HashiCorp

Terraform

Az IaC svájci bicskája

Láng Máté, 2021 március, HWSW free! meetup

Ki vagyok én?

- Szabadúszó konzultáns

- Ezelőtt:
  - Cloud TL @ Connatix
  - CTO @ SmartUp

- Tapasztalat:
  - Java, Go
  - AWS
  - Kubernetes
  - Terraform

https://unsplash.com/photos/DijA5f0voGQ

Chernobyl series, HBO

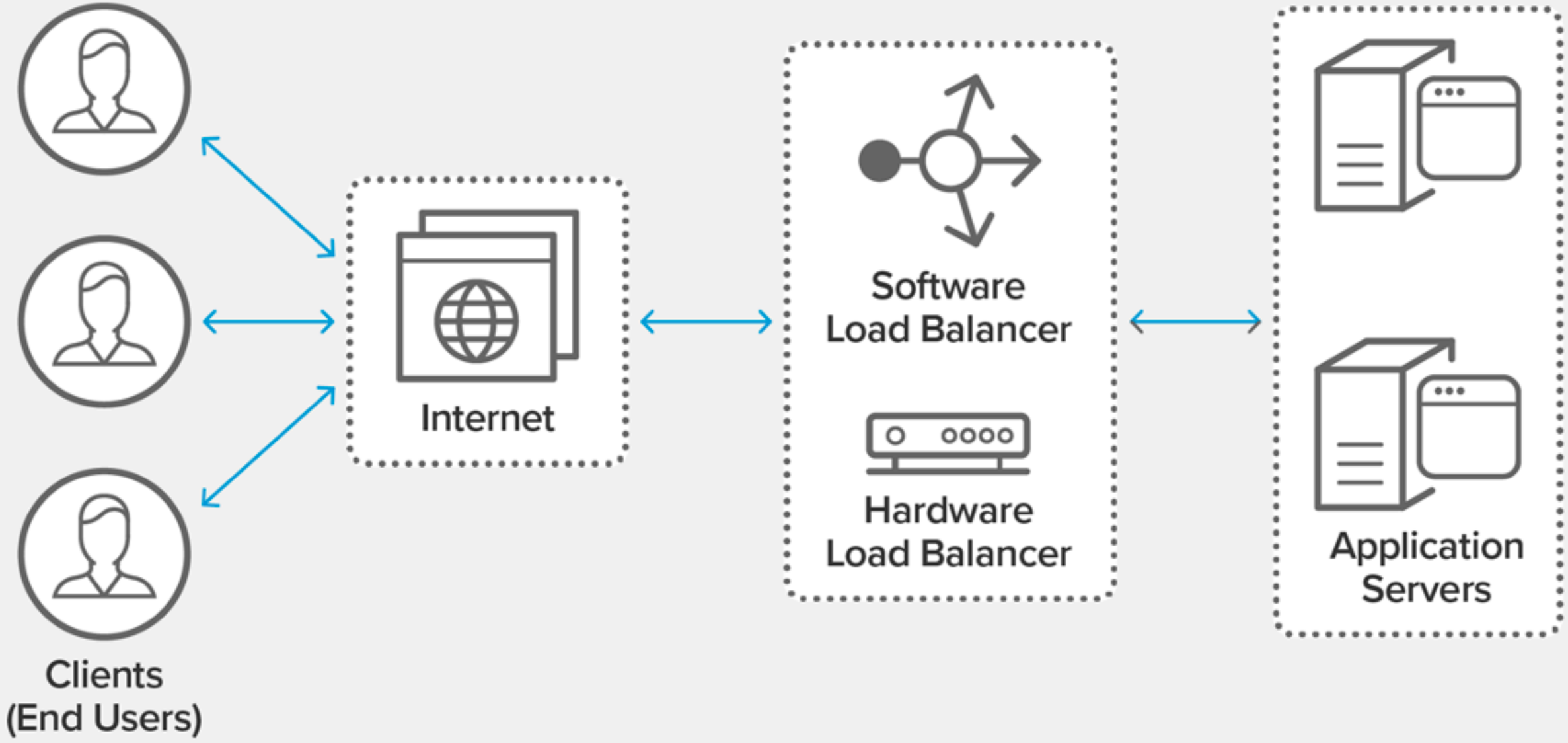
https://drivemag.com/news/first-pre-production-bmw-x7-models-roll-off-the-assembly-line

