Iway Cloud Platform - manažovaný Kubernetes
Čo? Prečo? Ako?

IWAY DAY 27.10.2022

InterWay, a. s.
Mlynské nivy 71, 821 05 Bratislava, Slovenská republika
T: +421 232 788 888 | **E:** sales@interway.sk | **W:** www.interway.sk

Program

- ✓ Cloud Native Architektúra
- ✓ Manažovaný Kubernetes a IWCP
- ✓ Iway Cloud Platform - IWCP
  - ✓ PaaS
  - ✓ ADPS
  - ✓ iPaas
- ✓ Bezpečnosť v IWCP

INTERWAY IT´s ABOUT YOU

IWAY CLOUD PLATFORM

Cloud Natívna Architektúra

Cloud technológie podporujú inovácie

- ✓ Využitie cloud natívnych a open source technológií na rýchlu modernizáciu a inováciu
- ✓ V prvom štvrťroku 2022 boli celosvetové výdavky na cloudovú infraštruktúru dvojnásobné v porovnaní s prvým štvrťrokom 2019
  - ✓ **55,9 miliardy USD vs. 27,5 miliardy USD ***
- ✓ Bezpečnosť sa stáva kritickou, riziká znásobuje viac používateľov, údajov a aplikácií

✓ *https://www.statista.com/statistics/967292/worldwide-cloud-infrastructure-services-market-revenue/
Published by Lionel Sujay Vailshery, Jun 10, 2022

Cloud Natívna Architektúra

- ✓ Pomáha navrhovať systémy, ktoré podporujú ciele cloud natívnej technológie
- ✓ Sleduje rýchle inovácie stabilitu a spoľahlivosť
- ✓ Odstraňuje prekážky na ceste k inováciám prostredníctvom:
  - ✓ Svižnosti dodávania softvéru
  - ✓ Automatizácie
  - ✓ Robustných a spoľahlivých systémov

Piliere pre Cloud Natívnych Aplikácie

- ✓ **Kontajnery** a voľne spojené **Mikroslužby** (považované za cloud natívnu prax)
- ✓ **DevSecOps, CI/CD** praktiky Dev Sec Ops spolupracujú
  - ✓ DevSecOps je centrom pre CNA filozofiou
  - ✓ Veľa platforiem vrátane IWCP obsahuje DevSecOps nástroje a potrebné metodiky
- ✓ Prevádzková **Automatizácia**
  - ✓ K8s – prináša podporu pre prevádzkové procesy nasadenie, automatizovanie úloh
- ✓ **Severless**
- ✓ **Orchestrácia** – náročné operácie pre aplikácie a ich manažment

INTERWAY IT´s ABOUT YOU

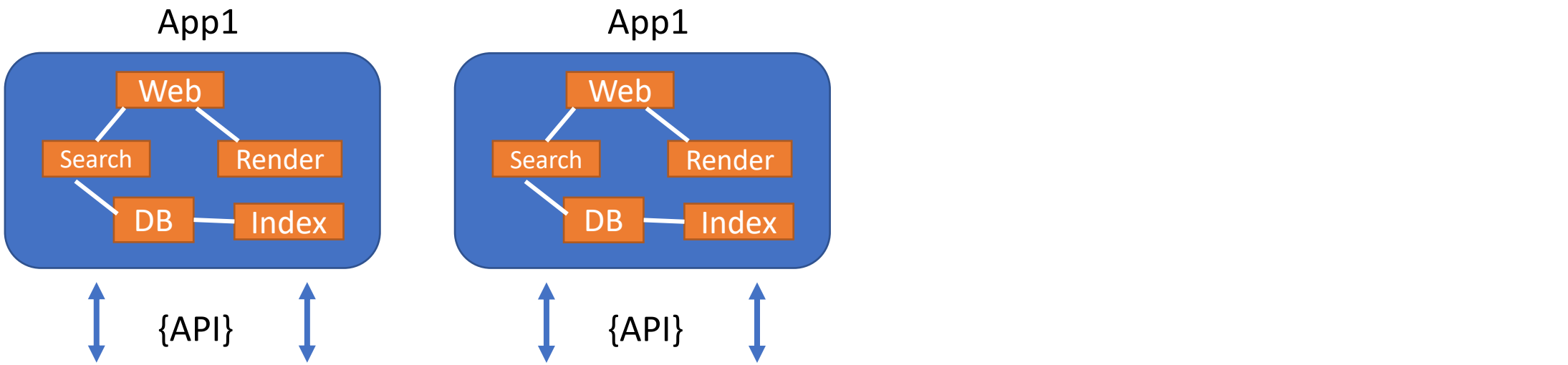
IWAY CLOUD PLATFORM

Manažovaný Kubernetes a IWCP

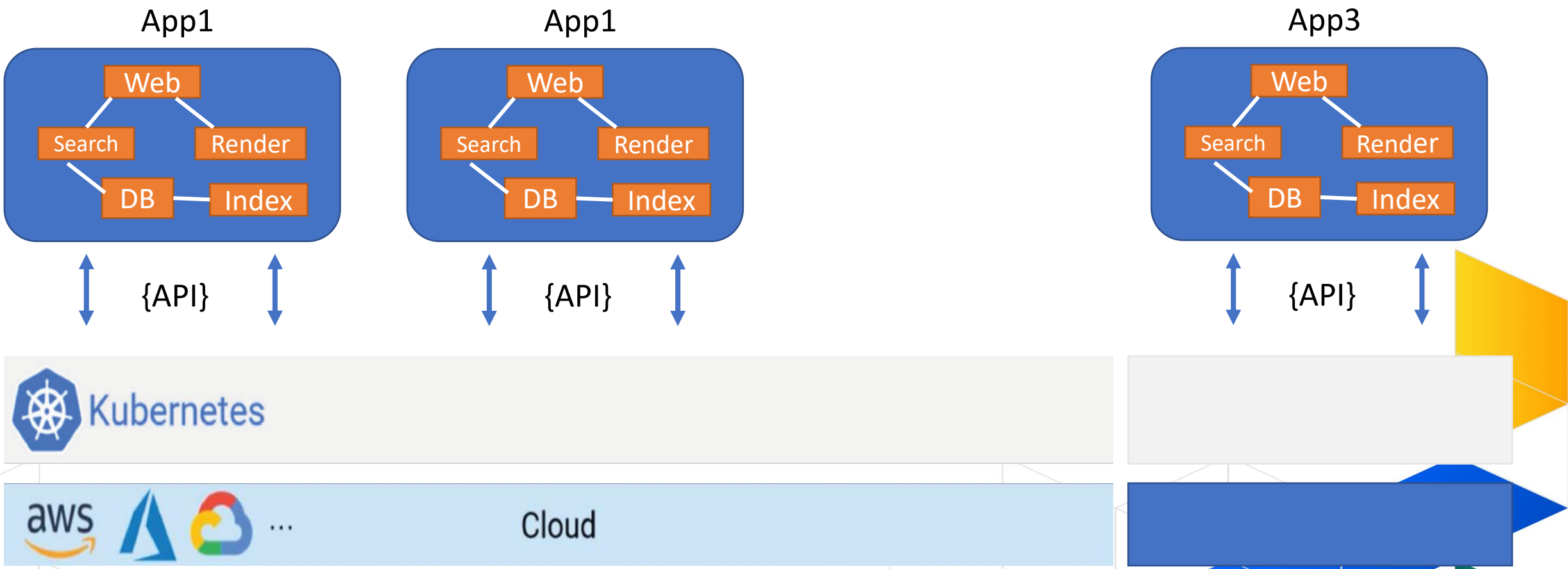
Kubernetes

- ✓ Štandard pre automatizáciu nasadzovanie a prevádzku cloud natívnych aplikácií
- ✓ Stáva sa cloudovým operačným systémom
- ✓ Dôvodom úspechu je **výkonnosť, všestrannosť a design s ohľadom na životné cykly vytvárania a prevádzky moderného softvéru**
- ✓ Nové technológie a architektúry vedú aj k širokej škále bezpečnostných rizík a výziev

