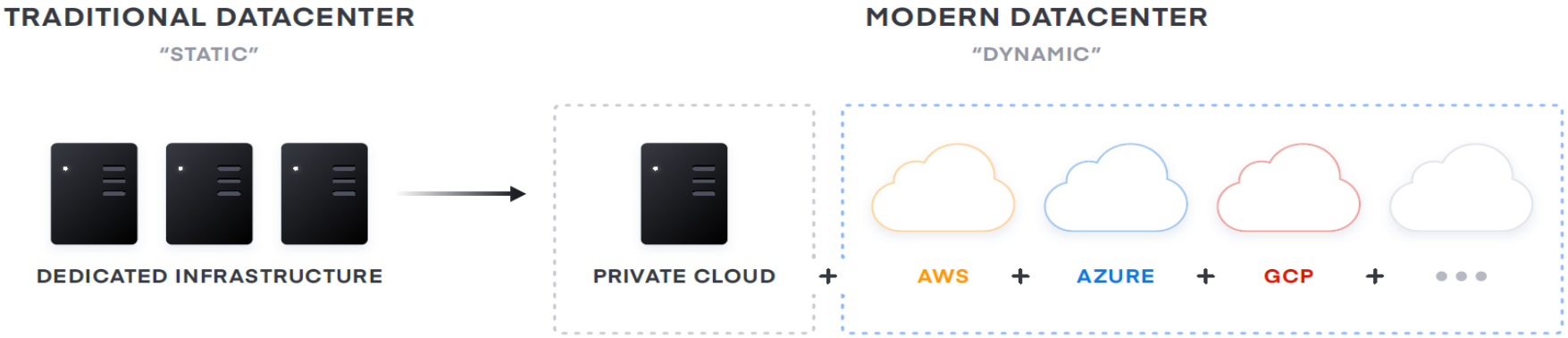
PosAm USEFUL TECHNOLOGIES

Infrastructure as code

Peter Mihalovič
Tomáš Kysela
PosAm spol. s r.o.
11.2.2021

Tranzícia k Multi-Cloud Datacentru



	STATIC		DYNAMIC
Run	Dedicated Infrastructure	→	Scheduled across the fleet
Connect	**Host**-based Dynamic IP	→	**Service**-based Dynamic IP
Secure	High trust **IP**-based	→	Low trust **Identity**-based
Provision	**Dedicated** servers Homogeneous	→	Capacity **on-demand** Heterogeneous

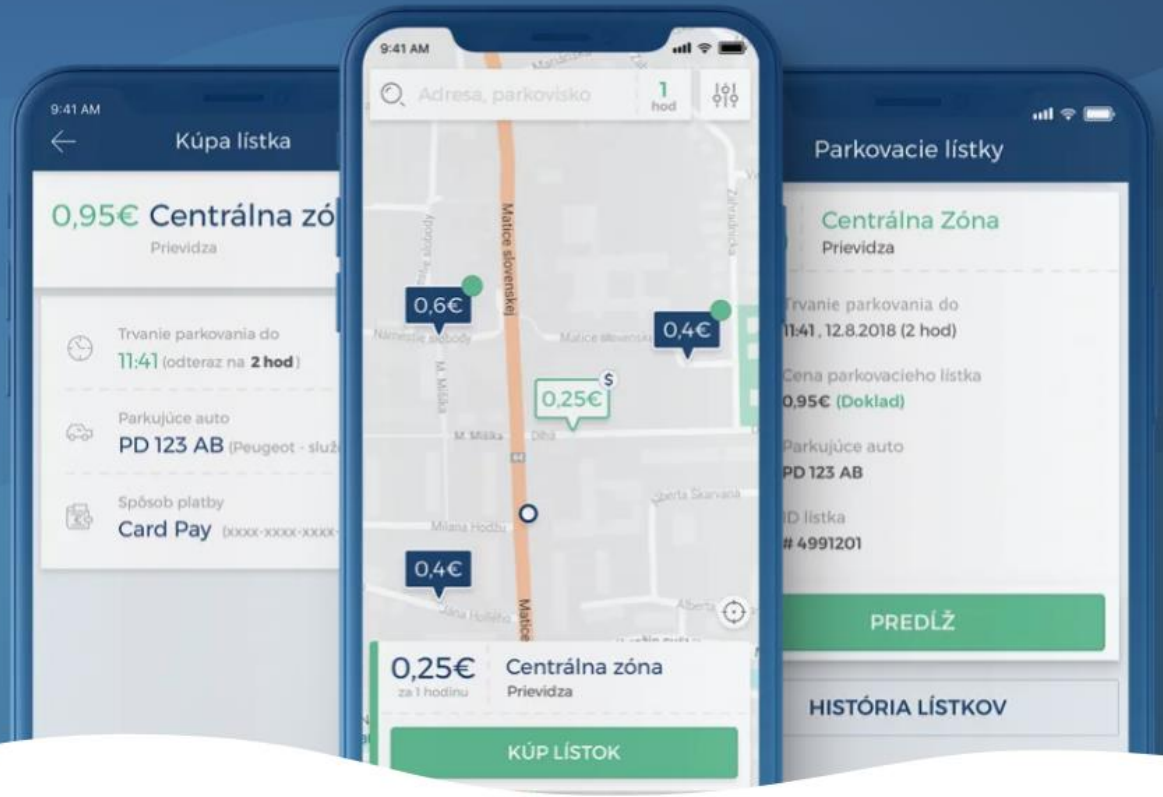
ParkDots - Nájdi ľahko voľné miesto a zaplať parkovné jedným ťahom

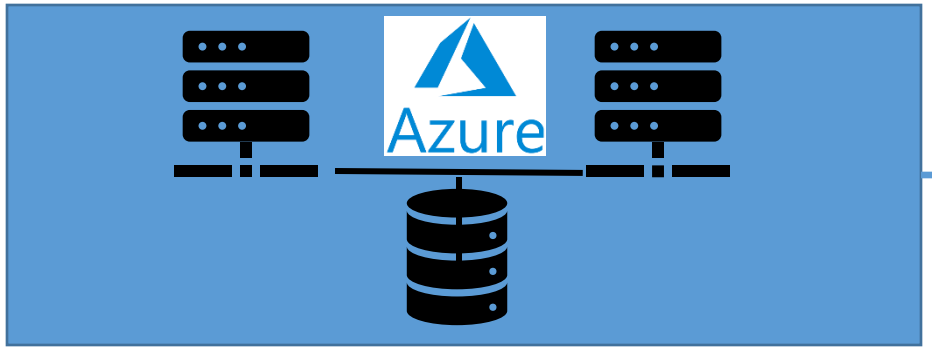
Partizánske, Stará Ľubovňa, Senec, Dolný Kubín, Prievidza, Liptovský Mikuláš, Trnava, Bratislava, Trenčín, Nitra, Modra, Banská Štiavnica...