https://unsplash.com/@jstrippa

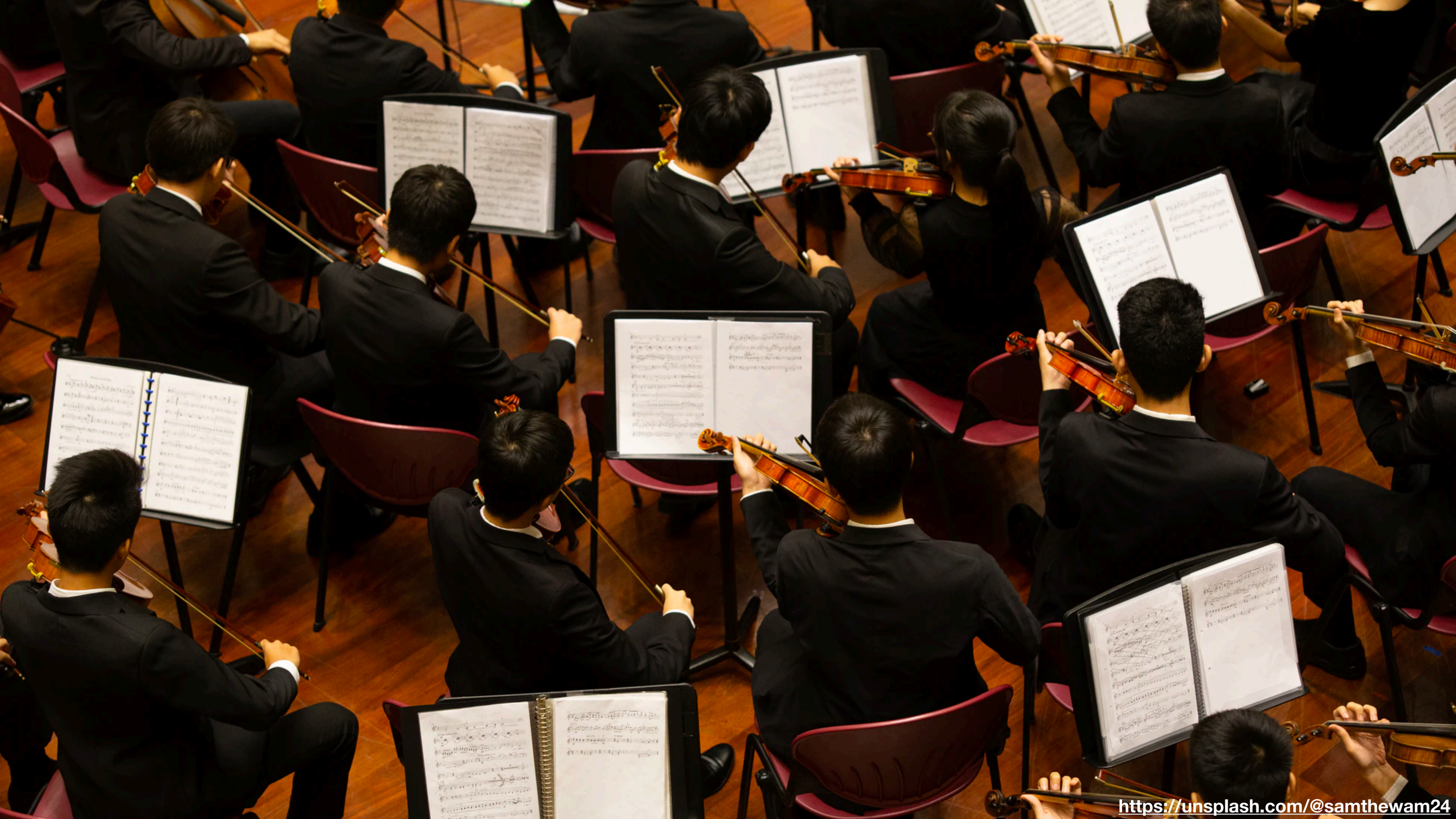
Ha egy dologról tanulhatunk a fejlesztőktől…