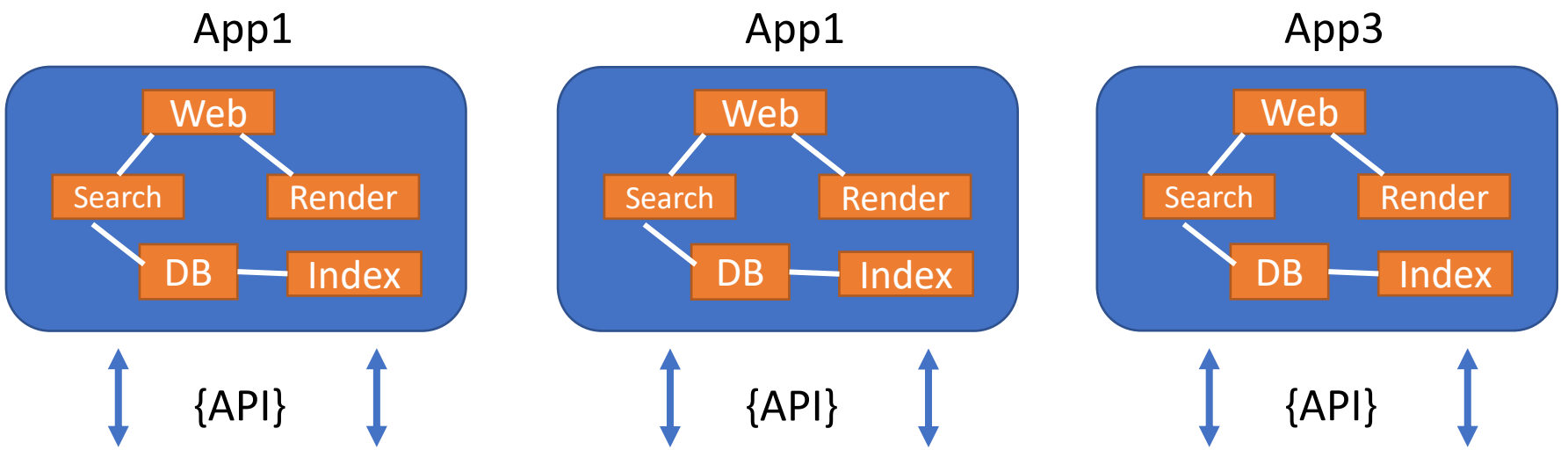
Prečo Kubernetes



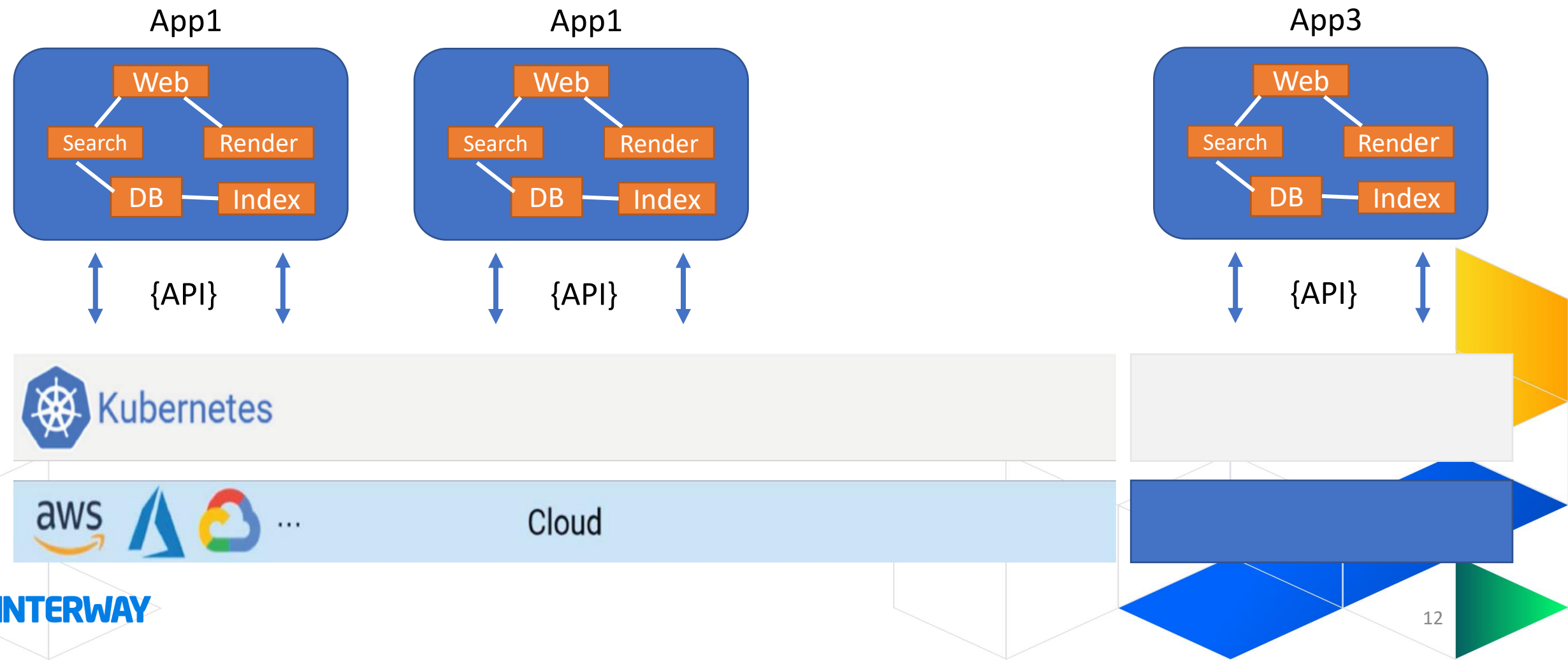
Prečo Kubernetes



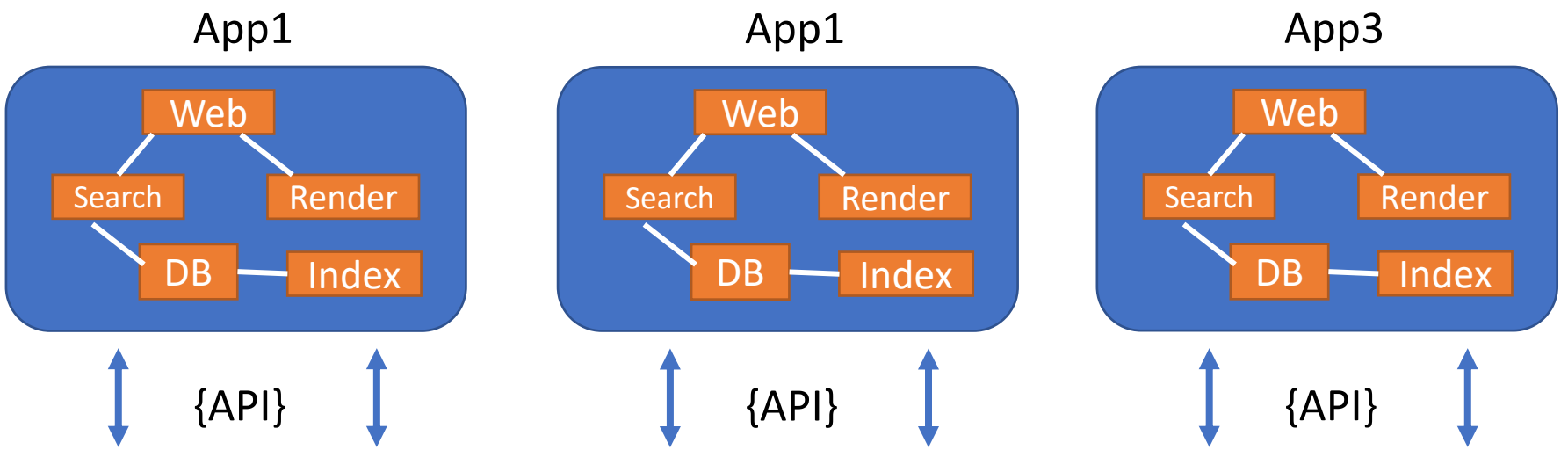
Prečo Kubernetes



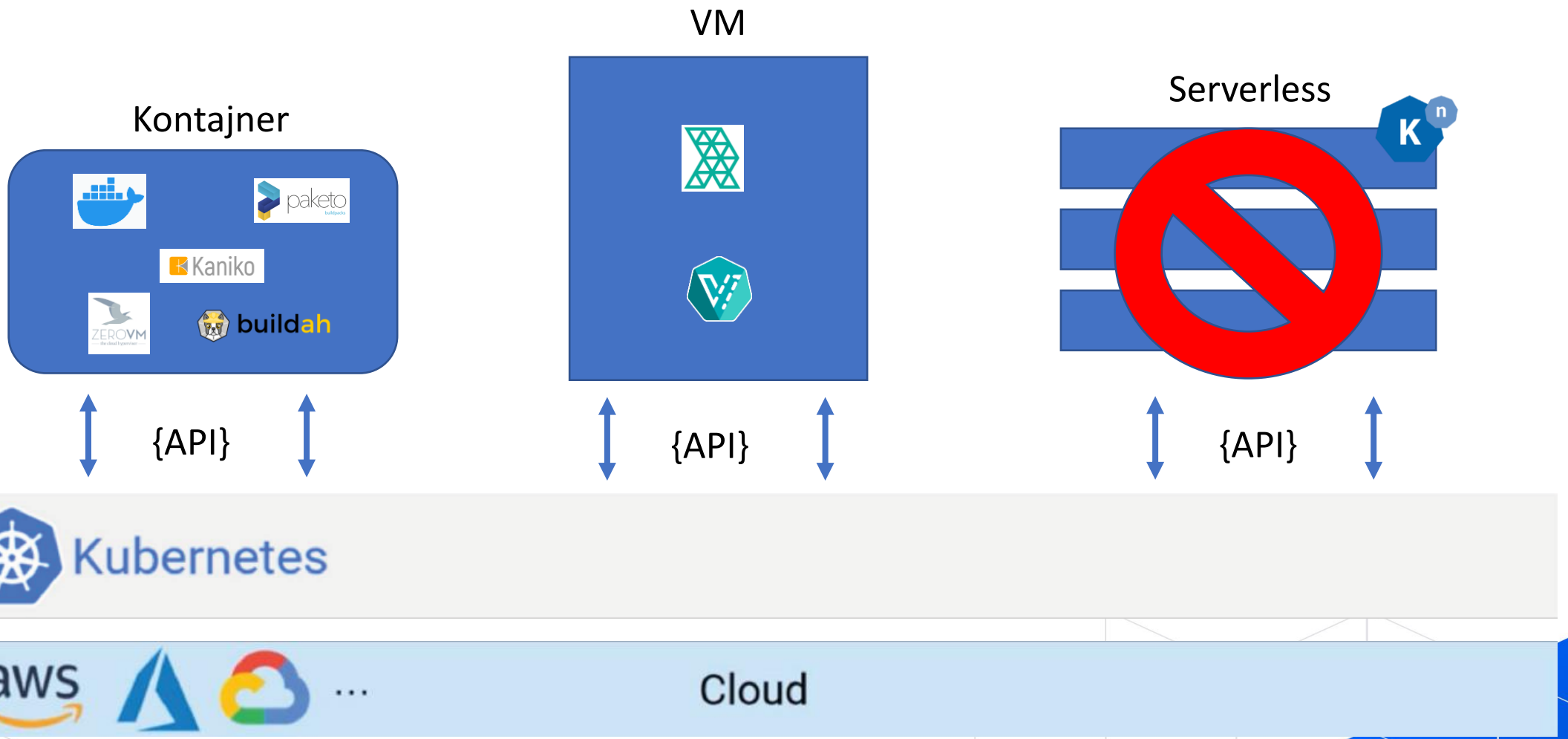
Prečo Kubernetes



Prečo Kubernetes



Kubernetes už za hranicami kontajnerov



Kubernetes pre cloud natívne aplikácie

Infraštruktúra

Privátny cloud

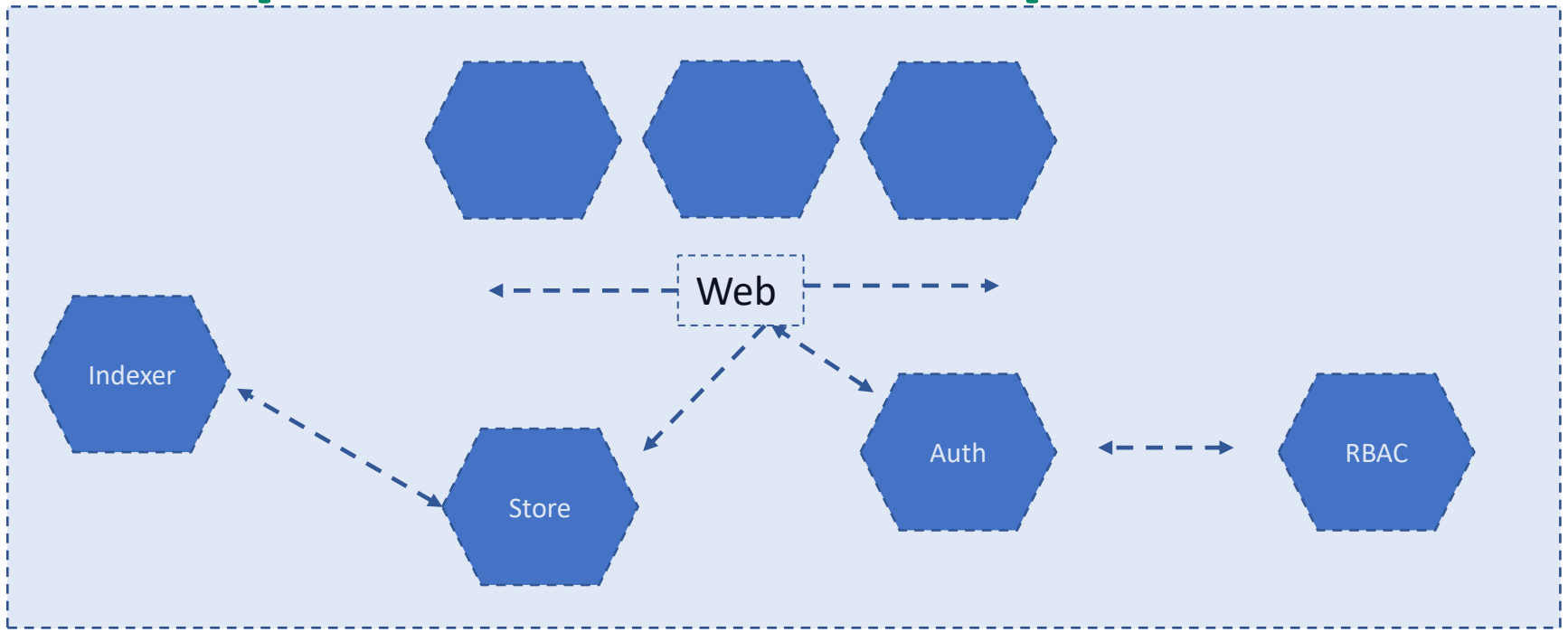
