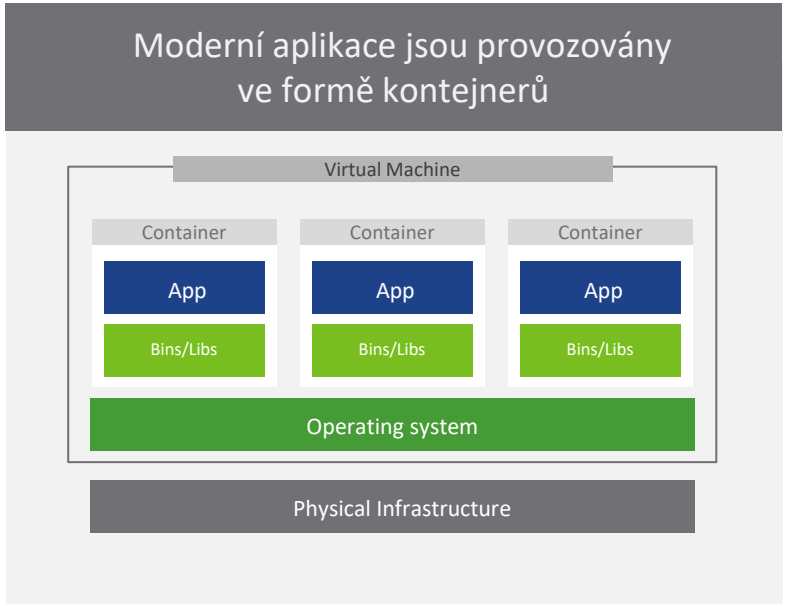
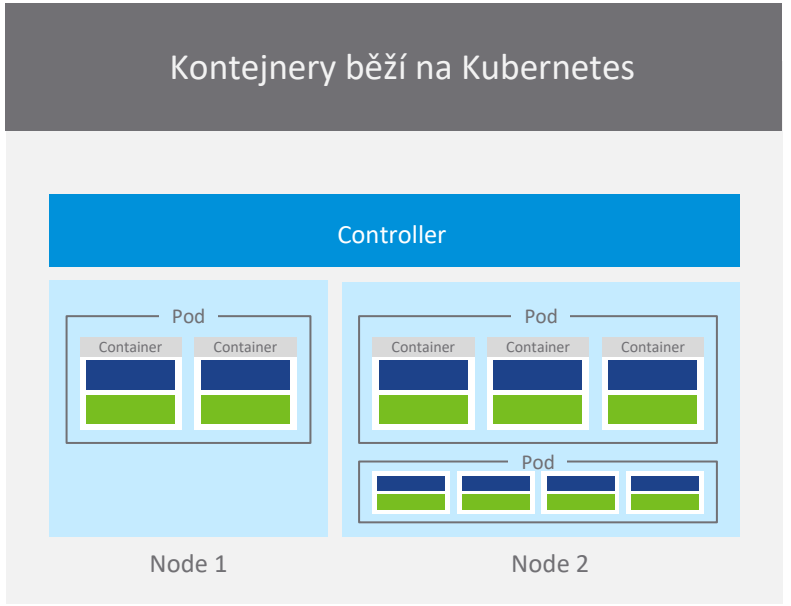
Kubernetes a úskalí jeho provozu v praxi

Workshop společnosti GAPP System

Hotel Jalta, Praha, 12. 4. 2023

Kubernetes je základem moderních aplikací





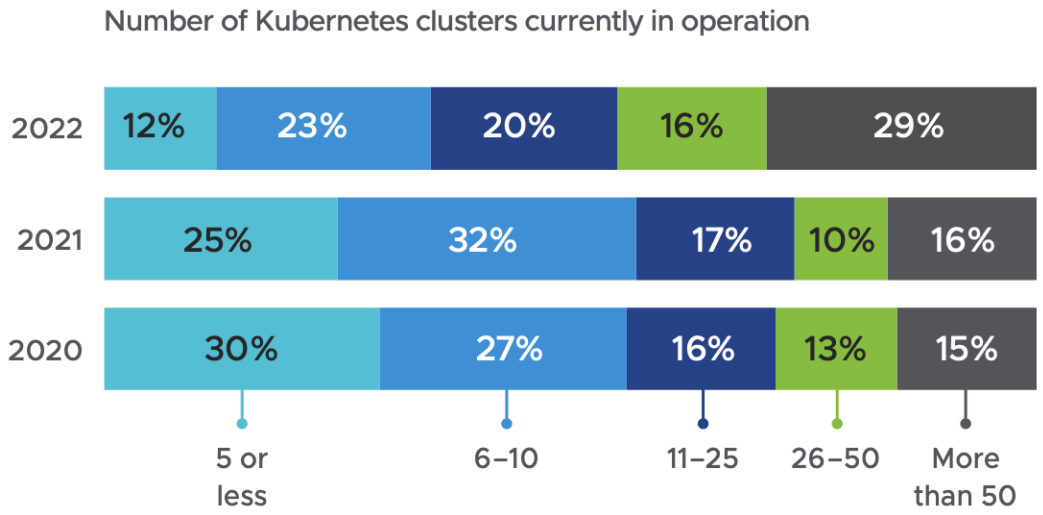
67% organizací investuje do kontejnerů pro dosažení vyšší míry agility

99% organizací jasně deklaruje akceptaci výhod Kubernetes jako platformy s těmito třemi stěžejními přínosy:

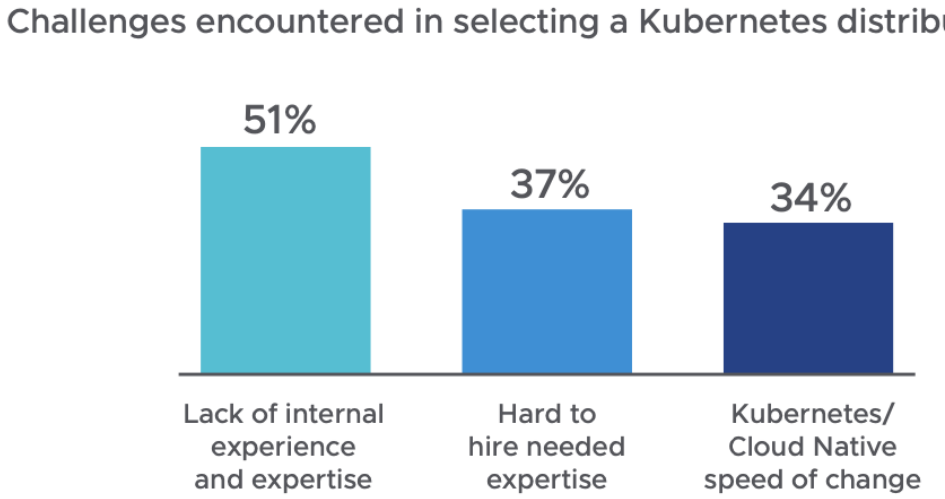
- efektivnější využití zdrojů
- jednodušší upgrade aplikací
- snadná možnost migrace do cloudu

Zdroje:
1- App Modernization in a Multi-cloud World, 2020 VMware Market Insights Report
2- The State of Kubernetes 2022, presented by VMware

Kubernetes je stále rozšířenější



Have difficulty selecting, deploying and managing Kubernetes



Zdroje:
The State of Kubernetes 2022, presented by VMware

What Kubernetes is not

Kubernetes is not a traditional, all-inclusive PaaS system

Kubernetes:

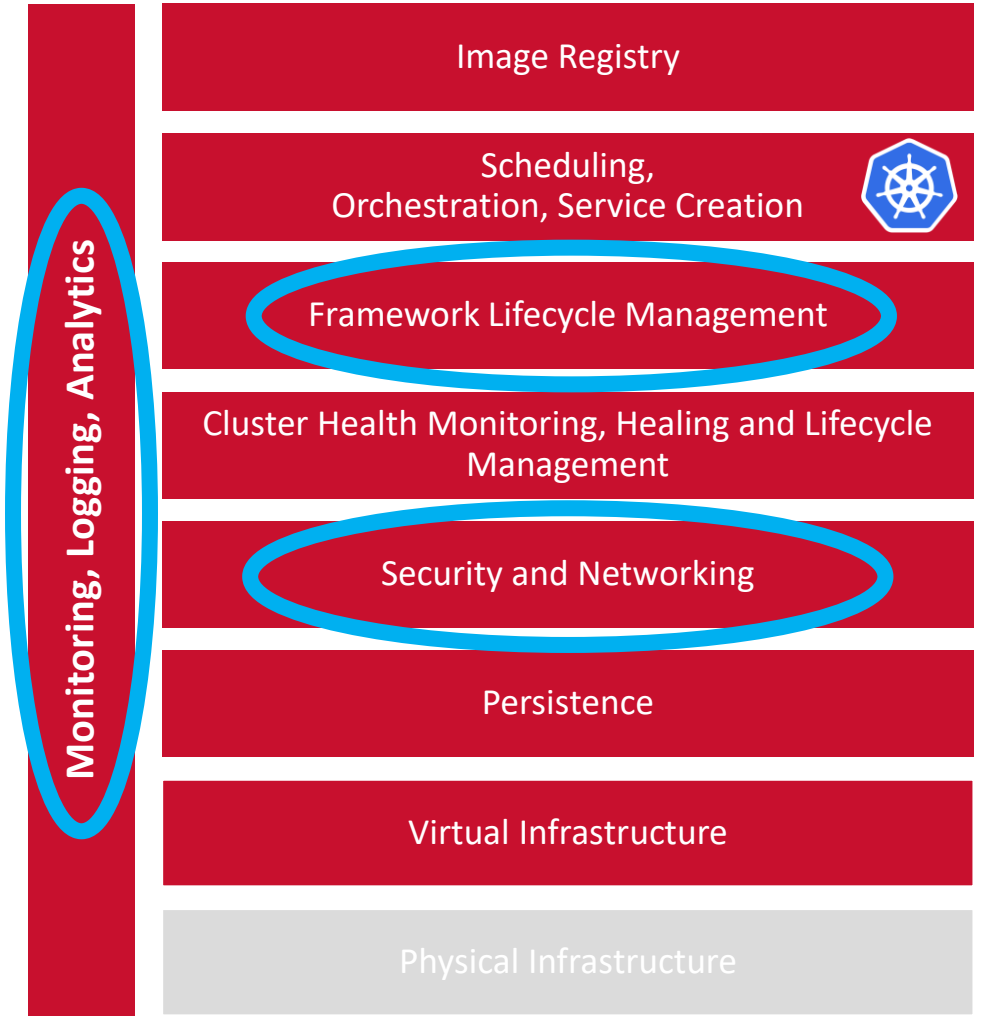
- Does not provide application-level services, such as … **middleware** … **cluster storage systems** … as built-in services.
- Does not provide nor adopt any comprehensive machine **configuration**, **maintenance**, **management**, or **self-healing** systems.
- Does not dictate **logging**, **monitoring**, or **alerting** solutions.

Source: https://kubernetes.io/docs/concepts/overview/what-is-kubernetes/

GAPP SYSTEM

Co vše je třeba řešit při nasazení Kubernetes v produkci?

Kubernetes je pouze jednou z vrstev celého prostředí!



VMware Tanzu Application Platform

GLOBAL CONTROL PLANE

Mission Control

- Lifecycle Management
- Identity and Access
- Security, Compliance, Audit
- Data Protection

+ API Driven Integrations

- Observability
- Service Mesh

BUILD AND DEPLOY

- Container Registry

CONNECTIVITY

- Kubernetes Ingress / Load Balancing
- Container Networking

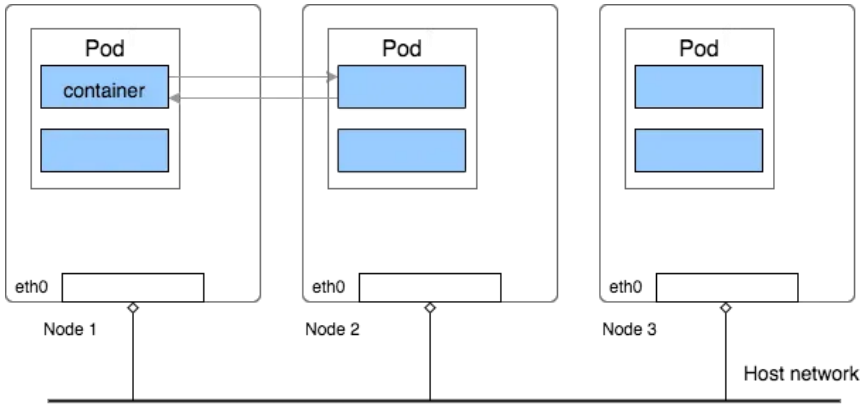
COMPUTE RUNTIME

- Platform Monitoring
- Kubernetes

MULTI-CLOUD

Security and Networking

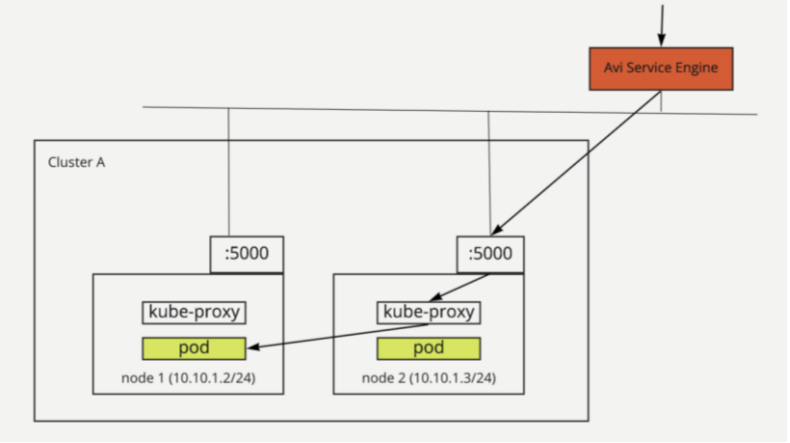
- Networking v prostředí K8s clusterů
  - Container Network Interface (CNI)
  - CNI plugins – Flannel, Calico, Canal, Antrea
- Základní bezpečnost při vzájemné komunikaci
  - Network Policies
- Zajištění přístupu ke službám
  - L4 load balancing – HAproxy, MetalLB
  - L7 ingress s TLS terminací – Contour, NSX ALB
  - Service Mesh pro vzájemnou komunikaci – Istio



NSX Advanced Load Balancer

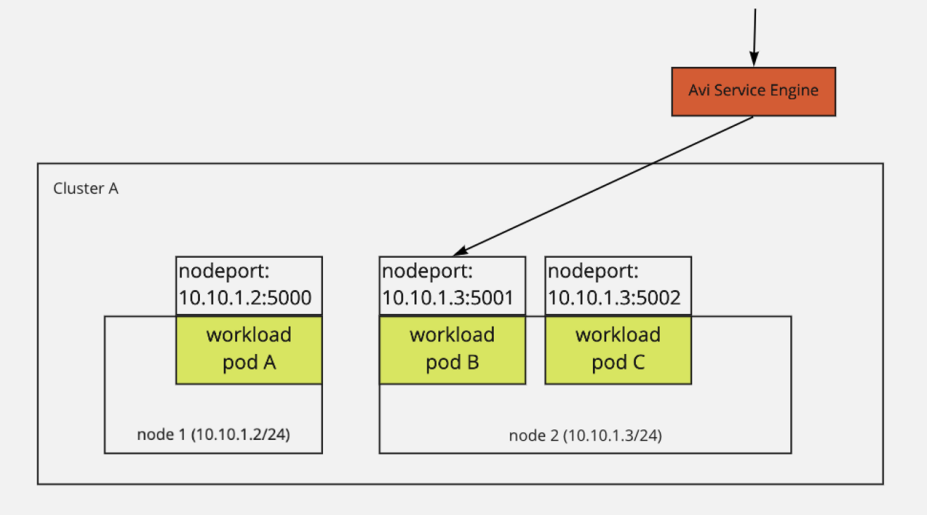
- **Enteprise-grade services**
  - L4 load balancing
  - L7 ingress controller
  - Web Application Firewall (WAF)
  - Domain Name System (DNS)
  - TLS termination