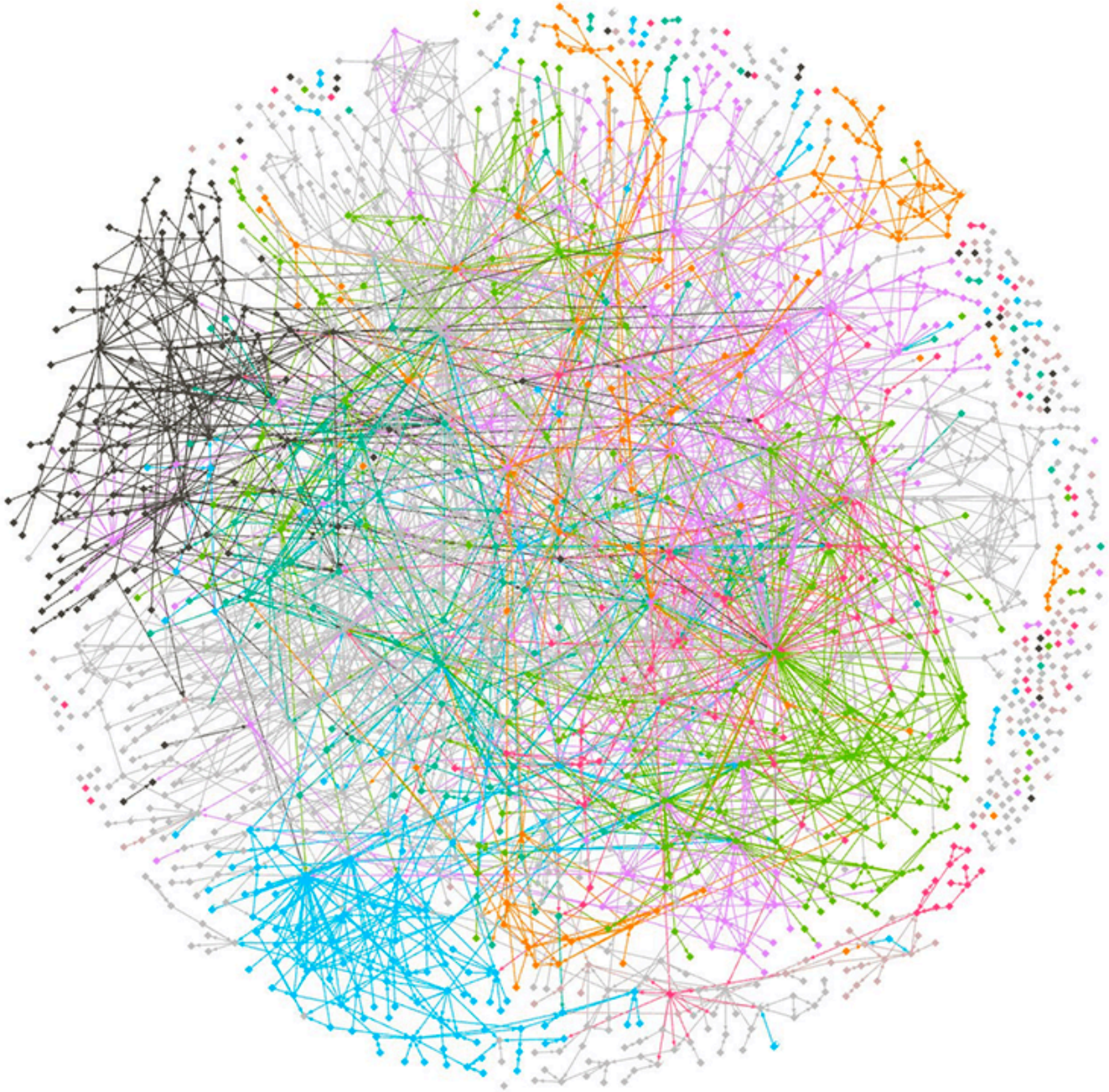
https://unsplash.com/@jstrippa

A fegyelemről



https://www.nginx.com/resources/glossary/load-balancing


https://unsplash.com/@samthewam24



Dependency Map
Monzo’s 1500 microservices

https://monzo.com/blog/we-built-network-isolation-for-1-500-services

A fegyelem nem skálázódik

https://unsplash.com/@samthewam24

Devolúció

Ha a programozók fegyelmezettebbek lennének, jobb kódot írhatnának

- Memória menedzsment tipikus példája
- malloc/free és new/delete C/C++-ban
  - A programozó mentális modellt épít a használt memória területek tulajdonosi gráfjáról és ezt tiszteletbe tartja
- A modern nyelvek automatikusan kezelik a memóriát (pl hivatkozás számolás)
  - A kapcsolatok jelentősségére fekteti a hangsúlyt

https://www.sicpers.info/2020/10/discipline-doesnt-scale

A számítógépek azért vannak, ismétlődő adatfeldolgozási feladatokat végezzenek.

Programozókat arra kötelezni, hogy szabályokat követve, adatfeldolgozási feladatokat hajtsanak végre, egyszerűen pazarlás.

