <https://voroeco.com>
- <https://tuxtor.shekalug.org>



This work is licensed under
Creative Commons Attribution-
NonCommercial-ShareAlike 3.0
Guatemala (CC BY-NC-SA 3.0 GT).