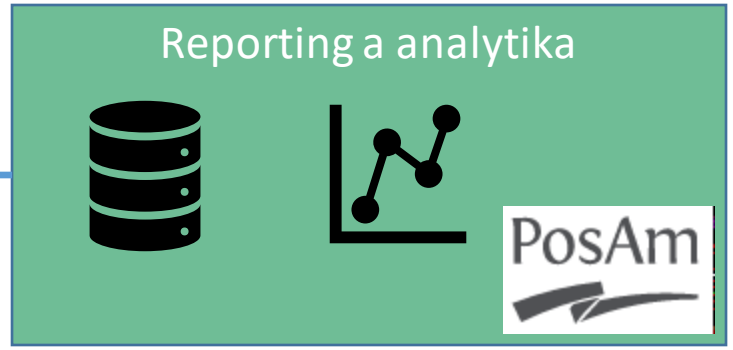
VYSKÚŠAJ SI PARKDOTS

Available on the App Store

GET IT ON Google play







Paradigmy správy infraštruktúry

- **Procedurálne versus deklaratívne definície**
  - Procedurálne definície sú väčšinou skripty, ktoré obsahujú sekvenčný postup krokov ktoré treba vykonať
  - Deklaratívne definície špecifikujú výsledný stav a systém sám vykoná príslušné kroky bez toho aby sme definovali ich poradie

- **Mutable versus immutable infraštruktúra**
  - Pri mutable infraštruktúre sa zmeny (OS update, patches) robia na živých, produkčných systémoch
  - Pri immutable infraštruktúre sa systémy neaktualizujú ale sa kompletne prenasadia keď to je potrebné

- **Orchestrácia versus správa konfigurácií**
  - Orchestračné nástroje *(Terraform alebo AWS CloudFormation)* zabezpečujú úvodné nasadenie alebo konfiguráciu infraštruktúry
  - Nástroje správy konfigurácie *(Ansible, Saltstack, Puppet, Cheff)* automatizujú konfiguráciu komponentov, aplikácií a kontrolu nasadených zdrojov

Prevádzkový toolset IaC

PosAm USEFUL TECHNOLOGIES

SALTSTACK.
Now part of VMware

Provision / Operations

Terraform

Multi-Cloud **Infrastructure Provisioning**

—

Reproducible Infrastructure as Code

Compliance & Management

HashiCorp Packer

Secure / Security

Vault

Multi-Cloud **Security**

—

Secrets Management

Encryption as a Service

Connect / Networking

Consul

Multi-Cloud **Service Networking**

—

Service Registry & Discovery

Service Mesh

Run / Development

Nomad

Multi-Cloud **Application Delivery**

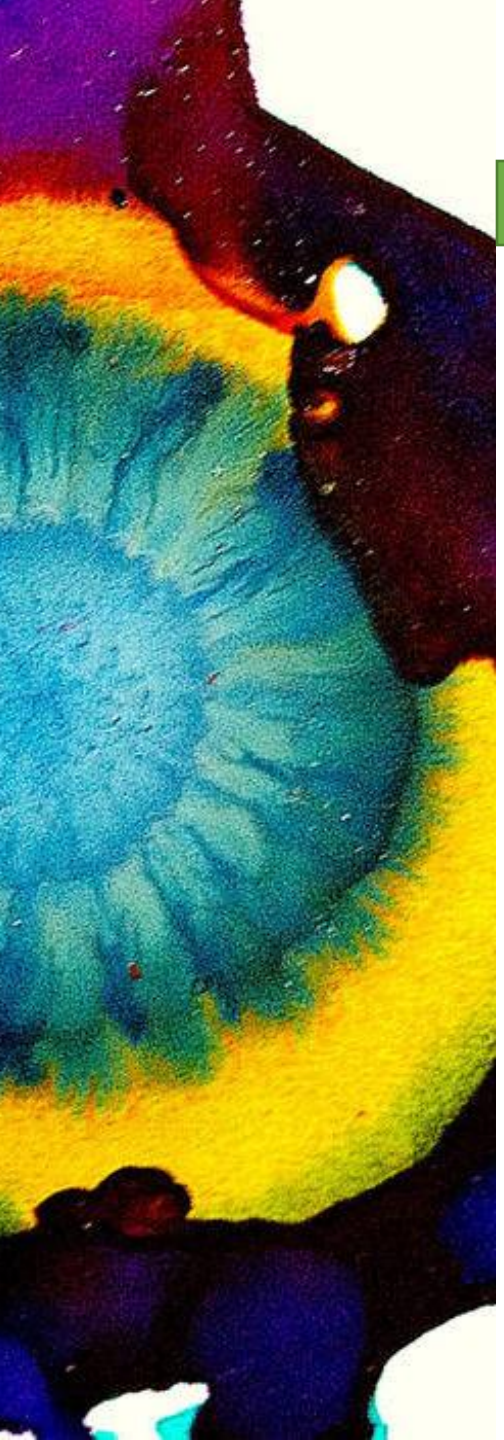
—

Heterogeneous Workload Orchestration

Multi-datacenter Orchestration

PosAm USEFUL TECHNOLOGIES

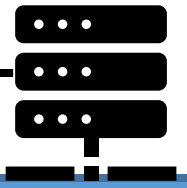
DEMO



Demo infraštruktúra

PosAm USEFUL TECHNOLOGIES

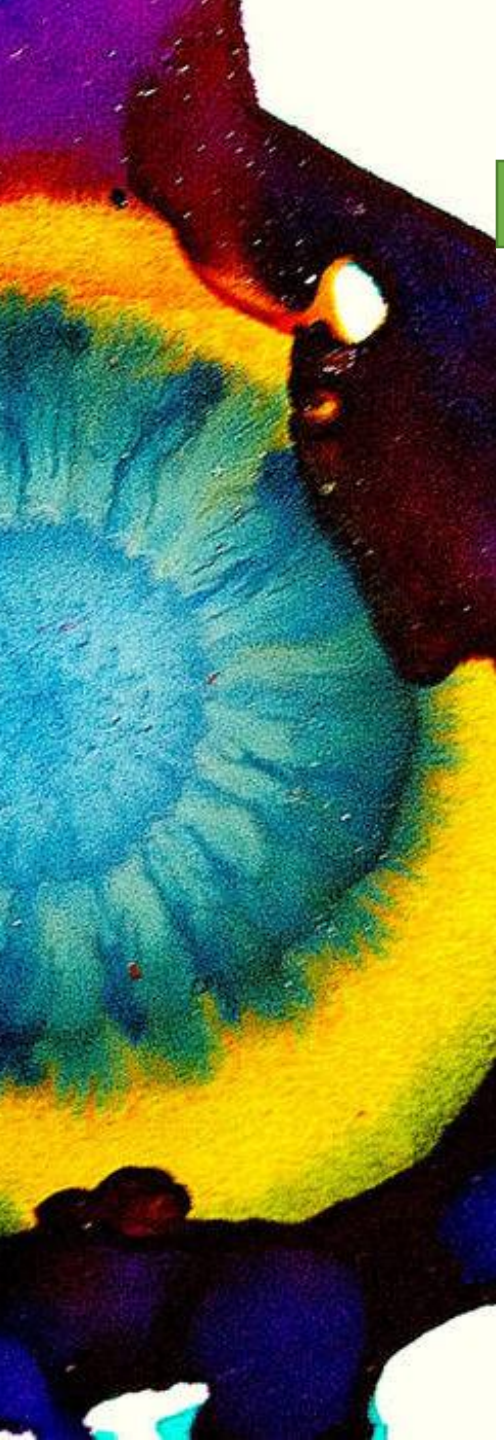
Corporate Network



Virtual router

Virtual Private Cloud

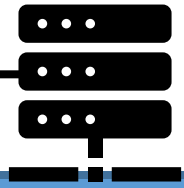
```
resource "cloudstack_vpc" "vpc1" {
  name           = "vpc1"
  cidr           = "10.0.0.0/16"
  vpc_offering   = "Default VPC offering"
  network_domain = "test.local"
  zone           = “p1_testdev“
}
```



