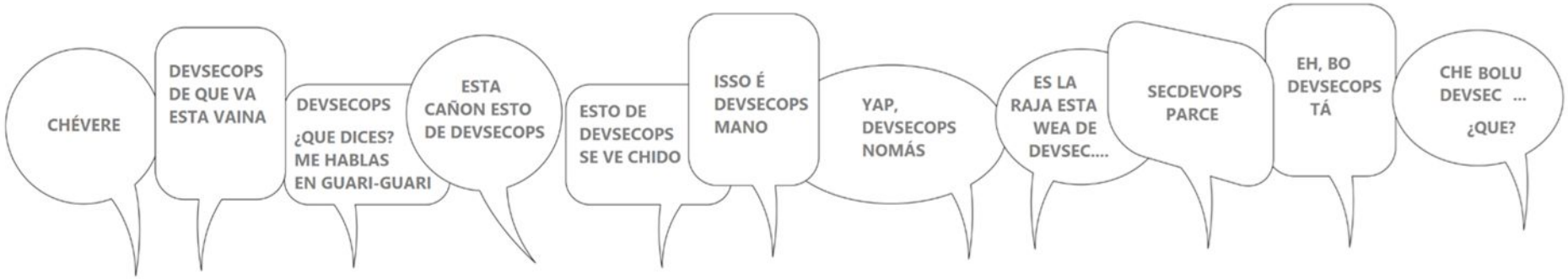
DSO LATAM 2020

“Porque lo único difícil de DevSecOps es pronunciarlo"



DEVSECOPS Latinoamérica

Patrones IaC para prevenir riesgos de TI

Terraformando para mejorar la postura de seguridad de la infraestructura

“Porque lo único difícil de DevSecOps es pronunciarlo”

DEVSECOPS Latinoamérica

Nahuel Perez

- Blue Team Lead @ appdirect
- Owning elesel
- <tw> @jnahuelperez </tw>
- <in>jnahuelperez</in>
- <git*>jnahuelperez</git*>

“Porque lo único difícil de DevSecOps es pronunciarlo”

IaC - primeros pasos

http://gitlab.com/elesel/mi_projecto

- desarrollo.tf
- vars.tf
- terraform.tfstate

desarrollo.tf

arquitectura > 01-terralith > desarrollo.tf

```
9
10  #-----------------------------------------------------------
11  # test
12  #-----------------------------------------------------------
13
14  resource "aws_instance" "splunk" {
15    ami                         = "ami-06cf02a98a61f9f5e"
16    instance_type               = "t2.micro"
17    subnet_id                   = aws_subnet.test.id
18    key_name                    = "NPerez_Key"
19    ebs_optimized               = false
20    monitoring                  = false
21    associate_public_ip_address = true
22    security_groups = [
23      aws_security_group.splunk.id
24      ]
25
26    # root_block_testice {
27    #   volume_type           = "gp2"
```

“Porque lo único difícil de DevSecOps es pronunciarlo”

IaC - primeros pasos

"Tenemos que ir a producción en 5 días"

desarrollo.tf

arquitectura > 01-terralith > desarrollo.tf

```
10  #------------------------------------
11  # test
12  #------------------------------------
13
14  resource "aws_instance" "splunk" {
15    ami                         = "ami-06
16    instance_type               = "t2.mic
17    subnet_id                   = aws_sub
18    key_name                    = "NPerez
19    ebs_optimized               = false
20    monitoring                  = false
21    associate_public_ip_address = true
22    security_groups = [
23      aws_security_group.splunk.id
24      ]
```

produccion.tf

arquitectura > 01-terralith > produccion.tf

```
1   #------------------------------------
2   # prod
3   #------------------------------------
4
5   resource "aws_instance" "splunk-prod"
6     ami                         = "ami-
7     instance_type               = "t2.m
8     subnet_id                   = aws_s
9     key_name                    = "NPer
10    ebs_optimized               = false
11    monitoring                  = false
12    associate_public_ip_address = true
13    security_groups = [
14      aws_security_group.splunk-prod.id
15      ]
16
17    # root_block_device {
18    #   volume_type           = "gp2"
```

"Porque lo único difícil de DevSecOps es pronunciarlo"

