TSP DATA

6.10.2026

Red Hat Innovate Together 2026

Business mimo DC, aneb jak do EDGE

Martin Klčovský | https://www.linkedin.com/in/mklcovsky/

martin.klcovsky@tspdata.cz

Jsme TSP DATA

Naší specializací je automatizace, observabilita, budování, správa a zabezpečení DevOps stacků.



Online



Secured



Everywhere

Co umíme

Specializujeme se na automatizaci, kontejnerizaci, virtualizaci a bezpečnost.

S Red Hatem, HashiCorpem, Isovalentem a Portworxem budujeme infrastrukturu, která obstojí v regulovaném prostředí – s plným pokrytím security hardeningu, správy certifikátů a síťové bezpečnosti na úrovni kernelu díky eBPF.

Každé nasazení je řízené kódem, verzované a opakovatelné. Žádná ruční práce, žádné překvapení při auditu.

Co dodáváme

Manažerské dashboardy poskytující okamžitý přehled o dostupnosti a spolehlivosti kritických systémů.

Detailní bezpečnostní a komunikační mapy urychlující řešení incidentů, odhalující rizika dříve, než se projeví, a podporující kapacitní plánování v souladu s požadavky regulátora.

Infrastrukturu stavíme na Kubernetes s plnou automatizací – škálovatelně, opakovatelně a bez závislosti na manuálních zásazích.

Co vyřešíme | IIT

DevOps a GitOps – jedeme Ansible a OpenShift – kompletní DevOps a GitOps. Jsme znalí, máme reálné zkušenosti i certifikace.

Secrets a Certifikáty – jedeme Vault – automaticky a bezpečně. Hashujeme secrets, píšeme IaC, budujeme autority... certifikační.

CNI/SDN – jedeme eBPF – v Kubernetes bezpečně. A vidíme to, co jiní přehlídnou.

Data – jedeme objekt, file i blok, šifrujeme data, škálujeme výkon.

TSP DATA 25 let díky vám

Red Hat HashiCorp ISOVALENT portworx by Everpure

Success driven by data.

Jsme TSP DATA

Naší specializací je automatizace, observabilita, budování, správa a zabezpečení DevOps stacků.



Online



Secured



Everywhere

Co umíme

Specializujeme se na automatizaci, kontejnerizaci, virtualizaci a bezpečnost.

S Red Hatem, HashiCorpem, Isovalentem a Portworxem budujeme infrastrukturu, která obstojí v regulovaném prostředí – s plným pokrytím security hardeningu, správy certifikátů a síťové bezpečnosti na úrovni kernelu díky eBPF.

Každé nasazení je řízené kódem, verzované a opakovatelné. Žádná ruční práce, žádné překvapení při auditu.

Co dodáváme

Manažerské dashboardy poskytující okamžitý přehled o dostupnosti a spolehlivosti kritických systémů.

Detailní bezpečnostní a komunikační mapy urychlující řešení incidentů, odhalující rizika dříve, než se projeví, a podporující kapacitní plánování v souladu s požadavky regulátora.

Infrastrukturu stavíme na Kubernetes s plnou automatizací – škálovatelně, opakovatelně a bez závislosti na manuálních zásazích.

Co vyřešíme | MIT

Full-stack observabilitu - End-to-end trasování požadavků napříč mikroslužbami, databázemi a externími API na základě OpenTelemetry. Sjednocený pohled na metriky, logy a traces zkrátí MTTR a sníží počet eskalací.

Monitoring celého stacku - Servery, VM, kontejnery, sítě, cloudové prostředí, aplikace, vše přehledně v jedné platformě. Incidenty vyřeší automatizace dříve, než začnou mít dopad na uživatele.

FinOps optimalizaci a forecasting - Identifikujeme předimenzované, nebo nevyužité zdroje, propojíme IT výdaje s business KPI a nastavíme kapacitní plánování s výhledem na měsíce dopředu.