Demo infraštruktúra

PosAm USEFUL TECHNOLOGIES

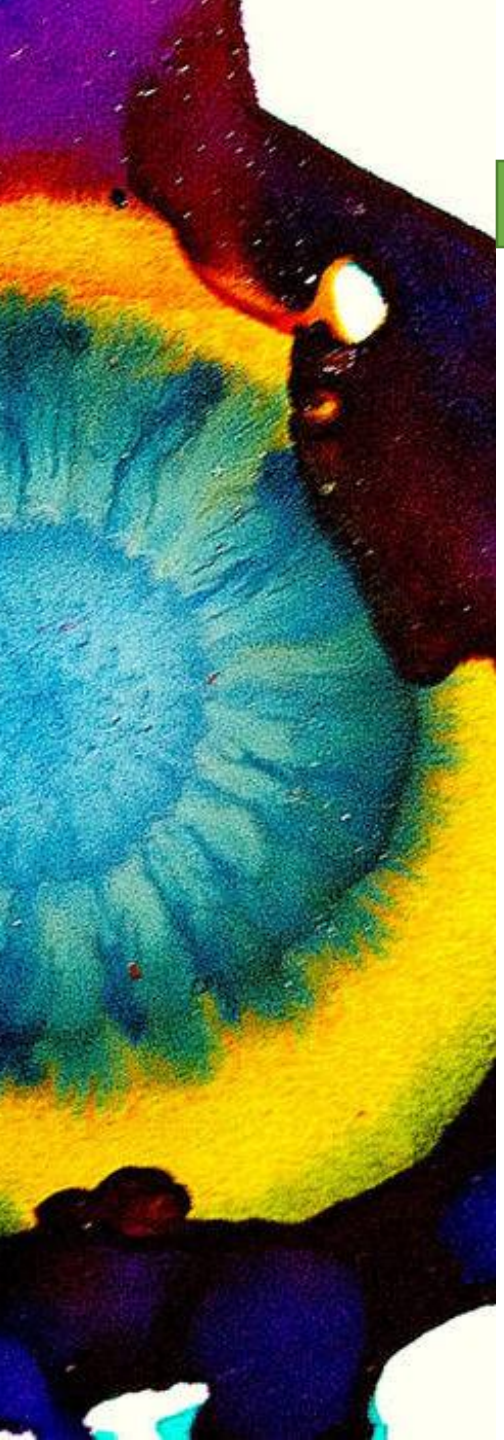
Corporate Network



Virtual router
+ Firewall

Virtual Private Cloud

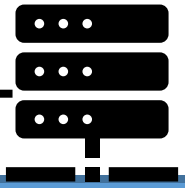
```
resource "cloudstack_network_acl_rule" "default" {
  acl_id = cloudstack_network_acl.default.id

  rule {
    action       = "allow"
    cidr_list    = ["0.0.0.0/0"]
    protocol     = "tcp"
    ports        = ["443", "22", "80", "9100"]
    traffic_type = "ingress"
  }

  rule {
    action       = "allow"
    cidr_list    = ["0.0.0.0/0"]
    protocol     = "all"
    traffic_type = "egress"
  }
}
```



Demo infraštruktúra

PosAm USEFUL TECHNOLOGIES

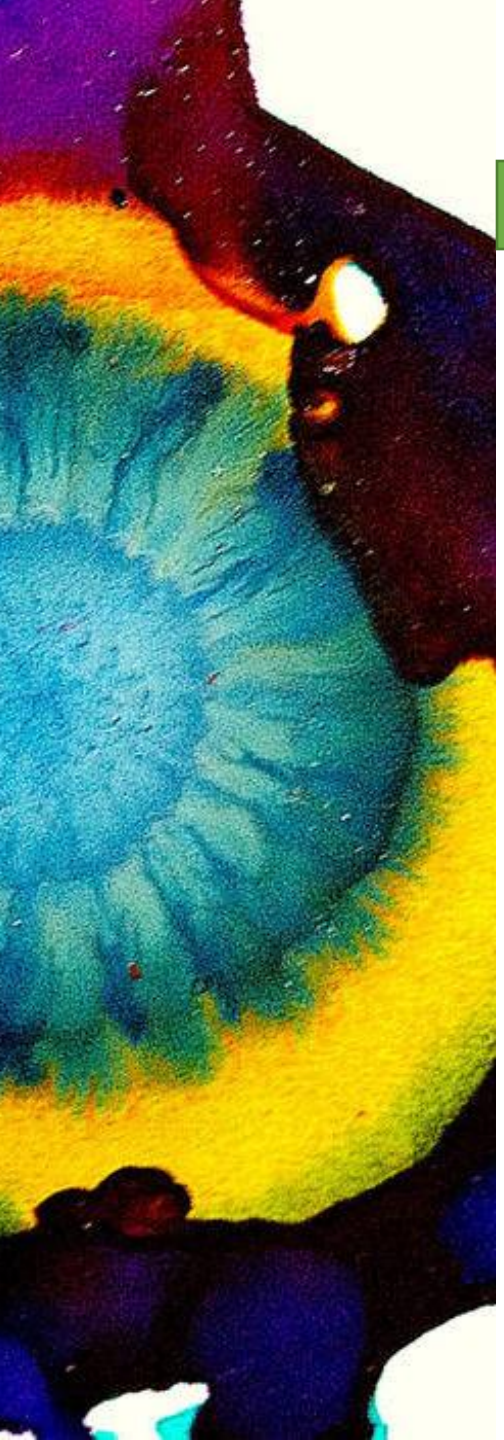
Corporate Network



Virtual router
+ Firewall + DHCP/DNS

Virtual Private Cloud

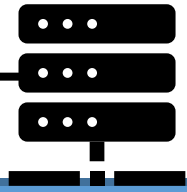
```
resource "cloudstack_network" „frontend" {
  name             = „frontend"
  cidr             = "10.0.1.0/24"
  network_offering = "DefaultIsolatedNetworkOfferingForVpcNetworks"
  zone             = var.zone
  vpc_id           = cloudstack_vpc.vpc1.id
  acl_id           = cloudstack_network_acl.default.id
}

resource "cloudstack_network" „backend" {
  name             = „backend"
  cidr             = "10.0.2.0/24"
  network_offering = "DefaultIsolatedNetworkOfferingForVpcNetworks"
  zone             = var.zone
  vpc_id           = cloudstack_vpc.vpc1.id
  acl_id           = cloudstack_network_acl.default.id
}
```