- **Multi-cloud**
  - Bare Metal Servers
  - Virtualized
  - Public Clouds
  - Containers

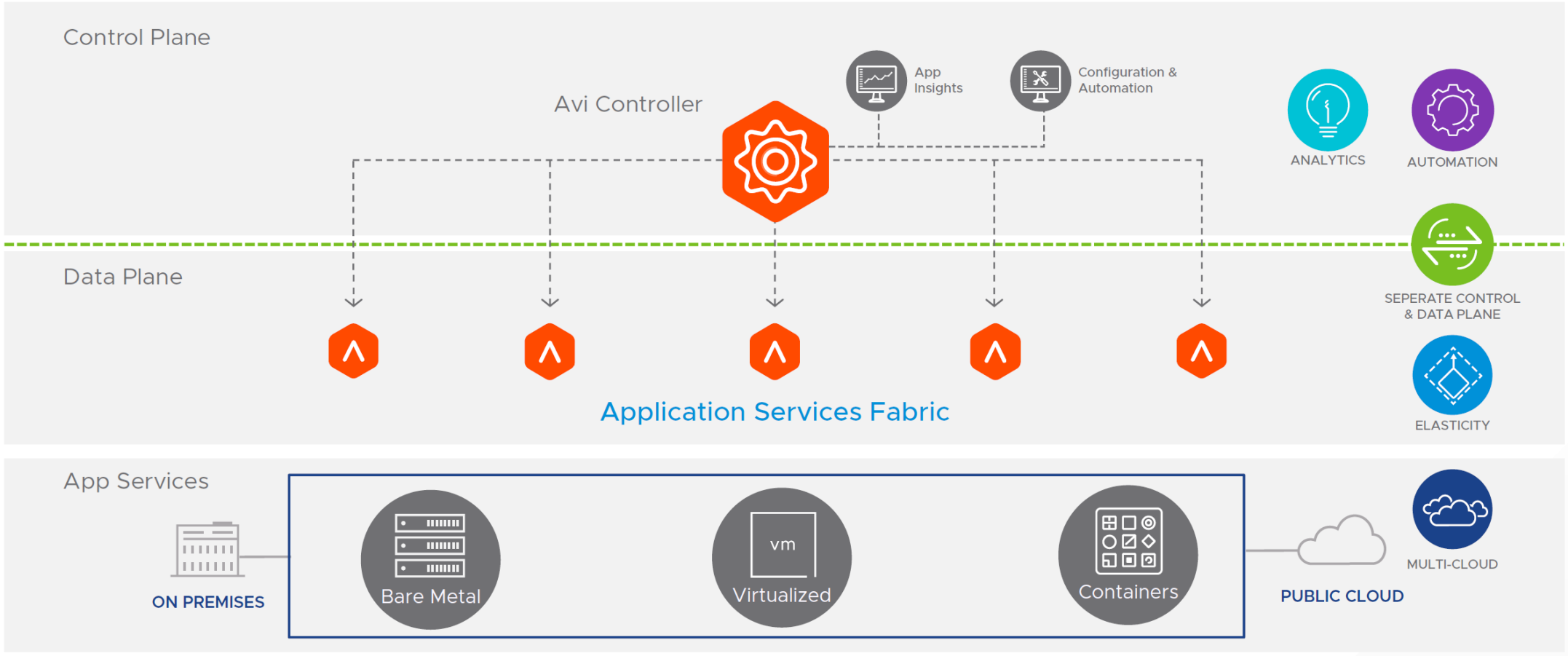


NodePort Mode

NodePortLocal Mode

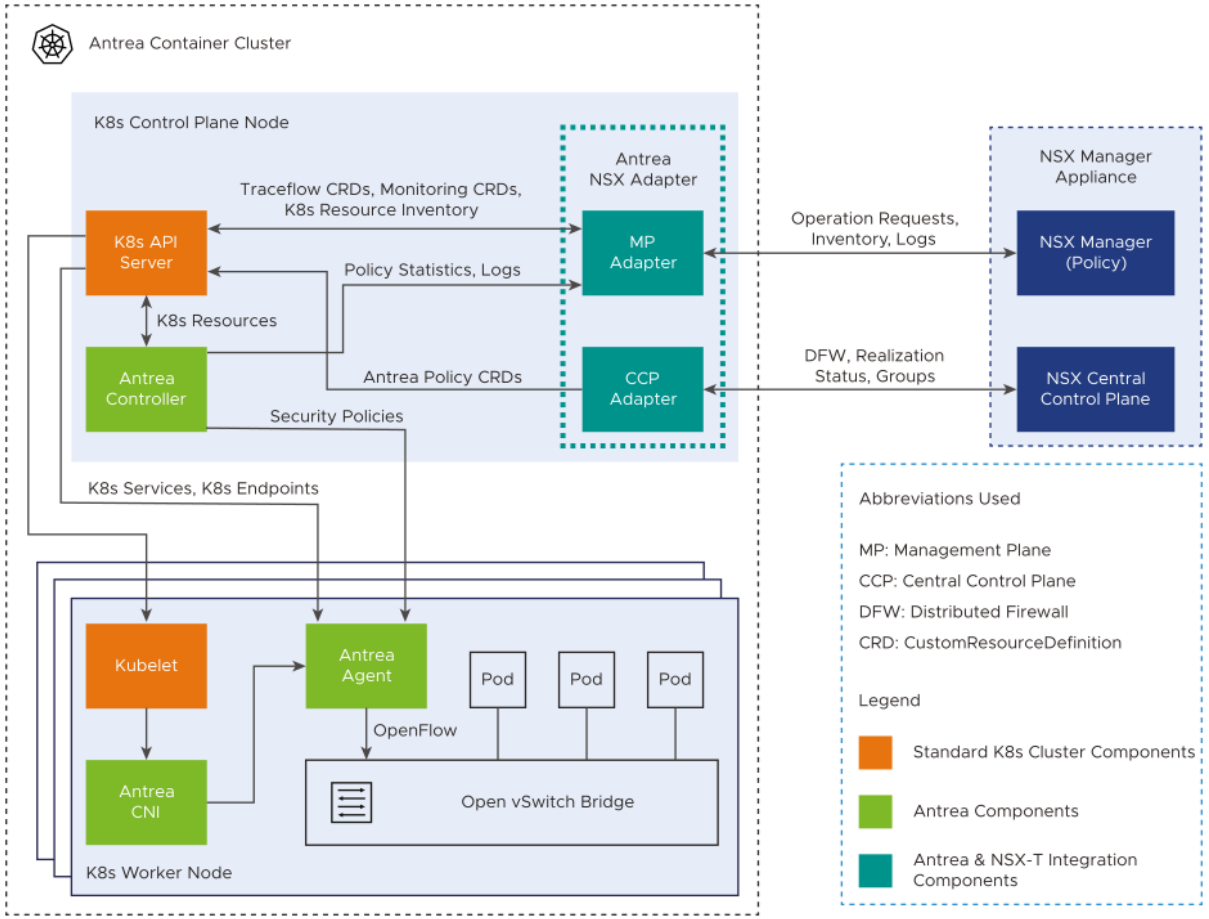


NSX Advanced Load Balancer

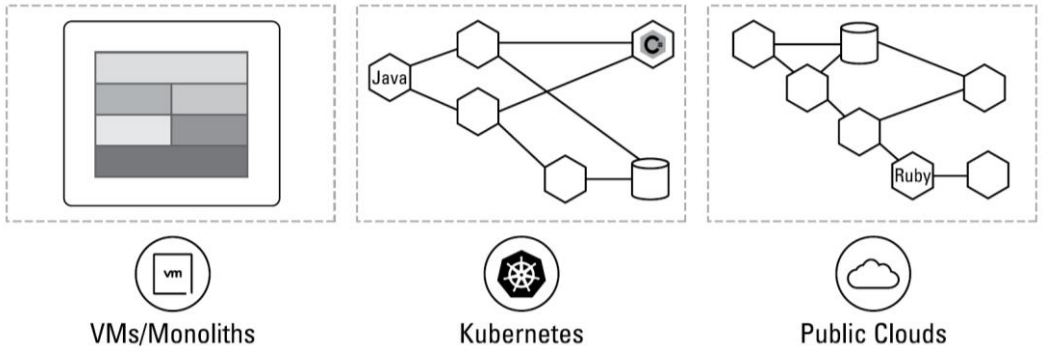


Integrace Tanzu a NSX-T Datacenter Networking

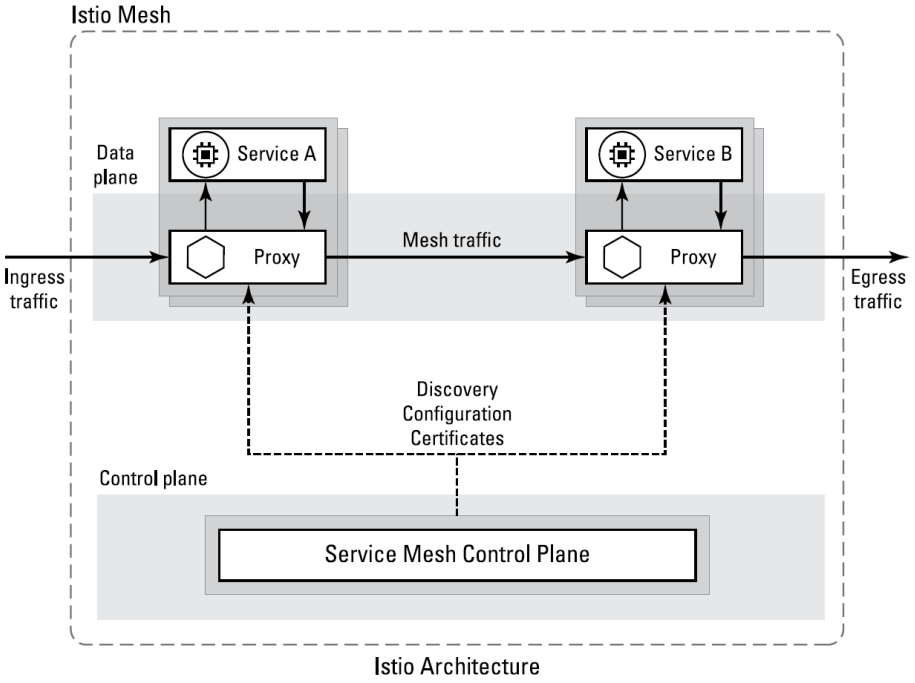
- Automatické vytvoření NSX síťového segmentu pro každý nový Tanzu cluster
- Automatické vytvoření a správa Tier1 routerů
- Integrace prvků distribuované bezpečnosti do prostředí Tanzu (např. firewall)
- Možnost využití K8s objektů přímo v NSX Manageru
  - Pods, Ingress, Services, Network Policies, Namespaces, Nodes
- Snadný dohled a logování síťové komunikace



Security and Networking



Istio