Viditelnost IT nákladů - Alokujeme náklady na infrastrukturu na úroveň procesu, aplikace, business jednotky nebo zákazníka. Hybridní model pokrývá cloud i on-prem bez slepých míst. Výsledkem jsou lepší rozpočtová rozhodnutí, ne jen škrty.

TSP DATA 25 let díky vám

aws

dynatrace

Grafana Labs

ZABBIX

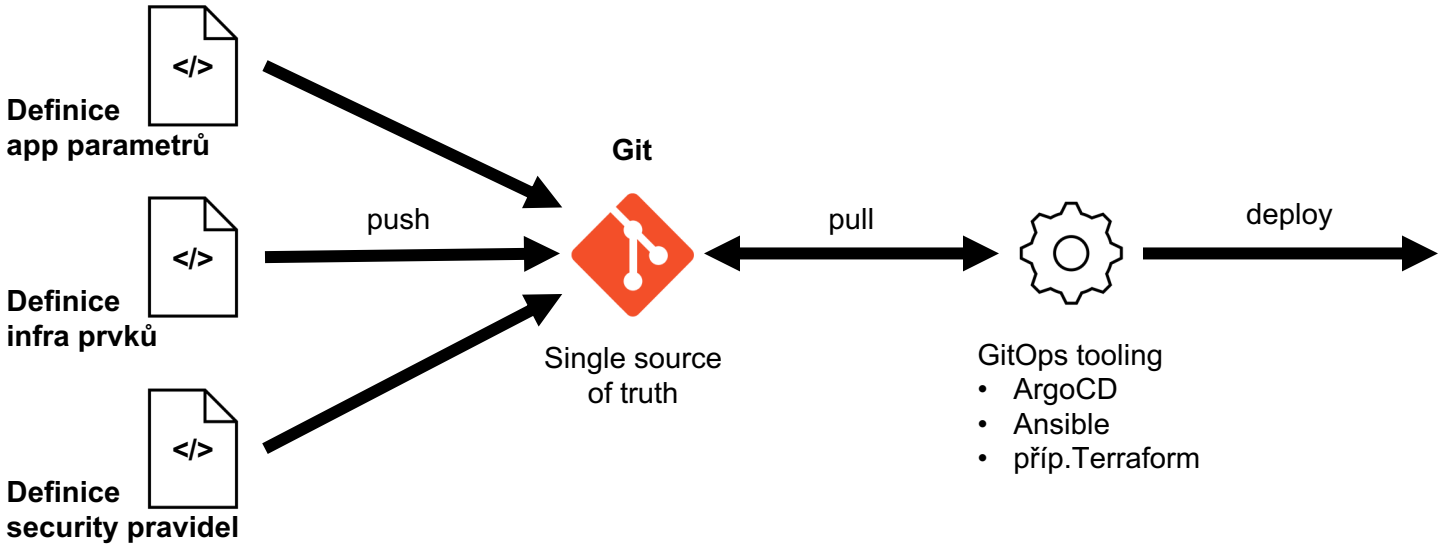
Success driven by data.

#GitOps

“S automatizací na věčné časy a nikdy jinak."

#GitOps = SECURITY

Automatizační koncepce



- **Konfigurace konkrétní aplikace**
- **Konfigurace konkrétního switche**
- **Rozšíření volumu na všech úrovních**
- **Přidání komunikačního pravidla**
- **Upgrade firmware konkrétní komponenty**
- **Obnova konfigurace ze zálohy**

Cílem je zbavit se opakujících se úloh, mít přímočaré DR, jasný standard a BEZPEČNÉ PROSTŘEDÍ.