Kubernetes pre cloud natívne aplikácie

Cloud Natívne Aplikácie

Infraštruktúra

Privátny cloud

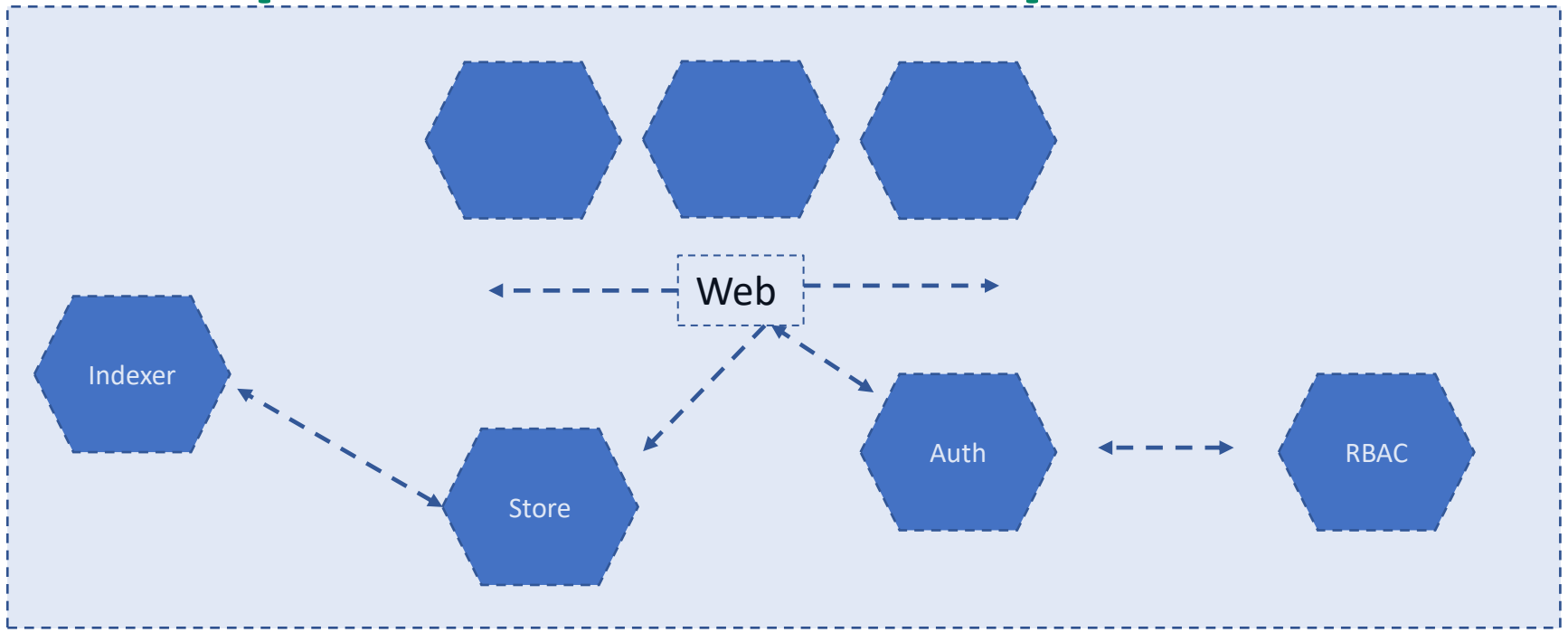
Kubernetes pre cloud natívne aplikácie



Infraštruktúra

Privátny cloud

Kubernetes pre cloud natívne aplikácie



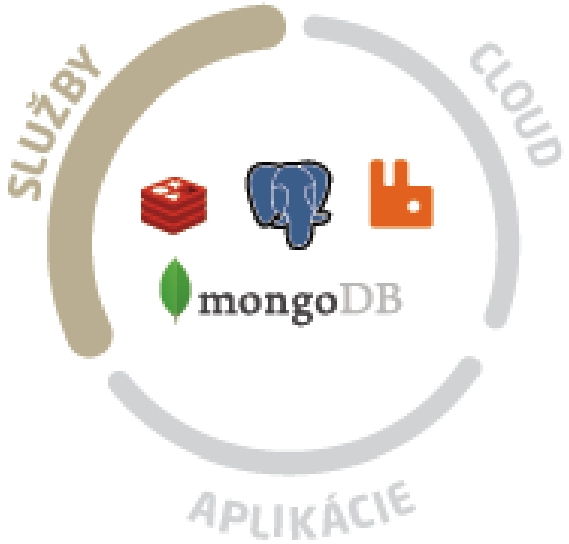
Privátny cloud

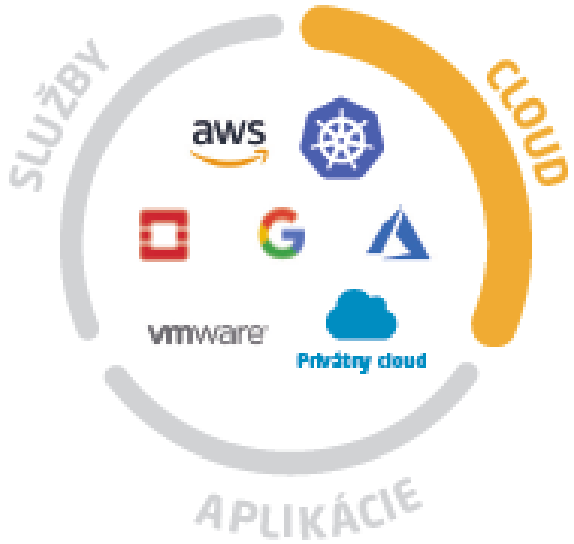
INTERWAY IT´s ABOUT YOU

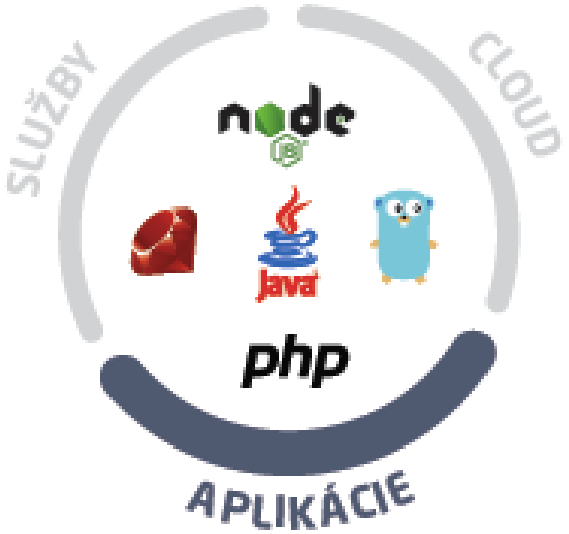