Demo infraštruktúra

PosAm USEFUL TECHNOLOGIES

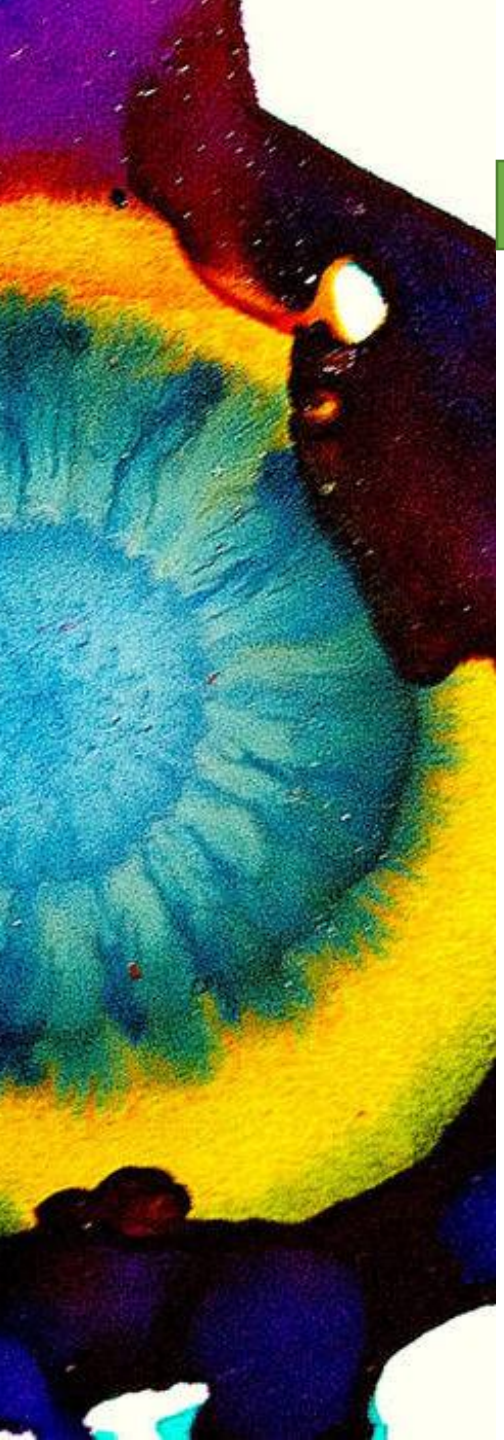
Corporate Network



Virtual router
+ Firewall + DHCP/DNS

Virtual Private Cloud

```
resource "cloudstack_instance" "server-1" {
  name             = "server-1"
  display_name     = "server-1"
  service_offering = "medium-v2"
  network_id       = cloudstack_network.frontend.id
  template         = "centos-75-v1.0"
  zone             = var.zone
}

resource "cloudstack_ipaddress" "server-1-publicip" {
  network_id = cloudstack_network.frontend.id
  vpc_id     = cloudstack_vpc.vpc1.id
}

resource "cloudstack_static_nat" "server-1-snat" {
  ip_address_id      = cloudstack_ipaddress.server-1-publicip.id
  virtual_machine_id = cloudstack_instance.server-1.id
}
```



Demo infraštruktúra

PosAm USEFUL TECHNOLOGIES

Corporate Network

Virtual router
+ Firewall + DHCP/DNS

Virtual Private Cloud

Frontend Network

Server-1

Backend Network

Server-2

Čo vie priniesť Infrastructure as Code?

- **Rýchlejšie a predikovateľné zmeny na infraštruktúre, menej chýb**
- **Rýchlejšie a menej nákladné nasadenie aplikácií**
- **Po zavedení IaC, flexibilnejšie využitie prostredí**
  - „Self service“ pre vývojárov – vytvorím/otestujem/zmažem
- **Štandardizácia konfigurácie prostredí, využitím „katalógových“ komponentov**
- **Lepšie využitie výkonu – vypínanie/mazanie nepotrených prostredí** (školiace, testovacie, developerské)