#EDGE

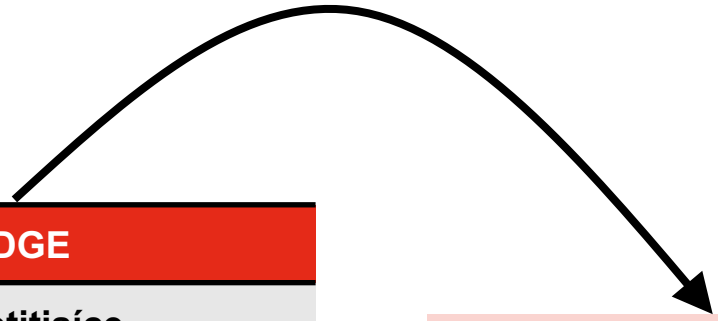
Co je to?

„Chci zpracovat data tam, kde vznikají – ve fabrice, na prodejně, benzince, v trafice, ve vlaku, rozvodně nebo třeba větrné elektrárně."

#EDGE

Co říká teorie?

#server #kiosek #shopfloor #rozvodna #bankomat #pokladna #VM



	DC	EDGE
Počet lokalit	Jednotky	**Stovky až desetitisíce**
Prostředí	Klimatizovaný sál, stabilní napájení	Prach, teplo, vibrace, výpadky proudu, psychicky labilní obsluha
Hardware	Výkonné servery	**Malá zařízení, omezené zdroje**
Konektivita	Rychlá a redundantní	**Omezená, nestabilní**
Fyzický přístup	Přísně chráněný	Často dostupné komukoli
IT personál	Na místě	Žádný
Správa	Centrální, ruční zásahy možné	**Vzdálená a automatizovaná**

→ **výjezdy techniků**

→ **nestabilní konektivita**

→ **roztříštěná správa**

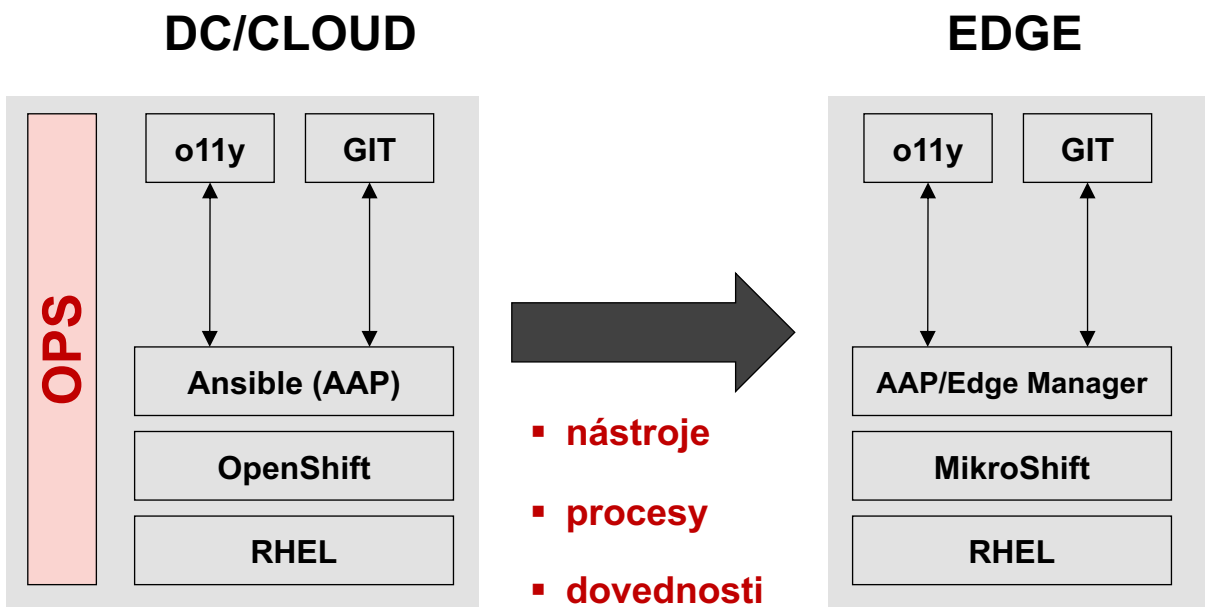
→ **bezpečnostní rizika**

„Jak spolehlivě a bezpečně spravovat tisíce zařízení?"