IWAY CLOUD PLATFORM

Iway Cloud Platform - IWCP

IWAY Cloud Platform



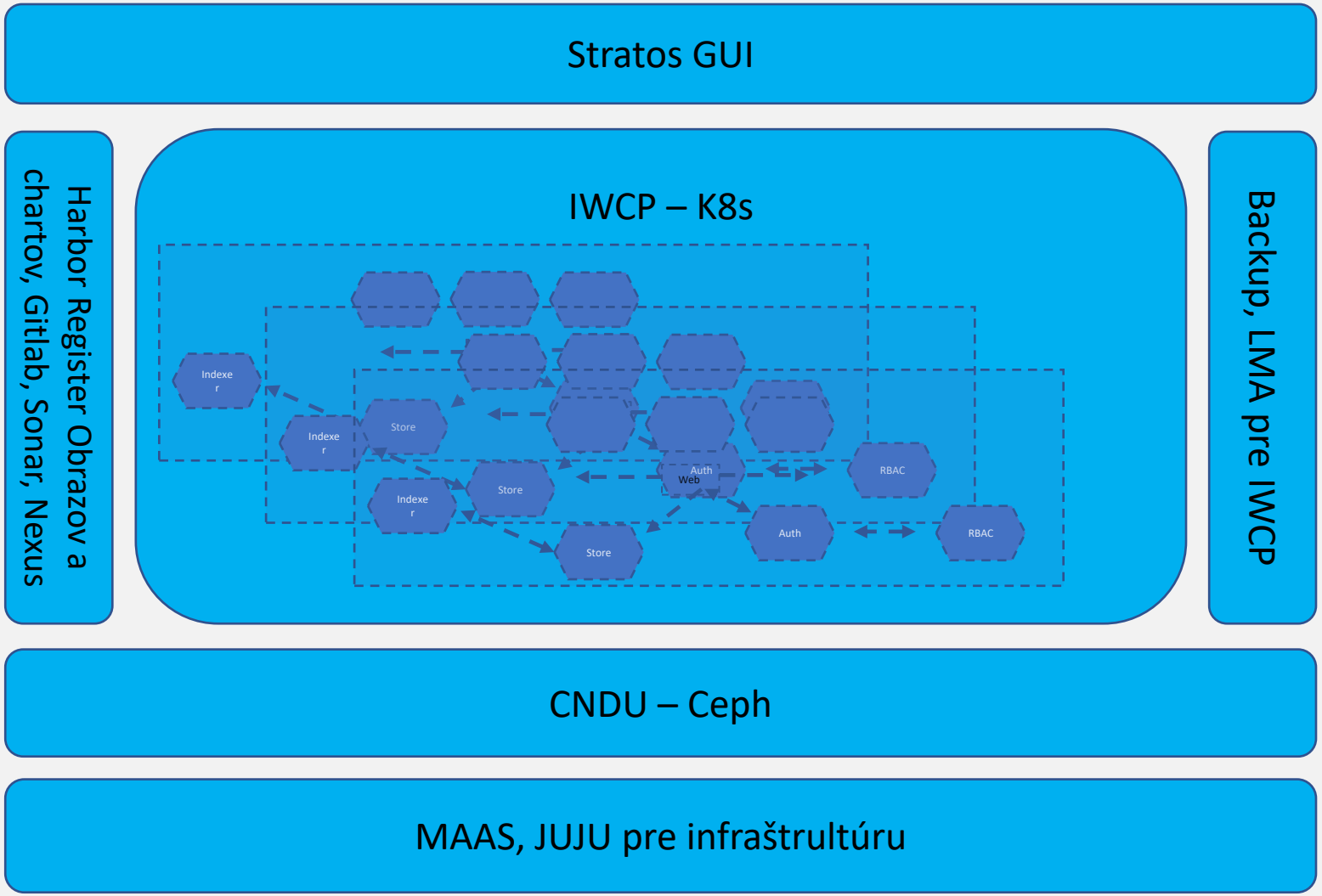




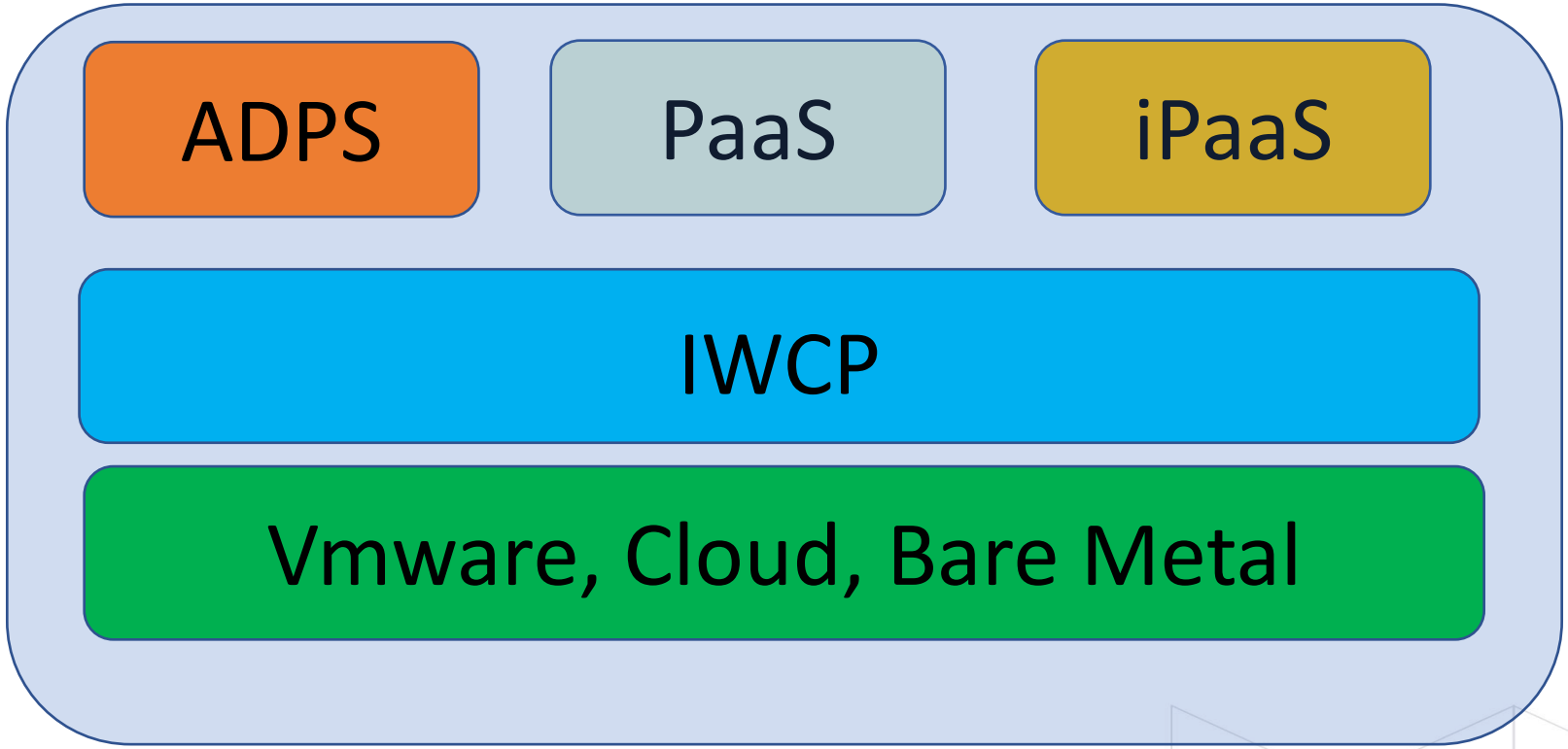
IWAY Cloud Platform

- ✓ Nová generácia vývoja, návrhu implementácie a prevádzky informačných systémov v multi-cloudovovom prostredí
- ✓ Zostavená ako kompletný softvérový balík, nasaditeľný aj vo forme uceleného systému hardvér – softvér