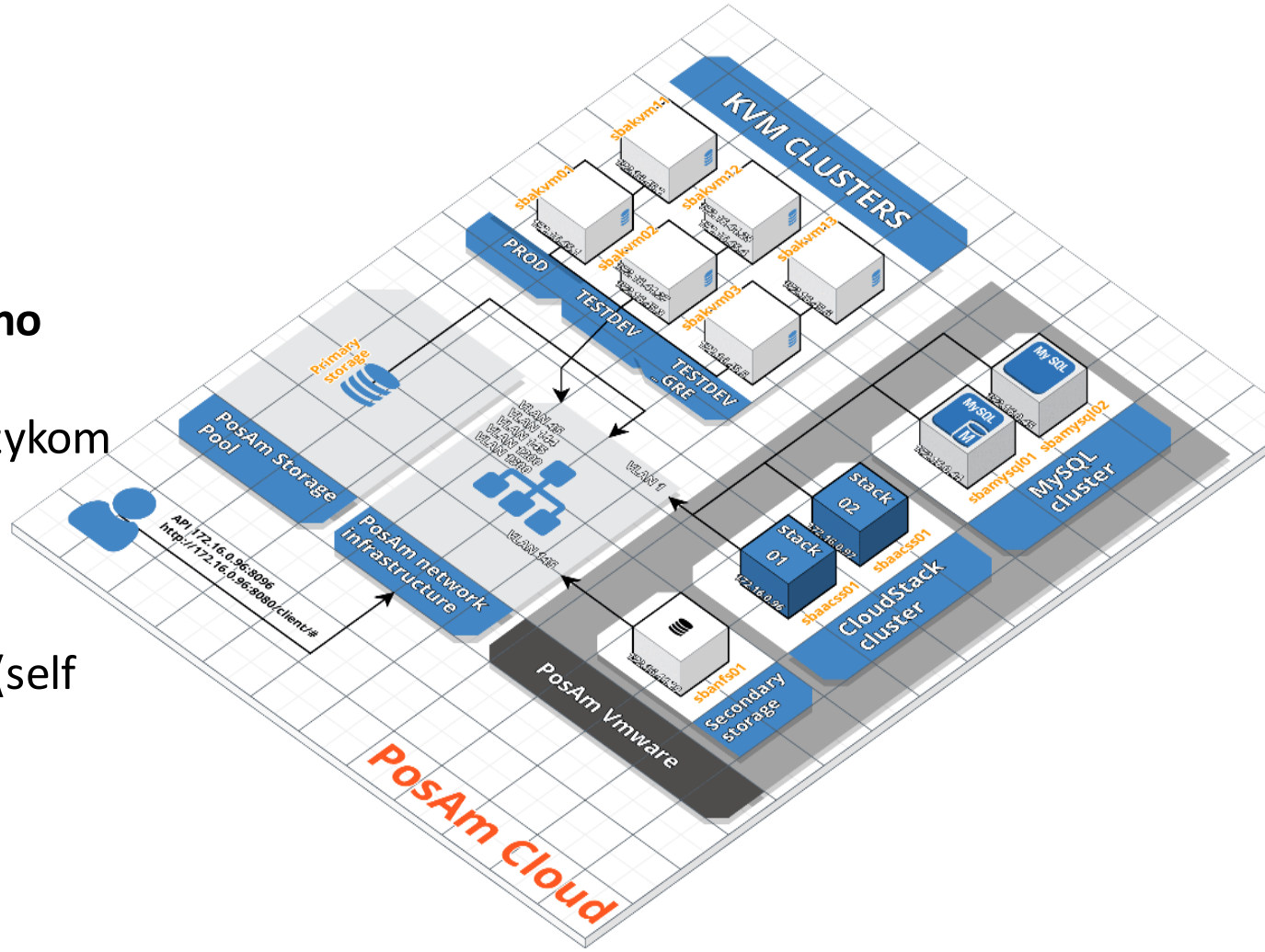
Výzvy pri implementácii IaC

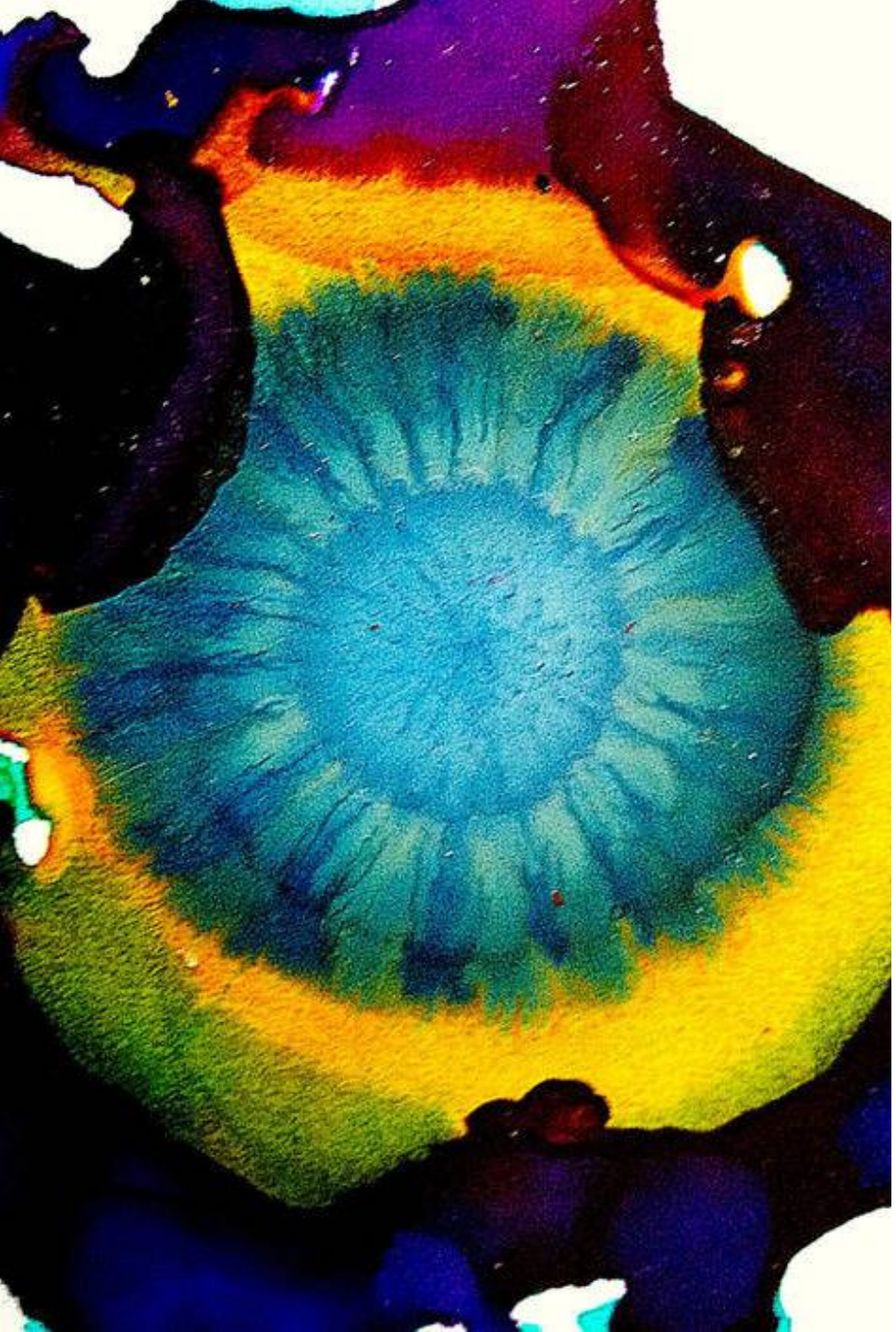
- **Podvozok pre IaC**
  - Zmena architektúry infraštruktúry
  - Vybudovanie Privátneho cloudu

- **Programátorské zručnosti infraštruktúrnych špecialistov**
  - Naučiť ich pracovať ako vývojárov

- **Zavedenie nástrojov orchestrácie a konfiguračného manažmentu**
  - IaC nástroje s jednoduchým deklaratívnym jazykom a modulmi pre infraštruktúrne komponenty

- **Zmena procesov a kultúry**
  - Eliminácia schvaľovania tam kde to je možné (self service)
  - Bez zmeny procesov a kultúry sa nedosahuje požadovaná efektivita





Zavádzanie IaC

PosAm USEFUL TECHNOLOGIES

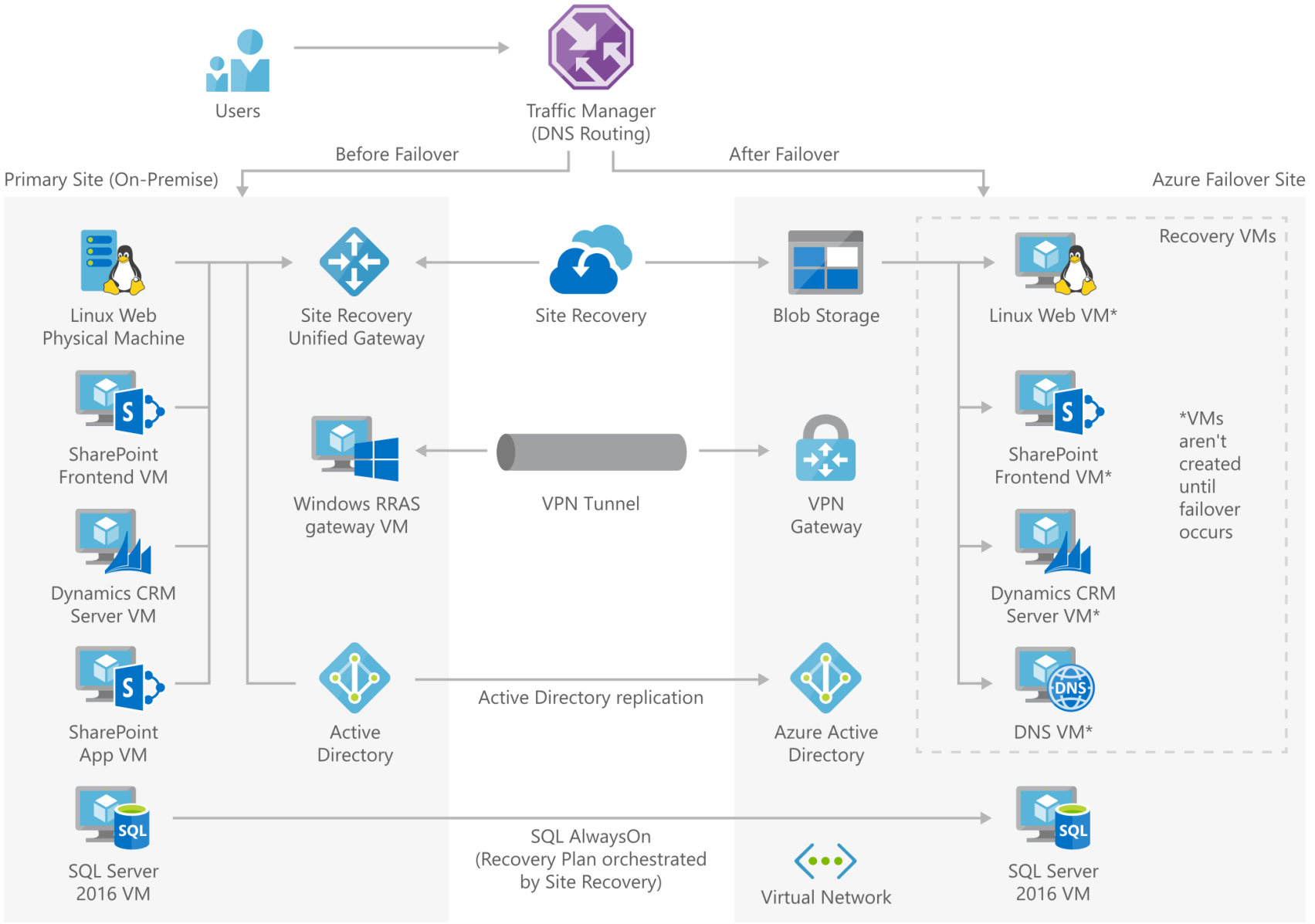
- **Zavedenie programovateľnej infra**
  - Privátny cloud alebo prechod do Cloudu
- **Vytváranie dočasných a nižších projektových prostredí**
  - Využívanie pri vytváraní serverov a sieťovej infraštruktúry
- **Rozšírenie využívania IaC použitím "katalógových" komponentov**
  - Vývoj a reuse štandardizovaných komponentov
- **Doplnenie ďalších nástrojov a techník**
  - Využívanie immutable konceptu (nielen kontajnery)
  - Validačné testovanie po nasadení (či bolo všetko nasadené správne a funguje ako má)
  - Dopojenie do CI/CD workflow