„Jak do EDGE spolehlivě a bezpečně distribuovat aplikace?"

#EDGE

Co je ideální stav?



- nástroje
- procesy
- dovednosti

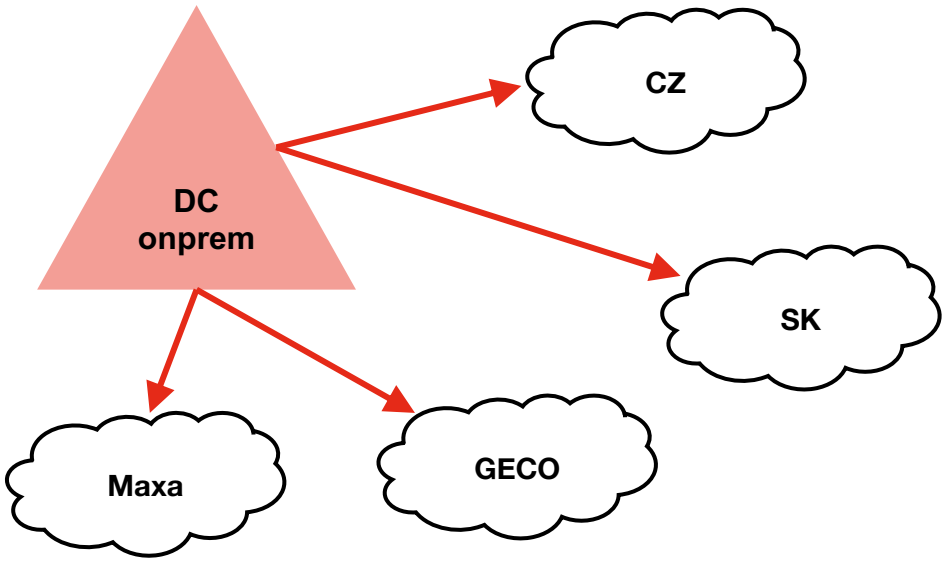
→ konzistence

- Zero-touch provisioning
- Automatický rollback
- Nízké nároky na HW a provoz i při výpadku konektivity
- Bezpečnost – image-based systém
- DevOps/GitOps praktiky

#Customer story

„Chci plně automatizovat provisioning a správu svých pobočkových terminálů na více jak 1200 místech. Chci mít přehled o dostupnosti a zdraví poboček, možnost vzdáleného troubleshootingu a z pohledu sítě všude any-any/deny pro incoming provoz."

#As is



#různé_terminály #různé_konfigurace

#různé_business_funkce

#debian #skripty #ad-hoc_update

#omezená_škálovatelnost

#nejednotnost #dost_manuální_správa

#Zadání

Umožnit kompletní správu zařízení včetně konfigurace, aktualizací a monitoringu.

Zajistit maximální míru automatizace během celého životního cyklu zařízení.

Podporovat zero-touch provisioning pro nově nasazovaná terminálová zařízení.

Umožnit jednotnou konfiguraci poboček pro dosažení provozní efektivity.

Minimalizovat manuální zásahy při migraci stávajících Debian terminálů na Red Hat Enterprise Linux for Edge.

Vytvořit základ pro dlouhodobou udržitelnost, bezpečnost a rozšiřitelnost pobočkové sítě.

#As is

#security #infra #provoz #vývoj

Krok 0
OS a balíčky

- bootc
- Containerfile
- web (ne GIT)
- interní skripty při sestavování image
- publikace do Nexusu
- bez skenování zranitelností

Krok 1
Instalace na terminály

- manuální instalace bootc install
- PXE/Kickstart
- pull z Nexusu
- Konfigurace z https
- manuální nasazování certifikátů

Krok 2
CI/CD pipelines

- GitLab CI/CD
- sestavení image a push do Nexusu

Krok 3
Centrální správa

- AAP based
- základní architektura a záměr
- post-install config
- správa SW skladby
- mas updates
- automatizovaný maintenance a change