  - ✓ Automatizovane podporuje cloud natívne princípy a zvyšuje produktivitu vývoja, rýchlosť nasadenia a celkové skrátenie nových projektov.
- ✓ Poskytuje integrované DevSecOps nástroje na spúšťanie, prevádzku a škálovanie kontajnerových aplikácií a služieb s pridanou hodnotou využívajúcich Kubernetes
- ✓ **Vychádza z Canonical distribúcie pre k8s a využíva Canonical nástroje pre automatizáciu**

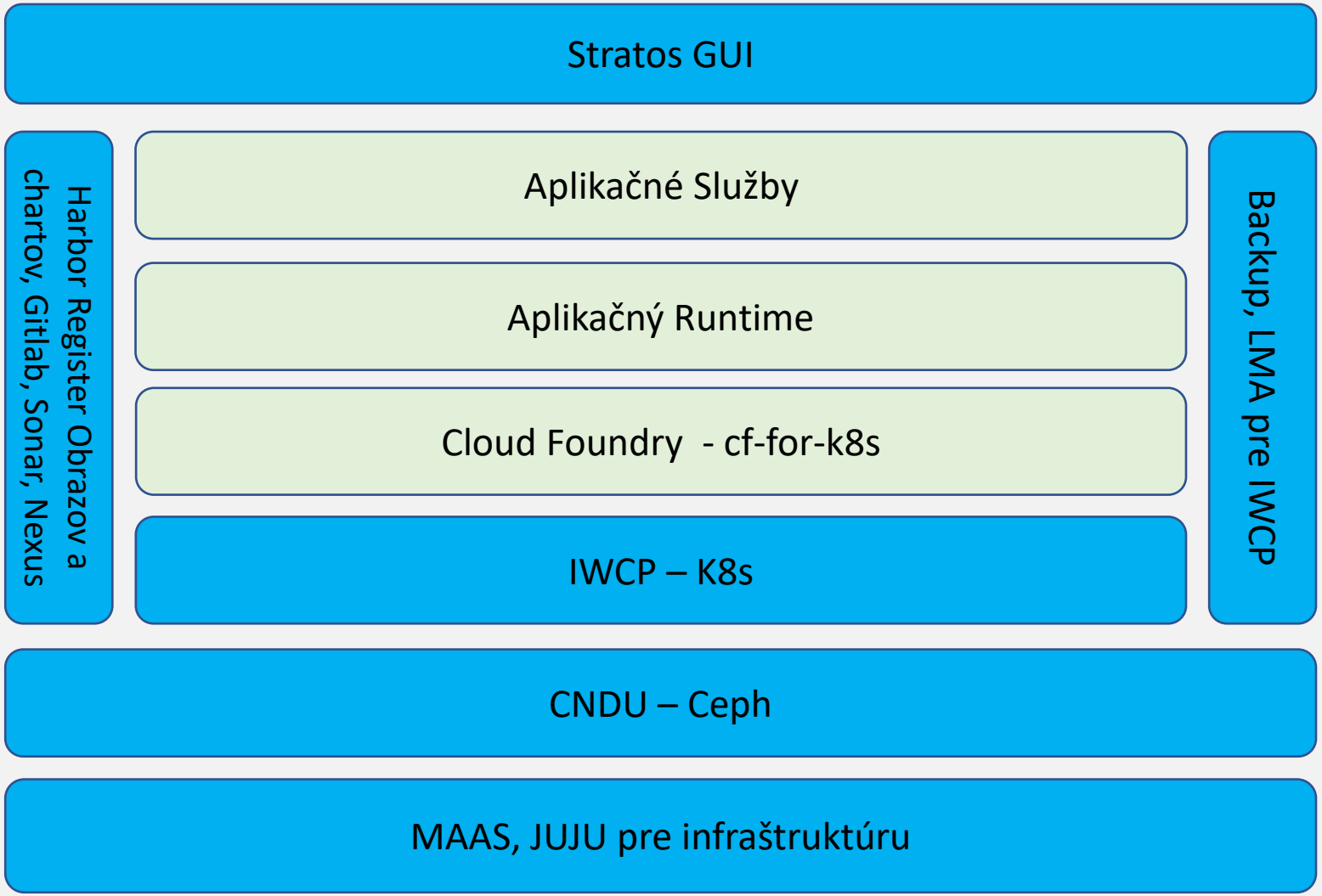
IWCP manažovaný Kubernetes - CaaS



IWCP a rozšírenia



IWCP PaaS – Aplikačná platforma



Ucelený komplet pre developerov a pre prevádzku

- ✓ K8s ako orchestračná platfoma
- ✓ Nasadenie kódu aplikácie **jedným príkazom**
- ✓ Škálovateľná prevádzka pre IWCP PaaS

Služby a programovacie jazyky pre IWCP Paas

Navrhnuté pre použitie v natívnych multi-cloud, multi-tenant a polyglotných projektoch