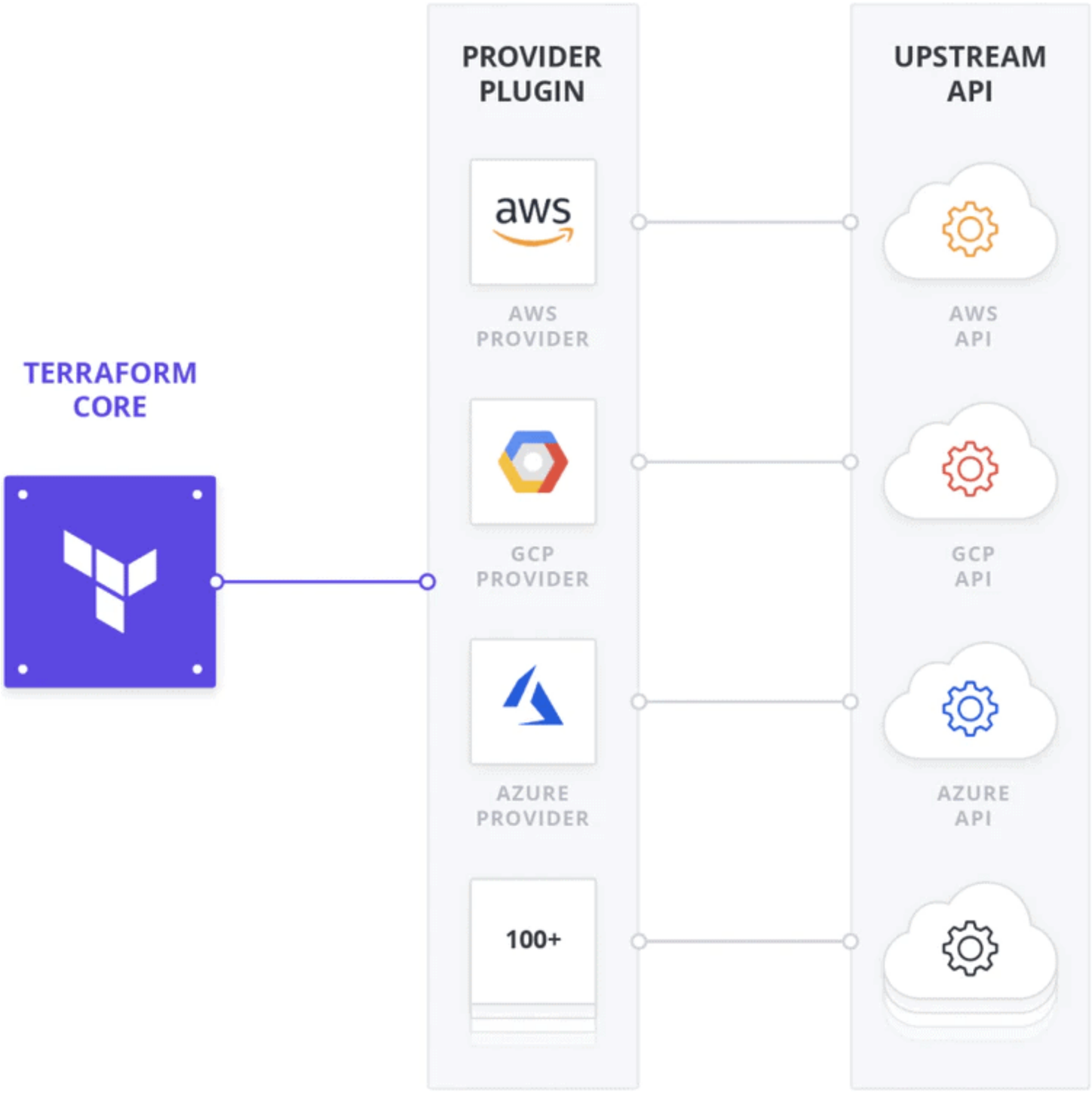
Graham Lee, 2020 (szabadfordítás)

https://www.sicpers.info/2020/10/discipline-doesnt-scale

Helló Terraform!

Az IaC svájci bicskája

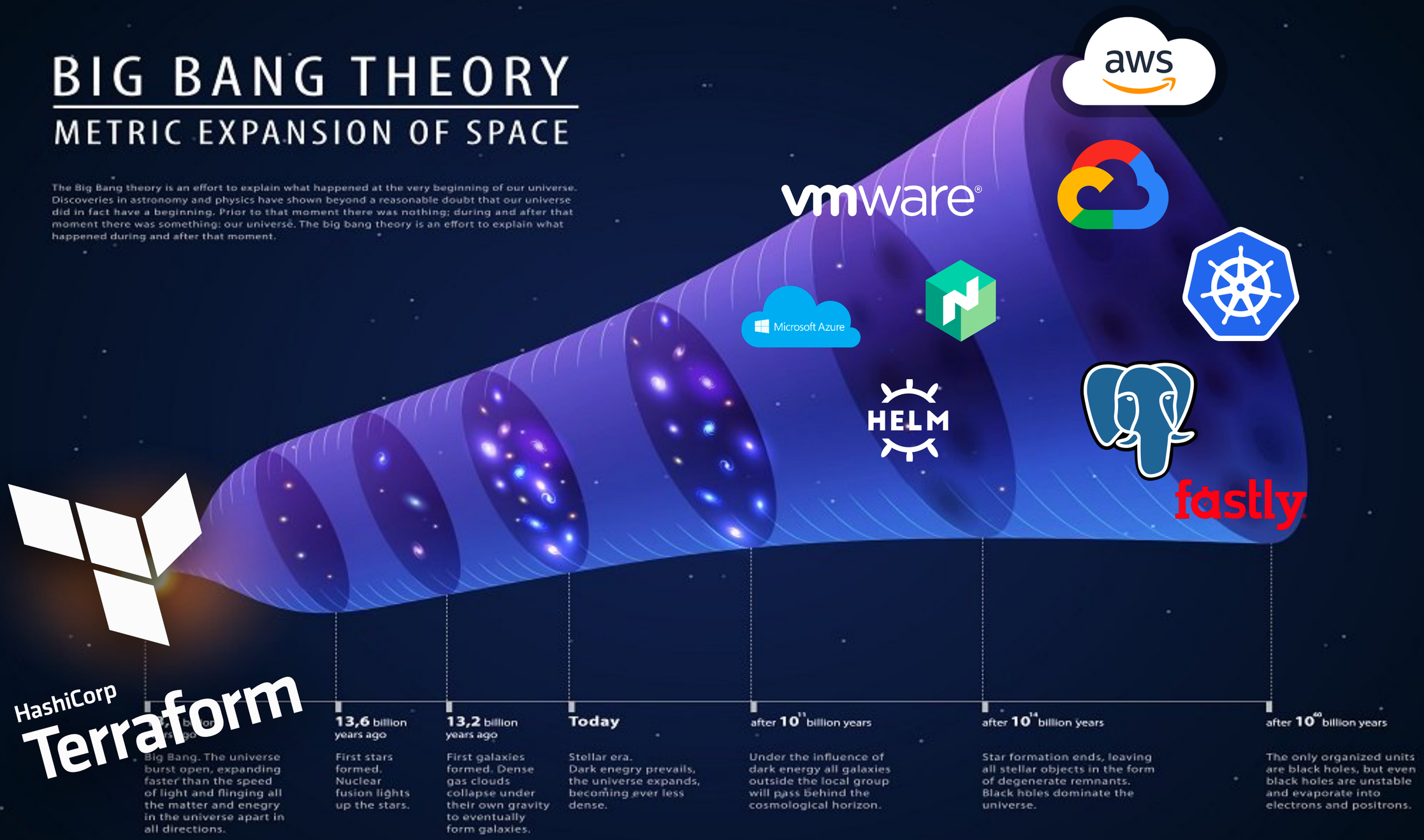
- Verziózható
- Deklaratív
- Barátságos leírónyelv (HCL)
- Rengeteg provider (és bővíthető)
- Beépített dry run
- Interpoláció
- Go alapú