Krok 4
Cokoliv dalšího

- 2 VPN (servisní a provozní)
- neznámá inventarizace
- neznámý monitoring
- neznámý update management
- neznáme security požadavky
- neznámý life-cycle terminálů

Vhodně rozpracovaný systém na sestavení OS image

Směr k plné automatizaci

Security
Life-cycle
Integrace

#Projektová mezihra

#security #infra #provoz #vývoj

Řízení lidí

- 4 týmy + dodavatel
- as-is workshop
- změny architektury i komponent
- konfigurační změny
- „kafrání do procesů“

Kolaborace

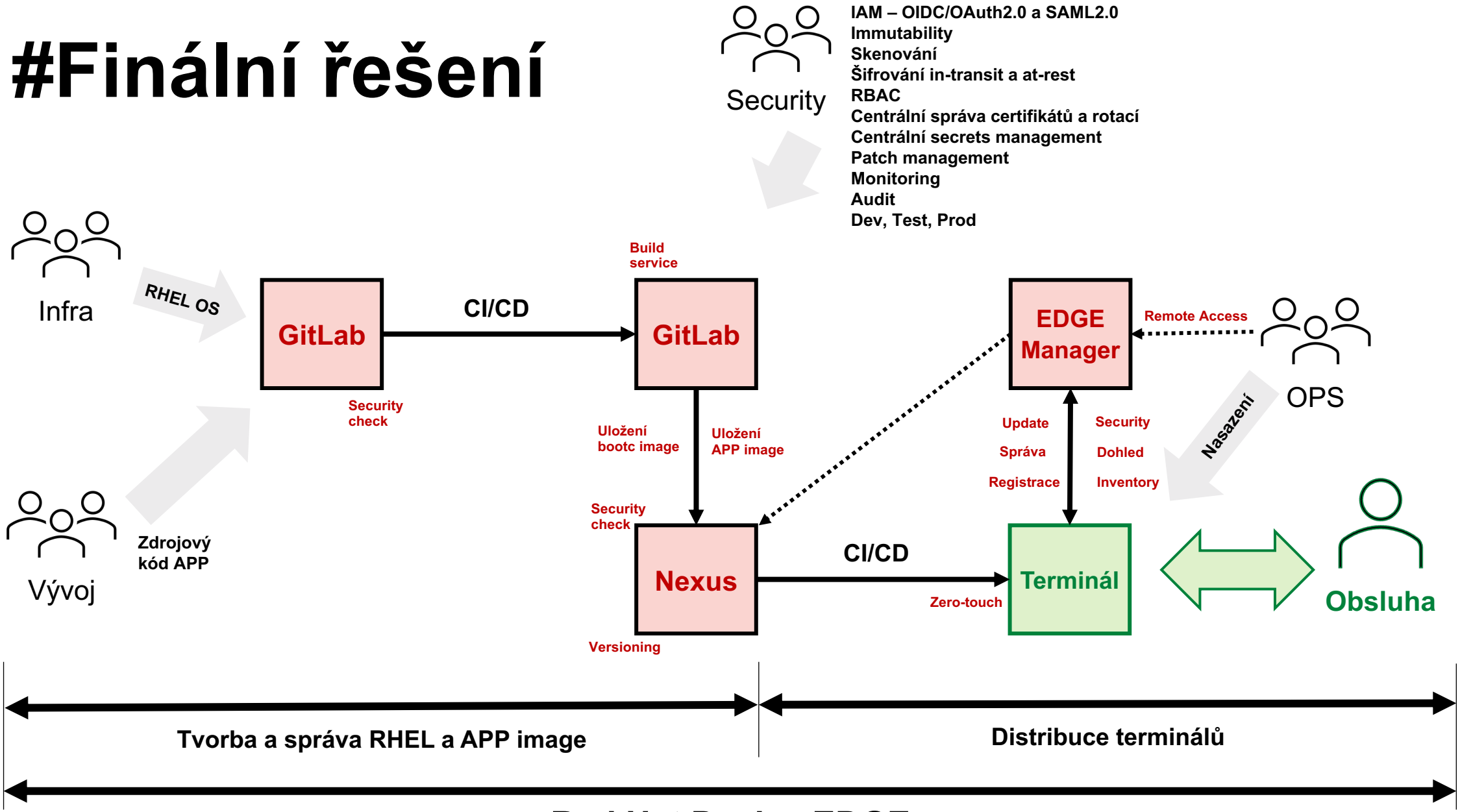
- pravidelné statusy/stand-ups
- dokumentace stavu
- udělat funkční tým a vytvořit důvěru