PaaS Služby

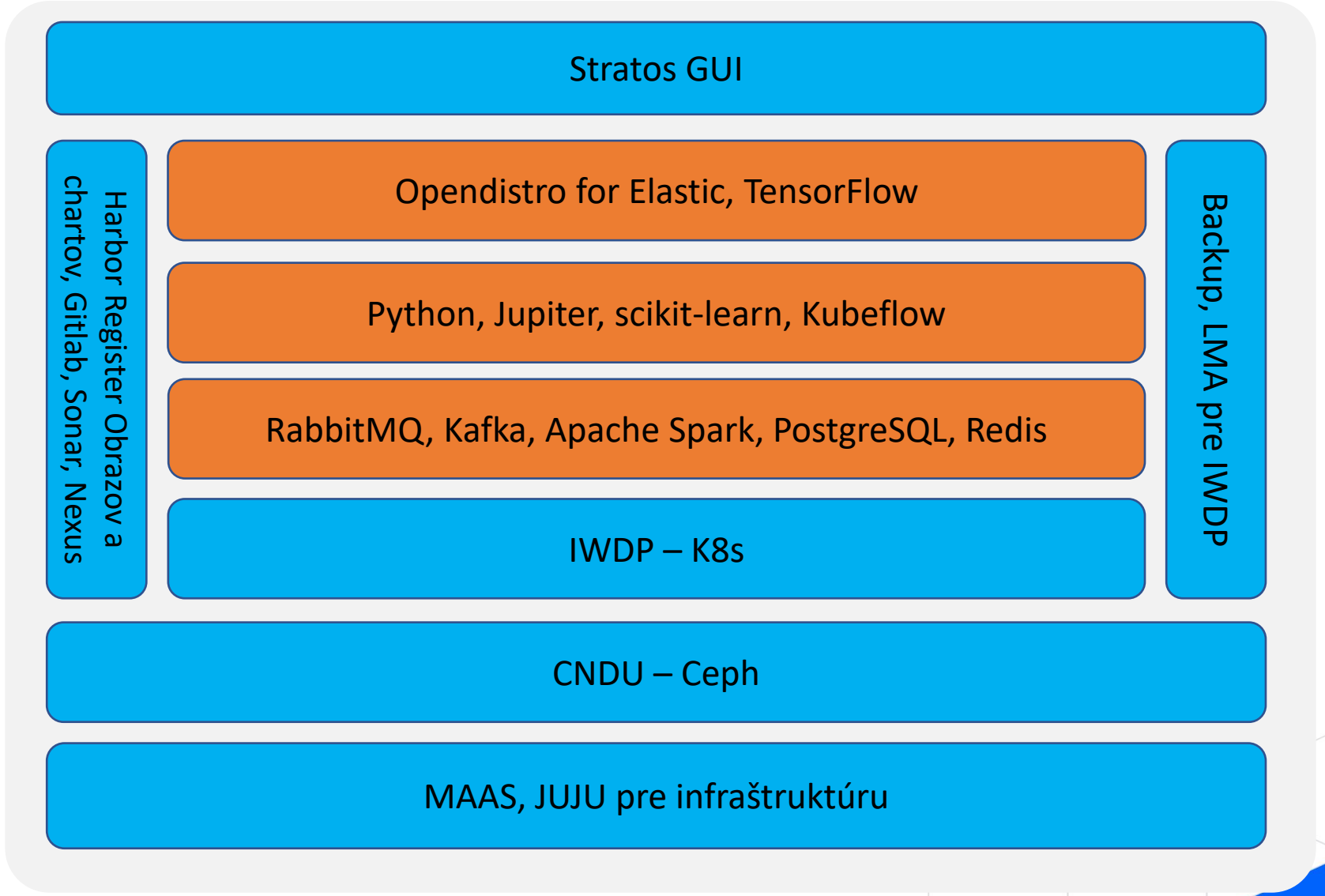
- ✓ Postgres
- ✓ MariaDB
- ✓ MongoDB
- ✓ Redis
- ✓ MemcacheD
- ✓ RabbitMQ
- ✓ Kafka
- ✓ Tomcat
- ✓ Nginx
- ✓ GitLab
- ✓ Nexus
- ✓ Sonar
- ✓ NFSv3 volumes
- ✓ Objekt storage