PosAm USEFUL TECHNOLOGIES

Pokročilé scenáre využitia IaC

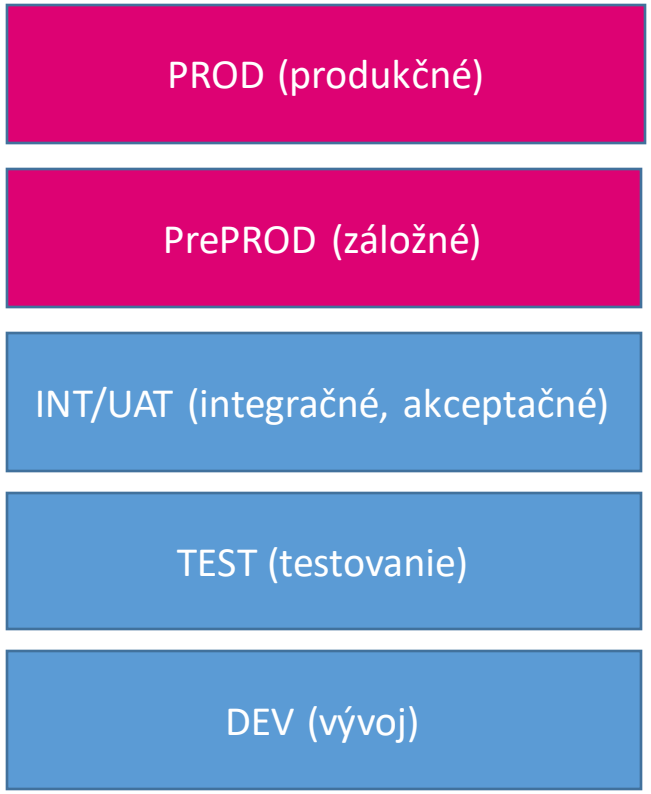
„Instantné“ Disaster Recovery

- **Klasické DR je veľmi nákladné**
- **Zvládnutie IaC je ale pre oblasť DR „Game changer“**
- **Väčšina zdrojov je vytvorených len keď nastane aktivácia DR**
  - Ekonomicky efektívnejšie
- **Dobre nastavenou automatizáciou sa výrazne skráti čas výpadku**



Automatizácia produkcie

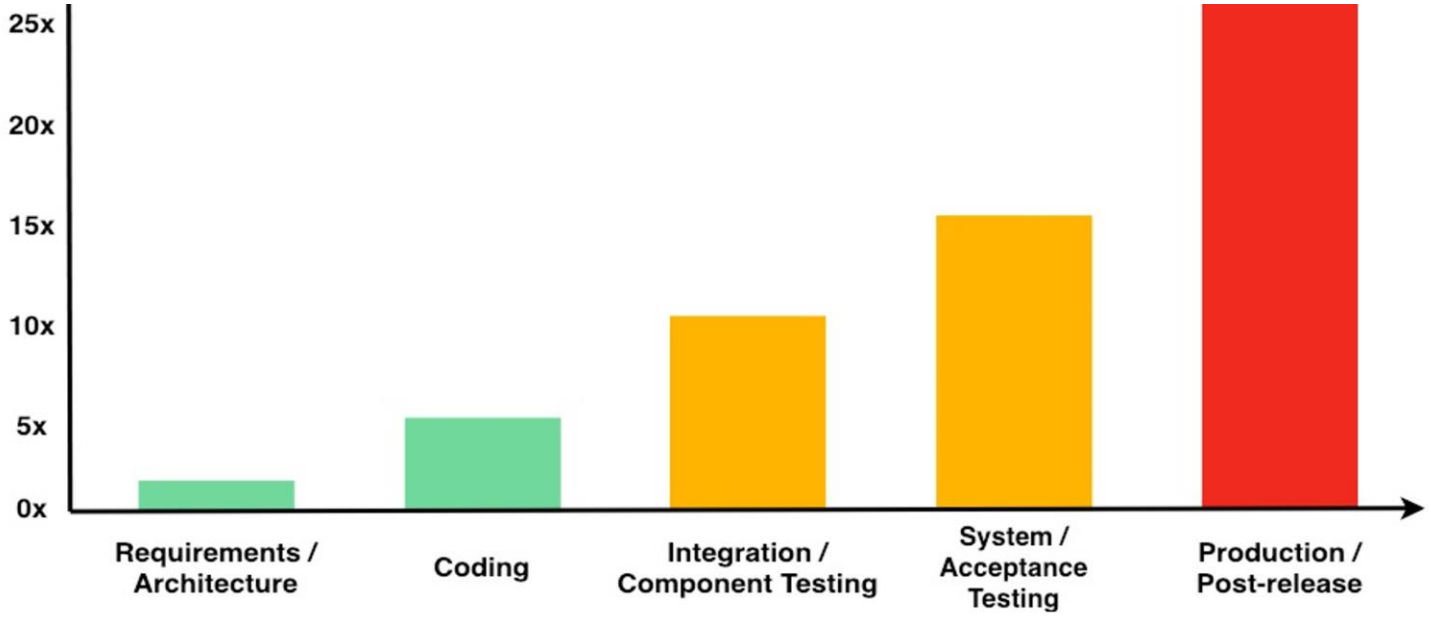
- **Dynamické pridávanie kapacity v produkčných prostrediach**
  - Schopnosť reagovať na „nárazové“ využívanie systémov ich používateľmi
- **Automatizovaný rollback**
  - Pomocou IaC je rollback v prípade problémov pri nasadení podstatne jednoduchší