PROVIDER PLUGIN
UPSTREAM API
TERRAFORM CORE
aws
AWS PROVIDER
AWS API
GCP PROVIDER
GCP API
AZURE PROVIDER
AZURE API
100+

BIG BANG THEORY

METRIC EXPANSION OF SPACE

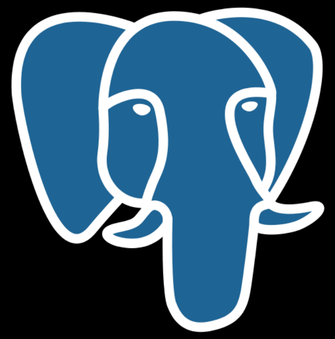
The Big Bang theory is an effort to explain what happened at the very beginning of our universe. Discoveries in astronomy and physics have shown beyond a reasonable doubt that our universe did in fact have a beginning. Prior to that moment there was nothing; during and after that moment there was something: our universe. The big bang theory is an effort to explain what happened during and after that moment.



Terraform Provider-ek

vmware®

fastly®



Logos owned by respective trademark owners

Terraform erőforrások

Azaz a Terraform építő kockája

- Egy telepített provider által kezelt erőforrás (resource)
- Azonosítóval ellátott
- Változók jelenléte
- Referencia más erőforrásokra
- Implicit függőségi viszony
- Erősen típusos

```
resource "aws_instance" "iac_in_action" {
  ami               = var.ami_id
  instance_type     = var.instance_type
  availability_zone = var.availability_zone

  // dynamically retrieve SSH Key Name
  key_name = aws_key_pair.iac_in_action.key_name

  // dynamically set Security Group ID (firewall)
  vpc_security_group_ids = [aws_security_group.iac_in_action.id]

  tags = {
    Name = "Terraform-managed EC2 Instance for IaC in Action"
  }
}
```