IaC - primeros pasos

“Quiero agrandar el CIDR del cluster de test”

- produccion.tfbkp
- desarrollo.tf
- vars.tf
- terraform.tfstate

terraform apply...

```
## Test VPC
resource "aws_vpc" "test" {
    cidr_block = "10.0.0.0/21"
    enable_dns_support = true
    enable_dns_hostnames = true
}

## Stage Bastion
resource "aws_instance" "test_bastic
    ami = "ami-1abc34567"
    instance_type = "m4.large"
    ...
}
```

```
## Prod VPC
resource "aws_vpc" "pr
    cidr_block = "172.
    enable_dns_support
    enable_dns_hostnam
}

## Stage Bastion
resource "aws_instance
    ami = "ami-1abc345
    instance_type = "m
    ...
}
```

“Porque lo único difícil de DevSecOps es pronunciarlo”

DEVSECOPS Latinoamérica

Mi ambiente de producción desapareció

{ } terraform.tfstate

“Porque lo único difícil de DevSecOps es pronunciarlo”

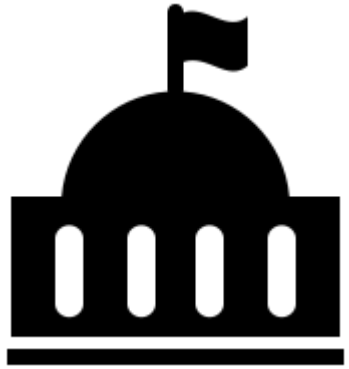
Motivación

- Quiero saber como ordenar el código
- Ambientes destruidos
- Dificultad al delegar el conocimiento
- Eliminar la tarea de estar en todos los reviews
- Mantenimiento de los secretos

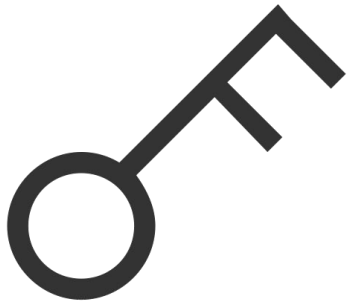
“Porque lo único difícil de DevSecOps es pronunciarlo”

Contexto - Agilidad vs Eficiencia

arquitectura



gobierno



gestión de secretos

“Porque lo único difícil de DevSecOps es pronunciarlo”

IaC - arquitectura

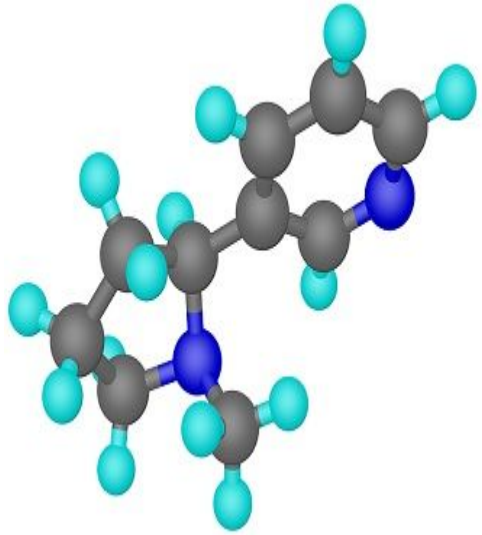
DEVSECOPS Latinoamérica

Terralitico

multi Terralítico

Terramod

Terraservice



“Porque lo único difícil de DevSecOps es pronunciarlo”