Relative Cost to Repair Defects When Found at Different Stages of Software Development

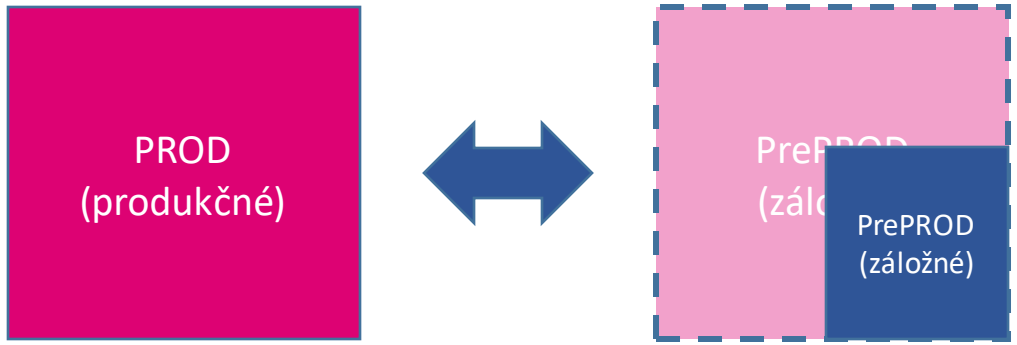
X is a normalized unit of cost and can be expressed terms of person-hours, dollars, etc.

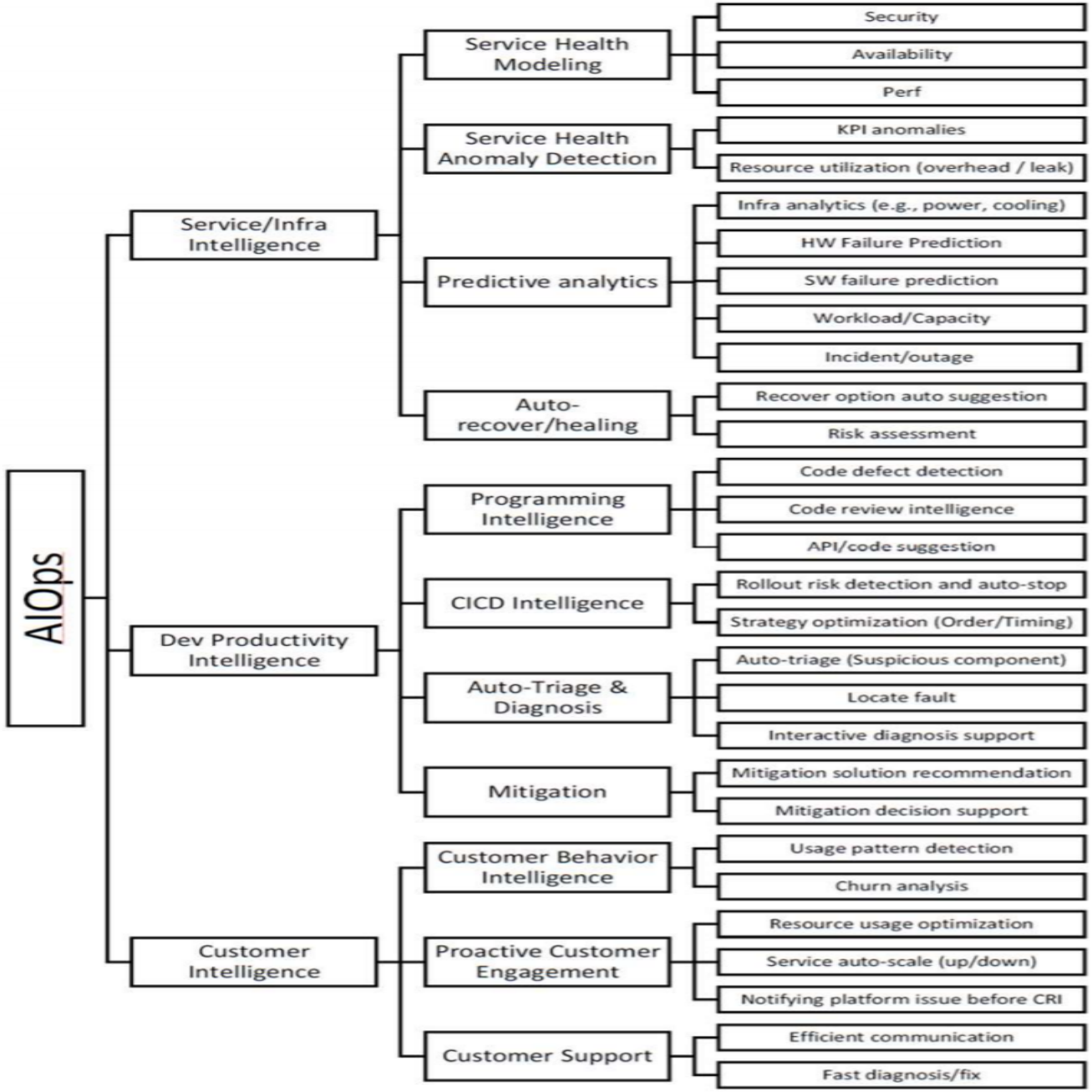
Requirements Gathering and Analysis/ Architectural Design	Coding/Unit Test	Integration and Component/RAISE System Test	Early Customer Feedback/Beta Test Programs	Post-product Release
1X	5X	10X	15X	30X



DevOps -> AIOps

- **Predikcia vyťaženosti zdrojov v prostrediach**
  - Ak vieme odhadnúť vyťaženie výpočtových zdrojov v budúcnosti, vieme tieto zdroje presúvať medzi PROD a PREPROD (napr. perf testy, endurance testy, Releasy bez „downtime-u“)
- **Príklady predikcií (Deep learning):**
  - Vyťaženie CPU pre VM (server) na 10 hodín dopredu (Dáta: PosAm 2020)
  - Počet dotazov na systém na 10 hodín dopredu (Dáta: NASA 1995)
  - Ale aj počet používateľov, dokumentov vo fronte, atď. (plus kombinácie)