Terraform data providerek

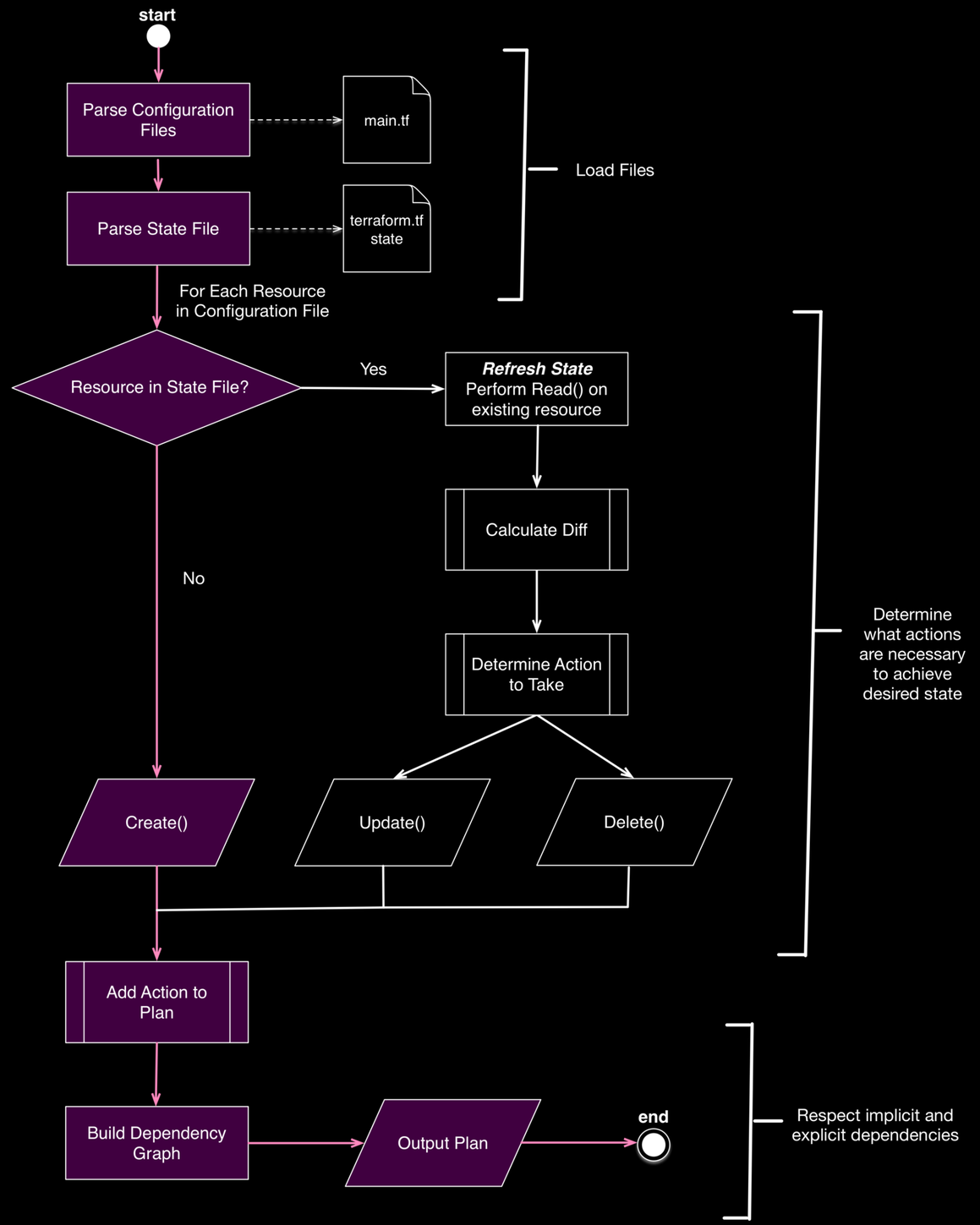
Lekérdezések

- Nem általunk kezelt erőforrások tulajdonságainak lekérdezésére használható
- Szűrési lehetőségek

```
data "aws_ami" "example" {
  executable_users = ["self"]
  most_recent      = true
  name_regex       = "^myami-\\d{3}"
  owners           = ["self"]

  filter {
    name   = "name"
    values = ["myami-*"]
  }

  filter {
    name   = "root-device-type"
    values = ["ebs"]
  }

  filter {
    name   = "virtualization-type"
    values = ["hvm"]
  }
}
```

Terraform - State

- A Terraform-nak szüksége van egy állapot file-ra
  - Egyfajta leltár, leképezés az eszköz által kezelt erőforrások és a valódi erőforrások között
  - Minden futtatás előtt frissítve van
- terraform.tfstate fájlban van tárolva (egyszerű esetben disken)
- Távoli tárolás (remote backend)
  - Engedélyezi a kollaboratív, párhuzamos fejlesztést.
    Backendek: s3, consul, gcs, azurerm, artifactory, http
  - Párhuzamos futtatás esetén lock használata ajánlott.
    Pl: Consul out-of-the box támogatja, S3+DynamoDB locking
  - Optimistic locking használata


start
Parse Configuration Files
main.tf
Parse State File
terraform.tf state
Load Files
For Each Resource in Configuration File
Resource in State File?
Yes
Refresh State
Perform Read() on existing resource
Calculate Diff
Determine Action to Take
No
Create()
Update()
Delete()
Determine what actions are necessary to achieve desired state
Add Action to Plan
Build Dependency Graph
Output Plan
end
Respect implicit and explicit dependencies

Gyakori munkamenet és parancsok

- init
- validate
- plan
- apply
- destroy

```
➜  iac-in-action git:(main) ✗
```

A svájci bicska

AzureAD csoport

- Azure Active Directory
- Csoport, felhasználó és tagság kezelése
- AzureAD Appok kezelése

```
resource "azuread_user" "example" {
  display_name        = "J Doe"
  password            = "notSecure123"
  user_principal_name = "jdoe@hashicorp.com"
}

resource "azuread_group" "example" {
  display_name = "MyGroup"
  members = [
    azuread_user.example.object_id,
    /* more users */
  ]
}
```

A svájci bicska

Helm release

- Helm, a Kubernetes ökoszisztéma népszerű package manager-je
- Komplex felhő alapú szolgáltatások esetén nagy segítség a Helm provider: injektálható értékek terraform állapotból.
- Pl. S3 bucket ARN

```
resource "helm_release" "example" {
  name       = "my-redis-release"
  repository = "https://charts.bitnami.com/bitnami"
  chart      = "redis"
  version    = "6.0.1"

  values = [
    "${file("values.yaml")}"
  ]

  set {
    name  = "cluster.enabled"
    value = "true"
  }

  set {
    name  = "metrics.enabled"
    value = "true"
  }

  set {
    name  = "service.annotations.prometheus\\.io/port"
    value = "9127"
    type  = "string"
  }
}
```