Istio Architecture

Vzájemná komunikace mnoha služeb v různých clusterech v různých sítích vyžaduje nový přístup k zajištění jak celkové funkčnosti, tak bezpečnosti.

Service Mesh

- **Service Discovery and Routing**
  - Zajištění bezproblémové komunikace mezi clustery

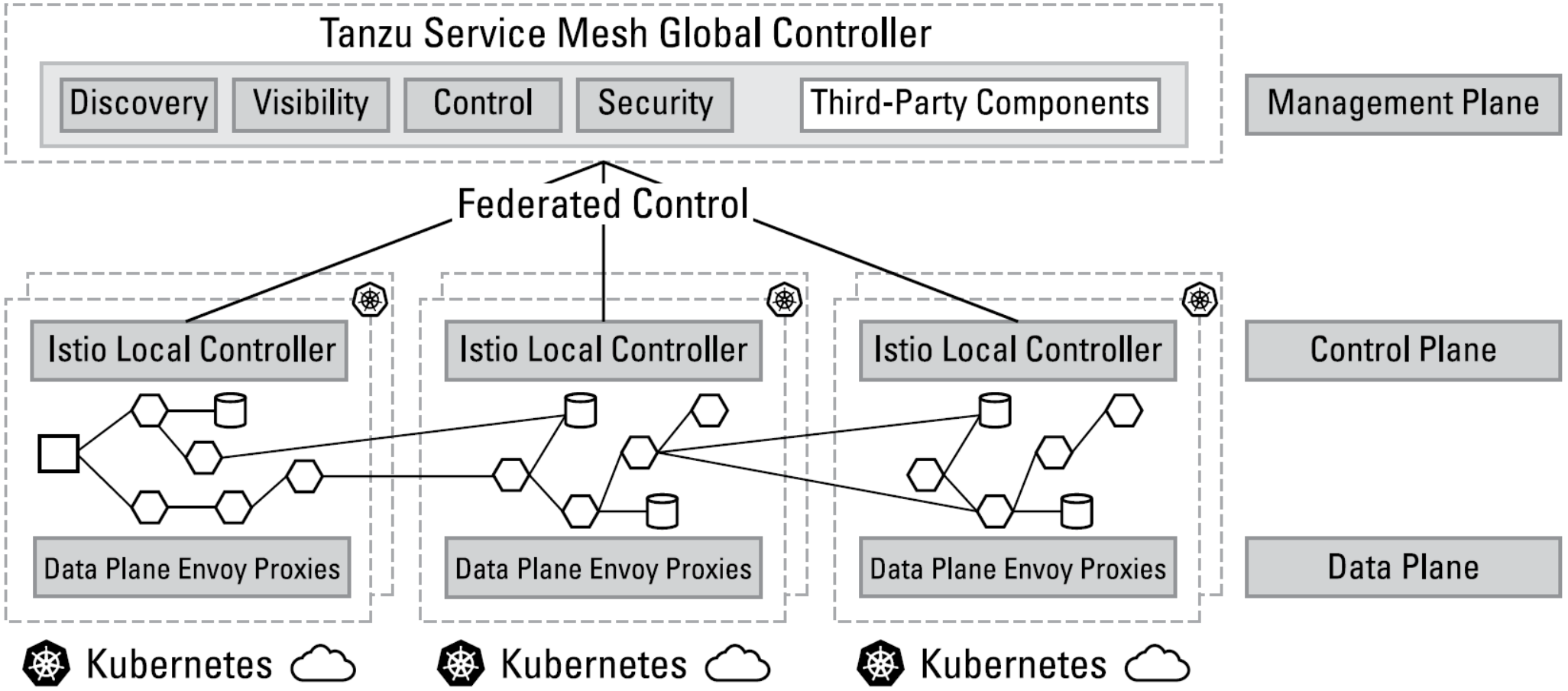
- **Observability**
  - Sběr metrik souvisejících s komunikací různých služeb
  - Tracing komunikace mezi službami

- **Availability and Resiliency**
  - Řízení provozu v závislosti na definovaných SLO
  - Auto-remediace běžných chyb – opakování požadavků, deaktivace nefunkčních instancí
  - Granulární řízení provozu

- **Bezpečnost**
  - Řízení komunikace mezi různými službami
  - Realizace bezpečné komunikace bez nutnosti jejího programování, např. šifrování