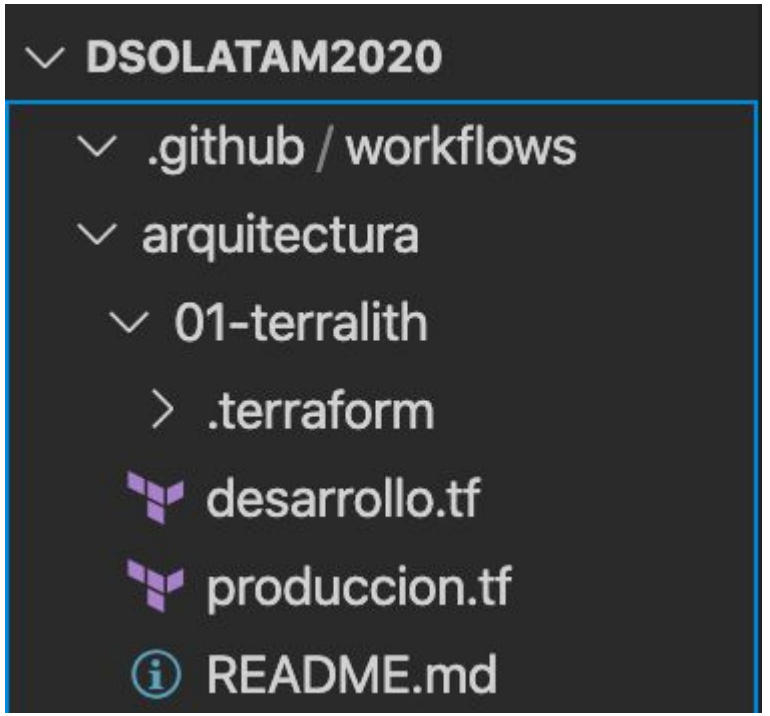
IaC - arquitectura

Terralitico

- único archivo de definiciones.
- valores hardcodeados
- único archivo de estado

Pain points

- administrar ambientes separados
- configuración confusa
- difícil el mantenimiento



“Porque lo único difícil de DevSecOps es pronunciarlo”

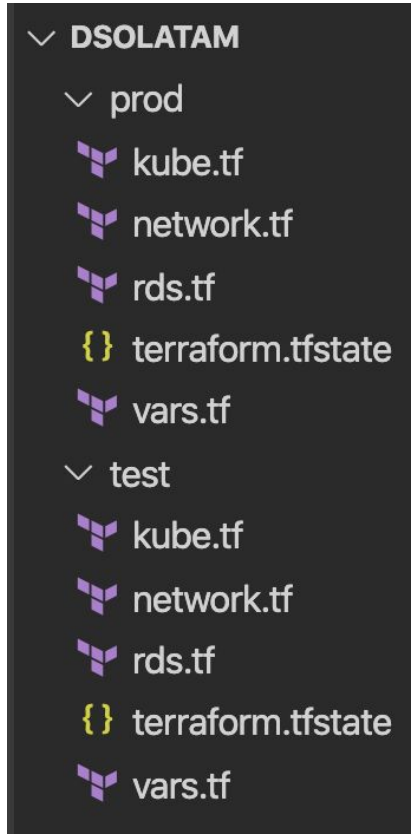
IaC - arquitectura

multi Terralítico

- ambientes separados
- múltiples archivos de definición
- mejor uso de variables
- la configuración es más intuitiva

Pain points

- la configuración intuitiva puede mejorar
- duplicación de definiciones



“Porque lo único difícil de DevSecOps es pronunciarlo”

IaC - arquitectura

Terramod

```
DSOLATAM
  ambientes / prod | test
    main.tf
    terraform.tfstate
    vars.tf
  modulos
    core
      main.tf
      output.tf
      vars.tf
    k8s-cluster
      main.tf
      output.tf
      vars.tf
```

“Porque lo único difícil de DevSecOps es pronunciarlo”