A svájci bicska

Kubernetes secret

- Kubernetes erőforrások
  - Namespace
  - Deployment
  - StatefulSet
  - stb

```
resource "kubernetes_secret" "example" {
  metadata {
    name = "basic-auth"
  }

  data = {
    username = "admin"
    password = "P4ssw0rd"
  }

  type = "kubernetes.io/basic-auth"
}
```

A svájci bicska

Fastly CDN szolgáltatás

- Fastly
- CloudFlare
- Akamai

```
resource "fastly_service_v1" "demo" {
  name = "demofastly"

  domain {
    name    = "demo.notexample.com"
    comment = "demo"
  }

  backend {
    address = "127.0.0.1"
    name    = "localhost"
    port    = 80
  }

  force_destroy = true
}
```

A svájci bicska

Saját Certificate Authority

```
resource "tls_private_key" "example" {
  algorithm   = "ECDSA"
  ecdsa_curve = "P384"
}
```

```
resource "tls_cert_request" "example" {
  key_algorithm   = "ECDSA"
  private_key_pem = "${file("private_key.pem")}"

  subject {
    common_name  = "example.com"
    organization = "ACME Examples, Inc"
  }
}
```

```
resource "tls_locally_signed_cert" "example" {
  cert_request_pem   = "${file("cert_request.pem")}"
  ca_key_algorithm   = "ECDSA"
  ca_private_key_pem = "${file("ca_private_key.pem")}"
  ca_cert_pem        = "${file("ca_cert.pem")}"

  validity_period_hours = 12

  allowed_uses = [
    "key_encipherment",
    "digital_signature",
    "server_auth",
  ]
}
```

ndmckinley / terraform-provider-dominos

Code | Issues 11 | Pull requests 3 | Actions | Security | Insights

master | 2 branches | 0 tags | Go to file | Add file | Code

ndmckinley Merge pull request #1 from davewongillies/tf_fmt ... 70f8407 on 7 May 2019 22 commits

bin	Add binary, for ease of distribution. should be low traffic.	2 years ago
docs	Merge pull request #1 from davewongillies/tf_fmt	2 years ago
.gitignore	Update docs to point to binary directly.	2 years ago
LICENSE	Create LICENSE	2 years ago
Makefile	Write docs first draft, rename address.	2 years ago
README.md	Fmt the example code	2 years ago
data_source_address.go	Write docs first draft, rename address.	2 years ago
data_source_menu.go	Initial commit - working dominos pizza orderer, tracker.	2 years ago
data_source_menu_item.go	Initial commit - working dominos pizza orderer, tracker.	2 years ago
data_source_store.go	Initial commit - working dominos pizza orderer, tracker.	2 years ago
data_source_tracking.go	Initial commit - working dominos pizza orderer, tracker.	2 years ago
main.go	Initial commit - working dominos pizza orderer, tracker.	2 years ago
provider.go	Write docs first draft, rename address.	2 years ago
resource_order.go	Update order with results from further testing.	2 years ago

Terraform Modulok

Azaz, Do Not Repeat Yourself

- Független, újrafelhasználhatóságot támogató egység
- Legfelsőbb szinten a root module található
- Példányosítható és paraméterezhető
- Kiválóan alkalmas egyes környezetek közötti különbségek meghatározására

```
module "vpc" {
  source = "terraform-aws-modules/vpc/aws"

  name = "my-vpc"
  cidr = "10.0.0.0/16"

  azs             = ["eu-west-1a", "eu-west-1b", "eu-west-1c"]
  private_subnets = ["10.0.1.0/24", "10.0.2.0/24", "10.0.3.0/24"]
  public_subnets  = ["10.0.101.0/24", "10.0.102.0/24", "10.0.103.0/24"]

  enable_nat_gateway = true
  enable_vpn_gateway = true

  tags = {
    Terraform = "true"
    Environment = "dev"
  }
}
```

Terraform | Registry

Search Providers and Modules

Browse Publish Sign-in

Providers Modules

FILTERS Clear Filters

Provider

Provider

Modules

Modules are self-contained packages of Terraform configurations that are managed as a group.

terraform-aws-modules / vpc

Terraform module which creates VPC resources on AWS

a month ago 8.2M aws provider

terraform-aws-modules / security-group

Terraform module which creates EC2-VPC security groups on AWS

a month ago 6.9M aws provider

terraform-aws-modules / eks

Terraform module to create an Elastic Kubernetes (EKS) cluster and associated worker instances on AWS

2 months ago 3.4M aws provider

terraform-aws-modules / rds

Terraform module which creates RDS resources on AWS

8 days ago 3.0M aws provider

terraform-aws-modules / iam

Terraform module which creates IAM resources on AWS

16 days ago 2.7M aws provider

terraform-google-modules / gcloud

A module for executing gcloud commands within Terraform.