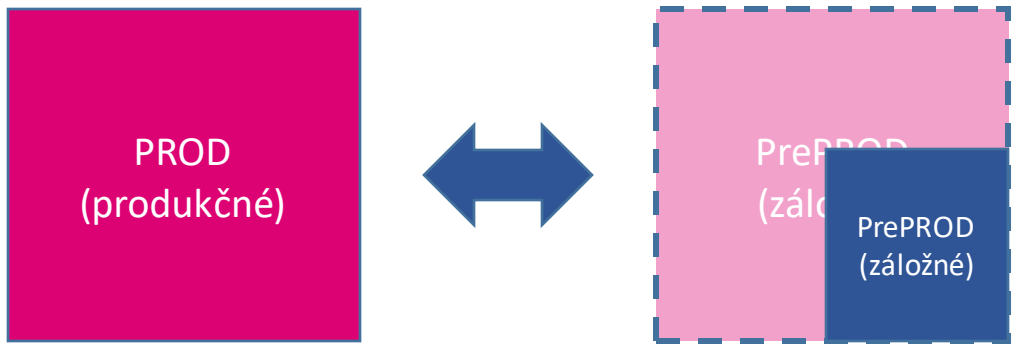




DevOps -> AIOps

PosAm USEFUL TECHNOLOGIES

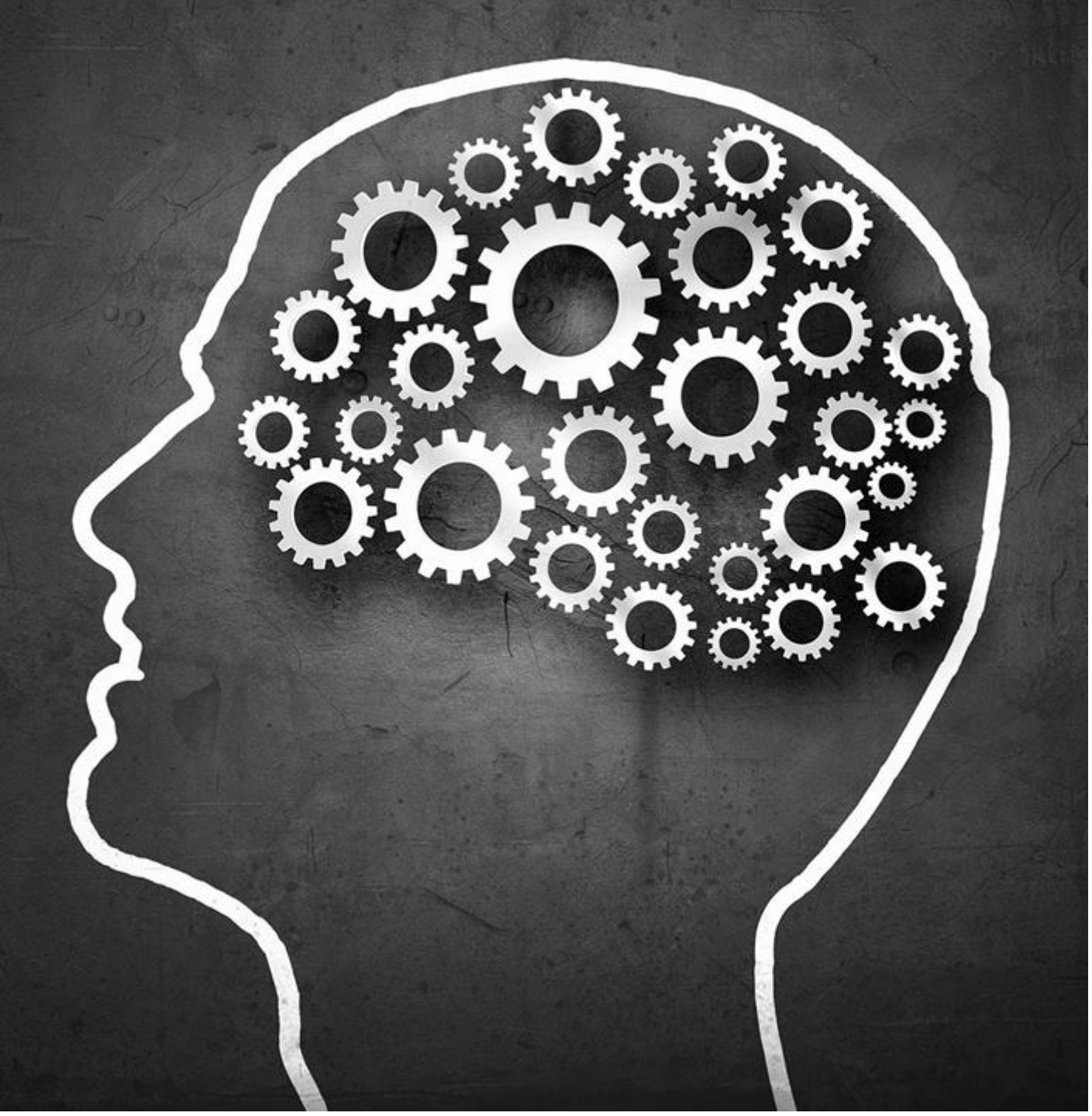
```
resource "cloudstack_instance" "server-1" {
  name                = "server-1"
  display_name        = "server-1"
  service_offering = "${lookup(local.densify_spec,"appr_type") == "all" ?
                      lookup(local.densify_spec,"rec_type") :
                      lookup(local.densify_spec,"cur_type")}"
  network_id          = cloudstack_network.frontend.id
  template            = "centos-75-v1.0"
  zone                = var.zone
}
```



Čo Vám vie ponúknuť PosAm?

PosAm USEFUL TECHNOLOGIES

- **Konzultácie k návrhu a zavedeniu IaC**
  - Analýza prostredia a návrh architektúry
  - Príprava biznis case
- **Vybudovanie „podvozku“ pre IaC**
  - Implementácia programovateľných komponentov
  - Implementácia Private Cloud
- **Implementáica IaC**
  - Implementáciu IaC platformy (Toolsetu)
  - Školenia pre vybrané IaC nástroje a postupy
- **Automatizácia aplikácií a podporných služieb**
  - Automatizácia prostredí (aj produkcie)
  - Instantné DR
  - AIOps



PosAm USEFUL TECHNOLOGIES

Diskusia

PosAm USEFUL TECHNOLOGIES

Infraštruktúra ako kód a prínos pre podnikové IT

1. Čo to je IaC
2. Demo – ukážka
3. Čo je potrebné pre IaC a prečo je to dôležité
   a) Podvozok pre IaC - Nasadiť programovateľné infraštruktúrne komponenty, privátny cloud
   b) Sefl-service ak tomu prispôsobenie architektúru infraštruktúry a procesy prevádzky
4. Spôsoby využitia
   a) Aut. Tvorbu a správu testovacích a „tých nižších“ prostredí (DEV, TEST, INT, UAT ak nie je PREPROD)
   b) Produkčné a Preprod prostredia automatizované. Do produkcie má prístup len úzka skupina ľudí.
      a) Nasadzovanie do PROD sa verifikuje pomocou PRE-PROD (ten kto ide nejaký balík nasadiť do PROD tak si skontroluje či to čo balík obsahuje, je aj aktuálny rozdiel preprod vs. prod.) – automated rollback and remedaition.
   c) Advanced scenáre.:
      1. DR pomocou cold start-tu
      2. Autoscaling PROD a PREPROD.

Čo je to Infrastructure as Code?

- **Vytvorenie, nasadenie a konfigurácia softvérovo definovanej výpočtovej, sieťovej a dátovej infraštruktúry prostredníctvom zdrojového kódu**
  - VLANs, IPs, VMs, Firewall a LBs, DNS, VPN, Monitoring, Log..
- **Aplikácia procesov a prostriedkov tradične spájaných so softvérovým vývojom na správu IT infraštruktúry**
  - Git, Nexus, IDE, Secret management, CI/CD Tools etc.
- **IaC je základným stavebným prvkom pre automatizáciu a môže podstatne zlepšovať DevOps**
- **K implementácii IaC je potrebné pridať aj nasadenie orchestrácie a nástroje na správu konfigurácií**
- **IaC nemusí byť použité pre celú infraštruktúru**