Kubernetes bez internetu

Co všechno přestane fungovat,
když opravdu odpojíte kabel



Presenter: Ing. Ondřej Dohnal
Date: 08. 11. 2026

Cluster běží. Co se stane po odpojení?

- Běžící workload není důkaz, že zvládneme další nasazení.
- První zkouška: restart podu, nový node a instalace aplikace.
- Druhá zkouška: aktualizace a obnova po havárii.



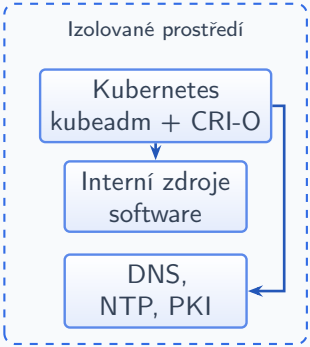
Běžící pod může fungovat dál. Další operace může potřebovat externí zdroj.

První past

Cache může skrýt chybějící závislosti.

Hranice offline prostředí

- Které sítě a služby jsou dostupné uvnitř izolovaného prostředí?
- Jak se dovnitř dostává software a kdo schvaluje jeho přenos?
- Výchozí stack přednášky: kubeadm a CRI-O.



Cesta přednáškou

01 / Instalace

Container images, systémové balíčky a Helm charty.

02 / Provoz

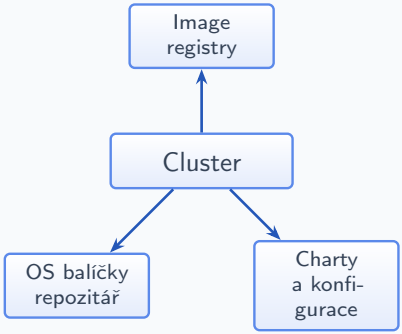
DNS, čas, důvěra, monitoring a licence.

03 / Životní cyklus

Deployment artifact, aktualizace a test odpojení.

Vlastní registry je jen část řešení

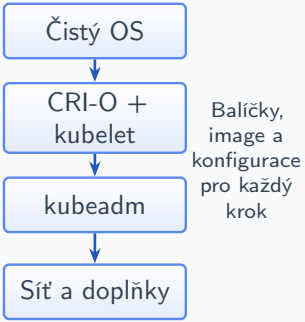
- Container images jsou jedna z vrstev dodávky.
- Nody potřebují také OS balíčky a jejich závislosti.
- Charty, konfigurace a provozní služby mají vlastní zdroje.



Registry není kompletní dodávka.

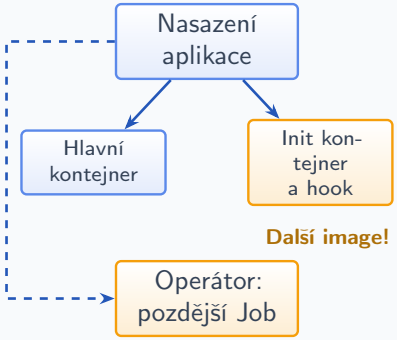
Bootstrap: kubeadm a CRI-O

- Připravit instalační balíčky i konfiguraci pro konkrétní verze.
- Sjednotit zdroje image pro control plane, runtime a doplňky.
- Ověřit start na čistém nodu bez předchozí cache.



Image, které v prvním seznamu chybí

- Vedle aplikace prověřit init kontejnery a instalační hooky.
- Zahrnout image používané operátory a pozdějšími úlohami.
- Zaznamenat původ, digest a cílové umístění každé image.

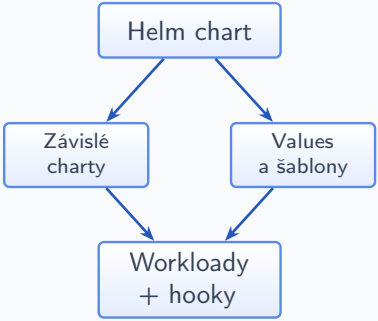


Skrytá závislost

Image může být potřeba až při další operaci.

Offline repozitáře a Helm

- Přenést uzavřenou sadu balíčků včetně metadat a klíčů.
- Přibalit charty, jejich závislosti a hodnoty pro dané prostředí.
- Prověřit i skripty a hooky, které mohou stahovat další obsah.



DNS a čas uvnitř izolované sítě

DNS / kam se obracíme

Interní zóny a resolvery.

Definované chování pro externí jména.

NTP / jaký je čas

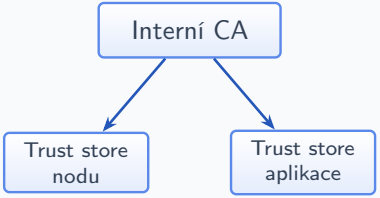
Interní zdroj času.

Postup při jeho výpadku a při obnově nodu.

Restart a obnova musí fungovat s dostupnými interními službami.