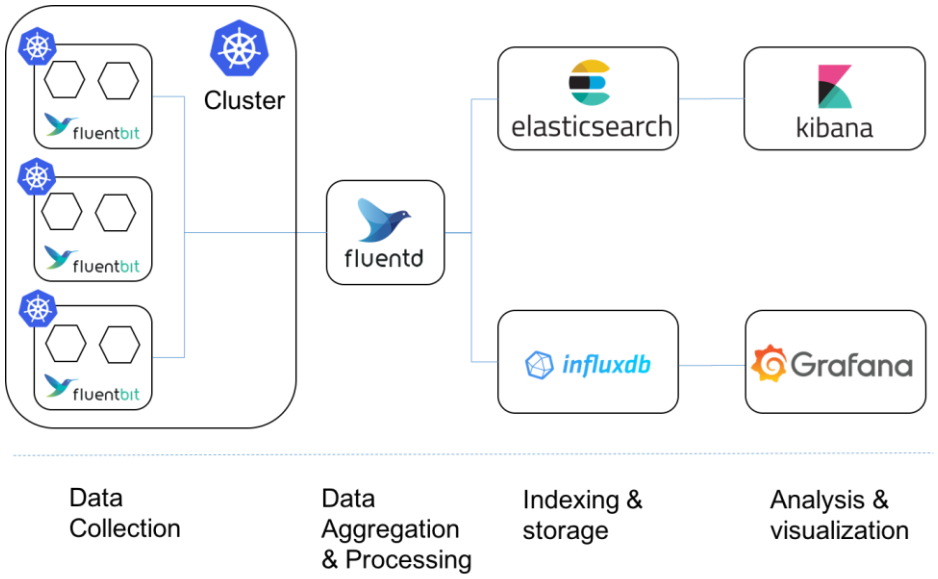
GAPP SYSTEM

Tanzu Service Mesh



Ukládání a správa logů

- **Centrální logování je v prostředí kontejnerů extrémně důležité**
  - Pody vznikají a zanikají
  - Služby běží ve více instancích
- **Nástroje pro sběr logů**
  - Umísťují se na jednotlivé nody clusteru
  - fluentd, fluentbit, filebeat, …
- **Nástroje pro centrální ukládání logů**
  - Udržují veškeré logy a umožňují přístup k nim
  - Elasticsearch + Kibana
  - VMware Log Insight

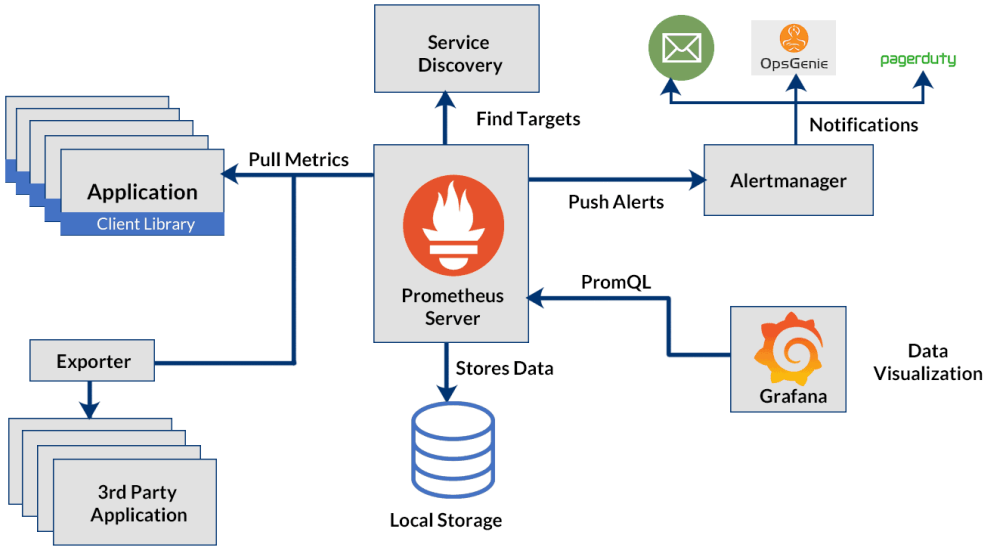


Sledování a prezentace metrik

- **Metriky poskytují rychlou a jasnou informaci o fungování systému**
  - Kvantitativní vyjádření sledovaných událostí/stavů (počet chyb, počet požadavků, …)
  - Vývoj hodnoty metriky v čase umožňuje analyzovat chování systému
  - Mohou být poskytovány Kubernetes platformou i samotnými aplikacemi

- **Nástroje pro sběr metrik**
  - Umísťují se na jednotlivé nody clusteru
  - Prometheus Exporter

- **Nástroje pro prezentaci a analýzu metrik**
  - Ukládají získané hodnoty a prezentují je
  - Prometheus Server + Grafana

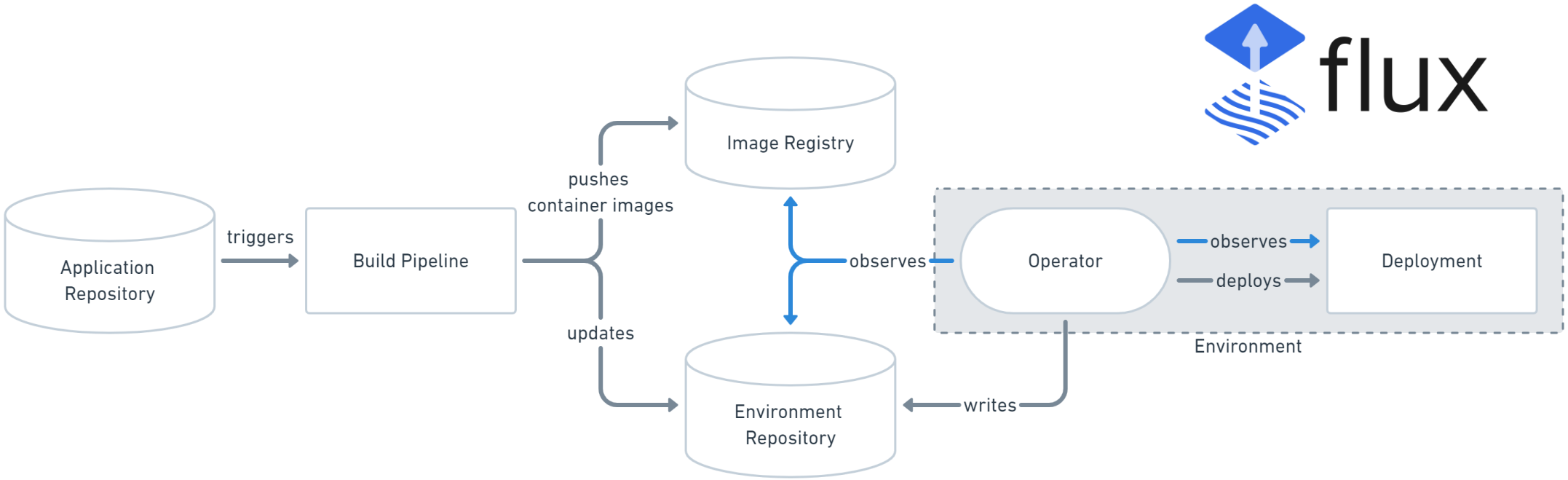


Řízení životního cyklu řešení

1. **Životní cyklus vlastní Kubernetes platformy**
   - Instalace a upgrady samotných Kubernetes clusterů
   - Zpravidla integrováno v samotných komerčních produktech
   - Automatizace životního cyklu K8s v on-premise prostředích
     - VMware Tanzu, RedHat OpenShift, SuSE Rancher, …
   - Automatizace životního cyklu v cloudových K8s prostředích
     - AWS EKS, GC GKE, Azure AKS, …

2. **Životní cyklus instalovaných softwarových komponent**
   - Instalace a upgrady komponent, které jsou využívány reálném produkčním nasazení
   - Z dnes diskutovaných např.: NSX ALB, Istio, Elastic, Prometheus Server, Fluentbit, Grafana, …