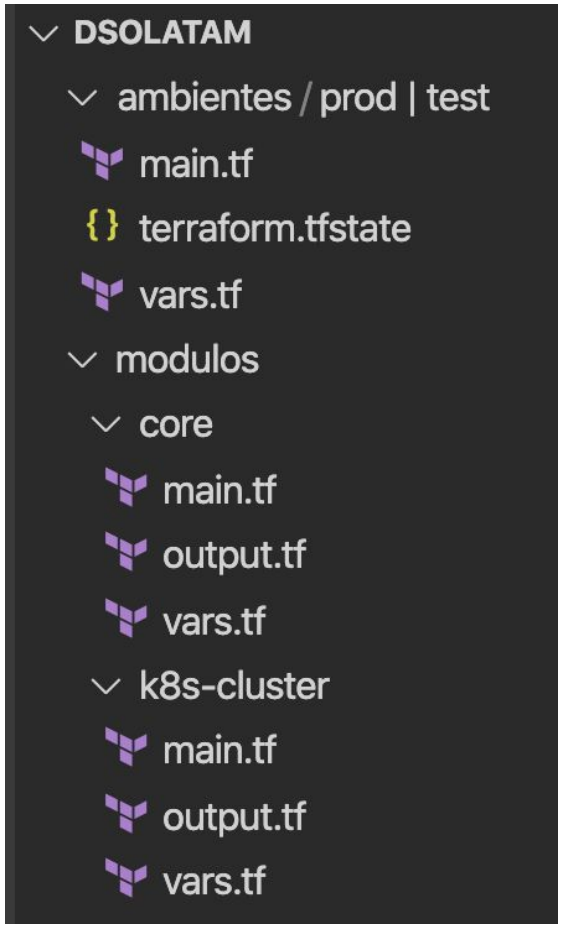
IaC - arquitectura

Terramod

- módulos reutilizables
- ambientes que se componen de módulos
- requiere cambios en la estructura del repo
- configuración mucho más intuitiva

Ojo con la reutilización de variables:

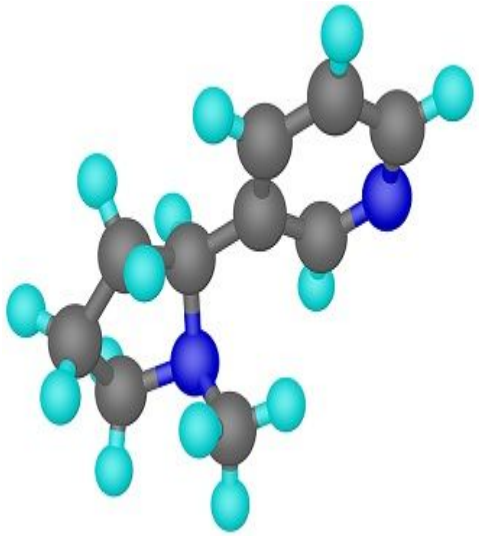
var.instance_type



“Porque lo único difícil de DevSecOps es pronunciarlo”

IaC - arquitectura

Terraserv



```
DSOLATAM
  ambientes / prod | test
    main.tf
    terraform.tfstate
    vars.tf
  modulos
    core
      main.tf
      output.tf
      vars.tf
    k8s-cluster
      main.tf
      output.tf
      vars.tf
```

```
DSOLATAM
  terra_service / envs
    prod
      core
      database
        tf.tfstate
        vars.tf
        xxx.tf
      k8s-cluster
        tf.tfstate
        vars.tf
        xxx.tf
```

“Porque lo único difícil de DevSecOps es pronunciarlo”

IaC - arquitectura

DEVSECOPS Latinoamérica

Terraserv

xxx.tf

terra_service > envs > prod > core > xxx.tf

```
terraform {
    backend "s3" {
        region = "us-east-1"
        bucket = "elesel/dsolatam-2020"
        key = "core/tf.tfstate"
        encrypt = "true"
    }
}

module "core" {
    source = "../../modules/core"
    cidr = var.vpc_cidr
}
```

outputs.tf

terra_service > envs > prod > core > outputs.tf

```
output "priv_subnet_id" {
    value = module.core.priv_subnet_id
}
```

xxx.tf

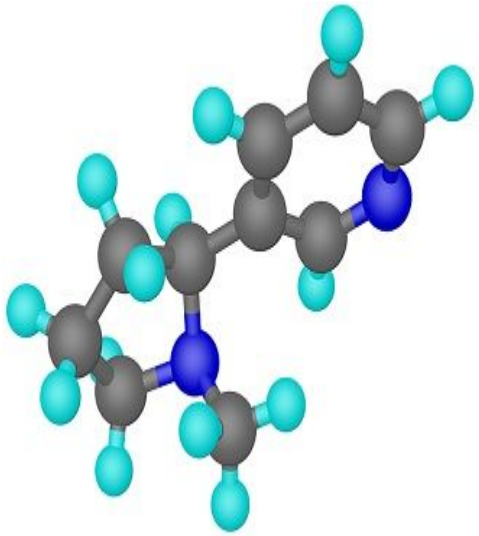
terra_service > envs > prod > database > xxx.tf

```
data "terraform_remote_state" "core" {
    backend "s3" {
        region = "us-east-1"
        bucket = "elesel/dsolatam-2020"
        key = "core/tf.tfstate"
        encrypt = "true"
    }

module "k8s-cluster" {
    source = "../../modules/k8-cluster"
    nodes_num = var.nodes_num
    priv_subnet = data.terraform_remote_state.core.priv_subnet_id
}
```