3 months ago 1.6M provider

ORGANIZATION SETTINGS

hashicorp-v2

General
Teams
VCS Providers
API Tokens
Authentication
SSH Keys
Policies
Policy Sets

Policy Sets

Create a new policy set

Policy sets are groups of policies which may be enforced on workspaces. Please see the Sentinel in Terraform Enterprise documentation.

global

This set has been created for you to maintain previous behavior. Feel free to re-organize your policies as y...

All workspaces — Last updated 8 months ago

tfe-feature-flags

Policies managed individually

A set of feature flag policies.

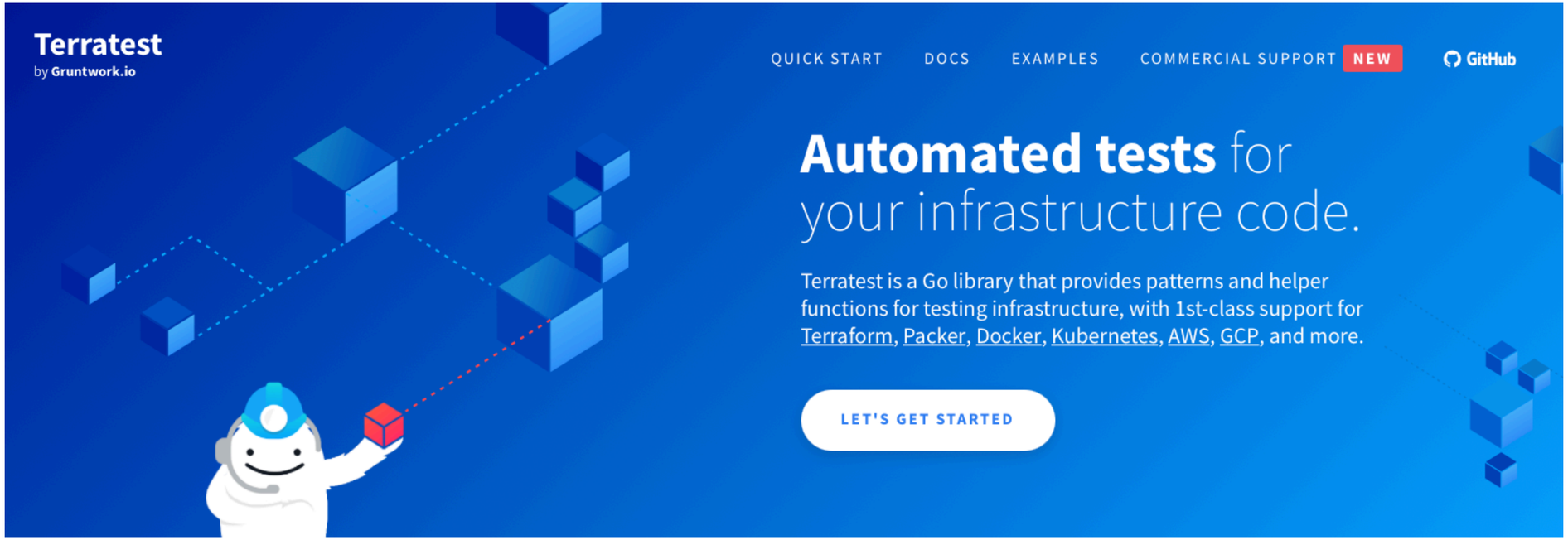
1 Workspace · 1 Policy — Last updated 8 months ago

tfe-policies-examples

Policies managed individually

Applies the example policies to this workpace.

1 Workspace · 4 Policies — Last updated 8 months ago



Test infrastructure code with Terratest **in 4 steps**

Write test code using Go

Create a file ending in `_test.go` and run tests with the go test command. E.g., `go test my_test.go`.

Use Terratest to deploy infrastructure

Use Terratest to execute your real IaC tools (e.g., Terraform, Packer, etc.) to deploy real infrastructure (e.g., servers) in a real environment (e.g., AWS).

Validate infrastructure with Terratest

Use the tools built into Terratest to validate that the infrastructure works correctly in that environment by making HTTP requests, API calls, SSH connections, etc.

Undeploy

Undeploy everything at the end of the test.

Útravaló

Legalább ez maradjon meg!

- 2020 szívás 🦠
- 2021 is szívás 🦠
- A szoftverek komplexitása hatalmasat nőtt és a trend egyáltalán nem torpant meg.
- Nincs élő ember aki 1500 szolgáltatás és a köztük levő kapcsolat mentális modelljét agyban eltárolna. Ha mégis, légyszi szóljatok.
- A szoftverfejlesztésből ismert elvek üzemeltetésben is használhatóak
- Bízz az eszközben, ne az emberben.

Köszönöm a figyelmet!

Láng Máté
mate.lang@binhatch.com

linkedin.com/in/matelang