Životní cyklus komponent s využitím Flux

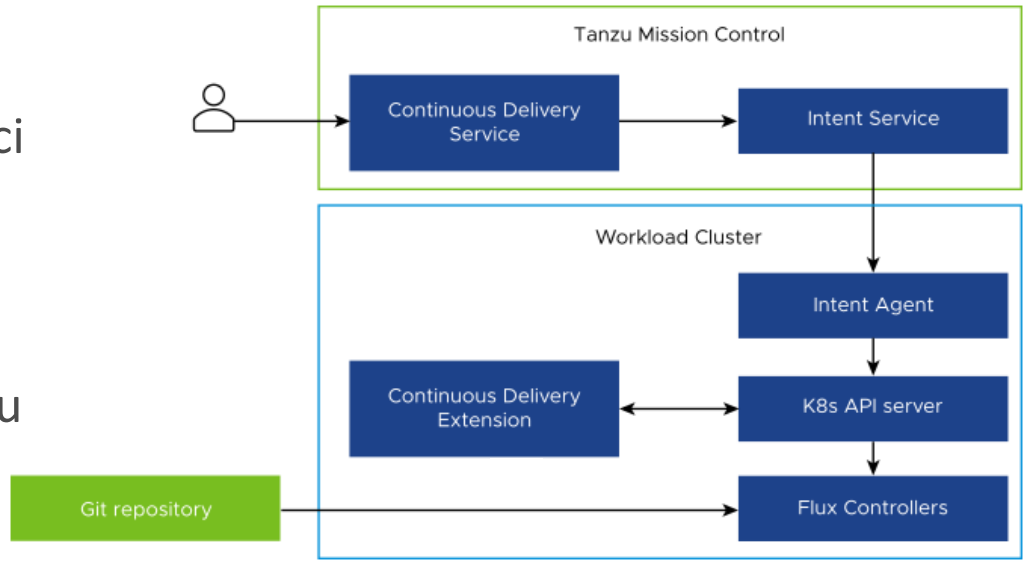


1. Aktualizace definic požadovaného stavu.
2. Uložení do „Environment Repository“.
3. Flux zajistí synchronizaci definic a skutečného stavu

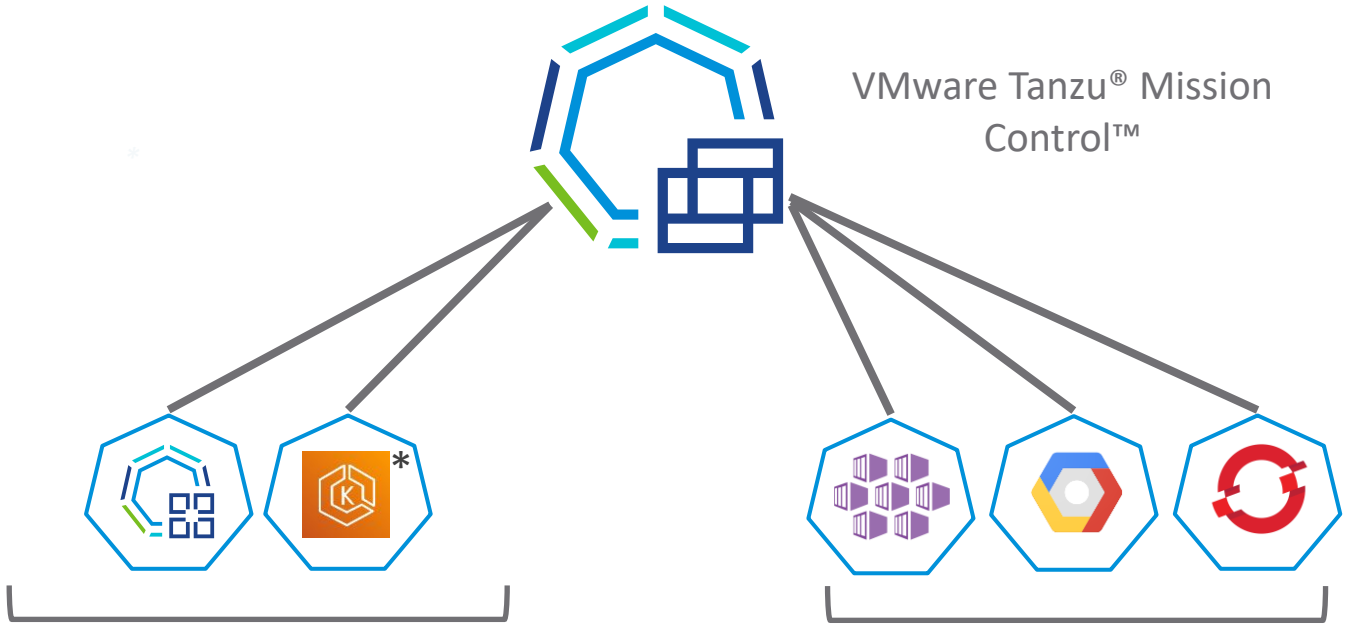
Tanzu Mission Control (TMC)

- **Automatizace životního cyklu instalovaných komponent**
  - TMC řídí celý proces a spravuje instalaci Flux na jednotlivých clusterech
  - Flux zajišťuje synchronizaci definic a jejich aplikaci

- **Princip fungování**
  1. Konfigurace Git Repository v TMC
  2. Povolení Continuous Delivery na daném clusteru
  3. Automatická instalace Flux komponent na daný cluster
  4. Flux zajistí synchronizaci definic mezi Git Repository a vlastním clusterem a uvedení do souladu



Tanzu Mission Control



Vlastnosti

Jednoduchý a unifikovaný management na všech typech podporovaných K8s clusterů:

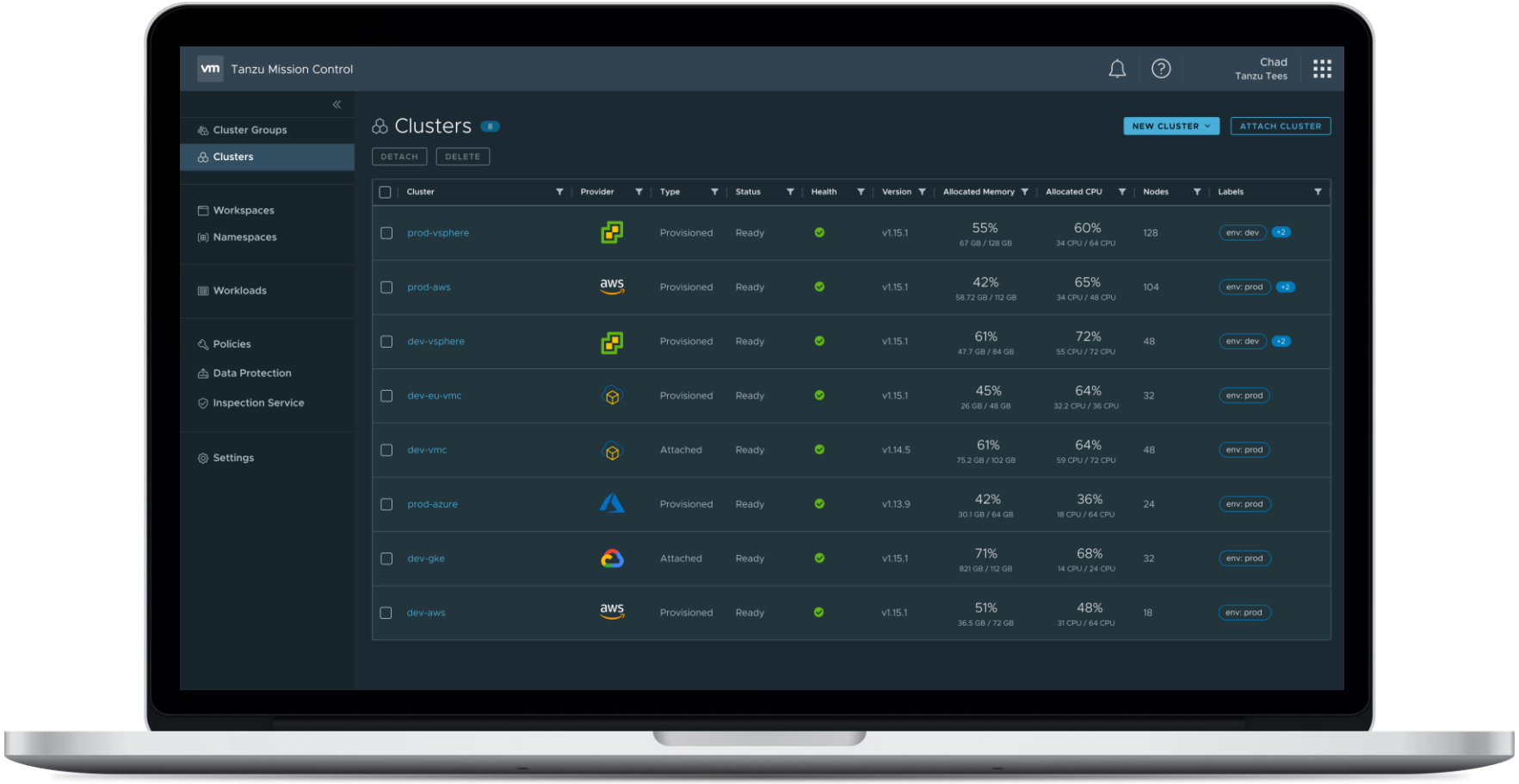
- Vysoká míra bezpečnosti
- Lepší přehled o prostředí
- Správa nákladů
- Monitoring stavu clusterů
- Sjednocení politik a kvót