“Porque lo único difícil de DevSecOps es pronunciarlo”

IaC - arquitectura

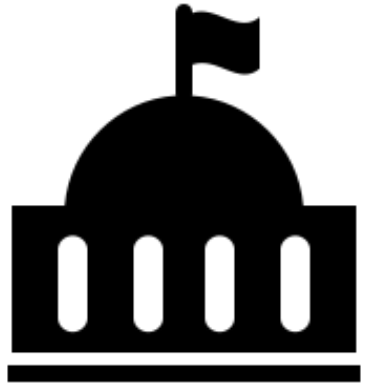
Terraserv



- adm componentes lógicos independiente
  - aislamos y reducimos el riesgo
  - mejor para setup de múltiples equipos.
- estado distribuido

“Porque lo único difícil de DevSecOps es pronunciarlo”

IaC - Gobierno



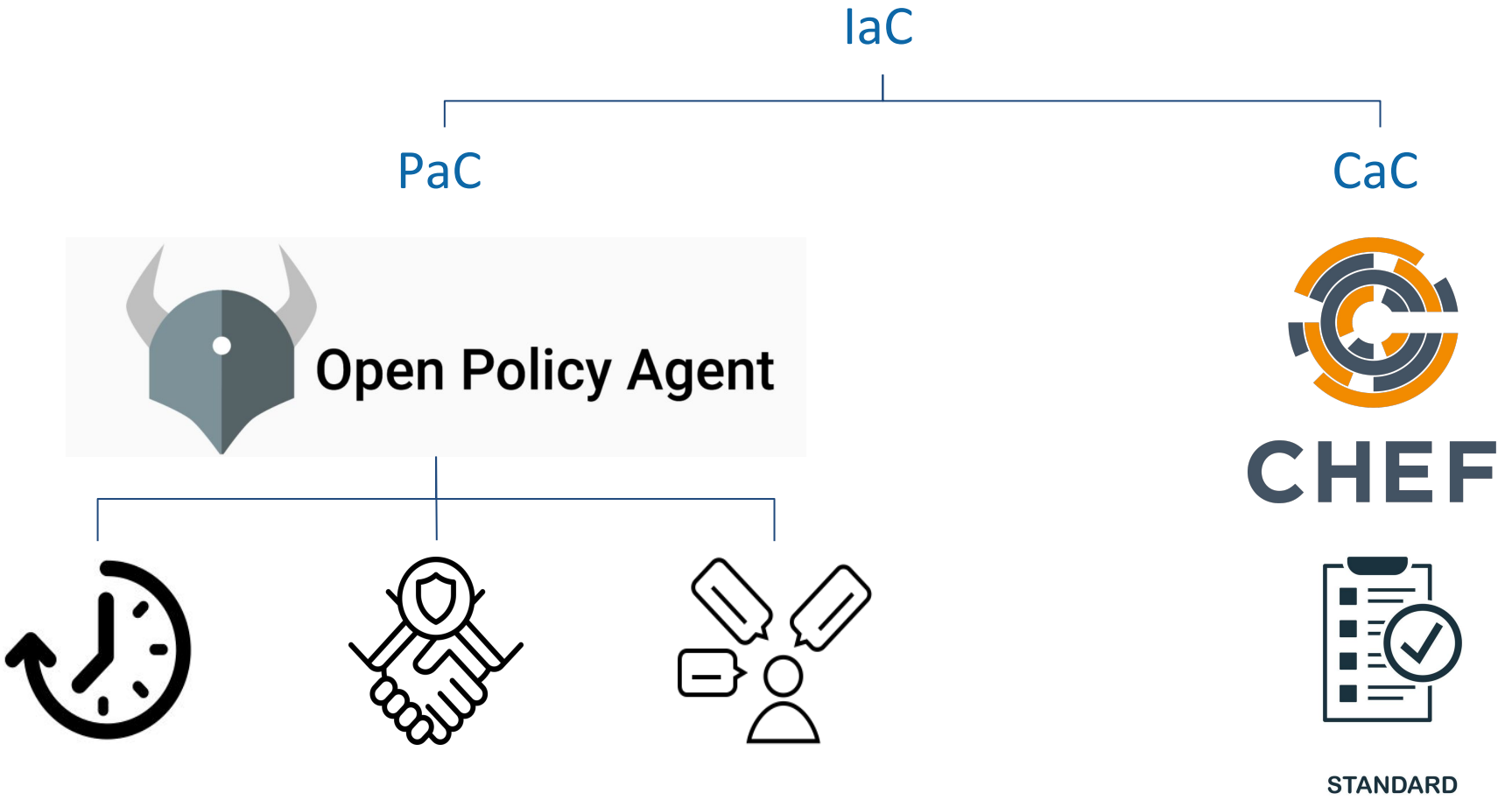
- Prevenir deploys no deseados.
- Cómo hacemos un shift to the left?
- Garantizar aplicacion de estandares