Časování

- assessment 4 týdny
- pilot 2 měsíce
- produkce 6 měsíců
- jedeme dál... ☺

Legenda: DC, EDGE

#Finální řešení



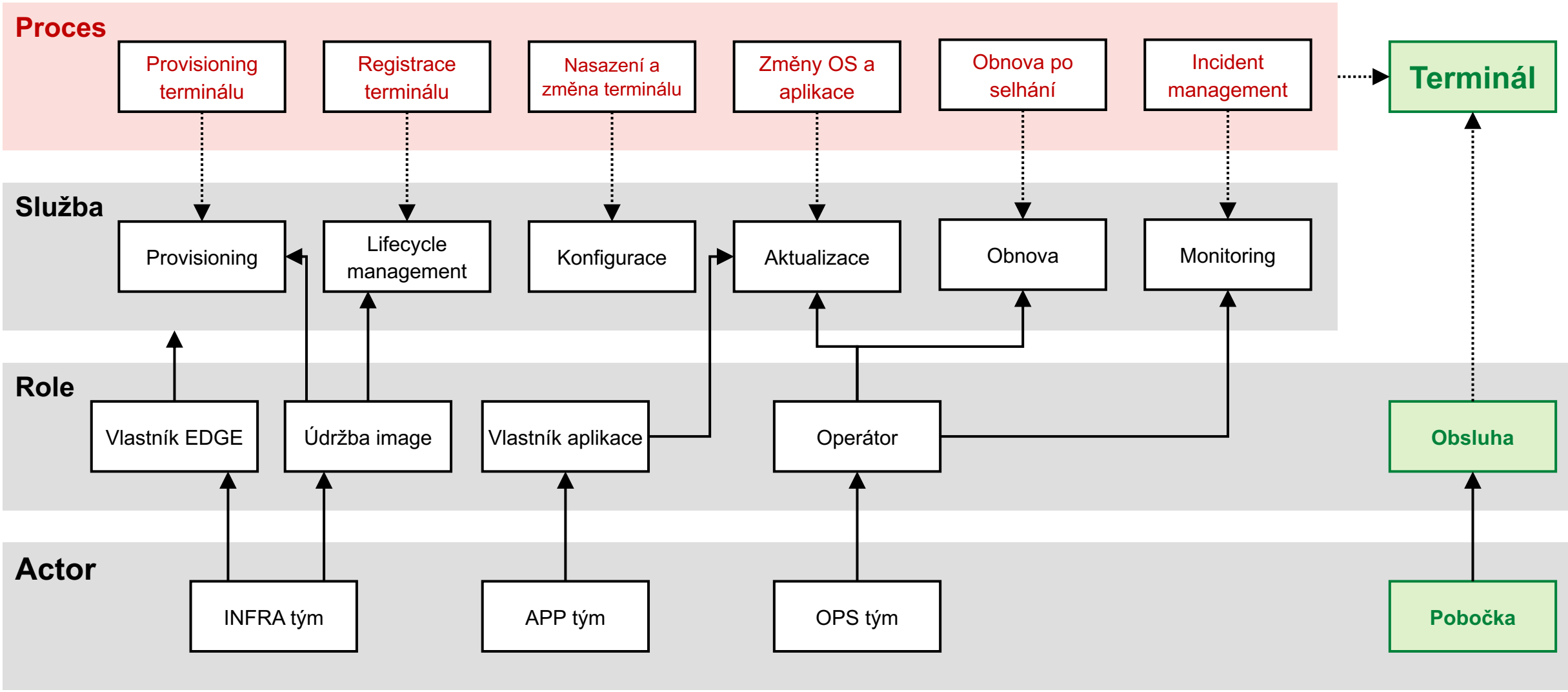
Red Hat Device EDGE

(RHEL + MicroShift + Edge Manager)