Přínosy

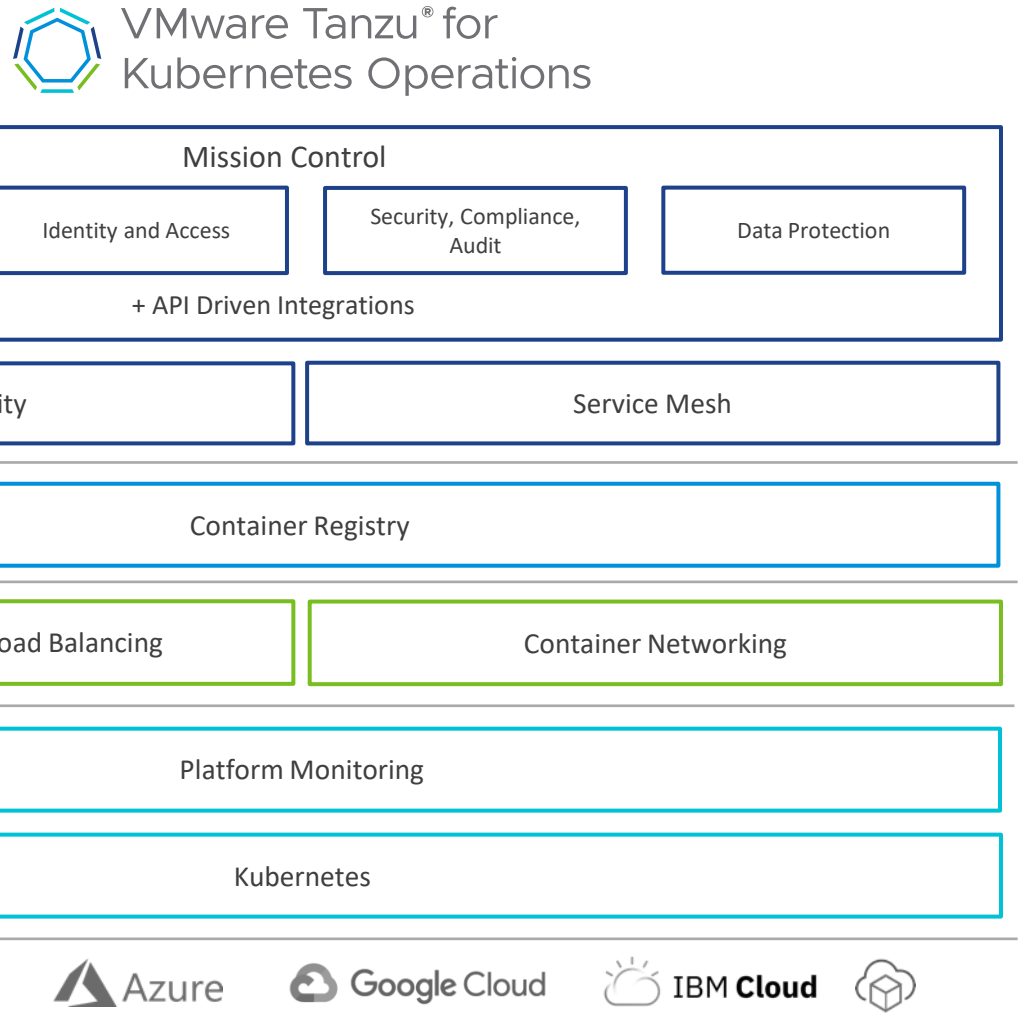
Konsistentní pravidla v rámci všech provozovaných prostředí výrazně usnadňují spolupráci a zvyšují agilitu.

Unifikace nastavení zlepšuje přehled a zajišťuje opakovatelnost u dalších prostředí.