“Porque lo único difícil de DevSecOps es pronunciarlo”

IaC - Gobierno

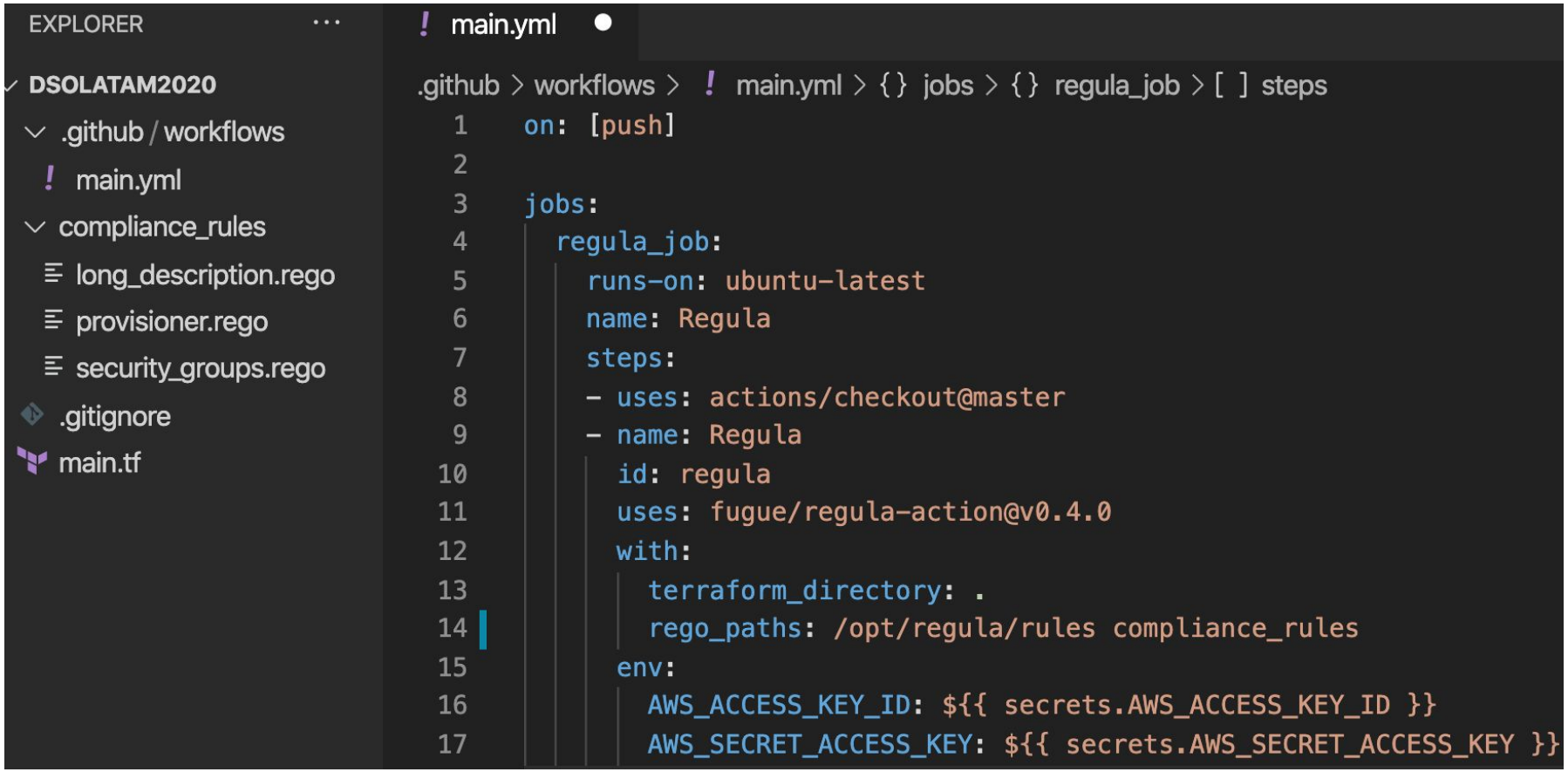
“Porque lo único difícil de DevSecOps es pronunciarlo”