Programovacie Jazyky

- ✓ Java
- ✓ Python
- ✓ Go
- ✓ Ruby
- ✓ PHP
- ✓ Node

paketo buildpacks

IWCP Analytická Dátová Platforma pre BD/ML

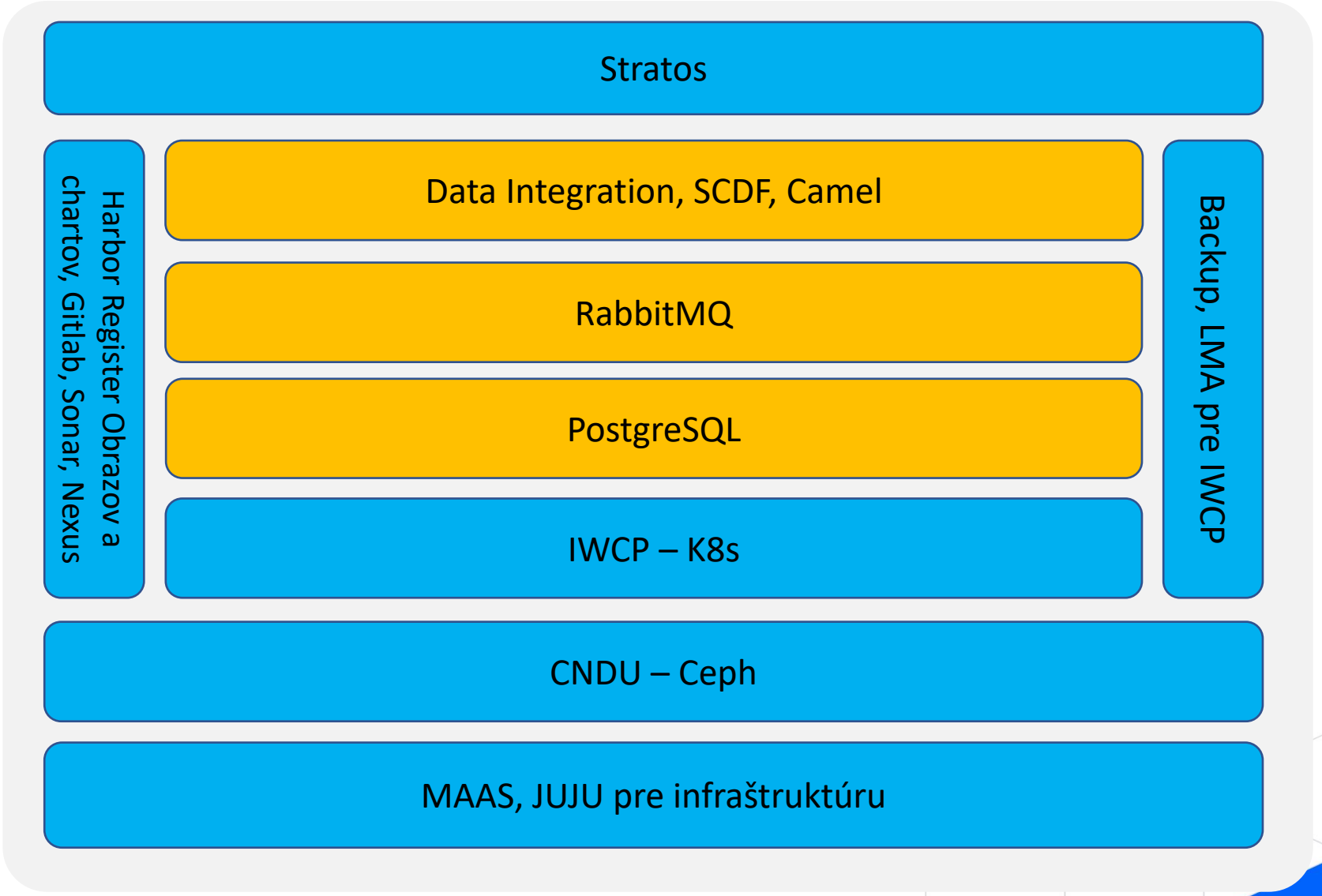


Trénovanie a Validácia

Prototypovanie a Transformácie

Data Ingestion

IWCP iPaaS – clopud integračná platforma



INTERWAY IT´s ABOUT YOU

Bezpečnosť v IWCP

Bezpečnosť pre Kubernetes a CNA

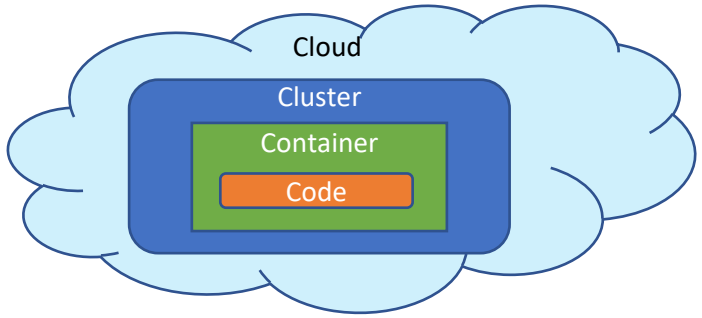
- ✓ Kubernetes sa stáva základnou infraštruktúrou platformou, ktorá podporuje poskytovanie moderného softvéru

- ✓ Komunita okolo Kubernetes vynaložila významné úsilie na zvýšenie povedomia o bezpečnosti:
  - ✓ Vykonanie bezpečnostného auditu Kubernetes platformy
  - ✓ Vytvorenie matice útokov Kubernetes založenej na MITER ATT&CK
  - ✓ Publikovanie bezpečnostnej bielej knihy o osvedčených postupoch
  - ✓ Open Source Security Foundation (OpenSSF) vedie projekt Alpha-Omega na zlepšenie dodávateľského reťazca softvéru
  - ✓ Na strane aplikácie OWASP Top 10 obsahuje prehľad „Nezabezpečeného dizajnu“ a „Zlej konfigurácie bezpečnosti“ (https://owasp.org/www-project-top-ten/)

- ✓ Efektívne stratégie na implementáciu bezpečnostných opatrení, ochrany aplikácií a Kubernetes infraštruktúry

Bezpečnosť pre Kubernetes a CNA

- ✓ Na zabezpečenie cloud natívnych aplikácií, je nevyhnutné chrániť základné prostredie Kubernetes a jeho relevantnú útočnú plochu
- ✓ Miesta útoku v rámci klastra Kubernetes pozostávajú z troch hlavných oblastí:
  - ✓ Dodávateľský reťazec softvéru na vytváranie artefaktov, používa sa na nasadenie a spustenie kontajnerov
  - ✓ Komponenty infraštruktúry, ktoré musia byť zabezpečené a nakonfigurované na spustenie Kubernetesu
  - ✓ Nasadené a spustené kontajnery, ktoré tvoria jednotlivé aplikácie Kubernetes
- ✓ Bezpečnostná filozofia je založená na tzv. 4C modeli pre cloud natívnu bezpečnosť



Zabezpečenie dodávateľského reťazca softvéru

DevSecOps Linka

- ✓ Bezpečnosť základných obrazov – base Image
- ✓ Zabezpečenie komponentov obrazov
- ✓ Bezpečnostné skenovanie obrazov kontajnerov a Register obrazov
- ✓ Zabezpečenie build systémov

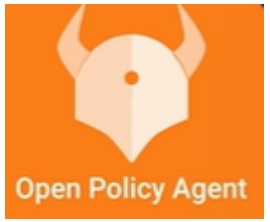
Zabezpečenie komponentov infraštruktúry

- ✓ Kubernetes je kritickým základom pre cloud natívne aplikácie
- ✓ Bezpečnostné opatrenia na ochranu komponentov, ktoré tvoria samotný Kubernetes, vrátane opráv zraniteľnosti alebo predchádzaniu nesprávnej konfigurácii k8s klastrov
- ✓ Každý klaster Kubernetes obsahuje sadu komponentov infraštruktúry potrebných na prevádzku platformy a aplikácií
  - ✓ Komponenty control plane/riadiacej roviny – spravujte operácie v celom rozsahu klastra.
  - ✓ Komponenty worker node/pracovného uzla – spúšťajú kontajnerové aplikácie v podoch.

Infraštruktúra

Zabezpečenie nasadených a prevádzkovaných aplikácií

- ✓ Kontroly vstupu
- ✓ Bezpečnostné kontexty
- ✓ Bezpečnosť siete kubernetes
- ✓ Autentifikácia
- ✓ Autorizácia
- ✓ Vytváranie a vyžadovanie politík
- ✓ Správa “secretov” pomocou HasiCorp Vault
- ✓ Service mesh manažuje komunikáciu medzi aplikačnými komponentami



Zabezpečenie v runtime aplikáciw

✓ Zabezpečenie v runtime aplikácie

- ✓ Bezpečnostné koncepty musia byť stále platné doplnené o detekciu hrozieb v runtime
- ✓ Aktivita na úrovni systému, monitorovanie vykonávania procesov a sieťovej komunikáciu na úrovni jednotlivých kontajnerov
- ✓ Nástroje ako **Falco** dokážu monitorovať systémové volania a protokoly Kubernetes API

Záver

- ✓ IwayCloud platforma predstavuje novú generáciu vývoja, návrhu implementácie a prevádzkovania informačných systémov v multi-cloudovovom prostredí.
- ✓ Platforma je zostavená ako kompletný softvérový balík, nasaditeľný aj vo forme uceleného systému hardvér - softvér, ktorý automatizovane podporuje cloud natívne princípy a zvyšuje produktivitu vývoja, rýchlosť nasadenia a celkové skrátenie nových projektov.
- ✓ Poskytuje integrované DevSecOps nástroje na spúšťanie, prevádzku a škálovanie kontajnerových aplikácií a služieb s pridanou hodnotou využívajúcich Kubernetes.
- ✓ **Vychádza z Canonical distribúcie pre k8s a využíva Canonical nástroje pre automatizáciu**

Záver

- ✓ Kubernetes je výkonný, ale komplexný systém, ktorý podporuje rýchlu transformáciu spôsobu, akým organizácie vytvárajú, dodávajú a prevádzkujú moderné softvérové aplikácie
- ✓ Jeho výhody prichádzajú so súvisiacimi požiadavkami na bezpečnosť musia byť riešené množstvom open-source a komerčných zdrojov nástrojov na minimalizáciu rizík a hrozieb
- ✓ Účinný prístup k zabezpečeniu prostredí Kubernetes a spustených aplikácií inside je založená na použití ovládacích prvkov na zabezpečenie kľúčových oblastí:
  - ✓ **Dodávateľský reťazec softvéru** používaný na vytváranie obrazov kontajnerov, vrátane základných obrázov a komponentov obrazov
  - ✓ **Komponentov infraštruktúry** potrebnej na spustenie klastrov Kubernetes, vrátane jeho riadiacej roviny a pracovných uzlov
  - ✓ Nasadené a spustené kontajnerové pracovné zaťaženia v **runtime**
- ✓ Realizáciou viacvrstvového 4C prístupu k bezpečnosti môžete škálovať svoje produkčné využitie Kubernetes.

INTERWAY IT´s ABOUT YOU

IWAY CLOUD PLATFORM

Ďakujem za pozornosť