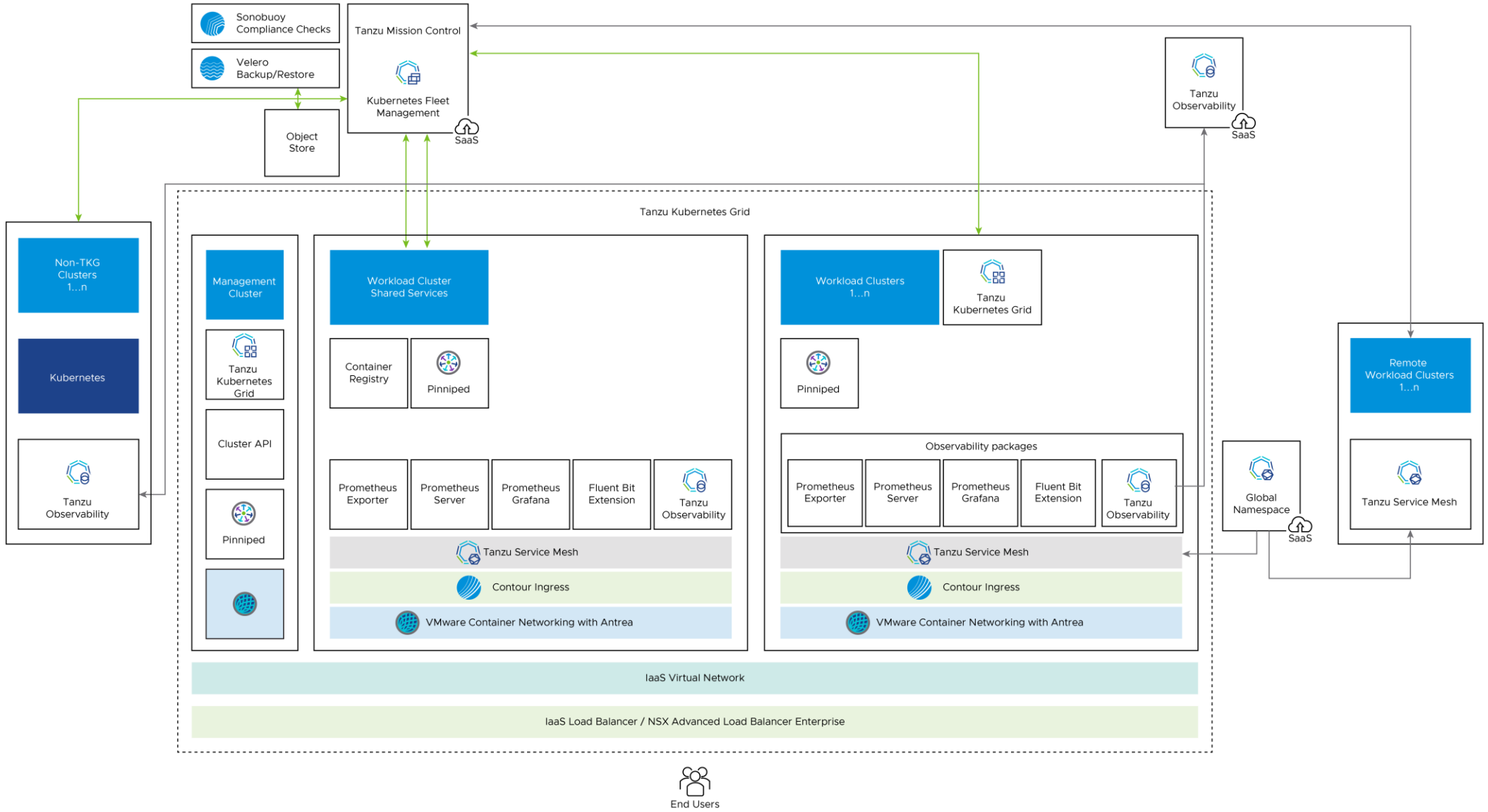
Tanzu Mission Control



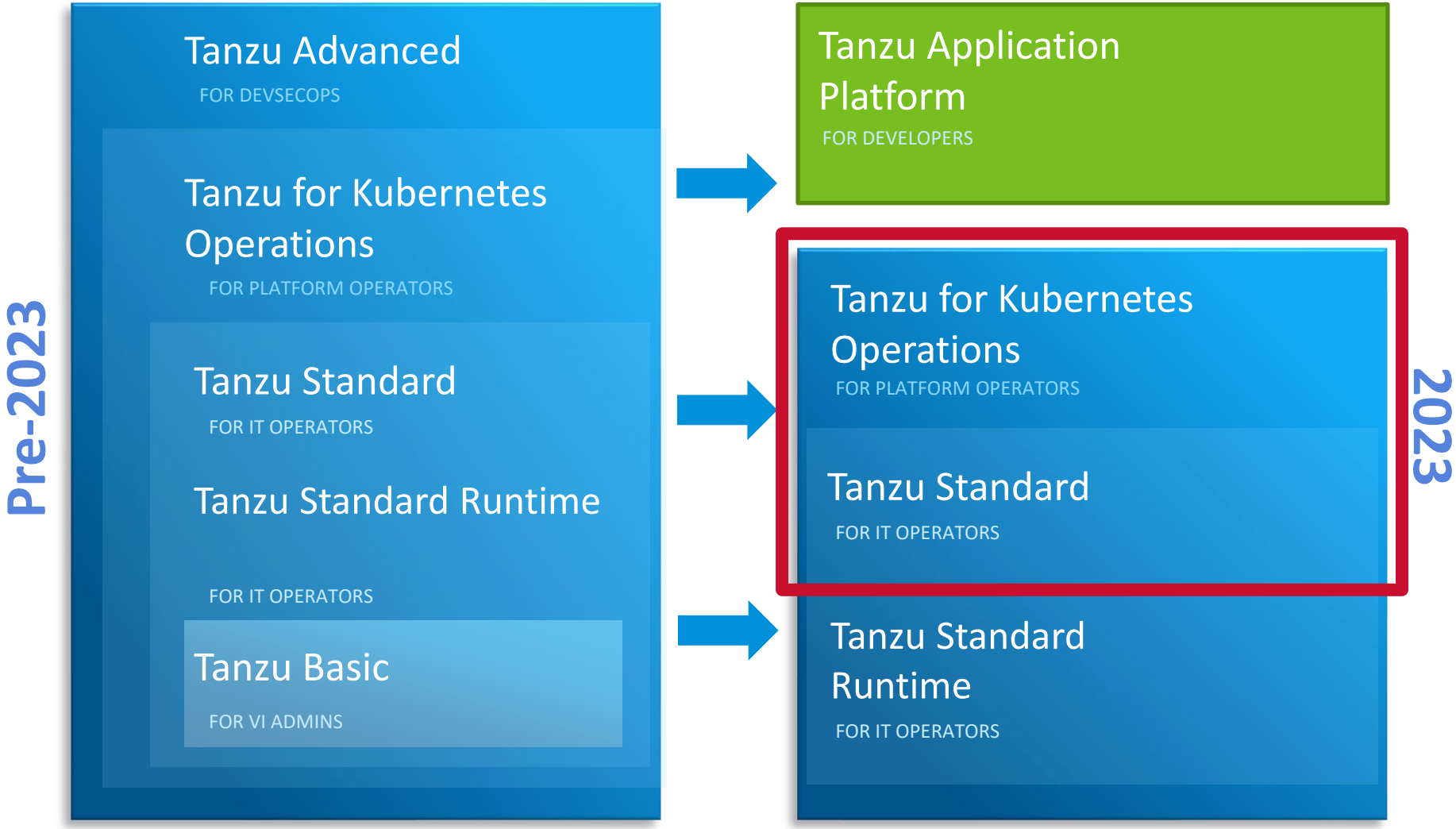
Kubernetes v reálném nasazení



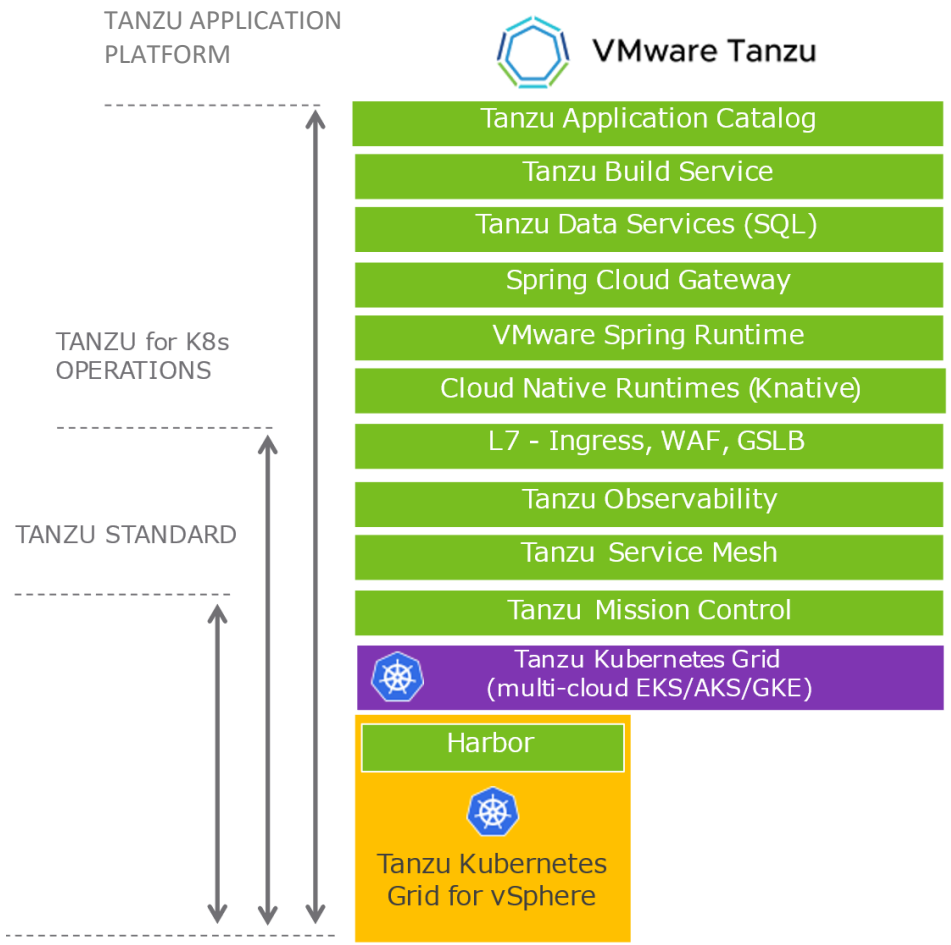
Tanzu for Kubernetes Operations – referenční architektura



VMware Tanzu – licenční edice



VMware Tanzu – obsah licenčních edicí



Proč zvolit řešení VMware Tanzu?

1. **Plná integrace do platformy datového centra VMware.**
2. **Široká škála předpřipravených a integrovaných nástrojů K8s světa.**
3. **Automatizace životního cyklu celého řešení.**

SIMPLIFY • SECURE • OPTIMIZE

GAPP SYSTEM

Děkujeme za pozornost.