IaC - Gobierno



“Porque lo único difícil de DevSecOps es pronunciarlo”

IaC - Gobierno



“Porque lo único difícil de DevSecOps es pronunciarlo”

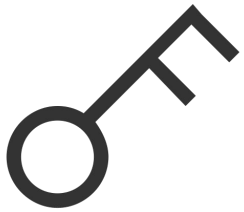
IaC - Gobierno

DEVSECOPS Latinoamérica

```
provisioner "chef" {
  node_name   = "${format("${var.environment}-splunk", count.index + 1)}"
  environment = "${var.environment}"

  run_list = [
    "elesel-org::base",
    "elesel-org::splunk-indexer",
    "elesel-org::cis-centos",
  ]

  secret_key      = "${file(var.secret_key_file)}"
  server_url      = "${var.server_url}"
  user_name       = "${var.user_name}"
  user_key        = "${file("${var.user_key}")}"
  recreate_client = true
  skip_install    = false
  version         = "${var.chef_client_version}"

  connection {
    type        = "ssh"
    user        = "${var.ssh_user}"
    private_key = "${tls_private_key.bootstrap-key.private_key_pem}"
  }
```

“Porque lo único difícil de DevSecOps es pronunciarlo”

IaC - Gestion de Secretos



- Secretos por todas partes
- Secretos expuestos por todas partes
- Acceso a los secretos

- tf_var_access_key
- tf_var_secret_key
- tf_var_rds_password
- ….

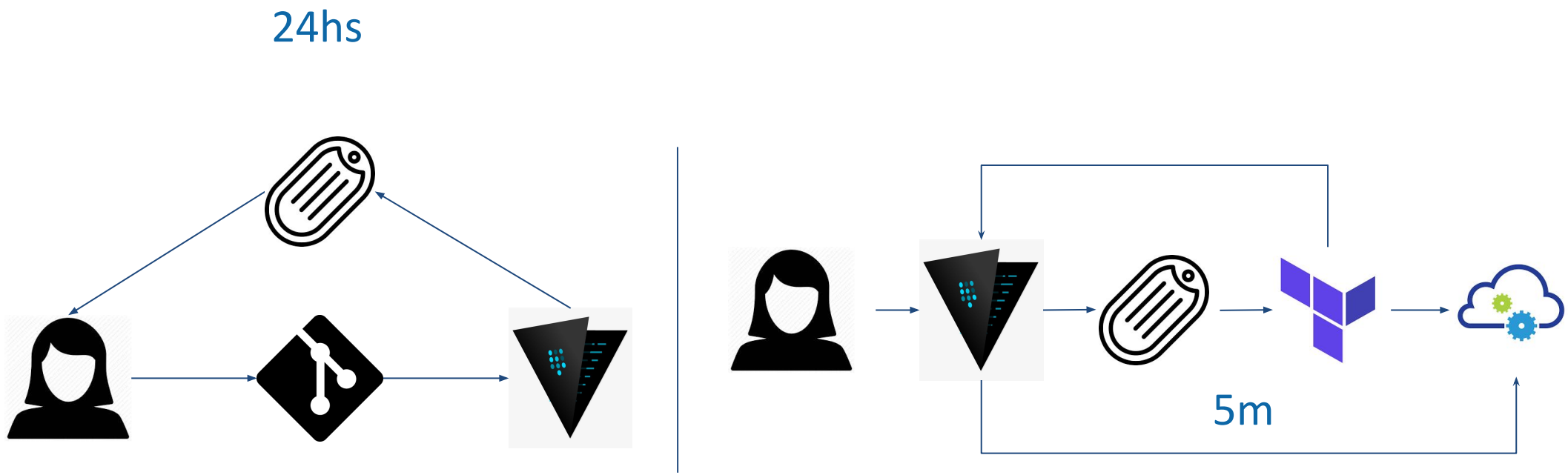
“Porque lo único difícil de DevSecOps es pronunciarlo”