#Architektura

„Pro fajnšmekry – nejspíš nám nezbývá čas, vyřeší to kluci na stánku."

#Business architektura



#Security architektura

Bezpečnostní principy řešení

- centrální řízení identit, přístupů, klíčů i aktualizací
- zero trust – nic není důvěryhodné implicitně
- image-based security – immutabilní OS image
- Least privilige a RBAC – práva na základě rolí
- Auditovatelnost – vše je logováno a řízeno GitOps
- Oddělená prostředí – vývoj, test, produkce

Identita, autentizace a autorizace

- Autentizace uživatelů vůči IdP skrze SSO
- Jsou používány výhradně autentizační protokoly OIDC/OAuth 2.0 a SAML 2.0
- Nepoužívané built-in účty jsou deaktivovány
- Vynucovaná politika hesel

Zabezpečení OS bootc image a updaty

- Terminál běží na operačním systému Red Hat Enterprise Linux for Edge
- Aktualizace OS a aplikací řízeny centrálně a podporují rollback

Kryptografie, tajemství a šifrování

- Kryptografické klíče a certifikáty jsou centrálně spravovány, pravidelně rotovány a bezpečně obnovovány
- Terminály neobsahují statická tajemství v plain-textu
- Je nasazena centrální správa hesel, API klíčů a certifikátů
- Veškerá komunikace je šifrována
- Šifrování je v principech „in transit“ a „at rest“

Logování, audit a dohled

- Veškeré bezpečnostní a provozní události centrálně logovány
- Odesílány do existujícího SIEM
- Auditní logy zahrnují přihlášení uživatelů, změny konfigurací, provisioning a aktualizaci terminálů a bezpečnostní události

Provozní bezpečnost a governance

- Pro aplikace je definován businessový i technický vlastník
- Pro Red Hat Device Edge platformu a přidružené systémy existují DR plány a probíhají BCM testy
- Každá aplikace je zahrnuta do aplikačního monitoringu

#Cíle?

„Co ze zadání bylo naplněno?"

#High Level Cíle

Okénko business marketingu ☺

1. Rychlejší uvedení produktů na trh (Time-to-Market)

85%

2. Lepší využití infrastruktury a snížení nákladů

↓1/2

3. Podpora digitální transformace a modernizace aplikací

4. Zvýšení spolehlivosti a škálovatelnosti

...to je snad jasné!

...a samozřejmě i AI, protože Red Hat Lightspeed!

#Reálné Cíle

Umožnit kompletní správu zařízení včetně konfigurace, aktualizací a monitoringu.	**SPLNĚNO** EDGE MANAGER
Zajistit maximální míru automatizace během celého životního cyklu zařízení.	**SPLNĚNO** EDGE MANAGER + GitLab
Podporovat zero-touch provisioning pro nově nasazovaná terminálová zařízení.	**SPLNĚNO** PXE/Kickstart
Umožnit jednotnou konfiguraci poboček pro dosažení provozní efektivity.	**SPLNĚNO** EDGE Manager + bootc RHEL image
Vytvořit základ pro dlouhodobou udržitelnost, bezpečnost a rozšiřitelnost pobočkové sítě.	**SPLNĚNO** Standard – už ho jenom dodržovat... ☺

Co si odnést?

„Že EDGE odřídíte stejně jako kubernetes – DevOpsem a GitOpsem!"

#Losovačka o ceny







14:15
- **QR kód**

15:00
- **účast na AI ve 14:30 nutná ☺**