PKI a distribuce důvěry

- Dostat interní CA na nody i do aplikací, které ji potřebují.
- Popsat vydávání, obnovu a výměnu certifikátů.
- Prověřit externí služby používané při ověřování certifikátů.



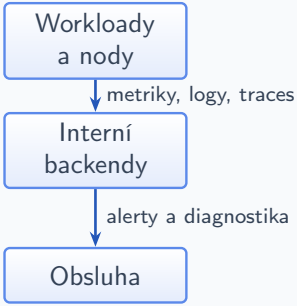
Vydání certifikátu a distribuce důvěry jsou dva samostatné úkoly

Dvě různé věci

Vydaný certifikát ještě neznamená, že mu aplikace důvěřuje.

Observability bez externího backendu

- Určit, kde zůstávají metriky, logy a traces.
- Prověřit cíle exportérů, alertů a notifikací.
- Zajistit diagnostiku i při výpadku interní registry nebo DNS.



Licence a další externí služby

- U každého produktu ověřit podmínky offline aktivace a obnovy.
- Prověřit přihlášení, telemetrii a automatické aktualizace.
- Zaznamenat časová omezení a postup při nedostupnosti služby.

Co se stane po vypršení licence?

Kompletní deployment artifact

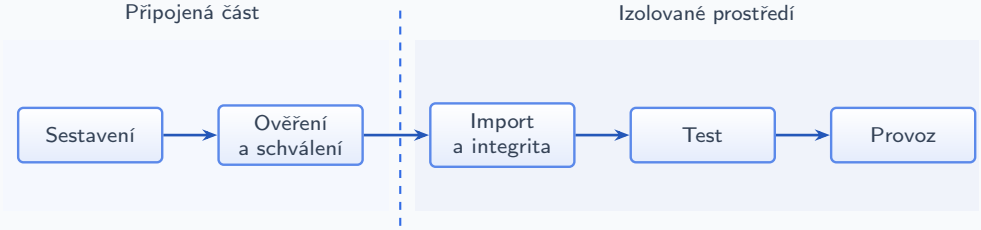
- Obsah: balíčky, image, charty, konfigurace a instalační postup.
- Manifest verzí, digesty, původ a podklady pro ověření integrity.
- Jedno vydání musí obsahovat vše pro deklarované cílové prostředí.



Cíl dodávky

Stejné vydání. Opakovatelné nasazení.

Cesta vydání přes hranici prostředí

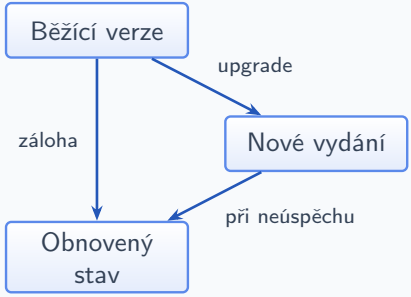


Přes hranici putuje identifikované vydání; způsob přenosu určuje prostředí

- Připravit a ověřit obsah v připojené části.
- Schválit přenos a ověřit integritu po importu.
- Nasadit stejnou identifikovanou sadu do testu a následně do provozu.

Aktualizace a obnova

- Dodat nové vydání včetně všech změněných závislostí.
- Otestovat upgrade a postup obnovy při neúspěchu.
- Uchovat předchozí artefakty a ověřené zálohy potřebné k obnově.



Záloha potřebuje ověřený postup obnovy.

Zkouška se skutečně odpojeným internetem



Zachytit a vysvětlit pokusy o externí komunikaci v každém kroku

- Čistý node: instalace, připojení do clusteru a nové nasazení.
- Provoz: restart, škálování a obnova certifikátů.
- Životní cyklus: upgrade a obnova ze zálohy.
- Sledovat pokusy o externí komunikaci a vysvětlit každý z nich.

Co můžu udělat lépe?

Od první instalace k ověřené obnově bez internetu

Na co si dát pozor?

Na co si dát pozor

- **Warm cache**: běžící pod skryje chybějící image.
- **Neúplná dodávka**: chybí hook, balíček nebo závislý chart.
- **Externí služby**: DNS, čas, ověření licence či identity.
- **Neověřená obnova**: záloha existuje, postup není vyzkoušený.

Co můžu udělat lépe

- **Sepsat závislosti**: včetně těch použitých až později.
- **Uzavřít vydání**: verze, digesty, konfigurace a původ.
- **Zajistit interní služby**: včetně důvěry a obnovy certifikátů.
- **Odpojit a ověřit**: čistý node, upgrade i obnova.

Závěr: Co si odnést?

Kompletní dodávka

Image, balíčky, charty i konfigurace patří ke stejnému vydání.

Identita vydání

Známe verze, digesty a původ jednotlivých závislostí.

Ověřený životní cyklus

Nasazení, aktualizace a obnova fungují i bez internetu.

Běžící cluster ještě neznamená obnovitelný cluster.

Air-gapped Kubernetes je především práce se software supply chainem.

Děkuji za pozornost

Otázky & diskuse

Ing. Ondřej Dohnal
GINA Software s.r.o.