IaC - Gestion de Secretos

- Centralizar los secretos
- Secretos dinámicos
- Auditabilidad de los secretos

“Porque lo único difícil de DevSecOps es pronunciarlo”

IaC - Gestion de Secretos



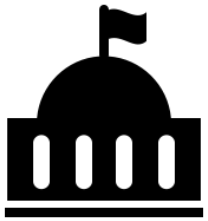
“Porque lo único difícil de DevSecOps es pronunciarlo”

IaC - Gestion de Secretos

Multi Terralith / Modular

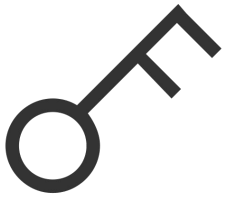
Remote state

- versionado
- state lock



Policy as Code

Config as Code



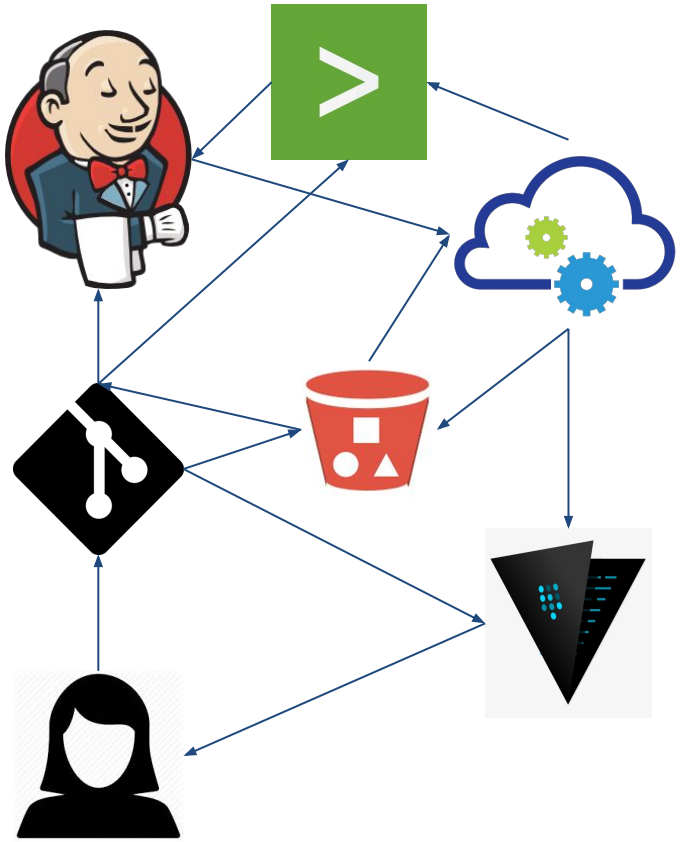
Dynamic Secrets

“Porque lo único difícil de DevSecOps es pronunciarlo”

```
export VAULT_ADDR='http://127.0.0.1:8200'
```

DEVSECOPS Latinoamérica

IaC - arquitectura



Quien crea (y mantiene) la infraestructura

que crea la infraestructura?

“Porque lo único difícil de DevSecOps es pronunciarlo”

IaC - arquitectura

No se trata solamente de la estructura del código..

Si no también de la arquitectura de soporte y orquestación

“Porque lo único difícil de DevSecOps es pronunciarlo”

Gracias! / Preguntas?

DEVSECOPS Latinoamérica

Muchas gracias!

Preguntas?

Contenido de esta charla

https://github.com/jnahuelperez/dsolatam2020

“Porque lo único difícil de DevSecOps es pronunciarlo”